ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ

(Τ.Ε.Ι.) ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ Μ.Μ.Ε.

(ΠΑΡΑΡΤΗΜΑ ΠΥΡΓΟΥ)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΚΑΣΤΙΚΑ ΘΕΜΑΤΑ ΣΤΟΥΣ ΗΛΕΚΤΡΟΝΙΚΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ ΜΕ ΕΜΦΑΣΗ ΣΤΙΣ ΑΠΟΔΕΙΞΕΙΣ

ΟΝΟΜΑ/ΕΠΩΝΥΜΟ: ΠΛΑΚΙΔΑ ΕΥΘΑΛΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΑΝΙΑΤΗΣ ΑΝΤΩΝΙΟΣ

ΠΥΡΓΟΣ 2014

ΠΕΡΙΕΧΟΜΕΝΑ

«Όλη η περιβόητη τεχνολογική μας πρόοδος -ο ίδιος ο πολιτισμός μας- είναι σαν ένα τσεκούρι στα χέρια ενός ψυχοπαθούς»

Αλβέρτος Αϊνστάιν

Εισαγωγή

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του Διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων, στην παραγωγική διαδικασία, στις συναλλαγές, στην εκπαίδευση, στη διασκέδαση, ακόμα και στον τρόπο σκέψεως του σύγχρονου ανθρώπου. Μαζί με αυτές τις αλλαγές, οι οποίες κατά κανόνα βελτιώνουν την ποιότητα της ζωής μας, υπεισέρχονται και οι παράμετροι που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας θεσμοθετούνται με τον όρο «Ηλεκτρονικό Έγκλημα».

Η δικαστική των υπολογιστών (Computer Forensics) λοιπόν, έρχεται να παίξει σημαντικό ρόλο στην εξιχνίαση του ηλεκτρονικού εγκλήματος. Είναι η εφαρμογή του υπολογιστή σε τεχνικές έρευνας και ανάλυσης για τη συγκέντρωση στοιχείων τα οποία θα χρησιμοποιηθούν και θα παρουσιασθούν στο δικαστήριο αποδηκνίωντας την ενοχή.

Πιο αναλυτικά, η επιστήμη αυτή, που έχει ως αντικείμενο της την διατήρηση, την αναγνώριση, την εξόρυξη, τη συλλογή ,την ανάλυση, τη διαφύλαξη, και την παρουσίαση των ψηφιακών αποδεικτικών στοιχείων με τρόπο που είναι νομικά αποδεκτός, χρησιμοποιείται στο πλαίσιο της ποινικής δίκης, παρέχοντας «εμπειρογνωμοσύνη».

Στόχος της πειθαρχίας είναι η εκτέλεση μιας δομημένης έρευνας, διατηρώντας παράλληλα μια τεκμηριωμένη αλυσίδα των αποδεικτικών στοιχείων για να μάθουμε τι ακριβώς συνέβη σε έναν υπολογιστή και ποιος ήταν υπεύθυνος γι 'αυτό.

Η πειθαρχία περιλαμβάνει τεχνικές και αρχές για την ανάκτηση των δεδομένων , αλλά με πρόσθετες κατευθυντήριες γραμμές και πρακτικές που αποσκοπούν στη δημιουργία ενός νομικού ελέγχου.

Η **Ανακριτική**, που είναι ιδιαίτερος κλάδος της Ποινικής Επιστήμης, της Εγκληματολογίας, και που έχει ως αντικείμενο μελέτης το έγκλημα, την αποκάλυψη του δράστη και του εγκληματία και που ακριβώς σε αυτό το σημείο θα παίξει συστηματικό ρόλο, αφού ασχολείται με τα προβλήματα της ανάκρισης του εγκλήματος στην ποινική δίκη.
Το ενδιαφέρον της ανακριτικής αρχίζει από την διάπραξη του ηλεκτρονικού εγκλήματος, ή και από την πρόληψη σχεδιαζόμενου μέχρι την έκδοση δικαστικής απόφασης ενοχής ή αθώωσης κατηγορουμένου.

Η Ανακριτική ως προς το αντικείμενο προσδιορισμού των οργάνων που επιλαμβάνονται της ανάκρισης των εγκλημάτων, καθώς και για την έρευνα, τη συλλογή και τον έλεγχο των αποδεικτικών στοιχείων που σχετίζονται με τη διάπραξη ενός εγκλήματος για την αποκάλυψη της ταυτότητας του δράστη, ταυτίζεται με το Ποινικό Δικονομικό Δίκαιο ή Ποινική Δικονομία, που προσδιορίζει και τα όρια μέσα στα οποία μπορούν να δράσουν τα όργανα της ανάκρισης.

Το ουσιώδες όμως σημείο της Ανακριτικής είναι η έρευνα σύγχρονων και αποτελεσματικών μεθόδων ανάκρισης καθώς μέσων και τρόπων διαλεύκανσης εγκλημάτων που δια της νομοθετικής οδού εμπλουτίζουν και εκσυγχρονίζουν την Ποινική Δικονομία.

Ας υποθέσουμε ότι βρισκόμαστε μπροστά σε ένα ηλεκτρονικό έγκλημα, πώς μπορεί η επιστήμη της Ανακριτικής να βοηθήσει στην οργάνωση της ανάκρισης του εγκλήματος αφενός και αφετέρου στο βασικό πρόβλημα της εξακρίβωσης της ταυτότητας είτε του δράστη είτε του θύματος; Τι είναι η διαδικτυακή και τι η λεγομένη ηλεκτρονική απόδειξη (electronic evidence). Σε όλα αυτά τα ερωτήματα θα εστιάσουμε δίνοντας τεκμηριωμένες απαντήσεις.

ΚΕΦΑΛΑΙΟ 1.

Ηλεκτρονικό έγκλημα

1.1. Τι είναι έγκλημα;

Έγκλημα είναι κάθε πράξη, που προσβάλλει βαριά την κοινή συνείδηση και γι΄ αυτό αυτή αντιδρά έντονα. Σύμφωνα με τον Durkheim (Φαρσεδάκης, 1996) τα εγκλήματα συνίστανται σε πράξεις, που αποδοκιμάζονται καθολικά από τα μέλη κάθε κοινωνίας. Επίσης πρέπει να αναφέρουμε πως σύμφωνα με τον Garofalo (Φαρσεδάκης, 1996) έγκλημα διαπράττει εκείνος, που παραβαίνει τα στοιχειώδη αισθήματα φιλαλληλίας – και συγκεκριμένα του οίκτου και της εντιμότητας – μιας συγκεκριμένης κοινωνίας μιας ορισμένης εποχής, τα απαραίτητα για την κοινωνική συμβίωση (κατά τις αντιλήψεις αυτής της κοινωνίας) .

Ο ίδιος όμως ο Ποινικός Κώδικας στην διάταξη του άρθρου 14 μας δίνει το δογματικό ορισμό του εγκλήματος. Έτσι σύμφωνα με το άρθρο 14 Π.Κ. «έγκλημα είναι πράξη άδικος και καταλογιστή εις τον πράξαντα, τιμωρούμενη υπό του νόμου».

Το ουσιαστικότερο περιεχόμενο του εγκλήματος συνίσταται στο ότι :είναι η πράξη εκείνη που θίγει τις αξίες της κοινωνικής ζωής στις γενικότερης αποδοχής πλευρές της, και που η τέλεση της εκφράζει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται κοινωνικά απόλυτα αναγκαία.

Το εγκληματικό φαινόμενο αποτελεί ιστορικό, κοινωνικό φαινόμενο καθώς ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Έτσι τα επιμέρους χαρακτηριστικά του,(κοινωνικά αγαθά, έγκλημα, ποινή)έχουν και αυτά ιστορικότητα, δηλαδή σχετικότητα, διαφοροποιούμενα από τόπο σε τόπο και από εποχή σε εποχή[1]. Αυτό που έχει ιδιαίτερη σημασία να επισημάνουμε είναι η διαχρονικότητα του στο πέρασμα των αιώνων. Καμιά κοινωνία δεν έχει απαλλαχθεί από αυτό, αν και σε κάθε έγκλημα (προσβολή), υπήρχε, υπάρχει και θα υπάρχει ποινή (αντίδραση). Αντίθετα αυτό που παρατηρείται είναι μια αύξηση του εγκληματικού φαινομένου και συγχρόνως εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς.

[1] Μανωλεδάκης Ι. «Ποινικό Δίκαιο», ζ' έκδοση, εκδόσεις Σάκκουλα, 2005

Το έγκλημα είναι το αναμενόμενο στα πλαίσια της κοινωνικής πραγματικότητας. Είναι το εμφανές σύμπτωμα της κοινωνικής κρίσης, της διάρρηξης του κοινωνικού ιστού, το βαθύ σημάδι μιας κοινωνίας που γερνά[2].

1.1.1. Χαρακτηριστικά του εγκλήματος

Τα κύρια χαρακτηριστικά του εγκλήματος σύμφωνα με τον Φαρσεδάκη (Φαρσεδάκης, 1996) είναι:

- **v** Η παγκοσμιότητα: Όσο και αν οι μορφές, η έκταση και το είδος της αντίδρασης της πολιτείας έναντι συγκεκριμένης συμπεριφοράς ποικίλλουν ανά χώρα ενδεχομένως και ανά συγκεκριμένη γεωγραφική περιοχή, το κοινωνικό αυτό φαινόμενο είναι κοινό παντού. Κοινωνία χωρίς έγκλημα δεν υπάρχει.

- **v** Η διαχρονικότητα: Η ιστορική έρευνα έχει αποδείξει ότι το εγκληματικό φαινόμενο υπήρξε σε όλες τις κοινωνίες, χωρίς καμιά εξαίρεση. Μπορεί να υπήρξαν διαφοροποιήσεις ως προς το περιεχόμενο των νόμων και τα επιμέρους χαρακτηριστικά των παραβάσεων και των παραβατών, όμως πάντοτε υπήρξε παραβίαση κανόνων και επιβολή κυρώσεων.

- **v** Η αλληλεξάρτηση των στοιχείων του εγκληματικού φαινομένου: Τα τρία βασικά στοιχεία του εγκληματικού φαινομένου, δηλαδή ο κανόνας, το έγκλημα και η κύρωση αποτελούν έναν κύκλο, ο οποίος δεν μπορεί να διασπαστεί. Κανένα από τα τρία αυτά στοιχεία δεν μπορεί να υπάρξει χωρίς το άλλο. Δεν θα υπήρχε έγκλημα, αν δεν υπήρχε κανόνας συμπεριφοράς, για να τον παραβεί κάποιος. Η κοινωνική αντίδραση θα ήταν ανύπαρκτη χωρίς έγκλημα και εγκληματία.

- **v** Η δυσχέρεια ορισμού του εγκλήματος: Όπως ήδη προαναφέρθηκε, το έγκλημα είναι αναπόσπαστο κομμάτι κάθε κοινωνίας, παράλληλα όμως χρησιμοποιεί διαφορετικούς κανόνες ανάλογα με το συγκεκριμένο πολιτικό, κοινωνικό, ηθικό κ.λπ. καθεστώς που επικρατεί σε κάθε οργανωμένο σύνολο ανθρώπων. Το γεγονός αυτό δυσχεραίνει τον ορισμό και προσδιορισμό του, καθότι τόσο αυτή η διαφοροποίηση όσο και η συνεχής μετεξέλιξη των κοινωνιών καθιστά πολλές φορές δυσδιάκριτο το τι αποτελεί έγκλημα και τι όχι.

[2] Πιπερόπουλος Γ., Κοινωνικά Προβλήματα, Εκδόσεις Ελληνικά Γράμματα, 1998.

1.2. Τι είναι διαδίκτυο

Το **Διαδίκτυο** (αγγλ. Internet) είναι ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί εκατομμύρια χρηστών καθημερινά σε ολόκληρο τον κόσμο. Οι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές ανά τον κόσμο, οι οποίοι βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας, ανταλλάσσουν μηνύματα (πακέτα) με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Το κοινό αυτό δίκτυο καλείται Διαδίκτυο.

1.2.1. Ιστορική αναδρομή

Την δεκαετία του 1960 η κυβέρνηση των ΗΠΑ ανέθεσε σε ερευνητές του στρατού το καθήκον της δημιουργίας ενός αποκεντρωμένου επικοινωνιακού δικτύου με τέτοιο τρόπο έτσι ώστε αν ένας ενδιάμεσος κόμβος δεχόταν επίθεση η επικοινωνία ανάμεσα στους υπόλοιπους κόμβους να μην σταματούσε. Το 1967 λειτούργησε για πρώτη φορά το ARPANET με 4 κόμβους οι οποίοι βρίσκονταν σε διαφορετικά γεωγραφικά σημεία και με ταχύτητα 50kbps. Το συγκεκριμένο δίκτυο υλοποιούσε ένα σύστημα ανταλλαγής πακέτων πράγμα που σημαίνει ότι η πληροφορία τεμαχιζόταν σε πακέτα τα οποία αργότερα αποστέλλονταν αυτόνομα από τον κόμβο προέλευσης στον κόμβο προορισμού.

Το 1972 οι κόμβοι του ARPANET είχαν φτάσει τους 23 και εφαρμόστηκε για πρώτη φορά το σύστημα του ηλεκτρονικού ταχυδρομείου. Με συνεχείς τεχνολογικές βελτιώσεις και προσθήκες νέων υποδικτύων και υπηρεσιών το ARPANET μετεξελίχθηκε σε αυτό που ονομάζουμε σήμερα “Διαδίκτυο” ή “Internet”.

1.3. Τι είναι ηλεκτρονικό έγκλημα

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί το ηλεκτρονικό έγκλημα. Ένας ορισμός που δόθηκε από τους Forester and Morrison (1994) προσδιόρισε το

ηλεκτρονικό έγκλημα ως «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της». Ωστόσο, το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. Υιοθετώντας μια τριπλή προσέγγιση που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- **v** μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών
- **v** μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
- **v** μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ΄ οποιονδήποτε τρόπο ένας ηλεκτρονικός υπολογιστής.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν: *e-crime, cybercrime, computer-crime, internet related crime και hitech-crime* είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους computer crime, e-crime, hitech-crime ως γενικότερους και τους όρους cybercrime και internet related crime ως ειδικότερους, καθότι στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι *ηλεκτρονικό έγκλημα*, *δικτυακό έγκλημα* και *έγκλημα του κυβερνοχώρου*. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους.

Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop, notepad κλπ.

Κυρίαρχο ρόλο διαδραματίζει ο Η/Υ, ο οποίος μπορεί:

- **Να αποτελεί τον στόχο κάποιας επίθεσης**. Στην περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης.
- **Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης**, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή).

- **Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος**, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

1.3.1. Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο

- Το έγκλημα στον Κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

- Είναι εύκολο στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά…

- Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.

- Μπορεί να διαπραχθεί χωρίς την μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, μέσω του υπολογιστή του.

- Δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (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 σε chat rooms..

- Οι “εγκληματίες του Κυβερνοχώρου” πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα , αποστέλλουν ηλεκτρονικά μηνύματα(e-mail) με ψευδή στοιχεία.

- Είναι έγκλημα διασυνοριακό και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.

- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεως του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί στην Α χώρα και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.

- Η έρευνα απαιτεί κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (του κράτους στο οποίο έγινε αντιληπτό το αποτέλεσμα της εγκληματικής συμπεριφοράς, και του κράτους όπου βρίσκονται τα αποδεικτικά στοιχεία). Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους είναι σπάνια.

- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου

καταγγέλλονται διεθνώς. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι «ακόμα πιο σκοτεινό», από ότι στον «κοινό» εγκληματικό χώρο.

1.3.2. Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Η «συσκευή» αυτή επέτρεπε την επανάληψη μιας σειράς ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία.

Είναι λοιπόν εύκολο να αντιληφθεί κάποιος πως με την ραγδαία ανάπτυξη της τεχνολογίας και συγκεκριμένα των ηλεκτρονικών υπολογιστών, οι ευκαιρίες για την ανάπτυξη της ηλεκτρονικής εγκληματικότητας πολλαπλασιάζονται.

1.4. Σχέση εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή

Το έγκλημα στον κυβερνοχώρο (cyber crime) είναι μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος (computer crime), το οποίο με τη σειρά του είναι μια 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 χαρακτηρισθεί κάθε παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά που σχετίζεται με την επέμβαση, επεξεργασία ή μετάδοση δεδομένων.

1.5. Κατηγορίες ηλεκτρονικών εγκλημάτων

1.5.1. Γνήσια Ηλεκτρονικά εγκλήματα

Τα κυριότερα και πιο διαδεδομένα εγκλήματα που περιλαμβάνονται σε αυτήν την κατηγορία είναι :

- Κακόβουλες εισβολές σε δίκτυα (hacking, cracking)
- Ανεπιθύμητη αλληλογραφία (spamming)

- Ηλεκτρονικό «Ψάρεμα» (phising - pharming)
- Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - trojan horses)
- Πειρατεία ονομάτων χώρου (domain names piracy)
- Απάτη με τη Νιγηριανή Επιστολή (Nigerian scam)
- Επιθέσεις Άρνησης Εξυπηρέτησης (DoS, Denial of Service)

1.5.1.1. Κακόβουλες εισβολές σε δίκτυα

α) Hacking

Hacking είναι η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα[3].

Η έννοια του hacking είναι ευρεία. Μπορεί να αφορά από το νομικό και έγκριτο πληροφορικό προγραμματισμό έως μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να οριστούν ως παράνομες και εγκληματικές[4]. Η εισβολή στο δίκτυο ακόμα και αν δεν είναι κακόβουλη, θα λέγαμε ότι ενέχει κακόβουλο χαρακτήρα. Αυτό γιατί ο επιτιθέμενος ή αλλιώς hacker, εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του, εντοπίζει πιθανά αδύνατα σημεία του και έτσι μπορεί στη συνέχεια αν θέλει να διαπράξει κακόβουλη επίθεση ή ακόμα και να διαθέσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει στην επίθεση. Η δράση των hackers δεν είναι πάντα καταστροφική και συνδεδεμένη με εγκληματικές πράξεις βανδαλισμού, αλλά μια πτυχή των παραβιάσεων σχετίζεται με την ανάγκη επίδειξης των τεχνικών δυνατοτήτων τους.

Όπως σε μια πραγματική μάχη, έτσι και στο ιντερνέτ το βασικότερο πράγμα πριν από μια επίθεση είναι η συλλογή πληροφοριών για τον αντίπαλο.

Συνοπτικά **ως χάκερ (hacker) μπορεί να ορισθεί 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.**

[3] www.go-online.gr/e-business/specials/article/html?article_id_370,πρόσβαση

[4] Λάζος Γρ., «Πληροφορική και Έγκλημα, Νομική Βιβλιοθήκη», Αθήνα 2001, σελ.96.

Γενικά υπάρχουν τρεις (3) κατηγορίες hacker:

1. White hat-hackers: Στόχος τους είναι να καταπολεμούν το ηλεκτρονικό έγκλημα και τους black hat – hackers. Οι grey hats τους ταυτίζουν με τους ειδικούς ασφαλείας και διαχειριστές συστημάτων. Οι ηλικία τους κυμαίνεται από 25 έως και 40 έτη, μερικές φορές οι grey hats μετατρέπονται σε white hats όταν μεγαλώσουν.

2 Black hat- hackers: Είναι αυτοί που εμπλέκονται στο ηλεκτρονικό έγκλημα. Χρησιμοποιούν τις γνώσεις τους σε οργανωμένες ομάδες φτιάχνοντας παράνομα προγράμματα, όπως ηλεκτρονικούς ιούς και κατασκοπευτικά προγράμματα. Διεισδύουν σε δίκτυα και τα κατασκοπεύουν, σπάνε κωδικούς από ιστοσελίδες και τις καταστρέφουν. Το κίνητρο τους είναι χρηματικό τις περισσότερες φορές και όχι ιδεολογικό.

3. Grey hat-Hackers: Εδώ μπαίνουμε στην γκρίζα ζώνη του ιντερνετ. Σε αυτή την κατηγορία ανήκουν χάκερ που παραβιάζουν τον νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Μπορεί να ανακαλύψουν κενά ασφαλείας ξένων δικτύων ή προγραμμάτων και να τα σπάσουν για να αποδείξουν την αδυναμία τους. Αυτοί οι χάκερ είναι επί το πλείστο μικρής ηλικίας, ξεκινούν σε ηλικία 15 χρονών και φτάνουν στο αποκορύφωμα των γνώσεων τους ως φοιτητές.

β) Cracking

Το **Cracking** αποτελεί την παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα, η αλλαγή των σχετικών κωδικών πρόσβασης και η άρνηση προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους. Βασικός σκοπός είναι η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους ζημιάς.

Ποινικοποίηση του Hacking

Σύμφωνα με το άρθρο 370 Γ παρ. 2 όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον 29 € . Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται με ιδιαίτερη ποινή και συγκεκριμένα με την ποινή που επιβάλλεται για την κατασκοπεία.

Όταν θεσπίστηκε ο συγκεκριμένος νόμος η χρήση του Διαδικτύου, αλλά και των Η/Υ δεν είχε λάβει τις σημερινές της διαστάσεις. Οι διατάξεις του συγκεκριμένου νόμου χαρακτηρίζονται από την ευρύτητα της διατύπωσής τους, με σκοπό να περιληφθεί

στο πεδίο εφαρμογής του κάθε πιθανή μελλοντική μορφή αξιόποινης συμπεριφοράς που θα δημιουργούσε η εξέλιξη της τεχνολογίας. Βέβαια η εκπλήρωση του σκοπού αυτού ήταν εξ αρχής ιδιαιτέρως δύσκολη και εν μέρει μόνο επιτεύχθηκε. Για την πλήρωση της αντικειμενικής υπόστασης του 370Γ παρ.2 ΠΚ απαιτείται: α) η απόκτηση πρόσβασης, β) χωρίς δικαίωμα, γ) σε στοιχεία, δ) που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

1.5.1.2 Ανεπιθύμητη αλληλογραφία (spamming)

Η ανεπιθύμητη αλληλογραφία ή spamming είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα. Παρά το γεγονός ότι ο όρος spamming αναφέρεται περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπρόσθετα για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως «ενοχλητικό» για αυτόν που το λαμβάνει. Η αλληλογραφία αυτή θα μπορούσε να χαρακτηριστεί «απρόκλητη» καθώς άτομα χωρίς προηγούμενη έμπρακτη εκδήλωση ενδιαφέροντος, γίνονται αποδέκτες διαφημίσεων από εταιρίες που απέκτησαν με νόμιμο ή παράνομο τρόπο τις διευθύνσεις της ηλεκτρονικής τους αλληλογραφίας[5].

Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του spamming :

• **Απρόκλητο**: Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα η οποία θα δικαιολογούσε ή θα προκαλούσε τη σχέση αυτή.

• **Εμπορικό:** Το spamming αφορά την αποστολή μηνυμάτων με εμπορικό σκοπό κατά κύριο λόγο, σκοπεύοντας την προβολή και διαφήμιση προϊόντων και υπηρεσιών και εν συνεχεία διεύρυνση πελατολογίου και πραγματοποίηση πωλήσεων.

• **Μαζικό**: Το spamming συνίσταται στη μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών.

Για να προστατευτεί ο χρήστης που λαμβάνει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει μόλις το εντοπίσει στο φάκελο των εισερχομένων μηνυμάτων του, να το διαγράψει αμέσως χωρίς να προσπαθήσει να το ανοίξει και να το διαβάσει, και αυτό γιατί υπάρχει πιθανότητα να εμπεριέχει απάτη ή να «μολύνει» με κακόβουλο λογισμικό τον ηλεκτρονικό υπολογιστή του. Κρίνεται σκόπιμο κάθε χρήστης να εγκαταστήσει στον Η/Υ ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων όπως επίσης να αποφεύγει να δίνει την ηλεκτρονική του διεύθυνση σε

[5] Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2001, σελ.169.

οποιονδήποτε τη ζητήσει.

Νομοθεσία για το Spamming

Η Οδηγία 2002/58 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (12/07/2002)

Από την πλευρά της Ε. Ε. θεωρήθηκε αναγκαία η δημιουργία ενός κοινοτικού νομικού πλαισίου που θα έδινε ένα κοινό τρόπο προστασίας και αντιμετώπισης της μη ζητηθείσας επικοινωνίας για όλα τα κράτη – μέλη. Πιο συγκεκριμένα αποφασίστηκε η υποχρεωτική υιοθέτηση ενός opt – in[6] συστήματος, σύμφωνα με το οποίο η αποστολή μη ζητηθείσας εμπορικής αλληλογραφίας δεν επιτρέπεται έκτος και εάν ο καταναλωτής έχει δώσει προηγουμένως τη συγκατάθεσή του. Η υποχρέωση αυτή επιβάλλεται από την Οδηγία 2002/58/ΕΚ «για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες». Ειδικότερα, το άρθρο 13 παρ. 1 αυτής, υποχρεώνει τα κράτη – μέλη να απαγορεύουν την αποστολή τέτοιων μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου εκτός και αν οι συνδρομητές έχουν εκ προτέρων συγκαταθέσει για την επικοινωνία αυτή.

Προσαρμογή της Οδηγίας 2002/58/ΕΚ στο Ελληνικό Νομικό Πλαίσιο

Σύμφωνα με την παραπάνω οδηγία της Ε.Ε. (2002/58, Άρθρο 17), όλα τα κράτη-μέλη είναι υποχρεωμένα να προσαρμόσουν τις εσωτερικές τους νομοθεσίες τους. Κάποια κράτη μέλη της Ε.Ε. έχουν ήδη προσαρμόσει τη νομοθεσία τους, ενώ στη χώρα μας, καθώς και σε κάποιες άλλες, η διαδικασία αυτή βρίσκεται σε εξέλιξη.

Ο Έλληνας νομοθέτης μετέφερε στην ελληνική νομοθεσία της διατάξεις της παραπάνω Οδηγίας στο ΠΔ131_2003. Συγκεκριμένα στο άρθρο 6 παρ. 2, αναφέρεται ότι οι φορείς παροχής υπηρεσιών που αναλαμβάνουν δραστηριότητες μη ζητηθείσας εμπορικής επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου, υποχρεώνονται να τηρούν μητρώα (αρνητικών) επιλογών (opt – outregisters ή λίστες του Ροβινσώνα), στα οποία θα εγγράφονται τα φυσικά πρόσωπα που δεν επιθυμούν τη λήψη τέτοιων μηνυμάτων.

1.5.1.3 Ηλεκτρονικό «Ψάρεμα» (phishing - pharming)

α) Phishing

Στην περίπτωση αυτή ο απατεώνας προσπαθεί μέσω των μηνυμάτων που στέλνει να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα email, αποστολέας του οποίου φαίνεται να είναι η τράπεζα του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του λογαριασμού

[6] www.lawnet.gr

του που διακινεί μέσω web. Η σχετική αιτιολογία αναφέρεται σε προβλήματα σε Η.Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί. Το email αυτό έχει σύνδεσμο προς τον δικτυακό τόπο της τράπεζας, ο οποίος όμως δεν είναι πραγματικός και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα.

- **Vishing**

Vishing είναι η προσαρμογή του ηλεκτρονικού ψαρέματος (phishing) σε αυτούς που χρησιμοποιούν το τηλέφωνο ή το VoIP (Voice over IP tools). Ο χρήστης λαμβάνει e-mail ή SMS με το οποίο του ζητείται να καλέσει έναν αριθμό χωρίς χρέωση με στόχο να επιβεβαιώσει τα στοιχεία του. Μπορεί ακόμα να λάβει ένα τηλέφωνο με μαγνητοφωνημένο μήνυμα που να του ζητά να εισάγει τα προσωπικά του στοιχεία.

β) Pharming

Pharming είναι η εκμετάλλευση μιας ευπάθειας στην υπηρεσία DNS (Domain Name), που επιτρέπει σε έναν hacker να ανακατευθύνει την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο δικτυακό τόπο. Οι δράστες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Οι δράστες δεν επιζητούν να πείσουν το θύμα, αλλά χρησιμοποιούν προγράμματα που στην πραγματικότητα επαναδρομολογούν την κυκλοφορία των δεδομένων. Με παρεμβάσεις στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές, ο χρήστης που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται σε άλλη σελίδα που είναι αντίγραφο της γνήσιας. Έτσι, ο χρήστης καταχωρεί τα στοιχεία του νομίζοντας ότι βρίσκεται στην γνήσια ιστοσελίδα, ενώ στην πραγματικότητα τα «παραδίδει» στην ιστοσελίδα του δράστη. Σε άλλες περιπτώσεις, οι δράστες αποστέλλουν μέσω e-mail προγράμματα, τα οποία μετά την εγκατάστασή τους στον υπολογιστή του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) τα οποία τους ενδιαφέρουν. Κατόπιν τα χρησιμοποιούν προκαλώντας περιουσιακή ζημία στο θύμα.

Νομοθεσία για το Phising

Το Διαδίκτυο είναι μη ελεγχόμενο, με την έννοια ότι δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη αντίστοιχη αρχή, η οποία θα ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί. Ωστόσο οι κρατικές υπηρεσίες και η αστυνομία κάθε χώρας, καθώς και οι αντίστοιχες νομοθετικές ρυθμίσεις, παρεμβαίνουν για την αναστολή των αξιόποινων πράξεων που διαπράττονται μέσω Διαδικτύου. Από το 2004 έως σήμερα έχει καταγραφεί μεγάλος αριθμός συλλήψεων ανά τον κόσμο για ηλεκτρονικά εγκλήματα που έχουν διαπραχθεί μέσω της μεθόδου phishing. Επιπλέον, πρέπει να σημειώσουμε πως το 2006 θεσπίστηκε η «Fraud Act» στο Ηνωμένο Βασίλειο η

οποία ορίζει την ηλεκτρονική απάτη ως αδίκημα το οποίο τιμωρείται με ποινή φυλάκισης έως και 10 ετών και απαγορεύει ρητά τη δημιουργία ή κατοχή εργαλείων ηλεκτρονικού ψαρέματος. Ακόμη, το 2005 θεσπίστηκε στις Ηνωμένες πολιτείες η «Anti-Phishing Act», νομοθεσία που καταδικάζει σε ποινή φυλάκισης 5 ετών την κλοπή ταυτότητας μέσω παραποιημένων εταιρικών ιστοσελίδων ή μυνημάτων ηλεκτρονικού ταχυδρομείου. Όσον αφορά την ελληνική νομοθεσία δηλώνεται ρητά πως εφόσον οι δράστες έχουν γνώση και θέληση σχετικά με την παράνομη δραστηριότητά τους, συμπεραίνεται ότι το «phishing» συνιστά απάτη, κατά το άρθρο 386 του Ποινικού Κώδικα, σύμφωνα με το οποίο «όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών».

1.5.1.4. Διασπορά κακόβουλου λογισμικού (ιοί - viruses, σκουλήκια - worms, δούρειοι ίπποι - trojan horses)

Η λέξη «malware» είναι σύντμηση των λέξεων malicious και software. Ο όρος αναφέρεται σε προγράμματα τα οποία έχουν ως στόχο να παραβιάσουν την ασφάλεια των προσωπικών υπολογιστών για να προκαλέσουν ζημιά ή για να υποκλέψουν προσωπικά στοιχεία. Οι πιο γνωστοί τρόποι διαδικτυακής παραβατικότητας μέσω δημιουργίας και διασποράς κακόβουλου λογισμικού είναι οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms) καθώς και οι δούρειοι ίπποι (Trojan horses).

α) Ιοί (Viruses)

Ο ιός είναι ένα πρόγραμμα Η/Υ που έχει σχεδιαστεί με σκοπό να μολύνει άλλα προγράμματα με αντίγραφά του. Επειδή δε έχει την δυνατότητα να αναπαράγεται συνεχώς μπορεί να μεταδοθεί από ένα σύστημα σε άλλο, με σκοπό να εκτελέσει την αποστολή του η οποία περιλαμβάνει την δυσλειτουργία ή και την καταστροφή ολόκληρων συστημάτων, την διαγραφή αρχείων ή το σβήσιμο του συνόλου των σκληρών δίσκων. Ουσιαστικά είναι ένας βλαβερός εκτελέσιμος κώδικας, ο οποίος επιζεί με το να «κολλάει» ή να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Δεν μπορεί να υπάρξει αυτόνομα σαν ξεχωριστό πρόγραμμα. Έχουν παρασιτική συμπεριφορά, καθώς επιζούν με το να «μολύνουν» άλλα αρχεία, ακολουθώντας έτσι πιστά την ανάλογη συμπεριφορά (ο τρόπος που ζουν και πολλαπλασιάζονται) των οργανικών ιών. Σήμερα ο συνηθέστερος τρόπος μετάδοσης των ιών είναι η διανομή τους μέσω ηλεκτρονικού ταχυδρομείου (e-mail).

Ξεκίνησαν σαν πνευματικά παιχνίδια των ερευνητών σε επιστημονικά εργαστήρια αμερικανικών πανεπιστημίων όπως του M.I.T. ή εταιριών προϊόντων

υψηλής τεχνολογίας όπως XEROX, BELL κλπ.

Σύμφωνα με τον Kyas (1997) και με βασικά κριτήρια το προσβαλλόμενο μέρος του Η/Υ καθώς επίσης και τις προσπάθειες που καταβάλλουν οι εγκληματίες προκειμένου να μην γίνουν αντιληπτοί, έχουμε τον παρακάτω διαχωρισμό:

1. Ιοί που μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, ο οποίος περιέχει εντολές εκκίνησης του υπολογιστή (Boot Viruses).
2. Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα (System Cluster Viruses).
3. Ιοί που προσβάλλουν προγράμματα Η/Υ και κρύβονται μέσα σε εκτελέσιμα αρχεία (*.exe). Αυτοί τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (Software Viruses).
4. Ιοί που μπορούν και αναπαράγονται με πολλούς και διάφορους τρόπους με σκοπό να εξασφαλίζουν έτσι την ανθεκτικότητα τους έναντι των διαφόρων προγραμμάτων Anti-Virus (Polymorphous Viruses).
5. Ιοί που «καμουφλάρουν» τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, επεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος (Stealth Viruses).
6. Ιοί που στόχο έχουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus (Retroviruses).
7. Ιοί που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (Data Viruses).

β) Δούρειοι ίπποι (Trojan Horses)

Ένας **δούρειος ίππος** αποτελείται από δύο (2) μέρη, το server και το client. Για να μπορέσει να μολυνθεί ένας υπολογιστής από ένα πρόγραμμα δούρειου ίππου θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεστεί σε αυτόν το μέρος server. Στη συνέχεια, αφού εκτελεστεί το μέρος client στον υπολογιστή του επιτιθέμενου και δοθεί η IP διεύθυνση του υπολογιστή που έχει προσβληθεί, ο έλεγχος του θα είναι πλέον εύκολος. Τα προγράμματα μέσω των οποίων μεταφέρονται οι δούρειοι ίπποι στον ηλεκτρονικό υπολογιστή λέγονται droppers. Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω διαφόρων θυρών (ports) του υπολογιστή τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τοίχους προστασίας (firewall).

Είναι προγράμματα που ενώ φαίνονται να λειτουργούν κανονικά, παράλληλα εκτελούν και κάποιες εργασίες μη επιτρεπόμενες. Έτσι ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή παιχνιδιού , αυτό που κάνει όμως στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του Διαδικτύου.

Στις περισσότερες των περιπτώσεων, ένας δούρειος ίππος δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτό. Κερκόπορτα (trapdoor) είναι ένα μυστικό

σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης.

γ) Σκουλήκια (worms)

Τα σκουλήκια είναι και αυτά προγράμματα που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων προγραμμάτων. Για τον λόγο αυτό χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα δίκτυο με σκοπό να μεταφέρουν κάποιο καταστρεπτικό πρόγραμμα δηλαδή έναν ιό στα διάφορα συστήματα του δικτύου αυτού. Η διαφορά τους από τους ιούς αναφέρεται ότι δεν χρειάζεται ανθρώπινη παρεμβολή για την ενεργοποίηση τους[7].

Άλλα είδη κακόβουλου λογισμικού.

- **Dialers**

Οι dialers είναι μια υποκατηγορία των κακόβουλων προγραμμάτων spyware που είναι σχεδιασμένα με σκοπό να υποκλέπτουν σημαντικές πληροφορίες (κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, στοιχεία λογαριασμών κλπ) για τον χρήστη, χωρίς τη γνώση και έγκρισή του. Σκοπός των δημιουργών προγραμμάτων spyware είναι η προσκόμιση πολλών χρημάτων εύκολα και γρήγορα. Οι dialers αλλάζουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (dial up networking) ώστε να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο σε αυτόν αριθμό που είθισται να είναι διεθνής κλήση με υψηλό κόστος. Στη συνέχεια προχωρούν στη διαγραφή του αριθμού του παρόχου υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και τον αντικαθιστούν με τον δικό τους πάροχο. Με αυτόν τον τρόπο κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο χρησιμοποιεί τον αριθμό του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου.

- **Λογική βόμβα**

Οι λογικές βόμβες είναι μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον πρόγραμμα ή τροποποιούν κάποιον υπάρχοντα κώδικα. Ονομάζονται έτσι λόγω του γεγονότος ότι είναι προγραμματισμένες να «εκραγούν» ηλεκτρονικά κάτω από ορισμένες προϋποθέσεις. Η λογική βόμβα προστίθεται στο πρόγραμμα από χρήστη ο οποίος έχει πρόσβαση στο σύστημα και φυσικά την απαιτούμενη γνώση για την εγκατάσταση της. Είναι περισσότερο επικίνδυνες από τα σκουλήκια και τους δούρειους ίππους γιατί κατασκευάζονται ευκολότερα και έχουν δυνατότητα να προκαλέσουν σοβαρές ζημιές ακόμα και καταστροφές σε σωσμένα αρχεία αλλά και σε ολόκληρο το λογισμικό ενός ηλεκτρονικού υπολογιστή.

[7] Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2001, σελ.112.

v Rootkits

Τα rootkits είναι ένα σύνολο εργαλείων και υπηρεσιών που ο χάκερ μπορεί να χρησιμοποιήσει για να διατηρήσει την πρόσβαση του στο σύστημα που έχει χακάρει από τη στιγμή που θα εισβάλει σε αυτό. Τα εργαλεία του rootkit θα του επιτρέψουν να αναζητήσει ονόματα χρηστών και κωδικούς πρόσβασης, να εξαπολύσει επιθέσεις κατά συστημάτων από απόσταση και να αποκρύψει τις δράσεις του με την απόκρυψη αρχείων και την διαγραφή κάθε δραστηριότητας από τα αρχεία καταγραφής του συστήματος.

Μια και με το rootkit αποκτά πρόσβαση, μπορεί να κάνει σχεδόν ότι θέλει, έχοντας δικαιώματα διαχειριστή, παραδείγματος χάριν, να ελέγξει την κίνηση, την πληκτρολόγηση, να επιτίθεται σε άλλους υπολογιστές στο δίκτυο, ή να δημιουργήσει κερκόπορτες συστήματος για την εξυπηρέτηση των εισβολέων.

v Ransomware

Είναι μια κατηγορία κακόβουλου λογισμικού, το οποίο από απόσταση κρυπτογραφεί δεδομένα του χρηστή και για να τα αποκρυπτογραφήσει απαιτεί «λύτρα».

v Bots – zombies

Μία «bot» είναι ένα είδος κακόβουλου λογισμικού που επιτρέπει σε έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο πάνω στον «πληγέντα» υπολογιστή. Οι υπολογιστές που έχουν μολυνθεί με bot γενικά αναφέροντα ως ζόμπι. Υπάρχουν κυριολεκτικά χιλιάδες υπολογιστές στο Ιντερνετ που έχουν μολυνθεί με κάποιο είδος bot και δεν το συνειδοτοποιούν ακόμα. Συχνά ο ιδιοκτήτης δεν γνωρίζει ότι έχει εξαπολύσει έναν ιό ή εγκαταστήσει έναν δούρειο ίππο ο οποίος ενεργοποιεί τον υπολογιστή να λειτουργήσει σαν ένα Zombie. Ο εισβολέας μπορεί να χρησιμοποιήσει το μολυσμένο υπολογιστή για να επιτεθεί ή να στείλει spam σε άλλους υπολογιστές χωρίς να το ξέρουν οι ιδιοκτήτες τους[8].

v Scareware

Το scareware είναι προγράμματα εξαπάτησης. Γνωστά και ως fraudware, τα οποία τις περισσότερες φορές εμφανίζονται με τη μορφή pop-up παραθύρων, με σκοπό να εκφοβίσουν τους χρήστες του διαδικτύου (π.χ. προειδοποιώντας τους ότι ο υπολογιστής τους έχει μολυνθεί με κακόβουλο λογισμικό) και να τους πείσουν να προβούν στην αγορά ή/και εγκατάσταση συγκεκριμένου λογισμικού που υποτίθεται πως θα τους προστατέψει από επιθέσεις και απειλές.

[8] http://www.spamfigher.com/LANG_FAQ_Glossary.asp,

- **Βακτήρια (bacteria)**

Τα βακτήρια (bacteria) είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία. Ο μοναδικός τους σκοπός είναι να πολλαπλασιάζονται. Ένα τυπικό βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να τρέχει ταυτόχρονα δύο αντίγραφά του σε ένα πολυπρογραμματιζόμενο σύστημα ή πιθανόν να δημιουργεί δύο νέα αρχεία, καθένα απ' τα οποία είναι αντίγραφο του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να αντιγράψουν τον εαυτό τους δύο φορές κ.ο.κ. Τα βακτήρια αναπαράγονται εκθετικά και τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες.

Όσον αναφορά την ποινική νομοθεσία , αδικήματα που σχετίζονται με τη διασπορά κακόβουλου λογισμικού και με επιθέσεις άρνησης εξυπηρέτησης δε μπορούν να τιμωρηθούν με βάση την ισχύουσα νομοθεσία. Το κενό της νομοθεσίας για τα εν λόγο εγκλήματα καλύπτονται από τη νομοθεσία των συμβατικών εγκλημάτων.

1.5.1.5 Πειρατεία ονομάτων χώρου (domain names piracy).

α) Βασική προϋπόθεση για την άσκηση ηλεκτρονικού εμπορίου αποτελεί η δημιουργία ενός χώρου στο διαδίκτυο, όπου θα καθίσταται δυνατή η πρόσβαση πελατών και η κατάρτιση των συναλλαγών. Μέσο (εισιτήριο) για την είσοδο στο διαδίκτυο αποτελεί το «domain name» (όνομα πεδίου ή όνομα χώρου), το οποίο κατ' ουσίαν επιτελεί ρόλο ηλεκτρονικής διευθύνσεως ή «κυβερνοδιευθύνσεως», επιτρέποντας την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως.

Το «domain name» αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία, διαιρείται δε σε τρία μέρη. Το πρώτο μέρος είναι κοινό για όλα τα «domain names» και αποτελείται από τα αρκτικόλεξα «http://www» (Hyper Text Transfer Protocol – World Wide Web) που δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο World Wide Web (παγκόσμιο διαδίκτυο).

Το δεύτερο μέρος (second level domain – SLD) ή Μεταβλητό Πεδίο αποτελείται από τα εκάστοτε ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το κατ' εξοχήν όνομα, την κατ' εξοχήν διαδικτυακή διεύθυνση.

Το τρίτο μέρος αποτελεί το επονομαζόμενο top level domain (TLD), που δηλώνει το είδος της τοποθεσίας (ιστοθέσης) ή τη γεωγραφική προέλευση, όπως «.com» για όσους ασκούν εμπορική δραστηριότητα, «.edu» για εκπαιδευτικούς

οργανισμούς, «.org» για οργανισμούς, «.net» για παροχές υπηρεσιών διαδικτύου, «.gov» για κυβερνητικούς οργανισμούς, «.int» για διεθνείς οργανισμούς, «.gr» για τη χώρα αρχειακής καταχωρίσεως του «domain name» του χρήστη, εν προκειμένω για την Ελλάδα (βλ. Ι. Καράκωστα, Δίκαιο & Internet, 2003, σελ. 27).

Το «domain name» δεν μπορεί κατ' αρχήν να ταυτιστεί με την εμπορική επωνυμία, τον διακριτικό τίτλο και το εμπορικό σήμα. Πρέπει, ωστόσο, να αποδίδεται σ' αυτό λειτουργία τόσο διακριτικού τίτλου όσο και σήματος, κατά έμμεσο τρόπο, όταν αυτό χρησιμοποιείται ως διακριτικό στοιχείο για το πρόσωπο ή την επιχείρηση στο διαδίκτυο, διότι, έχει πρωταρχικά εξατομικευμένη και αναγνωριστική λειτουργία. Η ευχέρεια ελεύθερης χρήσεως οποιασδήποτε ονομασίας, όσο γνωστή και φημισμένη και αν είναι, από τον πρώτο τυχόντα, θα προκαλούσε τεράστιες ή ανεπανόρθωτες ζημίες στην επιχείρηση που καθιερώθηκε στις συναλλαγές με την επίμαχη ονομασία. Για τη διαφύλαξη έτσι των νομίμων συμφερόντων των παραπάνω επιχειρήσεων, θα πρέπει να αποδοθεί στο «domain name» μια οιονεί λειτουργία διακριτικού τίτλου και σήματος. Τούτο ενισχύεται και από το ότι οι κάτοχοι «domain names» στην πράξη εμφανίζονται στο διαδίκτυο με τα διακριτικά γνωρίσματα που τους κατέστησαν γνωστούς στον υλικό κόσμο, δηλαδή χρησιμοποιούν το όνομα, την επωνυμία ή το σήμα τους, δεδομένων μάλιστα των περιορισμένων ορίων παροχής «domain names» για κάθε χρήση αλλά και της επιβαλλόμενης συντομίας γι' αυτού του είδους την επικοινωνία.

β) Έννομη Προστασία: Δεδομένων των ανωτέρω, θα πρέπει να απολαμβάνει προστασίας αντίστοιχης με εκείνη των διακριτικών γνωρισμάτων (εφαρμοζομένων αναλόγως των σχετικών διατάξεων), αλλά και ένα διακριτικό γνώρισμα θα πρέπει να προστατεύεται (εφόσον βεβαίως πληρούνται προϋποθέσεις προστασίας του) από τη χρήση ενός ονόματος διαδικτύου, παρά το γεγονός ότι προηγήθηκε χρονικά η καταχώριση αυτού στο διαδίκτυο, λαμβανομένων όμως υπόψη, υπό τα εκάστοτε κρίσιμα πραγματικά περιστατικά, των ιδιαιτεροτήτων του διαδικτύου, και συγκεκριμένα της παγκοσμιότητας του διαδικτύου ως μέσου ενημέρωσης, της μοναδικότητας των ηλεκτρονικών διευθύνσεων, της πεπερασμένης δυνατότητας συνδυασμών διευθύνσεων, του ιδιόρρυθμου συστήματος καταχωρίσεως των ονομασιών, κατά το οποίο η εξυπηρέτηση των αιτήσεων γίνεται κατά τη σειρά άφιξής τους χωρίς διενέργεια προληπτικού ελέγχου, αρκεί να μην έχει χορηγηθεί το συγκεκριμένο όνομα σε άλλον αιτούντα.

Η καταχώριση γνωστού ξένου διακριτικού γνωρίσματος ως «domain name» ενδέχεται να συνιστά και αθέμιτο παρεμποδιστικό ανταγωνισμό (άρθρο 1 Ν 146/1914), ενώ δεν αποκλείεται ότι μπορεί να συντρέχουν και οι προϋποθέσεις εφαρμογής του άρθρου 13 Ν 146/1914, όταν το διακριτικό γνώρισμα χρησιμοποιείται στο διαδίκτυο.

1.5.1.6 Απάτη με τη Νιγηριανή Επιστολή.

Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Ο αποστολέας-απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρίας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητάει τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφτεί με προμήθεια ένα σημαντικό χρηματικό ποσό.

Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής.

Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχτεί. Ξεκινάει λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν[9].

1.5.1.7. Επιθέσεις άρνησης εξυπηρέτησης (DoS, Denial of Service)

Οι επιθέσεις άρνησης εξυπηρέτησης (DoS), είναι ηλεκτρονικές επιθέσεις ενός εισβολέα ο οποίος προσπαθεί να υπερφορτώσει ή να σταματήσει τη λειτουργία μιας υπηρεσίας δικτύου, για παράδειγμα ενός διακομιστή ιστοσελίδας(web server) ή ενός διακομιστή αρχείων(file server). Ο υπολογιστής- θύμα για ένα χρονικό διάστημα, δεν είναι σε θέση να εξυπηρετήσει αιτήσεις από άλλους χρήστες, λόγω του τεράστιου

[9] Τσουραμάνης Χρ., «Ψηφιακή Εγκληματικότητα», εκδόσεις Β. Ν. Κατσαρού, Αθήνα 2005, σελ.22,23.

πλήθους των «ψεύτικων» αιτήσεων που δέχεται από τον επιτιθέμενο. Οι επιθέσεις άρνησης εξυπηρέτησης επηρεάζουν άμεσα τις επιδόσεις του δικτύου (κάνοντας τες σαφώς χαμηλότερες έως και μηδενικές) καθώς επίσης την ακεραιότητα των δεδομένων και τη γενικότερη λειτουργία του συστήματος.

Οι βασικότεροι στόχοι που επιτυγχάνονται με τις επιθέσεις άρνησης εξυπηρέτησης είναι:

- **v** Η παρεμπόδιση της μετάδοσης δεδομένων στο δίκτυο.
- **v** Η αδυναμία σύνδεσης μεταξύ δύο σημείων, με άμεση συνέπεια τη μη πρόσβαση σε συγκεκριμένες υπηρεσίες.
- **v** Υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες.

1.6. Παραδοσιακά (συμβατικά) εγκλήματα που τελούνται και χωρίς τη χρήση Η/Υ ή και του Διαδικτύου

Στην κατηγορία αυτή εντάσσονται εγκλήματα που προϋπήρχαν της πληροφορικής τεχνολογίας δηλαδή εγκλήματα του κοινού Ποινικού Κώδικα τα οποία τελούνται και χωρίς τη χρήση Η/Υ και Διαδικτύου. Η τεχνολογία έχει δώσει δυνατότητες για νέους και πιο πρόσφορους τρόπους τέλεσης τους.
Τα κυριότερα εγκλήματα αυτής της κατηγορίας είναι τα εξής:

- **v** Ξέπλυμα χρήματος
- **v** Πειρατεία Λογισμικού
- **v** Παιδική Πορνογραφία
- **v** Διαδικτυακή Τρομοκρατία

1.6.1. Ξέπλυμα χρήματος

Ο όρος «ξέπλυμα χρήματος» χρησιμοποιείται για να περιγράψει τις διαδικασίες μέσω των οποίων τα κέρδη των εγκλημάτων (βρώμικο χρήμα) υπόκεινται σε μία σειρά διαδικασιών οι οποίες καλύπτουν τις παράνομες ρίζες τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές (καθαρό χρήμα).

Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί τα παρακάτω τρία βασικά στάδια[10]:

1. **Τοποθέτηση**: Ο δράστης τοποθετεί τα χρήματα που προέρχονται από παράνομη δραστηριότητα ως επένδυση στο γενικότερο οικονομικό σύστημα, σε παραδοσιακό ή

[10] Γ.Χλούπη, Νομιμοποίηση εσόδων από παράνομες δραστηριότητες: περιγραφή του φαινομένου και τρόποι αντιμετώπισης, Ποιν. Δικ. 2003/369 επ

μη χρηματοοικονομικό οργανισμό, όπως τράπεζα με κατάθεση σε λογαριασμό, χρηματιστήριο με αγορά μετοχών εισηγμένων σε αυτό, ανταλλακτήριο συναλλάγματος, καζίνο και άλλες συναφείς επενδύσεις.
2. **Στρωματοποίηση**: Ο δράστης επιχειρεί σειρά κινήσεων και συναλλαγών με αποκλειστικό σκοπό να απομακρύνει τα ίχνη των κεφαλαίων από την αρχική τους προέλευση και έτσι να μεταμφιέσει τις αληθινές πηγές κεφαλαίων, εμποδίζοντας τον εντοπισμό τους από τα ελεγκτικά όργανα του φορέα στον οποίο επενδύθηκαν τελικά.
3. **Ενσωμάτωση**: Ο δράστης επανατοποθετεί τα κεφάλαια σε κλάδους νόμιμης οικονομικής δραστηριότητας όπως για παράδειγμα σε αγορά ακινήτων, επιχειρηματικές και εμπορικές δραστηριότητες κλπ, έτσι ώστε τα εν λόγω κεφάλαια να επιστρέφουν στο χρηματοοικονομικό σύστημα ως καθόλα νόμιμα κεφάλαια.
Έτσι λοιπόν, βλέπει κανείς ένα παραδοσιακό έγκλημα του ποινικού κώδικα να διαπράττεται με τη βοήθεια πλέον της τεχνολογίας και των νέων μέσων που αυτή προσφέρει, με σύγχρονους τρόπους και μεθόδους πάντα όμως με τον ίδιο επιδιωκόμενο σκοπό.

Το βασικό «πλεονέκτημα» του ξεπλύματος χρήματος μέσω ίντερνετ είναι ότι δεν υπάρχει προσωπική επαφή μεταξύ των συναλλασσόμενων μερών με άμεσο επακόλουθο, οι δράστες να νιώθουν μεγαλύτερη ασφάλεια και κρυμμένοι πίσω από την ανωνυμία τους να νομιμοποιούν έσοδα παράνομων δραστηριοτήτων.

1.6.2. Πειρατεία λογισμικού

Ο όρος **πειρατεία λογισμικού** αναφέρεται στην αναπαραγωγή ή/και διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους[11].

1.6.2.1. Μορφές πειρατείας λογισμικού

Οι κυριότερες μορφές πειρατείας λογισμικού είναι οι εξής:

1) Χρήση ενός προγράμματος σε περισσότερους υπολογιστές καθ' υπέρβαση της αδείας χρήσης: Είναι η πιο συνηθισμένη μορφή παράνομης χρήσης εφόσον απαιτείται ξεχωριστή άδεια για κάθε υπολογιστή στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα. Εκδηλώνεται δε ως εξής:

α. Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες.
β. Με δήλωση μικρότερου από τον πραγματικό αριθμού εγκαταστάσεων σε μια

[11] Βλαχόπουλος Κωνσταντίνος, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2007, σελ.61.

εταιρεία που διαθέτει άδειες για έναν συγκεκριμένο αριθμό χρηστών υπολογιστών (η άδεια χρήσης παραδίδεται μαζί με το λογισμικό καθώς ορίζεται πως αφορούν σε ένα και μοναδικό εμπόρευμα).
γ. Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών.
δ. Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες τους.
Συχνά οι πωλητές υπολογιστών προκειμένου να κάνουν την αγορά ενός υπολογιστή πιο ελκυστική προσφέρουν προγράμματα χωρίς τις άδειες. Έτσι χρειάζεται μεγάλη προσοχή και έλεγχος των αδειών κατά την αγορά υπολογιστή που διαθέτει προεγκατεστημένα προγράμματα. Το λογισμικό αυτό δεν συνοδεύεται από οδηγίες χρήσης ή βοηθητικές δισκέτες για προγράμματα.

2) Πλαστογράφηση ή αλλιώς πλήρης απομίμηση του προϊόντος: Η παράνομη αναπαραγωγή και πώληση λογισμικού με τέτοιο τρόπο ώστε να φαίνεται νόμιμο. Περιλαμβάνει πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. Το λογισμικό και η συσκευασία του αντιγράφονται με σύνθετες τεχνικές και έπειτα, επαναδιανέμονται ως απομίμηση νόμιμου προϊόντος. Η αυξανόμενη επιλογή του εμπορίου μέσω ιντερνέτ έχει αυξήσει και τις πιθανότητες να βρεθούν οι καταναλωτές αντιμέτωποι με το πρόβλημα της χρήσης πλαστών προϊόντων. Η όλο και περισσότερο εξελιγμένη τεχνολογία που χρησιμοποιούν οι πλαστογράφοι, καθιστούν ακόμα και τους πιο απαιτητικούς καταναλωτές συχνά ανήμπορους να διακρίνουν το νόμιμο λογισμικό από το πλαστό. Το πλαστό λογισμικό συνήθως κατασκευάζεται και προωθείται με τρόπο ώστε να μοιάζει και να ανταγωνίζεται το αυθεντικό προϊόν.

1.6.3. Παιδική πορνογραφία

Τι είναι όμως παιδική πορνογραφία; Σύμφωνα με το «Προαιρετικό Πρωτόκολλο της Σύμβασης για τα δικαιώματα του Παιδιού για την εμπορία παιδιών, την παιδική πορνεία και την παιδική πορνογραφία» και συγκεκριμένα στο άρθρο 2,

«παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση, με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες, ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς».

Το φαινόμενο της πορνογραφίας ανηλίκων αποτελεί μάστιγα των σύγχρονων κοινωνιών σε παγκόσμιο επίπεδο και αποκτά ολοένα και μεγαλύτερες διαστάσεις με τους ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Η μεγέθυνση του κυβερνοχώρου παρέχει στους παραγωγούς και διακινητές του πορνογραφικού υλικού δυνατότητες γρήγορης και εύκολης προώθησης του παράνομου προϊόντος τους. Οι εγκληματίες διακίνησης πορνογραφικού υλικού ανηλίκων μέσα στον αχανή χώρο του διαδικτύου εξασφαλίζουν την ανωνυμία τους και δρουν ανενόχλητα

εκμεταλλευόμενοι την παιδική αθωότητα[12].

Με τη χρήση του διαδικτύου:

- Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη-εγκληματία να αποκρύψει την ταυτότητά του.
- Υπάρχει προσβασιμότητα του επίμαχου υλικού ανά πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με μικρό σχετικά κόστος.
- Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την σεξουαλική κακοποίηση ανηλίκων.
- Διευκολύνεται η ανταλλαγή πορνογραφικού υλικού (ταινίες, φωτογραφίες κλπ) το οποίο μέσα σε λίγα λεπτά μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών μέσω ηλεκτρονικού ταχυδρομείου.

Η παιδική πορνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα οργανωμένη «επιχειρηματική» δραστηριότητα. Αποτελεί προϊόν μιας επικερδέστατης επιχείρησης καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό υλικό ανηλίκων που παρέχουν διάφορες ιστοσελίδες καταβάλουν διόλου ευκαταφρόνητα ποσά.

Οι επιπτώσεις εις βάρος των ανηλίκων, μπορούν να ειδωθούν από πολλές οπτικές γωνίες. Οι ανήλικοι μετατρέπονται σε θύματα των ενηλίκων, αποφέροντάς τους ιδιαίτερα υψηλά κέρδη, εφόσον μετατρέπονται σε εμπορεύσιμα είδη υψηλής αξίας. Επιπλέον μετατρέπονται σε «μέσα» ικανοποίησης των σεξουαλικών τους ορέξεων. Όμως υπάρχει και ένας άλλος κίνδυνος για τους ανηλίκους, που δεν είναι τόσο φανερός όσο οι προηγούμενοι, αλλά που είναι όμως εξίσου σοβαρός και ικανός να προκαλέσει ανεπανόρθωτες βλάβες, κυρίως ως προς τη σεξουαλική τους ωρίμανση. Ο ανήλικος από την πλευρά του, είναι ικανότατος χρήστης των υπολογιστών και συνήθης επισκέπτης του διαδικτύου. Εξαιτίας λοιπόν κάποιων φυσικών γνωρισμάτων του νεαρού της ηλικίας του, όπως της έντονης περιέργειας και του ατίθασου του χαρακτήρα, μπορεί εύκολα να πέσει στις παγίδες του διαδικτύου. Έτσι μπορεί εύκολα ένας ανήλικος να γίνει ο ίδιος καταναλωτής του πορνογραφικού υλικού ή ακόμα να συμμετάσχει στην παραγωγή του, πειθόμενος από αυτούς που γνώρισε δια μέσου του ιστού.

1.6.3.1. Τρόποι εγκληματικής δράσης

Με βάση το άρθρο 348Α του Ποινικού Κώδικα, οι τρόποι εγκληματικής δράσης είναι:

1. Κατασκευή υλικού πορνογραφίας (κινηματογραφική λήψη, μοντάζ, επεξεργασία εικόνων κλπ).
2. Κατοχή πορνογραφικού υλικού δηλαδή φυσική εξουσίαση επί του υλικού.

[12] A textbook of cybercrimes and penalties, σελ 8-16

3. Προμήθεια και αγορά υλικού (πραγματική μετακίνηση του πορνογραφικού υλικού στην κατοχή του δράστη).
4. Μεταφορά πορνογραφικού υλικού.
5. Κυκλοφορία πορνογραφικού υλικού (διακίνηση, διάθεση, πώληση)[13].

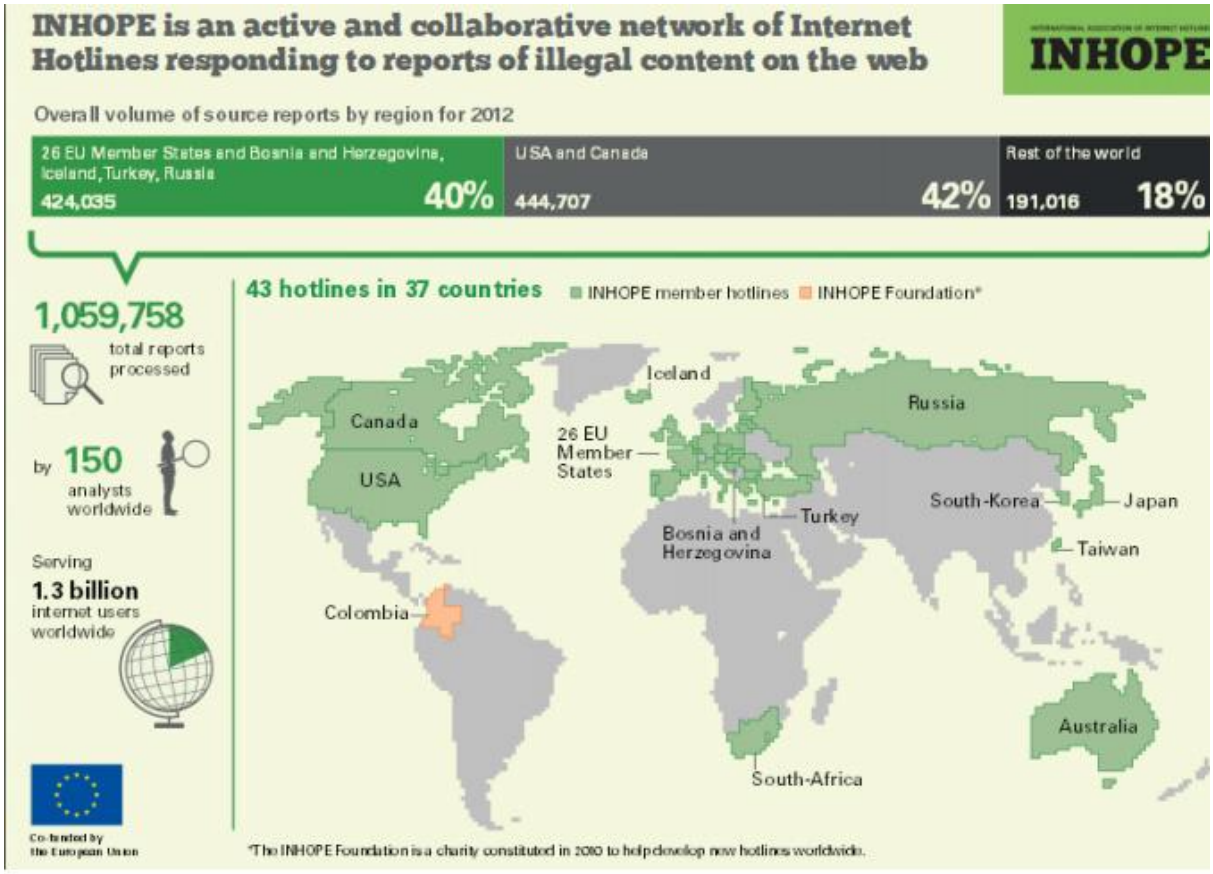
Έχουμε λοιπόν δύο εκφάνσεις της παιδικής πορνογραφίας στο διαδίκτυο: από τη μία τη βιομηχανοποιημένη δημιουργία και διακίνηση πορνογραφικού υλικού με στόχο την πραγματοποίηση κέρδους και από την άλλη την ατομοκεντρική εκδοχή προς ικανοποίηση της προσωπικής διαστροφής του δράστη.

Ο INHOPE, ο Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου, δημοσίευσε τα στατιστικά του στοιχεία για το 2012. Στον Σύνδεσμο ανήκουν 43 Ανοικτές Γραμμές σε 37 χώρες. Τα στατιστικά στοιχεία του INHOPE συγκεντρώθηκαν μέσω του Συστήματος Διαχείρισης Καταγγελιών INHOPE (IHRMS), μια μοναδική βάση δεδομένων που χρησιμοποιείται από τις Ανοικτές Γραμμές για την καταγραφή και προώθηση καταγγελιών του CSAM. Στην Ελλάδα, η SafeLine αποτελεί τον εθνικό εκπρόσωπο στο δίκτυο αυτό από το 2005.

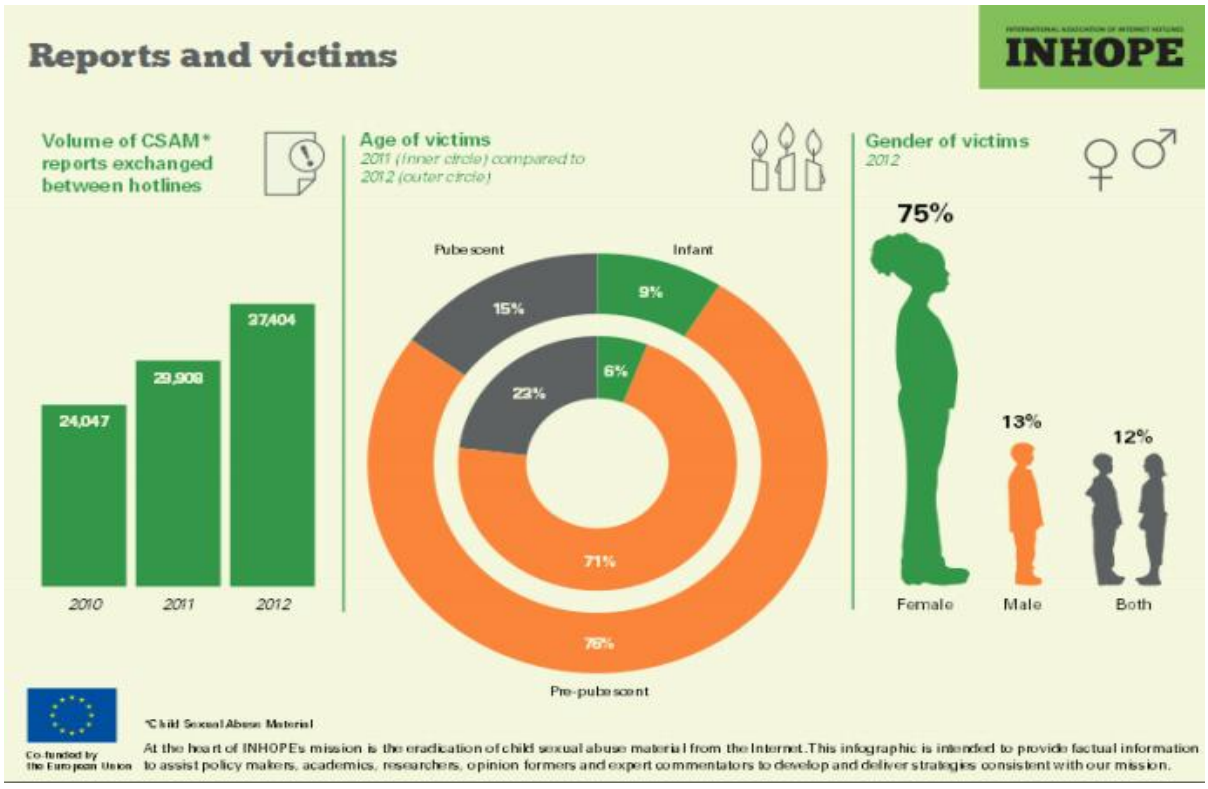
Το 2012 επιτεύχθηκε εντυπωσιακή πρόοδος στον χρόνο που απαιτείται για να αφαιρεθούν εικόνες και βίντεο σεξουαλικά κακοποιημένων παιδιών στο διαδίκτυο.

Ενώ στο παρελθόν αποδείξεις αυτών των φρικιαστικών εγκλημάτων μπορεί να παρέμειναν στο διαδίκτυο για πολλούς μήνες και μερικές φορές για χρόνια, ο INHOPE μπορεί τώρα να βεβαιώσει ότι στην πλειονότητα των περιπτώσεων το περιεχόμενο προβλέπεται να «κατεβαίνει» από το διαδίκτυο μέσα σε λίγες ημέρες και μερικές φορές λίγες μόνο ώρες. Το 2012, ο INHOPE επεξεργάστηκε 1,059,758 καταγγελίες με 150 αναλυτές ανά τον κόσμο, εξυπηρετώντας με αυτόν τον τρόπο 1,3 δις χρήστες του διαδικτύου. Από τις καταγγελίες αυτές το 40% προήλθαν από την ΕΕ, 42% από τις ΗΠΑ και 18% από τον υπόλοιπο κόσμο (βλέπε Εικ.1). Ευρωπαϊκή πρωτιά στην προέλευση αυτού του παράνομου περιεχομένου κατείχε η Ολλανδία (62%) και ακολουθεί η Ρωσία με 23%, ενώ στην Ασία την θέση αυτή την κατείχε το Βιετνάμ (24%). Το μεγαλύτερο ποσοστό των θυμάτων αυτών των εγκλημάτων ήταν νεαρά κορίτσια (75%). Μικρότερο ποσοστό (13%) ανήκε σε νεαρά αγόρια ενώ 13% των δραστηριοτήτων αυτών ήταν θύματα και από τα δύο φύλλα (12%) (βλέπε Εικ.2).

[13] Ε.Συμεωνίδου-Καστανίδου, «Εγκλήματα κατά προσωρινών αγαθών», Νομική Βιβλιοθήκη, 2006, σελ. 249,250.



Εικ. 1 Στατιστικά στοιχεία καταγγελιών



Εικ. 2. Καταγγελίες και θύματα

1.6.3.2. Νομοθεσία για την παιδική πορνογραφία

Άρθρο 348Α όπως αυτό αντικαταστάθηκε από το άρθρο 10 του Ν. 3625/2007 και τροποποιήθηκε με την παρ. 12 του άρθρου 3 του Ν. 3727/2008. Η διάταξη αυτή προβλέπει τα εξής:

1. Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην επικράτεια ή εξάγει από αυτή, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.

4. Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ:

«α. αν τελέσθηκαν κατ' επάγγελμα ή κατά συνήθεια»

«β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή σωματικής δυσλειτουργίας λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος».

Αν η πράξη της περίπτωσης β' είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται ισόβια κάθειρξη.

1.6.4. Διαδικτυακή τρομοκρατία[14]

Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες».

Η χρήση του διαδικτύου παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα:

1. Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.
2. Οι ενέργειες τους δύσκολα εντοπίζονται.
3. Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.
4. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρόντας την ανωνυμία του. Με τη χρήση λοιπόν του Διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων.

Ένα παράδειγμα είναι το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, ο άνθρωπος που είναι ύποπτος ότι βρίσκεται πίσω από τον βομβαρδισμό των Αμερικανικών βάσεων στην Ανατολική Αφρική το 1998 και συνεπώς στην κορυφή του καταλόγου των καταζητούμενων του FBI. Στον Chameleon δόθηκαν 1000 $ προκαταβολικά για την ανταλλαγή με το software και θα έπαιρνε επιπλέον 10.000 $ με την πρόοδο της εργασίας. Ευτυχώς το FBI τον συνέλαβε προτού να έχει την ευκαιρία να διανέμει τα στοιχεία.

Πάντως στο σημείο αυτό θα πρέπει να αναφερθεί πως σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime and Punishment» κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω δέκα κατηγορίες:

- Παρεμπόδιση (κυβερνο)κυκλοφορίας

[14] www.fbi.gov

- Τροποποίηση και Κλοπή δεδομένων
- Εισβολή και Σαμποτάζ σε δίκτυο
- Μη εξουσιοδοτημένη πρόσβαση
- Διασπορά ιών
- Υπόθαλψη αδικημάτων
- Πλαστογραφία και Απάτη

1.7. Μορφές ηλεκτρονικών εγκλημάτων στον Ελλαδικό χώρο

Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ:

1**. Απάτες μέσω Διαδικτύου**

2. **Παιδική πορνογραφία**

3. **Cracking και hacking**

4. **Διακίνηση-πειρατεία λογισμικού**

5**. Πιστωτικές κάρτες**

6. **Διακίνηση ναρκωτικών**

7**. Έγκλημα στα chat rooms**

1.8. Αυτοκτονίες μέσω Internet και αποτροπή αυτών

Η πληθώρα αλλά και η ποικιλία πληροφοριών που διατίθενται σε καθημερινή βάση, αποτελούν μία μόνο από τις πτυχές της τεράστιας και συνεχώς αυξανόμενης δυναμικής που εμφανίζει το Διαδίκτυο την τελευταία δεκαετία. «Επικοινωνία» είναι η λέξη-κλειδί. Αυτό κάνουν εκατομμύρια άνθρωποι από όλα τα μήκη και τα πλάτη του κόσμου μέσω του Internet: ανταλλάσσουν πληροφορίες, απόψεις, ιδέες και εμπειρίες.

Το διαδίκτυο αποτελεί ένα χώρο όπου τα άτομα μπορούν να δράσουν ελεύθερα, χωρίς αναστολές και πραγματοποιούν πιο εύκολα κάτι που στην πραγματική ζωή, στην κοινωνία δεν θα τολμούσαν. Το διαδίκτυο αποτελεί μια παράλληλη κοινωνία και δίνει τη δυνατότητα στα άτομα να συναλλάσσονται και να επικοινωνούν ξεφεύγοντας από τη ρουτίνα της καθημερινής ζωής, βρίσκοντας συντροφιά και κοινά ενδιαφέροντα στα fora, ξεφεύγουν από τη μοναξιά και την απομόνωση και προβάλλουν μια δεύτερη προσωπικότητα στον απαλλαγμένο από συνέπειες χώρο των blogs και ιστοσελίδων κοινωνικών δικτύων.

Πίσω από εικονίδια και καλλιτεχνικές φωτογραφίες το υποκείμενο τολμά να προβάλλει στους άλλους κρυφές πτυχές της προσωπικότητάς του, τολμά να διαμαρτυρηθεί, να φλερτάρει και να εκφραστεί καλλιτεχνικά. Τί γίνεται όμως όταν αυτή η απελευθέρωση οδηγεί σε ενέργειες καταστροφικές, τόσο για το ίδιο το άτομο όσο και για τους άλλους ανθρώπους; Αναφερόμαστε βέβαια στην αυτοκτονία με τη βοήθεια του διαδικτύου. Υπάρχουν αρκετά περιστατικά αυτόχειρων που πήραν ιδέες από άλλους χρήστες του internet ή ομαδικών αυτοκτονιών που συντονίστηκαν μέσω διαδικτύου. Τίθεται ένα ηθικό θέμα μείζονος σημασίας, όσον αφορά την ενοχοποίηση του διαδικτύου σχετικά με τα παραπάνω θέματα. Τα μέλη των διαδικτυακών κοινοτήτων τάσσονται και στις 2 πλευρές. Οι μεν κατηγορούν την αυξημένη πρόσβαση του καθενός σε πληθώρα "απαγορευμένων" πληροφοριών και οι δε πιστεύουν πως οι αυτοκτονίες θα συνέβαιναν ούτως ή άλλως και πως είναι άδικο και ανούσιο να κατηγορούνται οι "σύμβουλοι αυτοκτονιών" ως ηθικοί αυτουργοί.

Η πρώτη υπόθεση που προκάλεσε το δημόσιο ενδιαφέρον και παρουσιάζει για πρώτη φορά τη σύνδεση μεταξύ αυτοκτονίας και διαδικτύου ήταν η υπόθεση «Doctor Kiriko» που συνέβη στην Ιαπωνία το 1998. Σύμφωνα με τη συγκεκριμένη περίπτωση, ένας 27χρονος άνδρας δημιούργησε έναν ιστοχώρο με το όνομα «The counseling Office of Dr. Kiriko» μέσω του οποίου έστειλε ποτάσιο σε έξι άτομα που ήθελαν να αυτοκτονήσουν, με αποτέλεσμα μια γυναίκα να πραγματοποιήσει την επιθυμία της με το συγκεκριμένο δηλητήριο που της στάλθηκε. Έκτοτε, έχει παρουσιαστεί σημαντικός αριθμός αναφορών για αυτοκτονίες που περιλαμβάνουν τη διαμεσολάβηση του διαδικτύου.

1.8.1. Ορισμός

Η αυτοκτονία είναι η πράξη κατά την οποία ένα άτομο εσκεμμένα δίνει τέλος στην ζωή του. Δεν υπάρχει ένας καθολικά αποδεκτός παράγοντας ο οποίας προκαλεί την πράξη της αυτοκτονίας. Παρόλα αυτά, ένα κύριο χαρακτηριστικό που μοιράζονται οι αυτόχειρες είναι η κατάθλιψη. Δεν είναι όμως ασυνήθιστο ορισμένα άτομα να οδηγούνται στην αυτοκτονία λόγω πιέσεων από το κοινωνικό ή οικογενειακό περιβάλλον στο οποίο ζουν. Ακολουθούν και άλλοι παράγοντες:

- Πόνος (π.χ. σωματικός ή συναισθηματικός χωρίς περιθώρια βελτίωσης).
- Στρες (π.χ. θρήνος μετά από τον θάνατο αγαπημένου προσώπου).
- Έγκλημα (π.χ. η προσπάθεια αποφυγής ευθυνών σε έγκλημα που διέπραξε το άτομο)

- Ψυχική ασθένεια και αναπηρία (π.χ. κατάθλιψη, διπολική διαταραχή, τραύμα, και σχιζοφρένεια).

- Σοβαρός τραυματισμός (π.χ. παράλυση, παραμόρφωση, αποκοπή άκρου).

- Κατάχρηση ουσιών.

- Αρνητικό περιβάλλον (π.χ. σεξουαλική κακοποίηση, φτώχεια, έλλειψη στέγης, διακρίσεις.

- Οικονομική ζημία (π.χ. εθισμός σε τυχερά παιχνίδια, απώλεια εργασίας, χρηματιστηριακή κατάρρευση, χρέη).

- Σεξουαλικά θέματα (π.χ. σεξουαλικός προσανατολισμός, έρωτας χωρίς ανταπόκριση, χωρισμός).

- Αποφυγή ατίμωσης.

- Θρησκευτικές πεποιθήσεις (π.χ. επιθέσεις αυτοκτονίας).

- Υπερεθνικιστική ιδεολογία (π.χ. επιθέσεις καμικάζι).

Οι πιο συχνοί λόγοι που ωθούν τους νέους στην αυτοκτονία και το γνωστοποιούν στο διαδίκτυο είναι:

- Ερωτική απογοήτευση.

- School/Cyber Bullying(Σχολικός εκφοβισμός).

- Γενικότερα ψυχολογικά προβλήματα.

- Κάθε μορφής απόρριψης.

1.8.2. Ο Ρόλος του Διαδικτύου στην αυτοκτονία

Το Ίντερνετ ασκεί τρομερή επιρροή στην γνώση και τη διαμόρφωση απόψεων. Μέσα από την αναζήτηση λέξεων-κλειδιών (key words) μέσω της χρήσης μηχανών αναζήτησης όπως το Google, εκατομμύρια άνθρωποι έχουν εύκολη και άμεση πρόσβαση σε ένα τεράστιο, παγκόσμιο και ποικίλο όγκο πληροφοριών.

Μια γενική ανησυχία αναφορικά με το Διαδίκτυο πηγάζει από μέρος του περιεχομένου του που είναι αρκετά αμφισβητήσιμο. Το Διαδίκτυο έχει κατηγορηθεί ως παράγοντας που έπαιξε ρόλο σε θανάτους. Ο Μπράντον Βέντας(Brandon Vedas)

πέθανε από υπερβολική δόση ενός μίγματος νομίμων και παρανόμων ναρκωτικών παρακινούμενος από συνομιλητές του στο IRC. Ο Σων Γούλευ(Shawn Woolley) αυτοκτόνησε με πιστόλι για λόγους που σχετίζονται με τον εθισμό του με το EverQuest, ένα Μαζικά Πολυχρηστικό Διαδικτυακό Παιχνίδι Ρόλων(MMORPG), όπως ισχυρίστηκε η μητέρα του. Ο Άρμιν Μάιβες (Armin Meiwes) μαχαίρωσε μέχρι θανάτου και έφαγε μέρος του σώματος του Μπέρντ-Γιούργκεν Μπράντες (Bernd Jürgen Brandes) όταν ο τελευταίος απάντησε στην αγγελία του πρώτου που ζητούσε έναν «μεγαλόσωμο άνδρα έτοιμο να σφαγιαστεί και μετά να καταβροχθιστεί».

Πρόκειται για το περίφημο «σύμφωνο αυτοκτονίας» το οποίο περιγράφουμε.

1.8.3. Σύμφωνο αυτοκτονίας CYBERSUICIDE PACT)

Αποτελεί μια ιδιαίτερη συνεννόηση μεταξύ δυο ατόμων μέσω του internet. Αφορά νέους αποκλειστικά, οι οποίοι τείνουν να είναι άγνωστοι μεταξύ τους ή να συνδέονται με πλατωνική φιλία και έχουν κοινό χαρακτηριστικό την κλινική κατάθλιψη σύμφωνα με άρθρο που δημοσιεύθηκε στη Νέα Ζηλανδία το 2005. Το πρώτο περιστατικό συμφώνου αυτοκτονίας σημειώθηκε στην Ιαπωνία το 2000.Οπως υποστηρίζουν οι ειδικοί τα περιστατικά αυτά είναι σπάνια αφού στην Ιαπωνία αποτελούν το 2% των αυτοκτονιών και λιγότερο από το 0.01% του συνόλου των αυτοκτονιών. Παρ'όλα αυτά με την πάροδο του χρόνου η συχνότητά τους αυξάνεται.

1.8.4. Πρόληψη – Παρέμβαση αυτοκτονιών

Η παρέμβαση της αυτοκτονίας είναι η προσπάθεια για άμεση δράση ώστε το άτομο με τάσεις αυτοκτονίας να εμποδιστεί να θέσει τέρμα στη ζωή του ή να βλάψει τον εαυτό του. Άτομα που πάσχουν από κατάθλιψη θεωρούνται ομάδα υψηλού κινδύνου.

Ιατρικοί επαγγελματίες συμβουλεύουν πως οι άνθρωποι που έχουν εκφράσει πως σχεδιάζουν να θέσουν τέρμα ζωή τους πρέπει να ενθαρρύνονται να ζητούν άμεσα ιατρική συμβουλή. Αυτό είναι ιδιαίτερα σημαντικό σε περιπτώσεις που τα μέσα (όπλα,ναρκωτικά ή άλλες μέθοδοι) είναι διαθέσιμα.

Αξίζει να σημειωθεί ότι έχουν δημιουργηθεί πολλοί δικτυακοί τόποι αποτροπής αυτοκτονιών. Τόποι που προσφέρουν τη βοήθεια ειδικών, αλλά και ομάδες συνομιλίας με άλλους χρήστες που είχαν περάσει από ανάλογη κατάσταση. Οι υπευθύνοι τέτοιων δικτυακών τόπων θεωρούν την κάθε περίπτωση ξεχωριστή και προσπαθούν να βοηθήσουν όσο μπορούν περισσότερο τον άνθρωπο που υποφέρει.

Ακόμα κι αν πιστέψουν ότι δεν το εννοεί πραγματικά, συνεχίζουν να τον βοηθούν, καθότι το θέμα της αυτοκτονίας «είναι πολύ σοβαρό για να παίζει κανείς μαζί του». Πράγματα που πρέπει να γνωρίζει κανείς (αποτυχημένες απόπειρες που έχουν

συνέπειες σε όλη την υπόλοιπη ζωή, συνέπειες για τους συγγενείς, εμπειρίες άλλων, μέρη για βοήθεια, ψυχολογική στήριξη, πληροφορίες για το πώς οι συγγενείς μπορούν να καταλάβουν αν κάποιος έχει τάσεις αυτοκτονίας) διατίθενται εύκολα προς άμεση χρήση, με ένα σύνθημα που ισχύει για όλες τις περιπτώσεις: ποτέ δεν είναι αργά για ζωή.

Σημαντικό είναι βέβαια και το έργο της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος η οποία απέτρεψε συνολικά 159 προθέσεις αυτοκτονίας ατόμων μέσω διαδικτύου, από την αρχή του έτους. Από αυτές τις περιπτώσεις, οι 38 απετράπησαν το χρονικό διάστημα από 1-7-2014 μέχρι και 12-8-2014.

Σύμφωνα με τον προϊστάμενο της Δίωξης, ταξίαρχο Μανώλη Σφακιανάκη, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διενεργεί στο πλαίσιο των αρμοδιοτήτων της, ψηφιακή διαδικτυακή έρευνα σε 24ωρη βάση, για τον εντοπισμό συνανθρώπων μας, που τυχόν εκδηλώνουν πρόθεση αυτοκτονίας μέσω διαδικτύου.

Ειδικότερα, σε όλες τις περιπτώσεις, στο πλαίσιο της ψηφιακής έρευνας και ανάλυσης των ηλεκτρονικών ιχνών, προηγήθηκε επικοινωνία με τους διαχειριστές του εκάστοτε ιστοτόπου, όπου πραγματοποιούνταν η επίμαχη ανάρτηση. Ύστερα από την ψηφιακή ανάλυση των ηλεκτρονικών ιχνών κάθε περίπτωσης, ταυτοποιήθηκαν τα πλήρη στοιχεία του εκάστοτε κατόχου της επίμαχης σύνδεσης του διαδικτύου.

Στη συνέχεια, με την άμεση συνδρομή των κατά τόπους αρμόδιων Αστυνομικών Τμημάτων εντοπίστηκαν τα άτομα που προέβησαν στις αναρτήσεις με περιεχόμενο αυτοκτονικού ιδεασμού.

- Σε 15 περιπτώσεις κρίθηκε σκόπιμη η μεταφορά των εμπλεκομένων ατόμων σε εφημερεύουσες ψυχιατρικές κλινικές, ενώ 8 περιπτώσεις, εκ των οποίων 3 τον τελευταίο μήνα, κρίθηκε αναγκαία η παραμονή των ατόμων σε αυτές για νοσηλεία.
- Σε 4 περιπτώσεις τα εμπλεκόμενα άτομα μεταφέρθηκαν σε ιδιαίτερα άσχημη κατάσταση στα εφημερεύοντα νοσοκομειακά ιδρύματα, κατόπιν κατάποσης ποσότητας χαπιών, και παρέμειναν σε αυτά για νοσηλεία.
- Σε 14 περιπτώσεις, προέκυψε ότι τα εμπλεκόμενα άτομα διέμεναν στο εξωτερικό και ενημερώθηκαν οι αρμόδιες αστυνομικές αρχές μέσω της Διεθνούς Αστυνομικής Συνεργασίας (Interpol ή Sirene).

Συγκεκριμένα, δύο περιπτώσεις εκδήλωσης πρόθεσης αυτοκτονίας μέσω διαδικτύου σημειώθηκαν στην Κύπρο, τρεις στη Γερμανία, δύο στην Ιταλία και από μία σε Αυστρία, Αγγλία, Ισλανδία, Μολδαβία, Ολλανδία, Κροατία και Γαλλία.

Σύμφωνα με τον κ. Σφακιανάκη, το 30% των ατόμων που εκδηλώνουν πρόθεση αυτοκτονίας μέσω διαδικτύου είναι ανήλικοι. Όπως εξηγεί ο ίδιος σε συνέντευξή του

στο zougla.gr, η ιδέα της αυτοκτονίας μπορεί να αρχίσει ακόμα και από ένα παιχνίδι στο διαδίκτυο.

Παράλληλα επισημαίνει πως και τα οικονομικά προβλήματα οδηγούν πολλούς συνανθρώπους μας στο να αναρτήσουν ακόμα και σε μέσα κοινωνικής δικτύωσης τη σκέψη τους για αυτοκτονία.

ΚΕΦΑΛΑΙΟ 2.

Εγκληματολογική έρευνα συλλογή στοιχείων και εντοπισμός του ηλεκτρονικού εγκληματία

2.1. Ηλεκτρονική Εγκληματολογία (Computer Forensic)

Η *Εγκληματολογική Επιστήμη* (Forensic Science), ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο, ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία. Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες της επιστήμης αυτής.

Η Ηλεκτρονική Εγκληματολογία (Computer Forensic Science), είναι *«η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό»*. Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε έναν υπολογιστή. Είναι αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, αλλά και να τις συγκεντρώσουμε με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι διωκτικές αρχές πρέπει να αποδείξουν, ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορουμένου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατέστρεψε αποδείξεις σχετικές με την αθωότητα του κατηγορουμένου[15].

Ο Angus Marshall (Marshall 2008) ορθά αναφέρει στο βιβλίο του «Ηλεκτρονική Εγκληματολογία», ότι η ηλεκτρονική εγκληματολογία διαφέρει ώς κλάδος από τους υπόλοιπους κλάδους που απαρτίζουν το πεδίο της γενικότερης Εγκληματολογίας στο ότι το είδος των αποδεικτικών στοιχείων υπό έρευνα είναι προϊόν ανθρώπινης ιδιοφυΐας. Εμβαθύνοντας, αναφέρει ότι αντίθετα με τα στοιχεία που αφήνει μια βιολογική οντότητα σε μια σκηνή εγκλήματος, τα ηλεκτρονικά στοιχεία είναι εφήμερα, από την άποψη του ότι βασίζονται σε μια τεχνολογία που αλλοιώνεται και ανανεώνεται με τρομακτικό ρυθμό.

[15] e-crime.gr

ΣΥΝΤΟΜΗ ΙΣΤΟΡΙΑ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΚΛΗΜΑΤΟΛΟΓΙΑΣ	
1984	Πρόγραμμα Μαγνητικού Υλικού του FBI
1993	Το Παγκόσμιο Συνέδριο σε Στοιχεία Ηλ. Υπολογιστών
1995	Δημιουργία του Παγκόσμιου Οργανισμού Αποδεικτικών Στοιχείων Ηλ. Υπολογιστών (IOCE)
1997	Κλήση του IOCE και της G8 για πρότυπα
1998	Η G8 δίνει την εποπτεία του θέματος στον IOCE και το πρώτο Συμπόσιο Εγληματολογίας της INTERPOL για το θέμα του Ηλ. Εγκλήματος
1999	Το Παγκόσμιο Συνέδριο Προηγμένου Εγκλήματος και Εγκληματολογίας (IHCFC) και σχέδια προτύπων παρουσιάζονται στο G8
2000	Πρώτο Εργαστήριο Ηλ. Εγκληματολογίας του FBI

Όπως βλέπουμε στον παραπάνω πίνακα, η Ηλεκτρονική Εγκληματολογία, ώς επιστήμη, είναι αρκετά νέα στον χώρο της Εγκληματολογίας (υπάρχει απο τον 18ο με 19ο αιώνα), και είναι ουσιαστικά μείγμα κλασσικής Εγκληματολογίας και Επιστήμης Ηλ. Υπολογιστών.

2.2. Ανακριτική

Η **Ανακριτική** είναι ιδιαίτερος κλάδος της Ποινικής Επιστήμης, της Εγκληματολογίας, που έχει ως αντικείμενο μελέτης το έγκλημα, την αποκάλυψη του δράστη αυτού, τον εγκληματία και ως σκοπό την καταπολέμηση της εγκληματικότητας. Το ενδιαφέρον της ανακριτικής αρχίζει από την διάπραξη του εγκλήματος, ή και από την πρόληψη σχεδιαζόμενου μέχρι την έκδοση δικαστικής απόφασης ενοχής ή αθώωσης κατηγορουμένου.

Η Ανακριτική ως προς το αντικείμενο προσδιορισμού των οργάνων που επιλαμβάνονται της ανάκρισης των εγκλημάτων, καθώς και για την έρευνα, τη συλλογή και τον έλεγχο των αποδεικτικών στοιχείων που σχετίζονται με τη διάπραξη ενός εγκλήματος για την αποκάλυψη της ταυτότητας του δράστη, περίπου ταυτίζεται με το Ποινικό Δικονομικό Δίκαιο ή Ποινική Δικονομία(αποτελεί το σύνολο των κανόνων του δικαίου που καθορίζουν αφενός την αρμοδιότητα των οργάνων της πολιτείας και αφετέρου την διαδικασία δράσης των οργάνων αυτών, προκειμένου να βεβαιώσουν ενοχή κατηγορουμένου ώστε να επιβάλουν σε αυτή την από το ουσιαστικό Ποινικό Δίκαιο προβλεπόμενη ποινική κύρωση), που προσδιορίζει και τα όρια μέσα στα οποία μπορούν να δράσουν τα όργανα της ανάκρισης[16].

[16] http://users.sch.gr/efstratiou/ANAKRISI/anakritikesprajeis.pdf

Το ουσιώδες όμως σημείο της Ανακριτικής είναι η έρευνα σύγχρονων και αποτελεσματικών μεθόδων ανάκρισης καθώς μέσων και τρόπων διαλεύκανσης εγκλημάτων που δια της νομοθετικής οδού εμπλουτίζουν και εκσυγχρονίζουν την Ποινική Δικονομία, π.χ. η καθιέρωση πραγματογνωμόνων, η εισαγωγή επιστημονικών μεθόδων διάγνωσης κρίσιμων θεμάτων, όπως και άλλοι μέθοδοι και μέτρα, αποτελούν κατακτήσεις της Ανακριτικής.

Στο προβάδισμα αυτό της Ανακριτικής ακολουθούν πλέον οι διατάξεις της Ποινικής Δικονομίας που τακτικά αναπροσαρμόζονται στις σύγχρονες εξελίξεις, επιστημονικές και τεχνικές κατακτήσεις της Ανακριτικής.

Πρωτοπόρος και πατέρας της Ανακριτικής ως επιστημονικού κλάδου θεωρείται ο Χανς Γκρος (1847 – 1915), Αυτριακός ανακριτής και στη συνέχεια καθηγητής στο Πανεπιστήμιο του Γκρατς της Αυστρίας. Αυτός με τα περισπούδαστα έργα του «*Handbuch für Untersuchungsrichter als System der Kriminalistik*» και «*Handbuch fur Untersuchungsrichter, Polizeibeamte, Gendarmen, USW*» που αποτελούσαν Εγχειρίδια για τους ανακριτικούς υπαλλήλους της Αστυνομίας και της Αυτοκρατορικής χωροφυλακής, συστηματοποίησε και έθεσε σε ενιαίο σύγγραμμα τις βάσεις αλλά και τις αρχές καθώς και τις γνώσεις και μεθόδους που απαιτούνται για τον κάθε δικαστή – ανακριτή και ανακριτικό υπάλληλο προκειμένου να συλλέξει τις αποδείξεις και συνάγει αυτές σε κρίση και εκδίκαση υπόθεσης.

Το πρώτο παραπάνω σύγγραμμα του Χ. Γκρος μετέφρασε στην ελληνική ο μοίραρχος και μετέπειτα αντιστράτηγος της Ελληνικής Βασιλικής Χωροφυλακής Φ. Ζήρος.

Στην Ελλάδα πρώτος που ασχολήθηκε συστηματικά με την Ανακριτική ήταν ο Χ. Γιώτης ο οποίος και εξέδωσε συστηματικό έργο με τον τίτλο Ανακριτική. Πραγματικός όμως θεμελιωτής της Ανακριτικής στην Ελλάδα θεωρείται ο καθηγητής Κ. Γαρδίκας που τιτλοφόρησε το δεύτερο τόμο της εγκληματολογίας του «Αστυνομική», όπως ομοίως τιτλοφόρησε ο παραπάνω αντιστράτηγος ε.α. Φ. Ζήρος. Στη συνέχεια ο Σ. Τσαούσης δημοσίευσε σχετική εργασία με τον τίτλο «Αστυνομική Ανακριτική», ενώ ο Δ. Καρανίκας κάνει λόγο για «Επιστημονική ή Τεχνική Αστυνομία ή Ανακριτική». Τέλος ο Κ. Πίττος ως και οι καθηγητές Χωραφάς και Φιλιππίδης χρησιμοποιούν τον όρο «Εγκληματολογική Τακτική» ή «Εγκληματολογική Τεχνική» και ο Μαρκάτος τον όρο «Επιστημονική Αστυνομία».

Οι πράξεις αυτές περιγράφονται ρητά στο άρθρο 128 του Υ.Κ. και είναι όμοιου περιεχομένου με το άρθρο 228 του Π.Δ .611 /77. Οι ανακριτές, οφείλουν να συλλέγουν πληροφορίες :

α) εξετάζοντας μάρτυσες και τον κατηγορούμενο

β) να μεταβαίνουν επί τόπου για διενέργεια αυτοψίας, ή εν ανάγκη να χρησιμοποιούν πραγματογνώμονες

γ) να καταλαμβάνουν πειστήρια

δ) να πράττουν το παν αναγκαίο για τη συλλογή και διατήρηση των αποδείξεων ή των ιχνών του αδικήματος

Οι ανακριτικές πράξεις σύμφωνα με το άρθρο 22 του υπ' αριθμ. 285/1972 Β. Δ. (τώρα άρθρο 228 Π.Δ. 611/77) είναι οι εξής[17]:

α) η αυτοψία
β) η πραγματογνωμοσύνη
γ) η εξέταση μαρτύρων
δ) η εξέταση του διωκομένου
ε) η εκτίμηση των εγγράφων

2.2.1. Αυτοψία

Η αυτοψία είναι η δικονομική πράξη, με την οποία ο ενεργών προβαίνει στη διαπίστωση γεγονότων δια της εξετάσεως, μέσω των δικών του αισθήσεων, αντικειμένου ή αντικειμένων που έχουν σχέση με την διερευνούμενη πράξη. Η συναγωγή των παρατηρήσεων μπορεί να γίνει με οιανδήποτε των αισθήσεων και όχι μόνον δια της οράσεως, όπως θα νόμιζε κάποιος από τον όρο αυτοψία. Η αυτοψία ενεργείται με σκοπό την βεβαίωση των περιστάσεων κάτω από τις οποίες έγινε ορισμένο γεγονός (άρθρο 181 §1 ΚΠΔ). Αντικείμενο της μπορεί να είναι οποιοδήποτε γεγονός υπό την υλική του υπόσταση, όπως τόπος, πράγματα κλπ υπό την προϋπόθεση ότι αυτό έχει σχέση με την εξεταζόμενη υπόθεση.

Αυτοψία μπορεί να ενεργήσει και ο ανακριτής (άρθρο 251 ΚΠΔ) και είτε αυτοπροσώπως είτε με ειδικό υπάλληλο ή εμπειρογνώμονα να λάβει ιχνογραφήματα, φωτογραφίες ή άλλες απεικονίσεις. (αρθρο 181 ΚΠΔ). Όπως σε κάθε άλλη ανακριτική πράξη έτσι και στην αυτοψία συντάσσεται έκθεσης η οποία πρέπει να είναι λεπτομερείς ως προς την περιγραφή τόσον του τρόπου ή μεθόδου ενεργείας, όσο και των γενόμενων παρατηρήσεων, επισυναπτομένων σε αυτήν των ιχνογραμμάτων , φωτογραφιών κλπ.

2.2.2. Πραγματογνωμοσύνη

Εάν απαιτούνται για βεβαίωση, διάγνωση ή κρίση οποιουδήποτε γεγονότος ειδικές επιστημονικές ή τεχνικές γνώσεις, ο ενεργών της διοικητικής ανάκρισης δύναται να ορίσει πραγματογνώμονες.

[17] users.sch.gr

Όσον αφορά την διαδικασία του διορισμού των πραγματογνωμόνων, την υποχρέωση αποδοχής του διορισμού, τον όρκον και την θέση αυτών προς την εξέταση ζητημάτων, εφαρμόζονται οι ανάλογες διατάξεις του Κώδικα Ποινικής Δικονομίας.

Ως πραγματογνώμονες ορίζονται δημόσιοι υπάλληλοι, υπάλληλοι νομικών προσώπων δημοσίου δικαίου, καθώς και αξιωματικοί των ενόπλων δυνάμεων και σωμάτων ασφαλείας και του λιμενικού σώματος. Οι πραγματογνώμονες, πριν από τη διενέργεια της πραγματογνωμοσύνης, ορκίζονται σύμφωνα με τις διατάξεις του Κώδικα Ποινικής Δικονομίας.

Σύμφωνα με το άρθρο 251 ΚΠΔ, ο ανακριτής και οι ανακριτικοί υπάλληλοι που αναφέρονται στα άρθρα 33 και 34 όταν λάβουν παραγγελία του εισαγγελέα, και στις περιπτώσεις του άρθρου 243 παρ.2 αυτεπαγγέλτως, οφείλουν χωρίς χρονοτριβή να συγκεντρώνουν πληροφορίες για το έγκλημα και τους υπαιτίους του, να εξετάζουν μμάρτυρες και κατηγορουμένους, να μμεταβαίνουν επί τόπου για ενέργεια αυτοψίας, αφού πάρουν μαζί τους, αν υπάρχει ανάγκη, ιατροδικαστές ή άλλους πραγματογνώμονες, να διεξάγουν έρευνες, να καταλαμβάνουν πειστήρια και γενικά να ενεργούν οτιδήποτε είναι αναγκαίο για τη συλλογή και τη διατήρηση των αποδείξεων, καθώς και για την εξασφάλιση των ιχνών του εγκλήματος.

2.3. Η Δικαστική των ηλεκτρονικών υπολογιστών[18]

Η δικαστική των ηλεκτρονικών υπολογιστών όπως αποδίδεται στα ελληνικά ο όρος «Computer Forensics», είναι πλέον σημαντική για την εξιχνίαση των ηλεκτρονικών εγκλημάτων. Το ενδιαφέρον είναι ότι ενώ η Ανακριτική επικεντρώνεται μόνο στην ποινική δίκη, η νέα πειθαρχία, η οποία έχει ως αντικείμενο την αναγνώριση και τον εντοπισμό, τη συλλογή, τη διαφύλαξη, την ανάλυση και την παρουσίαση των ψηφιακών αποδεικτικών στοιχείων με τρόπο που είναι νομικά αποδεκτός, χρησιμοποιείται και στο πλαίσιο της αστικής δίκης, πράγμα που έχει γίνει σε πολλές σημαντικές υποθέσεις. Ο κλάδος αυτός έχει διαμορφωθεί μέσα από διάφορες τάσεις οι οποίες έχουν προκύψει κατά τη διάρκεια της ιστορίας των υπολογιστών.

Οι κύριες τάσεις έχουν, με τη σειρά τους, προκαλέσει πολλές άλλες μικρότερες τάσεις, και όλες έχουν αλληλεπιδράσει και ενδυναμώσει η μία την άλλη. Αυτές είναι:
α) η αύξηση σε χρήση και ισχύ των προσωπικών υπολογιστών
β) η κίνηση στο σχεδιασμό των εταιρικών υπολογιστικών συστημάτων μακριά από τον κεντρικό μονολιθικό υπολογιστή προς την πολλαπλότητα μικρότερων αλλά ισχυρών μηχανημάτων τα οποία αλληλεπιδρούν και αλληλοσυνδέονται σε μία μορφή που ονομάζεται κατανεμημένη επεξεργασία
γ) η αύξηση δικτύων, τόσο των ιδιωτικών όσο και, στη μορφή του Διαδικτύου,

[18] Αντώνιος Π. Μανιάτης, ΔiΜΕΕ, Τεύχος 4/2011, Έτος 8ο

παγκοσμίως δημοσίων. Όλες αυτές οι αλλαγές είχαν αντίκτυπο όχι μόνο στο τι θα μπορούσαν να μεταφέρουν οι υπολογιστές στους ιδιοκτήτες τους, αλλά και στους τύπους των αποδείξεων τις οποίες μπορεί να βρει
κανείς εκεί μέσα.

2.4. Τεχνικές της Δικαστικής των Ηλεκτρονικών Υπολογιστών εκτός Διαδικτύου[19]

Η πρώτη, και πιο προφανής τεχνική, περιλαμβάνει την κατάσχεση του εξοπλισμού πληροφορικής. Όταν γίνει αυτό, νόμοι και κατευθυντήριες οδηγίες θα διέπουν τη διαδικασία. Ο ίδιος ο υπολογιστής θα φωτογραφίζεται επιτόπου ενώ τα καλώδια και κάθε ξεχωριστό, εξωτερικό μέσο αποθήκευσης δεδομένων, όπως λόγου χάρη τα «φλασάκια», οι δίσκοι συμπίεσης και οι δισκέτες, θα πρέπει να καταγράφονται με ακρίβεια. Εξάλλου, οι υπολογιστές που λειτουργούν κατά τη στιγμή της επιδρομής θα πρέπει να απενεργοποιηθούν με ασφάλεια και επίσης θα πρέπει να καταχωρηθεί ξεχωριστά ο χρόνος, κατά τον οποίο σημειώθηκε το γεγονός. Καθώς οι ανακριτικές ενέργειες έχουν ως αντικείμενο και σημείο αναφοράς τους τον υπολογιστή, ο χρόνος απενεργοποίησης δηλώνεται όχι σύμφωνα με τα δεδομένα των διωκτικών αρχών αλλά όπως είναι καταγεγραμμένος στο εσωτερικό ρολόι του υπολογιστή.

2.4.1. Νομική αναπαράσταση

Τέλος, θα πρέπει να δημιουργηθεί ακριβές αντίγραφο κάθε σκληρού δίσκου, διαδικασία που ονομάζεται «νομική αναπαράσταση» («legal imaging»). Μάλιστα, διευκρινίζεται ότι συνήθως, στην πράξη, δημιουργούνται δύο αντίγραφα, με το ένα να λειτουργεί ως έλεγχος.

Ένας από τους λόγους για τους οποίους γίνεται η αναπαράσταση είναι να αποφευχθεί η μόλυνση των δεδομένων τα οποία βρίσκονται αποθηκευμένα στον υπολογιστή. Η ίδια η διαδικασία της ενεργοποίησης του υπολογιστή και της αντιγραφής των δεδομένων που περιέχει, μπορεί να αλλοιώσει τα δεδομένα σε τέτοιο βαθμό που αυτά να μολυνθούν. Η διαδικασία της νομικής αναπαράστασης θα πρέπει να πραγματοποιείται όσο το δυνατόν πιο σύντομα από τη στιγμή κατάσχεσης του υπολογιστή έπειτα από αυτό, θα ακολουθεί εξέταση των αντιγράφων του σκληρού δίσκου. Ο υπολογιστής πραγματοποιεί εκκίνηση με τον οδηγό δισκέτας μέσω ενός απλού λειτουργικού συστήματος. Το σύστημα αυτό διαθέτει οδηγούς οι οποίοι δίνουν εντολή στον υπολογιστή να αναγνωρίσει μια εξωτερική συσκευή αποθήκευσης.

Η αναπαράσταση που έχει καταγραφεί στην εξωτερική συσκευή αποτελεί ακριβές

[19] Αντώνιος Π. Μανιάτης, ΔiΜΕΕ, Τεύχος 4/2011, Έτος 8ο

αντίγραφο του σκληρού δίσκου (ενός ή και περισσότερων) του υπολογιστή. Ωστόσο, ένα από τα ουσιαστικά πλεονεκτήματα της διαδικασίας αυτής είναι ότι δεν καταγράφει μόνο τα αρχεία που συνήθως φαίνονται αλλά και τα μέρη του δίσκου τα οποία περιέχουν και άλλες χρήσιμες πληροφορίες, όπως τα ονόματα/μεγέθη των αρχείων και τις καταγραφές ώρας/ημερομηνίας. Επιπλέον, από τη διαδικασία αυτή μπορούν να ανακτηθούν περισσότερες αποκαλυπτικές πληροφορίες, όπως τμήματα από προηγουμένως διαγεγραμμένα αρχεία. Συνεπώς, ένας ειδικός της Δικαστικής των Ηλεκτρονικών Υπολογιστών θα μπορούσε να προσπαθήσει να «συναρμολογήσει» τέτοια έγγραφα. Ωστόσο, δεν είναι αυτός ο μόνος τρόπος με τον οποίο μπορούν να ανακτηθούν τα διαγεγραμμένα αρχεία.

Πολλές φορές τα αρχεία αυτά φαίνεται ότι απλώς δεν μπορούν να διαγραφούν. Τα λειτουργικά συστήματα των σύγχρονων υπολογιστών διαθέτουν ενσωματωμένες εφαρμογές ασφαλείας για να εμποδίζουν την τυχαία διαγραφή, δηλαδή το κατά λάθος σβήσιμο ενός αρχείου. Αυτό σημαίνει ότι ακόμη και αν ένα αρχείο έχει επιλεχθεί για διαγραφή, τα περιεχόμενά του δεν θα εξαφανιστούν, παρά μόνο όταν η συγκεκριμένη χωρική περιοχή που καταλάμβανε, καλυφθεί από καινούργια αρχεία. Όπως είναι σαφές, τέτοιες λειτουργίες που συγκεντρώνουν στοιχεία μπορεί να αποδειχτούν πιο προβληματικές στις περιπτώσεις κατά τις οποίες η έρευνα οδηγεί σε εταιρικές υποθέσεις. Σε μια μεγάλη εταιρία θα υπάρχουν συνήθως πολλοί υπολογιστές, οι οποίοι συχνά συνδέονται σε ένα ευρύ δίκτυο, μεταξύ συγκεκριμένων τμημάτων του οργανισμού, και/ή σε όλη την εταιρία. Οι πιθανές διακλαδώσεις του εξοπλισμού πληροφορικής που έχει κατασχεθεί είναι, υπό αυτές τις συνθήκες, πιο σοβαρές και ποικίλες. Υπάλληλοι, πελάτες και πιστωτές, ενδέχεται όλοι να επηρεαστούν. Πραγματικά, ανάλογα με τη συναλλαγές θα μπορούσε να διακοπεί. Σε καταστάσεις όπως αυτή, οι ερευνητές θα μπορούσαν να αναζητήσουν έναν υπάλληλο της εταιρίας για να τους βοηθήσει. Ειδικότερα, συνιστάται ο προσεταιρισμός ενός στελέχους που θα είναι υπεράνω υποψίας και θα διαθέτει επαρκή τεχνική γνώση γύρω από τους υπολογιστές έτσι ώστε να μπορεί να τους βοηθήσει στη διαδικασία της «νομικής αναπαράστασης».

Αν, όπως συχνά συμβαίνει στις έρευνες ηλεκτρονικού εγκλήματος, κάποια από τα στοιχεία προέρχονται από το Διαδίκτυο, η εφαρμογή αυτή θα μπορούσε να τοποθετηθεί είτε στον υπολογιστή του υπόπτου, είτε σε απομακρυσμένους ιστοτόπους. Συνεπώς, θα πρέπει να χρησιμοποιηθούν διαφορετικές ανακριτικές τεχνικές. Μαζί με τον ίδιο τον υπολογιστή του υπόπτου, άλλες πιθανές πηγές στοιχείων ενδεχομένως να περιέχουν το καταγεγραμμένο ιστορικό επικοινωνιών από την υπηρεσία παροχής Διαδικτύου που αυτός έχει επιλέξει, δεδομένα που βρίσκονται σε απομακρυσμένους ιστοτόπους και, φυσικά, το ιστορικό κλήσεων που διατηρεί η εταιρία τηλεφωνίας. Οι προσωπικοί υπολογιστές διατηρούν αρχεία που καταγράφουν τη δραστηριότητα στο Διαδίκτυο. Για παράδειγμα, διατηρούν αρχεία εισερχόμενης και εξερχόμενης ηλεκτρονικής αλληλογραφίας, συνδρομές σε ομάδες συζητήσεων και, πιθανώς, πρόσβαση σε καταγεγραμμένες ιδιωτικές συνομιλίες στο Διαδίκτυο.

Επιπλέον, οι υπολογιστές θέτουν σε «κρυφή μνήμη» (κρύπτη) προσφάτως χρησιμοποιημένα δεδομένα, σε περίπτωση που χρειαστεί να επαναχρησιμοποιηθούν σε σύντομο χρονικό διάστημα. Η συγκεκριμένη διαδικασία, χρησιμοποιούμενη σε συνδυασμό με το Διαδίκτυο, αποβαίνει ιδιαίτερα χρήσιμη, καθώς τα κρυφά αρχεία διατηρούν αντίγραφα των ιστοσελίδων όπως ακριβώς τις επισκέφθηκε κάποιος. Συνήθως αυτά τα αρχεία διατηρούνται για εβδομάδες ή μήνες αργότερα.

Επομένως, εξοικονομείται χρόνος, καθώς μια ιστοσελίδα μπορεί να ανακτηθεί από το αρχείο κρυφής μνήμης του φυλλομετρητή Διαδικτύου, χωρίς να χρειάζεται να την επισκεφτεί κανείς πάλι. Αυτό το γεγονός, με τη σειρά του, σημαίνει ότι η κυκλοφορία στο Διαδίκτυο ελαττώνεται. Το πλεονέκτημα που δίνεται στους ερευνητές μέσω αυτής της διαδικασίας έγκειται στο ότι μερικοί φυλλομετρητές και μερικά ειδικευμένα λογισμικά μπορούν να χρησιμοποιηθούν για να δει κανείς κρυφά αρχεία και, επίσης, συναφή αρχεία από το ιστορικό, τα οποία διατηρούν κάποιες πληροφορίες σχετικές με ώρα και ημερομηνία. Συνεπώς, είναι πιθανό να προσδιοριστεί αυτό που έβλεπαν, μέχρι το χρονικό σημείο της κατάσχεσης του υπολογιστή, στο Διαδίκτυο οι χρήστες ενός συγκεκριμένου υπολογιστή και επίσης, σε περιορισμένο βαθμό και μετά από προσεκτική ερμηνεία, και ο χρόνος της θέασης.

2.4.2. Sniffing

Ένας άλλος τρόπος με τον οποίο οι ερευνητές του ηλεκτρονικού εγκλήματος μπορούν να συλλέγουν αποδεικτικά στοιχεία, είναι να ωτακουστούν, ακριβέστερα να οσφραίνονται, την κυκλοφορία στο Διαδίκτυο κατά τη διαμετακόμιση μερικές φορές, η μέθοδος αυτή αναφέρεται ως «μύρισμα». Σε κάθε περίπτωση, στους ειδικούς της Πληροφορικής η μέθοδος αυτή είναι γνωστή με τον αγγλικό όρο «sniffing». Αρχικά, θα πρέπει να σημειωθεί ότι η συγκεκριμένη διαδικασία καθίσταται δύσκολη λόγω της έννοιας των επικοινωνιών πάνω στην οποία βασίζεται το Διαδίκτυο, η οποία ονομάζεται «ανταλλαγή πακέτων». Με απλά λόγια, προτού να σταλούν στον κυβερνοχώρο, τα μηνύματα σπάνε σε κομμάτια τα οποία στη γλώσσα των ειδικών ονομάζονται «πακέτα». Τα τμήματα αυτά επανασυναρμολογούνται μετά, όταν φτάνουν στον προορισμό τους. Η έννοια αυτή έχει στρατιωτικές καταβολές, καθώς υιοθετήθηκε από την Προηγμένη Υπηρεσία Ερευνητικών Προγραμμάτων (ARPA) υπό την αιγίδα του Υπουργείου Άμυνας των Η.Π.Α. στα τέλη της δεκαετίας του 1960, ως η βάση του δικού της δικτύου (ARPANET).

Τα προφανή στρατιωτικά πλεονεκτήματα που διασφάλιζε η συγκεκριμένη μέθοδος ήταν τόσο η μυστικότητα όσο και η ανθεκτικότητα των επικοινωνιών. Γνωρίζοντας αυτό, γίνεται προφανές ότι το να «αφουγκραστεί» κανείς, δηλαδή το να «μυρίσει» σαν τα λαγωνικά στο φυσικό κόσμο, το Διαδίκτυο απαιτεί όχι μόνο κατοχή δεδομένων, αλλά και επανασυναρμολόγησή τους. Το κάθε πακέτο χωριστά περιέχει πληροφορίες που αποκαλύπτουν την προέλευση, τον προορισμό και το περιεχόμενό

του. Καθένα από αυτά τα πακέτα έχει αριθμηθεί έτσι ώστε να διευκολύνει την επανασυναρμολόγηση.

Ωστόσο, αυτές οι τεχνολογικές πραγματικότητες μπορούν να προκαλέσουν γνήσιες δυσκολίες στους ερευνητές που μετέρχονται το «μύρισμα». Τα πρακτικά προβλήματα είναι ότι σε ορισμένα σημεία κατά μήκος της διαδρομής θα υπάρχει συντριπτική ποσότητα διαδικτυακής κυκλοφορίας και δεν θα μπορέσει κανείς να την επεξεργαστεί προκειμένου να εντοπίσει το αντικείμενο που ψάχνει· επίσης, σε κάθε περίπτωση, είναι θεμελιώδες για το σχεδιασμό του Διαδικτύου το γεγονός ότι, ακόμη και με τη μεταφορά ενός απλού μηνύματος του ηλεκτρονικού ταχυδρομείου, τα επιμέρους πακέτα μπορεί να ακολουθήσουν εντελώς διαφορετικές διαδρομές, δημιουργώντας έτσι το ενδεχόμενο να μην καταστεί δυνατή η απομόνωση ολόκληρης της σχετικής κυκλοφορίας». Συχνά αυτό σημαίνει ότι αν οι ερευνητές δεν εστιάζουν σε ένα συγκεκριμένο σημείο, στο δίκτυο, το οποίο να βρίσκεται πολύ κοντά είτε στον αποστολέα είτε στον παραλήπτη των μηνυμάτων, η διαδικασία μπορεί να αποβεί άκαρπη. Υπάρχει το θέμα της δικαιοδοσίας των ανώτερων αστυνομικών αρχών στο να ζητούν από τις υπηρεσίες παροχής Διαδικτύου να αποκαλύπτουν, για συγκεκριμένους λόγους, τού του θέματος να εξετάσουμε κάποιες από τις δυσκολίες που προέκυψαν από την ερμηνεία του όρου «επικοινωνιακά δεδομένα», στη διάρκεια της 22ης Πράξης Ρύθμισης των Ελεγκτικών Εξουσιών («RIPA») 2000.

Το Διοικητικό Επιτελείο δήλωσε ότι «Είναι σημαντικό να προσδιορίσουμε το τι περιλαμβάνει ο όρος επικοινωνιακά δεδομένα, εξίσου σημαντικό, όμως, είναι και το να αποσαφηνίσουμε το τι δεν περιλαμβάνει. Ο όρος επικοινωνιακά δεδομένα δεν περιλαμβάνει την έννοια κανενός είδους επικοινωνίας». Αυτή η διαφοροποίηση είχε γίνει, επίσης, και στο κομμάτι της νομοθεσίας το οποίο η RIPA 2000 αντικατέστησε. Σημαίνει ότι το περιεχόμενο των επικοινωνιών μπορεί να χρησιμοποιηθεί μόνο για ερευνητικούς σκοπούς· δεν γίνεται παραδεκτό από το δικαστήριο.

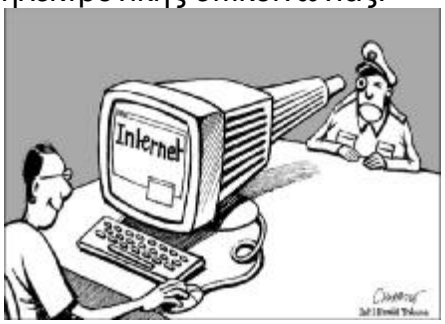
Αυτή η νομική διαφοροποίηση δεν συναντάται εύκολα σε άλλες δικαιοδοσίες που είναι παρόμοιες με αυτές του Ηνωμένου Βασιλείου. Ένα ακόμη πρακτικό πρόβλημα προκύπτει όταν αναφέρεται κανείς σε επικοινωνία που βασίζεται στο Διαδίκτυο. Στον ψηφιακό κόσμο, συχνά τα τεχνικά μέσα για τη συλλογή των δύο τύπων δεδομένων (είτε «επικοινωνία» είτε «περιεχόμενο») είναι τα ίδια. Συνεπώς, αυτό σημαίνει ότι μερικές φορές ο διαχωρισμός του ενός από το άλλο μπορεί να είναι δύσκολος. Για παράδειγμα, κάποια αιτήματα του Ιστού μπορεί να εμπίπτουν και στις δύο κατηγορίες.

2.5. Δίωξη ηλεκτρονικού εγκλήματος

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί ζήτημα υψίστης σημασίας για τις αστυνομικές αρχές, όπως άλλωστε και τα κοινά διαπραχθέντα εγκλήματα. Συγκεκριμένα, όσο αφορά τα ηλεκτρονικά εγκλήματα, που έχουν εισέλθει

στην καθημερινότητά μας τα τελευταία χρόνια, το ενδιαφέρον της αστυνομίας εστιάζεται περισσότερο στις ασταμάτητες αλλαγές που προκύπτουν στους κόλπους της τεχνολογίας και έτσι καθιστούν το ηλεκτρονικό έγκλημα ένα σχετικά δύσκολο ανιχνεύσιμο έγκλημα, τόσο στο εξωτερικό όσο και στον Ελλαδικό χώρο. Έτσι, αυτό που φαίνεται να κάνει αποτελεσματικότερο το έργο των διωκτικών αρχών είναι η συνεχής εκπαίδευση και επιμόρφωση του προσωπικού της αστυνομικής αρχής σε θέματα κυρίως τεχνικής φύσεως σχετικά με τη διερεύνηση και τη δίωξη του ηλεκτρονικού εγκλήματος.

Έτσι η Ελληνική αστυνομία (ΕΛ.ΑΣ) προχώρησε στη δημιουργία της Δίωξης ηλεκτρονικού εγκλήματος, η οποία ως αυτόνομη Κεντρική υπηρεσία έχει αποστολή την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών,που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.



Η Δίωξη Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή, αποτελείται από τέσσερα τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου.

Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

- Το Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων που ασχολείται με τις εγκληματικές πράξεις που διαπράττονται στα μέσα ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης ή μέσω αυτών σε ολόκληρη τη χώρα.
- Το Τμήμα Προστασίας Ανηλίκων που ασχολείται με τα εγκλήματα που διαπράττονται κατά των ανηλίκων με τη χρήση του διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.
- Το Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων που ασχολείται με τις υποθέσεις παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων, που τελούνται σε ολόκληρη τη χώρα.
- Το Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών, που ασχολείται με την πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών.

Η Δίωξη Ηλεκτρονικού Εγκλήματος αναπτύσσει έντονη δραστηριότητα για την ενημέρωση μικρών και μεγάλων χρηστών του διαδικτύου. Οργανώνει ημερίδες για την ασφαλή πλοήγηση - σε όλη τη Ελλάδα - με στόχο την ενημέρωση των πολιτών στις νέες τεχνολογίες και ειδικότερα στους κινδύνους ελλοχεύουν κατά την πλοήγηση στο διαδίκτυο.

Μάλιστα το Υπουργείο Προστασίας του Πολίτη και το Αρχηγείο της Ελληνικής Αστυνομίας με την υλοποίηση της Δίωξης Ηλεκτρονικού εγκλήματος προχώρησαν στην δημιουργία του www.cyberkid.gr , στο πλαίσιο ενημέρωσης και αισθητοποίησης παιδιών μέχρι ηλικίας 12 ετών, καθώς και των γονέων τους σχετικά με την ασφάλεια στο διαδίκτυο.

Το Cyberkid αποσκοπεί στην ασφαλή εξοικίωση του κοινού με τις νέες τεχνολογίες και ειδικότερα με internet.

Στόχος της δημιουργίας του Cyberkid είναι η προβολή των θετικών πλευρών του διαδικτύου, όπως είανι η ανεύρεση χρήσιμων πληροφοριών και η ψυχαγωγία. Παράλληλος στόχος είναι η ενημέρωση για τους πιθανούς κινδύνους που κρύβονται.

Οι γονείς μπορούν να επισπευτούν το Cyberkid μαζί με τα παιδιά τους, να διασκεδάσουν και να ενημερωθούν για το πώς μπορούν να πλοηγηθούν με ασφάλεια.

Στο πλαίσιο της πρωτοβουλίας www.cyberkid.gr δημιουργήθηκε και η εφαρμογή Cyberkid smartphones & tablets**.** Μάλιστα λίγες μόνο ημέρες μετά την επίσημη πρώτη της εφαρμογής για smartphones & tablets, το cyberkid βρίσκεται ήδη στις πρώτες θέσεις σε App store (No 21) στην κατηγορία news καιPlay Store (No 43) στην κατηγορία νέα applications. Παράλληλα και την ίδια περίοδο, η επισκεψιμότητα στο site www.cyberkid.gr αυξήθηκε κατά 300%.

Το γεγονός αυτό καταδεικνύει όχι μόνο τη χρηστικότητα της εφαρμογής, αλλά και τη διαρκή ανάγκη γονέων και παιδιών για έγκυρη ενημέρωση σχετικά με θέματα που αφορούν στην ασφαλή χρήση του διαδικτύου.

Ειδικότερα, το cyberkid ξεχωρίζει για την καινοτόμο - όχι μόνο σε ευρωπαϊκό επίπεδο αλλά και παγκοσμίως – Γραμμή SOS - Cyber Alert η οποία δίνει τη δυνατότητα στα παιδιά να επικοινωνούν άμεσα (touchscreen call) και σε πραγματικό χρόνο με το Κέντρο Επιχειρήσεων της Δίωξης Ηλεκτρονικού Εγκλήματος, με πρωταρχικό σκοπό τη διασφάλιση της σωματικής ακεραιότητας των παιδιών, καθώς και κάθε γεγονότος το οποίο έχει να κάνει με κίνδυνο ή απειλή ζωής κατά αυτών.

Επιπλέον στην Ελλάδα, σχετικός με καταγγελίες για το ηλεκτρονικό έγκλημα είναι και

ο ιστότοπος www.safeinternet.gr. Στο συγκεκριμένο ιστότοπο δράσης, ενημέρωσης και επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου(υπό την αιγίδα της Ευρωπαϊκής Ένωσης) υπάρχουν πολλές, χρήσιμες πληροφορίες και συμβουλές για την ορθή χρήση του Διαδικτύου, του κινητού τηλεφώνου και άλλων διαδραστικών τεχνολογιών.

2.6. Ψηφιακές αποδείξεις και δεδομένα

Η λεγόμενη ψηφιακή απόδειξη (digital evidence) δεν ταυτίζεται με τα παραδοσιακά αποδεικτικά μέσα, καθότι τα τελευταία είναι χειροπιαστά, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα τα ψηφιακά αποδεικτικά μέσα είναι κατά κανόνα μη χειροπιαστά. Επίσης μπορεί να τα κατευθύνει κάποιος ή και να τα διαχειρίζεται από μακριά, να αλλάζει την μορφή και το περιεχόμενό τους ή ακόμα και να τα εξαφανίζει με το πάτημα ενός πλήκτρου.

Γενικά στη Δικονομία και την Ανακριτική με τον όρο απόδειξη, χαρακτηρίζεται το σύνολο των ενεργειών, μεθόδων, δια των οποίων είναι δυνατόν να σχηματιστεί η πεποίθηση για την αλήθεια ή όχι γεγονότων ή προβαλλομένων ισχυρισμών. Κάθε μία ενέργεια ή μέσο που λαμβάνεται ή ακολουθείται επ΄ αυτού αποτελεί αποδεικτικό στοιχείο.

Οι ψηφιακές αποδείξεις αποτελούν το πιο σπουδαίο αποδεικτικό μέσο, κατά την εξέταση μιας υπόθεσης ηλεκτρονικού εγκλήματος και γενικά κατά την εξέταση οποιουδήποτε στοιχείου έχει ψηφιακή μορφή. Ο SWGDE (Scientific Working Group on Digital Evidence), μια κοινοπραξία διεθνών οργανισμών, που δραστηριοποιείται στον τομέα των ψηφιακών αποδείξεων, τον Οκτώβριο του 1999 προτυποποίησε τις αποδείξεις που έχουν ψηφιακή μορφή, διαχωρίζοντάς τις σε[20]:

- ***Ψηφιακές αποδείξεις (digital evidence)****:* Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή.
- ***Αντικείμενα δεδομένων (data objects)****:* Αντικείμενα ή πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.

[20] E-crime.gr

- ***Φυσικά αντικείμενα (physical items):*** Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω τον οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.
- ***Γνήσιες ψηφιακές αποδείξεις (original digital evidence):*** Φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.
- ***Διπλότυπες ψηφιακές αποδείξεις (duplicate digital evidence):*** Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.
- ***Αντίγραφο (copy):*** Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο, ανεξάρτητα από το αντικείμενο αυτό.

Οι ψηφιακές αποδείξεις μπορεί να είναι αποθηκευμένες σε οποιαδήποτε συσκευή, όπως ηλεκτρονικό υπολογιστή, laptop, κινητό τηλέφωνο κ.α., καθώς και σε οποιοδήποτε μέσο αποθήκευσης, όπως δισκέτες, CDs, DVDs, κάρτες μνήμης κ.α.

Βασικό χαρακτηριστικό των ψηφιακών αποδείξεων είναι ο μεγάλος βαθμός μεταβλητότητάς τους. Μπορούν πολύ εύκολα να τροποποιηθούν ή να καταστραφούν με τη χρήση διαφόρων εργαλείων και μεθόδων. Ο ερευνητής, λοιπόν, πρέπει να αναζητεί και να μεταχειρίζεται τις πληροφορίες αυτές με ιδιαίτερη δεξιότητα.

Οι ψηφιακές αποδείξεις αποτελούνται από *ψηφιακά δεδομένα* (digital data). Μια πολύ σημαντική διάκριση των ψηφιακών δεδομένων είναι σε *μεταβλητά δεδομένα* (volatile data) και σε *διαρκή δεδομένα* (persistent data).

Τα μεταβλητά, είναι δεδομένα που αποθηκεύονται στην μνήμη του συστήματος (π.χ. μητρώο συστήματος, cache, μνήμη RAM) και χάνονται αν σταματήσει η τροφοδοσία του υπολογιστή με ρεύμα, αν γίνει τερματισμός της λειτουργίας του ή επανεκκίνηση.

Τα διαρκή δεδομένα είναι αποθηκευμένα στους σκληρούς δίσκους του συστήματος ή σε άλλες συσκευές μόνιμης αποθήκευσης, όπως οδηγοί USB, CDs και κάρτες μνήμης. Τα δεδομένα αυτά δεν χάνονται, όταν τερματιστεί η λειτουργία του υπολογιστή ή γίνει επανεκκίνηση.

2.6.1. Βασική διάκριση των αποδείξεων στη ποινική δικονομία

Βασική διάκριση των αποδείξεων στη ποινική δικονομία είναι

- **v** Η Άμεση ή ευθεία απόδειξη και η έμμεση απόδειξη, όπου στη μεν πρώτη το γεγονός που ερευνάται προκύπτει αμέσως, π.χ. από επίσημο έγγραφο, ενώ

στη δεύτερη αποτελεί ένδειξη.

- **v** Η Πλήρης απόδειξη και η ατελής απόδειξη, όπου στη μεν πρώτη η δικανική πεποίθηση παράγεται ευθέως και δεν χρήζει άλλων τινών, ενώ στη δεύτερη παράγονται πιθανολογήσεις.
- **v** Η Γενική απόδειξη και η ειδική απόδειξη, όπου η μεν πρώτη αναφέρεται γενικά στην αξιόποινη πράξη, ενώ η δεύτερη σε κάποιο συγκεκριμένο έμα ή στάδιο αυτής.
- **v** Η Εκούσια απόδειξη και ακούσια απόδειξη που χαρακτηρίζονται εκ της παραγωγής τους.

2.6.2. Τρόπος εκτίμησης αποδεικτικών στοιχείων

Ιδιαίτερη διάκριση της απόδειξης κατά θεωρητική αλλά και πρακτική σημασία είναι: η νομική απόδειξη και η ηθική απόδειξη.

Νομική απόδειξη λέγεται εκείνη που φέρεται σε κανόνες ρητά διατυπωμένους σε νόμους προκειμένου να αποτελέσουν οδηγία στους δικαστές στη κατάρτιση της απόφασή τους. όπως π.χ. ο νόμος ορίζει «*δύο μάρτυρες = πλήρης απόδειξη, ένας μάρτυρας = κανείς μάρτυρας*». Στην περίπτωση αυτή ισχύει η Αρχή της Νομικής Απόδειξης.

Αντίθετα, ηθική απόδειξη λέγεται εκείνη δια της οποίας η δικανική πεποίθηση προέρχεται από άμεση και ελεύθερη διάγνωση που απορρέει συνηθέστερα από την πείρα και τη σκέψη. Στην περίπτωση αυτή ισχύει η Αρχή της ηθικής απόδειξης όπως ορίζει το Άρθρο 177 ΚΠοινΔ. Σύμφωνα με το οποίο:

Οι δικαστές δεν είναι υποχρεωμένοι να ακολουθούν νομικούς κανόνες αποδείξεων, πρέπει όμως να αποφασίζουν κατά τη πεποίθησή τους, ακολουθώντας τη φωνή της συνείδησής τους και οδηγούμενοι από την απροσωπόληπτη κρίση που προκύπτει από τις συζήτησεις και που αφορά την αλήθεια των πραγματικών γεγονότων, την αξιοπιστία των μαρτύρων και την αξία των άλλων αποδείξεων.

Αποδεικτικά μέσα, που έχουν αποκτηθεί με αξιόποινες πράξεις ή μέσω αυτών, δεν λαμβάνονται υπόψη στην ποινική διαδικασία." *** Το κείμενο του άρθρου 177 αριθμήθηκε ως παράγραφος 1 και η παρ.2 προστέθηκε με την παρ.7 άρθρ.2 Ν.2408/1996 (Α 104) και αντικαταστάθηκε στη συνέχεια ως άνω με το άρθρο 10 παρ.2 Ν.3674/2008,ΦΕΚ Α 136/10.7.2008.

Το ουσιαστικό στη πράξη των δύο παραπάνω ειδών είναι ότι ενώ στη νομική απόδειξη ένας μάρτυρας ισοδυναμεί με κανένα, στην ηθική απόδειξη μπορεί ο ένας μάρτυρας κρινόμενος αξιόπιστος να διαμορφώσει δικανική πεποίθηση περί

αθώωσης ή ενοχής παρά την ύπαρξη περισσοτέρων μαρτύρων πλην όμως αναξιόπιστων με αντίθετες καταθέσεις.

2.7 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).

Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασυμμετρική κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασυμμετρική κρυπτογραφία αποδεικνύει την ακεραιότητας του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα).

Σε μερικές χώρες όπως τις ΗΠΑ και κάποιες χώρες της Ευρωπαϊκής ένωσης, οι ψηφιακές υπογραφές έχουν και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές υλοποιούνται - εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επίσης το φυσικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε (όσο το ιδιωτικό κλειδί που χρησιμοποίησε δεν υποκλάπηκε).

Κάποιες υλοποιήσεις των ψηφιακών υπογραφών προσθέτουν και την ημερομηνία υπογραφής του εγγράφου, ώστε και τον ιδιωτικό κλειδί να υποκλαπεί, η ψηφιακή υπογραφή να είναι έγκυρη. Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από bits (δηλαδή δεδομένα): παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου,έγγραφα, μηνύματα που στέλνονται στο

Διαδίκτυο κλπ. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύγεται η αποστολή τυπωμένων εγγράφων (επικυρωμένα με χρήση σφραγίδων και υπογραφών).

Η ψηφιακή υπογραφή αποτελείται από τρεις αλγόριθμους:

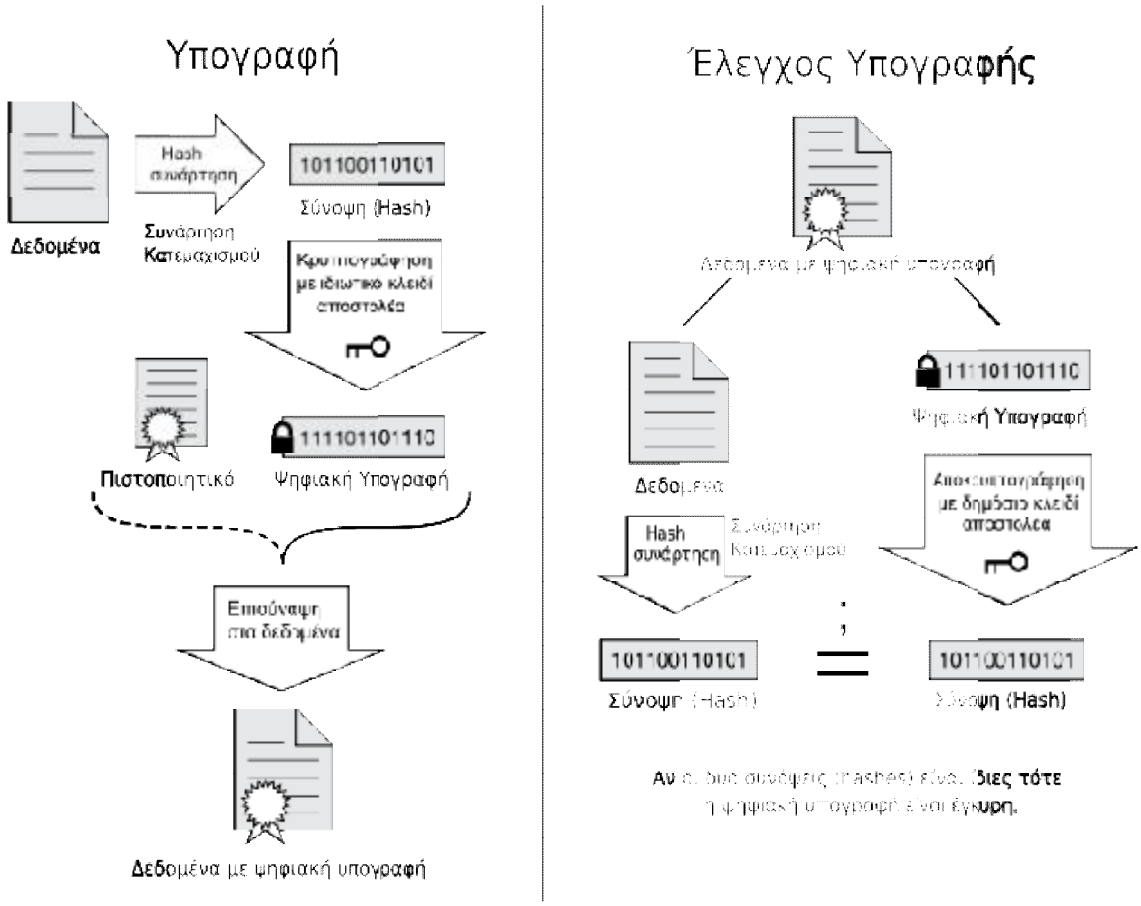
- Ο αλγόριθμος δημιουργίας δημόσιου και ιδιωτικού κλειδιού: Ο αλγόριθμος αυτός χρησιμοποιεί μια γεννήτρια τυχαίων αριθμών και με βάση αυτόν τον τυχαίο αριθμό δημιουργεί το δημόσιο και ιδιωτικό κλειδί (με το ιδιωτικό κλειδί δημιουργείται η ψηφιακή υπογραφή και με το δημόσιο κλειδί ελέγχεται η ψηφιακή υπογραφή).
- Ο αλγόριθμος προσθήκης ψηφιακής υπογραφής σε μηνύματα ή έγγραφα: Χρησιμοποιώντας το μήνυμα/έγγραφο και το ιδιωτικό κλειδί (το οποίο ανήκει μόνο σε αυτόν που υπογράφει το έγγραφο), δημιουργεί την ψηφιακή υπογραφή.
- Ο αλγόριθμος έλεγχου ψηφιακής υπογραφής μηνύματος ή εγγράφου:

Χρησιμοποιώντας το μήνυμα/έγγραφο και το δημόσιο κλειδί (το δημόσιο κλειδί είναι διαθέσιμο σε όλους, και συσχετίζεται με το ιδιωτικό κλειδί και ανήκει αυτόν που υπέγραψε ψηφιακά το μήνυμα/έγγραφο), ελέγχει την αυθεντικότητα (ποιος το υπέγραψε) αλλά και ακεραιότητα (ότι το μήνυμα δεν παραποιήθηκε) του μηνύματος/εγγράφου.

Σύμφωνα με την ασυμμετρική κρυπτογράφηση κάποιος που γνωρίζει το δημόσιο κλειδί δεν μπορεί να δημιουργήσει (είναι υπολογιστικά ανέφικτο) το αντίστοιχο ιδιωτικό κλειδί. Επίσης κάποιος ο οποίος έχει το δημόσιο κλειδί μπορεί να ελέγξει την αυθεντικότητα και ακεραιότητα ενός μηνύματος/εγγράφου το οποίο είναι ψηφιακά υπογεγραμμένο.

Ένα πρόβλημα με τις ψηφιακές υπογραφές είναι ότι δεν γνωρίζουμε αν το δημόσιο κλειδί (κατά την διάρκεια ελέγχου της υπογραφής) που έχουμε ανήκει σε αυτόν που ισχυρίζεται ότι είναι. Για αυτό ακριβώς τον λόγο υπάρχει ο Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος είναι ένας οργανισμός-οντότητα ο οποίος πιστοποιεί την σχέση ενός ανθρώπου με το δημόσιο κλειδί του.

Ο Πάροχος Υπηρεσιών Πιστοποίησης θα πρέπει να εμπνέει εμπιστοσύνη γιατί είναι η αρχή η οποία εκδίδει ψηφιακά πιστοποιητικά. Τα ψηφιακά πιστοποιητικά ταυτοποιούν ένα δημόσιο κλειδί με τον δικαιούχο του. Πολλές φορές αυτός που υπογράφει ψηφιακά ένα ηλεκτρονικό έγγραφο, ενδέχεται να επισυνάψει στο έγγραφο μαζί με την ψηφιακή υπογραφή και το ψηφιακό πιστοποιητικό του δημόσιου κλειδιού.



Διάγραμμα χρήσης ψηφιακής υπογραφής: Η ψηφιακή υπογραφή είναι η σύνοψη του μηνύματος κωδικοποιημένη με το ιδιωτικό κλειδί του αποστολέα. Μαζί με την ψηφιακή υπογραφή μπορεί να επισυνάπτει και το πιστοποιητικό (από έμπιστη/ο αρχή-οργανισμό) το οποίο πιστοποιεί τον ιδιοκτήτη του δημόσιου κλειδιού (το πιστοποιητικό μπορεί να χρησιμοποιηθεί αργότερα στον έλεγχο της υπογραφής).

Στο Ποινικό Δίκαιο ο Νομοθέτης προσδιορίζει την έννοια του ηλεκτρονικού εγγράφου στο άρθρο 13 περίπτ. γ του Π.Κ., όπως αυτό τροπ. με άρθρο 2 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. ΄Εγγραφο 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

μηχανική απεικόνιση.

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.

2.8. Διάρκεια της διαδικτυακής έρευνας

Η έρευνα των Ηλεκτρονικών Εγκλημάτων είναι αρκετά δύσκολη και ιδιαίτερα χρονοβόρος διαδικασία του εντοπισμού των «ηλεκτρονικών ιχνών». Μία έρευνα μπορεί να διαρκέσει από ένα μήνα έως και δύο χρόνια. Ο λόγος της μεγάλης διάρκειας είναι διότι οι χρήστες του Διαδικτύου που ερευνώνται και που έχουν καταγγελθεί στην υπηρεσία ότι έχουν διαπράξει μια αξιόποινη πράξη λαμβάνουν διάφορα διαδικτυακά μέτρα προστασίας, έτσι ώστε ο εντοπισμός του να καθίσταται αρκετά δύσκολος.

Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του «ηλεκτρονικού ίχνους» του δράστη, το οποίο για κάθε χρήστη του Ιντερνέτ είναι μοναδικό, και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Η λεγομένη ηλεκτρονική απόδειξη (electronic evidence) δεν ταυτίζεται με τα παραδοσιακά αποδεικτικά μέσα. Τα τελευταία, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα, τα ηλεκτρονικά αποδεικτικά μέσα είναι ψηφιακά.

Σύμφωνα με τον Προϊστάμενο του Τμήματος Ηλεκτρονικού Εγκλήματος/ΔΑΑ, Αστυνόμο Α΄ κ. Εμμανουήλ Σφακιανάκη «ο σωστός συνδυασμός των τεχνικών μέσων μαζί με τον ανθρώπινο παράγοντα είναι η χρυσή συνταγή για καλά αποτελέσματα. Εάν υπάρχουν τα τεχνολογικά μέσα (η/υ μαζί με λογισμικό) χωρίς την κατάλληλη εξειδίκευση του αστυνομικού προσωπικού, τότε τα αποτελέσματα δεν θα είναι τα αναμενόμενα. Στην υπηρεσία μας πιστεύω ότι υπάρχει η σωστή αναλογία σε τεχνικά μέσα και προσωπικό».

Η ηλεκτρονική έρευνα ενός εγκλήματος ή μιας αξιόποινης ενέργειας που γίνεται στον υπολογιστή (όπου αναζητούμε ψηφιακά πειστήρια) διαφέρει σημαντικά από την «παραδοσιακή έρευνα» που αναζητά απτά στοιχεία. Ο ηλεκτρονικός ερευνητής δεν αναζητά σε κάποιο συρτάρι ή σε κάποιο φυσικό χώρο αλλά σε ηλεκτρονικούς φακέλους, αρχεία, αποθηκευτικά μέσα, υπολογιστικά συστήματα.

Τα ψηφιακά αποδεικτικά στοιχεία που συλλέγονται και τα ψηφιακά πειστήρια που προκύπτουν από την ανάλυση, θεωρούνται ιδιαιτέρως ευαίσθητα, γι' αυτό σημαντικό κομμάτι της ηλεκτρονικής έρευνας αποτελεί η διατήρησή τους και η διασφάλιση της μη αλλοίωσής τους.

Η έρευνα ψηφιακών πειστηρίων, πρέπει να διεξάγεται σύμφωνα με την ισχύουσα κατά περίπτωση νομοθεσία, καθώς πολλές αμφιβολίες δημιουργούνται για την επάρκεια των γνώσεων ενός ερευνητή και για το αν η ανάλυση και διατήρηση των στοιχείων ακολουθεί τις προβλεπόμενες διαδικασίες. Κατά συνέπεια, πολλές φορές παρατηρείται το φαινόμενο σε μία δίκη να αμφισβητείται είτε η έρευνα, είτε να κατάσχονται οι πληροφορίες, επειδή δεν υφίσταται ειδικό νομοθετικό πλαίσιο στην περίπτωση των ερευνών στον κυβερνοχώρο.

Κατά τη διεξαγωγή μιας έρευνας σε ηλεκτρονικά δεδομένα, είναι σημαντικό να μην παραβιάζεται η ιδιωτικότητα του ατόμου κατά την εύρεση κάποιου ψηφιακού πειστηρίου. Κατόπιν τούτου, απαιτείται συνήθως ένταλμα που θα πρέπει να καθορίζει με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν και ακόμα και αν ο ερευνητής θεωρεί ότι μπορεί να αντλήσει στοιχεία και από άλλα εκτός των παραπάνω αντικείμενα, τα στοιχεία αυτά δεν θα έχουν αποδεικτική αξία στη δικαστική αίθουσα.

Ο ερευνητής ενός ηλεκτρονικού εγκλήματος χρησιμοποιεί τα εξειδικευμένα εργαλεία του ακολουθώντας συγκεκριμένα βήματα κατά τη διαδικασία της έρευνας:

- Προσδιορισμός μέσων εγγραφής των δεδομένων και φωτογράφηση ώστε να μπορεί να αποδειχθεί το φυσικό περιβάλλον και η κατάσταση των στοιχείων.

- Δημιουργία χώρων ασφάλισης των δεδομένων.

- Κατάρτιση καταλόγου των στοιχείων που μπορεί να περιλαμβάνει: φορητούς ηλεκτρονικούς υπολογιστές, σκληρούς ή εξωτερικούς δίσκους, μέσα εγγραφής εφεδρικών αντιγράφων, DVD, CD κλπ., κλειδιά USB, υπολογιστές τσέπης, έξυπνα τηλέφωνα, ανάλυση δραστηριοτήτων δικτύου.

- Δημιουργία φακέλου εγκληματολογικών αποδεικτικών στοιχείων, που δεν είναι δυνατόν να διαγραφούν ή να απομακρυνθούν, ώστε να διασφαλίζεται η ακεραιότητα των δεδομένων.

- Καταχώριση και ασφάλιση της ηλεκτρονικής εικόνας του δίσκου εγκληματολογικών δεδομένων και εργασία του υπευθύνου σε αντίγραφο εργασίας.

- Αναζήτηση και άλλων πηγών άντλησης δεδομένων, όπως υποδεικνύει η πορεία της υπόθεσης.

- Εξέταση των δεδομένων με το κατάλληλο λογισμικό ώστε να καταστούν

αναγνώσιμα τα αναζητούμενα δεδομένα και χρήση π.χ. λέξεων κλειδιών για τον εντοπισμό δεδομένων σχετικών με την υπόθεση. Επιβαρυντικά και μη στοιχεία συλλέγονται και αποκρυπτογραφούνται αρχεία και σπάνε κωδικοίασφαλείας.

- Στη συνέχεια συντάσσεται έκθεση στην οποία καταγράφεται κάθε στάδιο της ηλεκτρονικής εγκληματολογικής έρευνας με τα ευρήματα.
- Αν θεωρηθεί απαραίτητο, ο ερευνητής παρίσταται ως μάρτυρας στη δικαστική αίθουσα.

Η έρευνα ψηφιακών πειστηρίων πρέπει να πραγματοποιείται βάσει των κάτωθι αρχών:

1. Καμία ενέργεια δε δύναται να μεταβάλει δεδομένα που τηρούνται σε υπολογιστή ή μέσο αποθήκευσης, τα οποία μπορεί να προσκομισθούν στο δικαστήριο.
2. Χρήση αρχέτυπων δεδομένων από τρίτο άτομο, κατόπιν εξουσιοδότησης.
3. Δημιουργία ιστορικού ελέγχου των διαδικασιών.
4. Το άτομο που έχει οριστεί ως υπεύθυνος της έρευνας, επιφορτίζεται με τη γενική ευθύνη για τη διασφάλιση τήρησης της επικείμενης νομοθεσίας και των εν λόγω αρχών.

2.9. **Το προφίλ του δράστη και του ερευνητή της Δίωξης Ηλεκτρονικού Εγκλήματος**

Στο σημείο αυτό θα προσπαθήσουμε να σκιαγραφήσουμε το προφίλ του cybercriminal επιλέγοντας κάποια γενικά χαρακτηριστικά καθώς και τα χαρακτηριστικά που πρέπει να συγκεντρώνει ένας καλός ερευνητής, ο οποίος χειρίζεται την διαλεύκανση μιας υπόθεσης που αφορά την τέλεση ηλεκτρονικού εγκλήματος.

2.9.1. Τα χαρακτηριστικά ενός cybercriminal[21].

Στην μεγάλη πλειοψηφία τους οι εγκληματίες αυτής της κατηγορίας συγκεντρώνουν κάποια από τα ακόλουθα χαρακτηριστικά:

Ένα ελάχιστο επίπεδο γνώσης σε τεχνολογικά θέματα: Το χαρακτηριστικό αυτό βασίζεται στην κοινή λογική. Οι άνθρωποι γενικά χρησιμοποιούν εργαλεία με τα οποία αισθάνονται άνετα, πολύ περισσότερο όταν το εγχείρημα τους εμπεριέχει μια δόση κινδύνου, όπως είναι η τέλεση εγκλήματος. Ο τυπικός «κυβερνοεγκληματίας» δεν είναι «κομπιουτεροφοβικός» ή κάποιος που συνδέθηκε στο Ιντερνετ για πρώτη

[21] Debra Littlejohn Shinder, Ed Tittel , «Scene of cybercrime Computer Forensics Handbook» σελ. 111-11

φορά.

Δυσαρέσκεια ως προς τον Νόμο ή θεωρούν τον εαυτό τους πάνω από τον νόμο : Πολλοί διαπράττοντας μία πράξη ενάντια στον νόμο, θεωρούν ότι ο νόμος είναι κακός και όχι αυτοί που τον παραβαίνουν. Με αυτό τον τρόπο δείχνουν την δυσαρέσκεια τους.

Χώρος μιας φανταστικής ζωής: Πολύ χρησιμοποιούν τον κυβερνοχώρο σαν μία διέξοδο από την καθημερινότητα τους. Με τον τρόπο αυτό και το πέπλο τις ανωνυμίας υποδύονται διαφορετικές προσωπικότητες καλύπτοντας τις ατέλειες τους και ικανοποιώντας τις φαντασιώσεις τους.

Ρίσκο / επιζητούν τον έλεγχο μιας κατάστασης: Είναι πρόκληση ότι κάνουν κάτι απαγορευμένο, του οποίου έχουν τον απόλυτο έλεγχο αφού είναι δύσκολα εντοπίσιμοι.

Ισχυρά κίνητρα –διαφορετικά: Οι περισσότεροι έχουν ένα ισχυρό κίνητρο το οποίο μπορεί να είναι η επιθυμία πλουτισμού, σεξουαλική ικανοποίηση, πολιτικά κίνητρα ή κάποια βαθύτερη αιτία που κινείται στον χώρο της ψυχικής ασθένειας. Ξεχωρίζοντας το κίνητρο είναι ένα σημαντικό κριτήριο για να κατασκευάσουμε το προφίλ του κυβερνοεγκληματία.

2.9.1.1. Αναγνωρίζοντας τα κίνητρα των «cybercriminals»[22].

Πολλοί πιστεύουν ότι η απάντηση στο ερώτημα «Τι ωθεί τους εγκληματίες στην διάπραξη αξιόποινων πράξεων» είναι «γιατί είναι εγκληματίες». Όμως η απάντηση δεν είναι τόσο απλή.

Οι άνθρωποι σπάζουν τα όρια των νόμων για πολλούς και διαφορετικούς λόγους. Κάποιοι από τους λόγους αυτούς είναι εν μέρει δικαιολογήμενοι, όπως όταν η μητέρα δεν έχει χρήματα για να αγοράσει το γάλα του παιδιού της, κλέβει ένα μπουκάλι γάλα.

Γιατί έχει σημασία το κίνητρο; Σε πολλά δικονομικά συστήματα, το λεγόμενο τρίγωνο του εγκλήματος απαρτίζεται από: τον τρόπο διάπραξης , το κίνητρο (ο λόγος διάπραξης του εγκλήματος) και η δυνατότητα (να είσαι στο σωστό μέρος την κατάλληλη στιγμή για την διάπραξη του εγκλήματος). Έτσι καταλαβαίνοντας το κίνητρο, μας εξυπηρετεί στην εξιχνίαση του εγκλήματος.

Τα συνηθέστερα κίνητρα για την διάπραξη ενός cybercrime είναι:
α) Διασκέδαση
β) Χρηματικό όφελος.

[22] . Debra Littlejohn Shinder, Ed Tittel , «Scene of cybercrime Computer Forensics Handbook» σελ. 113-11

γ) Θυμό, εκδίκηση και άλλου τύπου συναισθήματα.
δ) Πολιτικά κίνητρα.
ε) Σεξουαλικά κίνητρα.
στ) Σοβαρές ψυχικές ασθένειες.

Στο σημείο αυτό θα προσπαθήσουμε να αναλύσουμε τα κίνητρα αυτά.

α) Διασκέδαση.

Νεαροί hackers είναι αυτοί που εμπίπτουν σε αυτή την κατηγορία. Σύμφωνα με τον J. Maxwell in the Electronic Processing Audit, Control and Security Newsletter, οι hachers αυτής της κατηγορίας μπορούν να ταξινομηθούν σε περαιτέρω κατηγορίες:

Pioneer types: οι οποίοι μαγεύονται από την τεχνολογία. Βρίσκουν ενδιαφέρον πως λειτουργεί ένα σύστημα και προσπαθούν να «σπάσουν» τα συστήματα ασφαλείας του και έτσι το κάνουν για εμπειρία.

Scamps:οι οποίοι δεν ενδιαφέρονται να κάνουν ζημιά. Είναι τύποι που τους ενδιαφέρει να μπούν σε κάποια σελίδα και να αφήσουν ένα μήνυμα τύπου «Η Μαρία ήταν εδώ».

Explorers:οι οποίοι ικανοποιούνται «μπαίνοντας εκεί που άλλοι hackers δεν έχουν μπει»- η τουλάχιστον «μπαίνοντας εκεί που οι ίδιοι δεν έχουν ξαναμπεί». Η περιέργεια τους είναι εκείνη που ωθεί να δουν πράγματα που δεν έχουν ξαναδεί.

Game players: οι οποίοι προσπαθούν να μπούν σε ένα σύστημα βλέποντας το σαν παιχνίδι και προσπαθούν να σπάσουν τα συστήματα ασφαλείας για να κερδίσουν το παιχνίδι.

Addict: είναι οι τύποι εκείνοι οι οποίοι ξεκινώντας από μια από τις παραπάνω κατηγορίες, μετατράπηκε σε ψυχικά εξαρτώμενος από αυτές. Στην περίπτωση αυτή το έχουν ανάγκη να χακάρουν για να νοιώθουν καλά ή φυσιολογικά.
Όλοι αυτοί των ανωτέρω κατηγοριών το βλέπουν ως παιχνίδι, δεν έχουν κάποιο οικονομικό όφελος.

β) Χρηματικό όφελος.

Το χρήμα αποτελεί, όπως συχνά λέγεται, τη ρίζα του κακού, και φυσικά αυτό ισχύει και για την διάπραξη ενός ηλεκτρονικού εγκλήματος. «Hacking για χρήμα» μπορεί να καλύπτει διάφορα αδικήματα πχ ξέπλυμα χρήματος . Επίσης μπορεί κάποιος να πουλάει της υπηρεσίες του σε κάποιον άλλο για την απόκτηση χρήματος χωρίς ωστόσο αυτός να αποκομίζει ο ίδιος όφελος από την αυτή την πράξη καθ΄αυτή. Σε αυτή την κατηγόρια ανήκουν άτομα όλων των κατηγοριών, άντρες, γυναίκες, παιδιά.

γ) Θυμό, εκδίκηση και άλλου τύπου συναισθήματα.

Το χρήμα δεν αποτελεί το μόνο κίνητρο για την διάπραξη εγκλημάτων. Έχει παρατηρηθεί ότι ο θυμός μπορεί να οδηγήσει τον άνθρωπο σε πράξεις που υπό άλλες συνθήκες δεν θα μπορούσε να φανταστεί ότι θα τις έκανε. Ψυχολόγοι επισημαίνουν ότι η κατάσταση υπό θυμό προσομοιάζει με μια κατάσταση υπό επήρεια αλκοόλ ή ναρκωτικών.

δ) Πολιτικά κίνητρα.

Cybercriminals υποκεινούμενοι από πολιτικά κίνητρα περιλαμβάνουν εξτρεμιστές, οι οποίοι χρησιμοποιούν το Ιντερνετ για να σπείρουν την προπαγάνδα τους, να επιτεθούν σε ιστοσελίδες και δίκτυα των πολιτικών εχθρών τους, να κλέψουν χρήματα, να βρούν χρήματα για τις μαχητικές δραστηριότητες τους ή να σχεδιάσουν και να οργανώσουν τα εγκλήματα τους στον πραγματικό κόσμο.
Παράδειγμα αποτελεί ο κυβερνοπόλεμος μεταξύ ΗΠΑ και Κίνας το καλοκαίρι του 2000 ως επακόλουθο της Αμερικάνικης Κατασκοπίας στην Κίνα.
Οι cybercriminals της κατηγορίας αυτής έχουν ένα ευρύ φάσμα ως προς την δραστηριότητα τους από το να διαδόσουν τις πολιτικές πεποιθήσεις τους ή να κάνουν γνωστή την ύπαρξη μίας πολιτικής οργάνωσης.

ε) Σεξουαλικά κίνητρα.

Το σεξ αποτελεί ένα από τα δυνατότερα ένστικτα των ζώων συμπεριλαμβανομένου και του ανθρώπου. Στην κατηγορία αυτή συμπεριλαμβάνονται οι ακόλουθοι τύποι:

«Παθητικοί παιδόφιλοι»: οι οποίοι χρησιμοποιούν το ίντερνετ για να έχουν πρόσβαση και να κατεβάζουν παιδικό πορνό, χρησιμοποιούν φωτογραφίες και ιστορίες στις οποίες συμμετέχουν παιδιά, βλέποντας τα να ικανοποιούν τις δικές τους φαντασιώσεις.

«Ενεργητικοί παιδόφιλοι»: οι οποίοι χρησιμοποιούν το Ιντερνετ για να βρίσκουν τα θύματα τους. Αυτοί συλλέγουν και υλικό στο οποίο συμμετέχουν παιδιά αλλά δεν αρκούνται σε αυτό. Συνήθως χρησιμοποιούν chat rooms με παιδιά, αρχίζουν συζήτηση αποκτούν την εμπιστοσύνη τους και στην συνέχεια τα παρασύρουν σε μια συνάντηση. Συνήθως επακολουθεί βιασμός του παιδιού .

«Οπαδοί του σαδομαζοχιστού σεξ»: οι οποίοι ικανοποιούνται προκαλώντας πόνο σε άλλους (σαδιστής) ή ικανοποιώντας πόνο στον εαυτό 54

τους (μαζοχιστής). Παρόλο που γενικά η συμπεριφορά αυτή μεταξύ ενηλικών δεν είναι συνιστά έγκλημα, ωστόσο η ανεύρεση παρτενερ μέσο ιντερνετ, και η πέραν από τα συμφωνηθέντα μεταξύ των δύο οδηγεί πολλές φορές στον τραυματισμό ή και στον θάνατο.

«**Κατ΄ εξακολούθηση βιαστές (serial rapist)»:** οι οποίοι αναπτύσσουν σχέση

online και στην συνέχεια προσκαλούν τα θύματα τους να τους συναντήσουν στην πραγματική ζωή, με απώτερο σκοπό τον βιασμό και μόνο. Είναι άτομα τα οποία αντιμετωπίζουν προβλήματα στην σεξουαλική ζωή τους. Ικανοποιούνται μόνο όταν το σεξ είναι βίαιο . Οι ψυχολογοι αποκαλούν τον βιασμό ως πράξη βίας, και το σεξ αποτελεί απλά το εργαλείο /μέσο του εγκλήματος.

«**Κατ εξακολούθηση sexual killers»**, οι οποίοι προσομοιάζουν με τους κατ εξακολούθηση βιαστές, σερφάρουν στα chat rooms και forums αναζητώντας θύματα. Το λεξικό της ψυχιατρικής αναγνωρίζει δύο κατηγορίες: τους οργανωμένους (organized) και τους ανοργάνωτους (disorganized). Οι organized δολοφόνοι συχνά είναι άτομα με δείκτη ευφυΐας πάνω από το μέσο όρο, ευγενικοί, παντρεμένοι ή συζούν . Οι disorganized killers είναι άτομα ακριβώς το αντίθετο: το IQ τους είναι κάτω του μέσου όρου, είναι άτομα μοναχικά και έχουν πολύ άγχος κατά την διάπραξη του εγκλήματος. Στην πράξη οι sexual serial killers, παρότι το κίνητρο διάπραξης των εγκλημάτων τους είναι σεξουαλικό, ανήκουν στην κατηγορία κινήτρου: σοβαρή ψυχιατρική ασθένεια.

στ) Σοβαρές ψυχικές ασθένειες.

Μία εγκληματική συμπεριφορά, δεν είναι από μόνο της ενδεικτική ψυχικής ασθένειας γιατί αν ήταν πιθανόν να μπορούσε να θεραπευτεί φαρμακευτικά. ‘Ατομα τα από οποία πάσχουν από σχιζοφρένεια, διπολική συναισθηματική διαταραχή, επιθετικότητα, μελαγχολία , διαταραχές προσαρμογής και διαταραχές σεξουαλικής φύσης είναι σύμφωνα Psychiatric Illness Associated with Criminality , by William H. Wilson, MD and Kathleen A. Trott, MD.

2.9.2. Χαρακτηριστικά ενός ερευνητή[23]

Παρατηρητικότητα: Στο πιο μικρό πράγμα.

Καλή μνήμη: Πρέπει να θυμάται γεγονότα, ονόματα, μέρη και ημερομηνίες διαφορετικά μπορεί να χάσει ζωτικής σημασίας πληροφορίες.

Οργανωτική Σκέψη: Δεν αρκεί να θυμάται πληροφορίες, αλλά πρέπει να οργανώνει σε μια λογική συνέχεια.

[23] Debra Littlejohn Shinder, Ed Tittel , «Scene of cybercrime Computer Forensics Handbook» σελ. 113-11

Ικανότητα καταγραφής: Πρέπει να καταγράφει με λεπτομέρεια κάθε πληροφορία και να μην την κρατάει στο μυαλό του, ετσι ώστε να μπορεί να τις μοιράζεται με όλους τους συμμετέχοντες στην έρευνα.

Αντικειμενικότητα: Δεν πρέπει να επιτρέπει προσωπικές διαφορές, σχέσεις ή συναισθήματα να εμπλέκονται στην διαδικασία της έρευνας, έτσι ώστε να διασφαλίζεται η αντικειμενικότητα του.

Γνώση: Ένας καλός ερευνητής είναι γνώστης των νόμων των κανονισμών, της θυματολογίας, της ψυχολογίας του εγκληματία, των ερευνητικών διαδικασιών και των αποδεικτικών μέσων.

Ικανότητα να σκέφτεται σαν εγκληματίας: Οι καλύτεροι των ερευνητών έχουν την ικανότητα να βάζουν τον εαυτό τους στην θέση του εγκληματία, οπότε μπορούν να καταλάβουν τον τρόπο που ένας εγκληματίας θα προστατεύσει την πράξη του.

Περιέργεια: Οι καλύτεροι των ερευνητών έχουν μία έμφυτη περιέργεια δεν αρκούνται στο γεγονός ότι διαπράχθηκε ένα έγκλημα, αλλά θέλουν να ξέρουν πως και γιατί διαπράχθηκε.

Αντοχή και Υπομονή: Πολλές φορές απαιτούνται πολλές ώρες έρευνας, οπότε θα πρέπει να έχει αντοχή ώστε να ανταπεξέλθει.

Αγάπη για γνώση: Πέρα από τα ανωτέρω χαρακτηριστικά που πρέπει να έχει και τα ειδικότερα χαρακτηριστικά που εξαρτώνται από την ίδια φύση του ηλεκτρονικού εγκλήματος.

Βασικές γνώσεις Η/Υ: Όσα περισσότερα γνωρίζει για το πώς δουλεύει ο Η/Υ (υλικό και λογισμικό) τόσο το καλύτερο.

Γνώση της αργκό των Η/Υ: Πρέπει να είναι σε θέση «να μιλήσει την γλώσσα αυτή».

Να μπορεί να καταλάβει την κουλτούρα των hackers: Πρέπει να είναι σε θέση να καταλάβει την κουλτούρα και τον τρόπο σκέψη ενός χακερ για να μπορέσει να τον «πιάσει».

Γνώση των κανόνων ασφαλείας των Η/Υ και του δικτύου: Για να είναι σε θέση να διαλευκάνει μια υπόθεση χάκινγκ ή επίθεση σε ένα δικτύου, πρέπει να είναι γνώστης των κανόνων ασφαλείας , των κανόνων ασφαλείας και των πρακτικών καθώς και των προϊόντων ασφαλείας που κυκλοφορούν.

2.10. Διαδικασία εντοπισμού ηλεκτρονικού εγκλήματος

Οι αρμόδιες αρχές που διερευνούν το ηλεκτρονικό έγκλημα έχουν ως κύριο στόχο την ανακάλυψη του δράστη καθώς και την όσο το δυνατόν πληρέστερη συγκέντρωση αποδεικτικών στοιχείων και ιχνών ώστε να μπορεί στη συνέχεια να τεκμηριωθεί και από νομική σκοπιά η κάθε προκύπτουσα υπόθεση. Οι τεχνολογικές εξελίξεις αναμφισβήτητα είναι με το μέρος των δραστών, που εκμεταλλευόμενοι τις νέες ψηφιακές καινοτομίες, βρίσκουν τρόπους να διατηρούν την ανωνυμία τους και να διαφεύγουν από τη σύλληψη. Βέβαια, συγχρόνως η τεχνολογία συνδράμει και στο έργο των διωκτικών αρχών, αφού πλέον υπάρχουν πολλοί τρόποι που μπορούν εύκολα να οδηγήσουν στον ηλεκτρονικό εγκληματία και μάλιστα με όλα τα απαραίτητα αποδεικτικά στοιχεία που τεκμηριώνουν την ενοχή του.

Στο σημείο αυτό θα αναφερθούν κάποιοι από τους πιο βασικούς τρόπους που χρησιμοποιούνται από τους ειδικούς για την εξιχνίαση υποθέσεων σχετιζόμενων με το ηλεκτρονικό έγκλημα.

2.10.1. Εντοπισμός IP

Η εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε δίκτυα από τις διωκτικές αρχές βασίζεται στον εντοπισμό της IP διεύθυνσης. Οι ηλεκτρονικοί εγκληματίες για να πραγματοποιήσουν επίθεση σε ένα σύστημα προκειμένου να παραπλανήσουν τις διωκτικές αρχές, χρησιμοποιούν πλαστές IP διευθύνσεις. Κάθε διεύθυνση στο Διαδίκτυο έχει και έναν αντίστοιχο αριθμό IP.

Το Σύστημα Ονομάτων Χώρου (Domain Name System D.N.S.) μετατρέπει τα ονόματα των διευθύνσεων σε αριθμούς (IP διευθύνσεις), έτσι ώστε να μπορεί να τις επεξεργαστεί το δίκτυο[24]. Ο επιτιθέμενος λοιπόν κατά την εκδήλωση μιας επίθεσης πλαστογραφεί τη διεύθυνση του με σκοπό να φαίνεται ότι είναι ένας νόμιμος χρήστης, δεν μπορεί όμως να πλαστογραφήσει την IP διεύθυνση.

Κάθε υπολογιστής που συνδέεται στο Internet, αποκτά μια διεύθυνση που είναι γνωστή με τον όρο IP διεύθυνση (Internet Protocol address) και η οποία είναι μοναδική στον κόσμο. Η διεύθυνση αυτή αποτελείται από 4 ακεραίους αριθμούς, όπου ο καθένας μπορεί να πάρει μια τιμή από 0 έως και 255, και ένα χαρακτηριστικό παράδειγμα IP διεύθυνσης είναι το εξής : 192.10.42.30. Αυτός ο συνδυασμός των τεσσάρων ακεραίων αριθμών της IP διεύθυνσης προσδιορίζει μοναδικά έναν υπολογιστή παγκοσμίως και αποτελεί το κλειδί για τον εντοπισμό των χρηστών που

[24] Debra Littlejohn Shinder, Ed Tittel , «Scene of cybercrime Computer Forensics Handbook» σελ. 113-11

παρανομούν στο Διαδίκτυο.

Στην περίπτωση που ο χρήστης συνδέεται στο Internet από το σπίτι του μέσω ενός ISP, τότε κάθε φορά που συνδέεται αποκτά και μια διαφορετική IP διεύθυνση, όπως 192.10.42.30 ή 192.10.42.32 ή 192.10.42.65 κοκ. Βλέπουμε ότι στην περίπτωση αυτή αλλάζει μόνο ο τελευταίος από τους τέσσερις αριθμούς, ενώ οι τρεις πρώτοι αριθμοί παραμένουν ίδιοι για όλους τους χρήστες που συνδέονται στον συγκεκριμένο ISP. Ο ISP καταγράφει τα στοιχεία των χρηστών (συνδρομητών) του που συνδέονται στο Internet μέσω των servers που αυτός διαθέτει, όπως όνομα χρήστη (user name), αριθμός τηλεφώνου, ώρα σύνδεσης, IP διεύθυνση, ιστοσελίδες που επισκέφθηκε ο χρήστης κ.ά., σε ειδικά αρχεία που αποκαλούνται log files (αρχεία καταγραφής).

Στην περίπτωση λοιπόν που εντοπισθεί κάποια παράνομη ή ύποπτη ενέργεια στο Διαδίκτυο, το πρώτο πράγμα που εντοπίζουν οι Αρχές είναι η IP διεύθυνση του δράστη, κάτι που είναι πολύ εύκολο να επιτευχθεί με απλά προγράμματα, ενσωματωμένα στον κωδικό των ιστοσελίδων.

Από την IP διεύθυνση εντοπίζουν τον ISP που εξυπηρέτησε τον δράστη και μετά θα πρέπει να εκδοθεί εισαγγελική εντολή ώστε να υποχρεωθεί ο ISP να δώσει τα στοιχεία του συνδρομητή του που κάποια συγκεκριμένη ημέρα και ώρα είχε αποκτήσει την συγκεκριμένη IP διεύθυνση.

Τα στοιχεία του συνδρομητή του που μπορεί να αποκαλύψει ο ISP είναι μόνο το τηλέφωνο από το οποίο κάλεσε ο δράστης και το όνομα χρήστη (user name) που χρησιμοποίησε. Μετά είναι δουλειά της Αστυνομίας να εντοπίσει το ποιος χρησιμοποίησε τα στοιχεία αυτά για να κάνει την όποια παράνομη ενέργεια. Δεν είναι σε θέση δηλαδή ο ISP να εντοπίσει συγκεκριμένο πρόσωπο.

Στην περίπτωση που ο χρήστης συνδέεται στο Internet μέσω ενός τοπικού δικτύου υπολογιστών, όπως για παράδειγμα από ένα Internet Cafe ή από ένα πανεπιστημιακό ή σχολικό εργαστήριο, τότε όλοι οι χρήστες του ίδιου δικτύου θα φαίνονται έξω από το δίκτυο και προς το Internet με την ίδια IP διεύθυνση, ενώ μέσα στο τοπικό δίκτυο θα έχει ο καθένας διαφορετική IP διεύθυνση. Μάλιστα, στην περίπτωση αυτή η IP διεύθυνση που φαίνεται προς τα έξω είναι συνήθως στατική (μόνιμη) και όχι δυναμική. Αν κάποιος δράστης αποφασίσει να κάνει παράνομες ενέργειες στο Internet και χρησιμοποιεί κάθε φορά διαφορετικά τοπικά δίκτυα υπολογιστών από διαφορετικά Internet Cafe, τότε ο εντοπισμός του θα είναι πολύ δύσκολος αλλά όχι αδύνατος.

Σε αυτό το σημείο αξίζει να σημειωθεί το εξής:

- **v** Σε κάθε περίπτωση η IP διεύθυνση αποτελεί στοιχείο του απορρήτου της επικοινωνίας του χρήστη.

Αυτό προκύπτει με σαφήνεια από τον συνδυασμό των άρθρων 2 και 4 του Ν.3471/2006, ο οποίος ορίζει:

Άρθρο 3 ν. 3471/2006:

"«δεδομένα κίνησης» είναι τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία.

"Δεδομένα θέσης" είναι τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών

Αρθρο 4 ν. 3471/2006

"Απόρρητο"

Οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, όπως ορίζονται στις διατάξεις του άρθρου 2 του παρόντος νόμου, προστατεύεται από το απόρρητο των επικοινωνιών. Η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος."

- **v** Η IP διεύθυνση είναι σε κάθε περίπτωση προσωπικό δεδομένο του κάθε χρήστη.

Αυτό προκύπτει από τον ορισμό του τι αποτελεί προσωπικό δεδομένο, όπως αποτυπώνεται στο άρθρο 2 του Ν 2472/1997:

Δεδομένα προσωπικού χαρακτήρα, κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

"Υποκείμενο των δεδομένων", το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαροκτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική

Στο σημείο αυτό θα γίνει μια αναφορά στην ορθή διαδικασία άρσης απορρήτου σχετικά με την IP διεύθυνση, αλλά και στην πρακτική όψη αυτής της διαδικασίας.

- **v** Η IP διεύθυνση ως στοιχείο του απορρήτου της επικοινωνίας του χρήστη εμπίπτει στις διατάξεις του Π.Δ. 47/2005. Η άρση του απορρήτου γίνεται

όπως επιτάσσει ο ν. 2225/1994 και για τις περιπτώσεις αυτών των συγκεκριμένων αδικημάτων.

Καταρχάς δηλαδή ελέγχεται από τις αρμόδιες αρχές, αλλά και από τον πάροχο που του ζητάνε να αποκαλύψει στοιχεία του απορρήτου των χρηστών του δικτύου του, αν το αδίκημα για το οποίο του ζητείται η γνωστοποίηση στοιχείων, είναι από τα περιοριστικώς αναγραφόμενα στον νόμο, για τα οποία επιτρέπεται η άρση απορρήτου.

Αν λοιπόν για το συγκεκριμένο αδίκημα προβλέπεται στο νόμο άρση απορρήτου (π.χ. παιδική προνογραφία), ελέγχεται στην συνέχεια κατά πόσον αυτή ζητείται αρμοδίως.

Αρμοδίως ζητείται όταν υπάρχει σύμφωνα με το νόμο ειδικό βούλευμα του Συμβουλίου Πλημμελειοδικών, το οποίο όμως μπορεί να παρασχεθεί και στην συνέχεια ως επικυρωτικό της διάταξης του εισαγγελέα. Συνεπώς το συνηθέστερο είναι να μας ζητηθεί με διάταξη εισαγγελέα να γνωστοποιήσουμε όποιο στοιχείο διαθέτουμε.

Αυτό σημαίνει ότι οι αστυνομικές αρχές για να ζητήσουν από τον πάροχο οποιασδήποτε υπηρεσίας την γνωστοποίηση στοιχείων που εμπίπτουν στο απόρρητο -όπως και την IP διεύθυνση κάποιου χρήστη- οφείλουν να έχουν έγγραφη εισαγγελική διάταξη.

(Είναι προφανές ότι για λόγους κατεπείγοντος αρκεί και η προφορική εντολή του εισαγγελέα.)

2.10.2. Συναγερμοί (Alarms)[25]

Τα Firewalls αποστέλλουν μηνύματα υψηλής προτεραιότητας σε συγκεκριμένους παραλήπτες όταν διαπιστωθεί κάποια ύποπτη δραστηριότητα. Τα μηνύματα αυτά αποστέλλονται με e-mail στο διαχειριστή του συστήματος και παράλληλα η ύποπτη δραστηριότητα αποθηκεύεται στα αρχεία καταγραφής. Η συγκεκριμένη λειτουργία των firewalls είναι εξαιρετικά μεγάλης σημασίας καθώς μπορεί να αποτρέψει την επίθεση κατά τη διαδικασία γέννησης της.

2.10.3. Αναφορές (Reports)[26]

Μια αναφορά δίνει αρκετές πληροφορίες για την εκδήλωση της επίθεσης όπως για παράδειγμα τη συχνότητα αποτυχημένων προσπαθειών για την απόκτηση μη εξουσιοδοτημένης πρόσβασης, τη συχνότητα σφαλμάτων και άλλα.

[25] 51 www.netsecurity.about.com προσβαση 27/08/2014

[26] 2 www.netsecurity.about.com προσβαση 27/08/2014

2.10.4. Αρχεία καταγραφής (Log- Files)[27]

Στα αρχεία καταγραφής αποθηκεύονται πληροφορίες σχετικές με τη λειτουργία του συστήματος. Η χρησιμότητα τους μεγιστοποιείται όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές (group policies). Εφόσον δεν έχει οριστεί συγκεκριμένη πολιτική ασφαλείας για μια ομάδα χρηστών, τα security logs παραμένουν κενά. Ο διαχειριστής του συστήματος είναι υπεύθυνος για τον καθορισμό πολιτικών ασφαλείας.

Ο ερευνητής του ηλεκτρονικού εγκλήματος μπορεί με τη βοήθεια των αρχείων καταγραφής να εξακριβώσει εάν κάποια συγκεκριμένη εφαρμογή χρησιμοποιήθηκε από χρήστη και αν ο χρήστης αυτός είχε ή όχι εξουσιοδοτημένη πρόσβαση στο σύστημα.

2.10.5. Μηνύματα Ηλεκτρονικού Ταχυδρομείου (E-mail)

Η εύρεση του αποστολέα των μηνυμάτων ηλεκτρονικού ταχυδρομείου αποτελεί βασική εργασία προς την αναζήτηση και τον εντοπισμό ηλεκτρονικών ιχνών του δράστη. Το ηλεκτρονικό ταχυδρομείο είναι πολύ διαδεδομένο μέσο για τη διάπραξη πολλών αδικημάτων όπως η μετάδοση κακόβουλου λογισμικού, οι απάτες, οι απειλές κλπ.

Η αναγραφή των στοιχείων του αποστολέα-δράστη στο μήνυμά του και στην περίπτωση πάντα που τα στοιχεία αυτά δεν είναι παραπλανητικά, οδηγεί εύκολα τις διωκτικές αρχές στον εντοπισμό του. Τα μηνύματα ηλεκτρονικού ταχυδρομείου καθώς μεταβαίνουν από τον αποστολέα στον παραλήπτη, διέρχονται από ενδιάμεσους υπολογιστές, καθένας από τους οποίους προσθέτει στην επικεφαλίδα του μηνύματος τις δικές του πληροφορίες.

Αυτές οι πληροφορίες στην επικεφαλίδα του μηνύματος είναι καταγεγραμμένες σε διάφορα πεδία που αφορούν τις επικεφαλίδες του παραλήπτη και του αποστολέα, τις επικεφαλίδες ημερομηνίας και άλλες. Στην αναζήτηση του αποστολέα κακόβουλων μηνυμάτων, οι κρίσιμες πληροφορίες βρίσκονται στις επικεφαλίδες του αποστολέα. Αυτές είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, το μονοπάτι (διεύθυνση) προς τον αποστολέα και τους διακομιστές από τους οποίους πέρασε το μήνυμα για να φτάσει στον τελικό παραλήπτη του.

Ο εντοπισμός του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου είναι μια εξαιρετικά δύσκολη διαδικασία. Υπάρχουν διάφοροι μέθοδοι που βοηθούν τους δράστες στην απόκρυψη των στοιχείων της ταυτότητας τους.

[27] 3 www.ip.gr/el/dictionary/155-Log_File πρόσβαση 27/08/2014

2.10.6. Honeypots & Honeynets

Τα honeypots είναι μια συλλογή συστημάτων που εμφανίζονται ως πραγματικοί στόχοι με σκοπό να ξεγελάσουν τον επιτιθέμενο εγκληματία και έτσι να τον ωθήσουν στην παραβίαση τους. Τα Honeypots αποτελούν ένα από τα πιο σύγχρονα εργαλεία που έχουν στη διάθεση τους οι αρμόδιες διωκτικές αρχές για τον εντοπισμό του ηλεκτρονικού εγκλήματος. Η λειτουργία τους είναι να παρακολουθούν τις ενέργειες του επιτιθέμενου και να τις καταγράφουν έτσι ώστε στη συνέχεια να αναλυθεί η μεθοδολογία της επίθεσης. Υπάρχουν 2 κατηγορίες honeypots τα πραγματικά (real) που είναι για παράδειγμα ένας διακομιστής και τα εικονικά (virtual) που είναι συνδυασμός υλικού και λογισμικού και προσομοιάζει σε ένα πραγματικό διακομιστή.

Το honeynet είναι ένας ακόμα τύπος honeypot, ένας από τους πιο σύνθετους τύπους υψηλής αλληλεπίδρασης (high-interaction) honeypot. Προσπαθεί να παρέχει τη μέγιστη δυνατότητα αλληλεπίδρασης, δίνοντας πραγματικά συστήματα για να αλληλεπιδρούν με αυτά οι επιτιθέμενοι. Συχνά, σχεδιάζονται με σκοπό να αντιγράφουν την πραγματικότητα, να παρέχουν δηλαδή ολοκληρωμένα αντίγραφα δικτύων και συστημάτων παραγωγής. Τα honeynets είναι μια πολύ ισχυρή λύση honeypot, ικανή να συλλέξει πληροφορίες και συγχρόνως μια από τις πιο σύνθετες λύσεις honeypot, καθώς απαιτούν πολύ εργασία για την κατασκευή, τη συντήρηση αλλά κυρίως για την παρακολούθηση τους.

2.10.7. Ασφάλεια βάσεων δεδομένων[28]

Οι βάσεις δεδομένων αποτελούν βασικό συστατικό του συνόλου των πληροφορικακών συστημάτων. Οι απαιτήσεις ασφαλείας βάσεων δεδομένων είναι παρόμοιες με τιςαντίστοιχες οποιουδήποτε πληροφοριακού συστήματος. Οι απειλές προς τις βάσεις δεδομένων έχουν ως αποτέλεσμα την απώλεια ή την υποβάθμιση μερικών απαραίτητων στοιχείων ασφαλείας, όπως η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα. Η ασφάλεια των βάσεων δεδομένων έχει ιδιαίτερη σημασία γιατί τα δεδομένα που βρίσκονται αποθηκευμένα στις βάσεις δεδομένων είναι τις περισσότερες φορές ιδιαιτέρως ευαίσθητα (π.χ. πληροφορίες όπως μισθοί εργαζομένων σε έναν οργανισμό, ιατρικά δεδομένα ασθενών ενός νοσοκομείου που πρέπει να τηρούνται απόρρητα) και η προστασία τους αποτελεί έτσι πρωταρχικό μέλημα κάθε οργανισμού. Επίσης μια βάση δεδομένων λόγω της ιδιαίτερης δομής που έχει καθώς και των πολύπλοκων μηχανισμών για τη διαχείρηση της, απαιτεί εξειδικευμένο χειρισμό και εργαλεία για την επίτευξη ικανοποιητικού επιπέδου ασφαλείας. Τυπικά, ένα σύστημα διαχείρησης βάσεων δεδομένων περιλαμβάνει ένα

[28] Elmasri R. –Navathe S.B, «Θεμελιώδεις αρχές συστημάτων δεδεμένων», Τόμος Α' , μετάφραση Χατζόπουλος Μιχ., Βασιλάκης Κώστας, εκδόσεις Δίαυλος, Αθήνα 1998.

υποσύστημα ασφαλείας και δικαιοδοσίας της βάσης δεδομένων, το οποίο είναι υπεύθυνο για την εξασφάλιση των τμημάτων της βάσης δεδομένων από προσπελάσεις χωρίς εξουσιοδότηση. Σήμερα υπάρχουν δύο τύποι μηχανισμών ασφαλείας :

Επιλεκτικοί μηχανισμοί ασφαλείας

Χρησιμοποιούνται για την εκχώρηση προνομίων στους χρήστες καθώς επίσης και της δυνατότητας προσπέλασης συγκεκριμένων αρχείων δεδομένων, εγγράφων ή πεδίων με συγκεκριμένο τρόπο (ανάγνωση, εγγραφή, διαγραφή, ενημέρωση).

Υποχρεωτικοί μηχανισμοί ασφαλείας

Χρησιμοποιούνται για την επιβολή ασφάλειας πολλών επιπέδων, διαχωρίζοντας τα δεδομένα και τους χρήστες σε διάφορες κλάσεις (επίπεδα) ασφαλείας και στη συνέχεια υλοποιώντας την κατάλληλη πολιτική ασφαλείας του οργανισμού.

Για να εκπονηθεί ορθά η διεξαγωγή της έρευνας σε συμβάντα ηλεκτρονικού εγκλήματος, θα πρέπει να πληρούνται οι παρακάτω προϋποθέσεις:

- Τα δεδομένα να βρίσκονται όσο πιο κοντά στην κατάσταση που ήταν όταν ανακαλύφθηκαν, να υπάρχει καθόλου ή όσο το δυνατόν λιγότερη τροποποίηση στις συσκευές και τα φυσικά μέσα αποθήκευσης
- Δημιουργία πιστού αντιγράφου του αρχικού μέσου αποθήκευσης για αποφυγή ζημιάς κατά την έρευνα
- Τα αντίγραφα δημιουργούνται σε μέσα αποθήκευσης τα οποία χρησιμοποιούνται για πρώτη φορά και δεν υπάρχει πιθανότητα διαρροής δεδομένων ή σφάλματος υλικού. (forensically-sterile)
- Κάθε βήμα της εξέτασης να τεκμηριώνεται

2.11. Προσδιορισμός τόπου ηλεκτρονικού εγκλήματος

Το έγκλημα εκτός από τη λεγόμενη αντικειμενική υπόσταση (δηλ. την περιγραφή των πράξεων που συνιστούν κολάσιμη συμπεριφορά) προσδιορίζεται από α) τον χρόνο τέλεσης, β) τον τόπο τέλεσης και γ) τα εμπλεκόμενα πρόσωπα (θύμα, παραβάτης κλπ.).

Ο προσδιορισμός του τόπου τέλεσης του (διαδικτυακού) εγκλήματος έχει κρίσιμη σημασία καθώς από αυτόν εξαρτάται καταρχήν ο προσδιορισμός του εφαρμοστέου δικαίου και τα αρμόδια δικαστήρια. Εν γένει ο προσδιορισμός του τόπου εξαρτάται κατά περίπτωση από τον τόπο εκδήλωσης της αξιόποινης συμπεριφοράς και τον

τόπο επέλευσης των αποτελεσμάτων της.

Ως τόπος τελέσεως ενός εγκλήματος θεωρείται από τις περισσότερες έννομες τάξεις (στις οποίες συμπεριλαμβάνεται και η ελληνική) τόσο ο τόπος στον οποίο ο υπαίτιος προέβη, ολικά ή εν μέρει, στην αξιόποινη ενέργεια/παράλειψη όσο και ο τόπος, στον οποίο επήλθε το λεγόμενο αξιόποινο αποτέλεσμα. Η χρήση των υπολογιστών και το Διαδίκτυο δημιουργούν εντελώς νέα δεδομένα σχετικά με τον προσδιορισμό του τόπου καθώς είτε δεν είναι ευχερής ο προσδιορισμός του τόπου εκδήλωσης μιας συμπεριφοράς/επέλευσης ενός αποτελέσματος είτε συντρέχουν περισσότεροι τόποι όπου τελείται ένα έγκλημα Στην περίπτωση εγκλημάτων που τελούνται/εκδηλώνονται στο Διαδίκτυο ο τόπος επέλευσης είναι ο κυβερνοχώρος, ο οποίος θα μπορούσε να ερμηνευτεί ως «κάθε χώρος στον οποίο αποκτάται πρόσβαση στα δεδομένα, δηλ. παντού» (Κιούπης).

Ως τόπος επελεύσεως του αποτελέσματος στην πραγματικότητα μπορεί να θεωρηθεί το Διαδίκτυο, κάθε χώρος δηλαδή στον οποίο αποκτάται πρόσβαση στα δεδομένα. Ο τόπος του κυβερνοεγκλήματος είναι διαφορετικός από τον τόπο του εγκλήματος στον «φυσικό» κόσμο δεδομένου ότι ο τόπος του κυβερνοεγκλήματος είναι δυναμικός, αυξάνεται και μπορεί να μεταμορφωθεί.

Ως ψηφιακός τόπος τελέσεως του εγκλήματος μπορεί να θεωρηθεί το εικονικό περιβάλλον που δημιουργείται από το λογισμικό και το υλικό στα οποία υπάρχουν τα ψηφιακά στοιχεία ενός εγκλήματος και τα οποία παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του θύματός του ή μπορούν να παρέχουν μια σύνδεση μεταξύ ενός εγκλήματος και του δράστη του. Λόγω της φύσης του Διαδικτύου είναι πολύ δύσκολο να εντοπιστεί τόσο ο τόπος στον οποίο εκδηλώθηκε η συμπεριφορά του εγκληματία όσο και ο τόπος στον οποίο επήλθε το αξιόποινο αποτέλεσμα. Ενδέχεται μάλιστα να υπάρχουν περιπτώσεις με περισσότερους τόπους τέλεσης της εγκληματικής πράξης [IRC (Internet Relay Channel), τα newsgroups (ομάδες συζητήσεως), το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol) κλπ.]

Σύμφωνα με τη θεωρία της συμπεριφοράς προτείνεται ως τόπος τέλεσης ο τόπος όπου βρισκόταν ο δράστης όταν εκδήλωνε την συμπεριφορά του. Σύμφωνα με την θεωρία αυτή σαν τόπος τελέσεως του εγκλήματος «θεωρείται μόνο ο τόπος στον οποίο ο δράστης διέπραξε το έγκλημα του». Έτσι λοιπόν εδώ δεν υπάρχουν χιλιάδες τόποι τελέσεως του εγκλήματος αλλά μονάχα ένας, εκεί που βρίσκεται ο παραβάτης και έχει αποθηκευμένα τα ψηφιακά στοιχεία Η λύση αυτή θα είχε το πλεονέκτημα ότι θα υπήρχε ένας τόπος τέλεσης. Η προσέγγιση αυτή όμως είναι ασύμβατη με την εγγενώς παγκόσμια φύση του διαδικτύου και επιπρόσθετα θα είχε τον κίνδυνο εγκλήματα που δεν τιμωρούνται στον τόπο συμπεριφοράς να μένουν ατιμώρητα στον τόπο όπου επιφέρουν τα αποτελέσματά τους.

Ο M. Collardin προτείνει μία άλλη θεωρία, σύμφωνα με την οποία πρέπει να περιλαμβάνεται και ο τόπος που επήλθε το αξιόποινο αποτέλεσμα υπό την προϋπόθεση να καλύπτεται από τη γνώση και τον δόλο του δράστη. Είναι γεγονός

ότι στις διαδικτυακές πράξεις υπάρχει πάντα ο δόλος του δράστη. Η πιθανότητα, οι περιορισμοί των τόπων τέλεσης της εγκληματικής πράξης να γίνονται περισσότεροι και ακριβέστεροι υπάρχει στους τόπους εκείνους στους οποίους ο δράστης ενήργησε με δόλο πρώτου βαθμού δηλαδή σε εκείνους τους τόπους που ο δράστης είχε σκοπό να επέλθει το αποτέλεσμα.

Μια άλλη λύση που αναπτύχθηκε για να προσδιοριστεί ο τόπος τέλεσης μιας παράνομης ενέργειας είναι ο διαχωρισμός των εγκλημάτων σε διάφορες κατηγορίες. Παραδείγματος χάριν στα τυπικά εγκλήματα ή όπως αλλιώς λέγονται εγκλήματα συμπεριφοράς, αποφασιστικός είναι ο τόπος που εκδηλώθηκε η συμπεριφορά του δράστη, δηλαδή ο τόπος που ο υπαίτιος διέπραξε την αξιόποινη πράξη και όχι ο τόπος που κατά τύχη επήλθε ο κίνδυνος. Φυσικά η λύση αυτή δεν είναι και τόσο εύκολο να επιτευχθεί για το λόγο ότι είναι αρκετά δύσκολο να διαχωριστούν τα εγκλήματα συμπεριφοράς με τα εγκλήματα αποτελέσματος καθώς επίσης τα εγκλήματα συγκεκριμένης διακινδυνεύσεως με τα εγκλήματα αφηρημένης διακινδυνεύσεως.

Στην περίπτωση της αποστολής μηνύματος αξιόποινου περιεχομένου στις ομάδες συζητήσεως ο αποστολέας δρα σε δύο χρονικές φάσεις και σε δύο τόπους. Οι αντίστοιχοι τόποι ενέργειας είναι ο τόπος δημιουργίας των δεδομένων και ο τόπος στον οποίο αποθηκεύονται τα δεδομένα (servers). Η κρίση σχετικά με την τέλεση της πράξης (δηλαδή του τόπου όπου ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια) συναρτάται φυσικά με την συγκεκριμένη αντικειμενική υπόσταση, που αναλόγως της διατυπώσεως της μπορεί να καλύπτει ήδη την παραγωγή ή κατοχή των αξιόποινων δεδομένων ή μόνο τη θέση τους σε κυκλοφορία. Η πρακτική σημασία της διακρίσεως αυτή είναι πολύ μεγάλη. Αν τόπος τέλεσης της ενέργειας θεωρηθεί ο τόπος που βρίσκονται τα δεδομένα όταν τα στέλνει ο αποστολέας, τότε το δίκαιο του τόπου εκείνου θα κρίνει αν υπάρχει αξιόποινη πράξη. Αν θεωρηθεί όμως ότι είναι ο τόπος όπου δημοσιεύονται τα δεδομένα τότε είναι όλοι οι τόποι που υπάρχουν οι διακομιστές συζητήσεων (servers) και εδώ εμφανίζεται και πάλι το πρόβλημα των πολλών τόπων τελέσεως της πράξης.

Στην περίπτωση των ιστοσελίδων, τα δεδομένα αποθηκεύονται στους υπολογιστές των ατόμων που τα έχουν δημιουργήσει. Στην περίπτωση των μεγάλων εταιρειών τα δεδομένα αυτά είναι αποθηκευμένα στους δικούς τους διακομιστές που είναι συνεχώς συνδεδεμένοι με το δίκτυο. Στην περίπτωση των απλών χρηστών τα δεδομένα είναι αποθηκευμένα στους διακομιστές του παροχέα πρόσβασης υπηρεσιών Διαδικτύου (ISP) ή στους διακομιστές μιας άλλης εταιρείας – το λεγόμενο web hosting. Αναμφισβήτητο είναι ότι, σαν τόπος τέλεσης της πράξης θεωρείται ο τόπος στον οποίο αποθηκεύονται τα δεδομένα. Σύμφωνα όμως με το web hosting δεν είναι ο μοναδικός. Αυτό φαίνεται καλύτερα από το παράδειγμα που παραθέτουμε πιο κάτω. Ένας χρήστης που βρίσκεται σε μια χώρα Χ θέλει να προσθέσει στην σελίδα που έχει δημιουργήσει και δημοσιεύσει κάποιες φωτογραφίες με όχι και τόσο

κατάλληλο περιεχόμενο. Δεν είναι όμως εις γνώσιν του αν οι νόμοι της χώρας στην οποία βρίσκεται θεωρήσουν το περιεχόμενο των φωτογραφιών άξιο να υποστεί κάποια τιμωρία. Η ιστοσελίδα του φιλοξενείται από τους διακομιστές μιας εταιρείας που βρίσκεται στο εξωτερικό όπου στην χώρα αυτή οι νόμοι δεν τιμωρούν το περιεχόμενο των φωτογραφιών. Το ερώτημα που σαφώς τίθεται εδώ είναι αν μπορεί να εφαρμοστεί το δίκαιο της χώρας στην οποία βρίσκεται ο χρήστης.Το γενικό συμπέρασμα είναι ότι στην περίπτωση των εγκλημάτων που τελούνται στο Διαδίκτυο, ως τόπος τέλεσης του εγκλήματος μπορεί να θεωρηθεί είτε ο τόπος από όπου η ηλεκτρονική σελίδα μπορεί να αναγνωσθεί, είτε ο τόπος όπου φιλοξενείται από τον παροχέα πρόσβασης στο Διαδίκτυο η συγκεκριμένη ηλεκτρονική σελίδα.

Ο αριθμός των τόπων τελέσεως εξαρτάται από την συγκεκριμένη λειτουργία του Διαδικτύου (newsgroups, Internet Relay Chat – IRC κλπ). Η εξωτερίκευσή του εγκλήματος μπορεί να εντοπίζεται σε μια χώρα πλην όμως τα αποδεικτικά στοιχεία μπορεί να βρίσκονται σε άλλη ή σε περισσότερες χώρες. Γι' αυτόν ακριβώς τον λόγο, για τη διερεύνησή του απαιτείται η συνεργασία δυο τουλάχιστον κρατών, του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία. Σε κάθε περίπτωση όμως δημιουργείται πρόβλημα όχι μόνο σε θέματα Δικαστικής και Αστυνομικής συνεργασίας, αλλά και σε θέματα κατά τόπον αρμοδιότητος ως προς την εκδίκαση της πράξεως. Ένα σχετικό ζήτημα αφορά την ανεπάρκεια των περισσοτέρων Διεθνών Συμβάσεων περί αμοιβαίας Δικαστικής Συνδρομής και Συνεργασίας, λόγω της φύσεως του αποδεικτικού υλικού, δηλαδή της ηλεκτρονικής απόδειξης (electronic evidence) που πρέπει να εντοπιστεί και να κατασχεθεί σε συνδυασμό με την ταχύτητα ενεργείας των διωκτικών Αρχών.

ΚΕΦΑΛΑΙΟ 3.

Νομοθετικό πλαίσιο που διέπει το ηλεκτρονικό έγκλημα

3.1. Ανάγκη νομικής ρύθμισης του Διαδικτύου

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του Διαδικτύου. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες, μέσω του Διαδικτύου, υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς, που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του Διαδικτύου (Ζάννη,2005).

Τα επιχειρήματα υπέρ της ρύθμισης του Διαδικτύου είναι τα ακόλουθα:

• Είναι ανοιχτό σε όλους και απαιτείται η ρύθμισή του για τον έλεγχο του παράνομου περιεχομένου του.
• Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με το ραδιόφωνο και την τηλεόραση, τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις.
• Υπάρχει πολύ επιβλαβές υλικό σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που γεννά την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπισή της.
• Οι περισσότεροι χρήστες, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους, έναντι επιθέσεων κακόβουλων χρηστών.

Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης συνοψίζονται στα ακόλουθα:

• Η ελευθερία του λόγου που προσφέρεται μέσω του Διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις.
• Το Διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός.
• Το Διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντοτε αντιμέτωπη με το ζήτημα της λογοκρισίας.
• Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του Διαδικτύου και όχι τα κράτη με νομοθετικές ρυθμίσεις. .

3.2. Το πρόβλημα της νομικής προσέγγισης θεμάτων που αφορούν τον κυβερνοχώρο

Η προσέγγιση των νομικών θεμάτων που αφορούν τον κυβερνοχώρο ενέχει πολλές δυσκολίες καθώς προϋποθέτει όχι μόνο νομικές αλλά, μέχρι ένα βαθμό τουλάχιστον τεχνικές γνώσεις.

Ένα εξίσου σημαντικό πρόβλημα που αντιμετωπίζει αυτός που ασχολείται με τη νομική πλευρά του θέματος από ποινική άποψη είναι η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων και αυτή οφείλεται στο γεγονός πως το έγκλημα στον κυβερνοχώρο αποτελεί μια νέα μορφή εγκλήματος.

Ένα επιπλέον πρόβλημα έχει να κάνει με την ελληνική νομική ορολογία. Τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι διατυπωμένη, κατά κανόνα, στην αγγλική γλώσσα και η αντίστοιχη μεταφορά αυτών των όρων στα ελληνικά δεν είναι ούτε εύκολη ούτε δόκιμη. Το πρόβλημα αυτό της ορολογίας παρουσιάζεται όχι μόνο στο πεδίο του ουσιαστικού ποινικού δικαίου αλλά και στο αντίστοιχο του ποινικού δικονομικού δικαίου.

Αυτό που έχει αποφασισθεί από τα κρατικά νομικά μέσα για την αντιμετώπιση αυτού του θέματος είναι να ακολουθηθεί η παραδοσιακή δικονομική ορολογία και μόνο όπου και όταν κριθεί αναγκαίο να ακολουθηθεί μια μικτή, δηλαδή σε μια υπόθεση ηλεκτρονικού εγκλήματος να αναφερθούν τόσο οι παραδοσιακοί όροι όσο και οι τεχνικοί, για παράδειγμα οι όροι έρευνα ή παρόμοια πρόσβαση (search or similar access), κατάσχεση ή παρόμοια διαφύλαξη (seize or similar secure).

Τέλος, τα ηλεκτρονικά αποδεικτικά μέσα δεν μπορούν σε καμία περίπτωση να ταυτιστούν με τα παραδοσιακά αποδεικτικά μέσα και αυτό γιατί οι αποδείξεις ενός εγκλήματος που λαμβάνει χώρα στο «φυσικό» κόσμο έχουν, κατά κανόνα, υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα, οι ηλεκτρονικές αποδείξεις, δεν είναι χειροπιαστές, μπορεί να τις κατευθύνει ή να τις διαχειριστεί κάποιος από μακριά, να αλλάξει τη μορφή και το περιεχόμενο τους ακόμα και να τις εξαφανίσει με το πάτημα ενός πλήκτρου.

3.3. Το πρόβλημα της δικαιοδοσίας στο διαδίκτυο

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο διαδίκτυο είναι πολύπλοκο εξαιτίας της παγκοσμιότητας του.

Δικαιοδοσία: είναι η αρμοδιότητα ενός δικαστηρίου να δικάσει μια συγκεκριμένη υπόθεση αλλά συγχρόνως και η αντίστοιχη αρμοδιότητα των διωκτικών αρχών να διερευνήσουν μια εγκληματική συμπεριφορά.
Η ανεύρεση της αρμοδιότητας του δικαστηρίου είναι συνυφασμένη με τον καθορισμό του τόπου τέλεσης του αδικήματος.

Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις

θεωρίες:

1. **Η θεωρία του τόπου του αποτελέσματος**. Τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

2. Η **θεωρία του τόπου ενέργειας**. Ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου έχει τελεστεί η ενέργεια που έτεινε στο άδικο αποτέλεσμα. Εφόσον η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος ενέργειας είναι αυτός όπου ολοκληρώθηκε η ενέργεια.

3. **Η μικτή θεωρία**. Τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

4. **Η θεωρία του βαρύνοντος τόπου**. Σύμφωνα με την αυτήν την θεωρία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Όμως υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας καθώς είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. **Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου**.

3.4. Διαδίκτυο και Ποινική Νομοθεσία

Στην Ελλάδα δεν υπάρχουν ειδικές διατάξεις για τα ηλεκτρονικά εγκλήματα. Οι περισσότερες υποθέσεις που έχουν προκύψει μέχρι σήμερα έχουν διωχθεί με τις διατάξεις του Ν. 1805/1988 ο όποιος πρόσθεσε τα άρθρα 370Β και 386Α στον ποινικό κώδικα, τα οποία αναφέρονται στα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές. Επίσης το άρθρο 370Α αναφέρεται στην παραβίαση του απορρήτου των τηλεφωνημάτων και το άρθρο 348Α στην πορνογραφία ανηλίκων. Τα άρθρα αυτά δεν αρκούν για τη δίωξη των σύγχρονων ηλεκτρονικών εγκλημάτων γιατί δεν έχουν προβλέψει την ύπαρξη του διαδικτύου. Αδικήματα που σχετίζονται με τη διασπορά κακόβουλου λογισμικού και με επιθέσεις άρνησης εξυπηρέτησης δε μπορούν να τιμωρηθούν με βάση την ισχύουσα νομοθεσία. Το κενό της νομοθεσίας για τα εν λόγο εγκλήματα καλύπτονται από τη νομοθεσία των συμβατικών εγκλημάτων**.**

Στην ελληνική έννομη τάξη δεν υπάρχει νόμος που να αναφέρεται σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει την συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού δικαίου. Ο νόμος ν.1805/88, ο οποίος τροποποίησε και συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (370Β, 370Γ, 386Α), αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές, δηλαδή αναφέρεται γενικά στην ηλεκτρονική εγκληματικότητα.

3.5. Άρθρα ποινικού κώδικα σχετικά με το ηλεκτρονικό έγκλημα

Άρθρο 370 Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Η χρησιμοποίηση από τον δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκαν με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση.

2. 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 τουλάχιστον ενός έτους. Με την ίδια ποινή τιμωρείται και όποιος μαγνητοφωνεί ιδιωτική συνομιλία μεταξύ αυτού και τρίτου χωρίς τη συναίνεση του τελευταίου. Το δεύτερο εδάφιο της παραγράφου 1 αυτού του άρθρου εφαρμόζεται και σε αυτή την περίπτωση.

3. Με φυλάκιση τουλάχιστον ενός έτους τιμωρείται όποιος κάνει χρήση των πληροφοριών ή των μαγνητοταινιών ή των μαγνητοσκοπήσεων που αποκτήθηκαν με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.

Άρθρο 370Β- Παράνομη πρόσβαση σε απόρρητα

Η ρύθμιση του άρθρου 370 Β προβλέπει ότι όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Το άρθρο 370Β, παρέχει ικανοποιητική προστασία μόνο όμως για κρατικά, επιστημονικά και επαγγελματικά απόρρητα, αποκλείοντας τα ιδιωτικά απόρρητα.

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται

τρίτοι να λάβουν γνώση τους.

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

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

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

Άρθρο 370Γ - Παράνομη «παρέμβαση» στο σύστημα και στα δεδομένα

Η πιο ουσιαστική διάταξη, όσον αφορά το χώρο του Διαδικτύου, περιλαμβάνεται στο άρθρο 370Γ, που τιμωρεί τη χωρίς άδεια πρόσβαση σε δεδομένα αποθηκευμένα σε Η/Υ. Το απόρρητο στην περίπτωση αυτή προστατεύεται υπό μία ευρεία έννοια. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από τη φύση τους απόρρητα, αλλά προστατεύεται το δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε όλα τα δεδομένα, που είναι αποθηκευμένα στον υπολογιστή του.

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

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

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

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

Άρθρο 386Α – Απάτη με υπολογιστή

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

Τα εγκλήματα του κυβερνοχώρου τελούνται με απαραίτητη προϋπόθεση τη χρήση τηλεπικοινωνιών, σταθερής ή κινητής τηλεφωνίας (Υπηρεσίες WAP). Ο νόμος 2246/26-10-1994 ψηφίσθηκε για την οργάνωση και εν γένει λειτουργία του τομέα τηλεπικοινωνιών και ρυθμίζει θέματα σχετικά με το διαδίκτυο. Προσδιορίζει συγκεκριμένα ότι φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι τα φυσικά ή νομικά πρόσωπα τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες υπό καθεστώς ελεύθερου ανταγωνισμού.

Σύμφωνα με το άρ. 2 παρ. 3 Ν. 2246/1994 συνιστάται η Εθνική Επιτροπή Τηλεπικοινωνιών, η οποία έχει τεχνικές, νομικές και προανακριτικές αρμοδιότητες, γνωμοδοτεί για την έκδοση των κωδίκων δεοντολογίας, επιβάλλει διοικητικά πρόστιμα, και ελέγχει γενικώς την ομαλή και ορθή λειτουργία του τομέα τηλεπικοινωνιών.
Σύμφωνα με το νόμο 2472/1997 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) προβλέπονται ποινικές κυρώσεις για όποιον προβαίνει σε διασύνδεση αρχείων χωρίς να τη γνωστοποιήσει στην αρμοδία αρχή.

Ανεξάρτητα από το εάν ο νόμος ν.1805/88 επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής, το βέβαιο είναι ότι δεν επαρκεί να καλύψει τα εγκλήματα που έχουν παρουσιαστεί από τη χρήση του διαδικτύου. Είναι γνωστό ότι για να αποκτήσει κάποιος πρόσβαση στο Κυβερνοχώρο, απαραίτητη προϋπόθεση αποτελεί η χρήση των τηλεπικοινωνιών, η οποία επιτυγχάνεται με τη σύνδεση του χρήστη με μια εταιρεία παροχής υπηρεσιών.

3.6. Η Σύμβαση για τον κυβερνοχώρο

Το Συμβούλιο της Ευρώπης συνειδητοποίησε πως επήλθαν σοβαρές και βαθιές αλλαγές στην ψηφιοποίηση, στη σύγκλιση και στη συνεχιζόμενη παγκοσμιοποίηση των ηλεκτρονικών υπολογιστών. Εξέφρασε την ανησυχία του για την ολοένα αυξανόμενη εγκληματικότητα στο κυβερνοχώρο και αναγνώρισε ότι η αποτελεσματική αντιμετώπιση του εγκλήματος αυτού μπορεί να γίνει μόνο με αναπτυγμένη, γρήγορη και καλά εφαρμοσμένη διεθνή συνεργασία σε ποινικά θέματα.

Ο σκοπός αυτός επιτεύχθηκε με το Συνέδριο για το Ηλεκτρονικό Έγκλημα

(Convention on Cybercrime), του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη στην Βουδαπέστη από όλα σχεδόν τα μέλη της Ευρωπαϊκής Ένωσης, μεταξύ τους και η Ελλάδα, στις 23 Νοεμβρίου 2001.

Σκοπός της Σύμβασης είναι η προστασία της κοινωνίας από το έγκλημα στο κυβερνοχώρο με τη θέσπιση της κατάλληλης νομοθεσίας που είναι απαραίτητη για την έρευνα, δίωξη και εκδίκαση των εγκλημάτων του κυβερνοχώρου, καθώς και των εγκλημάτων που διαπράττονται με τη χρήση συστημάτων ηλεκτρονικών υπολογιστών αλλά και για τη συλλογή αποδεικτικών στοιχείων που βρίσκονται σε ηλεκτρονική μορφή ενώ κύριο χαρακτηριστικό της είναι ότι καθιερώνει την υποχρέωση εναρμόνισης των εθνικών νομοθεσιών σε θέματα εγκλημάτων στο διαδίκτυο, όπως για παράδειγμα η διανομή πορνογραφικού υλικού στο internet, η εμπλοκή ανηλίκου σε ερωτική επαφή με τη χρήση του διαδικτύου, η χωρίς δικαίωμα αντιγραφή έργων πνευματικής ιδιοκτησίας.

Η Σύμβαση της Βουδαπέστης, περιλαμβάνει : α) διατάξεις ουσιαστικού ποινικού δικαίου, β) διατάξεις ποινικού δικονομικού δικαίου και γ) διατάξεις διεθνούς δικαστικής συνεργασίας.

Οι διατάξεις ουσιαστικού ποινικού δικαίου αφορούν:

- διατάξεις που αναφέρονται σε εγκλήματα κατά της εμπιστευτικότητας (confidentiality (περιορισμός της πρόσβασης στα δεδομένα μόνο σε άτομα που επιτρέπεται να έχουν πρόσβαση σε αυτά), ακεραιότητας (integrity)(διασφάλιση ότι τα δεδομένα έχουν υποστεί αλλαγές μόνο από εξουσιοδοτημένα άτομα) και διαθεσιμότητας (availability)(αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης πληροφορίας σε εξουσιοδοτημένους χρήστες) πληροφόρησης των δεδομένων και των συστημάτων ηλεκτρονικού υπολογιστή. Τέτοια αδικήματα είναι η παράνομη πρόσβαση και υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών
- διατάξεις για εγκλήματα σχετιζόμενα με υπολογιστές (Computer related offences), όπως η απάτη μέσω Η/Υ και η πλαστογραφία
- διατάξεις για εγκλήματα σχετικά με το περιεχόμενο, όπως το αδίκημα της παιδικής πορνογραφίας
- διατάξεις για αδικήματα σχετικά με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων (offences related to infringement of copyright and related rights).

Οι διατάξεις ποινικού δικονομικού δικαίου αναφέρονται σε θέματα :

- ταχείας διαφύλαξης δεδομένων αποθηκευμένων σε σύστημα υπολογιστή (Expedited preservation of stored computer data),
- ταχείας διαφύλαξης και γνωστοποίησης διακινουμένων δεδομένων (Expedited preservation and disclosure of traffic data),
- εντολής παροχής πληροφοριών (Production order),

- έρευνας και κατάσχεσης αποθηκευμένων στοιχείων σε ηλεκτρονικό υπολογιστή (Search and Seizure of stored Computer data),
- πραγματικού χρόνου συλλογής διακινουμένων δεδομένων (Real time collection of traffic data),
- παγίδευσης – υποκλοπής περιεχομένου δεδομένων (Interception of content data).

Οι διατάξεις διεθνούς δικαστικής συνεργασίας αναφέρονται :

- στην έκδοση,
- σε γενικές αρχές σχετικές με την αμοιβαία συνδρομή,
- σε παροχή αυθόρμητων πληροφοριών,
- στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστών (Expedited preservation of stored computer data),
- στην ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων δεδομένων (Expedited disclosure of preserved traffic data).

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

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 αυτός προσδιορίζεται σύμφωνα με το εσωτερικό δίκαιο κάθε μέλους κράτους. Οι περισσότερες νομοθεσίες των κρατών μελών του Συμβουλίου της Ευρώπης περιλαμβάνουν διατάξεις σχετικές με την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή.

β) Η αθέμιτη παγίδευση - υποκλοπή (illegal interception)

Σύμφωνα με το άρθρο 3 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως η παγίδευση - υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σ' ένα σύστημα υπολογιστών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που "μεταφέρει" τέτοια στοιχεία. Ένα μέλος μπορεί να απαιτήσει ότι το αδίκημα διαπράττεται με παράνομο σκοπό ή σε σχέση με ένα σύστημα υπολογιστών, το οποίο συνδέεται με άλλο σύστημα.

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

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

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

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 των ή με άλλες σχετικές συσκευές, μια ή περισσότερες από τις οποίες επεξεργάζονται αυτομάτως δεδομένα (data), σύμφωνα με κάποιο πρόγραμμα.

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

Σύμφωνα με το άρθρο 5 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα, για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την Εθνική του Νομοθεσία, όταν διαπράττεται εκ προθέσεως η σοβαρή παρεμπόδιση, χωρίς δικαίωμα, της λειτουργίας ενός συστήματος υπολογιστή, που γίνεται με πρόσθεση (Inputting), μεταφορά (transmitting), καταστροφή (damaging), διαγραφή (deleting), χειροτέρευση (deterioration), μεταβολή (alteration), ή απόκρυψη (suppression) δεδομένων υπολογιστών.

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

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.

3.7. Περί ηλεκτρονικών επικοινωνιών

Ο ρόλος του παροχέα υπηρεσιών (ISP – Internet Service Provider) στην ασφάλεια και στη μυστικότητα του διαδικτύου είναι πολύ σημαντικός καθώς αποτελεί κομβικό σημείο για τον εντοπισμό των παρανομιών και τη συλλογή των αποδεικτικών στοιχείων δεδομένου ότι όλα τα δεδομένα περνούν από τις εγκαταστάσεις του.

Κατά συνέπεια, οι σχετικοί με τις τηλεπικοινωνίες νόμοι έχουν άμεση ή έμμεση σχέση με τη χρήση του διαδικτύου. Με λίγα λόγια, το διαδικτύου είναι μια μορφή επικοινωνίας που γίνεται με την βοήθεια ή δια μέσου των τηλεπικοινωνιών.

3.7.1. Δίκαιο Τηλεπικοινωνιών

Σχετικοί, λοιπόν, νόμοι είναι :

i. Ο v.2867/19-12-2000 για την οργάνωση και λειτουργία των τηλεπικοινωνιών,
ii. Ο v.2774/22.12.99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα σε συνδυασμό με το v.2472/10.4.97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα,
iii. Ο v.2225/20.7.94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας,
iv. Ο v.2867/19-12-2000 που ρυθμίζει κάθε είδος τηλεπικοινωνιακής δραστηριότητας που αναπτύσσεται εντός της ελληνικής επικράτειας,
v. Ο v.2774/22.12.99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα σε συνδυασμό με το v.2472/10.4.97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα,
vi. Ο v.2774/22.12.1999, ο οποίος αναφέρεται στην προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα,
vii. Ο v.2472/1997 (ΦΕΚ 50 Α/10.4.1997) που προστατεύει το άτομο από την αυτοματοποιημένη ή μη επεξεργασία δεδομένων προσωπικού χαρακτήρα και
viii. Ο v.2225/94, για την προστασία της ελευθερίας της ανταπόκρισης.

3.8. Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

Η ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων),είναι η Ανεξάρτητη

Αρχή η οποία αποτελεί τον Εθνικό Ρυθμιστή που ελέγχει, ρυθμίζει και εποπτεύει: (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. Επιπλέον, η ΕΕΤΤ ασκεί τις αρμοδιότητες Επιτροπής Ανταγωνισμού στις εν λόγω αγορές.

Ιδρύθηκε το 1992 με τον Ν.2075 με την επωνυμία Εθνική Επιτροπή Τηλεπικοινωνιών (ΕΕΤ) και οι αρμοδιότητές της επικεντρώνονταν στην εποπτεία της απελευθερωμένης αγοράς των τηλεπικοινωνιών. Η λειτουργία της όμως ξεκίνησε το καλοκαίρι του 1995. Με την ψήφιση του Ν.2668/98 ο οποίος καθόριζε τον τρόπο οργάνωσης και λειτουργίας του τομέα των ταχυδρομικών υπηρεσιών, ανατέθηκε στην ΕΕΤ και η ευθύνη για την εποπτεία και ρύθμιση της αγοράς των ταχυδρομικών υπηρεσιών και μετονομάστηκε σε Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ). Με τον Ν.2867/2000 ενισχύθηκε ο εποπτικός, ελεγκτικός και ρυθμιστικός ρόλος της ΕΕΤΤ ενώ με τον ισχύοντα Ν. 4070/2012 περί ηλεκτρονικών επικοινωνιών, καθορίζεται το πλαίσιο παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και συναφών ευκολιών εντός της Ελληνικής Επικράτειας σύμφωνα με το ισχύον κοινοτικό δίκαιο και προσδιορίζονται οι αρμοδιότητές της.

Η ΕΕΤΤ σύμφωνα με το Άρθρο 12, εδ. κ του Ν. 3431/2006 εποπτεύει και ελέγχει τη χρήση του φάσματος επιβάλλοντας και τις σχετικές κυρώσεις, όπως αυτές προβλέπονται στο Άρθρο 63 του ίδιου Νόμου.

Παράλληλα στα πλαίσια των προβλέψεων του Ν. 2801/2000 όπως ισχύει και σύμφωνα με το ΠΔ. 387/2002 (ΦΕΚ 335/Α/2002) η ΕΕΤΤ υποστηρίζει τεχνικά τις αρμόδιες αρχές (Αστυνομία, Εισαγγελία) για τη διαπίστωση της διάπραξης αυτόφωρων αδικημάτων σύμφωνα με την κείμενη νομοθεσία.

Σε κάθε περίπτωση διαπίστωσης παραβάσεων αναφορικών με την τήρηση ή μη των όρων χρήσης των δικαιωμάτων χρήσης ραδιοσυχνοτήτων επιβάλλονται οι διοικητικές κυρώσεις του άρθρου 63. Πιο συγκεκριμένα αποστέλλεται στον πάροχο επιστολή συμμόρφωσης παρέχοντάς του τη δυνατότητα να εκθέσει τις απόψεις του ή να αποκαταστήσει τη νομιμότητα εντός χρονικού διαστήματος ενός μήνα ή λιγότερο. Μετά την παρέλευση του παραπάνω διαστήματος, εκκινείται η διαδικασία κλήσης σε ακρόαση για την επιβολή των προβλεπόμενων διοικητικών κυρώσεων.

3.9. Άρση απορρήτου των επικοινωνιών

Η προστασία της ελεύθερης ανταπόκρισης ή επικοινωνίας πρώτιστος κατοχυρώνεται Συνταγματικά από την πρώτη παράγραφο του άρθρου 19 του Συντάγματος, το οποίο ορίζει: <Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το

απόρρητο για λόγους εθνικής ασφαλείας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων>. Η έννοια του απόλυτα απαραβίαστου του αγαθού ενισχύεται ακόμη περισσότερο από το άρθρο 5 1 της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με τίτλο <Απόρρητο των επικοινωνιών σχετικά με την επεξεργασία των δεδομένων χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομές των ηλεκτρονικών επικοινωνιών>, η οποία και ενσωματώθηκε στο ελληνικό δίκαιο με το ΠΔ 47/2005. Το προεδρικό αυτό διάταγμα μαζί με το Ν. 3115/03 που ιδρύει την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών συμπληρώνουν το Ν. 2225/94, ο οποίος ορίζει περιοριστικά για ποια εγκλήματα επιτρέπεται η άρση του απορρήτου και την διαδικασίας αυτής. Τα προβλεπόμενα εγκλήματα για α οποία δύναται να εκδοθεί άρση του απορρήτου των επικοινωνιών είναι:

α) τα άρθρα 134, 135 παρ. 1, 2, 135Α, 137Α, 137Β, 138, 139, 140, 143, 144, 146, 148 παρ. 2, 150, 151, 157 παρ. 1, 168 παρ. 1, 187 παρ. 1, 2, 207, 208 παρ. 1, 264 περ. β', γ', 270, 272, 275 περ. β', 291 παρ. 1 εδ. β', γ', 299, 322, 324 παρ. 2, 3, 374, 380, 385 του Ποινικού Κώδικα".

β) τα άρθρα 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 64, 76, 93 και 97 του Στρατιωτικού Ποινικού Κώδικα,

γ) το άρθρο 15 παρ. 1 του ν. 2168/1993,

δ) τα άρθρα 5, 6, 7 και 8 του ν. 1729/1987,

ε) τα άρθρα 89, 90 και 93 του ν. 1165/1918.

Επίσης επιτρέπεται η άρση του απορρήτου για τη διακρίβωση των προπαρασκευαστικών πράξεων για το έγκλημα της παραχάραξης νομίσματος κατά το άρθρο 211 του Ποινικού Κώδικα.
«1α. Η άρση του απορρήτου είναι επίσης επιτρεπτή για τη διακρίβωση παραβάσεων των άρθρων 3 έως 7, 29 και 30 του ν. 3340/2005 (ΦΕΚ 112 Α').»

«1β.Επιτρέπεται, επίσης, η άρση του απορρήτου για τη διακρίβωση των κακουργημάτων που προβλέπονται από το ν. 3028/2002 «Για την προστασία των Αρχαιοτήτων και εν γένει της Πολιτιστικής Κληρονομιάς» (ΦΕΚ 153 Α΄), όπως ο νόμος αυτός εκάστοτε ισχύει.».

3.10. Αρχή διασφάλισης του απορρήτου των επικοινωνιών(Α.Δ.Α.Ε.)

Η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών είναι η ανεξάρτητη διοικητική αρχή, η οποία κατά το Σύνταγμα (άρθρο 19 παράγραφος 2) έχει ως αποστολή τη

διασφάλιση του απορρήτου των επικοινωνιών. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) είναι μία από τις πέντε (5) συνολικώς ανεξάρτητες αρχές, των οποίων η ύπαρξη προβλέπεται από το Σύνταγμα, μετά τη συνταγματική αναθεώρηση του έτους 2001.

Πρόβλεψη ιδρύσεως της ΑΔΑΕ

Υλοποιώντας τη διάταξη του άρθρου 19§2 του Συντάγματος, η οποία προστέθηκε μετά την αναθεώρηση του Συντάγματος από την Z' Αναθεωρητική Βουλή, ο ν. 3115/2003 (που φέρει τον τίτλο « Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» και είναι δημοσιευμένος στο ΦΕΚ Α΄ 47/27-2-2003) προέβλεψε τη σύσταση και λειτουργία αυτής της ανεξάρτητης αρχής. Σκοπός της Α.Δ.Α.Ε. είναι η προστασία του απορρήτου της επικοινωνίας, στον οποίο συμπεριλαμβάνεται ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

3.10.1 Αρμοδιότητες της ΑΔΑΕ

Οι προβλεπόμενες από τον Νόμο αρμοδιότητες της Α.Δ.Α.Ε. διακρίνονται σε

α)αρμοδιότητες ελέγχου,

β)κανονιστικές αρμοδιότητες ,

γ)κατασταλτικές αρμοδιότητες ,

δ)αρμοδιότητες έμμεσης συμμετοχής στη διαδικασία άρσης του απορρήτου,

ε)γνωμοδοτικές αρμοδιότητες ,

στ) αρμοδιότητες επιβολής διοικητικών κυρώσεων,

ζ) εσωτερικές αρμοδιότητες για την εύρυθμη λειτουργία της ,

η) αρμοδιότητες συνεργασίας με άλλους φορείς.

Οι κυριότερες αρμοδιότητες ελέγχου της Α.Δ.Α.Ε. είναι :

α)Η διενέργεια ελέγχων σε δημόσιους και ιδιωτικούς φορείς .

β)Η λήψη πληροφοριών από τους φορείς τους οποίους είναι αρμόδια να ελέγχει και από τους εποπτεύοντες Υπουργούς .

γ)Η κλήση σε ακρόαση κάθε προσώπου που κατά την κρίση της μπορεί να συμβάλει στην αποστολή της .

Κατασταλτικές αρμοδιότητές της συνιστούν :

α)Η κατάσχεση των μέσων παραβίασης του απορρήτου που υποπίπτουν στην

αντίληψή της . Τα αντικείμενα αυτά διατηρεί στην κατοχή της, ως μεσεγγυούχος, μέχρι να αποφανθούν για την τύχη τους τα αρμόδια δικαστήρια.

β)Η καταστροφή πληροφοριών ή στοιχείων ή δεδομένων που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

Αρμοδιότητες της Α.Δ.Α.Ε. που αφορούν την έμμεση συμμετοχή της στη διαδικασία άρσης του απορρήτου είναι οι εξής:

α)Η εξέταση καταγγελιών αναφορικά με τη διαδικασία άρσης του απορρήτου (6§1περ. ε΄ ν. 3115/2003).

β)Ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου (κατά τα άρθρα 3-5 ν. 2225/1994) ,χωρίς να υπεισέρχεται στην κατ' ουσίαν κρίση των αρμόδιων δικαστικών αρχών (6§1περ. α΄ ν. 3115/2003).

γ)Η τήρηση αρχείου απόρρητης αλληλογραφίας ,στο οποίο περιέχονται οι κοινοποιούμενες στην Α.Δ.Α.Ε. διατάξεις των δικαστικών αρχών ,με τις οποίες αποφασίζεται η άρση του απορρήτου (6§1περ. ζ΄ ν. 3115/2003, 5§4 ν. 2225/1994 ,όπως αντικαταστάθηκε με το άρθρο 12 περ. β΄ ν. 3115/2003)

δ)Η δυνητική γνωστοποίηση της επιβολής άρσης του απορρήτου στους θιγόμενους , μετά τη λήξη του μέτρου και εφόσον δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε (5§9 ν. 2225/1994,όπως αντικαταστάθηκε από το άρθρο 12 περ. δ΄ ν. 3115/2003) .

Η αρμοδιότητα της Α.Δ.Α.Ε. για την επιβολή διοικητικών κυρώσεων θεσπίζεται με το άρθρο 11 ν. 3115/2003, το οποίο ορίζει ως κυρώσεις που μπορεί να επιβάλει σε φυσικά ή νομικά πρόσωπα, σε περίπτωση παραβάσεως της νομοθεσίας που αφορά το απόρρητο των επικοινωνιών, τις εξής: α)σύσταση για συμμόρφωση σε συγκεκριμένη διάταξη της νομοθεσίας με προειδοποίηση επιβολής κυρώσεων σε περίπτωση υποτροπής, β)πρόστιμο από δεκαπέντε χιλιάδες (15.000) ευρώ έως ένα εκατομμύριο πεντακόσιες χιλιάδες (1.500.000) ευρώ. Για την επιβολή κυρώσεων ρητώς ο νόμος απαιτεί αιτιολογημένη απόφαση της Α.Δ.Α.Ε. , ύστερα από προηγούμενη κλήση των παραπάνω προσώπων για παροχή εξηγήσεων .

Η πιο σημαντική αρμοδιότητά της Α.Δ.Α.Ε. (απολογιστική-γνωμοδοτική) είναι η κατάρτιση ,στο τέλος κάθε έτους, της έκθεσης πεπραγμένων της . Η ετήσια έκθεση πεπραγμένων υποβάλλεται στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης, στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στους αρχηγούς των κομμάτων που εκπροσωπούνται στο Ευρωπαϊκό Κοινοβούλιο.

Επίσης, ο νόμος προβλέπει την αρμοδιότητα της Α.Δ.Α.Ε. να συνεργάζεται με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς και διεθνείς οργανισμούς για θέματα της αρμοδιότητάς της.

3.11. Νομοθεσία διαδικτυακών εγκλημάτων στην αλλοδαπή

Στην Αγγλία από τον Φεβρουάριο του 2001, οι hacker, αναλόγως με τη σημασία του χτυπήματος θεωρούνται και τρομοκράτες.
Στην Αμερική θεωρείται τρομοκρατική οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ, και τιμωρείται με φυλάκιση ως και ισόβια (ανάλογα με τη σημασία της εισβολής), χωρίς δυνατότητα μείωσης τις ποινής.

Κεφάλαιο 4

Προστασία προσωπικών δεδομένων

4.1. Προσωπικά δεδομένα

Τι είναι τα δεδομένα προσωπικού χαρακτήρα (ή αλλιώς προσωπικά δεδομένα);

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως:

- Στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.),
- Φυσικά χαρακτηριστικά
- Εκπαίδευση
- Εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ)
- Οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά)
- Ενδιαφέροντα
- Δραστηριότητες
- Συνήθειες

Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.

4.1.1. Ευαίσθητα προσωπικά δεδομένα

Τι είναι ευαίσθητα προσωπικά δεδομένα;

Ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται σε:

- Φυλετική ή εθνική του προέλευση
- Πολιτικά του φρονήματα
- Θρησκευτικές ή φιλοσοφικές του πεποιθήσεις
- Συμμετοχή του σε συνδικαλιστική οργάνωση
- Υγεία
- Κοινωνική πρόνοια
- Ερωτική ζωή
- Ποινικές διώξεις και καταδίκες του
- Συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.

4.2. Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Επεξεργασία δεδομένων προσωπικού χαρακτήρα λέγεται κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως:

- **v** Συλλογή
- **v** Καταχώριση
- **v** Οργάνωση
- **v** Διατήρηση ή αποθήκευση
- **v** Τροποποίηση
- **v** Εξαγωγή
- **v** Χρήση
- **v** Διαβίβαση
- **v** Διάδοση ή κάθε άλλης μορφής διάθεση
- **v** Συσχέτιση ή ο συνδυασμός
- **v** Διασύνδεση
- **v** Δέσμευση (κλείδωμα)
- **v** Διαγραφή
- **v** Καταστροφή.

4.3. Προϋποθέσεις επεξεργασίας προσωπικών δεδομένων

Για να έχει κάποιος φορέας ή φυσικό πρόσωπο δικαίωμα επεξεργασίας των προσωπικών δεδομένων άλλου ατόμου, πρέπει να πληρούνται οι παρακάτω προϋποθέσεις:

- **v** Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του. Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν:
- **v** Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου .
- **v** Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του

υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

- **v** Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
- **v** Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.
- **v** Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

Η Αρχή Προστασίας Προσωπικών Δεδομένων μπορεί να εκδίδει ειδικούς κανόνες επεξεργασίας για τις πλέον συνήθεις κατηγορίες επεξεργασιών και αρχείων, οι οποίες προφανώς δεν θίγουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κατηγορίες αυτές προσδιορίζονται με κανονισμούς που καταρτίζει η Αρχή και κυρώνονται με προεδρικά διατάγματα, τα οποία εκδίδονται με πρόταση του Υπουργού Δικαιοσύνης.

Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει :

- **v** Να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.
- **v** Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται για τους σκοπούς της επεξεργασίας.
- **v** Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.
- **v** Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής Προστασίας Προσωπικών Δεδομένων, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς, εφόσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων.Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά παράβαση του νόμου πρέπει να καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή

μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει την διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλεχθεί ή έχουν επεξεργαστεί.

4.3.1. Επεξεργασία ευαίσθητων προσωπικών δεδομένων

Συγκεκριμένα για τα **ευαίσθητα προσωπικά δεδομένα**, ισχύουν τα εξής:

Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων. Κατ΄ εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:

- Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη.
- Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
- Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.
- Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.
- Η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία είτε για λόγους εθνικής ασφάλειας, είτε για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας είτε για λόγους προστασίας της δημόσιας υγείας, είτε για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.
- Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων

στα οποία αναφέρονται.

- Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της Αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται με οποιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.

Η Αρχή χορηγεί άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Εφόσον η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, η γνωστοποίηση αρχείου επέχει θέση αιτήσεως για τη χορήγηση άδειας.

Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων. Πριν χορηγήσει την άδεια, η Αρχή καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπο του και τον εκτελούντα την επεξεργασία.

Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με τον σκοπό της επεξεργασίας. Μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

4.4. Δικαιώματα ατόμου για την προστασία επεξεργασίας των προσωπικών του δεδομένων

Ο νόμος 2472/1997 αφορά τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Αυτός όπως και η ευρωπαϊκή οδηγία 95/46/ΕΚ απονέμει δικαιώματα στο υποκείμενο που τοθ επιτρέπουν να ελέγχει ποιος, που, πότε και με τι τρόπο επεξεργάζεται τα προσωπικά του δεδομένα.

Τα δικαιώματα αυτά είναι:

Δικαίωμα ενημέρωσης

Ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το υποκείμενο για τα εξής τουλάχιστον στοιχεία:

- Την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του
- Τον σκοπό της επεξεργασίας.
- Τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων.
- Την ύπαρξη του δικαιώματος πρόσβασης

Δικαίωμα πρόσβασης

Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, τις ακόλουθες πληροφορίες:

- Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους.
- Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών.
- Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του.
- Τη λογική της αυτοματοποιημένης επεξεργασίας.
- Κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσμευση (κλείδωμα) των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του παρόντος νόμου, ιδίως λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων, και
- Την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή δέσμευσης (κλειδώματος) που διενεργείται, εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες.

Δικαίωμα αντίρρησης

Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την επεξεργασία δεδομένων που το αφορούν. Οι αντιρρήσεις απευθύνονται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχουν αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή. Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να απαντήσει εγγράφως επί των αντιρρήσεων μέσα σε αποκλειστική προθεσμία δεκαπέντε ημερών. Στην απάντησή του οφείλει να ενημερώσει το υποκείμενο για τις ενέργειες στις οποίες προέβη ή, ενδεχομένως, για τους λόγους που δεν ικανοποίησε το αίτημα. Η απάντηση σε περίπτωση απόρριψης των αντιρρήσεων πρέπει να κοινοποιείται και στην Αρχή.

Δικαίωμα προσωρινής δικαστικής προστασίας

Καθένας έχει δικαίωμα να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, την οποία έχει λάβει

διοικητική αρχή, νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει στην αξιολόγηση της προσωπικότητάς του και ιδίως της αποδοτικότητάς του στην εργασία, της οικονομικής φερεγγυότητάς του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.

4.5. Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), γνωστή (ανεπίσημα) και ως Αρχή Προστασίας Προσωπικών Δεδομένων, είναι συνταγματικά κατοχυρωμένη ανεξάρτητη διοικητική Αρχή. Ιδρύθηκε με τον Νόμο 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ο οποίος ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ. Η οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης. Η λειτουργία της Αρχής ξεκίνησε στις 10 Νοεμβρίου 1997.

4.5.1. Σκοπός της αρχής προστασίας προσωπικών δεδομένων

Ο σεβασμός και η προστασία της αξιοπρέπειας, της ιδιωτικής ζωής και της ελεύθερης ανάπτυξης της προσωπικότητας αποτελούν θεμελιώδη και πρωταρχική επιδίωξη κάθε δημοκρατικής κοινωνίας. Με την πάροδο του χρόνου, η τεράστια πρόοδος στον τομέα της πληροφορικής, η ανάπτυξη νέων τεχνολογιών, οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών και η ανάγκη της ηλεκτρονικής οργάνωσης του κράτους έχουν σαν συνέπεια την αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να προκαλέσει προβλήματα στην ιδιωτική ζωή του πολίτη.

Οι κίνδυνοι αυτοί αυξάνονται με τις νέες δυνατότητες ταχύτατης επεξεργασίας εκατομμυρίων δεδομένων μέσω ηλεκτρονικού υπολογιστή και μεταφοράς πληροφοριών παγκοσμίως μέσω του Ίντερνετ. Αποθήκευση και έρευνα μεγάλου όγκου δεδομένων που παλαιότερα θα απαιτούσε μεγάλους αποθηκευτικούς χώρους και επίπονη εργασία έχει πλέον απλοποιηθεί και γίνεται πολύ πιο εύκολα και ανέξοδα. Για την προστασία του ατόμου στην κοινωνία της πληροφορίας δεν επαρκούν οι παραδοσιακές θεσμικές εγγυήσεις και ρυθμίσεις, αλλά χρειάζεται ειδική αντιμετώπιση. Για τον σκοπό αυτό στην Ελλάδα, ιδρύθηκε με τον Νόμο 2472/1997 ως ανεξάρτητος διοικητικός φορέας η ΑΠΔΠΧ, η οποία λειτουργεί από τον Νοέμβριο

του 1997. Άλλες αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων είναι στην Ελλάδα η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και στην Ευρώπη ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων.

4.5.2. Αρμοδιότητες της αρχής προστασίας προσωπικών δεδομένων

- **v** Να εκδίδει οδηγίες και κανονιστικές πράξεις για την εφαρμογή των διατάξεων που αφορούν στην προστασία προσωπικών δεδομένων και να γνωμοδοτεί για σχετικά θέματα.
- **v** Να απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας και να επιβάλλει/βοηθάει όσους διατηρούν αρχεία να καταρτίζουν κώδικες δεοντολογίας
- **v** Να χορηγεί τις άδειες .
- **v** Να καταγγέλλει τις παραβάσεις στις αρμόδιες διοικητικές και δικαστικές αρχές αλλά και να επιβάλλει κυρώσεις.
- **v** Να ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας ελέγχους σε κάθε αρχείο.

Σύμφωνα με το άρθρο 9 η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη:

α) προς χώρες μέλη της Ευρωπαϊκής Ένωσης

β) προς χώρα μη μέλος της Ευρωπαϊκής Ένωσης, μετά από άδεια της Αρχής που παρέχεται εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Προς τούτο, λαμβάνει υπόψη ιδίως τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων.

Δεν απαιτείται άδεια της Αρχής εφόσον η Ευρωπαϊκή Επιτροπή έχει αποφανθεί, με τη διαδικασία του άρθρου 31 παρ. 2 της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995, ότι η χώρα αυτή εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, κατά την έννοια της παρ. 2 του άρθρου 25 της ανωτέρω Οδηγίας."

Εάν η εν λόγω χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας επιτρέπεται κατ' εξαίρεση, με άδεια της αρχής, εφόσον συντρέχει μια ή περισσότερες από τις παρακάτω προϋποθέσεις:

2. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ` εξαίρεση, με άδεια της Αρχής, εφόσον συντρέχει μία ή περισσότερες από τις κατωτέρω προϋποθέσεις:

α) Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη.

β)Η διαβίβαση είναι απαραίτητη: i) για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων, εφόσον αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή "ii). για τη συνομολόγηση και εκτέλεση σύμβασης μεταξύ αυτού και του υπευθύνου επεξεργασίας ή μεταξύ του υπευθύνου επεξεργασίας και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων".

γ) Η διαβίβαση είναι απαραίτητη για την αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη υπέρτερου δημόσιου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες Αρχές της άλλης χώρας, εφόσον ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και την άσκηση των σχετικών δικαιωμάτων.

δ) Η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου.

ε) Η μετάδοση πραγματοποιείται από δημόσιο μητρώο, το οποίο κατά το νόμο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι προσιτό στο κοινό ή σε κάθε πρόσωπο που αποδεικνύει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι νόμιμες προϋποθέσεις για την πρόσβαση στο μητρώο.

"στ. Ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων των υποκειμένων και την άσκηση των σχετικών δικαιωμάτων τους, όταν οι εγγυήσεις προκύπτουν από συμβατικές ρήτρες, σύμφωνες με τις ρυθμίσεις του παρόντος νόμου. Δεν απαιτείται άδεια εάν η Ευρωπαϊκή Επιτροπή έκρινε, κατά το άρθρο 26 παρ. 4 της Οδηγίας 95/46/ΕΚ, ότι ορισμένες συμβατικές ρήτρες παρέχουν επαρκείς εγγυήσεις για την προστασίατων προσωπικών δεδομένων."

4.6. Ευρωπαίος επόπτης προστασίας δεδομένων

Η θέση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ) δημιουργήθηκε το 2001. Έργο του ΕΕΠΔ είναι να εξασφαλίζει ότι τα όργανα και οι οργανισμοί της Ένωσης σέβονται το δικαίωμα ιδιωτικής ζωής των πολιτών όταν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

4.6.1 Αρμοδιότητα του ευρωπαίου επόπτη προστασίας δεδομένων

Όταν τα θεσμικά όργανα ή οι οργανισμοί της Ένωσης επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ατόμου του οποίου η ταυτότητα μπορεί να εξακριβωθεί, πρέπει να σέβονται το δικαίωμα ιδιωτικής ζωής του. Ο ΕΕΠΔ εξασφαλίζει ότι αυτό συμβαίνει και παρέχει τις συμβουλές του για όλα τα θέματα που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Η εν λόγω «επεξεργασία» καλύπτει δραστηριότητες όπως η συλλογή πληροφοριών, η καταγραφή και αποθήκευσή τους, η ανάκτησή τους για ανάγνωση, η αποστολή ή διάθεσή τους καθώς επίσης και η παρεμπόδιση της μετάδοσης, η διαγραφή, ή η καταστροφή δεδομένων.

Υπάρχουν αυστηροί κανόνες που διέπουν τις εν λόγω δραστηριότητες. Για παράδειγμα, τα θεσμικά όργανα και οι οργανισμοί της Ένωσης δεν επιτρέπεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή σας, τα πολιτικά φρονήματα, τις θρησκευτικές ή πολιτικές πεποιθήσεις ή τη συμμετοχή σας σε συνδικαλιστικές οργανώσεις. Επίσης δεν επιτρέπεται να επεξεργάζονται δεδομένα όσον αφορά την υγεία ή τη σεξουαλική ζωή σας, εκτός εάν τα δεδομένα απαιτούνται για σκοπούς υγειονομικής περίθαλψης. Ακόμη και στην περίπτωση αυτή, τα δεδομένα πρέπει να επεξεργάζεται επαγγελματίας του τομέα της υγείας ή κάποιο άλλο πρόσωπο που δεσμεύεται από το επαγγελματικό απόρρητο.

Ο ΕΕΠΔ συνεργάζεται με τους υπαλλήλους προστασίας δεδομένων σε κάθε όργανο ή οργανισμό της Ένωσης για να εξασφαλισθεί η εφαρμογή των κανόνων όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα.

Το 2009 ο κ. Peter Hustinx ανέλαβε και πάλι τα καθήκοντα του Ευρωπαίου ΕπόπτηΠροστασίας Δεδομένων, ενώ ο κ. Giovanni Buttarelli διορίστηκε βοηθός επόπτη. Η θητεία αμφοτέρων λήγει τον Ιανουάριο του 2014.

Γενικός στόχος του ΕΕΠΔ είναι να διασφαλιστεί ότι τα ευρωπαϊκά θεσμικά όργανα και φορείς σέβονται το δικαίωμα στην προστασία της ιδιωτικής ζωής κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ανάπτυξη νέων πολιτικών. Μια σειρά ειδικών καθηκόντων του ΕΕΠΔ καθορίζονται στον κανονισμό (ΕΚ) αριθ 45/2001.

Οι τρεις κύριες λειτουργίες του ΕΕΠΔ είναι:

α) **Εποπτεία:** ο ΕΕΠΔ παρακολουθεί την επεξεργασία δεδομένων προσωπικού χαρακτήρα στη διοίκηση της ΕΕ και εξασφαλίζει τη συμμόρφωση με τους κανόνες προστασίας των δεδομένων. Τα εποπτικά καθήκοντα που κυμαίνονται από δραστηριότητες επεξεργασίας προκαταρκτικού ελέγχου ενδέχεται να παρουσιάσουν

ιδιαίτερους κινδύνους, για τη διεκπεραίωση των καταγγελιών και τη διενέργεια ερευνών.

β) **Διαβούλευση:** ο ΕΕΠΔ συμβουλεύει την Ευρωπαϊκή Επιτροπή, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με τις προτάσεις για τη νέα νομοθεσία και ένα ευρύ φάσμα άλλων θεμάτων που έχουν αντίκτυπο στην προστασία των δεδομένων.

γ) **Συνεργασία**: ο ΕΕΠΔ συνεργάζεται με άλλες αρχές προστασίας των δεδομένων, προκειμένου να προαχθεί η συνεκτική προστασία των δεδομένων σε ολόκληρη την Ευρώπη. Η κεντρική πλατφόρμα για τη συνεργασία με τις εθνικές αρχές προστασίας δεδομένων είναι η ομάδα εργασίας του άρθρου 29.

- Μερικές από τις ελληνικές αποφάσεις είναι οι εξής:

- Η *1129.2001* του Μον.Πρωτ.Τρ. σχετικά με την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα.
- Η *1988.2002* του Μον.Πρωτ.Αθ. σχετικά με την πώληση προϊόντων εξ αποστάσεως και την παράνομη αποστολή διαφημιστικών εντύπων
- Η *2950.2002* του Μον.Πρωτ.Θεσ. σχετικά με την δωσιδικία νομικού προσώπου σε υπόθεση επεξεργασία δεδομένων προσωπικού χαρακτήρα
- Η *2279.2001* του ΣτΕ σχετικά με την σύσταση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Η *2286.2001* του ΣτΕ σχετικά με την άσκηση αίτησης ακυρώσεως κατά πράξεως της Αρχής Προστασίας Προσωπικών Δεδομένων από Πολιτικό κόμμα.
- Η *984.2001* του Συμβουλίου Εφετών για την παράνομη γνώση, αλλοίωση και ανακοίνωση ευαίσθητων προσωπικών δεδομένων
- Η *3545/2002* του ΣτΕ σχετικά με την συμμετοχή σε συνεδρίαση της Αρχής Προστασίας Προσωπικών Δεδομένων αναπληρωματικού μέλους της, στο οποίο έχουν ανατεθεί καθήκοντα εισηγητή.

  Κάποιες από τις ξένες δικαστικές αποφάσεις σχετικά με τα προσωπικά δεδομένα είναι οι ακόλουθες:

  - Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση Ιδιωτικής Ζωής μέσω του Διαδικτύου όπου αναφέρεται ότι η παροχή συμβουλευτικών υπηρεσιών και οι κάθε είδους γραπτές αναφορές μέσω ηλεκτρονικού ταχυδρομείου (e-mail) στο κοινό δεν παρέχει το δικαίωμα ελέγχου των

προσωπικών δεδομένων του παρόχου και αποκάλυψης της ηλεκτρονικής του αλληλογραφίας.

- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση Ιδιωτικής Ζωής που ρυθμίζει υπόθεση όπου ηλεκτρονικές βιβλιοθήκες χρησιμοποιήθηκαν για την παροχή πληροφοριών μέσω Internet
- Απόφαση Αμερικανικού Δικαστηρίου για παραβίαση ιδιωτικής ζωής εργαζομένου που ρυθμίζει υπόθεση όπου εργαζόμενος, ο οποίος απολύθηκε από την εταιρία που εργαζόταν διατυπώνει την επιφύλαξη του κατά πόσο η δημιουργία εσωτερικού δικτύου επικοινωνίας με τους υπόλοιπους εργαζομένους από αυτόν συνιστά παραβίαση της ιδιωτικής του σφαίρας μετά την απόλυσή του.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η τεχνολογία, οι ηλεκτρονικοί υπολογιστές και ο κυβερνοχώρος έχουν εισέλθει για τα καλά στη ζωή μας. Απόρροια αυτής της καλπάζουσας τεχνολογικής προόδου είναι το ηλεκτρονικό έγκλημα. Το ηλεκτρονικό έγκλημα πλέον παρουσιάζεται με πολλές μορφές έγκλημα, περιλαμβάνει ένα ευρύ φάσμα αξιόποινων πράξεων, μεταξύ των οποίων η διάδοση ιών, η χρήση πλαστού λογισμικού, η παράνομη πρόσβαση, η υποκλοπή πληροφοριών η πορνογραφία κ.α.

Η αντιμετώπιση του είναι ζήτημα υψίστης σημασίας, αφού χάρις σε αυτό διακιβέβευτε η ασφάλεια των πληροφοριακών συστημάτων της σύγχρονης ψηφιακής τεχνολογίας, ενώ σε ειδικές περιπτώσεις και η προσωπικής ασφάλεια των χρηστών του διαδικτύου.

Το ηλεκτρονικό έγκλημα αυξάνεται ραγδαία, ενώ ο διεθνής χαρακτήρας των εν λόγω δραστηριοτήτων, συχνά σημαίνει ακόμα και την εμπλοκή των διωκτικών αρχών του εξωτερικού αλλά και ανάκυψη ζητημάτων διεθνούς δικαιοδοσίας.

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 στον 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 διαδικτίου, 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 Δικαϊκο χώρο».

Οι Εισαγγελικές, Δικαστικές καθώς και οι Αστυνομικές Αρχές δεν έχουν μέχρι στιγμής τις απαιτούμενες γνώσεις, για την αντιμετώπισή του εγκλήματος στον κυβερνοχώρο. Και αυτό είναι πολύ λογικό, αφού ουδεμία εκπαίδευση έχουν υποστεί μέχρι στιγμής.

Είναι σχεδόν βέβαιο δε ότι, εάν η πολιτεία δεν φροντίσει για την εκπαίδευσή των προαναφερθέντων αρχών, στα αντίστοιχα θέματα, θα υπάρξει (στο πολύ σύντομο μέλλον) αδυναμία απονομής ορθής δικαιοσύνης σε θέματα εγκληματικότητας του κυβερνοχώρου και ηλεκτρονικής εγκληματικότητας γενικότερα.

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) σε θέματα διαδικτύου και ηλεκτρονικής εγκληματικότητας γενικότερα.

Τέλος, σχετικά με τις διωκτικές αρχές θα πρέπει να υπάρχει η συνεχής εκπαίδευση και κατάρτιση σχετικά με την διερεύνηση και αντιμετώπιση των ηλεκτρονικών εγκλημάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Βιβλιογραφία

1. Βλαχόπουλος Κ.(2007), «Ηλεκτρονικό Έγκλημα-Μορφές, Πρόληψη, Αντιμετώπιση», Αθήνα, Νομική Βιβλιοθήκη.

2. Λ. Μήτρου, το δίκαιο στην κοινωνία της πληροφορίας, Εκδόσεις Σάκκουλα Αθήνα – Θεσσαλονίκη 2002.

3. Μανωλεδάκης Ι. (2005), «Ποινικό Δίκαιο (επιτομή γενικού μέρους άρθρα 1-49ΠΚ)», ζ' έκδοση, Αθήνα, Σάκκουλας.

4. Ζάννη Αν.(2005), «Το διαδίκτυακό έγκλημα, Αθήνα», Αντ. Ν. Σάκκουλας.

5. Κιούπης Δ. – Ιωαννίδου Α. (2007), «Η παιδική πορνογραφία στο διαδίκτυο», Αθήνα Νομική Βιβλιοθήκη.

6. Γεωργιάδης Αστ. – Γκουτζιαμάνη Ε. (2005), «Αστικός Κώδικας και Ειδικοί Αστικοί Νόμοι», Αθήνα, Σάκκουλας.

7. Συκιώτου Αθ.(2009), «Το διαδίκτυο ως σύγχρονο όχημα θυματοποίησης», Αθήνα, Αντ. Ν. Σάκκουλας.

8. Debra Littlejohn Shinder, Ed Tittel, "Scene of cybercrime Computer Forensic Handbook.

9. Δ. Χαραλάμπης, Τηλεπικοινωνίες στην κοινωνία της πληροφορίας. Εκδόσεις Σάκκουλα Αθήνα – Θεσσαλονίκη.

Ξένη Βιβλιογραφία

1. Magid Yar (2006), "Cyber Crime and Society", Sage Publications.

2. Marshall A., (2008), "Digital Forensics: Digital Evidence in Criminal Investigation", John Wiley & Sons, Ltd., Oxford, UK

Πηγές έρευνας στο Διαδίκτυο

http://www.e.crime.gr

Διαδικτυακός τόπος για το ηλεκτρονικό έγκλημα, με πληροφορίες σχετικές με το Ηλεκτρονικό Έγκλημα

http://www.astynomia.gr

Ιστοχώρος Ελληνικής αστυνομίας

http://www.lawnet.gr

Portal Νομικών θεμάτων

http://www.eett.gr

Διαδικτυακή παρουσία της επιτροπής με πληροφορίες για την οργάνωση, τις τηλεπικοινωνίες και τα ταχυδρομία.

http://www.adae.gr

Ιστότοπος της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.

http://electroniccrime.wordpress.com/

Ιστότοπος με νομοθεσία περί ηλεκτρονικού εγκλήματος.

http://en.wikipedia.org/wiki/Computer_forensics

Computer forensic, Ανάκτηση κειμένου 14/6/2014

http://www.zougla.gr/greece/article/apotrepsame-159-pro8esis-aftoktonias-meso-diadiktiou-apo-tin-arxi-tou-etous-1060881

Άρθρο από το ενημερωτικό portal zougla.gr για την αποτροπή αυτοκτονιών, Ανάκτηση κειμένου 19/8/2014.

http://internetandsuicide.blogspot.gr/

Ανώνυμος, Αυτοκτονία και διαδίκτυο, Ανάκτηση κειμένου 5/8/2014

http://www.no-spam.gr/laws.htm

Νομοθεσία σχετική με το spamming

http://www.pharming-fishing.gr

Ιστότοπος σχετικός με το pharming και το spamming

http://www.dpa.gr/

Ιστότοπος της Αρχής Προστασίας Προσωπικών Δεδομένων

http://users.otenet.gr/

Ανακριτικές πράξεις