ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΠΑΡΑΡΤΗΜΑ ΠΥΡΓΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΜΕΣΩΝ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ

«Η ΔΙΕΥΘΥΝΣΗ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ»

ΜΑΥΡΟΜΜΑΤΗ ΧΡΙΣΤΙΝΑ

ΓΑΤΣΟΥΛΑ ΘΕΟΔΩΡΑ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΑΝΙΑΤΗΣ ΑΝΤΩΝΙΟΣ

ΠΥΡΓΟΣ 2013

«Κανείς δεν είναι ειλικρινής όταν τον κοιτάζεις κατά πρόσωπο. Δωσ' του μια μάσκα και θα σου πει όλη την αλήθεια.»

Oscar Wilde

ΕΥΧΑΡΙΣΤΙΕΣ

Η εκπόνηση της πτυχιακής αυτής εργασίας έγινε με τη βοήθεια πολλών ανθρώπων που συνετέλεσαν ο καθένας από την θέση του στην ολοκλήρωσή της, προσφέροντάς μας απλόχερα κάθε βοήθεια. Για το λόγο αυτό θα θέλαμε να ευχαριστήσουμε θερμά την οικογένειά μας για την ψυχολογική και οικονομική βοήθεια που μας προσέφεραν κατά τη διάρκεια των σπουδών μας, για την βοήθεια και την υποστήριξη τον καθηγητή κ. Αντώνιο Μανιάτη, για τη συμβολή του στην συγγραφή της πτυχιακής μας καθώς και τις συμβουλές που μας προσέφερε οποτεδήποτε ζητήθηκαν ώστε να μπορέσουμε να φέρουμε εις πέρας το δύσκολο αυτό εγχείρημα.

ΠΡΟΛΟΓΟΣ

Η σύγχρονη κοινωνία ξεχωρίζει για την πολυπλοκότητα του τρόπου ζωής και των προβλημάτων με τα οποία έρχεται αντιμέτωπος καθημερινά ο άνθρωπος. Είναι η εποχή της έκρηξης των γνώσεων και της ραγδαίας ανάπτυξης της τεχνολογίας, με ξεχωριστή θέση της τεχνολογίας των ηλεκτρονικών υπολογιστών. Η δειλή στην αρχή εμφάνιση των ηλεκτρονικών υπολογιστών και στη συνέχεια η εισβολή τους σχεδόν σε κάθε πτυχή της ζωής μας συμβάλλει στη αστραπιαία διακίνηση των γνώσεων και των ιδεών, καθώς και στην αντιμετώπιση πολλών πολύπλοκων καταστάσεων. Παρόλα αυτά, είναι ταυτόχρονα παραδεκτό πως πολλά από τα προβλήματα με τα οποία έρχεται αντιμέτωπος ο σύγχρονος άνθρωπος θα μπορούσαν να επιλυθούν πιο εύκολα και πιο αποτελεσματικά με τη συνεργασία και την αλληλοβοήθεια, αφού ζούμε σε μια κοινωνία αλληλεξάρτησης.

Οι νέες τεχνολογίες,όσον αφορά στον τομέα του διαδικτύου, συμβάλλουν στην διάχυση της γνώσης, ενώ ταυτόχρονα εξυπηρετούν ανάγκες που έχουν δημιουργηθεί, όπως η γρήγορη ενημέρωση του κοινού για τα τεκταινόμενα ανά τον κόσμο, η προστασία από το ηλεκτρονικό έγκλημα το οποίο μέσα από την γιγάντωση του παγκόσμιου κοινωνικού ιστού έχει βρει πρόσφορο έδαφος να εξαπλωθεί κτλ.Παράλληλα λοιπόν με την συνεχή ανάπτυξη του διαδικτύου και των δυνατοτήτων που προσφέρει παρατηρείται ταυτόχρονη εμφάνιση κακόβουλων στοιχείων.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Χρησιμοποιώντας τους ηλεκτρονικούς υπολογιστές και το Διαδίκτυο ανοίγεται μπροστά μας ένας τεράστιος όγκος δεδομένων, χωρίς αυτός να προϋποθέτει και την ασφαλή πλοήγησή μας. Ολοένα και περισσότερο στη σύγχρονη ζωή, οι υπολογιστές και άλλες συνδεδεμένες συσκευές στο Διαδίκτυο γίνονται ακόμα πιο ευάλωτες για τους επίδοξους εγκληματίες, οι οποίοι κλέβουν πληροφορίες και διαπράττουν άπατες εις βάρος ανυποψίαστων πολιτών.

Η χρήση των ηλεκτρονικών υπολογιστών και του διαδικτύου αποτελεί πλέον αναπόσπαστο κομμάτι της καθημερινότητας μας, της εκπαιδευτικής, επαγγελματικής, αλλά και κοινωνικής μας πραγματικότητας. Η χρήση του διαδικτύου έχει αναμφισβήτητα θετικά αποτελέσματα, μαζί με αυτά όμως, παρουσιάστηκαν και πολλές αρνητικές συνέπειες. Σε ότι μας αφορά εν προκειμένω, το Διαδίκτυο επέτρεψε την εμφάνιση νέων μορφών εγκληματικής δράσης και τον εκσυγχρονισμό παραδοσιακών εγκλημάτων.

Ξεκινώντας, στο πρώτο κεφάλαιο επιχειρούμε μια θεωρητική προσέγγιση στην έννοια της Γραφειοκρατίας, παρουσιάζοντας τα βασικά της χαρακτηριστικά και πώς μέσα από το χρόνο φτάσαμε στην σημερινή έννοια της Διοικητικής Επιστήμης. Ακόμη, γίνεται μια πρώτη αναφορά στην Δίωξη Ηλεκτρονικού Εγκλήματος (Δ.Η.Ε) και το πώς αυτή σχετίζεται με τη γραφειοκρατία. Στο δεύτερο κεφάλαιο, προσεγγίζουμε αναλυτικότερα την Δ.Η.Ε και τον τρόπο που αυτή οργανώνεται, πλησιάζοντας και το διαρθρωτικό της κομμάτι. Το τρίτο κεφάλαιο είναι αφιερωμένο στον τρόπο με τον οποίο δραστηριοποιείται στην πράξη η Δ.Η.Ε, κυρίως όσον αφορά τους διαδικτυακούς κινδύνους. Τον τρόπο που αυτοί εμφανίζονται και εξαπλώνονται, τα σημάδια αναγνώρισης και τη στρατηγική της δίωξης ώστε να εξαλειφθεί το πρόβλημα.

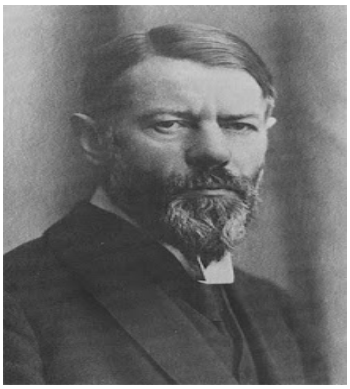
Το τέταρτο και τελευταίο κεφάλαιο πραγματεύεται τις δυσχέρειες και τα εμπόδια που αντιμετωπίζουν τα μέλη της Δ.Η.Ε και πως τα αντιμετωπίζουν ώστε να πετύχουν την εκάστοτε διάσωση. Παρίστανται στοιχεία για το βαθμό των επιτυχιών της ομάδας και ταυτόχρονα ο τρόπος με τον οποίο κατάφεραν να προσπεράσουν τα όποια εμπόδια υπήρξαν για να κάνουν την δουλειά τους απέναντι στον συνάνθρωπο με απόλυτη επιτυχία.

ΚΕΦΑΛΑΙΟ 1^{Ο}

- Η ΓΡΑΦΕΙΟΚΡΑΤΙΑ-

1.1 **Maximilian Carl Emil Weber (1864-1920)**

Ο Max Weber γεννήθηκε στην Γερμανία, στην πόλη Erfurt στις 21 Απριλίου του 1864. Σπούδασε νομικά και σε ηλικία 30 ετών έλαβε την έδρα του καθηγητή Πολιτικής οικονομίας στο Πανεπιστήμιο του Freiburg.



Εικόνα 1.Max Weber

Η γραφειοκρατική διοίκηση, παρατήρησε ο Βέμπερ, σημαίνει ουσιωδώς την άσκηση ελέγχου πάνω στη βάση της γνώσης, γεγονός που την καθιστά ορθολογική και της παρέχει τη δυνατότητα μιας ασύγκριτης υπεροχής έναντι άλλων μορφών οργάνωσης. Η γραφειοκρατική γνώση διακρίνεται στη συνέχεια σε *"τεχνική γνώση"* (Fachwissen) του εκάστοτε ειδικού και επιμέρους αντικειμένου της διοίκησης (λ.χ., ιατρικά, νομικά, οικονομικά, τεχνικά ζητήματα), ένα είδος γνώσης (τεχνογνωσίας) που συσσωρεύεται στις σύγχρονες γραφειοκρατίες (πολύπλοκα οργανωτικά συστήματα) και αρκεί συχνά για να θεμελιώσει την τεχνική της υπεροχή. Επιπλέον, όμως, αυτής της μορφής ειδικής γνώσης του επιμέρους αντικειμένου, αναπτύσσεται και καλλιεργείται στους κόλπους της γραφειοκρατικής οργάνωσης και μια άλλη ακαταμάχητη μορφή γνώσης, η *"ειδική γνώση των δεδομένων"* (Dienstwissen) της ίδιας της γραφειοκρατικής διαδικασίας. Αυτό το είδος γνώσης αναφέρεται στην οργάνωση και λειτουργία του ίδιου του συστήματος της γραφειοκρατίας, πρόκειται για τη γνώση και την εξοικείωση με τα μυστικά ή τα απόκρυφα της ίδιας της γραφειοκρατίας. Στις επόμενες παραγράφους θα προσεγγίσουμε αναλυτικότερα την ουσία και τη λειτουργία της Γραφειοκρατίας.

1.2 **Ορισμός της Γραφειοκρατίας**

Η λέξη Γραφειοκρατία προέρχεται από την λέξη «*Γραφείο*». "*Γραφειοκρατία*" είναι ο κανόνας που δημιουργήθηκε μέσω ενός γραφείου και απεστάλη από αυτό στα εκτελεστικά

όργανα. Στο γραφείο τηρούνται αρχεία των επικοινωνιών που αποστέλλονται και λαμβάνονται. Είναι ο αόρατος ανώτατος υπάλληλος της κυβέρνησης, ένα μέσο με το οποίο μια μοναρχία, αριστοκρατία, δημοκρατία, ή άλλη μορφή διακυβέρνησης, δημιουργεί και εφαρμόζει τους κανόνες. Ο Max Weber ασχολήθηκε με το φαινόμενο της γραφειοκρατίας τονίζοντας ότι κάθε γραφειοκρατία έχει καθήκον να είναι αντικειμενική και ουδέτερη και να υπηρετεί την κοινωνία. Όμως στην κορυφή του γραφειοκρατικού οργανισμού, θα πρέπει να υπάρχει οπωσδήποτε ένα στοιχείο το οποίο να μην είναι καθαρά γραφειοκρατικό, αλλά να δίδει κατευθύνσεις πολιτικής.

Όπως ο Weber επισημαίνει, γραφειοκρατικά συστήματα δεν έχουν μόνο οι κυβερνήσεις αλλά και οι στρατοί, τα πολιτικά κόμματα, οι εκκλησίες, τα εκπαιδευτικά ιδρύματα, οι ιδιωτικές επιχειρήσεις και πολλοί άλλοι οργανισμοί. Δηλαδή διαθέτουν ένα επαγγελματικό προσωπικό το οποίο τηρεί αρχεία και αποστέλλει γενικούς κανόνες και κατευθύνσεις. Γραφειοκρατικά συστήματα συναντάμε στην αρχαία Αίγυπτο, την αρχαία Ρώμη, στο Βυζάντιο. Ο Weber πίστευε ότι η γραφειοκρατία είναι ένα κυρίαρχο χαρακτηριστικό των σύγχρονων κοινωνιών με διαρκώς αυξανόμενη σημασία. Ακριβώς όπως ο Adam Smith είδε στον καταμερισμό της εργασίας την αιτία προόδου των σύγχρονων οικονομιών, έτσι ο Weber βλέπει την γραφειοκρατία ως μία από τις πιο σημαντικές αιτίες ανάπτυξης του καπιταλισμού. Ο Weber ορίζει ως «*ιδανικό τύπο γραφειοκρατίας*» αυτή που χαρακτηρίζεται από ένα ιεραρχικό καταμερισμό της εργασίας, διέπεται από ρητούς κανόνες οι οποίοι εφαρμόζονται απρόσωπα, και στελεχώνεται από υπαλλήλους πλήρους απασχόλησης, με αποκλειστική πηγή εσόδων τον μισθό της εργασίας τους. Εάν ο υπάλληλος δεν έχει οποιαδήποτε άλλη πηγή εισοδήματος, εκτός από τον μισθό του τότε θα ακολουθήσει αξιόπιστα τους κανόνες, προκειμένου να μην διακινδυνεύσει η θέση του.

Ο γραφειοκράτης χρειάζεται χρόνο και εμπειρία για να μάθει τη δουλειά, όχι τόσο επειδή είναι δύσκολο να εκπληρώσει την ιδιαίτερη αποστολή που του έχει ανατεθεί, αλλά επειδή απαιτείται ιδιαίτερος συντονισμός με τα άλλα μέρη του συστήματος. Λόγω της φύσης των γραφειοκρατικών εργασιών, αλλά ίσως και λόγω της σημασίας της κατάρτισης και του συντονισμού των θέσεων εργασίας, τα στελέχη που απαρτίζουν το σύστημα απαιτείται να διαθέτουν υψηλό επίπεδο μόρφωσης και εκπαίδευσης. Η εκπαίδευση τους θα πρέπει να είναι πιστοποιημένη, έτσι ώστε να εκπληρώνονται τα απρόσωπα κριτήρια πρόσληψης. Χαρακτηριστικά, όπως:

1. οι τίτλοι σπουδών – πιστοποιήσεις εκπαίδευσης,

2. ο σταθερός μισθός,
3. η προϋπηρεσία,
4. η σταθερότητα του αριθμού του προσωπικού,

αποτελούν τον ορισμό του «*ιδανικού τύπου γραφειοκρατίας*» που απαιτείται για την αποτελεσματική λειτουργία της διοικητικής μηχανής. Η γραφειοκρατία διέπεται από συγκεκριμένες αρχές και χαρακτηριστικά, τα οποία συμβάλλουν ουσιαστικά στην αποτελεσματική εφαρμογή της.

1.2.1 Οι βασικές αρχές Γραφειοκρατίας

1. Η τυπική Εξουσία(Authority) ενός στελέχους αντλεί την ισχύ της από την θέση που καταλαμβάνει.

2. Οι θέσεις στην επιχείρηση θα πρέπει να καταλαμβάνονται με βάση την απόδοση (performance) και όχι μέσω κοινωνικών γνωριμιών.

3. Τα καθήκοντα και η εξουσία σε κάθε θέση και οι σχέσεις της με άλλες θέσεις πρέπει είναι ξεκάθαρα ορισμένα. Οι υπάλληλοι θα πρέπει να γνωρίζουν τι αναμένεται από αυτούς.

4. Για να ασκείται αποτελεσματικά η εξουσία θα πρέπει οι θέσεις να είναι ιεραρχικά διευθετημένες σε μια ξεκάθαρη «γραμμή εξουσίας». Οι εργαζόμενοι θα πρέπει να γνωρίζουν ποιος αναφέρεται σε ποιον.

5. Θα πρέπει να ορίζεται ένα σαφώς διατυπωμένο σύστημα Κανόνων (Rules), Τυπικών Λειτουργικών Διαδικασιών (Standard Operating Procedures (SOPs)), αλλά και άτυπων κανόνων (norms) για τον έλεγχο της συμπεριφοράς στο εσωτερικό της οργάνωσης.

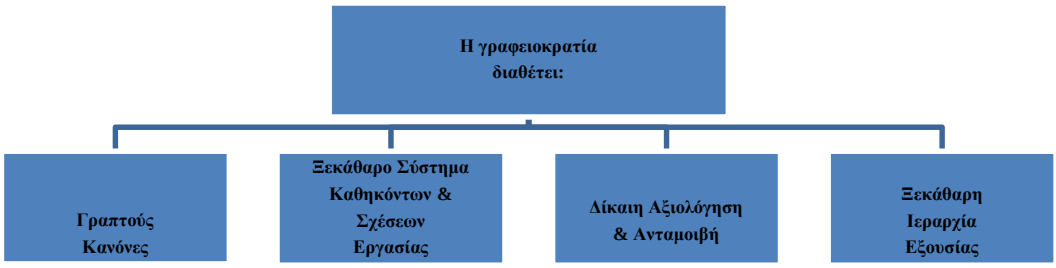
6. Δίκαιη και ισότιμη αξιολόγηση και ανταμοιβή των εργαζομένων. Μερικές φορές τα παραπάνω οδηγούν σε “red -tape” (υπερβολική γραφειοκρατία) και άλλα προβλήματα.

1.2.2 Τα χαρακτηριστικά της Γραφειοκρατίας

Ο Max Weber ορίζει έξι βασικά χαρακτηριστικά της γραφειοκρατίας:

- Οι εξουσίες και οι ευθύνες του υπαλλήλου ορίζονται με απόλυτη ευκρίνεια και νομιμοποιούνται ως επίσημα καθήκοντα.
- Οι θέσεις εξουσίας οργανώνονται με μια ιεραρχία εξουσίας από πάνω προς τα κάτω.
- Το προσωπικό επιλέγεται και εξελίσσεται βάσει προσόντων, τα οποία εκτιμώνται με εξέταση, με την εκπαίδευση και με την εμπειρία.
- Οι διοικητικές δράσεις και αποφάσεις καταγράφονται και αποτελούν τμήμα μόνιμου και διαρκούς αρχείου. Η φύλαξη των εγγράφων παρέχει οργάνωση και συνέχεια στον χρόνο.
- Η διοίκηση είναι διακριτή από την ιδιοκτησία του οργανισμού.
- Τα διοικητικά στελέχη υπόκεινται σε κανόνες και διαδικασίες, οι οποίες εξασφαλίζουν αξιόπιστη συμπεριφορά. Οι κανόνες είναι απρόσωποι και ομοιόμορφοι και εφαρμόζονται σε όλους τους εργαζομένους.

Στο παρακάτω σχήμα παρουσιάζουμε τις αρχές της γραφειοκρατίας.



Σχήμα 1. Αρχές Γραφειοκρατίας

Οι βασικές αρχές της γραφειοκρατίας και τα κύρια χαρακτηριστικά που την καθιστούν αποτελεσματική συνοψίζονται σε τέσσερις (4) κατηγορίες, όπως φαίνεται και από το παραπάνω Σχήμα 1:

1. *Γραπτοί κανόνες:* Η ύπαρξη γραπτών κανόνων οι οποίοι θεσπίστηκαν και εφαρμόζονται πιστά, καθιστούν τη λειτουργία της γραφειοκρατίας ευκολότερη, ταχύτερη και ως εκ τούτου αποτελεσματικότερη.

2. *Ξεκάθαρα καθήκοντα και εργασιακές σχέσεις:* Ο διαυγής διαχωρισμός του ρόλου και των καθηκόντων του κάθε εργαζόμενου που εμπλέκεται σε κάποια διαδικασία καθιστά την εργασία του πιο αποδοτική, ενώ ταυτόχρονα μειώνει τις προστριβές με τους συναδέλφους και την σύγχυση και σύγκρουση καθηκόντων μεταξύ αυτών, που αποτελούν συνήθη εργασιακά ζητήματα. Ειδικότερα στα γραφειοκρατικά ζητήματα που χαρακτηρίζονται από έντονη πολυπλοκότητα, ο σαφής διαχωρισμός των ρόλων θα αποβεί μείζονος σημασίας για τη σωστή λειτουργία της.

3. *Δίκαιη αξιολόγηση και ανταμοιβή:* Το βασικότερο εργασιακό κίνητρο, σε οποιονδήποτε τομέα είναι η ανταμοιβή, οικονομική και μη, των κόπων που καταβάλλει καθένας. Έτσι, ένα δίκαιο σύστημα αξιολόγησης του κόπου κάθε υπαλλήλου και αντιστοίχως ένα ανάλογο μισθολογικό επίπεδο, συμβάλουν δραματικά στη καταβολή της μέγιστης προσπάθειας του εργαζόμενου στα καθήκοντα και τις υποχρεώσεις του.

4. *Ανέλιξη στην ιεραρχία*: Σαν απόρροια της προηγούμενης κατηγορίας, ένας άλλος τρόπος ανταμοιβής της εργασιακής προσφοράς είναι η αναγνώριση των προσπαθειών του μέσω προαγωγών και ανέλιξης στην ιεραρχική κλίμακα του εργασιακού του περιβάλλοντος. Μια δίκαιη αξιολόγηση των δυνατοτήτων και της προσφοράς κάθε εργαζομένου και μια αντίστοιχη εξέλιξη στην ιεραρχική κλίμακα, επιβραβεύοντας τους κόπους του και ωφελώντας εν τέλει τους ίδιους τους κόλπους της επιχείρησης.

1.3 **Η ιστορία της Θεωρίας της Διοίκησης (Management Theory History)**

Ιστορικά, η θεωρία της διοίκησης πέρασε από τρεις (5) χρονικές περιόδους, όπως διακρίνουμε και στο Σχήμα 2. Την Προ-κλασική, την Κλασική, όπου αναπτύχθηκε έντονα το

management, μέσω της επιστημονικής, γραφειοκρατικής και διαχειριστικής μορφής του, την Συμπεριφορική, όπου υπήρξε ένας έντονος ανθρωποκεντρισμός και ο τρόπος συμπεριφοράς απέκτησε ιδιαίτερη αξία, την Ποσοτική, όπου έκανε την εμφάνιση της η διοίκηση ως επιστήμη, συμβάλλοντας σε παραγωγή και υπηρεσίες και , τέλος, η Σύγχρονη όπου μιλάμε πλέον για συστήματα, συσχετιζόμενες φάσεις και νέες θεωρήσεις, έχοντας πάντα τα εργαλεία του management ως όπλο.

1.3.1 Χρονολογική εξέλιξη Θεωρίας Διοίκησης

Αν επιχειρούσαμε να κάνουμε και μια χρονολογική προσέγγιση στην εξέλιξη της Διοικητικής επιστήμης, θα μπορούσαμε να την παρουσιάσουμε μέσω του Σχήματος 3, όπου συνολικά βλέπουμε μια δραστηριότητα που βρίσκει τις απαρχές της στο 1890 και συνεχίζει την εξέλιξη της μέχρι και τις μέρες μας εν έτει 2010. Πολλά εξελικτικά στάδια συνέπεσαν χρονικά, κάνοντας έτσι πιο ομαλή την μετάβαση από το ένα «σκαλοπάτι» στο επόμενο. Βλέπουμε ότι μέχρι και την τελευταία δεκαετία του 20^{ου} αιώνα, η διοίκηση κατείχε μια περισσότερο θεωρητική μορφή, φτάνοντας στο 2000 έχουμε όμως έντονη πλέον την παρουσία των συστημάτων, η οποία και αναπτύχθηκε δραματικά οδηγώντας μας σήμερα σε καθαρά τεχνολογικά εργασιακά περιβάλλοντα μέσω των οποίων πραγματοποιείται η πλειονότητα των καθημερινών μας δραστηριοτήτων. Παρακάτω αναφέρουμε κατά χρονολογική σειρά την εξέλιξη της Θεωρίας Διοίκησης.

- The Technology-Driven Workplace 2000-2010
- The Learning Organization 1990-2010
- Total Quality Management 1980- 2000
- Contingency Views 1970- 2000
- Systems Theory 1950- 2000
- Management Science Perspective 1940- 1990
- Humanistic Perspective 1930- 1990
- Classical 1890- 1940

1.3.2 Διοικητική Επιστήμη

Χρησιμοποιεί ακριβείς ποσοτικές τεχνικές για να μεγιστοποιήσει την αξιοποίηση των χρησιμοποιούμενων πόρων[1]

i.Ποσοτική Διοίκηση (Quantitative management): χρησιμοποιεί γραμμικό προγραμματισμό, μοντελοποίηση, και μεθόδους προσομοίωσης.
ii.Διοίκηση Παραγωγής (Operations management): τεχνικές για την ανάλυση όλων των παραμέτρων της παραγωγής.
iii.Διοίκηση Ολικής Ποιότητας (TQM): επικεντρώνεται στην βελτίωση της ποιότητας.
iv.Διοίκηση Πληροφοριακών Συστημάτων (MIS): παρέχει πληροφορίες σχετικά με την επιχείρηση[2].

1.4 Η Αποστολή της Δ.Η.Ε

Η αποστολή της Δίωξης Ηλεκτρονικού Εγκλήματος (Δ.Η.Ε) συμπεριλαμβάνει 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.

---

[1] Βλ. σχετικά, ΠΑΝΤ. ΤΕΡΛΕΞΗΣ, *Ο Καπιταλισμός στα όριά του*, Τομ. 2ος, εκδ. Παπαζήση, Αθήνα, 1999, κεφ. XI, σελ. 241 επ., και Ν.Χ.ΤΑΤΣΗΣ (επιμ.), *Max Weber - ερμηνευτικά κείμενα, εκδ. Οδυσσέας, Αθήνα, 1998, σελ. 106 επ.*
[2] Βλ. MAX WEBER, *The Theory of Social and Economic Organization*, επιμ. Talcott Parsons, The Free Press, NY, 1964,σελ. 339. Βλ., επίσης, ΑΝΤ. ΜΑΚΡΥΔΗΜΗΤΡΗ, *Διοίκηση και Κοινωνία. Η δημόσια διοίκηση στην Ελλάδα*, εκδ. Θεμέλιο, Αθήνα, 1999, σελ. 418

- 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.
Το Διαδίκτυο είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί εκατομμύρια 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.

ΚΕΦΑΛΑΙΟ 2^{Ο}

-ΟΡΓΑΝΩΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ -

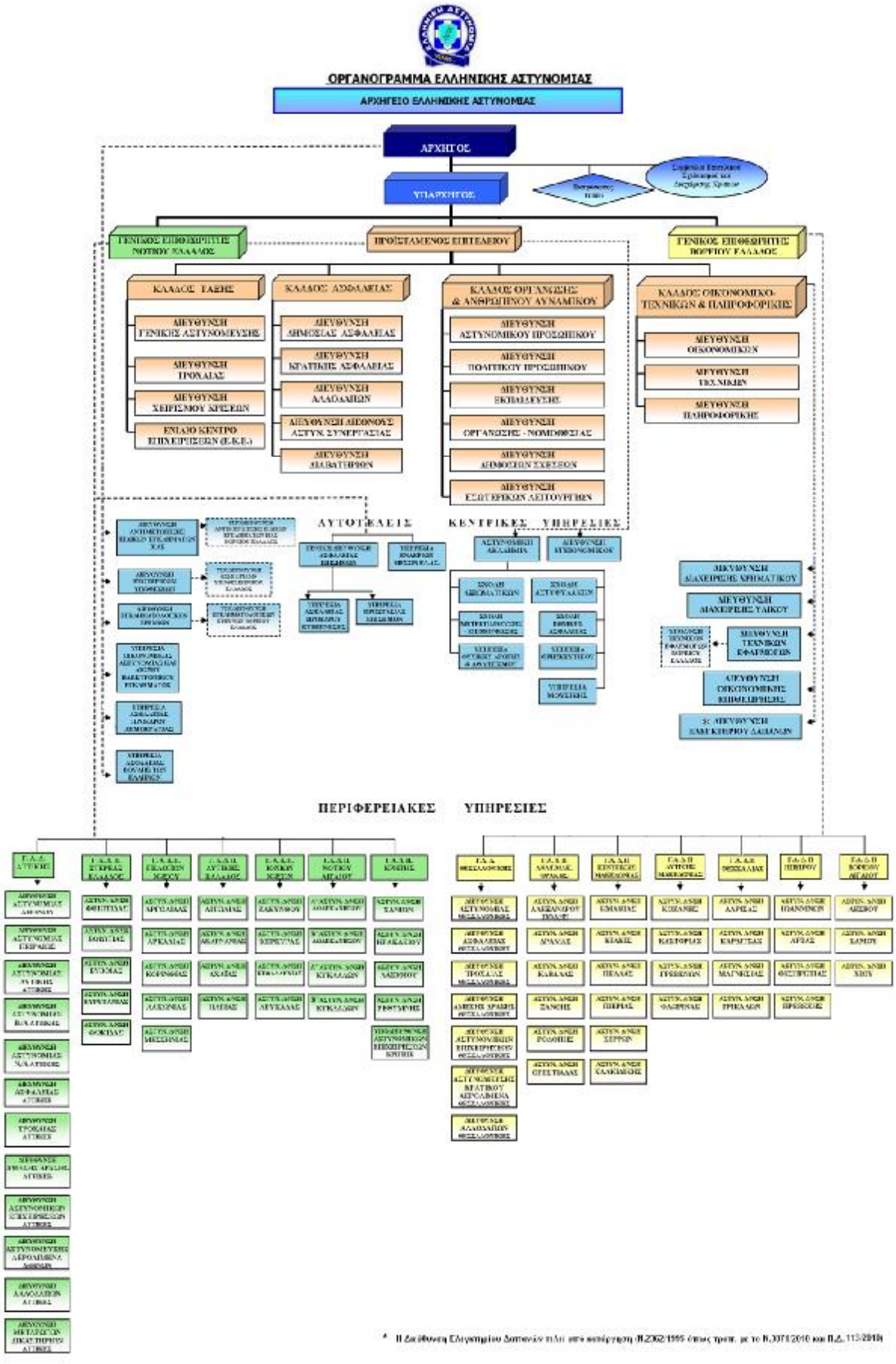
2.1 **Θεωρία των οργανώσεων**

Ένα βασικό χαρακτηριστικό γνώρισμα των «υπέρ-οργανωμένωνν» κοινωνιών της εποχής μας είναι ότι σε όλους σχεδόν τους τομείς της κοινωνικής δράσης και της συμπεριφοράς, από την πολιτική και τη δημόσια διοίκηση ως τις επιχειρήσεις, τις υπηρεσίες και τη βιομηχανία, και από τις εθελοντικές οργανώσεις ως τους μηχανισμούς ασφάλειας και τα συστήματα καταστολής του κράτους, σημειώνεται μια εντεινόμενη γραφειοκρατικοποίηση του οργανωτικού και του διοικητικού πεδίου. Γενικότερα, η οργάνωση του κοινωνικού κεφαλαίου σχεδόν στην ολότητά του, σε όλες δηλαδή τις εκφάνσεις και τους σχηματισμούς του, στην πολιτική, στην οικονομία, στον πολιτισμό και στις πάσης φύσεως κοινωνικές συμπεριφορές, μοιάζει να αποτελεί μια περίπου αναπόφευκτη διαδικασία που συνάπτεται οργανικά με την ίδια τη λογική και τη δυναμική του εκσυγχρονισμού των κοινωνιών. Κατά τρόπο μάλιστα φαινομενικά παράδοξο, ακόμα και η κριτική και η ριζοσπαστική αμφισβήτηση του οργανωτικού παραδείγματος, ή μάλλον των «παραδειγμάτων» της νεωτερικότητας, δεν αποφεύγει την υποταγή της στην οργανωτική αναγκαιότητα.

Το Σώμα Δίωξης από την αρχή της ίδρυσης και λειτουργίας του έως σήμερα έχει καταφέρει να αποτρέψει και να εξιχνιάσει πλειάδα ηλεκτρονικών παραβάσεων ιδιαίτερα σοβαρών και επικίνδυνων για την ασφάλεια μας στο Διαδίκτυο. Είναι με λίγα λόγια ο φορέας εκείνος που οφείλει κάποιος να αποταθεί όταν γίνεται δέκτης μιας συμπεριφοράς που εντάσσεται στα πλαίσια της παραβατικότητας. Στο Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος καταγγέλλονται πράξεις όπως η παιδική πορνογραφία και κακοποίηση των παιδιών, η διακίνηση παράνομου - πειρατικού λογισμικού, οι απάτες μέσω διαδικτύου, οι απάτες μέσω πιστωτικών καρτών και το Cracking (ψηφιακοί βανδαλισμοί - Deface και άλλα). Επιπλέον η διακίνηση ναρκωτικών, η εκβίαση μέσω του Διαδίκτυο και τέλος η συκοφαντική δυσφήμηση και η παραβίαση προσωπικών δεδομένων μέσω του διαδικτύου. Θεματοφύλακες της ασφάλειας της χρήσης του διαδικτύου και προαγωγοί της, είναι οι άνθρωποι που πλαισιώνουν

την υπηρεσία αυτή και έχουν ανώτερες γνώσεις πάνω στο Διαδίκτυο και στην ασφάλεια. Από τον Οκτώβριο του 2011 η Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος συνενώθηκε με την Οικονομική Αστυνομία και μετονομάστηκε σε Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΠ.Ο.Α.Δ.Η.Ε).

Στο σημείο αυτό παρατίθεται το βασικό οργανόγραμμα της Ελληνικής Αστυνομίας, ξεκινώντας από τους βασικούς πυλώνες και φτάνωντας μέχρι και τα τελευταία επιμέρους τμήματα. Σκοπός είναι η όσο το δυνατόν πληρέστερη κατανόηση του τρόπου διαβάθμισης και λειτουργίας του ελληνικού αστυνομικού σώματος.



Σχήμα 2. Οργανόγραμμα Ελληνικής Αστυνομίας

2.2 **Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος**

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος είναι ειδική αυτοτελής κεντρική υπηρεσία της Ελληνικής Αστυνομίας με αποστολή τη διερεύνηση, εξιχνίαση και δίωξη εγκλημάτων που τελέστηκαν σε βάρος των συμφερόντων του δημοσίου και της Εθνικής Οικονομίας ή έχουν τα χαρακτηριστική του οργανωμένου οικονομικού εγκλήματος, καθώς και οποιαδήποτε εγκλήματα διαπράττονται με τη χρήση του διαδικτύου. Υπάγεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας και εποπτεύεται στην προανακριτική της δράση από τον Εισαγγελέα του Οργανωμένου Εγκλήματος. Άρχισε τη λειτουργία της τον Ιούλιο του 2011 και διέπεται από ειδικό θεσμικό πλαίσιο.

Έχει ως αποστολή τη διερεύνηση, εξιχνίαση και δίωξη εγκλημάτων που τελέστηκαν σε βάρος των συμφερόντων του δημοσίου και της Εθνικής Οικονομίας ή έχουν τα χαρακτηριστική του οργανωμένου οικονομικού εγκλήματος, καθώς και οποιωνδήποτε εγκλημάτων διαπράττονται με τη χρήση του διαδικτύου. Υπάγεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας και εποπτεύεται στην προανακριτική της δράση από τον Εισαγγελέα του Οργανωμένου Εγκλήματος. Άρχισε τη λειτουργία της τον Ιούλιο του 2011 και διέπεται από ειδικό θεσμικό πλαίσιο.

Η ΥΠ.Ο.Α.Δ.Η.Ε. διαρθρώνεται από το Επιτελείο, καθώς επίσης και από τους δύο επιχειρησιακούς τομείς αστυνομικής δράσης: την Υποδιεύθυνση Οικονομικής Αστυνομίας και την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος. Η ΥΠΟΑΔ.Η.Ε εδρεύει στην Αθήνα, στον 13ο και 14ο όροφο του Αστυνομικού Μεγάρου Αθηνών, στη Λεωφόρο Αλεξάνδρας 173. Η τοπική της αρμοδιότητα εκτείνεται σε όλη την Ελλάδα. Η δράση της υποστηρίζεται στην περιφέρεια από τους κατά τόπους Αστυνομικούς Συνδέσμους που έχει αναπτύξει. Τα στελέχη αυτά έχουν εκπαιδευτεί ειδικά με σκοπό να εξασφαλιστεί το μέγιστο της αποτελεσματικής συνεργασίας των Υπηρεσιών στις περιπτώσεις κοινής ή επικουρικής επιχειρησιακής δράσης. Η ΥΠ.Ο.Α.Δ.Η.Ε. στελεχώνεται με έμπειρα στελέχη της Ελληνικής Αστυνομίας, που προέρχονται κυρίως από Υπηρεσίες της Ασφάλειας, καθώς και Αξιωματικούς Ειδικών Καθηκόντων, πτυχιούχους ανώτατων εκπαιδευτικών ιδρυμάτων, με μεταπτυχιακούς τίτλους στα γνωστικά αντικείμενα:

- Χρηματοοικονομικής

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

Η επιλογή του προσωπικού γίνεται με αυστηρά κριτήρια. Σε αυτά συνεκτιμάται η επαγγελματική επάρκεια, οι επιστημονικές γνώσεις, η αποδοτικότητα και το ήθος. Η αστυνομική και προανακριτική έρευνα της Οικονομικής Αστυνομίας και της Δίωξης Ηλεκτρονικού Εγκλήματος ακολουθεί τους κανόνες και τις διατάξεις του Κώδικά Ποινικής Δικονομίας. Όλες οι καταγγελίες ή πληροφορίες, ανώνυμες ή επώνυμες, εξετάζονται από Ομάδα Αξιολόγησης και ταξινομούνται σύμφωνα με το είδος, το περιεχόμενο της καταγγελίας και την γεωγραφική της περιοχή. Η δράση της περιλαμβάνει μόνο εκείνες τις συμπεριφορές που έχουν αξιόποινο χαρακτήρα και εξετάζονται από τις Δικαστικές Αρχές. Κατά τη διάρκεια της προκαταρκτικής εξέτασης ή προανάκρισης δεν ισχύει το φορολογικό, τραπεζικό, χρηματιστηριακό ή επιχειρηματικό απόρρητο. Η ΥΠΟΑΔ.Η.Ε έχει πρόσβαση στα αρχεία οποιασδήποτε αστυνομικής υπηρεσίας, καθώς και σε αρχεία άλλων υπηρεσιών, αρχών, οργανισμών και φορέων, ενώ ανταλλάσσει πληροφοριακά και άλλα στοιχεία με υπηρεσίες του Υπουργείου Οικονομικών, τα οποία είναι αναγκαία για την εφαρμογή της φορολογικής και τελωνειακής νομοθεσίας. Τέλος, χρησιμοποιεί ειδικό λογισμικό για την ανάλυση εγκληματολογικών πληροφοριών, τη λεπτομερή μελέτη και υποστήριξη της διερεύνησης σοβαρών υποθέσεων, καθώς και την στρατηγική ανάλυση για την εξέλιξη του οικονομικού και ηλεκτρονικού εγκλήματος στην Ελλάδα. Για κάθε περίπτωση συλλογής προανακριτικού υλικού ενημερώνει τις αντίστοιχες φορολογικές αρχές για την επιβολή των αντίστοιχων διοικητικών παραβάσεων.

Στο παραπάνω οργανόγραμμα παριστάνεται η ιεραρχική διαβάθμιση της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, η οποία και αποτελείται από τρεις (3) κύριους πυλώνες: Το Επιτελείο, την Οικονομική αστυνομία και την Δ.Η.Ε καθαρά. Οι 3 υποδιευθύνσεις χωρίζονται σε περαιτέρω τμήματα όπως παρατηρούμε, με σκοπό την αποδοτικότερη λειτουργία τους.

2.3 **Σύσταση Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος**

Συμφώνα με το Προεδρικό Διάταγμα υπ' αριθμ. 9/2011, με βάση το άρθρο 1:

Η ΥΠ.Ο.Α.Δ.Η.Ε[3]. διαρθρώνεται ως εξής:

α. Επιτελείο.

β. Υποδιεύθυνση Οικονομικής Αστυνομίας.

γ. Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.

Το Επιτελείο της ΥΠ.Ο.Α.Δ.Η.Ε[4]. διαρθρώνεται στα ακόλουθα τμήματα:

- Τμήμα Διοικητικής Υποστήριξης το οποίο είναι αρμόδιο για το χειρισμό θεμάτων προσωπικού, τη διαχείριση του χρηματικού και υλικού, τη γραμματειακή και τεχνική υποστήριξη και γενικά την εξυπηρέτηση των λειτουργικών αναγκών της Υπηρεσίας.

- Τμήμα Εκπαίδευσης, το οποίο είναι αρμόδιο για τη διαρκή εξειδικευμένη εκπαίδευση και μετεκπαίδευση του προσωπικού της ΥΠ.Ο.Α.Δ.Η.Ε. καθώς και προσωπικού άλλων Υπηρεσιών της Ελληνικής Αστυνομίας σε θέματα καταπολέμησης του οικονομικού και ηλεκτρονικού εγκλήματος. Προς τούτο, καταρτίζει και υλοποιεί σχετικά προγράμματα εκπαίδευσης και μετεκπαίδευσης, σε συνεργασία με τη Διεύθυνση Εκπαίδευσης του Αρχηγείου της Ελληνικής Αστυνομίας, καθώς και με άλλες αρμόδιες υπηρεσίες ή φορείς της χώρας μας και άλλων χωρών.

- Τμήμα Μελετών, το οποίο είναι αρμόδιο για τη συλλογή, μελέτη, ανάλυση και επεξεργασία πληροφοριών, στοιχείων και δεδομένων σχετικών με την αποστολή της Υπηρεσίας και την προώθηση των επεξεργασμένων στοιχείων στις Υποδιευθύνσεις για επιχειρησιακή

[3] Το άρθρο 11 παρ. 1 περιπτ. α΄, β΄, στ΄ και ζ΄ του ν. 1481/1984 «Οργανισμός Υπουργείου Δημόσιας Τάξης» (Α΄ 152), όπως το άρθρο αυτό αντικαταστάθηκε με το άρθρο 1 παρ. 1 του ν. 1590/1986 (Α΄ 49).
[4] Τα άρθρα 14 παρ. 7 και 28 παρ. 1 του ν. 2800/2000 «Αναδιάρθρωση Υπηρεσιών Υπουργείου Δημόσιας Τάξης, σύσταση Αρχηγείου Ελληνικής Αστυνομίας και άλλες διατάξεις» (Α΄ 41).

αξιοποίηση, κατά λόγο αρμοδιότητας. Επίσης, είναι αρμόδιο για την παρακολούθηση των εξελίξεων σε θέματα οικονομικού και ηλεκτρονικού εγκλήματος, τόσο σε εσωτερικό όσο και σε διεθνές επίπεδο, την εκπόνηση σχετικής ετήσιας μελέτης, με συναγωγή συμπερασμάτων για την εγκληματικότητα επί των αδικημάτων αυτών στη χώρα μας και την υποβολή συγκεκριμένων αιτιολογημένων προτάσεων για την αντιμετώπισή τους. Στο Επιτελείο της ΥΠ.Ο.Α.Δ.Η.Ε.

- Λειτουργεί Κέντρο Επιχειρήσεων το οποίο εξασφαλίζει το συντονισμό και την επικοινωνία του προσωπικού της Υπηρεσίας κατά τη διάρκεια της επιχειρησιακής του δράσης. Επίσης, στο Κέντρο Επιχειρήσεων λειτουργεί σε 24ωρη βάση τηλεφωνικό κέντρο με ειδική γραμμή καταγγελιών καθώς και ηλεκτρονική διεύθυνση για την επικοινωνία των πολιτών με την Υπηρεσία.

Η ΥΠ.Ο.Α[5]. διαρθρώνεται στα ακόλουθα τμήματα:

- Τμήμα Προστασίας Δημόσιας Περιουσίας, το οποίο είναι αρμόδιο για την έρευνα και τη δίωξη οικονομικών εγκλημάτων τα οποία διαπράττονται από φυσικά ή νομικά πρόσωπα και βλάπτουν ή απειλούν τα συμφέροντα του ελληνικού δημοσίου ή του ευρύτερου δημόσιου τομέα και αφορούν,

- Τμήμα Κοινωνικής και Ασφαλιστικής Προστασίας, το οποίο είναι αρμόδιο για την έρευνα και τη δίωξη παραβάσεων σε βάρος οργανισμών κοινωνικής ασφάλισης, πρόνοιας και περίθαλψης των πολιτών και ιδίως η μη καταβολή των προβλεπομένων ασφαλιστικών εισφορών από φυσικά ή νομικά πρόσωπα, εταιρείες, οργανισμούς και γενικά από κάθε υπόχρεο προς τούτο.

Η Δίωξη Ηλεκτρονικού Εγκλήματος[6], 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:

[5] Το άρθρο 90 του Κώδικα Νομοθεσίας για την Κυβέρνηση και τα κυβερνητικά όργανα, που κωδικοποιήθηκε με το άρθρο πρώτο του π.δ. 63/2005 (Α΄ 98).
[6] Το άρθρο 22 παρ. 3 του ν. 2362/1995 «Περί δημοσίου λογιστικού ελέγχου των δαπανών του κράτους και άλλες διατάξεις» (Α΄ 247).

- 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.

- Ένα ακόμη τμήμα με το όποιο ασχολείται η Δ.Η.Ε είναι αυτό της αποτροπής της αποκλίνουσας συμπεριφοράς (αυτοκτονιών).

Η ΥΠ.Ο.Α.Δ.Η.Ε[7]. είναι ισότιμη με τις υπηρεσίες της Ελληνικής Αστυνομίας επιπέδου Αστυνομικής Διεύθυνσης. Οι Υποδιευθύνσεις Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος είναι μεταξύ τους και προς όλες τις Υπηρεσίες επιπέδου Υποδιεύθυνσης της Ελληνικής Αστυνομίας ισότιμες. Τα Τμήματα του Επιτελείου και των Υποδιευθύνσεων καθώς και το Κέντρο Επιχειρήσεων της ΥΠ.Ο.Α.Δ.Η.Ε. είναι μεταξύ τους και προς όλες τις αυτοτελείς ή μη υπηρεσίες, αντίστοιχου επιπέδου, της Ελληνικής Αστυνομίας ισότιμα. Ο προϊστάμενος της ΥΠ.Ο.Α.Δ.Η.Ε. είναι Ταξίαρχος της Ελληνικής Αστυνομίας και φέρει τον τίτλο του Διευθυντή. Στην ΥΠ.Ο.Α.Δ.Η.Ε. τοποθετούνται ως βοηθοί του Διευθυντή, μέχρι δύο αξιωματικοί με το βαθμό του Αστυνομικού Διευθυντή, οι οποίοι φέρουν τον τίτλο του Υποδιευθυντή και είναι αρχαιότεροι των Διευθυντών των Υποδιευθύνσεων. Σε περίπτωση απουσίας ή κωλύματός του, ο Διευθυντής της Υπηρεσίας αναπληρώνεται από τον κατά βαθμό ανώτερο ή αρχαιότερο Υποδιευθυντή. Οι προϊστάμενοι των Υποδιευθύνσεων Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος είναι Αστυνομικοί Διευθυντές και φέρουν τον τίτλο του Διευθυντή. Στις Υποδιευθύνσεις

[7] Το π.δ. 184/2009 «Σύσταση Υπουργείου Προστασίας του Πολίτη και καθορισμός των αρμοδιοτήτων του» (Α΄ 213).

Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος τοποθετούνται ως βοηθοί των Διευθυντών Αστυνομικοί Διευθυντές ή Αστυνομικοί Υποδιευθυντές. Οι προϊστάμενοι των Τμημάτων του Επιτελείου και των Υποδιευθύνσεων είναι Αστυνομικοί Υποδιευθυντές ή Αστυνόμοι Α΄ και φέρουν τον τίτλο του Τμηματάρχη.

2.3.1 Αρμοδιότητες Διευθυντή της ΥΠ.Ο.Α.Δ.Η.Ε

Ο Διευθυντής της υπηρεσίας συντονίζει, εποπτεύει και ελέγχει το έργο των υπηρεσιών δικαιοδοσίας του. Εφαρμόζει τα προγράμματα δράσης του Αρχηγείου, παρέχει κατευθύνσεις στις Υποδιευθύνσεις δικαιοδοσίας του και θέτει επιμέρους στόχους για την υλοποίησή τους. Παρακολουθεί την εφαρμογή από τις ως άνω Υποδιευθύνσεις των μέτρων, μεθόδων και διαδικασιών που προβλέπονται από τις ισχύουσες διατάξεις και τις διαταγές της Υπηρεσίας, για την εκπλήρωση της αποστολής τους. Αξιολογεί τα αποτελέσματα της δράσης των ως άνω Υποδιευθύνσεων, ως προς τη λειτουργία των προγραμμάτων και την επίτευξη των στόχων και εισηγείται τις απαραίτητες διορθώσεις και προσαρμογές. Παρακολουθεί την πορεία της εγκληματικότητας σε ότι αφορά στην αποστολή της Υπηρεσίας του και λαμβάνει ή προτείνει τα αναγκαία μέτρα για την αντιμετώπισή της. Αναλαμβάνει προσωπικά τη διεύθυνση αστυνομικών επιχειρήσεων, όταν κρίνει τούτο σκόπιμο ή διαταχθεί σχετικά.

Μεριμνά να μορφώνει ασφαλή γνώμη για την επαγγελματική επάρκεια, τα προσόντα ή τις αδυναμίες, την ικανότητα ως προς την άσκηση της διοίκησης, την ενημέρωση στα υπηρεσιακά θέματα και τη γενικότερη συμπεριφορά όλων των αξιωματικών των υπηρεσιών δικαιοδοσίας του και ιδιαίτερα των διοικούντων, ώστε να είναι σε θέση, σε κάθε περίπτωση, να αποφαίνεται για την επάρκεια και καταλληλότητά τους για τις διάφορες υπηρεσίες, εργασίες και αποστολές. Συνεργάζεται με τις λοιπές υπηρεσίες της Ελληνικής Αστυνομίας καθώς και με τις δικαστικές, στρατιωτικές και άλλες δημόσιες αρχές, φορείς και υπηρεσίες μέσα στο πλαίσιο των αρμοδιοτήτων του. Εκτελεί κάθε άλλη αρμοδιότητα που ανατίθεται σ’ αυτόν από τον οργανισμό και τους κανονισμούς της Ελληνικής Αστυνομίας ή από ειδικές διατάξεις. Συντάσσει τις εκθέσεις ικανότητας των Υποδιευθυντών της ΥΠ.Ο.Α.Δ.Η.Ε. και γνωματεύει σε εκείνες που συντάσσουν οι τελευταίοι.

2.3.2 Καθήκοντα Υποδιευθυντών της ΥΠ.Ο.Α.Δ.Η.Ε

Οι υποδιευθυντές είναι άμεσοι βοηθοί του Διευθυντή της ΥΠ.Ο.Α.Δ.Η.Ε. και εκτελούν τα καθήκοντά τους σύμφωνα με τους ισχύοντες νόμους και κανονισμούς και ανάλογα με τις διαταγές και οδηγίες του. Αναλαμβάνουν προσωπικά την εποπτεία και το συντονισμό αστυνομικών επιχειρήσεων ή την ευθύνη υλοποίησης συγκεκριμένων προγραμμάτων σε περιπτώσεις μείζονος σπουδαιότητας ή όταν διαταχθούν σχετικά. Λαμβάνουν γνώση της εισερχόμενης και εξερχόμενης αλληλογραφίας και διατυπώνουν τη γνώμη τους στις εισηγήσεις των Υποδιευθύνσεων[8]. Ενεργούν τακτικές ή έκτακτες επιθεωρήσεις στις Υποδιευθύνσεις της ΥΠ.Ο.Α.Δ.Η.Ε. σύμφωνα με τις διαταγές του Διευθυντή της. Ενημερώνονται για όλα τα λειτουργικά και επιχειρησιακά ζητήματα της Υπηρεσίας και παρεμβαίνουν για την άμεση επίλυση τυχόν προβλημάτων ή εισηγούνται μέτρα και ρυθμίσεις για την αντιμετώπισή τους. Ο ανώτερος κατά βαθμό ή αρχαιότερος των Υποδιευθυντών συντάσσει τις εκθέσεις ικανότητας των προϊσταμένων των Τμημάτων του Επιτελείου, καθώς και των Διευθυντών των Υποδιευθύνσεων της ΥΠ.Ο.Α.Δ.Η.Ε. και γνωματεύει σ' εκείνες που συντάσσουν αυτοί. Εκτελούν κάθε άλλη αρμοδιότητα που ανατίθεται σ΄ αυτούς από τις ισχύουσες διατάξεις και τις διαταγές του προϊσταμένου τους.

2.3.3 Αρμοδιότητες Διευθυντών και Υποδιευθυντών της ΥΠ.Ο.Α.Δ.Η.Ε

Οι διευθυντές της ΥΠ.Ο.Α.Δ.Η.Ε προγραμματίζουν και ελέγχουν τη δράση των Υποδιευθύνσεων με τη βοήθεια των Υποδιευθυντών και των προϊσταμένων των Τμημάτων. Μεριμνούν ώστε η δράση των Τμημάτων να έχει κοινή κατεύθυνση. Καθιερώνουν κριτήρια, με βάση τα οποία αξιολογείται η απόδοση των Τμημάτων των Υποδιευθύνσεων, μεριμνούν για τη μέτρηση της απόδοσής τους, σε καθημερινή και μεγαλύτερων χρονικών περιόδων βάση, μελετούν και αξιολογούν τις σχετικές πληροφορίες και τέλος προβαίνουν στη διόρθωση των παρεκκλίσεων. Τοποθετούν το προσωπικό σε θέσεις, ανάλογα με τις δυνατότητες και τα προσόντα του, φροντίζουν για την ορθολογική, δίκαιη και αντικειμενική κατανομή της υπηρεσίας και αναθέτουν με διαταγή τους καθήκοντα στους Υποδιευθυντές αυτών. Φροντίζουν για τη διατήρηση σχέσεων καλής επικοινωνίας, συνεργασίας και αμοιβαίας κατανόησης μεταξύ του προσωπικού καθώς και για τη διατήρηση της συνοχής της υπηρεσίας.

[8] Την 2672/3−12−2009 απόφαση του Πρωθυπουργού και του Υπουργού Οικονομικών «Καθορισμός αρμοδιοτήτων του Υφυπουργού Οικονομικών Φιλίππου Σαχινίδη (Β΄ 2408).

Ενεργούν συγκεντρώσεις του προσωπικού, στο σύνολό του ή κατά Τμήμα, δίδουν κατευθύνσεις και οδηγίες αναφορικά με την αποστολή και τη δράση της Υποδιεύθυνσης, ελέγχουν την καθαριότητα και κατάσταση του οπλισμού, του υλικοτεχνικού εξοπλισμού, των μέσων και των λοιπών εφοδίων που κατέχει το προσωπικό και διατάσσουν τη λήψη των αναγκαίων μέτρων για τη συντήρησή του. Μελετούν την εισερχόμενη αλληλογραφία, επισημαίνουν τα ιδιαίτερης σημασίας και επείγουσας φύσης έγγραφα και σημειώνουν σ΄ αυτά τις τυχόν παρατηρήσεις και οδηγίες τους προς τα αρμόδια Τμήματα.

Προκαλούν τις ενέργειες των προϊσταμένων τους για τον εφοδιασμό της Υποδιεύθυνσης με τον αναγκαίο υλικοτεχνικό εξοπλισμό. Συνεργάζονται αρμονικά με τις αρμόδιες κατά περίπτωση διοικητικές, δικαστικές και αστυνομικές αρχές για την αποτελεσματικότερη εκπλήρωση της αποστολής τους. Ενημερώνουν τον Υποδιευθυντή ή άλλον αρμόδιο αξιωματικό όταν αναχωρούν από το χώρο εργασίας τους ή το κατάστημα της Υπηρεσίας, για το μέρος στο οποίο σε περίπτωση ανάγκης πρέπει να αναζητηθούν. Συντάσσουν τις εκθέσεις ικανότητας των Υποδιευθυντών τους και γνωματεύουν σ' αυτές που συντάσσουν οι τελευταίοι. Συνεργάζονται μεταξύ τους στο πλαίσιο του σχεδιασμού και της αντιμετώπισης κοινού ενδιαφέροντος υποθέσεων και εποπτεύουν άμεσα ή αναλαμβάνουν τη διεύθυνση ιδιαιτέρως σοβαρών υποθέσεων σε περιπτώσεις που εμπλέκονται επιχειρησιακά περισσότερα του ενός Τμήματα της Υποδιεύθυνσής τους. Ασκούν και κάθε άλλη αρμοδιότητα που προβλέπεται από τις ισχύουσες διατάξεις ή τους ανατίθενται με διαταγή των προϊσταμένων τους.

2.3.4 Αρμοδιότητες προϊσταμένων και αναπληρωτών προϊσταμένων Τμημάτων

Οι Προϊστάμενοι των Τμημάτων του Επιτελείου και των Υποδιευθύνσεων έχουν τις αρμοδιότητες που ορίζονται στο άρθρο 26 του π.δ. 141/1991 (Α΄ 58). Επίσης, συντάσσουν τις εκθέσεις αξιολόγησης των αξιωματικών της Υπηρεσίας τους και γνωματεύουν στις εκθέσεις ικανότητας που συντάσσουν οι αναπληρωτές αυτών για το λοιπό προσωπικό. Οι αναπληρωτές προϊστάμενοι των ως άνω Τμημάτων έχουν τις ακόλουθες αρμοδιότητες:

[Είναι άμεσοι βοηθοί των τμηματαρχών και αναπληρώνουν αυτούς σε περίπτωση απουσίας ή κωλύματος. Επιβλέπουν τη διεξαγωγή των εργασιών και συντονίζουν τη δράση στους τομείς ευθύνης που τους ανατίθεται. Ενημερώνονται για τα προβλήματα των τομέων ευθύνης τους,

αξιολογούν αυτά και συμμετέχουν στο σχεδιασμό διάταξης της υπηρεσίας, για την αντιμετώπισή τους. Λαμβάνουν γνώση της εισερχόμενης αλληλογραφίας και προσυπογράφουν όλα τα έγγραφα τα οποία υπογράφει ο διοικητής, ανάλογα με τους τομείς ευθύνης τους. Συντάσσουν τις εκθέσεις ικανότητας του προσωπικού του Τμήματος. Εκτελούν κάθε άλλη αρμοδιότητα που ανατίθεται σ' αυτούς από τον οργανισμό και κανονισμούς της Ελληνικής Αστυνομίας ή από ειδικές διατάξεις] .

2.3.5 Τρόπος άσκησης αρμοδιοτήτων

Για την εκπλήρωση της αποστολής της η ΥΠ.Ο.Α.Δ.Η.Ε. συνεργάζεται με τις κατά τόπο αρμόδιες υπηρεσίες της Ελληνικής Αστυνομίας, καθώς και με άλλες αρμόδιες υπηρεσίες, αρχές και φορείς και εξοπλίζονται με τα απαραίτητα υλικοτεχνικά μέσα. Επίσης, στο πλαίσιο της αποστολής της, συνεργάζεται με αντίστοιχες υπηρεσίες, οργανισμούς και φορείς ευρωπαϊκών και άλλων χωρών, σύμφωνα με τις ισχύουσες διατάξεις και τις διεθνείς συμφωνίες και συμβάσεις. Κατά την επεξεργασία και ανταλλαγή πληροφοριακού υλικού και δεδομένων που πραγματοποιούνται στο πλαίσιο εκπλήρωσης της αποστολής της Υπηρεσίας, εφαρμόζονται οι διατάξεις του νόμου 2472/1997 (Α΄ 50), όπως ισχύει κάθε φορά, σε σχέση με την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το προσωπικό της ΥΠ.Ο.Α.Δ.Η.Ε. εκπαιδεύεται και μετεκπαιδεύεται στο εσωτερικό και στο εξωτερικό, για την αποτελεσματική εκπλήρωση της αποστολής του. Οι αρμοδιότητες άλλων κρατικών ή ανεξάρτητων αρχών, υπηρεσιών και φορέων δεν επηρεάζονται από τις ρυθμίσεις του παρόντος διατάγματος. Οι υποχρεώσεις προσωπικού και Υπηρεσιών είναι οι ακόλουθες:

Το προσωπικό της ΥΠ.Ο.Α.Δ.Η.Ε. έχει καθήκον εχεμύθειας για πληροφορίες, στοιχεία ή άλλο διαβαθμισμένο υλικό των οποίων λαμβάνει γνώση στο πλαίσιο της άσκησης των καθηκόντων του. Η παράβαση του καθήκοντος αυτού, πέραν των προβλεπομένων, από τις ισχύουσες κάθε φορά διατάξεις, κυρώσεων, αποτελεί και λόγο απομάκρυνσης των παραβατών από την Υπηρεσία. Οι υπηρεσίες της Ελληνικής Αστυνομίας υποχρεούνται να παρέχουν τη συνδρομή τους στην ΥΠ.Ο.Α.Δ.Η.Ε. και να διαβιβάζουν σ' αυτήν οποιαδήποτε σχετική πληροφορία ή στοιχείο αναφορικά με αδικήματα που ανάγονται στην αποστολή της.

2.4 **Διυπηρεσιακή Συνεργασία & παράλληλη δράση**

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, στο πλαίσιο της διυπηρεσιακής συνεργασίας, συνεργάζεται με το Σώμα Δίωξης Οικονομικού Εγκλήματος (Σ.Δ.Ο.Ε.), τις φοροελεγκτικές, τελωνειακές και λοιπές Υπηρεσίες του Υπουργείου Οικονομικών. Στο πλαίσιο της επιχειρησιακής αστυνομικής της δράσης συνεργάζεται με το Κέντρο Συλλογής & Διαχείρισης Επιχειρησιακών Πληροφοριών (ΚΕ.ΣΥ.Δ.Ε.Π.) του Αρχηγείου της Ελληνικής Αστυνομίας, την Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.), το Λιμενικό Σώμα, την Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες, καθώς και με οργανισμούς και φορείς της Ευρωπαϊκής Ένωσης και άλλων χωρών (Europol, Interpol, SECI, OLAF κ.λπ.). Επίσης, αναπτύσσει συνεργασία με την Κτηματική Υπηρεσία Δημοσίου, την Υπηρεσία Εποπτείας Αγοράς, τη Διεύθυνση Εποπτείας Καζίνο, το Ίδρυμα Κοινωνικών Ασφαλίσεων (Ι.Κ.Α.), τους Επιθεωρητές Τομέα Υγειονομικού και Φαρμακευτικού Ελέγχου, πιστωτικά ιδρύματα, οργανισμούς προστασίας προϊόντων πνευματικής ιδιοκτησίας κ.λπ.

Η ΥΠ.Ο.Α.Δ.Η.Ε. συμμετέχει στο τριετές Εθνικό Επιχειρησιακό Πρόγραμμα Καταπολέμησης της Φοροδιαφυγής, όπου δρα σε τομείς έκνομης δραστηριότητας και κυρίως στα οικονομικά εγκλήματα, που εμφανίζουν χαρακτηριστικά οργανωμένου εγκλήματος. Στο πλαίσιο αυτό εφαρμόζει αυτοτελές Επιχειρησιακό Σχέδιο Δράσης για τη δίωξη των εγκλημάτων που αφορούν στην εφαρμογή της Φορολογικής και Τελωνειακής Νομοθεσίας. Το Σχέδιο αυτό προσανατολίζεται στην αντιμετώπιση εγκλημάτων που σχετίζονται άμεσα με την απώλεια εσόδων του κράτους. Οι επιχειρησιακές δράσεις καταπολέμησης της φοροδιαφυγής εστιάζουν στην αντιμετώπιση του λαθρεμπορίου, του παραεμπορίου, του παράνομου στοιχηματισμού των τυχερών παιχνιδιών, της φοροδιαφυγής φυσικών και νομικών προσώπων (με ποινική διάσταση) και της φοροδιαφυγής με τη χρήση του διαδικτύου. η οποία επιτυγχάνεται με την δορυφορική πειρατεία, τις παραβάσεις προστασίας πνευματικών δικαιωμάτων, τις απάτες σε βάρος οργανισμών κοινωνικής ασφάλισης, το διαδικτυακό εμπόριο και την παροχή διαδικτυακών υπηρεσιών καθώς την διενέργεια παράνομων τυχερών παιχνιδιών μέσω διαδικτύου (online Καζίνο) και την υποβολή απατηλών φορολογικών δηλώσεων.

Ο 21^{ος} αιώνας έχει φέρει την έντονη τεχνολογική εξέλιξη, χωρίς όμως αυτό να έχει μόνο θετικές απόρροιες. Το Διαδίκτυο είναι το κατ’ εξοχήν πλέον μέσο, για την εμφάνιση και

εξάπλωση φαινομένων που απαιτούν την παρέμβαση της Δ.Η.Ε.Αξίζει να σημειώσουμε και να υπογραμμίσουμε ότι η συγχώνεσυη των τμημάτων της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος έχει ως αποτέλεσμα την ορθότερη και αμεσότερη λήψη αποφάσεων καθώς το εύρος ελέγχου μειώνεται με αποτέλεσμα η διοίκηση των τμημάτων αυτών να γίνεται ευκολότερη. Ταυτόχρονα, εάν αναλογιστούμε το γεγονός ότι η πληθώρα των συναλλαγών στην εποχή μας, γίνεται μέσω πιστωτικών καρτών λαμβάνοντας τη μορφή ηλεκτρονικών συναλλαγών μέσω διαδικτύου και λοιπών ηλεκτρονικών μέσων, τότε οδηγούμαστε στο συμπέρασμα ότι η ενσωμάτωση της Δ.Η.Ε στο τμήμα της Υπηρεσίας Οικονομικής Αστυνομίας, μόνο ως ορθολογική απόφαση μπορεί να θεωρηθεί(e-shopping, e-commerce) σκεπτόμενοι παράλληλα την προσπάθεια μείωσης του διοικητικού κόστους , αλλά και του οικονομικού κόστους, ελέω οικονομικής κρίσης.

2.5 **Συνεργασία Δ.Η.Ε με άλλες υπηρεσίες**

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, στο πλαίσιο της διυπηρεσιακής συνεργασίας, συνεργάζεται με το Σώμα Δίωξης Οικονομικού Εγκλήματος (Σ.Δ.Ο.Ε.), τις φοροελεγκτικές, τελωνειακές και λοιπές Υπηρεσίες του Υπουργείου Οικονομικών[9].

Στο πλαίσιο της επιχειρησιακής αστυνομικής της δράση συνεργάζεται με το Κέντρο Συλλογής & Διαχείρισης Επιχειρησιακών Πληροφοριακών (ΚΕ.ΣΥ.Δ.Ε.Π.) του Αρχηγείου της Ελληνικής Αστυνομίας, την Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.), το Λιμενικό Σώμα, την Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες, καθώς και με οργανισμούς και φορείς της Ευρωπαϊκής Ένωσης και άλλων χωρών (Europol, Interpol, SECI, OLAF κ.λπ.). Επίσης, αναπτύσσει συνεργασία με την Κτηματική Υπηρεσία Δημοσίου, την Υπηρεσία Εποπτείας Αγοράς, τη Διεύθυνση Εποπτείας Καζίνο, το Ίδρυμα Κοινωνικών Ασφαλίσεων (Ι.Κ.Α.), τους Επιθεωρητές Τομέα Υγειονομικού και Φαρμακευτικού Ελέγχου, πιστωτικά ιδρύματα, οργανισμούς προστασίας προϊόντων πνευματικής ιδιοκτησίας κ.λπ.

[9] http://www.astynomia.gr , *Διυπηρεσιακή Συνεργασία & παράλληλη δράση* , Ελληνική Αστυνομία, Υπουργείο Δημόσιας Τάξης

ΚΕΦΑΛΑΙΟ 3^0

-ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ-

3.1 **Διαδίκτυο και κοινωνικό περιβάλλον**

Το Διαδίκτυο έχει συντελέσει αποφασιστικά στη δημιουργία νέων μορφών συμπεριφοράς σε όλους τους τομείς της ανθρώπινης ζωής και δραστηριότητας, καθώς παρέχει ποικιλία υπηρεσιών και εργασιών. Οι συναλλαγές, το εμπόριο, η πολιτική, η εκπαίδευση, η δικαιοσύνη, η διασκέδαση και κυρίως η επικοινωνία και η πληροφόρηση έχουν επηρεαστεί ριζικά την τελευταία δεκαετία από τη νέα αυτή πραγματικότητα. Το Διαδίκτυο που ξεκίνησε ως ιδέα, όταν το Υπουργείο Εθνικής Αμύνης των Η.Π.Α. αποφάσισε, στις αρχές της δεκαετίας του 1960, να υιοθετήσει τη λύση ενός δικτύου επικοινωνίας απαλλαγμένου από εξωτερικές παρεμβάσεις και παρεμβολές, ξεκίνησε να χρησιμοποιείται από το ευρύ κοινό, στις αρχές της δεκαετίας του 1990, με την εμφάνιση των πρώτων εμπορικών ISPs (Παροχών Διαδικτυακών Υπηρεσιών) κι έχει σήμερα, σχεδόν μια δεκαπενταετία μετά, καταστεί αναγκαίο συστατικό της πραγματικότητάς μας. Είναι χαρακτηριστικό ότι αυτή τη στιγμή, πάνω από 1 δισεκατομμύριο διακόσιες χιλιάδες χρήστες ηλεκτρονικών υπολογιστών είναι συνδεδεμένοι με το Διαδίκτυο, οι περισσότεροι από τους οποίους (ποσοστό 37%) βρίσκονται στην Ασία. Όσον αφορά στην ελληνική πραγματικότητα, ένα στα δύο νοικοκυριά διαθέτει Η/Υ και ένα στα τέσσερα είναι συνδεδεμένο στο Διαδίκτυο, ενώ από το σύνολο των χρηστών Διαδίκτυο στην Ελλάδα, ποσοστό 42% ανήκει στην ηλικιακή ομάδα των 16 έως 24 ετών.

Παράλληλα όμως με το νέο κοινωνικό περιβάλλον, το Διαδίκτυο δημιούργησε κι ένα νέο περιβάλλον για τη διάπραξη εγκλημάτων. Υποστηρίζεται από πολλούς, ότι το Διαδίκτυο, αφού έχει κατασκευασθεί από ανθρώπους που ανήκουν σε μία συγκεκριμένη κοινωνία, δεν θα μπορούσε παρά να αποτελεί αντανάκλαση της εικόνας που δίνει η κοινωνίας αυτή. Η ανωνυμία, η ταχύτητα και η ευκολία διάπραξης εγκλημάτων στον κυβερνοχώρο, έχουν ως αποτέλεσμα, από τη μία την αύξηση των διαδικτυακά τελουμένων αδικημάτων κι από την άλλη, την μεγέθυνση του σκοτεινού αριθμού της εγκληματικότητας. Βρισκόμαστε λοιπόν, μπροστά σε νέες καταστάσεις, που δεν δύνανται να υπαχθούν στους έως πρότινος

υφιστάμενους γενικούς ποινικούς κανόνες, του ουσιαστικού και δικονομικού ποινικού πεδίου. Η νομοθεσία και η δικαιοσύνη καλούνται να προσαρμοστούν και να προβλέψουν νέους τρόπους πρόληψης και αντιμετώπισης των πρωτότυπων αυτών ανθρωπίνων συμπεριφορών στον καινοφανή χώρο του διαδικτύου, προσεγγίσεις όμως που απαιτούν όχι μόνο νομικές αλλά και τεχνικές γνώσεις σε θέματα Η/Υ και Διαδίκτυο[10].

3.2 **Χαρακτηριστικά ηλεκτρονικού εγκλήματος**

Δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός για το ηλεκτρονικό έγκλημα ούτε στη διεθνή νομοθεσία ούτε στη διεθνή νομολογία. Στην παρούσα εργασία θα προχωρήσουμε σε μία δημιουργική σύνθεση απόψεων με σκοπό την πληρέστερη και πλέον σφαιρική απόπειρα καθορισμού της έννοιας του ηλεκτρονικού εγκλήματος. Ως ηλεκτρονικό έγκλημα λοιπόν[11], αναφερόμαστε σε "*κάθε παράνομη-παραβατική ενέργεια που τελείται μέσω ενός συνδεδεμένου στο Διαδίκτυο υπολογιστή* online. *Ο υπολογιστής μπορεί να έχει χρησιμοποιηθεί για τη διάπραξη ενός εγκλήματος, ή μπορεί να είναι ο στόχος*". Η λέξη Netcrime αναφέρεται σε μια εγκληματική εκμετάλλευση του Διαδικτύου.Τα εγκλήματα στον κυβερνοχώρο ορίζονται ως εξής: «εγκλήματα που διαπράττονται εις βάρος ατόμων ή ομάδων ατόμων με ποινικό κίνητρο να βλάψουν σκόπιμα τη φήμη του θύματος ή αιτία σωματικής ή ψυχικής βλάβης στο θύμα, άμεσα ή έμμεσα, με τη χρήση σύγχρονων τηλεπικοινωνιακών δικτύων, όπως το Διαδίκτυο.

Πρόκειται θα λέγαμε, για μια εγκληματική και παράνομη πράξη προσβολής περιουσιακών ή άλλων δικαιωμάτων φυσικών και νομικών προσώπων που γίνεται μέσω της χρήσης μιας οποιασδήποτε συσκευής ηλεκτρονικής επεξεργασίας δεδομένων. Μέσο τέλεσης της πράξης μπορεί να είναι ένας ηλεκτρονικός υπολογιστής συνδεδεμένος σε ένα δίκτυο επικοινωνιών όπως το Διαδίκτυο ή άλλη τερματική συσκευή, όπως ένα σταθερό ή κινητό τηλέφωνο. Το ηλεκτρονικό έγκλημα, για το οποίο έχουν δοθεί διεθνώς πολλοί ορισμοί (computer crime, cyber -crime, hitechcrime) σε χώρους που χρησιμοποιούνται δίκτυα υπολογιστών.

Τα εγκλήματα αυτά μπορεί να απειλήσουν την ασφάλεια ενός έθνους και την ασφάλεια των συναλλαγών. Θέματα γύρω από αυτό το είδος του εγκλήματος έχουν γίνει υψηλού προφίλ, ιδίως εκείνων των εγκλημάτων που περιλαμβάνουν: παραβίαση δικαιωμάτων

[10] Τσουραμάνης Χ., *«Διαδίκτυο και ποινική δικαιοσύνη: Πορνογραφία και Διαδίκτυο»,* Ποινική Δικαιοσύνη, Τεύχος 4/2002, Νομική Βιβλιοθήκη, σελ. 400.
[11] www.saferinternet.gr, Η επίσημη ιστοσελίδα του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου

πνευματικής ιδιοκτησίας , παιδική πορνογραφία και προσωπικά δεδομένα. Υπάρχουν επίσης προβλήματα προστασίας της ιδιωτικής ζωής , όταν εμπιστευτικές πληροφορίες που έχουν χαθεί ή υποκλαπεί νόμιμα ή με άλλο τρόπο. Σε διεθνές επίπεδο, τόσο κυβερνητικοί όσο και μη κρατικοί παράγοντες ασχολούνται με εγκλήματα στον κυβερνοχώρο, συμπεριλαμβανομένων των: κατασκοπεία, κλοπή και διασυνοριακά εγκλήματα. Περαιτέρω, τα ηλεκτρονικά εγκλήματα ανάλογα με τον τρόπο και το περιβάλλον τέλεσής τους διακρίνονται σε εγκλήματα ηλεκτρονικών υπολογιστών.

3.3 **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.

3.4 **Έργο Δίωξης Ηλεκτρονικού Εγκλήματος**

Τα περιθώρια για να ξεφύγει κάποιος από τη Δίωξη Ηλεκτρονικού Εγκλήματος όταν πρόκειται για το Διαδίκτυο στενεύουν. Και όπως λένε οι άνθρωποι που γνωρίζουν καλά τον κυβερνοχώρο, τα προβλήματα που μπορεί να αντιμετωπίσει κανείς, σερφάροντας, γράφοντας ή συζητώντας σε διάφορους ιστότοπους ή φόρουμ κοινωνικής δικτύωσης δεν λύνονται εύκολα αφού μπορεί ο καθένας να βρεθεί, χωρίς να το γνωρίζει, αντιμέτωπος με τη Δικαιοσύνη. Είναι χαρακτηριστικό ότι εάν κάποιος εκβιάσει, συκοφαντήσει ή απειλήσει τη ζωή κάποιου (και γίνει αναφορά από άλλα άτομα), να βρεθεί αντιμέτωπος με το Νόμο.

«Στο Διαδίκτυο, σύμφωνα με τη γνωμοδότηση του Αρείου Πάγου, δεν υπάρχει απόρρητο», λένε καλά πληροφορημένες πηγές. Κι αυτό σημαίνει ότι εφαρμόζεται η γνωμοδότηση του εισαγγελέα απευθείας προκειμένου να αποδοθούν ευθύνες σε αυτούς για τους οποίους υπάρχουν καταγγελίες. «Από εκεί και πέρα πρέπει να αποδείξει ο κάθε ένας, στην περίπτωση που υπάρχουν καταγγελίες, ότι δεν μιλούσε σοβαρά», συνεχίζουν οι γνώστες

του κυβερνοχώρου.Οι παιδόφιλοι είναι ειδική κατηγορία και πάντοτε είναι στο στόχαστρο των Διωκτικών Αρχών που παρακολουθούν τα διαδικτυακά τους ίχνη και καταγράφουν κάθε κίνησή τους. Όταν δηλαδή, οι αστυνομικοί εντοπίσουν κάποιο περίεργο στοιχείο, κινητοποιούνται προκειμένου να τους πιάσουν. Το ίδιο συμβαίνει και με αντίστοιχες πορνογραφικές ιστοσελίδες, οι οποίες εντοπίζονται από τους αστυνομικούς. Φυσικά, οι καταγγελίες απλών πολιτών που φθάνουν στην Ασφάλεια, βοηθούν το έργο των Αρχών.

Οι Αρχές έχουν φτάσει στην εξιχνίαση αρκετών υποθέσεων χάρη στη βοήθεια των ανθρώπων που κατήγγειλαν τα περιστατικά και χάρη στο έμπειρο δυναμικό της Δίωξης Ηλεκτρονικού Εγκλήματος. Σε κάθε περίπτωση οι ποινές φτάνουν (για πλημμελήματα) μέχρι τα πέντε έτη. Πάντως, οι μη γνωρίζοντες τα δικαιώματά τους στο Διαδίκτυο μπορούν να πέσουν εύκολα θύματα λόγω μίας λάθος ανάρτησης και να έρθουν αντιμέτωποι με τη Δικαιοσύνη.

3.4.1 Κατηγορίες ηλεκτρονικών εγκλημάτων

Τα cyber crimes διακρίνονται σε *α) κοινού ποινικού δικαίου με τη χρήση του διαδικτύου*, σε εγκλήματα δηλαδή που διαπράττονται τόσο σε «κοινό», όσο και σε διαδικτυακό περιβάλλον και β) *γνήσια εγκλήματα του κυβερνοχώρου*, με την έννοια της ποινικοποίησης συμπεριφοράς που έχει σχέση αποκλειστικά με το Διαδίκτυο. Τα δωμάτια ανοιχτής επικοινωνίας, γνωστά και ως chat rooms και τα δίκτυα μέσω των οποίων γίνονται αμοιβαίες ανταλλαγές αρχείων αποτελούν τα κατ' εξοχήν πεδία όπου διαπράττονται ηλεκτρονικά εγκλήματα.

3.4.2 Μορφές Ηλεκτρονικού Εγκλήματος

· *Κακόβουλες εισβολές σε δίκτυα (Hacking και cracking)*

Η χωρίς δικαίωμα πρόσβαση σε ένα δίκτυο υπολογιστών. Όταν ο επιτιθέμενος έχει ως σκοπό να προκαλείσει ζημιά ή να αποκομίσει οικονομικό όφελος αναφέρεται ως hacker ενώ σε αντίθετη περίπτωση ως cracker.

· *Επιθέσεις Άρνησης Εξυπηρέτησης*

Αποσκοπούν στην εξάντληση των πόρων ενός υπολογιστή ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Αυτό συχνά ισοδυναμεί με τη διακοπή λειτουργίας μιας

κρίσιμης υπηρεσίας ή συνόλου υπηρεσιών που προφέρονται από έναν ή περισσότερους διακομιστές, με απρόβλεπτες συνέπειες για την εταιρεία ή τον οργανισμό

· *Κακόβουλο λογισμικό*

Είναι προγράμματα Ηλεκτρονικού Υπολογιστή (Η/Υ) που δημιουργούνται με σκοπό να προκαλέσουν ζημιά σε Η/Υ ή να εισχωρήσουν σε ένα Η/Υ για την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Το κακόβουλο λογισμικό διακρίνεται σε τρεις βασικές κατηγορίες: Ιούς, (viruses), σκουλήκια (worms) και Δούρειους ίππους (Trojan Horses).

· *Ανεπιθύμητη Αλληλογραφία (Spamming)*

Είναι η χρήση οποιοδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων σε πολύ μεγάλες ποσότητες. Αν και ο όρος αναφέρεται, περισσότερο, στην αποστολή μεγάλων ποσοτήτων μηνυμάτων, με διαφημιστικό περιεχόμενο, χρησιμοποιείται, επίσης, για να καταδείξει την αποστολή οποιοδήποτε μηνύματος, το οποίο μπορεί να χαρακτηριστεί ενοχλητικό, από αυτόν που το λαμβάνει.

· *Επιθέσεις σε δικτυακούς τόπους (sites)*

Αποσκοπούν στην αλλοίωση τον περιεχομένου ενός δικτυακού τόπου, κατά τρόπο χιουμουριστικό, προπαγανδιστικό ή και προσβλητικό.

· *Ηλεκτρονικό ψάρεμα (Phising)*

Με το phising ή "ηλεκτρονικό ψάρεμα" επιχειρείται η απόσπαση προσωπικών πληροφοριών του θύματος, όπως ο αριθμός της πιστωτικής του κάρτας, κωδικοί πρόσβασης κλπ. προκειμένου να χρησιμοποιηθούν σ’ άλλες παράνομες δραστηριότητες. Οι επιθέσεις αυτές στηρίζονται στην εξαπάτηση του θύματος με διάφορους τρόπους και μεθόδους όπως π.χ., την αποστολή ενός e-mail με παραπλανητικό περιεχόμενο.

· *Πειρατεία λογισμικού*

Αναφέρεται στην αναπαραγωγή και/ή διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους.

· *Απάτη στο Διαδίκτυο*

Αποτελεί τη ηλεκτρονική έκφανση της συμβατικής μορφής της απάτης. Μπορεί να συντελεστεί με διάφορους τρόπους και μεθόδους. Κυρίως οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά e-mail, αποστέλλοντας Νιγηριανές Επιστολές ή ενημέρωση για κέρδη στο Ισπανικό Λόττο. Επίσης πολλές απάτες πραγματοποιούνται με τη χρήση πιστωτικών καρτών.

· *Κλοπή ταυτότητας*

Η υποκλοπή στοιχείων ταυτότητας ανυποψίαστων ατόμων και η χρήση τους για παράνομες δραστηριότητες.

· *Ξέπλυμα χρήματος*

Η προσπάθεια εξαφάνισης χρήματος που προέρχεται από παράνομες δραστηριότητες . Χαρακτηριστικό παράδειγμα αποτελεί η αγορά μέσω του Διαδικτύου ασυνήθιστα μεγάλων ποσοτήτων αγαθών.

· *Διακίνηση παιδικού πορνογραφικού υλικού*

Αναφέρεται στη διακίνηση παιδικού πορνογραφικού υλικού μέσω του Διαδικτύου που μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή οποιαδήποτε άλλη μορφή πολυμέσων.

· *Διαδικτυακή τρομοκρατία*

Αναφέρεται στη χρήση της τεχνολογίας των ηλεκτρονικών υπολογιστών και δικτύων για την πραγματοποίηση μιας τρομοκρατικής επίθεσης.

· *Επιθέσεις παρενόχλησης (cyberbulling)*

Είναι μια εγκληματική συμπεριφορά όπου ο επιτιθέμενος με τη χρήση ηλεκτρονικών μέσων επικοινωνίας όπως το Διαδίκτυο και τα κινητά τηλέφωνα, εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματά του, για διάφορους λόγους, όπως εκδίκηση, επίλυση προσωπικών διαφορών κ.α.

· *Hackers και Crackers*

Όταν σε οποιαδήποτε ενέργεια, που σχετίζεται με τους ηλεκτρονικούς υπολογιστές και τα δίκτυα, υπεισέρχεται το στοιχείο της εγκληματικής πρόθεσης ο επιτιθέμενος χαρακτηρίζεται ως cracker. Οι crackers είναι hackers που χρησιμοποιούν την γνώση τους για τους

ηλεκτρονικούς υπολογιστές για να αποκομίσουν όφελος για τους ίδιους ή για τους τρίτους. Εκτός από τους όρους hacker και cracker, έχουν κατά καιρούς χρησιμοποιηθεί και άλλοι όροι για να περιγράψουν τους εγκληματίες του Διαδικτύου όπως, hacktivists, vandals και cyberterrorists. Σε όλες αυτές τις περιπτώσεις, αναφερόμαστε στους hackers, που λόγω του συγκεκριμένου τρόπου υλοποίησης των εγκληματικών τους προθέσεων έχουν λάβει και τα ανάλογα προσωνύμια.

Ο όρος hacktivist, αποτελεί το συνδυασμό των λέξεων hacker και activist (ακτιβιστής). Ο γενικότερος όρος hacktivism, αναφέρεται σε μια "ηλεκτρονική απείθεια κατά των αρχών" που πραγματώνεται στον κυβερνοχώρο. Με τον όρο vandals, αναφέρονται οι hackers που εισβάλουν σε δικτυακούς τόπους με μοναδικό σκοπό την τροποποίηση τους κατά τρόπο προπαγανδιστικό, προσβλητικό ή ακόμη και χιουμοριστικό, ανάλογα με το σκοπό που θέλουν να επιτύχουν. Ο όρος cyberterrorist, αναφέρεται σ' αυτούς που χρησιμοποιούν το Διαδίκτυο για την εκπλήρωση τρομοκρατικών επιθέσεων. Ειδικότερα, μετά το χτύπημα της 11ης Σεπτεμβρίου 2001 στον δίδυμους πύργους, ο φόβος για τρομοκρατικές επιθέσεις μέσω του Διαδικτύου είναι ακόμη μεγαλύτερος[12].

3.5 **Ψηφιακές Αποδείξεις**

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 στις παρακάτω κατηγορίες:

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

[12] http://www.astynomia.gr/, Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος

3. Φυσικά αντικείμενα (physical items): Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω τον οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.
4. Γνήσιες ψηφιακές αποδείξεις (original digital evidence): Φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.
5. Διπλότυπες ψηφιακές αποδείξεις (duplicate digital evidence): Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.
6. 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, palmtop, 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.

3.5.1 Δωμάτια ανοιχτής επικοινωνίας (Chat rooms)

Τα chat rooms είναι το πλέον προτιμώμενο μέσο διαδικτυακής επικοινωνίας τόσο για τα παιδιά όσο και για τους ενήλικους, καθώς επιτρέπει τη σύγχρονη επικοινωνία με περισσότερους και άγνωστους χρήστες σε πραγματικό χρόνο[18]. Παράλληλα όμως χρησιμεύει και ως μέσο ανταλλαγής πορνογραφικού υλικού, κυρίως φωτογραφιών και μικρής διάρκειας

ταινιών, συνομιλίας μεταξύ των συλλεκτών παιδικής πορνογραφίας, καθώς και ως τόπος γνωριμίας μεταξύ παιδιών και παιδόφιλων ή παραγωγών τέτοιου υλικού. Τα δωμάτια ανοιχτής επικοινωνίας φέρνουν σε επαφή ανθρώπους με τα ίδια ενδιαφέροντα, στη συγκεκριμένη περίπτωση με το ίδιο πάθος για την παιδική πορνογραφία, οι οποίοι συνομιλούν μεταξύ τους, διακηρύσσουν τον τρόπο ζωής τους, αλληλοδικαιώνονται ως προς τις επιλογές τους, ανταλλάσσουν πληροφορίες και συμβουλές για την αποτροπή αποκάλυψης των δραστηριοτήτων τους και διακινούν σε πραγματικό χρόνο και δωρεάν αποτυπώσεις παιδικής πορνογραφίας[13].

3.6 **Δίκτυα αμοιβαίας ανταλλαγής αρχείων (Peer to peer networks)**

Τα τελευταία πέντε χρόνια έχουν γνωρίσει μεγάλη άνθιση τα δίκτυα αμοιβαίας ανταλλαγής αρχείων, με πρωτοπόρο το Napster και δημοφιλέστερα πλέον τα E-mule, Bearshare, Gnutella, Limewire, Kazaa κ.α. Τα δίκτυα αυτά παρέχουν στους χρήστες τους, μέσω ειδικού προγράμματος τη δυνατότητα να ψάξουν μέσω λέξεων-κλειδιών, τα αρχεία των υπόλοιπων χρηστών του ίδιου προγράμματος και να «κατεβάσουν» (να κάνουν download) οποιοδήποτε αρχείο αυτοί επιθυμούν. Συνήθως, στα πλαίσια της αμοιβαιότητας του προγράμματος, για να κατεβάσει κάποιος ένα αρχείο στον υπολογιστή του οφείλει να έχει κι ο ίδιος αρχεία προς διανομή στον «κοινό φάκελο» (shared folder). Περαιτέρω, τα δίκτυα αυτά παρέχουν στους χρήστες τους τη δυνατότητα να συνομιλήσουν με τον κάτοχο του αρχείου το οποίο επιθυμούν να κατεβάσουν, μέσω προγράμματος άμεσης συνομιλίας (instant messenger program). Στην πλειονότητα των περιπτώσεων τα προγράμματα αυτά χρησιμοποιούνται για το downloading μουσικής σε ψηφιακή μορφή (mp3), εικόνων και κινηματογραφικών ή τηλεοπτικών ταινιών. Δεν είναι λίγες οι φορές όμως που διακινητές ή συλλέκτες παιδικής πορνογραφίας κατεβάζουν με τη βοήθεια των δικτύων αμοιβαίας ανταλλαγής αρχείων πορνογραφικό υλικό σε μορφή εικόνων η ταινιών, απλά με την πληκτρολόγηση της κατάλληλης λέξης-κλειδιού ή επικοινωνούν μεταξύ τους, μέσω ενός συστήματος που λόγω του αποκεντρωμένου του χαρακτήρα, καθιστά πολύ δυσκολότερο τον εντοπισμό των ιχνών τους.

[13] Αγγελόπουλος Δ. - Πάσχος Ι., *Κατάσχεση-Ανάλυση ψηφιακών πειστηρίων*, Ποινική Δικαιοσύνη, *Τεύχος 4/2003*, Νομική Βιβλιοθήκη, σελ. 439.

3.7 **Εγκληματολογικές Προσεγγίσεις**

Στην προσπάθειά ανεύρεσης θεωρητικού υποβάθρου για τα ηλεκτρονικά εγκλήματα αντιμετωπίσαμε αρκετές δυσκολίες, καθώς η πολύ πρόσφατη εμφάνιση του φαινομένου της ηλεκτρονικής εγκληματικότητας και η εξαιρετικά περιορισμένη βιβλιογραφία και θεωρητική ενασχόληση με το θέμα μας οδήγησε σε αδιέξοδο ως προς την θεμελίωση αυτού του είδους εγκλημάτων σε κάποια συγκεκριμένη εγκληματολογική θεωρία[14].

Όσον αφορά στη στάση της Εγκληματολογίας απέναντι στο νέο αυτό φαινόμενο της διαδικτυακής εγκληματικότητας γίνεται πολύς λόγος τα τελευταία χρόνια, ορθά κατά την άποψή μας, για την ανάγκη επαναπροσδιορισμού των στόχων, των θεωρητικών προσεγγίσεων και των μεθοδολογικών της εργαλείων, για να μπορέσει να ανταποκριθεί επιτυχώς στο συνεχώς εξελισσόμενο τεχνολογικά περιβάλλον. Κλείνοντας, λοιπόν, θα παραθέσουμε κάποιες απόψεις που διατυπώνει ο Ronald V.Clarke, θιασώτης της παραπάνω γνώμης, σε άρθρο του[15].

«Στην εγκληματολογία του μέλλοντος, η καταφυγή των εγκληματολόγων στο δίκαιο, την ψυχολογία και την κοινωνιολογία, πρέπει να πάψει να αποτελεί την πηγή της αυθεντίας και του κύρους της. Αυτό σημαίνει ότι η εγκληματολογία οφείλει να ετοιμαστεί να εγκαταλείψει τις θεωρίες, που για δεκαετίες υπήρξαν το “μεσοδόκι” της. Συγκεκριμένα, οι εγκληματολόγοι οφείλουν[34] να υποβαθμίσουν τη σημασία των θεωριών που προσδιορίζουν το έγκλημα ως το αποτέλεσμα μειονεξιών. Επειδή η εγκληματικότητα συνεχίζει να αυξάνει παρά την αύξηση του εισοδήματος και τη βελτίωση των υπολοίπων κοινωνικών δεικτών, οι θεωρίες αυτές έχουν χάσει την αξιοπιστία τους. Σε καμία περίπτωση δεν μπορούν να εξηγήσουν τα εγκλήματα που τελούνται στο Διαδίκτυο, τα οποία σπάνια διαπράττονται από μειονεκτούντες παραβάτες[16]. Περισσότερο θα βοηθούσε στην αντιεγκληματική πολιτική η «εγκληματολογία της καθημερινής ζωής».

Επιπλέον, για τον σχεδιασμό αποτελεσματικών πολιτικών οι εγκληματολόγοι οφείλουν να αναζητήσουν τη βοήθεια αρχών, τις οποίες είχαν παλαιότερα αποκηρύξει, με

---

[14] Ζάνη Α., ***Media*** *και έγκλημα: Το διαδικτυακό έγκλημα,* Αντ. Ν. Σάκκουλα, Αθήνα 2005, σελ 49-57

[15] Clarke R.V. «Technology, Criminology and Crime Science», ***European Journal on criminal Policy and Research, Vol 10,*** Kluwer Academic Publishers 2004, σελ 58.

[16] Αγγελής Ι., «Διαδίκτυο και ποινικό δίκαιο», *Έγκλημα στον κυβερνοχώρο* ***(Cybercrime-*** *Διαδίκτυο* ***Crime****),* ***Ν/2000,*** σελ. 667-668 και Δ. Αγγελόπουλος - Ι. Πάσχος, *Κατάσχεση - Ανάλυση ψηφιακών πειστηρίων*, Ποινική Δικαιοσύνη Τεύχος 4/2003 σελ. 439.

προφανέστερες τα οικονομικά, τη βιολογία, τη δημογραφία, τη γεωγραφία και τον πολεοδομικό σχεδιασμό. Σε ένα περιβάλλον διαρκώς εξελισσόμενο τεχνολογικά, οφείλουν να επικουρούνται εξάλλου από επιστήμονες και μηχανικούς.Τα περισσότερα εγκληματολογικά σχόλια σχετικά με το Διαδίκτυο, ήταν προκατειλημμένα σχετικά με την «απαγορευτική», για τους φτωχότερους ανθρώπους, διάπραξη εγκλήματος, διότι αυτοί δεν μπορούν να αντέξουν το κόστος ενός υπολογιστή. Τα περισσότερα από αυτά τα σχόλια όμως, παρέβλεψαν το γεγονός πως το Διαδίκτυο προσέφερε πληθώρα νέων ευκαιριών για τη διάπραξη εγκλήματος και δεν ανέφεραν την άμεση ανάγκη να βρεθούν τρόποι για την πρόληψη του εγκλήματος αυτού.»

3.8 **Εμπόδια αντιμετώπισης ηλεκτρονικών εγκλημάτων**

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

Η διερεύνηση των ηλεκτρονικών και διαδικτυακών εγκλημάτων άλλωστε, είναι αρκετά δύσκολη και ιδιαίτερα χρονοβόρος, καθώς για τον εντοπισμό των «ηλεκτρονικών ιχνών» η έρευνα μπορεί να διαρκέσει από ένα μήνα έως και δύο χρόνια. Αυτό συμβαίνει διότι οι διερευνώμενοι χρήστες του Διαδίκτυο λαμβάνουν μέτρα προστασίας, τα οποία καθιστούν τον εντοπισμό τους ιδιαίτερα δύσκολο. Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του «ηλεκτρονικού ίχνους» του δράστη, το οποίο για κάθε χρήστη του Διαδίκτυο είναι μοναδικό και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Η λεγομένη ηλεκτρονική απόδειξη (electronic evidence) ωστόσο, δεν ταυτίζεται με τα παραδοσιακά αποδεικτικά μέσα. Κυριότερες πηγές ψηφιακών αποδείξεων αποτελούν:

α. *Ο υπολογιστής του παραβάτη*, στον σκληρό δίσκο του οποίου συνήθως ανευρίσκονται αποθηκευμένες πορνογραφικές αναπαραστάσεις ή αποκαλύπτονται με τη βοήθεια εξειδικευμένων τεχνικών αρχεία και στοιχεία κρυφά ή αόρατα με γυμνό μάτι, όπως η ημερομηνία, η ώρα και η διάρκεια περιήγησης στο Διαδίκτυο, οι ιστοσελίδες που ο παραβάτης επισκέφθηκε, με ποιους συνομίλησε κ.α.

β. *Βοηθητικές συσκευές*, οι οποίες χρησιμοποιούνται παράλληλα με τον Η/Υ όπως ψηφιακές κάμερες, φωτογραφικές μηχανές και κινητά τηλέφωνα, συσκευές στις κάρτες μνήμης των οποίων καταγράφονται οι παράνομες δραστηριότητες κι από τις οποίες συνήθως γίνεται uploading στο Διαδίκτυο.

γ. *Παροχείς υπηρεσιών διαδικτύου*, οι οποίοι δίδουν πληροφορίες και με τη βοήθεια των οποίων καθίσταται δυνατός ο εντοπισμός χρηστών μέσω ενός μοναδικού για κάθε χρήστη ψηφιακού αριθμού ταυτότητας, του IP, ο οποίος εκτός από τα προσωπικά στοιχεία του ιδιοκτήτη του όνομα διεύθυνση κλπ, δίδει πληροφορίες για τις ιστοσελίδες και τα αρχεία τα οποία επισκέφθηκε.

δ. ***Online*** *δραστηριότητα.* Οι μηχανές διαδικτυακής αναζήτησης επιτρέπουν στις διωκτικές αρχές την καταγραφή της διαδικτυακής δραστηριότητας όπως αυτή αποκαλύπτεται μέσω του προσωπικού IP αριθμού τους.

Αλλά και μετά τη συλλογή των αποδεικτικών στοιχείων τίθεται το πρόβλημα της διατήρησής τους, καθώς αν δεν φυλαχθούν υπό τις κατάλληλες συνθήκες, ήτοι μακριά από σκόνη, υγρασία, ήλιο κ.λ.π. μπορεί να καταστραφούν κι επομένως να μη είναι δυνατή η περαιτέρω χρησιμοποίηση και αξιολόγησή τους[17].

Όλες οι παραπάνω δυσχέρειες εντοπισμού, ελέγχου και επιτυχούς αντιμετώπισης των κυβερνοεγκλημάτων, εντείνονται από την συνεχή πρόοδο και τελειοποίηση των τεχνικών μέσων και μεθόδων των διαδικτυακών εγκληματιών, στις οποίες αντιπαρατίθενται η συχνή έλλειψη εξειδικευμένης τεχνογνωσίας και σύγχρονης τεχνολογίας των διωκτικών αρχών αλλά και η έλλειψη στοιχειωδών τεχνικών γνώσεων Η/Υ και διαδικτύου από τις Δικαστικές αρχές. Η «Επιτροπή πρόβλεψης και πρόληψης εγκλήματος» (Foresight Crime Prevention Panel) μάλιστα, με βάση ειδική έρευνα που έγινε στη Μ. Βρετανία, οδηγήθηκε στην διαπίστωση ότι

[17] Αγγελής Ι., *Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης*, Ποινική Δικαιοσύνη Τεύχος 8-9/2005, σελ. 1063.

το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια την λειτουργία των συστημάτων ασφαλείας και των τεχνικών αναγνώρισης και θα μπορούν να ξεπεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο[18].

3.9 **Συνέπειες ηλεκτρονικού εγκλήματος**

Οι δυσμενείς κοινωνικές και οικονομικές συνέπειες του ηλεκτρονικού εγκλήματος είναι πολλαπλές για τους πολίτες, ιδιαίτερα δε τους ανηλίκους. Καθημερινά σχεδόν γίνεται λόγος στα ελληνικά και διεθνή ΜΜΕ για περιπτώσεις σεξουαλικής εκμετάλλευσης παιδιών και εφήβων που προσελκύονται μέσω φόρουμ συζήτησης του διαδικτύου και καταλήγουν να υφίστανται σοβαρές προσβολές της προσωπικότητας, της τιμής, της γενετήσιας αξιοπρέπειας, ακόμα και της ζωής τους. Η παρότρυνση των καταναλωτών, μέσω παραπλανητικών διαφημίσεων και απαγορευμένων εμπορικών πρακτικών, ήτοι αποστολής, χωρίς τη συναίνεση του χρήστη, ανεπιθύμητων μηνυμάτων (γνωστών ως spam) να αγοράσουν άγνωστης προέλευσης, διατροφικής αξίας και αμφίβολης ποιότητας προϊόντων και υπηρεσιών, μπορεί να βλάψει την υγεία, την ασφάλεια και την οικονομικά συμφέροντα των καταναλωτών. Η αθέμιτη πρόσβαση τρίτων εισβολέων σε κωδικούς τραπεζικών λογαριασμών μέσω web banking συνεπάγεται την υπεξαίρεση των ποσών των καταθέσεων και τη μεταφορά αποταμιευτικών κεφαλαίων του καταναλωτή τράπεζες του εξωτερικού και στη συνέχεια στις τσέπες των εγκληματιών. Η υποκλοπή μέσω διαδικτύου στοιχείων πιστωτικών καρτών των γονέων παιδιών και εφήβων έχει ως συνέπεια την αθέμιτη χρέωση των γονέων, της οποία όμως οι γονείς ανακαλύπτουν πολύ αργότερα μαζί με το εκκαθαριστικό του λογαριασμού που λαμβάνουν από την τράπεζα.

Είναι γεγονός ότι ο κάτοχος της κάρτας, βάσει της νομοθεσίας, μπορεί να αρνηθεί τη χρέωση οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί χωρίς την παρουσίαση του φυσικού σώματος της κάρτας. Συνεπώς, σε περίπτωση on line συναλλαγής με κλεμμένα στοιχεία καρτών, ο νόμιμος κάτοχος μπορεί να αρνηθεί την καταβολή του αντιτίμου, οπότε η τράπεζα κανονικά δεν θα καταβάλει το ποσό στον πωλητή αλλά κανονικά θα χρεώσει το κατάστημα με τα έξοδα ακύρωσης της συναλλαγής. Η συλλογή στοιχείων επικοινωνίας και προσωπικών δεδομένων των χρηστών, τα οποία χρησιμοποιούνται συχνά χωρίς τη συναίνεση των υποκειμένων, είτε από τους ίδιους τους προμηθευτές είτε διαβιβάζονται έναντι αντιτίμου σε

[18] Αγγελόπουλος Δ.-. Πάσχος Ι, *Κατάσχεση - Ανάλυση ψηφιακών πειστηρίων*, Ποινική Δικαιοσύνη, Τεύχος 4/2003 σελ. 441-442.

τρίτους για προωθητικές ενέργειες μέσω αποστολής μαζικών SMS και MMS, έρευνες αγοράς, direct marketing, απαγορεύεται από τη νομοθεσία καθότι προσβάλλει την ιδιωτική ζωή του ατόμου[19].

[19] «Ενημέρωση του Καταναλωτή για την προστασία από το ηλεκτρονικό έγκλημα»,Συνήγορος καταναλωτή, 2009

ΚΕΦΑΛΑΙΟ 4^0

-ΑΝΤΙΜΕΤΩΠΙΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ-

4.1 **Προβληματισμοί ως προς την εφαρμογή δικαίου και τη δικαιοδοσία των δικαστηρίων**

Όπως είδαμε το έγκλημα που διαπράττεται στον κυβερνοχώρο δεν γνωρίζει γεωγραφικά σύνορα, καθώς το αντικείμενο μπορεί να εντοπίζεται σε πολλούς υπολογιστές, οι οποίοι μάλιστα βρίσκονται σε διαφορετικές χώρες. Το πρόβλημα της εφαρμογής δικαίου, ήτοι το ερώτημα ποιο δίκαιο θα ισχύσει σε κάθε περίπτωση, είναι ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζουν οι διωκτικές αρχές κατά την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο, δεδομένου ότι η ίδια αξιόποινη πράξη μπορεί να διαπράττεται ταυτόχρονα σε εκατοντάδες ή ακόμη και χιλιάδες τόπους τελέσεως.

Το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη απ' όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της δικαιοδοσίας και κατ' επέκταση της αρμοδιότητας του δικαστηρίου είναι απαραίτητο να καθοριστεί ο τόπος τελέσεως του αδικήματος. Για τον καθορισμό του τόπου τελέσεως της αξιόποινης πράξης υποστηρίζονται τέσσερις διαφορετικές θεωρίες:

I. *Η θεωρία του τόπου ενέργειας*, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θεωρείται ο τόπος όπου τελέστηκε η ενέργεια, που έτεινε στο άδικο αποτέλεσμα, κι αν η ενέργεια έλαβε χώρα σε περισσότερα του ενός κράτη, ο τόπος όπου αυτή ολοκληρώθηκε.

II. *Η θεωρία του τόπου του αποτελέσματος*, σύμφωνα με την οποία ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

III. Η μικτή θεωρία, όπου ως τόπος τελέσεως της αξιόποινης πράξης θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος, με δικαίωμα επιλογής του παθόντος.

IV. Η θεωρία του βαρύνοντος τόπου, κατά την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Πολλές φορές ανακύπτουν εμπόδια κατά την εφαρμογή της εν λόγω θεωρίας, καθότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. Η τελευταία αυτή θεωρία είναι και η κρατούσα στην Ευρώπη και στη χώρα μας[20].

Δυσκολίες από τα χαρακτηριστικά του διαδικτυακού εγκλήματος δεν προκύπτουν μονάχα κατά τη διερεύνηση του, αλλά και μετά την εξιχνίασή των κυβερνοεγκλημάτων, κατά το στάδιο της απονομής της δικαιοσύνης. Το πρώτο σοβαρό πρόβλημα, το οποίο αντιμετωπίζει ιδιαίτερα ο Έλληνας νομικός- Δικαστής, Εισαγγελέας αλλά και Δικηγόρος- είναι η έλλειψη βασικών τεχνικών γνώσεων σε θέματα Η/Υ και διαδικτύου, οι οποίες μαζί με τις νομικές γνώσεις είναι απαραίτητες για την προσέγγιση των θεμάτων που αφορούν το ηλεκτρονικό και διαδικτυακό έγκλημα. Πρόβλημα συνιστά και η έλλειψη επαρκούς βιβλιογραφίας, αρθρογραφίας και νομολογίας σχετικά με την ποινική αντιμετώπιση της νέας αυτής μορφής εγκλήματος, ενώ τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι ως επί το πλείστον, διατυπωμένη στην αγγλική γλώσσα και η μεταφορά των όρων αυτών στην ελληνική δεν είναι ούτε εύκολη, ούτε δόκιμη.

Εξάλλου κατά την άσκηση της ποινικής δίωξης, λόγω της έλλειψης εξειδικευμένων γνώσεων από μεριάς του Εισαγγελέα, δεν είναι σπάνιες οι περιπτώσεις, όπου για τα ίδια πραγματικά περιστατικά ασκείται διαφορετική ποινική δίωξη, η οποία δύναται να οδηγήσει σε εσφαλμένη δικαστική απόφαση. Τέλος, κατά το στάδιο της ακροαματικής διαδικασίας, η έλλειψη των τεχνικών αυτών γνώσεων από μέρους των δικαστών καθιστά σημαντικότατες και ιδιαιτέρως βαρύνουσες τις πραγματογνωμοσύνες και τις καταθέσεις μαρτύρων με εξειδικευμένες γνώσεις, τόσο για την εκτίμηση των αποδεικτικών μέσων, όσο και για την έκδοση των αποφάσεων. Με τον τρόπο αυτό, καθίσταται εμφανής ο κίνδυνος έκδοσης δικαστικών αποφάσεων τυπικά μεν από τους Δικαστές, ουσιαστικά όμως από τους μάρτυρες και τους πραγματογνώμονες ή ελλοχεύει ο κίνδυνος έκδοσης λανθασμένων δικαστικών

[20] Κιούπης Δ., *Ποινικό δίκαιο και Διαδίκτυο*, σειρά *Ποινικά, No 57, 75.*

αποφάσεων, λόγω μη κατανόησης των εξειδικευμένων θεμάτων από το δικαστήριο, για την οποία απαιτούνται έστω και οι βασικές γνώσεις της σύγχρονης τεχνολογίας.

4.2 **Αποτροπή αυτοκτονιών από την Δ.Η.Ε**

. Η Δίωξη Ηλεκτρονικού Εγκλήματος έχει αποτρέψει 301 αυτοκτονίες από το 2006 ενώ το 2011 οι απόπειρες αυξήθηκαν κατά 150% σε σχέση με πέρυσι. Το 55% είναι ανήλικοι και το 45% είναι ενήλικοι. : «Μέσα από την ανωνυμία κάποιοι γράφουν ¨εγώ θέλω να δώσω τέλος στην ζωή μου¨. Έτσι, είτε το βλέπει η υπηρεσία σε κοινή θέα στα chat rooms είτε ειδοποιεί ένας τρίτος που έχει δει την συνομιλία. Με την σειρά της η Δ.Η.Ε κάνει ανάλυση και μιλά απευθείας με το facebook (από τις δέκα αυτοκτονίες, οι οκτώ είναι στο facebook). Έχει χτιστεί προσωπική σχέση Ελλάδα Αμερική με την αρμόδια εταιρία του facebook και μέσα σε οκτώ λεπτά υπάρχει ανταπόκριση», δηλώνει ο κ. Σφακιανάκης, προϊστάμενος της Δ.Η.Ε.

Ενημερώνεται ο προϊστάμενος της εισαγγελίας ο οποίος δίνει εντολή στον πάροχο που ανήκει το ίχνος και ο πάροχος αμέσως δίνει το όνομα και την διεύθυνση του ανθρώπου που προσπαθεί να αυτοκτονήσει. «Έχουμε σπάσει πόρτες σε σπίτια και έχουμε βρει ανθρώπους σε εξαθλιωμένη κατάσταση με κομμένες φλέβες, ημιθανείς, άνθρωπο με την ζώνη κρεμασμένο και ανθρώπους που έχουν καταπιεί πολλά χάπια» , δηλώνει ο προϊστάμενος της Δ.Η.Ε.

Σε μια χώρα όπως η Ελλάδα, όπου η πλειοψηφία του πληθυσμού δυσκολεύεται ακόμα να εξοικειωθεί με τον ομολογουμένως χαώδη κόσμο του Διαδικτύου, το πιο αποτελεσματικό και αποδοτικό τμήμα της Αστυνομίας να είναι εκείνο το οποίο ασχολείται με το διαδικτυακό έγκλημα σε κάθε μορφή του. Hackers, Crackers, εκβιαστές, παιδόφιλοι και πάσης φύσεως, Διαδικτυακοί «απατεώνες». Παρακάτω αναφέρουμε τα βασικότερα τμήματα της Δ.Η.Ε που ασχολούνται με τέτοιου είδους θέματα.

-Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων, το οποίο είναι αρμόδιο για τη συνεχή έρευνα του διαδικτύου και των άλλων μέσων ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης προς ανακάλυψη, εξιχνίαση και δίωξη των

εγκληματικών πράξεων που διαπράττονται σ’ αυτά ή μέσω αυτών σε ολόκληρη τη χώρα, πλην αυτών που προβλέπονται στη περίπτωση β΄ του παρόντος άρθρου.

- Τμήμα Προστασίας Ανηλίκων, το οποίο είναι αρμόδιο για την εξιχνίαση και δίωξη των εγκλημάτων που διαπράττονται κατά των ανηλίκων με τη χρήση του διαδικτύου και των άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.

- Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, το οποίο είναι αρμόδιο για το χειρισμό υποθέσεων παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων, που τελούνται σε ολόκληρη τη χώρα, καθώς και για την παροχή συνδρομής σε άλλες αρμόδιες υπηρεσίες που διερευνούν τις υποθέσεις αυτές, κατά την ισχύουσα νομοθεσία.

- Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών, το οποίο λειτουργεί σύμφωνα με τις διατάξεις της 7001/2/1261−κα από 28−8−2009 κοινής υπουργικής απόφασης των Υπουργών Εσωτερικών, Οικονομίας και Οικονομικών και Δικαιοσύνης (Β΄ 1879).

4.3 **Εγκληματικότητα στο ελληνικό Διαδίκτυο**

Όντας μικρογραφία της κοινωνίας, το Διαδίκτυο δεν αποτελεί σε καμία περίπτωση έναν ασφαλή, «αγγελικά πλασμένο» κόσμο. Η εγκληματικότητα στο Διαδίκτυο στην Ελλάδα είναι πολύ σοβαρή. Μέχρι στιγμής οι πιο συνηθισμένες περιπτώσεις που εξιχνιάζονται είναι η παιδική πορνογραφία, τα εγκλήματα περί τα ήθη, οι hackers , οικονομικά εγκλήματα με πιστωτικές κάρτες και εγκλήματα δορυφορικής πειρατείας

Χαρακτηριστικό παράδειγμα, η σχετικά πρόσφατη επιχείρηση «Butterfly», η οποία πραγματοποιήθηκε σε αρκετές πόλεις της Ελλάδας, για την καταπολέμηση του φαινομένου της παιδικής πορνογραφίας μέσω διαδικτύου. Κατηγορήθηκαν συνολικά για διακίνηση παιδικού πορνογραφικού υλικού δεκαπέντε άτομα υπεράνω πάσης υποψίας, εκ των οποίων έντεκα συνελήφθησαν στο πλαίσιο της αυτόφωρης διαδικασίας. Μάλιστα, είναι εντυπωσιακό το γεγονός ότι για συμμετοχή σε κυκλώματα διακίνησης παιδικής πορνογραφίας έχουν γίνει, από το 2004 έως σήμερα, παραπάνω από 700 συλλήψεις στην χώρα μας.

Τι γίνεται όμως, με το παράνομο κατέβασμα αρχείων ή «πειρατεία» όπως χαρακτηρίζεται διεθνώς; Κινδυνεύουν όσοι απλά κατεβάζουν αρχεία για ιδία χρήση**;** Ποιες είναι οι ενέργειες στις οποίες μπορεί να προβεί το Τμήμα Δ.Η.Ε; Το παράνομο downloading ερευνάται είτε μετά από σχετική καταγγελία, είτε μέσα από δική μας έρευνα στο Διαδίκτυο. Είναι ένα μεγάλο κομμάτι το οποίο απασχολεί πολύ την Δ.Η.Ε και κατά καιρούς έχουν εντοπιστεί και συλληφθεί άτομα τα οποία εμπορεύονται τα πνευματικά δικαιώματα τρίτων. Μέχρι στιγμής πάντως, δεν έχει συλληφθεί κάποιος απλά και μόνο επειδή κατέβασε παράνομα κάποιο αρχείο στον υπολογιστή του σύμφωνα με την ελληνική Δ.Η.Ε.

Ένας άλλος τομέας στον οποίο δραστηριοποιείται το τμήμα είναι αυτός των αυτοκτονιών**.** Χρησιμοποιώντας σύγχρονα τεχνολογικά μέσα, η υπηρεσία εντόπισε με ψηφιακές έρευνες στο Διαδίκτυο περισσότερους από τριακόσιους ανθρώπους που εκδήλωσαν πρόθεση να βάλουν τέλος στη ζωή τους και προχώρησε άμεσα στις απαραίτητες αστυνομικές ενέργειες για την αποτροπή. Μάλιστα, το 2011, οι απόπειρες αυτοκτονίας αυξήθηκαν κατά 150%, ενώ σύμφωνα με τα στοιχεία του Τμήματος περισσότεροι από τους μισούς που σκέφτονταν την αυτοκτονία ήταν ανήλικοι.

Μέσω τις Διεύθυνσης IP**,** του ηλεκτρονικού αποτυπώματος δηλαδή που έχει ο υπολογιστής ο οποίος συνδέεται στο Διαδίκτυο και το οποίο είναι μοναδικό στον κόσμο, εντοπίζονται όλα τα περιστατικά. Το ηλεκτρονικό αυτό ίχνος δίνεται από τον εκάστοτε πάροχο (otenet, forthnet κτλ.) και σε περιπτώσεις που διαπιστωθεί παράνομη δραστηριότητα, τότε εφαρμόζεται η νομική διαδικασία της άρσης απορρήτου, ώστε το Τμήμα να λάβει τα απαραίτητα στοιχεία όσων παρανομούν από τους τηλεπικοινωνιακούς παρόχους τους[21].

4.4 **Δράσεις του σώματος Δ.Η.Ε**

«Είμαστε στο εμείς και όχι στο εγώ». Αυτό είναι το μότο της Δίωξης Ηλεκτρονικού Εγκλήματος. Με το σύνθημα αυτό αλλά και με την εμπειρία του προϊστάμενου της υπηρεσίας Μανώλη Σφακιανάκη εκπαιδεύονται όλοι οι νέοι που μπαίνουν στην υπηρεσία. Η Δίωξη Ηλεκτρονικού Εγκλήματος έχει τον πιο προηγμένο εξοπλισμό ενώ η υπηρεσία έχει πιστοποιηθεί με ISO 2001.

[21] Δίωξη Ηλεκτρονικού Εγκλήματος: *Οι… Sherlock Holmes του Διαδικτύου*, Γεωργιακώδης Νικόλα0ς, 2/2012

«Όλος ο ποινικός κώδικας έχει μεταφερθεί στο Διαδίκτυο. Η παιδική πορνογραφία, το cyberbullying , τα παράνομα τυχερά παιχνίδια, ο τζόγος, η παραβίαση προσωπικών δεδομένων στο facebook, στο hi5, το cracking και το hacking. Μέχρι στιγμής στην Ελλάδα δεν έχει διαπιστωθεί παραγωγή υλικού παιδικής πορνογραφίας. Η Δίωξη Ηλεκτρονικού Εγκλήματος σε συνεργασία με τον εισαγγελέα Ηλεκτρονικού Εγκλήματος κ. Δραγάτση έχουν καταφέρει να εντοπίσουν τα ηλεκτρονικά ίχνη, να συλλάβουν και να οδηγήσουν στην δικαιοσύνη 695 παιδόφιλους.

Ανθίζουν τα οικονομικά εγκλήματα λόγω της οικονομικής ύφεσης. Οι απάτες και οι αρπαγές χρημάτων μέσω Διαδικτύου μαστίζουν την ελληνική κοινωνία και είναι υποθέσεις που «πονοκεφαλιάζουν» την Δίωξη Ηλεκτρονικού Εγκλήματος. Ύστερα από μεγάλη έρευνα εντοπίστηκε τον Ιανουάριο του 2011 το μεγάλο οικονομικό έγκλημα που γίνεται μέσω τραπεζών. Σύμφωνα με τον προϊστάμενο της Δ.Η.Ε ο κόσμος ακούει μόνο τα αρνητικά αλλά το Διαδίκτυο έχει χιλιάδες θετικά και οι κακοτοπιές του είναι ελάχιστες. Αυτό αποδεικνύεται και από μια πρόσφατη έρευνα, στην οποία αναφέρεται ότι το Διαδίκτυο κατά 98% έχει θετικά αποτελέσματα και μόνο το 2% επιφέρει επιπτώσεις.

Επιπλέον η Δ.Η.Ε ενθαρρύνουν τους γονείς να αφήνουν τα παιδιά τους να σερφάρουν από μικρή ηλικία στο Διαδίκτυο καθώς εάν ένα παιδί θωρακιστεί από τα πέντε του, στην εφηβεία του θα σερφάρει στα καλά μονοπάτια του Διαδικτύου. Αυτός είναι και ο στόχος της Δίωξης Ηλεκτρονικού Εγκλήματος, του υπουργείου Προστασίας του Πολίτη και του Αρχηγείου . Στην υπηρεσία Δ.Η.Ε υπάρχει μια ομάδα καινοτόμων δράσεων που αποτελείται από αξιωματικούς επιστήμονες και διοργανώνονται ημερίδες σε όλη την Ελλάδα προκειμένου να ενημερωθεί ο κόσμος πως θα αποφύγει τις διαδικτυακές κακοτοπιές.

4.5 **Α.Δ.Α.Ε (Αρχή Διασφάλισης Απορρήτου Επικοινωνιών)**

Με το άρθρο 1 του νόμου 3115/2003 συστάθηκε, σύμφωνα με την παράγραφο 2 του άρθρου 19 του Συντάγματος, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών

περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Η ΑΔΑΕ είναι Ανεξάρτητη Αρχή που απολαύει διοικητικής αυτοτέλειας. Έδρα της είναι η Αθήνα, μπορεί όμως με απόφασή της να εγκαθιστά και να λειτουργεί γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της ΑΔΑΕ κοινοποιούνται με μέριμνά της στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους υποβάλλεται Έκθεση των πεπραγμένων της στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο. Η ΑΔΑΕ υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον Κανονισμό της Βουλής.

Η Διεύθυνση Πληροφορικής του Αρχηγείου της Ελληνικής Αστυνομίας έχει ως αποστολή το σχεδιασμό μηχανογραφημένων πληροφοριακών συστημάτων, τη δημιουργία και υποστήριξη της κατάλληλης τεχνικής και λειτουργικής υποδομής και των αναγκαίων εφαρμογών πληροφορικής για την υποβοήθηση του έργου των Υπηρεσιών της Ελληνικής Αστυνομίας.

Επιπλέον, στη Διεύθυνση Πληροφορικής του Αρχηγείου της Ελληνικής Αστυνομίας λειτουργεί το Πληροφοριακό Σύστημα Schengen, ενώ παρέχεται τεχνική υποστήριξη στο διαδικτυακό κόμβο του Υπουργείου Προστασίας του Πολίτη και στα αυτόνομα Πληροφοριακά Συστήματα Europol, Interpol, Eurodac κ.λπ., που λειτουργούν στα πλαίσια της Ευρωπαϊκής Ένωσης για την εκπλήρωση υποχρεώσεων της Χώρας μας, που απορρέουν από Διεθνείς Συμβάσεις.

Διαθέτει ένα σύγχρονο Πανελλαδικό Δίκτυο Πληροφορικής, το οποίο πρόσφατα (Έτος 2007), πύκνωσε και επεκτάθηκε στο σύνολο των Αστυνομικών Υπηρεσιών της Χώρας επιπέδου Αστυνομικού Τμήματος και άνω, με το έργο «Συμμετοχή της Ελληνικής Αστυνομίας στον εκσυγχρονισμό της Δημόσιας Διοίκησης με τη χρήση Πληροφορικής (Police On Line)».

Το έργο «Συμμετοχή της Ελληνικής Αστυνομίας στον εκσυγχρονισμό της Δημόσιας Διοίκησης με τη χρήση Πληροφορικής (Police On Line)» υλοποιήθηκε στα πλαίσια του Γ΄

Κοινοτικού Πλαισίου Στήριξης, με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης (80% από Ε.Τ.Π.Α. και 20% από Εθνικούς Πόρους) και ανάθεσή του, με Προγραμματική Συμφωνία, στην εταιρεία «Κοινωνία της Πληροφορίας Α.Ε.».

Στο προαναφερόμενο Δίκτυο λειτουργούν διάφορες Επιχειρησιακές, Διοικητικές και Οικονομικές μηχανογραφικές εφαρμογές για την υποστήριξη όλων των δραστηριοτήτων των Υπηρεσιών της Ελληνικής Αστυνομίας.

Πλέον αυτών και στα πλαίσια του έργου Police On Line αναπτύσσονται μηχανογραφικές εφαρμογές και ηλεκτρονικές εξυπηρετήσεις, με στόχο τη βελτίωση των παρεχόμενων υπηρεσιών στον Πολίτη, την αμεσότερη, ταχύτερη και καλύτερη εξυπηρέτησή του, την άμεση πρόσβασή του στην πληροφόρηση, την καταπολέμηση της γραφειοκρατίας, την αποτελεσματικότερη λειτουργία των Υπηρεσιών της Ελληνικής Αστυνομίας, την αύξηση της παραγωγικότητάς τους , την προαγωγή των σχέσεών της με τους πολίτες και τη συνολική αναβάθμιση του παραγόμενου έργου της.

4.6 **Τρόποι αντιμετώπισης ηλεκτρονικών εγκλημάτων**

Οι κυριότερες αυτορρυθμιστικές στρατηγικές των παροχέων είναι:

α. Η απομάκρυνση των παράνομων ιστοσελίδων. Πολλοί παροχείς κατά τη σύναψη σχετικής συμφωνίας με κάποιον πελάτη, θέτουν περιορισμούς ως προς τη νομιμότητα του περιεχομένου της ιστοσελίδας, την οποία θα φιλοξενήσουν, ενώ μεγάλος αριθμός ενώσεων παροχέων διαδικτυακών υπηρεσιών υποχρεώνουν τα μέλη τους να μην δέχονται παράνομο υλικό στις ιστοσελίδες που φιλοξενούν ή να το απομακρύνουν μόλις αντιληφθούν την ύπαρξή του. Για τον εντοπισμό παράνομου περιεχομένου μάλιστα, κάποιοι ISP διαθέτουν ειδικές υπηρεσίες κυβερνο-περιπολίας, οι οποίες αναζητούν, εντοπίζουν και απομακρύνουν τις σχετικές ιστοσελίδες.

β. Θέσπιση ανοικτών γραμμών και ιστοσελίδων καταγγελιών. Κάποιοι παροχείς έχουν θέσει σε λειτουργία ιστοσελίδες ή ανοικτές γραμμές καταγγελιών, στις οποίες οι χρήστες του διαδικτύου μπορούν να αναφέρουν ιστοσελίδες με παράνομο περιεχόμενο, καταγγελίες τις οποίες οι παροχείς προωθούν στη συνέχεια στις αρμόδιες αρχές.

γ. Φιλτράρισμα μηχανών αναζήτησης. Οι ISP δύνανται να εφαρμόσουν φίλτρα στις μηχανές αναζήτησης, τις οποίες χρησιμοποιούν οι πελάτες τους για τον εντοπισμό κάποιας ιστοσελίδας, ώστε στα αποτελέσματα αναζήτησης να μην περιλαμβάνονται sites με παράνομο περιεχόμενο.

δ. Ειδοποίηση και συνεργασία με αρχές. Οι παροχείς υπηρεσιών Διαδίκτυο προκειμένου να συμβάλλουν ενεργά στην αντιμετώπιση του φαινομένου, πέραν της ειδοποίησης των διωκτικών αρχών για την ύπαρξη ενδεχόμενου παράνομου υλικού σε ιστοσελίδες που φιλοξενούν, οφείλουν να διατηρούν τις ψηφιακές αποδείξεις για όσο χρονικό διάστημα απαιτείται, να παραδίδουν τις αποδείξεις αυτές όταν τους ζητηθεί και γενικότερα να διευκολύνουν με κάθε τρόπο την έρευνα των αρμοδίων αρχών για τον εντοπισμό των δραστών.

Προτείνεται εξάλλου από διάφορες πλευρές, η αντικειμενικοποίηση της ποινικής ευθύνης των παροχέων για τις φιλοξενούμενες σε αυτούς σελίδες παιδικού πορνογραφικού περιεχομένου. Ήδη στην Ιταλία ψηφίστηκε ένας νέος νόμος, ο οποίος ορίζει ότι οι ISPs θα πρέπει να απαγορεύουν την πρόσβαση σε sites που φιλοξενούν παιδική πορνογραφία. Ο νόμος, ο οποίος τέθηκε άμεσα σε ισχύ, απαιτεί από τους ISPs να εγκαταστήσουν ένα σύστημα απαγόρευσης της πρόσβασης, ενώ ο χρόνος απόκρισης του ISP στο αίτημα ορίζεται επίσης από τον νόμο, ώστε να μην ξεπερνά τις 6 ώρες.

Αξίζει τέλος, να αναφέρουμε την εφεύρεση ενός Ισπανού ειδικού στην ασφάλεια υπολογιστικών συστημάτων, σε συνεργασία με την δίωξη ηλεκτρονικού εγκλήματος της Ισπανίας και κάποιων παροχέων υπηρεσιών διαδικτύου. Πρόκειται για μια νέα μηχανή αναζήτησης, η οποία έχει την ικανότητα να ανιχνεύει δίκτυα αμοιβαίας ανταλλαγής αρχείων (P2P) για παιδικό πορνογραφικό υλικό (φωτογραφίες, βίντεο κ.ά.) καθώς και τις IP διευθύνσεις των ατόμων που τα μοιράζονται. Το συγκεκριμένο πρόγραμμα που φέρει την ονομασία «Hispalis» είναι το μοναδικό του είδους στον κόσμο και η Ισπανική αστυνομία έχει ήδη ξεκινήσει να το χρησιμοποιεί σε συνεργασία με τους ISPs, ενώ έχει προκαλέσει το ενδιαφέρον και άλλων αρχών ασφαλείας, όπως του αμερικάνικου FBI. Το «Hispalis» χρησιμοποιώντας μια βάση δεδομένων από προηγούμενες αναζητήσεις παιδικής πορνογραφίας, εντοπίζει την διεύθυνση IP των χρηστών των δικτύων P2P, οι οποίοι είτε διανέμουν είτε κατεβάζουν το υλικό αυτό, καθιστώντας ουσιαστικά εφικτή την σύλληψή τους

μέσω του εντοπισμού της τοποθεσίας που αυτοί βρίσκονται[22].

Παρακάτω θα αναφέρουμε διάφορες κατηγορίες προστασίας για ην περιήγηση στο Διαδίκτυο.

I. Μέθοδος ταξινόμησης

Η κατηγορία προστασίας αυτή βασίζεται στην αξιολόγηση των ιστοσελίδων από τους δημιουργούς ή/και τους ιδιοκτήτες τους. Ορισμένοι παροχείς προτείνουν συστήματα αξιολόγησης του περιεχομένου στους κατασκευαστές ή τους υπευθύνους των ιστοσελίδων που φιλοξενούν, χωρίς ωστόσο να δύνανται να τους επιβάλλουν την αξιολόγηση. Τα συστήματα αυτά ονομάζονται ratings, με γνωστότερα τα PICS και RSACi και σε συνδυασμό με τα φίλτρα, τη λειτουργία των οποίων θα αναπτύξουμε παρακάτω.

II. Κώδικες δεοντολογίας

Αν και δεν έχει θεσπισθεί μέχρι σήμερα κάποιος επίσημος κώδικας δεοντολογίας από τη βιομηχανία του διαδικτύου, έχουν εμφανισθεί αρκετοί άτυποι κώδικες προερχόμενοι τόσο από δημόσιες όσο και από ιδιωτικές πρωτοβουλίες, με σκοπό τη δημιουργία αισθήματος εμπιστοσύνης και ασφάλειας στους χρήστες αναφορικά με την περιήγηση τους στο Διαδίκτυο[41]. Ήδη τον Σεπτέμβριο του 1997 υπήρξε μία σημαντική πρωτοβουλία από το Τηλεπικοινωνιακό Συμβούλιο της Ευρωπαϊκής Ένωσης για τη σύσταση ενός κώδικα δεοντολογίας των παροχέων και των χρηστών, καθώς και τη σύνταξη ενός κανονισμού λειτουργίας του διαδικτύου, με στόχο τον περιορισμό του παράνομου υλικού.

Στην Ελλάδα υπάρχουν φορείς, οι οποίοι συμμετέχουν σε σχετικά ερευνητικά προγράμματα, ενώ τον Νοέμβριο του 2000 το Κέντρο Προστασίας Καταναλωτών δημοσίευσε έναν κατάλογο 12 μέτρων που πρέπει να ακολουθούν οι χρήστες του διαδικτύου[23].

[22] Reuters, http://www.e-pcmag.gr/modules/news/article.php?storyid=2728

[23] Ζάνη Α., Media και έγκλημα: *Το διαδικτυακό έγκλημα,* Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα 2005, σελ. 160 επ

III. Λογισμικά φίλτρα

Κανένα λογισμικό πρόγραμμα φιλτραρίσματος δε μπορεί ελέγξει τον τρόπο περιήγησης στο Διαδίκτυο και τους επισκεπτόμενους διαδικτυακούς τόπους. Η αποτελεσματικότητα ενός φίλτρου εξαρτάται από την εξειδίκευση του λογισμικού καθώς και από τη συχνότητα ανανέωσης των καταλόγων με τους απαγορευμένους τόπους. Διαφορετικά φίλτρα είναι αποτελεσματικά στο να αποκλείουν την πρόσβαση σε τόπους με διαφορετικό τύπο επιβλαβούς περιεχομένου. Τα συστήματα φιλτραρίσματος λειτουργούν με ποικίλους τρόπους, οι κυριότεροι από τους οποίους είναι οι εξής:

1) *Οι λίστες με τα «Όχι»*. Συντάσσεται μια λίστα με «Όχι», ήτοι με ιστοσελίδες ακατάλληλου περιεχομένου, στις οποίες η επίσκεψη πρέπει να αποφευχθεί και όταν ο χρήστης προσπαθήσει να μπει σε κάποια από αυτές τις ιστοσελίδες, είτε εκούσια είτε επισκεπτόμενο ένα link, το οποίο εμφανίσθηκε τυχαία στην οθόνη του ή του απέστειλε κάποιος συνομιλητής του, η πρόσβαση αποκλείεται αυτόματα. Ορισμένα προγράμματα λειτουργούν κατά τον ίδιο τρόπο αλλά με λίστες απαγορευμένων λέξεων, όπως π.χ. porn, sex κ.α. Μόλις βρεθεί κάποια από αυτές τις λέξεις σε κάποια ηλεκτρονική διεύθυνση ή στο περιεχόμενο της ίδιας της ιστοσελίδας, μπλοκάρεται η πρόσβαση. Το πρόβλημα με αυτές τις λίστες είναι ότι πρέπει να αναβαθμίζονται συνεχώς.

2) *Φιλτράρισμα σε πραγματικό χρόνο*. Το φίλτρο ελέγχει τις λέξεις ή τις φωτογραφίες τη στιγμή που εκφράζεται η επιθυμία επίσκεψης ή κατεβάσματος και σταματάει την εμφάνιση οποιασδήποτε ιστοσελίδας με ανεπιθύμητο κείμενο ή φωτογραφία. Το πρόβλημα με τα φίλτρα τέτοιου τύπου είναι ότι υπάρχει η πιθανότητα, πριν το φίλτρο εντοπίσει την προσβλητική λέξη ή φωτογραφία, να εμφανιστεί τμήμα της ιστοσελίδας ή της φωτογραφίας. Επίσης, το σύστημα αυτό μπορεί να επιβραδύνει την πρόσβαση σε ιστοσελίδες.

3) *Περιγραφή/αξιολόγηση ιστοσελίδας*. Ο δημιουργός μιας ιστοσελίδας, τοποθετεί εθελοντικά σε αυτή μία ετικέτα, η οποία δηλώνει αν η ιστοσελίδα περιέχει ανεπιθύμητο υλικό (π.χ. βία, γυμνό, τυχερά παιχνίδια, περιεχόμενο για ενηλίκους, κ.λ.π.). Οι ετικέτες και οι ανταποκρινόμενες σε αυτές κατηγορίες έχουν δημιουργηθεί από την Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου (ICRA - Διαδίκτυο Content Rating Association). Το φίλτρο διαβάζει αυτές τις ετικέτες και αποφασίζει αν θα επιτρέψει την πρόσβαση, σύμφωνα με την

προεπιλογή του χρήστη. Το πρόβλημα με το σύστημα αυτό, είναι ότι στηρίζεται αποκλειστικά στη διακριτική ευχέρεια των δημιουργών των site να αξιολογήσουν τις ιστοσελίδες τους.

4) *Περιφραγμένες τοποθεσίες*. Συντάσσονται λίστες από ιστοσελίδες κατάλληλες για ανηλίκους και εφεξής η πρόσβαση επιτρέπεται μόνο σε αυτές[24].

Αξίζει τέλος να σημειωθεί ότι οι περισσότερες δημόσιες βιβλιοθήκες σε όλο τον κόσμο είναι ενάντια στη χρήση φίλτρων στο λογισμικό των ηλεκτρονικών υπολογιστών τους, καθώς πιστεύουν ότι τα φίλτρα μπλοκάρουν και ουσιαστικά καταργούν το συνταγματικά κατοχυρωμένο δικαίωμα της ελευθερίας της έκφρασης και εμποδίζουν την ελεύθερη πρόσβαση σε οποιαδήποτε πληροφορία.

IV) Ιστοσελίδες και γραμμές καταγγελίας.

Οι ιστοσελίδες και ανοικτές γραμμές καταγγελίας είναι διαδικτυακοί τόποι και τηλεφωνικές γραμμές αντίστοιχα, οι οποίες λειτουργούν συνήθως σε συνεργασία με τους παροχείς υπηρεσιών Διαδίκτυο και δίνουν στους χρήστες του διαδικτύου, τη δυνατότητα να αναφέρουν πιθανές παράνομες εικόνες που εντοπίζουν στο Διαδίκτυο, αναφορές οι οποίες καταγράφονται σε μία βάση δεδομένων, από την οποία προωθούνται στη συνέχεια στις αρμόδιες υπηρεσίες καταστολής ή σε ανοικτές γραμμές άλλων χωρών.

Ανοικτές γραμμές διαδικτυακής καταγγελίας λειτουργούν σήμερα, σε πολλές Ευρωπαϊκές χώρες, αλλά και σε χώρες εκτός Ε.Ε., όπως η Αυστραλία, ο Καναδάς, η Ιαπωνία, οι Η.Π.Α. κ.α, η δράση των περισσοτέρων από τις οποίες συντονίζεται από τον Παγκόσμιο Σύνδεσμο Ανοικτών Γραμμών Διαδίκτυο, «INHOPE». Στην Ελλάδα η πιο γνωστή ιστοσελίδα και ανοικτή γραμμή καταγγελιών για διαδικτυακούς τόπους, newsgroups και peer to peer υπηρεσίες, που περιέχουν εικόνες κακοποίησης παιδιών σε οποιοδήποτε σημείο του κόσμου και γενικά παράνομο υλικό, είναι η «SafeLine» που λειτουργεί από τον Απρίλιο του 2003. Πρωταρχικός της στόχος είναι η εξάλειψη από το Διαδίκτυο τη παιδικής πορνογραφίας. Καταγγελίες υποβάλλονται μέσω Διαδίκτυο, στη διεύθυνση www.safeline.gr, με e-mail, τηλεφωνικά, ή ταχυδρομικά, ενώ ο καταγγέλλων δύναται είτε να αποκρύψει τα

[24] Βλ. www.kepka.org.

προσωπικά του στοιχεία, είτε να επιλέξει να τα παρέχει προκειμένου να ενημερωθεί για την εξέλιξη της καταγγελίας του.

Η SafeLine μετά την λήψη της καταγγελίας, προχωρεί σε τυπική επαλήθευση της, ότι δηλαδή το περιεχόμενο της καταγγελίας όντως υπάρχει και μπορεί ενδεχομένως να χαρακτηριστεί παράνομο, έπειτα εντοπίζει τη χώρα προέλευσης του διαδικτυακού τόπου με τη χρήση τεχνικών μέσων και αν το περιεχόμενο προέρχεται από την Ελλάδα, ενημερώνει την ελληνική αστυνομία, άλλως ενημερώνει την αντίστοιχη ανοικτή γραμμή της χώρας προέλευσης, ενώ αν τέτοια γραμμή δεν υπάρχει, ενημερώνεται η ελληνική αστυνομία, προκειμένου αυτή με τη σειρά της να ενημερώσει την Interpol. Ήδη το έτος 2006 το πλήθος των καταγγελιών τις οποίες έλαβε η SafeLine ήταν ιδιαίτερα αυξημένο σε σχέση με τις προηγούμενες χρονιές. Συγκεκριμένα, επεξεργάστηκε 375 καταγγελίες, η συντριπτική πλειονότητα των οποίων ήταν ανώνυμες και από τις οποίες, οι 175 αφορούσαν την εκμετάλλευση παιδιών. Από τις καταγγελίες συνολικά, οι 49 προωθήθηκαν στην ελληνική αστυνομία, 113 σε ανοικτές γραμμές καταγγελίας των χωρών προέλευσης και 138 σε άλλους αρμόδιους φορεί και υπηρεσίες.

4.7 **Τρόποι ανίχνευσης – αντιμετώπισης ηλεκτρονικής απάτης**

Πολλά ψεύτικα μηνύματα συνδέονται με πραγματικά εταιρικά λογότυπα. Ωστόσο, μπορείτε να αναζητήσετε τα παρακάτω στοιχεία για την ανίχνευση πιθανής απάτη:

i. Αιτήματα για προσωπικά στοιχεία σε μήνυμα ηλεκτρονικού ταχυδρομείου

Οι περισσότερες νόμιμες εταιρείες έχουν ως πολιτική να μην ρωτούν μέσω ηλεκτρονικού ταχυδρομείου τα προσωπικά στοιχεία των πελατών τους. Πρέπει να υποψιαστείτε αν λάβετε μήνυμα που σας ρωτάει τα προσωπικά σας στοιχεία, ακόμα και αν όλα φαίνονται νόμιμα.

ii. Φρασεολογία που εκφράζει έκτακτη ανάγκη ή βιασύνη

Η φρασεολογία σε μηνύματα ψαρέματος είναι συνήθως ευγενική και εξυπηρετική. Συνήθως σας προτρέπει να απαντήσετε στο μήνυμα ή να κάνετε κλικ στη

συμπεριλαμβανόμενη σύνδεση. Για μεγαλύτερο αριθμό απαντήσεων, οι εγκληματίες προσπαθούν να καλλιεργήσουν μια αίσθηση ανάγκης και βιασύνης, ώστε οι παραλήπτες να απαντήσουν χωρίς να το πολυσκεφτούν. Συνήθως, τα ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου ΔΕΝ είναι εξατομικευμένα, ενώ τα έγκυρα μηνύματα από την τράπεζά σας ή από την εταιρεία ηλεκτρονικού εμπορίου είναι. Ακολουθεί ένα παράδειγμα πραγματικής τακτικής ψαρέματος:

«Αγαπητέ πελάτη μας, υπέπεσε στην αντίληψή μας ότι πρέπει να ενημερώσετε τα στοιχεία του λογαριασμού σας καθώς έχουμε λάβει αναφορές για αδράνεια, απάτες και κλοπή. Αν δεν ενημερώσετε τα στοιχεία σας, ο λογαριασμός θα διαγραφεί. Ακολουθήστε την παρακάτω σύνδεση για να επιβεβαιώσετε τα στοιχεία σας.»

iii. Ψεύτικες συνδέσεις

Σε μηνύματα που έχουν μορφοποιηθεί με HTML, οι συνδέσεις που σας προτρέπουν να κάνετε κλικ σε όλο ή μέρος μιας εταιρικής επωνυμίας είναι συνήθως "μεταμφιεσμένες", δηλαδή η σύνδεση που βλέπετε δεν σας οδηγεί στη συγκεκριμένη διεύθυνση αλλά κάπου αλλού, συνήθως σε ψεύτικη τοποθεσία Web. Παρατηρήστε σε αυτό το παράδειγμα με το Outlook ότι αν τοποθετήσετε το δείκτη του ποντικιού πάνω στη σύνδεση θα εμφανιστεί η πραγματική διεύθυνση στο πλαίσιο με το κίτρινο φόντο. Η συμβολοσειρά με τους παράξενους αριθμούς δεν έχει την εμφάνιση μιας εταιρικής τοποθεσίας στο Web ή μιας διεύθυνσης URL και αποτελεί ένδειξη που πρέπει να κινήσει τις υποψίες σας.

Μια άλλη συνηθισμένη τακτική που χρησιμοποιούν οι εγκληματίες είναι μια διεύθυνση URL που με την πρώτη ματιά αποτελεί το όνομα γνωστής εταιρείας αλλά μετά από προσεχτική εξέταση μπορείτε να διαπιστώσετε ότι έχει μικρές αλλαγές. Για παράδειγμα, η διεύθυνση www.microsoft.com μπορεί να είναι:

- www.micosoft.com
- www.verify-microsoft.com
- www.mircosoft.com

Η Microsoft έχει κερδίσει πρόσφατα διάφορες δικαστικές αγωγές κατά ατόμων που

χρησιμοποιούσαν αυτούς τους τύπους URL για να γελοιοποιήσουν νόμιμες ιδιότητες της Microsoft. Ωστόσο, η πρακτική συνεχίζεται και συχνά προστατεύεται από τα εθνικά σύνορα.

iv. Το κυρίως μήνυμα είναι εικόνα

Για να αποφευχθεί ο εντοπισμός τους από τα φίλτρα ανεπιθύμητης αλληλογραφίας, τα ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν εικόνα αντί για κείμενο στο κυρίως μήνυμα. Αν το απεσταλμένο ανεπιθύμητο μήνυμα χρησιμοποιεί πραγματικό κείμενο, το φίλτρο ανεπιθύμητης αλληλογραφίας του Outlook θα μετακινήσει το μήνυμα στο φάκελο Ανεπιθύμητη αλληλογραφία. Η εικόνα στο κυρίως μήνυμα είναι συνήθως μια υπερ-σύνδεση. Αυτό μπορείτε να το καταλάβετε επειδή αν τοποθετήσετε το δείκτη του ποντικιού στο κυρίως μήνυμα, ο δείκτης θα μετατραπεί σε ένα χεράκι.

Άλλοι τύποι εικόνων που περιλαμβάνονται σε μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να συνδέονται με το διακομιστή του αποστολέα της ανεπιθύμητης αλληλογραφίας και να λειτουργούν ως Web beacon. Όταν ανοίγετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, γίνεται λήψη των εικόνων και οι πληροφορίες διαβιβάζονται στο διακομιστή. Αυτές οι πληροφορίες χρησιμοποιούνται για να επαληθεύσουν ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου είναι έγκυρη ώστε να σας αποσταλεί πάλι ανεπιθύμητη αλληλογραφία. Από προεπιλογή, το Outlook εμποδίζει αυτόματα αυτές τις εξωτερικές εικόνες. Για περισσότερες πληροφορίες δείτε την ενότητα Πληροφορίες για την προστασία του απόρρητου, αποκλείοντας τις αυτόματες λήψεις εικόνων.

v. Συνημμένα

Πολλές τακτικές ψαρέματος σας ζητούν να ανοίξετε συνημμένα αρχεία που μπορεί να μολύνουν τον υπολογιστή σας με ιούς. Δεν πρέπει να ανοίξετε τα συνημμένα αυτών των ύποπτων μηνυμάτων. Αποθηκεύστε πρώτα τα συνημμένα που θέλετε να δείτε και ανιχνεύστε τα αρχεία με ενήμερο πρόγραμμα αντιμετώπισης ιών (Στα Αγγλικά) πριν το ανοίξετε. Για την προστασία του υπολογιστή σας, το Outlook και το Microsoft Outlook Express εμποδίζουν αυτόματα ορισμένους τύπους συνημμένων αρχείων που μπορεί να μεταδώσουν ιούς. Για περισσότερες πληροφορίες, δείτε την ενότητα Πώς το Outlook βοηθάει στην προστασία του υπολογιστή σας από ιούς.

vi. *Υποσχέσεις που είναι μάλλον πολύ καλές για να είναι αληθινές*

Χρησιμοποιήστε την κοινή λογική σας και αντιμετωπίστε με καχυποψία κάθε προσφορά χρημάτων ή εκπτώσεων που είναι πολύ καλή για να είναι αληθινή.

4.8 **Η διαδικτυακή επιχείρηση «Αράχνη»**

Η «Αράχνη» είναι η μεγαλύτερη διαδικτυακή επιχείρηση εντοπισμού παιδικού πορνογραφικού υλικού παγκοσμίως, στην οποία οι αμερικανικές διωκτικές αρχές έχουν δώσει την ονομασία «operation Fair Play». Στην επιχείρηση ήδη συμμετέχουν οι περισσότερες από τις ευρωπαϊκές αστυνομίες. Ο τζίρος από την παιδική πορνογραφία το 2009 ξεπέρασε τα 500 δισεκατομμύρια ευρώ παγκοσμίως και σήμερα θεωρείται μία από τις πλέον κερδοφόρες εγκληματικές «επιχειρήσεις». Σε αρκετές ανατολικοευρωπαϊκές και ασιατικές χώρες μάλιστα λειτουργούν στούντιο παραγωγής βίντεο με σκληρό πορνογραφικό υλικό και θύματα βρέφη εως ανήλικα 7-8 ετών.

Στο λογισμικό «Αράχνη», οι Αμερικανοί έχουν καταχωρίσει όλες τις φωτογραφίες, τα βίντεο και όσα αρχεία έχουν συγκεντρώσει, τα οποία περιέχουν παιδοφιλικό υλικό. «Κάθε ηλεκτρονικό αρχείο έχει τον δικό του μοναδικό αριθμό. Το δικό του DNA. Ετσι το FBI έχει καταγράψει κάθε φωτογραφία και βίντεο παιδικού πορνογραφικού υλικού που έχει εντοπιστεί σε ολόκληρο τον κόσμο. Όταν το αρχείο αυτό στέλνεται από κάποιον χρήστη, αμέσως η “Αράχνη” ειδοποιεί τόσο για τον αποστολέα όσο και για τον παραλήπτη του. Στην «Αράχνη» βρίσκονται καταχωρημένα περισσότερες από 30 εκατομμύρια φωτογραφίες και βίντεο που κατά καιρούς έχουν εντοπισθεί σε αστυνομικές επιχειρήσεις. «Όταν η Αστυνομία ανακαλύπτει στο αρχείο ενός παιδόφιλου μια σειρά φωτογραφιών, δεν σημαίνει πως καταστρέφονται. Πρόκειται για αρχεία που ταυτόχρονα μπορούν να βρίσκονται αποθηκευμένα σε εκατομμύρια υπολογιστές.

Το λογισμικό ενημερώνεται καθημερινά και σε απευθείας σύνδεση διοχετεύει τις νέες πληροφορίες στις αστυνομίες-χρήστες του συστήματος. Η «Αράχνη» καταγράφει το IP (η ταυτότητα του υπολογιστή) τόσο του αποστολέα όσο και του παραλήπτη και στη συνέχεια με εισαγγελική εντολή ο πάροχος του Διαδικτύου παραδίδει στις διωκτικές αρχές τα στοιχεία τους. Αξιωματικοί του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος επισημαίνουν τους

κινδύνους από τη χρήση του WiFi οικιακής χρήσης. Όπως αποκαλύπτουν, σε αρκετές περιπτώσεις έχει χρησιμοποιηθεί το ασύρματο δίκτυο από παιδόφιλους για τη μεταφορά αρχείων τους. Στην περίπτωση αυτή όμως ο κωδικός που εμφανίζεται στην Αστυνομία είναι του ιδιοκτήτη του οικιακού WiFi. Για τον λόγο αυτό, συνιστούν το κλείδωμα του ασύρματου δικτύου και συχνή αλλαγή του κωδικού πρόσβασης.

ΚΕΦΑΛΑΙΟ 5^0

-ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ-

5.1 **Ελληνική νομοθεσία για το ηλεκτρονικό έγκλημα**

Η αντιμετώπιση της ηλεκτρονικής εγκληματικότητας, ανάλογα με τη μορφή που αυτή λαμβάνει, μπορεί να γίνει από το Ελληνικό δίκαιο συνδυάζοντας διάσπαρτες διατάξεις της κείμενης νομοθεσίας. Σε αυτές ανήκουν οι διατάξεις του Ποινικού Κώδικα περί απάτης με τη χρήση υπολογιστή, περί αθέμιτης πρόσβασης σε συστήματα πληροφοριών, υποκλοπής και παραβίασης απορρήτων, η ειδική νομοθεσία περί προστασίας προσωπικών δεδομένων (ν. 2472/1997 όπως τροποποιήθηκε με το ν. 3625/2007, ν. 3471/2006), η νομοθεσία περί διασφάλισης του απορρήτου των επικοινωνιών (ν. 3674/2008), οι κανονιστικές αποφάσεις διοικητικών αρχών όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και ούτω καθεξής.

Ειδικότερα, το άρθρο 5 του ν. 1805/1988, προσέθεσε στο άρθρο 386 του Ποινικού Κώδικα περί απάτης το ειδικό άρθρο $386^{Α}$ που αναφέρεται στην απάτη με υπολογιστή. Σύμφωνα με το άρθρο αυτό, όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία, επηρεάζοντας τα αρχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές φυλάκισης που προβλέπονται για την απάτη.

Ανάλογα με τη βαρύτητα του αδικήματος, οι ποινές αυτές μπορούν να ανέρχονται από φυλάκιση τουλάχιστον τριών μηνών έως φυλάκιση τουλάχιστον τριών ετών αν η ζημία που προκλήθηκε είναι ιδιαίτερα μεγάλη. Υπό συγκεκριμένες προϋποθέσεις, η διαδικτυακή εγκληματικότητα, στο μέτρο που οδηγεί σε παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας, παραβίαση επαγγελματικών απορρήτων ή παράνομη αντιγραφή προγραμμάτων ηλεκτρονικού υπολογιστή, τιμωρείται και από τα άρθρα 370Α και

370Β του Ποινικού Κώδικα, που προβλέπουν αντίστοιχες ποινές φυλάκισης κατά των δραστών.

Πρόσφατα, ο νόμος 3674/2008 ψηφίστηκε για να ενισχύσει το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, θεσπίζοντας ειδικές υποχρεώσεις του παρόχου υπηρεσιών για την ασφάλεια δικτύου και συγκεκριμένες διαδικασίες άρσης του απορρήτου υπό την εποπτεία της ΑΔΑΕ. Παράλληλα, ο νόμος αυτός προσέθεσε νέο άρθρο 292Α στον Ποινικό Κώδικα που τιμωρεί τα εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών με φυλάκιση τουλάχιστον ενός έτους και χρηματικές ποινές που αρχίζουν από είκοσι χιλιάδες 20.000) Ευρώ και αυξάνονται ανάλογα με τη βαρύτητα του παραπτώματος και την ιδιότητα του δράστη.

Ο ίδιος νόμος τροποποίησε ακόμα το άρθρο 370Α του Ποινικού Κώδικα θεσπίζοντας αυστηρές κυρώσεις, που μπορούν να φθάσουν ως κάθειρξη μέχρι δέκα ετών για όσους παραβιάζουν το απόρρητο της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας. Τέλος, θέσπισε διοικητικές κυρώσεις (χρηματικά πρόστιμα, ανάκληση αδειών κλπ) κατά των εκπροσώπων εταιριών παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών.

Προς την ίδια κατεύθυνση, το άρθρο 348 Α του Ποινικού κώδικα, που προστέθηκε με το άρθρο 6 του ν. 3064/2002 τιμωρεί με φυλάκιση και χρηματικές ποινές την πορνογραφία ανηλίκων, οποιοσδήποτε και αν είναι ο υλικός φορέας αποτύπωσης του πορνογραφικού υλικού. Παρόμοιες κυρώσεις προβλέπονται από την ισχύουσα ειδική νομοθεσία περί προστασίας καταναλωτή, σε ότι αφορά ειδικότερα τις εξ αποστάσεως συμβάσεις πρόσβασης σε υπηρεσίες ηλεκτρονικού εμπορίου. Η νομοθεσία αυτή απαγορεύει τις παραπλανητικές εμπορικές πρακτικές (ν. 2251/1994 όπως ισχύει μετά την τροποποίηση του από το ν. 3587/2007), ενώ προβλέπει επίσης διοικητικές κυρώσεις κατά των παραβατών. Αντίστοιχες διοικητικές, αστικές και ποινικές κυρώσεις προβλέπονται επίσης κατά των παραβατών, όπως προαναφέρθηκε, από τη νομοθεσία περί προστασίας προσωπικών δεδομένων (ν. 2472/1997 όπως ισχύει και 3471/2006). Τέτοιες πράξεις ηλεκτρονικής παραβατικότητας μπορούν ακόμα να συνιστούν πλαστογραφία, εξύβριση, δυσφήμιση, προσβολή της νομοθεσίας περί απορρήτου, του ν. 2121/1993 περί πνευματικής ιδιοκτησίας ή του ν. 3431/2006 περί ηλεκτρονικών επικοινωνιών.

Στην Ελλάδα το spam ρυθμίζεται από το αρ. 11 του ν. 3471/2006, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/ ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Σύμφωνα με το άρθρο αυτό η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς. Εκτός από την ποινική προστασία και την ειδική νομοθεσία του τομέα που προβλέπει προσφυγή στις αρμόδιες αρχές, ο χρήστης που έπεσε θύμα ηλεκτρονικής απάτης μπορεί θεωρητικά να στραφεί δικαστικά κατά του προσβολέα ζητώντας αποζημίωση με βάση το άρθρο 914 του Αστικού Κώδικα περί αδικοπραξίας.

Πλην όμως, στις περισσότερες περιπτώσεις εγκλημάτων του κυβερνοχώρου, η ταυτότητα και η χώρα εγκατάστασης των προσβολέων είναι άγνωστη ενώ οι δράστες εξαφανίζονται μετά την εγκληματική πράξη τους. Επίσης ο τόπος διάπραξης του κυβερνο-εγκλήματος είναι συχνά αμφισβητούμενος, αν π.χ. η τεχνική υποδομή τέλεσης του εγκλήματος, ήτοι ο εξυπηρετητής (server) που φιλοξενεί την απατηλή ιστοσελίδα είναι εγκατεστημένος στην αλλοδαπή, οπότε είναι ενδεχόμενο να μην μπορούν να εφαρμοστούν οι προβλεπόμενοι Ελληνικοί νόμοι που τιμωρούν αποκλειστικά εγκλήματα τελούμενα στην Ελλάδα.

Η διεθνής διάσταση των εγκλημάτων του κυβερνοχώρου απαιτεί τη διεθνή συνεργασία. Η Διεθνής Σύμβαση του Συμβουλίου της Ευρώπης (Νοέμβριος 2001), που έχει υπογραφεί και από την Ελλάδα, εντάσσεται σε αυτήν την προοπτική. Εκτός όμως ότι δεν έχει ακόμα κυρωθεί από όλες τις χώρες η Σύμβαση αυτή έχει τύχει αρκετής διεθνούς κριτικής για ασάφεια των περιγραφομένων εγκλημάτων και προβλήματα εφαρμογής. Προς την ίδια κατεύθυνση εντάσσονται οι σχετικές πρωτοβουλίες της Ευρωπαϊκής Ένωσης για την καταπολέμηση διακίνησης επιβλαβούς και παράνομου περιεχομένου μέσω ίντερνετ, που στοχεύουν στη δημιουργία συνθηκών ασφαλούς χρήσης του Διαδικτύου μέσω αυτορρύθμισης και κωδίκων δεοντολογίας.

Η πρόληψη υποστηρίζεται επίσης από τη λειτουργία ειδικών τηλεφωνικών γραμμών

(hotlines), όπου οι χρήστες μπορούν να καταγγείλουν παραβατική συμπεριφορά προς τις αρμόδιες διωκτικές αρχές των κρατών- μελών. Ο Ευρωπαϊκός Οργανισμός για την ασφάλεια ENISA, έχει επίσης εκδώσει δύο εκθέσεις για την ασφάλεια και μέτρα καταπολέμησης της ανεπιθύμητης εμπορικής επικοινωνίας που εφαρμόζουν οι Πάροχοι Υπηρεσιών Διαδικτύου στην Ευρώπη. Παρά τη διεθνή κινητοποίηση και συνεργασία, η δυσκολία εντοπισμού των δραστών, η πιθανή αρνητική δημοσιότητα για το θύμα που συνοδεύει τη δημοσιοποίηση περιπτώσεων ηλεκτρονικής απάτης, σε συνδυασμό με την μικρή ταχύτητα ενεργοποίησης των διωκτικών μηχανισμών και απονομής δικαιοσύνης, καθώς και το κόστος της, είναι συνήθως αποτρεπτικοί παράγοντες διεκδίκησης της βλάβης από τον ζημιωθέντα καταναλωτή. Για το λόγο αυτό, η πρόληψη, η ευαισθητοποίηση και η λήψη μέτρων προστασίας κατά του ηλεκτρονικού εγκλήματος από τον συνειδητοποιημένο καταναλωτή είναι προτιμότερη από την καταστολή τέτοιων πράξεων σε βάρος των συμφερόντων του.

5.2 **Ποινικός κώδικας για το ηλεκτρονικό έγκλημα**

Παρακάτω θα αναφέρουμε τα σημαντικότερα άρθρα του ελληνικού ποινικού κώδικα που αφορούν στο ηλεκτρονικό έγκλημα.

5.2.1 Άρθρο 337. Προσβολή της γενετήσιας αξιοπρέπειας

1. Όποιος με ασελγείς χειρονομίες ή προτάσεις που αφορούν ασελγείς πράξεις, προσβάλλει βάναυσα την αξιοπρέπεια άλλου στο πεδίο της γενετήσιας ζωής του τιμωρείται με Φυλάκιση μέχρι ενός έτους ή χρηματική ποινή.

2. Με Φυλάκιση τριών μηνών μέχρι δύο ετών τιμωρείται η πράξη της προηγούμενης παραγράφου, αν ο παθών είναι νεότερος από 12 ετών.

3. Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα δεκαπέντε έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με Φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση

τουλάχιστον τριών ετών.

4. Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που εμφανίζεται ως ανήλικο κάτω των δεκαπέντε ετών και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του στο πεδίο της γενετήσιας ζωής του, τιμωρείται με Φυλάκιση τουλάχιστον ενός έτους. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση με το εμφανιζόμενο ως ανήλικο πρόσωπο, τιμωρείται με Φυλάκιση τουλάχιστον τριών ετών."

5. Όποιος τελεί την πράξη της παραγράφου 1 του άρθρου αυτού, εκμεταλλευόμενος την εργασιακή θέση του παθόντος ή τη θέση προσώπου που έχει ενταχθεί σε διαδικασία αναζήτησης θέσης εργασίας διώκεται κατ` έγκληση και τιμωρείται με Φυλάκιση από έξι (6) μήνες μέχρι τρία (3) έτη και με χρηματική ποινή τουλάχιστον χιλίων (1.000) ευρώ.

5.2.2 Άρθρο 348 - Διευκόλυνση ακολασίας άλλων

1. Όποιος κατ` επάγγελμα διευκολύνει με οποιοδήποτε τρόπο την ασέλγεια μεταξύ άλλων τιμωρείται με Φυλάκιση μέχρι ενός έτους.

2. Με φυλάκιση μέχρι τριών ετών και με χρηματική ποινή τιμωρείται όποιος διευκολύνει την ασέλγεια μεταξύ άλλων χρησιμοποιώντας απατηλά μέσα και αν ακόμη δεν ενεργεί κατ` επάγγελμα.

3. Όποιος κατ` επάγγελμα ή από κερδοσκοπία επιχειρεί να διευκολύνει, έστω και συγκαλυμμένα, με τη δημοσίευση αγγελίας, εικόνας, αριθμού τηλεφωνικής σύνδεσης ή με τη μετάδοση ηλεκτρονικών μηνυμάτων ή με οποιονδήποτε άλλο τρόπο την ασέλγεια με ανήλικο τιμωρείται με Φυλάκιση και με χρηματική ποινή δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.

5.2.3 Άρθρο 348 Α - Πορνογραφία ανηλίκων

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.

5.2.4 Άρθρο 348Β - Προσέλκυση παιδιών για γενετήσιους λόγους

1. Όποιος με πρόθεση, μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας, προτείνει σε ενήλικο να συναντήσει ανήλικο, που δεν συμπλήρωσε τα δεκαπέντε έτη, με σκοπό τη διάπραξη σε βάρος του των αδικημάτων των παραγράφων 1 και 2 του άρθρου 339 και 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν στη διάπραξη των αδικημάτων αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ.

5.2.5 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.

4. Η πράξη της παραγράφου 3 δεν είναι άδικη, αν η χρήση έγινε ενώπιον οποιασδήποτε δικαστικής ή άλλης ανακριτικής αρχής για τη διαφύλαξη δικαιολογημένου συμφέροντος, που δεν μπορούσε να διαφυλαχθεί διαφορετικά.

5. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.

6. Όποιος διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει για εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων των παραγράφων 1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και με χρηματική ποινή.

5.2.6 Άρθρο 370 Β Παράνομη αντιγραφή απορρήτων δεδομένων

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 τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

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

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

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

5.2.7 Άρθρο 370 Γ – Παράνομη χρήση ή πρόσβαση σε προγράμματα ή στοιχεία Η/Υ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή "διακοσίων ενενήντα (290) ΕΥΡΩ έως πέντε χιλιάδων εννιακοσίων (5.900) ΕΥΡΩ
.
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον "είκοσι εννέα (29) ΕΥΡΩ". Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά 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 αρμόδιου υπαλλήλου του.

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

5.2.8 Άρθρο 386 Α - Απάτη με υπολογιστή

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

5.3 Νόμοι περί ηλεκτρονικού εγκλήματος

Ενδεικτικά θα αναφέρουμε τους νόμους που έχει θεσπίσει το ελληνικό κράτος και αφορούν την προστασία από το ηλεκτρονικό έγκλημα.

- Ν. 2472/1997 – «Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (ενσωματωμένες τροποποιήσεις).
- Ν. 2867/2000 - «Οργάνωση και Λειτουργία των Τηλεπικοινωνιών και άλλες διατάξεις».
- Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»
- Ν. 3115/2003 – «Αρχή Διασφάλισης του απορρήτου των επικοινωνιών»
- Ν. 3431/2006 – «Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις».
- Ν. 3471/2006 - «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997».
- Ν. 3917/2011 - «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».

5.4 **Προεδρικά Διατάγματα**

Στην ενότητα αυτή παραθέτουμε τα προεδρικά διατάγματα μέχρι και το 2005 που αφορούν στο ηλεκτρονικό έγκλημα και τα παρακλάδια του.

- Π.Δ. 131/2003 – «Ηλεκτρονικό εμπόριο κλπ Υπηρεσίες της Κοινωνίας της Πληροφορίας»
- Π.Δ. 150/2001 - «Ηλεκτρονικές Υπογραφές»
- Π.Δ. 47/2005 – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του».

5.5 **Οδηγίες Ευρωπαϊκής Ένωσης – Διεθνείς Συμβάσεις**

Πέραν της ελληνικής νομοθεσίας ωστόσο, η Ευρωπαϊκή Ένωση, με τις κοινοτικές οδηγίες που έχει εκδώσει, καταβάλει προσπάθεια να συμμορφώσει τα κράτη και να καλύψει τυχόν

παραθυράκια-τρύπες που έχουν οι νομοθεσίες των ευρωπαϊκών κρατών. Παρακάτω αναφέρουμε τις σημαντικότερες οδηγίες που έχουν εκδοθεί από την Ε.Ε.

- Οδηγία 87/102/ΕΟΚ του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

- Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

- Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision -ONP).

- Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.

- Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών

- Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.

- Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

- Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

- Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της

πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).

· Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση).

· Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).

· Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο).

· Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας).

· Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

· Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Επιπροσθέτως, σε διεθνές επίπεδο, έχουν υπογραφεί κατά καιρούς διεθνείς συμβάσεις που έχουν ως αντικείμενο το Διαδίκτυο και την ασφαλή λειτουργία του, καθώς επίσης και την υπεράσπιση των ανθρωπίνων δικαιωμάτων.

Διεθνείς Συμβάσεις

- Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας
- Σύμβαση για το Κυβερνοχώρο - Βουδαπέστη 23-11-2001
- Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948
- Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ)

Τέλος, θα παραθέσουμε ορισμένες αποφάσεις υπουργικές , αλλά και από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείου σχετικά με τις τηλεπικοινωνίες και το Διαδίκτυο γενικότερα.

Αποφάσεις

- Η Υπουργική Απόφαση με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».
- Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr»
- Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002 - «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής»

ΚΕΦΑΛΑΙΟ 6^{ο}

-ΠΕΡΙΠΤΩΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ-

6.1 **Παραβίαση λογαριασμού κοινωνικού δικτύου**

Δικογραφία σχηματίσθηκε από την Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, σε βάρος δύο (2) ημεδαπών (ενός 25χρονου άντρα και μίας 46χρονης γυναίκας), για τα κατά περίπτωση αδικήματα της παραβίασης υπολογιστικών συστημάτων και προσωπικών δεδομένων, εξύβρισης, εκβίασης και απειλών κατά της ζωής 36χρονης ημεδαπής. Ειδικότερα, η 36χρονη κατήγγειλε στη Δίωξη Ηλεκτρονικού Εγκλήματος, ότι δεχόταν, από άγνωστα άτομα, απειλές κατά της ζωής της, μέσω τηλεφωνικών κλήσεων, αλλά και μέσω αποστολής γραπτών μηνυμάτων (SMS), με απειλητικό και εξυβριστικό περιεχόμενο. Επιπλέον είχαν παραβιάσει το προσωπικό της λογαριασμό στο Facebook και δημοσιοποίησαν διάφορες φωτογραφίες της, οι οποίες δεν ήταν προσβάσιμες στον καθένα.

Από τη διαδικτυακή ψηφιακή έρευνα και στο πλαίσιο άρσης των επικοινωνιών, διερευνήθηκαν τα ηλεκτρονικά ίχνη, οι τηλεφωνικές κλήσεις αλλά και η αποστολή μηνυμάτων (SMS) που είχε δεχτεί η καταγγέλλουσα. Ακολούθησε ανάλυση των ηλεκτρονικών ιχνών και στοιχείων, από την οποία προέκυψε ότι ο 25χρονος είχε παραβιάσει τον διαδικτυακό της λογαριασμό στο Facebook και είχε δημοσιοποιήσει τις φωτογραφίες της, ενώ ταυτοποιήθηκε η 46χρονη ημεδαπή, ως η κάτοχος του λογαριασμού κινητού τηλεφώνου, από τον οποίο είχε σταλεί γραπτό μήνυμα SMS, με το απειλητικό και εξυβριστικό περιεχόμενο. Επιπλέον, κλιμάκιο αστυνομικών της Δίωξης Ηλεκτρονικού Εγκλήματος διενήργησε έρευνα, παρουσία Εισαγγελικού Λειτουργού, στο σπίτι του 25χρονου στην Αθήνα, κατά τη διάρκεια της οποίας κατασχέθηκε ένας (1) φορητός Η/Υ. Επίσης, κατασχέθηκε μία (1) συσκευή κινητού τηλεφώνου μαζί με μία (1) κάρτα SIM, την οποία παρέδωσε η 46χρονη. Η δικογραφία που σχηματίσθηκε σε βάρος τους υποβλήθηκε στον κ. Εισαγγελέα Πρωτοδικών Αθηνών.

6.2 **Υπόθεση Kevin Mitnick 1987**

Ο Κέβιν Ντέιβιντ Μίτνικ γεννήθηκε στις 6 Οκτωβρίου 1963 είναι ένας από τους πιο διάσημους Αμερικανούς χάκερ. Έχοντας εισβάλει σε πολλά τηλεπικοινωνιακά δίκτυα και κλέβοντας δεδομένα από αυτά, τον καταδίκασαν σε φυλάκιση για ηλεκτρονικά εγκλήματα και κατοχή πλαστών στοιχείων. Ο Μίτνικ απέκτησε πολλούς υποστηρικτές που πίστευαν ότι η τιμωρία του ήταν υπερβολική και τον θεώρησαν σαν τον μεγαλύτερο χάκερ της εποχής μας καθώς επίσης και ως τον καλύτερο κοινωνικό μηχανικό (social engineer). Ο Μίτνικ, παιδί χωρισμένων γωνιών μεγάλωσε σε προάστιο του Λος Άντζελες την δεκαετία του '70. Ανέπτυξε πολλά χόμπι εκ των οποίων ο Ραδιοερασιτεχνισμός, που αργότερα τον οδήγησε στο phreaking του τηλεφωνικού δικτύου.

Ως «μέλος» της κοινότητας των phreakers[25] ο Μίτνικ έμαθε τις αρχές της κοινωνικής μηχανικής, τις οποίες αργότερα ανέπτυξε και εφάρμοσε σε τέτοιο σημείο ώστε πλέον ο όρος κοινωνική μηχανική να είναι εφάμιλλο του ονόματος του Κέβιν Μίτνικ. Η πρώτη επαφή του Μίτνικ με υπολογιστή στα 17 του χρόνια ήταν και αυτό που άνοιξε το δρόμο στη μετέπειτα πορεία του. Από την πρώτη στιγμή που ήρθε σε επαφή με υπολογιστές, και συνδυάζοντας την ικανότητα του στο phreaking άρχισε να ασχολείται με την ιδέα την πρόσβασης σε απομακρυσμένους υπολογιστές. Το 1987 ήρθε και η πρώτη σύλληψη του Μίτνικ για εισβολή σε υπολογιστή. Αμέσως τον επόμενο χρόνο, πάλι κατηγορήθηκε για εισβολή σε σύστημα κλέβοντας πηγαίο κώδικα της Digital Equipment Corporation. Ο Μίτνικ τότε καταδικάστηκε σε 1 χρόνο φυλάκιση. Ο Μίτνικ από την περίοδο της αποφυλάκισης του και έπειτα συνέχισε να ασχολείται με το παράνομο χάκινγκ ταξιδεύοντας σε διάφορες πολιτείες της Αμερικής για να αποφύγει πάλι τη σύλληψη, χρησιμοποιώντας πλαστά στοιχεία. Σύντομα έγινε το επίκεντρο των Μέσων Μαζικής Ενημέρωσης αλλά και του FBI.

Τελικά το 1995 με την βοήθεια του Tsutomu Shimomura, τεχνικού ασφαλείας υπολογιστών, και του ρεπόρτερ των Times John Markoff, ο Κέβιν Μίτνικ συνελήφθη και καταδικάστηκε σε 5 χρόνια φυλάκιση. Όταν αποφυλακίστηκε το 2000 του απαγόρευσαν της χρήση συσκευών με πληκτρολόγιο για χρόνια. Σήμερα ο Μίτνικ έχει γράψει 2 βιβλία γύρω από την κοινωνική μηχανική και τα κενά ασφαλείας σε συστήματα. Έχει ιδρύσει την δικιά

[25] http://en.wikipedia.org/wiki/Phreaking, Phreaking:*Είναι η κλοπή χρημάτων ή η εκμετάλλευση συστημάτων με τέτοιο τρόπο ώστε να αποφεύγει ο χρήστης κάποιας υπηρεσίας (τηλεφωνικής, τράπεζας και παρόμοιες) να πληρώσει όσα πραγματικά χρωστάει σε αυτή.*

του εταιρία που ασχολείται με θέματα ασφαλείας σε δίκτυα (Mitnick Security Consulting). Επίσης κάνει σεμινάρια ασφαλείας σε μεγάλες εταιρίες του χώρου. Ο Μίτνικ θεωρείται ένα από τα πιο αξιόλογα πρόσωπα στην σκηνή των χάκερ. Με τις δραστηριότητες του αλλά και την φυλάκιση του ξεσήκωσε κίνημα που υποστήριζε στην απελευθέρωση του Free Kevin. Γύρω από το πρόσωπο του δημιουργήθηκε ένας μύθος κυρίως από την δημοσιότητα που απέκτησε. Ιστοσελίδες, ντοκιμαντέρ και ταινίες έχουν γυριστεί για τη ζωή του Μίτνικ κάνοντας τον έναν ζωντανό θρύλο για κάποιους, σύμβολο του ανήσυχου πνεύματος των χάκερ[26].

6.3 **Υπόθεση Robert Matthew Bentley**

Το Δικαστήριο των Ηνωμένων Πολιτειών καταδίκασε σε 41 μήνες φυλάκισης χάκερ, ο οποίος είχε κατορθώσει να εισβάλει σε εκατοντάδες ηλεκτρονικούς υπολογιστές χάρις στη δημιουργία ενός botnet. Επίσης το δικαστήριο επέβαλε πρόστιμο 65.000 δολαρίων στον Ρόμπερτ Μάθιου Μπέντλεϊ, όπως ονομάζεται ο δράστης, ενώ όπως ανακοινώθηκε, θα τεθεί σε πρόγραμμα παρακολούθησης διάρκειας τριών ετών αμέσως μετά την αποφυλάκισή του. Ο όρος botnet αναφέρεται συνήθως σε ένα σύστημα που έχει σχεδιασθεί και χρησιμοποιείται για παράνομους σκοπούς. Τα συστήματα αυτά αποτελούνται από προσβεβλημένους υπολογιστές που εξομοιώνονται χωρίς τη γνώση του ιδιοκτήτη τους.

Το botnet είναι ένα κακόβουλο λογισμικό (γνωστό και ως malware) που μπορεί να μετατρέψει τον υπολογιστή σας σε ένα bot (γνωστό ως ζόμπι). Όταν συμβαίνει αυτό, ο υπολογιστής σας μπορεί να εκτελέσει αυτοματοποιημένες εργασίες μέσω του διαδικτύου, χωρίς να το γνωρίζει. Οι εγκληματίες χρησιμοποιούν συνήθως bots για να μολύνουν μεγάλο αριθμό υπολογιστών. Αυτοί οι υπολογιστές αποτελούν ένα δίκτυο, ή ένα botnet. Οι εγκληματίες χρησιμοποιούν botnets για την αποστολή spam μηνυμάτων ηλεκτρονικού ταχυδρομείου, την εξάπλωση ιών, κάνοντας επίθεση σε υπολογιστές και διακομιστές ώστε να δεσμεύουν άλλα είδη του εγκλήματος και της απάτης. Εάν ο υπολογιστής σας γίνει μέρος ενός botnet, μπορεί να επιβραδύνει και ίσως κατά λάθος να βοηθήσει εγκληματίες. Οι δέσμιοι από τον εν λόγω χάκερ ηλεκτρονικοί υπολογιστές χρησιμοποιήθηκαν σε επιθέσεις εις βάρος

[26] http://en.wikipedia.org/wiki/Convention_on_Cybercrime

άλλων υπολογιστών και για την εγκατάσταση κακόβουλων προγραμμάτων που μόλυναν υπολογιστές μέσω της εμφάνισης διαφημίσεων pop-up[27].

Το κακόβουλο λογισμικό που χρησιμοποίησαν ήταν IRCBot, ένα σκουλήκι με ιδιότητες που ανιχνεύονται από Sophos ως W32/Vanebot-R. Μέσω των διαφημίσεων προωθούσαν το λογισμικό σε όλη την Ευρώπη χωρίς άδεια, έτσι για κάθε εγκατάσταση του λογισμικού λάμβαναν προμήθεια από μια εταιρεία που ονομάζεται DollarRevenue. Ο χάκερ συνελήφθη έπειτα από έρευνα του Τμήματος Ηλεκτρονικού Εγκλήματος της Μητροπολιτικής Αστυνομίας (CCU).Η έρευνα ξεκίνησε το Δεκέμβριο του 2006 όταν η εταιρεία μάρκετινγκ Newell Rubbermaid (είναι μια αμερικανική εταιρεία που πωλεί καταναλωτικά προϊόντα και εμπορικά) ενημέρωσε το τμήμα CCU για την εισβολή αγνώστων στο δίκτυο της εταιρείας. Η έρευνα του δικτύου της Newell Rubbermaid οδήγησε στη Φλόριντα από όπου ο Μπέντλεϊ και οι συνεργάτες του συντόνιζαν τις επιθέσεις. Ο καταδικασθείς και οι συνεργάτες του περνούσαν τόσα πολλά δεδομένα μέσα από τους υπολογιστές της Newell Rubbermaid με αποτέλεσμα να καταρρεύσει το δίκτυο της εταιρείας. Η εταιρεία υπέστη ζημία ύψους 150.000 δολαρίων. Στην έρευνα συνέδραμαν οι μυστικές υπηρεσίες των ΗΠΑ, το FBI και η εταιρεία παροχής υπηρεσιών ασφαλείας υπολογιστών, Sophos. Ο Μπέντλεϊ ομολόγησε την ενοχή του για τις κατηγορίες της απάτης, ενώ αυτοί που τον βοήθησαν καταζητούνται ακόμη από το υπουργείο.

6.4 **Ιρανοί hackers εισβάλλουν σε τράπεζες των ΗΠΑ**

Τον Σεπτέμβριο του 2012, τα μέσα μαζικής ενημέρωσης αναφέρθηκαν σε επιθέσεις στον κυβερνοχώρο σε τραπεζικά ιδρύματα των ΗΠΑ. Με όλες αυτές τις αναφορές δημιουργήθηκε ένα κλίμα πανικού για τις επιχειρήσεις καθώς και για τους πελάτες τους. Για τις επιθέσεις αυτές (στην JPMorgan Chase, στην Bank of America (BoA), στην Wells Fargo, στην US Bancorp και στην Citigroup) θεωρείται υπεύθυνη μια ανώνυμη και απρόσωπη ομάδα ιρανών χάκερ. Η είδηση αυτή βγήκε στον "αέρα" από την κυβέρνηση των ΗΠΑ, την οποία έδωσε ένας ισραηλινός πολίτης και πληροφοριοδότης του FBI, ο Sam Bacile.

Στην πορεία όμως εμφανίζεται ως ένοχος, πίσω από αυτές τις επιθέσεις, το Ιράν. Συγκεκριμένα οι Μυστικές υπηρεσίες των ΗΠΑ που λαμβάνουν πληροφορίες από την κοινή αρχηγία των Πληροφοριών Προσωπικού Διεύθυνσης ισχυρίζονται ότι το Ιράν συνωμοτεί με

[27] http://el.wikibooks.org/wiki/Τεχνική_Νομοθεσία_Για_Μηχανικούς_Πληροφορικής/Ηλεκτρονικό_Έγκλημα

οργανωμένες ενέργειες που έχουν πάντα στόχο τις επιθέσεις προς τις ΗΠΑ, χρησιμοποιώντας ένα ολόκληρο στρατό στον κυβερνοχώρο έτσι ώστε να χτυπήσει αμερικανικά χρηματοπιστωτικά ιδρύματα.

Από την ανάλυση που έκανε το Πεντάγωνο θεωρείται ότι η κυβερνητική επιθετικότητα του Ιράν γίνεται για ακόμη μια φορά προσπάθεια υποστήριξης της τρομοκρατίας στον πόλεμο της Τεχεράνη ενάντια στην Δύση. Ο γερουσιαστής Τζόζεφ Λίμπερμαν επισημαίνει πως είναι αδύνατο, απλά κάποιοι χάκερ, να καταφέρουν να αναστατώσουν αυτές τις επιχειρήσεις μέσω των ιστοσελίδων τους. Βέβαια οι Ιρανοί, σε καμία περίπτωση δεν παραδέχονται ότι το Ιράν έχει κάνει hacking τις τράπεζες των ΗΠΑ. Ο Λευκός Οίκος επιδιώκει ενεργά την ασφάλεια στον κυβερνοχώρο με κάποιο εκτελεστικό διάταγμα που δεν θα το ιδιωτικοποιούνταν μόνο το κογκρέσο αλλά και θα έδινε της εκτελεστικής εξουσίας μία περαιτέρω δύναμη, ώστε να έχει τη δυνατότητα να κηρύσσει νόμο χωρίς έγκριση από τους πολίτες των ΗΠΑ.

Η εμπιστοσύνη στο αμερικανικό τραπεζικό σύστημα βρίσκεται σε φθίνουσα πορεία καθώς οι "κυβερνοεπιθέσεις" μεγαλώνουν το πρόβλημα. Αφήνοντας τους απλούς πολίτες στο σκοτάδι ως προς τους υποχθόνιους σκοπούς που κρύβονται πίσω από τις επιθέσεις αυτές, η προπαγάνδα γίνεται όλο και πιο αποτελεσματική[28].

Ένα γεγονός που δεν αναφέρουν τα μέσα μαζικής ενημέρωσης είναι ότι τέτοιου είδους επιθέσεις άρνησης εισβολών, επιτυγχάνονται χωρίς να χρειάζεται κανένα hacking. Το ATM, οι τραπεζικές πληροφορίες και τα δεδομένα δεν έχουν κλαπεί ή διαταραχθεί. Επιθέσεις άρνησης υπηρεσίας είναι ένα lockout του πελάτη από το δημόσιο δικτυακό τόπο της τράπεζας. αυτό σημαίνει πως οι επιθέσεις αυτές είχαν σχεδιαστεί από τα χρηματοπιστωτικά ιδρύματα και τα μέσα μαζικής ενημέρωσης για να πείσουν το κοινό ότι η κατάσταση έγινε χειρότερη από πριν. Στην ουσία αυτό το ύφος της προπαγάνδας κάνει τον μέσο Αμερικάνο να μένει με το φόβο ότι υπάρχουν πολλοί που καραδοκούν να καταστρέψουν τις ΗΠΑ.

6.5 **Η υπόθεση Gary McKinnon**

Ο Gary McKinnon είναι ένας Σκωτσέζος διαχειριστής συστημάτων και hacker γνωστός για την μεγαλύτερη υπόθεση στρατιωτικού hacking όλων των εποχών. ο McKinnon

[28] http://el.wikibooks.org/wiki/Τεχνική_Νομοθεσία_Για_Μηχανικούς_Πληροφορικής/Ηλεκτρονικό_Έγκλημα

κατηγορείται για hacking σε 97 υπολογιστές του στρατού των Η.Π.Α και της NASA σε διάστημα 13 μηνών, από το Φεβρουάριο του 2001 μέχρι τον Μάρτιο του 2002 με το ψευδώνυμο 'solo'.Οι Αμερικανικές αρχές υποστηρίζουν ότι ο McKinnon διέγραψε κρίσιμα αρχεία του λειτουργικού συστήματος τα οποία προκάλεσαν το κλείσιμο του δικτύου 2000 υπολογιστών της στρατιωτικής περιφέρειας του στρατού της Washington για 24 ώρες. Μετά τις επιθέσεις της 11ης Σεπτεμβρίου ο McKinnon διέγραψε τα αρχεία καταγραφής όπλων από τη ναυτική βάση των Η.Π.Α

Earle Naval Weapons Station' καθιστώντας το δίκτυο 300 υπολογιστών της βάσης ακατάλληλο και παραλύοντας τις παραδόσεις ανεφοδιασμού πυρομαχικών του στόλου των Η.Π.Α.Ο McKinnon επίσης κατηγορείται για αντιγραφή δεδομένων, αρχείων λογαριασμών και κωδικών πρόσβασης στον προσωπικό του υπολογιστή. Οι αρχές των Η.Π.Α ισχυρίζονται ότι το κόστος της ανίχνευσης και επιδιόρθωσης των προβλημάτων που προκάλεσε ο McKinnon άγγιζαν τις 700.000$. Ο McKinnon για πρώτη φορά ανακρίθηκε από την αστυνομία στις 19 Μαρτίου 2002. Μετά από αυτή τη ανάκριση, ο υπολογιστής του κατασχέθηκε από τις αρχές. Ανακρίθηκε και πάλι στις 8 Αυγούστου 2002, αυτή τη φορά από την Εθνική ομάδα ηλεκτρονικού εγκλήματος του Ηνωμένου Βασιλείου. Τον Νοέμβριο του 2002,ο McKinnon κατηγορήθηκε από μια ομοσπονδιακή μεγάλη κριτική επιτροπή στην Ανατολική Περιφέρεια της Βιρτζίνια. Το κατηγορητήριο περιείχε επτά κατηγορίες ηλεκτρονικού εγκλήματος, καθεμία από τις οποίες περιείχε μια πιθανή δεκαετή ποινή φυλάκισης.

Ο McKinnon παρέμεινε ελεύθερος χωρίς περιορισμό μέχρι τον Ιούνιο του 2005.Όταν και τέθηκε το θέμα να τηρήσει τους όρους της εγγύησης συμπεριλαμβανομένης της απαίτησης να προσέρχεται στο τοπικό αστυνομικό τμήμα του κάθε απόγευμα και να παραμείνει στο σπίτι του το βράδυ. Εκπροσωπώντας τον McKinnon στη Βουλή των Λόρδων στις 16 Ιουνίου 2008, οι δικηγόροι είπαν ότι οι εισαγγελείς είχαν αναφέρει στον McKinnon ότι θα αντιμετώπιζε μια πιθανή ποινή φυλάκισης 8-10 ετών για κάθε κατηγορία, αν αμφισβητούσε τις κατηγορίες χωρίς καμία πιθανότητα επαναπατρισμού, αλλά μόνο 37-46 μήνες, εάν ο ίδιος συνεργάζονταν και πήγαινε εθελοντικά στις Ηνωμένες Πολιτείες. Ο McKinnon επίσης, υποστήριξε ότι ο ίδιος είχε πει ότι θα μπορούσε να εκτίσει μέρος της ποινής του στο Ηνωμένο Βασίλειο, αν συνεργαζόταν. Απέρριψε την προσφορά, διότι οι Αμερικανοί δεν θα μπορούσαν να εγγυηθούν αυτές τις παραχωρήσεις. Ο δικηγόρος του

McKinnon είπε ότι η βουλή των λόρδων θα μπορούσε να αρνηθεί την έκδοση, αν υπήρχε κατάχρηση της διαδικασίας.

Ο McKinnon προσέφυγε στο Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, το οποίο επέβαλε μια φραγή για την έκδοση, αλλά η αίτηση για άσκηση έφεσης απορρίφθηκε. Στις 23 Ιανουαρίου 2009,ο McKinnon κέρδισε την άδεια από το Ανώτατο Δικαστήριο να υποβάλει αίτηση για δικαστικό έλεγχο κατά την έκδοσή του. Στις 31 Ιουλίου 2009, το Ανώτατο Δικαστήριο ανακοίνωσε ότι McKinnon είχε χάσει αυτή την έκκληση. Στις 16 Οκτωβρίου 2012,Η Υπουργός Εσωτερικών Theresa May ανακοίνωσε στη Βουλή των Κοινοτήτων ότι η έκδοση είχε μπλοκαριστεί. Στις 14 Δεκεμβρίου, ο δικηγόρος, Keir Starmer, ανακοίνωσε ότι McKinnon δεν θα διωχθεί στο Ηνωμένο Βασίλειο, λόγω των δυσκολιών που υπάρχουν στο να φέρει μια υπόθεση εναντίον του, όταν τα αποδεικτικά στοιχεία ήταν στις Ηνωμένες Πολιτείες[29].

6.6 **Anonymous κατά Υπουργείου Οικονομικών Ελλάδας(2012)**

Επίθεση από τους Anonymous, με ταυτόχρονη διαρροή απόρρητων και διαβαθμισμένων εγγράφων, δέχθηκαν οι υπηρεσίες του Γενικού Λογιστηρίου του Κράτους όπως επιβεβαίωσε το υπουργείο Οικονομικών. Συγκεκριμένα, στοιχεία της Γενικής Γραμματείας Δημοσιονομικής Πολιτικής και ειδικότερα αρχεία της Γενικής Διεύθυνσης Θησαυροφυλακίου και Προϋπολογισμού υπεξαιρέθηκαν από τους χάκερς και εν συνεχεία δημοσιοποιήθηκαν. Η επίθεση είχε κύριο στόχο την διαρροή εγγράφων και πληροφοριών σχετικά με την κατάσταση της Ελληνικής οικονομίας. Μετά από εντολή του Εισαγγελέα Πρωτοδικών η Δίωξη Ηλεκτρονικού Εγκλήματος αναλαμβάνει τη διερεύνηση της υπόθεσης της κλοπής αρχείων από το Γενικό Λογιστήριο του κράτους. Η επίθεση αυτή αποτελεί μία από τις μεγαλύτερες ηλεκτρονικές κυβερνοεπίθεσεις που έχει πραγματοποιηθεί τα τελευταία χρόνια στον Ελλαδικό χώρο.

Το μήνυμα των Anonymous ήταν το εξής:
«Χαιρετούμε τους πολίτες του κόσμου. Χαιρετούμε τους πολίτες της Ελλάδας. Είμαστε οι Ανώνυμοι. Η ελληνική κυβέρνηση είναι έτοιμη να καταθέσει σε ψηφοφορία στη Βουλή των Ελλήνων το νέο πακέτο των οικονομικών μέτρων λιτότητας ύψους 13,5 δισεκατομμυρίων

[29] http://en.wikipedia.org/wiki/Computer_crime

ευρώ, τα οποία αναμένεται να παρατείνουν την ύφεση στην Ελλάδα. Σύμφωνα με τα μέτρα λιτότητας, οι συνταξιούχοι έχουν δει ένα 60% πτώση στις συντάξεις τους (…) Πολίτες της Ελλάδας πληρώνετε Τράπεζες και διεθνείς οίκους διαχείρισης αμοιβαίων κεφαλαίων υψηλού κινδύνου. Είναι η δική σας ζωή. Εξέγερση πριν να είναι πολύ αργά. Τα μέτρα λιτότητας δεν πρέπει να περάσουν. Δεν έχω να πω τίποτα περισσότερο».

Οι hackers ανάρτησαν εσωτερικούς κωδικούς πρόσβασης του Υπουργείου Οικονομικών και συνδέσμους με έγγραφα που μπορεί να κατεβάσει ο οποιοσδήποτε. Τα στοιχεία που δίνουν στην δημοσιότητα οι hackers περιλαμβάνουν ονόματα χρηστών και κωδικούς πρόσβασης πιθανόν από εσωτερικό σύστημα του Υπουργείου. Εντύπωση προκαλεί η συχνή χρήση ευκολομνημόνευτων κωδικών (ακόμα και 123456) από πλήθος χρηστών υπογραμμίζοντας σαφέστατα την έλλειψη επαρκούς πολιτικής ασφάλειας ακόμα και στο πιο απλό, δηλαδή την επιλογή ενδυναμωμένων κωδικών πρόσβασης.

Τα έγγραφα που αναρτήθηκαν ως προϊόν υποκλοπής είναι έγγραφα από τον Ιούνιο του 2012 έως και μέχρι τις 22 Οκτωβρίου. Παρουσιάζουν τεράστια διασπορά και περιλαμβάνουν έγγραφα: από τον Οργανισμό Δημοσίου Χρέους, από το Υπουργείο Οικονομικών, από σχεδόν όλες τις γνωστές Ελληνικές Τράπεζες, από το Υπουργείο Μεταφορών, από τον Οργανισμό Σιδηροδρόμων Ελλάδος, από χρηματοπιστωτικά ιδρύματα του εξωτερικού , από το Υπουργείο Παιδείας, από την Γενική Διεύθυνση Φορολογίας, από το Γενικό Λογιστήριο του Κράτους, από το Νομικό Συμβούλιο του Κράτους, από την Τράπεζα της Ελλάδος, από την Εθνική Τράπεζα, από το Υπουργείο Εργασίας & Κοινωνικής Ασφάλισης, από το Τμήμα Θεματοφύλαξης & Διαχείρισης Τίτλων, από τον ΟΑΣΑ, από την Γενική Διεύθυνση Θησαυροφυλακίου και Προϋπολογισμού και πολλά άλλα. Αξιοσημείωτο είναι το γεγονός ότι μεταξύ άλλων περιλαμβάνονται και δύο κρυπτο-τηλεγραφήματα προς το Υπουργείο Εξωτερικών.

Τα έγγραφα αφορούν τη διαχείριση του δημόσιου χρέους, ορισμένα χαρακτηρίζονται απόρρητα και άκρως εμπιστευτικά, και γι' αυτό το λόγο οι συγκεκριμένοι υπολογιστές δεν είχαν σύνδεση με το Διαδίκτυο. Επιπλέον, υπεύθυνη για την ασφάλεια των συστημάτων αυτών είναι η ΕΥΠ[30]. Οι ίδιοι οι «Anonymous»(αν είναι αυτοί)υποστηρίζουν ότι πέτυχαν την παραβίαση χάρη σε γνωστό τρωτό σημείο(vulnerability) των υπολογιστικών συστημάτων του

[30] http://www.inews.gr/253/epithesi-ton-ANONYMOUS-se-ellinika-kyvernitika-SITES.htm

υπουργείου, το οποίο δεν είχε διορθωθεί, πράγμα που μολονότι δεν είναι απίθανο, ενδέχεται να μην είναι αλήθεια στη συγκεκριμένη περίπτωση. Κι αυτό, γιατί όπως αποκαλύπτει το secnews.gr, τα περισσότερα από τα έγγραφα τα οποία αποκαλύφθηκαν σήμερα το πρωί φαίνεται πως είναι σκαναρισμένα από τα πρωτότυπα χαρτιά και όχι κανονικά ψηφιακά έγγραφα. Λόγω αυτών των δεδομένων, η υπόθεση φαίνεται πως μετατρέπεται από «ψηφιακή εισβολή» στο υπουργείο Οικονομικών σε κάτι πιθανώς χειρότερο.

6.7 **Η κατάσταση στην Ελλάδα στον χώρο του κυβερνοεγκλήματος**

Για πρώτη φορά, στην έρευνα της PwC για το Οικονομικό Έγκλημα, γίνεται λόγος για ηλεκτρονικό οικονομικό έγκλημα στην Ελλάδα. Τόσο στη χώρα μας όσο και διεθνώς, σχεδόν ένας στους δυο συμμετέχοντες δήλωσε ότι τους τελευταίους 12 μήνες δίνει περισσότερη προσοχή στο ηλεκτρονικό έγκλημα (computer crime ή cybercrime). Σε αντίθεση με τις άλλες μορφές οικονομικού εγκλήματος, το έγκλημα στον κυβερνοχώρο ενεργοποιείται με απίστευτη ταχύτητα και κρύβει νέους κινδύνους.

Σύμφωνα με τους συμμετέχοντες στην Ελλάδα αλλά και στη Δυτική Ευρώπη και διεθνώς, οι χώρες από τις οποίες προέρχονται τα περισσότερα περιστατικά ηλεκτρονικού εγκλήματος είναι οι: Η.Π.Α., Ρωσία, Χονγκ Κονγκ και Κίνα. Όσον αφορά στον κίνδυνο που προέρχεται μέσα από τον οργανισμό, οι περισσότεροι δήλωσαν ότι προέρχεται κυρίως από τα τμήματα Operations (39%) και Πληροφορικής (35%). Και περίπου οι μισοί από τους συμμετέχοντες είπαν ότι οι οργανισμοί είναι προσεκτικοί ως προς τη χρήση των social media από τους εργαζομένους τους. Σύμφωνα με την έρευνα, οι οργανισμοί εκπαιδεύουν και ενημερώνουν των εργαζομένους τους, κυρίως με e-mails και αφίσες, παρόλο που στην πλειοψηφία τους (46%) θεωρούν πιο αποτελεσματικά τα σεμινάρια.

Σύμφωνα με τους ερωτηθέντες στην Ελλάδα, η μορφή του οικονομικού εγκλήματος έχει αλλάξει αρκετά, συγκριτικά με το 2009. Το 75% των συμμετεχόντων αναφέρουν ότι κατά τους τελευταίους 12 μήνες αντιμετώπισαν περιστατικά υπεξαίρεσης στοιχείων ενεργητικού, ενώ το 2009 το συχνότερα εμφανιζόμενο περιστατικό ήταν η δωροδοκία και η διαφθορά. Μεγάλη διαφορά στις δύο μελέτες για την Ελλάδα εμφανίζεται ως προς την προέλευση των υπαιτίων του οικονομικού εγκλήματος και την αντιμετώπισή τους. Το 2011, σύμφωνα με το 63% των συμμετεχόντων, τα περιστατικά οικονομικού εγκλήματος προήλθαν

μέσα από τους οργανισμούς, ενώ το 2009 υπεύθυνοι ήταν, κυρίως, οι εξωτερικοί συνεργάτες (50%). Όσον αφορά στην αντιμετώπιση των υπαιτίων, σύμφωνα με τη μελέτη, οι οργανισμοί στην Ελλάδα λαμβάνουν αυστηρότερα μέτρα από το 2009. Στην πλειοψηφία τους, οι συμμετέχοντες δήλωσαν ότι κινήθηκαν δικαστικά και απέλυσαν τους υπαιτίους ή διέκοψαν τη συνεργασία μαζί τους.

Παρ' όλο που η μελέτη για την Ελλάδα δείχνει ότι το οικονομικό έγκλημα αντιμετωπίζεται με περισσότερη σοβαρότητα, δείχνει επίσης ότι οι επιχειρήσεις και οι οργανισμοί στη χώρα μας διστάζουν να δηλώσουν ότι έχουν πληγεί από οικονομικό έγκλημα, σε σύγκριση με τη Δυτική Ευρώπη και διεθνώς. Οι οργανισμοί στην Ελλάδα φαίνεται να αντιμετωπίζουν με μεγαλύτερη σοβαρότητα και αυστηρότητα το οικονομικό έγκλημα τα τελευταία δύο χρόνια, σύμφωνα με την πρόσφατη έρευνα της PwC. Τα συχνότερα εμφανιζόμενα περιστατικά, στην Ελλάδα και διεθνώς, αφορούν σε υπεξαίρεση στοιχείων του ενεργητικού. Η 6η Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα της PwC διεξήχθη κατά το χρονικό διάστημα Ιουλίου - Σεπτεμβρίου 2011, με τη συμμετοχή 4.000 περίπου ανωτέρων στελεχών από 78 χώρες. Στο πλαίσιο της παγκόσμιας έρευνας, η PwC στην Ελλάδα πραγματοποίησε για δεύτερη φορά μελέτη ειδικά για τη χώρα μας, όπου συμμετείχαν συνολικά 92 ανώτερα στελέχη. Η μελέτη αυτή συγκρίνει τα αποτελέσματα με την αντίστοιχη μελέτη για την Ελλάδα που διεξήγαγε η PwC το Νοέμβριο 2009[31].

Γράφημα 6.1 ανάλυσης ηλεκτρονικών εγκλημάτων στην Ελλάδα 2009-2011

Πηγή: Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας 2008-2011

[31] Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας, 2012

6.8 **Λίστα Lagarde**

Με τον τίτλο Λίστα Lagarde ή Λίστα Φαλτσιάνι, φέρεται στην ελληνική δημοσιογραφία ειδικός κατάλογος Ελλήνων καταθετών στην τράπεζα HSBC της Ελβετίας, που ήταν μεν προϊόν υποκλοπής, πλην όμως περιήλθε στις μυστικές υπηρεσίες της Γαλλίας και δι΄ αυτών στο γαλλικό Υπουργείο Οικονομικών και ο οποίος στη συνέχεια, κατά το μέρος που αφορούσε Έλληνες καταθέτες, διαβιβάστηκε στον Έλληνα υπουργό Οικονομικών. Το Σεπτέμβρη του 2012 ήρθε για πρώτη φορά στη δημοσιότητα η ύπαρξη της λίστας.

Από το σημείο αυτό και μετά άρχισαν να εγείρονται δικαιολογημένα ερωτηματικά και αμφιβολίες περί της εγκυρότητάς του, αν δηλαδή είχε υποστεί αλλοιώσεις - αφαιρέσεις κ.λπ. αν υπάρχουν αντίγραφα και πόσα, ποιοι τα κατέχουν κ.ά. στον εν λόγω κατάλογο που δημοσιεύτηκε περιλαμβάνονται ονόματα πολιτικών και συγγενών των, καθώς επίσης εφοπλιστών, επιχειρηματιών κλπ. που ενδεχομένως ο κύκλος εργασιών τους να δικαιολογεί καταθέσεις στο εξωτερικό με δεδομένο ότι το μεγαλύτερο μέρος της δραστηριότητάς τους γίνεται στο εξωτερικό π.χ. εφοπλιστές, πλοιοκτήτες κλπ. πλην όμως περιλαμβάνονται και ονόματα Ελλήνων που δεν δικαιολογούν καταθέσεις στο εξωτερικό χωρίς όμως αυτό να σημαίνει ότι είναι και απόλυτα παράνομο.

Ωστόσο ηγέρθηκαν ερωτήματα για το αν πρέπει ή όχι να διαβιβάσουν στην Διεύθυνση Ηλεκτρονικού Εγκλήματος το επίμαχο στικάκι, καθώς οι προθεσμίες ήταν ασφυκτικές από την πλευρά της Βουλής. Στις 17.1.2013 θα αποφασιζόταν η συγκρότηση ή όχι προανακριτικής επιτροπής για την λίστα Lagarde. Σε περίπτωση που εσυστήνετο προανακριτική επιτροπή θα έπρεπε αμέσως η δικογραφία να διαβιβαστεί από τους δύο οικονομικούς εισαγγελείς στη Βουλή. Η τελευταία θα αποφάσιζε τόσο για την τύχη των εμπλεκομένων πολιτικών προσώπων, όσο και για τους συμμέτοχους μη πολιτικά πρόσωπα. Δηλαδή, εάν θα δικαστούν οι συμμέτοχοι μαζί με τα πολιτικά πρόσωπα στο Ειδικό Δικαστήριο (εφόσον παραπεμφθούν) ή θα δικαστούν ανεξάρτητα από την Ποινική Δικαιοσύνη.

Εάν οι δύο εισαγγελείς διαβίβαζαν το επίμαχο στικάκι στην Διεύθυνση Ηλεκτρονικού Εγκλήματος, θα απαιτούνταν περίπου 7 με 8 ημέρες για να γνωμοδοτήσει για την νόθευσή του. Παράλληλα, ένα από τα εμπλεκόμενα πρόσωπα θα μπορούσε να ασκήσει ένσταση ότι κατά την επεξεργασία δημιουργήθηκε παρέμβαση στο αποδεικτικό υλικό (στικάκι) που

μπορεί να αλλοιώσει την εικόνα του και πιθανά ανεπανόρθωτα. Την ίδια στιγμή όμως θα απαιτείτο χρόνος για να εξεταστεί από τον αρμόδιο δικαστικό σχηματισμό η ένσταση του εμπλεκόμενου προσώπου. Δηλαδή, η Βουλή θα ανέμενε την δικογραφία αλλά εκείνη δεν θα μπορούσε να διαβιβαστεί, καθώς θα υπήρχε εκκρεμής ένσταση.

Σε κάθε περίπτωση, με την σύσταση προανακριτικής επιτροπής, αυτή θα είχε όλες τις αρμοδιότητες που έχουν οι εισαγγελικές αρχές, άρα μπορεί εκείνη να στείλει το στικάκι στην Διεύθυνση Ηλεκτρονικού Εγκλήματος. Ακόμη, οι τεχνικοί του ΣΔΟΕ έχουν πρόγραμμα που μπορεί να επαναφέρει τα διαγεγραμμένα τρία αρχεία από το στικάκι. Όμως οι δύο οικονομικοί εισαγγελείς δεν έδωσαν εντολή στο ΣΔΟΕ να προχωρήσουν οι τεχνικοί στην επαναφορά των διαγεγραμμένων αρχείων, καθώς αυτό θα έδινε την δυνατότητα οι εμπλεκόμενοι να καταθέσουν δικονομικά ενστάσεις. Όπως καταλαβαίνουμε , οι στενές προθεσμίες και τα γραφειοκρατικά γρανάζια σε συνδυασμό με την εμπλοκή μεγάλων ονομάτων στη λίστα Lagarde, αποτέλεσαν τους παράγοντες που σε πρώτο στάδιο, δεν απεστάλη το περιβόητο στικάκι στην Δ.Η.Ε[32].

Ο Μ. Σφακιανάκης κατέθεσε εν τέλει στην προανακριτική επιτροπή στις 30 Ιανουαρίου 2013 και δήλωσε ότι «είναι πιο εύκολο να βρεθούν ίχνη σε ένα CD, ακόμη και αν έχουν επιχειρηθεί αλλοιώσεις, από ότι σε ένα usb». Στο ερώτημα «αν η μεταγραφή αρχείου από cd σε usb και από usb σε usb δείχνει οργανωμένη διάθεση αλλοίωσης στοιχείων», ο Μ. Σφακιανάκης απάντησε θετικά σύμφωνα με το ΑΠΕ[33]. Ερωτηθείς για την τήρηση στοιχείων σε usb, ο επικεφαλής της Δίωξης Ηλεκτρονικού Εγκλήματος, απάντησε ότι οποιοσδήποτε μπορεί να σβήσει στοιχεία που αφορούν την ημερομηνία εγγραφής και την ταυτότητα του υπολογιστή, με ένα απλό πρόγραμμα.

Όπως μεταφέρουν μέλη της Επιτροπής, ο επικεφαλής της Δίωξης Ηλεκτρονικού Εγκλήματος ανέφερε ότι για την εξαγωγή συμπερασμάτων απαιτείται τουλάχιστον έρευνα και σε υπολογιστές, διότι, όπως είπε, ένα usb από μόνο του αν έχει υποστεί αλλοιώσεις ως προς την ημερομηνία εγγραφής και την ταυτότητα του υπολογιστή στον οποίο έγινε η επεξεργασία, είναι σχεδόν αδύνατο να οδηγήσει σε ασφαλή συμπεράσματα

[32] Εφημερίδα Το Παρασκήνιο .16-12-2012, *"Σεισμό προκαλεί η Λίστα Lagarde"*,.16-12-2012, σελ.28
[33] Αθηναϊκό Πρακτορείο Ειδήδεων

Όσον αφορά στην υπόθεση του κ. Παπακωνσταντίνου, ο δικηγόρος του κ. Παναγιώτης Βασιλακόπουλος, κατέθεσε γραπτό αίτημα του πελάτη του, με το οποίο ζητούσε να του δοθεί παράταση μέχρι τον Αύγουστο. Τα μέλη της Προανακριτικής απέρριψαν το αίτημα, κρίνοντας ότι μια προθεσμία 10 ημερών είναι αρκετή για να μπορέσει ο κ. Παπακωνσταντίνου να μελετήσει το υλικό που έχει ζητήσει και έχει πάρει στα χέρια του προκειμένου να προετοιμαστεί πριν από την κατάθεσή του. Κατόπιν υποβολής του υπομνήματος, η προανακριτική παρέπεμψε τον κ. Παπακωνσταντίνου σε Ειδικό Δικαστήριο για τα κάτωθι κακουργήματα[34]:

- Αδίκημα νόθευσης και απιστίας σχετικά με την υπηρεσία (σε βαθμό κακουργήματος)
- Παράβαση καθήκοντος (σε βαθμό πλημμελλήματος)

[34] Πόρισμα της προανακριτικής για την παραπομπή του Γεώργιου Παπακωνσταντίνου (λίστα Lagarde) http://content-mcdn.feed.gr/pegasus/Multimedia/pdf/porisma_id28620363.pdf

ΕΠΙΛΟΓΟΣ

Σε μια εποχή στην οποία η τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς, οι ανάγκες που δημιουργούνται ολοένα και αυξάνονται. Το διαδίκτυο αποτελεί πλέον μέσο επικοινωνίας, ανταλλαγής πληροφοριών, εμπορικών συναλλαγών κτλ. Σε πολλές χώρες αποτελεί θεμελιώδες δικαίωμα η πρόσβαση στο διαδίκτυο και κατατάσσεται στην κατηγορία που ανήκουν το νερό, το ηλεκτρικό ρεύμα. Ωστόσο, η χρήση του κρύβει κινδύνους ακόμα και για άτομα με γνώσεις και εμπειρία στο αντικείμενο αυτό.

Μια σειρά από ενέργειες όπως προαναφέραμε, γίνονται πλέον μέσω διαδικτύου και αφορούν και οικονομικές συναλλαγές. Το γεγονός αυτό δίνει τροφή σε επιτήδειους να εκμεταλλευτούν την απειρία χρηστών του διαδικτύου και να τους εξαπατήσουν. Η γιγάντωση του παγκόσμιου ιστού συνεπάγεται νέες και περισσότερες δυνατότητες , ωστόσο, παράλληλα, σημαίνει ευκαιρία για εξαπάτηση .Το ηλεκτρονικό έγκλημα μπορεί να λάβει διάφορες μορφές, όπως για παράδειγμα, πορνογραφία ανηλίκων, κλοπή προσωπικών ή επαγγελματικών δεδομένων, πλαστογραφία, απάτη, κλοπή κωδικών ATM, παράνομη πρόσβαση σε δεδομένα υπολογιστών, αποστολή ιών, απάτη με πιστωτικές κάρτες, παράνομη πρόσβαση σε υπηρεσία internet banking, παράνομη διακίνηση λογισμικού, ηλεκτρονική πειρατεία κ.τ.λ.

Η διάπραξη ηλεκτρονικών εγκλημάτων είναι ένα λεπτό ζήτημα που απαιτεί μία ειδικευμένη προσέγγιση, που συνεπάγεται όσμωση αφενός των τεχνικών που μετέρχονται οι ειδικοί της Πληροφορικής και αφετέρου των ερευνών των ανακριτικών υπαλλήλων11. Κάτι μάλιστα που δεν συνηθίζεται να αναφέρεται, είναι ότι οι δικαστές, ανάλογα με την έννομη τάξη κάθε κράτους και το είδος του εγκλήματος προς εκδίκαση, ενδέχεται να είναι απλοί πολίτες, ένορκοι οι οποίοι είναι πιθανό να έχουν μικρότερη εξοικείωση με τα ψηφιακά πειστήρια του εγκλήματος από ό,τι οι τακτικοί δικαστές[35].

Για την αποτροπή και την καταστολή του ηλεκτρονικού εγκλήματος οιασδήποτε μορφής έχει συσταθεί η Δίωξη Ηλεκτρονικού Εγκλήματος η οποία πλέον συνεργάζεται με την Οικονομική Υπηρεσία της ελληνικής αστυνομίας. Η Δ.Η.Ε είναι μια καίρια υπηρεσία με

[35] *A. Maniatis,* La modernisation digitale de l'Administration publique, in G. Petroni and F. Cloete (Eds.), New Technologies in Public Administration, IOS Press, 2005, σελ. 86-87, ιδίως σελ. 86.

επιτυχές μακροχρόνιο έργο και διεθνούς επιπέδου (επιχείρηση «Αράχνη») και έχει να αντιμετωπίσει κυρίως τα εξής:

- Κλοπή ταυτότητας στο Διαδίκτυο ονομάζεται η πρακτική του να χρησιμοποιεί κανείς την εικονική ταυτότητα ενός άλλου ατόμου, δηλαδή να χρησιμοποιεί το όνομα χρήσης (user ame) και τον κωδικό πρόσβασης (password) του ατόμου αυτού σε διάφορες διαδικτυακές υπηρεσίες, υποδύοντας έτσι το άτομο αυτό. Σκοπός όσων επιχειρούν κλοπή ταυτότητας μπορεί να είναι η οικονομική εξαπάτηση αλλά και ο εξευτελισμός ή η διάδοση φημών για ένα άτομο στο διαδικτυακό του περιβάλλον. Κάποιος για να δυσφημίσει ή να γελοιοποιήσει την ταυτότητα κάποιου άλλου ατόμου μπορεί να το κάνει είτε υποκλέπτοντας τους κωδικούς πρόσβασης, είτε ανοίγοντας ένα ψεύτικο προφίλ / λογαριασμό με το όνομα του άλλου ατόμου. Έτσι, πίσω από την κλεμμένη αυτή ταυτότητα, μπορεί να επικοινωνήσει με φίλους του ατόμου αυτού και να αναρτήσει φωτογραφίες και άλλο οπτικοακουστικό υλικό με σκοπό τον εξευτελισμό του ατόμου αυτού ή και τρίτων στο περιβάλλον του.

- Δικτυοπειρατεία είναι ένας όρος που χρησιμοποιείται για τη γενική χρήση του Διαδικτύου για την παράνομη αντιγραφή ή διανομή λογισμικού. Δικτυοπειρατεία συμβαίνει όταν το Διαδίκτυο χρησιμοποιείται για να διαφημίσει, ή να αποκτά ή να διανέμει πειρατικό λογισμικό. Υπολογίζεται ότι υπάρχουν εκατομμύρια ιστοσελίδες στο Διαδίκτυο πώληση παράνομου λογισμικού και περνώντας μακριά στους καταναλωτές ως γνήσιο προϊόν.

- Υπάρχουν τρεις διαφορετικοί τύποι απάτης με πιστωτικές κάρτες: πιστωτική κάρτα κλοπής, πιστωτική κάρτα λογαριασμού, κλοπή αριθμού και κλοπή ταυτότητας. Οι απάτες πιστωτικών καρτών είναι ένα τεράστιο πρόβλημα και το πιο προφανές είδος απάτης. Ο χρήστης είναι συχνά σε πλήρη άγνοια ότι η ασφάλειά του έχει τεθεί σε κίνδυνο. Υπάρχουν αρκετές δικλείδες ασφαλείας και μέθοδοι που διασφαλίζουν την καλή πίστη των συναλλαγών μέσω καρτών.

- Η διακίνηση ναρκωτικών γίνεται πλέον και μέσω του διαδικτύου, σύμφωνα με έρευνα πανεπιστημίου της Αυστραλίας. Κάποιοι έκαναν μελέτες για αυτά τα ναρκωτικά και υποστήριξαν ότι μέσω του διαδικτύου διακινούνται "νόμιμα" ναρκωτικά που όμως

περιέχουν ουσίες όπως και τα παράνομα και είναι ιδιαίτερα επικίνδυνα. Ακόμα υποστήριξαν πως μέσω του διαδικτύου διακινούνται εύκολα και τα παράνομα ναρκωτικά αφού είναι δύσκολο να εντοπιστούν από τις διωκτικές αρχές.

Καταλαβαίνει κανείς λοιπόν από τα παραπάνω ότι το έργο της Δίωξης Ηλεκτρονικού Εγκλήματος είναι δυσχερές καθώς έχει να αντιμετωπίσει άτομα με απρόσωπες, παραβατικές, ακόμα και εγκληματικές ενέργειες τα οποία έχοντας ως μάσκα την πρόσβαση στο διαδίκτυο μέσω λογαριασμών που ενδέχεται να περιέχουν ψεύτικα στοιχεία, προβαίνουν σε εξαπατήσεις πολιτών , εκβιασμούς κτλ. Παρολαυτά, η Δίωξη Ηλεκτρονικού Εγκλήματος, τα τελευταία χρόνια, έχει καταφέρει να αποτρέψει μια πλειάδα παράνομων δράσεων και ταυτόχρονα να σώσει ζωές ανθρώπων οι οποίοι έχοντας εθιστεί στο κόσμο του διαδικτύου, είχαν εκφράσει την επιθυμία να αυτοκτονήσουν σε προσωπικούς λογαριασμούς σε ιστότοπους κοινωνικής δικτύωσης.

Για την βελτίωση της λειτουργίας της Δ.Η.Ε θα μπορούσαν να γίνουν οι παρακάτω ενέργειες:

- Παρακολούθηση σεμιναρίων από ειδικούς στην εξάρθρωση ηλεκτρονικών απατών σε χώρες με ανεπτυγμένη τεχνολογία
- Συνεργασία με υπηρεσίες ασφαλείας εξωτερικού
- Συνεργασία με οικονομικές υπηρεσίες άλλων κρατών
- Πρόσληψη στην Δ.Η.Ε ατόμων που έχουν συλληφθεί για ηλεκτρονικές απάτες-Συνεργασία με χάκερς
- Τοποθέτηση ατόμων σε δημόσιες υπηρεσίες για την εποπτεία και διασφάλιση της εύρυθμης λειτουργίας των
- Ενημέρωση μέσω διαλέξεων-σεμιναρίων, όχι μόνο σε σχολεία, αλλά επίσης σε πολίτες επικεντρώνοντας σε άτομα που δεν έχουν μεγάλη εξοικείωση με τη χρήση του διαδικτύου
- Δημιουργία εγχειριδίων για ορθή-ασφαλή χρήση του διαδικτύου με συμβουλές για αποφυγή εξαπατήσεων
- Δημιουργία δημόσιας σχολής με κύριο στόχο την εκπαίδευση από την ηλικία των 18 ετών ατόμων που θα επανδρώσουν το τμήμα Δ.Η.Ε μετά το πέρας της εκπαίδευσης

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Βιβλιογραφία

- Αγγελής Ι., *Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, Ποινική Δικαιοσύνη Τεύχος 8-9/2005*
- Αγγελής Ι., «*Διαδίκτυο και ποινικό δίκαιο», Έγκλημα στον κυβερνοχώρο Cybercrime-Διαδίκτυο Crime, Τεύχος **4/2003,** Νομική Βιβλιοθήκη*
- Αγγελόπουλος Δ. - Πάσχος Ι., *Κατάσχεση-Ανάλυση ψηφιακών πειστηρίων, Ποινική Δικαιοσύνη, Τεύχος 4/2003, Νομική Βιβλιοθήκη*
- Βελέντζας Ε.Ι., *Δίκαιο Τεχνολογίας και Καινοτομίας, Θεσσαλονίκη, Εκδ.Ius,2008*
- Βλαχοπούλου Κ., *Ηλεκτρονικό Έγκλημα, Εκδ. Νομική Βιβλιοθήκη 2007*
- Διακονικολού Γ., *Επιχειρησιακή Διαδικτύωση, Εκδ. Κλειδάριθμος Αθήνα, 2007*
- Ζανή Α., *Media και έγκλημα: Το διαδικτυακό έγκλημα, Αντ. Ν. Σάκκουλα, Αθήνα 200*5
- Καϊάφα-Γκμπάντι Μ., *Κοινώς Επικίνδυνα Εγκλήματα, Γ΄ έκδ., Εκδ. Σάκκουλα Αθήνα 2005*
- Κιούπη Δ., *Ποινικό Δίκαιο και Internet, Εκδ. Αντ. Ν. Σάκκουλα, Αθήνα 1999*
- Λάζος Γρ., «*Πληροφορική και Έγκλημα», Αθήνα, Νομική Βιβλιοθήκη.,2001*
- Μαγκάκης Γ.Π *Ποινικό Δίκαιο, έκδοση γ΄βελτιωμένη, εκδόσεις Παπαζήση ,1984*
- Μακρυδημήτρη Αντ., *Διοίκηση και Κοινωνία. Η δημόσια διοίκηση στην Ελλάδα, εκδ. Θεμέλιο, Αθήνα, 1999*
- Μανιάτης Α., *Δίκαιο Πληροφορικής και Τηλεπικοινωνιών, Εκδόσεις Σάκκουλα, Αθήνα – Κομοτηνή, 2006*
- Πανούσης Ι., *Σύγχρονα θέματα εγκληματολογίας, Εκδόσεις Δανιά, Αθήνα, 1990*
- Σπινέλλη Κ, *Εγκληματολογία, ,Εκδόσεις Σάκκουλα, Αθήνα, 1985*
- Σταθόπουλος Π., *Κοινωνική Πρόνοια μία γενική θεώρης, Εκδόσεις Έλλην, Αθήνα, 1999*
- Τάτσης Ν.Χ (επιμ.), *Max Weber - ερμηνευτικά κείμενα, εκδ. Οδυσσέας, Αθήνα, 1998*
- Τερλέξης Π., *Ο Καπιταλισμός στα όριά του, Τομ. 2ος, εκδ. Παπαζήση, Αθήνα, 1999*
- Τσουραμάνης Χ., «*Διαδίκτυο και ποινική δικαιοσύνη: Πορνογραφία και Διαδίκτυο», Ποινική Δικαιοσύνη, Τεύχος 4/2002, Νομική Βιβλιοθήκη*

Ξένη Βιβλιογραφία

- Alex Thio, *Παρεκκλίνουσα συμπεριφορά, Εκδόσεις Έλλην, Αθήνα , 2003*
- Clarke R.V. «*Technology, Criminology and Crime Science», European Journal on criminal Policy and Research, Vol 10, Kluwer Academic Publishers 2004*
- Debra Littlejohn Shinder, Ed Tittel, "Scence of cybercrime Computer Forensic Handbook.
- Furnell St., *Κυβερνοέγκλημα – Καταστρέφοντας την κοινωνία της πληροφορίας, (μετάφραση: Φ. Μηλιώνη), Αθήνα, Εκδόσεις Παπαζήση, 2006*
- Maniatis A., *La modernisation digitale de l'Administration publique, in G. Petroni and F. Cloete (Eds.), New Technologies in Public Administration, IOS Press, 2005*
- Max Weber, *The Theory of Social and Economic Organization, επιμ. Talcott Parsons, The Free Press, NY, 1964*

ΑΛΛΕΣ ΠΗΓΕΣ-ΔΙΑΔΙΚΤΥΟ

- Μανιάτης Α., άρθρο «Η περιαγωγή μίας εκτροπής στις τηλεπικοινωνίες» , Εφημερίδα ΔΔ, 2006
- Μανιάτης Α.,FORUM , Δικαστική των Ηλεκτρονικών Υπολογιστών, 2011
- http://www.astynomia.gr , Διυπηρεσιακή Συνεργασία & παράλληλη δράση , Ελληνική Αστυνομία, Υπουργείο Δημόσιας Τάξης
- http://www.astynomia.gr/, Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος
- http://www.saferinternet.gr, Η επίσημη ιστοσελίδα του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου
- http://www.e-pcmag.gr/modules/news/article.php?storyid=2728
- http://en.wikipedia.org/wiki/Convention_on_Cybercrime
- http://el.wikibooks.org/wiki/Τεχνική_Νομοθεσία_Για_Μηχανικούς_Πληροφορικής/Ηλεκτρονικό_Έγκλημα
- http://el.wikibooks.org/wiki/Τεχνική_Νομοθεσία_Για_Μηχανικούς_Πληροφορικής/Ηλεκτρονικό_Έγκλημα
- http://en.wikipedia.org/wiki/Computer_crime
- http://www.kepka.org
- http://www.inews.gr/253/epithesi-ton-ANONYMOUS-se-ellinika-kyvernitika-SITES.htm
- http://content-mcdn.feed.gr/pegasus/Multimedia/pdf/porisma_id28620363.pdf

ΠΑΡΑΡΤΗΜΑ – ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

· **<u>Άρθρα Ποινικού Κώδικα</u>**

- Άρθρο 337 - Προσβολή της γενετήσιας αξιοπρέπειας
- Άρθρο 348 - Διευκόλυνση ακολασίας άλλων
- Άρθρο 348Α - Πορνογραφία ανηλίκων
- Άρθρο 348Β - Προσέλκυση παιδιών για γενετήσιους λόγους
- Άρθρο 370Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας
- Άρθρο 370Β - Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα.
- Άρθρο 370Γ - Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών.
- Άρθρο 386Α - Απάτη με υπολογιστή

· **Νόμοι**

- Ν. 2472/1997 – «Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (ενσωματωμένες τροποποιήσεις).
- Ν. 2867/2000 - «Οργάνωση και Λειτουργία των Τηλεπικοινωνιών και άλλες διατάξεις».
- Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»
- Ν. 3115/2003 – «Αρχή Διασφάλισης του απορρήτου των επικοινωνιών»
- Ν. 3431/2006 – «Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις».

- Ν. 3471/2006 - «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997».

- Ν. 3917/2011 - «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».

· **Προεδρικά Διατάγματα**

- Π.Δ. 131/2003 – «Ηλεκτρονικό εμπόριο κλπ Υπηρεσίες της Κοινωνίας της Πληροφορίας»

- Π.Δ. 150/2001 - «Ηλεκτρονικές Υπογραφές»

- Π.Δ. 47/2005 – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του».

· **Οδηγίες Ευρωπαϊκής Ένωσης**

- Οδηγία 87/102/ΕΟΚ του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

- Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη.

- Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision -ONP).

- Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.

- Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών

- Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.

- Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

- Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

- Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).

- Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση). 87

- Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).

- Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο).

- Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας).

- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον

τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

- Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

· **Αποφάσεις**

- Η Υπουργική Απόφαση με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».

- Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr»

- Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002 - «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής»