ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

Σχολή Διοίκηση και Οικονομίας

Παράρτημα Πύργου

Τμήμα Πληροφορικής και ΜΜΕ

«ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ»

Επιμέλεια Εργασίας: Λασηθιωτάκη Φανή

Επιβλέπων Καθηγητής: Δρ. Δρόσος Λάμπρος

2015

Θα ήθελα ιδιαίτερα να ευχαριστήσω τους γονείς μου, που με βοήθησαν και στήριξαν τόσο πολύ στις επιλογές μου και στην όλη προσπάθεια να τελειώσω επιτυχώς αυτήν την σχολή, τον Κ. Λάμπρο Δρόσο που χωρίς την αμέριστη βοήθεια του δεν θα είχα καταφέρει τίποτε καθώς και την αδερφή μου και τους φίλους μου που με βοήθησαν οχι μόνο ψυχολογικά αλλα και πνευματικά.

Περίληψη

Η σημερινή εποχή χαρακτηρίζεται από συνεχιζόμενες εξελίξεις και τεχνολογικές καινοτομίες με αποτέλεσμα το Διαδίκτυο και η Ευρυζωνικότητα να έχει διεισδύσει στην καθημερινή ζωή του μεγαλύτερου μέρους του πληθυσμού, ολόκληρου του πλανήτη. Το συγκεκριμένο «εργαλείο», πέρα από τα ποικίλα οφέλη που χαρίζει απλόχερα στους χρήστες του, ενέχει και ορισμένους κινδύνους, όπως αυτό του ηλεκτρονικού εγκλήματος (e-crime) ή κυβερνο-εγκλήματος (cyber crime).

Η παρούσα εργασία πραγματεύεται την έννοια του ηλεκτρονικού εγκλήματος, αφού πρώτα γίνει μια αναφορά στο εργαλείο Διαδίκτυο και στην έννοια του εγκλήματος εν γένει. Έπειτα ορίζεται το ηλεκτρονικό έγκλημα και πως αυτό έχει εξελιχθεί στις διάφορες μορφές του, και τέλος, αφού παρουσιαστεί η ελληνική νομοθεσία σχετικά με το ηλεκτρονικό έγκλημα και η υπηρεσία της Δίωξης Ηλεκτρονικού Εγκλήματος, παρουσιάζονται μερικά από τα πλέον γνωστά ηλεκτρονικά εγκλήματα στην ελληνική επικράτεια. Στο τελευταίο κομμάτι της εργασίας, παρουσιάζονται συνοπτικά οι τρόποι με τους οποίους μπορεί ο κάθε χρήστης να προστατευθεί από τα ηλεκτρονικά εγκλήματα, αλλά και το πώς ο ίδιος σα μεμονωμένος, ανεξάρτητος χρήστης μπορεί να συμβάλλει στην καταπολέμηση του.

Abstract

The present era is characterized by the ongoing technological developments and innovations resulting in Broadband Internet which has infiltrated the daily lives of the majority of the population of the entire planet. This tool (internet), apart from the various benefits that generously offers to the users, holds certain risks, such as electronic crime (e-crime) or cyber crime (cyber crime).

This paper discusses the concept of e-crime, having first become a reference tool on the Internet (1st Chapter) and the concept of crime (2nd Chapter) in general. The third section is designated to cyber crime and how it has evolved in different forms, while the fourth chapter presented after the Greek legislation on cybercrime and the service of Cyber Crime, presented some of the most well-known online crimes in the Greek territory. The last chapter summarizes the ways in which each user can be protected from online crime, but also how he, as a single, independent user can contribute to the fight.

Πίνακας Περιεχομένων

Ευρετήριο Πινάκων

Εισαγωγή

Η εξέλιξη της τεχνολογίας σήμερα και η ανάπτυξη της πληροφορικής και ιδιαίτερα των δικτύων των υπολογιστών έχουν φέρει σημαντικές αλλαγές στην καθημερινότητα των ατόμων. Η χρήση του Διαδικτύου έχει βρει ευρεία εφαρμογή σε διάφορους τομείς όπως το εμπόριο, η παραγωγή, οι οικονομικές συναλλαγές επιχειρήσεων, ατόμων και δημόσιου τομέα. Σημαντικές αλλαγές έχουν επίσης συντελεστεί στην εκπαίδευση, στον τρόπο ψυχαγωγίας, ακόμα και στον τρόπο σκέψης και ζωής των ανθρώπων, λόγω των παραπάνω εξελίξεων.

Το διαδίκτυο αποτελεί ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, στο οποίο οι άνθρωποι μπορούν να προσχωρήσουν και να χρησιμοποιήσουν ποικίλες υπηρεσίες όπως η εξεύρεση, αξιοποίηση και διανομή πληροφοριών[1].

Η ραγδαία εξάπλωση του Διαδικτύου, εκτός από τις θετικές επιπτώσεις που έφερε στη ζωή των ατόμων, εμφανίζει ταυτόχρονα αρκετά μειονεκτήματα, σημαντικά προβλήματα και δυσχερείς καταστάσεις. Στα πλαίσια αυτών των αλλαγών σημειώνεται ότι η εξέλιξη του διαδικτύου επέφερε σημαντικές αλλαγές, οι οποίες έχουν ευνοήσει την ανάπτυξη διαφόρων μορφών εγκληματικότητας. Οι μορφές αυτές της ηλεκτρονικής εγκληματικότητας πλέον έχουν θεσμοθετηθεί με τον όρο «Ηλεκτρονικό Έγκλημα».

Ως ηλεκτρονικό έγκλημα - όρος ο οποίος αποτελεί και αντικείμενο μελέτης της παρούσας εργασίας - θεωρούνται όλες εκείνες οι αξιόποινες πράξεις εγκλήματος που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων[2]. Οι συγκεκριμένες ενέργειες, οι οποίες χωρίζονται σε εγκλήματα που τελούνται με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime) τιμωρούνται από συγκεκριμένες ποινές[3].

---

[1] Cyberthetics, (2013), «Τι είναι το Διαδίκτυο», Διαθέσιμο ηλεκτρονικά: http://www.cyberethics.info/cyethics1/index.php?option=com_content&view=article&id=158&Itemid=66&lang=el, ανακτήθηκε στις 28/8/2014

[2] Internet και Ηλεκτρονικό Έγκλημα (2007), Διαθέσιμο ηλεκτρονικά: http://dide.flo.sch.gr/Plinet/Tutorials/Internet-ElectronicCrime-LionHeart.pdf, ανακτήθηκε στις 28/08/2014

[3] Internet και Ηλεκτρονικό Έγκλημα (2007), Διαθέσιμο ηλεκτρονικά: http://dide.flo.sch.gr/Plinet/Tutorials/Internet-ElectronicCrime-LionHeart.pdf, ανακτήθηκε στις 28/08/2014

Το ηλεκτρονικό έγκλημα εντοπίστηκε γύρω στη δεκαετία του 1970, στις τεχνολογικά αναπτυγμένες χώρες, ενώ λίγο αργότερα επεκτάθηκε και στις αναπτυσσόμενες χώρες με ταχύτατους ρυθμούς. Στα ηλεκτρονικά εγκλήματα, οι ηλεκτρονικοί υπολογιστές χρησιμοποιούνται με ποικίλους τρόπους (πχ για να τελεστεί η εγκληματική πράξη ή οι ίδιοι γίνονται το προσβαλλόμενο αντικείμενο της ηλεκτρονικής πράξης).

Τα παραπάνω συντέλεσαν στη δημιουργία επιτακτικής ανάγκης θεσμοθέτησης νόμων ως προς την ορθή και έννομη λειτουργία των υπολογιστών και του διαδικτύου. Μετά το 1980, όπου και η εξάπλωση πλέον του ηλεκτρονικού εγκλήματος ήταν ευρεία, ξεκίνησαν οι πρώτες εμπεριστατωμένες νομικές και εγκληματολογικές προσεγγίσεις ως προς τη νέα αυτή μορφή εγκληματικότητας.

Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και δη του διαδικτύου συνεχώς αυξάνονται με γεωμετρική πρόοδο. Για την αντιμετώπιση του κινδύνου αυτού, απαραίτητη ήταν η διακρατική συνεννόηση και η σχεδίαση μια συνολικής αναλυτικής και αποτελεσματικής στρατηγικής. Το παραπάνω επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα, το οποίο διεκπεραιώθηκε το 2001 στη Βουδαπέστη. Τα συμπεράσματα του καταγράφηκαν στη Συνθήκη της Βουδαπέστης, η οποία και υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου, το Νοέμβριο του ίδιου έτους από 26 Υπουργούς ευρωπαϊκών κρατών μεταξύ των οποίων και από τον τότε Έλληνα Υπουργό.

Αναφορικά με τις μορφές του ηλεκτρονικού εγκλήματος που έχουν παρουσιαστεί και εξιχνιαστεί στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, αυτές κυρίως αφορούν τις παρακάτω:

1. Απάτες μέσω Διαδικτύου
2. Παιδική Πορνογραφία
3. Cracking και Hacking
4. Διακίνηση – πειρατεία λογισμικού
5. Πιστωτικές κάρτες
6. Διακίνηση ναρκωτικών
7. Εγκλήματα σε ομάδες συζητήσεων (chat rooms)

Τα Ηλεκτρονικά Εγκλήματα απαιτούν σημαντικά μέτρα προστασίας, όχι μόνο από την Πολιτεία και το Κράτος, αλλά και από τους ίδιους τους χρήστες, οι οποίοι θα πρέπει να χρησιμοποιούν προληπτικά μέτρα προστασίας, προκειμένου να προφυλάσσονται από κινδύνους, παράνομες εισβολές και ενέργειες που μπορούν να τους βλάψουν σε οποιοδήποτε επίπεδο της ζωής τους. Ιδιαίτερα προστατευμένα πρέπει να είναι τα ανήλικα άτομα και τα μικρά παιδιά τα οποία ενδέχεται να εκτεθούν σε απρεπές υλικό, πορνογραφικού ή εν γένει προσβλητικού περιεχομένου ή να έρθουν σε επαφή με ανθρώπους που μπορούν να τους βλάψουν.

Σκοπός της παρούσας εργασίας είναι η διερεύνηση του όρου «Ηλεκτρονικό Έγκλημα», ποιος είναι ο τρόπος που εκδηλώνεται αυτή η μορφή εγκληματικότητας, ποιες είναι οι συνέπειες και ποιοι οι τρόποι αντιμετώπισης του.

Αναλυτικότερα, στο πρώτο κεφάλαιο παρουσιάζεται το διαδίκτυο και η ιστορική του εξέλιξη στην πορεία των χρόνων. Έπειτα, μέσα από δευτερογενή δεδομένα, παρουσιάζεται ο βαθμός διείσδυσης της τεχνολογίας του διαδικτύου στην καθημερινή ζωή των Ελλήνων, ενώ παράλληλα καταλήγει με μια σύντομη αναφορά στα πλεονεκτήματα και τα μειονεκτήματα που προκύπτουν από τη χρήση αυτού.

Το δεύτερο κεφάλαιο της παρούσας μελέτης, πραγματεύεται την έννοια του εγκλήματος γενικότερα, ενώ ο όρος αυτός τοποθετείται χρονολογικά μέσα στην ιστορία των λαών και παρουσιάζεται μέσω αυτού η εξέλιξη του. Έπειτα, γίνεται μια σύντομη αναφορά στο Ποινικό Δίκαιο και τον κλάδο της Εγκληματολογίας, αναφέροντας τους τρόπους όπου η Πολιτεία αντιμετωπίζει μέσω των θεσμοθετημένων κανόνων της, τις πράξεις των εγκλημάτων.

Το τρίτο κεφάλαιο αποτελείται από ενότητες αναφορικά με το Ηλεκτρονικό Έγκλημα, όπου αποτελεί και το αντικείμενο μελέτης της συγκεκριμένης εργασίας. Ειδικότερα, δίδεται στον αναγνώστη ο εννοιολογικός προσδιορισμός του ηλεκτρονικού εγκλήματος και παρουσιάζεται η ιστορική του εξέλιξη ξεκινώντας από το «πρώτο» ηλεκτρονικό έγκλημα. Στη συνέχεια, αναλύονται οι βασικές μορφές του ηλεκτρονικού εγκλήματος (παιδική πορνογραφία, πειρατεία λογισμικού, παραβίαση προσωπικών δεδομένων, μορφές ηλεκτρονικού οικονομικού εγκλήματος, spamming, hacking, διαδικτυακή τρομοκρατία).

Το τέταρτο κεφάλαιο πραγματεύεται την περίπτωση του ηλεκτρονικού εγκλήματος στην ελληνική πραγματικότητα βάσει της κείμενης νομοθεσίας. Δηλαδή, αναλύει τι συμβαίνει στην ελληνική νομοθεσία σχετικά με το ηλεκτρονικό έγκλημα και παρουσιάζει την Υπηρεσία Δίωξης ηλεκτρονικού εγκλήματος και το πώς αυτή ενεργεί στην περίπτωση κάποιου τέτοιου είδους εγκλήματος.

Τέλος το κεφάλαιο 5^{ο}, αναφέρει τους τρόπους προστασίας στο διαδίκτυο και τους τρόπους αποφυγής μετατροπής του χρήστη των υπηρεσιών του διαδικτύου σε θύμα ηλεκτρονικού εγκλήματος.

Το Διαδίκτυο

1.1 Διαχρονική Εξέλιξη

Το Διαδίκτυο έχει επιφέρει επανάσταση στον κόσμο των υπολογιστών και των επικοινωνιών, εν γένει όσο τίποτα άλλο μέχρι σήμερα. Το διαδίκτυο είναι μια τεχνολογία που συμβάλλει στην παγκόσμια επικοινωνία, καθώς αποτελεί έναν μηχανισμό για διασπορά πληροφοριών και ένα μέσο για συνεργασία και αλληλεπίδραση ανάμεσα σε ιδιώτες και τους υπολογιστές τους χωρίς να αποτελεί εμπόδιο η γεωγραφική τοποθεσία.

Διαδίκτυο ονομάζουμε το παγκόσμιο δίκτυο που συνδέει μεταξύ τους ηλεκτρονικούς υπολογιστές σε όλα τα μήκη και τα πλάτη του πλανήτη, παρέχοντας στους χρήστες του σημαντικές υπηρεσίες και πληροφορίες. Σήμερα, χρησιμοποιούν το διαδίκτυο περισσότερο από 1 δισεκατομμύριο άνθρωποι, οι οποίοι αναζητούν σε αυτό πληροφορίες από σημεία που ονομάζονται δικτυακοί τόποι (web sites). Η διεκπεραίωση επαγγελματικών και προσωπικών συναλλαγών, η εκπαίδευση, η ενημέρωση, η ψυχαγωγία και η επικοινωνία, είναι μόνο μερικές από τις ενέργειες στις οποίες κάποιος μπορεί να προβεί με τη χρήση του διαδικτύου[4].

Αναφορικά με τον τομέα της εκπαίδευσης, το διαδίκτυο μπορεί να συμβάλλει στην εύρεση πληροφοριών και ερευνητικού/εκπαιδευτικού υλικού από τα άτομα, στην ενημέρωση για προγράμματα διδασκαλίας, ακόμα και σε εξ αποστάσεως σπουδές. Μέσω του διαδικτύου, ο χρήστης μπορεί να έχει πρόσβαση σε βιβλιοθήκες και περιοδικά παγκόσμιου ενδιαφέροντος (επιστημονικού και μη), γεγονός που

[4] ΕΕΤΤ (2006), «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, «Το Διαδίκτυο και Εγώ», διαθέσιμο ηλεκτρονικά: http://www.eett.gr/opencms/export/sites/default/admin/downloads/Informative_Documentation/Διαδίκτυο_and_Me.pdf)

αυξάνει κατά πολύ το εκπαιδευτικό επίπεδο των ατόμων όπου κι αν αυτά βρίσκονται. Πέρα από ένα ανοιχτό σχολείο για όλους, το Διαδίκτυο αποτελεί και μια ανοιχτή πλατφόρμα εργασίας και καριέρας για όλους. Σε αυτό μπορεί κανείς να αναζητήσει θέματα σχετικά με τα παραπάνω, αλλά και νομικά θέματα και θέματα κοινωνικής ασφάλισης.

Οι πρώτες απόπειρες για την δημιουργία διαδικτύου ξεκίνησαν στις ΗΠΑ κατά την διάρκεια του Ψυχρού Πολέμου και μετά την επιτυχημένη αποστολή στο διάστημα τον δορυφόρο Σπούτνικ 1 από τη Ρωσία. Θέλοντας η Αμερική λοιπόν, να προστατευτεί από μια πιθανή επίθεση των Ρώσων δημιούργησε την υπηρεσία προηγμένων αμυντικών ερευνών ARPA (Advanced Research Project Agency) γνωστή ως DARPA (Defense Advanced Research Projects Agency) σκοπός της οποίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργήσουν ένα δίκτυο επικοινωνίας και προστασίας[5]. Το παραπάνω ήταν η απαρχή του διαδικτύου, το οποίο όμως καθυστέρησε να πάρει τη σημερινή του μορφή και να χρησιμοποιηθεί από ένα ευρύ κοινό όπως αυτό γίνεται σήμερα[6].

Αξίζει να σημειωθεί ότι το Διαδίκτυο αποκτά μια μαζικότητα ως φαινόμενο τη δεκαετία του 1990[7]. Το 1974, οι επιστήμονες της ARPA, εργαζόμενοι από κοινού με ειδικούς στο Stanford, ανέπτυξαν μια κοινή γλώσσα που θα επέτρεπε σε διαφορετικά δίκτυα να επικοινωνούν μεταξύ τους. Αυτό έγινε γνωστό με τον όρο transmission control protocol/Διαδίκτυο protocol, το πασίγνωστο σήμερα CP/IP. Η ανάπτυξη του TCP/IP ήταν ένα σημαντικό στάδιο στην ανάπτυξη της δικτύωσης και αξίζει να επικεντρωθούμε στις επιπτώσεις που υπήρξαν στις έννοιες της σχεδίασης (design concepts). Αν και το 1974 σημάδεψε το ξεκίνημα του TCP/IP, θα χρειάζονταν αρκετά χρόνια τροποποιήσεων και επανασχεδίασης πριν ολοκληρωθεί και γίνει παγκοσμίως αποδεκτό.

Την ίδια χρονιά το Stanford δημιούργησε το Telnet, την πρώτη δημόσια ευρέως αποδεκτή υπηρεσία πακέτου δεδομένων (packet data service), μια εμπορική

[5]Βικιπαίδεια (2013), «Το Διαδίκτυο», διαθέσιμο ηλεκτρονικά: http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

[6] Βλαχόπουλος Κ (χ.χ.), Υποψήφιος Διδάκτωρ Τμήματος Πληροφορικής Ιονίου Πανεπιστημίου, «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-crime.gr/301.pdf, Ανακτήθηκε στις 23/09/2013

[7] Λέανδρος (2005), «Το διαδίκτυο: ανάπτυξη και αλλαγή»

παραλλαγή του ARPANET. Αργότερα, το 1979 καθιερώθηκε το Usenet, το οποίο ήταν ένα ανοικτό σύστημα επικεντρωμένο στην επικοινωνία με e-mail και αφιερωμένο στις ομάδες ειδήσεων (newsgroups) και που βρίσκεται ακόμα και σήμερα σε πλήρη ανάπτυξη. Το Usenet εμφανίσθηκε στο τέλος του 1979, αμέσως μετά την εμφάνιση του V7 Unix με το πρωτόκολλο UUCP. Δύο απόφοιτοι σπουδαστές του Πανεπιστημίου του Duke στην Βόρεια Καρολίνα, ο Tom Truscott και ο Jim Ellis, σκέφθηκαν τη σύνδεση των υπολογιστών μεταξύ τους για την ανταλλαγή πληροφοριών με την κοινότητα του UNIX.

Το Μάρτιο του 1986 διανεμήθηκε ένα πακέτο που υλοποιούσε την αποστολή των ειδήσεων, τη δημοσίευσή τους και την ανάγνωσή τους χρησιμοποιώντας το πρωτόκολλο NNTP (Network News Transfer Protocol), όπως ορίσθηκε στο RFC 977. Αυτό το πρωτόκολλο δίνει τη δυνατότητα στους hosts να ανταλλάσσουν άρθρα (articles) μέσω TCP/IP συνδέσεων παρά να χρησιμοποιούν το παραδοσιακό uucp. Επιτρέπει επίσης στους χρήστες να διαβάζουν και να στέλνουν (δημοσιεύουν) ειδήσεις (news), χρησιμοποιώντας έναν τροποποιημένο news user agent, από μηχανήματα που δεν έχουν εγκατεστημένο το λογισμικό για USENET news[8].

Σημαντικό σημείο ανάπτυξης στην πορεία του Διαδικτύου ήταν η εισαγωγή το 1984 των DNS (Domain Name Servers). Μέχρι τότε ο κάθε host υπολογιστής είχε εκχωρημένο ένα όνομα και υπήρχε μια μοναδική λίστα ονομάτων και διευθύνσεων την οποία μπορούσε εύκολα να συμβουλευθεί ο καθένας. Το νέο σύστημα εισήγαγε μερικά επιθέματα στις διευθύνσεις Διαδίκτυο των ΗΠΑ, όπως edu (educational), com. (Commercial), Gov. (governmental) εκτός από την org. (international organization) και μια σειρά από κωδικούς κρατών. Το παραπάνω συνετέλεσε ώστε τα ονόματα των host υπολογιστών να είναι πιο ευκολομνημόνευτα[9].

Το 1984 η βρετανική κυβέρνηση ανακοίνωσε τη δημιουργία του JANET (Joint Academic Network) για την εξυπηρέτηση των βρετανικών ενώ, το επόμενο έτος, το US National Science Foundation καθιέρωσε το NSFNet για τον ίδιο σκοπό.

Σήμερα, παρατηρείται μια άνευ προηγουμένου διείσδυση του Διαδικτύου στη ζωή των ατόμων. Συγκεκριμένα, ΕΕ27, στα νοικοκυριά με σύνδεση στο διαδίκτυο, το ποσοστό των νοικοκυριών με ευρυζωνική σύνδεση έφτασε στο 80% το

[8] Βλαχόπουλος Κ (χ.χ.), Υποψήφιος Διδάκτωρ Τμήματος Πληροφορικής Ιονίου Πανεπιστημίου, «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-crime.gr/301.pdf, Ανακτήθηκε στις 23/09/2013

[9] Αγγελής Ι. (2000), «Διαδίκτυο (Διαδίκτυο) και ποινικό δίκαιο. Έγκλημα στον κυβερνοχώρο», Ποινικά Χρονικά, σελ. 675 επ., Εκδ. Δίκαιο και Οικονομία, Π.Ν. Σάκκουλας·

2008 (από 48% το 2005) και το ποσοστό των πολιτών που χρησιμοποίει συχνά το διαδίκτυο (σχεδόν κάθε μέρα) αυξήθηκε από 29% στο 43% την ίδια περίοδο. Αντίστοιχα στην Ελλάδα, στα νοικοκυριά με σύνδεση στο διαδίκτυο το ποσοστό των νοικοκυριών με ευρυζωνική σύνδεση αυξήθηκε κατά 51,7% (από 7,3% το 2005 σε 59% το 2008) και το ποσοστό των πολιτών που χρησιμοποιεί συχνά το διαδίκτυο (σχεδόν κάθε μέρα) αυξήθηκε από 11% σε 26% την ίδια περίοδο[10] .

1.2 Η διείσδυση του Διαδικτύου στην καθημερινή ζωή των ατόμων στην Ελλάδα

Από την ανάλυση των στοιχείων της έρευνας i2010 στα νοικοκυριά για την ΕΕ27, προκύπτει ότι το ποσοστό των Ευρωπαίων πολιτών που χρησιμοποιεί διαδικτυακές υπηρεσίες έχει αυξηθεί σημαντικά κατά την περίοδο 2005-2008 με τη μεγαλύτερη αύξηση (11%) να παρατηρείται στο ποσοστό των Ευρωπαίων πολιτών που χρησιμοποιεί το διαδίκτυο για ηλεκτρονικό ταχυδρομείο (53% το 2008), όπως επίσης και για ανεύρεση πληροφοριών για αγαθά και υπηρεσίες (50% το 2008). Το ποσοστό των πολιτών που κάνουν τραπεζικές συναλλαγές μέσω διαδικτύου έχει αυξηθεί κατά 10%, ενώ η χρήση άλλων λιγότερο δημοφιλών υπηρεσιών για τις οποίες απαιτούνται περισσότερες δεξιότητες στη χρήση διαδικτύου έχει επίσης διευρυνθεί, με το ποσοστό πολιτών που τις χρησιμοποιούν να έχει αυξηθεί κατά 6-8% την περίοδο 2005-2008[11] .

Τα τελευταία δέκα χρόνια, το διαδίκτυο έχει πραγματικά διεισδύσει στη ζωή μας, καθώς είναι εκπληκτικό το γεγονός ότι το 2003, μόλις το 9,1% του παγκόσμιου πληθυσμού είχε πρόσβαση στο διαδίκτυο, ενώ το αντίστοιχο ποσοστό το 2012,

---

[10] Κουντζέρης (2010), «Νέες τάσεις στη χρήση του διαδικτύου για επικοινωνία, πληροφόρηση και ψυχαγωγία», Ηλεκτρονικά διαθέσιμο: http://www.observatory.gr/files/meletes/E-WEBTRENDS_TX_%CE%A4%CE%AC%CF%83%CE%B5%CE%B9%CF%82%20%CF%83%CF%84%CE%B7%20%CF%87%CF%81%CE%AE%CF%83%CE%B7%20%CF%84%CE%BF%CF%85%20%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85.pdf

[11] Κουντζέρης (2010), «Νέες τάσεις στη χρήση του διαδικτύου για επικοινωνία, πληροφόρηση και ψυχαγωγία», Ηλεκτρονικά διαθέσιμο: http://www.observatory.gr/files/meletes/E-WEBTRENDS_TX_%CE%A4%CE%AC%CF%83%CE%B5%CE%B9%CF%82%20%CF%83%CF%84%CE%B7%20%CF%87%CF%81%CE%AE%CF%83%CE%B7%20%CF%84%CE%BF%CF%85%20%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85.pdf

ξεπερνούσε το 33%. Αδιαμφισβήτητος είναι λοιπόν, ο ρόλος που διαδραματίζει στην καθημερινή ζωή των ατόμων το Διαδίκτυο, καθώς συνδέεται άρρηκτα με διάφορες καθημερινές δραστηριότητες όλων των τομέων της ζωής του. Είναι χαρακτηριστική η διείσδυση αυτού του μέσου στη ζωή των ατόμων σε σημείο μάλιστα που πολλές φορές την επηρεάζει σε μεγάλο βαθμό και «κρίνει» πλήθος επιλογών[12].

Το 2010, το 50% των Ελλήνων δήλωσαν ότι χρησιμοποιούν Ηλεκτρονικό υπολογιστή και το 44% ότι χρησιμοποιεί το διαδίκτυο. Σημαντικό μέρος αυτών χρησιμοποιούν το διαδίκτυο μέσω υπηρεσιών 3ης γενιάς (3G Δίκτυα) είτε μέσω κινητού τηλεφώνου ή κάποιας σύνδεσης υπολογιστή. Η πρόσβαση στο διαδίκτυο για τους περισσότερους γίνεται από το σπίτι (περίπου το 86%), ενώ το 36,9% των ατόμων έχει πρόσβαση στο διαδίκτυο από το χώρο εργασίας του. Σύμφωνα με στοιχεία της ίδιας έρευνας, ανάλογα με την ηλικία των χρηστών, οι δραστηριότητες ποικίλλουν. Για παράδειγμα, πληροφορίες αναζητούν τα άτομα μεταξύ 25-34 και 35-44 ετών, ενώ τα άτομα μικρότερης ηλικίας αποστέλλουν κυρίως μηνύματα είτε μέσω mail, είτε μέσω σελίδων κοινωνικής δικτύωσης (Πίνακας 1). Η έρευνα τέλος αναδεικνύει συχνότερους χρήστες του Διαδικτύου τους άντρες μικρότερων ηλικιών που έχουν υψηλό μορφωτικό επίπεδο και κατοικούν σε μεγάλα αστικά κέντρα[13].

Πίνακας 1 – Δραστηριότητες χρηστών διαδικτύου ανά ηλικία

ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ανά ηλικία (% χρηστών)	16-24	25-34	35-44	45-54	55-74
Αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες	74	84	86	79	76
Αποστολή/ λήψη ηλεκτρονικού ταχυδρομείου (e-mail)	75	76	72	68	62
Ανάγνωση εφημερίδων / περιοδικών	46	59	62	64	58
Υπηρεσίες ταξιδίων/ διαμονής	46	63	64	57	52
Αναζήτηση πληροφοριών για θέματα υγείας	38	52	58	55	49
Αποστολή μυνημάτων σε σελίδες κοινωνικής δικτύωσης (facebook, blogs, chat sites), instant messaging	72	53	35	22	18
Κατέβασμα παιχνιδιών, εικόνων, μουσικής, ταινιών	58	45	33	26	19
Web ραδιόφωνο / web τηλεόραση	50	43	36	30	20
Συναλλαγή με δημόσιες υπηρεσίες	14	31	37	41	38
Τηλεφωνία, βιντεοκλήσεις	32	18	18	18	13
Δημιουργία περιεχομένου που και ανάρτησή του για κοινή χρήση	30	23	19	13	10
Για Τραπεζικές συναλλαγές	6	15	15	17	17
Αναζήτηση εργασίας / αίτηση για δουλειά	18	20	10	6	1
Για Πώληση αγαθών ή υπηρεσιών (π.χ. μέσω δημοπρασιών)	0	2	2	1	0

Πηγή:
http://www.observatory.gr/files/meletes/A100526_%CE%A0%CF%81%CE%BF%CF%86%CE%AF%CE%BB%20%CF%87%CF%81%CE%B7%CF%83%CF%84%CF%8E%CE%BD%20Διαδίκτυο%202010.pdf

[12] Βλαχόπουλος Κ (χ.χ.), Υποψήφιος Διδάκτωρ Τμήματος Πληροφορικής Ιονίου Πανεπιστημίου, «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-crime.gr/301.pdf, Ανακτήθηκε στις 23/09/2013

[13] Παρατηρητήριο για την Κοινωνία της πληροφορίας (2011), «Η χρήση του διαδικτύου από του Έλληνες»

Ο ρυθμός αύξησης σε επίπεδο χρήσης των παραδοσιακών διαδικτυακών υπηρεσιών από τους Έλληνες πολίτες την περίοδο 2005-2008, είναι συγκρίσιμος με τον αντίστοιχο Ευρωπαϊκό για όλες τις υπηρεσίες, με εξαίρεση τις υπηρεσίες για παραγγελία/αγορά αγαθών/υπηρεσιών για προσωπική χρήση και τις τραπεζικές συναλλαγές μέσω διαδικτύου, για τις οποίες τα ποσοστά των Ελλήνων πολιτών που τις χρησιμοποιούν αυξήθηκαν μόλις κατά 3% και 2% αντίστοιχα την τελευταία τετραετία. Ο ρυθμός αύξησης σε επίπεδο χρήσης των διαφορετικών διαδικτυακών υπηρεσιών από τους Έλληνες πολίτες την περίοδο 2005-2008 όμως δεν θεωρείται ικανοποιητικός, δεδομένου ότι θα έπρεπε να είναι μεγαλύτερος από τον αντίστοιχο ευρωπαϊκό προκειμένου να επιτευχθεί σύγκλιση[14].

Σύμφωνα με έρευνα το ΙΟΒΕ, το 2011 υπήρχε μια ταχεία διάδοση του διαδικτύου στην Ελλάδα, η οποία όμως ήταν αρκετά χαμηλότερη σε σχέση με αυτή που συναντούσε κανείς στην υπόλοιπη Ευρώπη. Το προφίλ του διαδικτυακού χρήστη είναι στην πλειοψηφία του άτομα ηλικίας μεταξύ 16-24 ετών, με υψηλό επίπεδο μόρφωσης και εισόδημα άνω των 75.000 ευρώ, ενώ υπάρχει μια μεγαλύτερη χρήση του από κατοίκους αστικών περιοχών[15].

[14] Κουντζέρης (2010), «Νέες τάσεις στη χρήση του διαδικτύου για επικοινωνία, πληροφόρηση και ψυχαγωγία», Ηλεκτρονικά διαθέσιμο: http://www.observatory.gr/files/meletes/E-WEBTRENDS_TX_%CE%A4%CE%AC%CF%83%CE%B5%CE%B9%CF%82%20%CF%83%CF%84%CE%B7%20%CF%87%CF%81%CE%AE%CF%83%CE%B7%20%CF%84%CE%BF%CF%85%20%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85.pdf

[15] Τσακανίκας Α. (2013), «Το Διαδίκτυο στην Ελλάδα: Εμπόδια και Προοπτικές», διαθέσιμο ηλεκτρονικά: http://www.iobe.gr/media/Hmerides/iobeGooglepresentationfinal.pdf

Την ίδια χρονιά (2011) παρατηρήθηκε αξιοσημείωτη απήχηση στα κοινωνικά δίκτυα, όπου το ποσοστό των Ελλήνων που τα χρησιμοποιούσαν διαμορφώθηκε στο 36%, αυξημένο κατά 22 μονάδες συγκριτικά με την προηγούμενη χρονιά[16]. Βέβαια, παρόλα αυτά, έρευνα του ΙΟΒΕ που δημοσιεύθηκε στις αρχές του τρέχοντος έτους αναδεικνύει ότι η τεχνολογική σύγκλιση της Ελλάδας με την υπόλοιπη Ευρώπη εξελίσσεται με αργούς ρυθμούς, πιθανότατα λόγω και της οικονομικής κρίσης που βιώνει η χώρα[17].

1.3 Πλεονεκτήματα & Μειονεκτήματα της χρήσης του Διαδικτύου

Στην παρούσα ενότητα θα προσπαθήσουμε να προσεγγίσουμε με διάφορους τρόπους τα πλεονεκτήματα και τα μειονεκτήματα του Διαδικτύου, τα οποία βέβαια είναι αρκετά γνωστά ήδη εμπειρικά στο μεγαλύτερο μέρος του πληθυσμού, είτε χρησιμοποιεί το Διαδίκτυο είτε όχι. Ξεκινώντας από τα πλεονεκτήματα του Διαδικτύου, αυτό που μπορεί να σημειωθεί ως ίσως το πλέον δημοφιλές είναι η ταχύτατη και εύκολη επικοινωνία που προσφέρει στους χρήστες του. Μέσω ηλεκτρονικού ταχυδρομείου, μέσω σελίδων κοινωνικής δικτύωσης και ειδικών εφαρμογών επικοινωνίας (SKYPE), μέσω ειδικά διαμορφωμένων ιστοσελίδων επικοινωνίας (instant chat), οι χρήστες μπορούν να επικοινωνήσουν μεταξύ τους, ανεξαρτήτως που βρίσκονται γεωγραφικά μέσα σε λίγα δευτερόλεπτα.

Σημαντικό θετικό χαρακτηριστικό του Διαδικτύου είναι η ταχύτατη διάδοση μιας πληροφορίας, καθώς δίνει στους χρήστες τη δυνατότητα άμεσης πρόσβασης σε πλήθος πληροφοριών, σε εφημερίδες, περιοδικά, συγγράμματα και βιβλία κάθε είδους, πανεπιστήμια, βιβλιοθήκες και οποιαδήποτε άλλη πηγή πληροφορίας σε όλο τον κόσμο, μόνο μέσα σε λίγα δευτερόλεπτα. Το παραπάνω συμβάλλει ουσιαστικά στην εκπαίδευση των ατόμων, καθώς δεν είναι λίγα τα προγράμματα που έχουν σχεδιασθεί ειδικά για την εκπαίδευση των ατόμων ακόμη και εξ αποστάσεως. Αναζητώντας στο Διαδίκτυο, κάποιος χρήστης, ο οποίος βέβαια έχει τις γνώσεις και τις ικανότητες μπορεί να παρακολουθήσει ακόμη και διδακτορικού επιπέδου

[16] ΣΚΑΙ (2011), «Κοινωνία της Πληροφορίας: Αυξάνεται η διείσδυση του Διαδικτύου», Διαθέσιμο ηλεκτρονικά: http://www.skai.gr/news/technology/article/170570/koinonia-tis-pliroforias-auxanetai-i-dieisdusi-tou-idernet/

[17] neolaia.grTeam (2013), «Ελλάδα. Στις τελευταίες θέσεις στη χρήση Διαδίκτυο», διαθέσιμο ηλεκτρονικά: http://www.neolaia.gr/2013/01/29/iove-Διαδίκτυο/#.UhH-5NLHYcY

προγράμματα στην επιστήμη που τον ενδιαφέρει εξ αποστάσεως[18].

Μια αρκετά διαδεδομένη χρήση του Διαδικτύου είναι και το Ηλεκτρονικό Εμπόριο (E-commerce), αλλά και το Ηλεκτρονικό Επιχειρείν (E-Business). Δεν είναι λίγες οι επιχειρήσεις εκείνες που δραστηριοποιούνται μέσω Διαδικτύου και συναλλάσσονται με το καταναλωτικό κοινό και τους πελάτες τους μέσω αυτού, διαθέτοντας σε ειδικά διαμορφωμένες ιστοσελίδες έναν πλήρη κατάλογο προϊόντων και υπηρεσιών. Μάλιστα, λόγω της ευρείας εξάπλωσης του Διαδικτύου, πολλές είναι οι επιχειρήσεις εκείνες που πλέον δε διατηρούν κάποιο φυσικό κατάστημα αλλά αρκούνται στην ηλεκτρονική τους δραστηριοποίηση. Επιπλέον, παρατηρείται αρκετές φορές ότι οι συναλλαγές μέσω Διαδικτύου προσφέρουν στο καταναλωτικό κοινό πολλές περισσότερες επιλογές, συγκριτικά με εκείνες που προσφέρονται στα φυσικά καταστήματα.

Επιπρόσθετα, πλέον πολλές είναι οι δημόσιες υπηρεσίες που έχουν πρόσβαση στο Διαδίκτυο (E-government-Ηλεκτρονική Διακυβέρνηση) και πολλά αιτήματα πολιτών εξυπηρετούνται μέσω αυτών. Το συγκεκριμένο, αν και στη χώρα μας δεν έχει γνωρίσει ακόμη την εξέλιξη που γνωρίζει στην υπόλοιπη Ευρώπη, είναι ιδιαίτερα χρήσιμο, καθώς εξοικονομεί χρόνο για τους πολίτες, βελτιώνει τη φυσική εικόνα των δημόσιων υπηρεσιών, στις οποίες μειώνονται οι ουρές και οι χρόνοι αναμονής και τέλος μπορεί να συμβάλλει αποτελεσματικά στη μείωση της γραφειοκρατίας, φαινομένου που αποτελεί μάστιγα για την ελληνική δημόσια διοίκηση. Γενικότερα μπορούμε να συνοψίσουμε τα πλεονεκτήματα του διαδικτύου (ειδικότερα για την Ελλάδα) ως εξής[19]:

- Εύκολη και γρήγορη επικοινωνία αμφίδρομης μορφής
- Άμεση και έγκαιρη ενημέρωση
- Ποικιλία πληροφοριών
- Διευκόλυνση οποιουδήποτε είδους συναλλαγών
- Μείωση και καταπολέμηση της γραφειοκρατίας
- Συμβολή στην εκπαίδευση και τη μόρφωση των ατόμων
- Προαγωγή της επιστημονικής έρευνας και τη διάχυση της γνώσης

[18] Βλαχόπουλος Κ (χ.χ.), Υποψήφιος Διδάκτωρ Τμήματος Πληροφορικής Ιονίου Πανεπιστημίου, «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-crime.gr/301.pdf, Ανακτήθηκε στις 23/09/2013

[19] Αγγελής Ι. (2000), «Διαδίκτυο (Διαδίκτυο) και ποινικό δίκαιο. Έγκλημα στον κυβερνοχώρο», Ποινικά Χρονικά, σελ. 675 επ., Εκδ. Δίκαιο και Οικονομία, Π.Ν. Σάκκουλας·

Τέλος το διαδίκτυο, ειδικότερα για την χώρα μας (αλλά και για τις υπόλοιπες) μπορεί να συμβάλλει ουσιαστικά στην οικονομία της χώρας και να αποτελέσει σημαντικό μοχλό ανάπτυξης. Συγκεκριμένα, το διαδίκτυο μπορεί να βελτιώσει τη διαφάνεια στις οικονομικές συναλλαγές μεταξύ ιδιωτών και επιχειρήσεων, ενώ αντίστοιχα μπορεί να αποτελέσει στοιχείο εξοικονόμησης χρόνου και χρημάτων για τους καταναλωτές. Είναι σημαντική η συμβολή του επίσης, ως προς τις επιχειρήσεις, τις οποίες μπορεί να βοηθήσει να επιτύχουν τους στόχους τους και να προωθήσει την απασχόληση. Το διαδίκτυο μπορεί να αποτελέσει τον κατάλληλο συνδετικό κρίκο, μεταξύ καταναλωτών και επιχειρήσεων.

Παρ' όλα αυτά πολλές ελληνικές επιχειρήσεις ακόμη διστάζουν να αξιοποιήσουν το Διαδίκτυο και να επεκτείνουν την πελατειακή τους βάση, μετασχηματίζοντας ταυτόχρονα τον τρόπο λειτουργίας τους. Αξίζει να σημειωθεί ότι ενώ η Ελλάδα δεν έχει ακόμη αξιοποιήσει το διαδίκτυο στο μέγιστο δυνατό βαθμό, η άμεση συμβολή του στην ελληνική οικονομία υπολογίζεται στα 2,7 δις ευρώ ή διαφορετικά στο 1,2% του συνολικού ελληνικού ΑΕΠ για το 2010. Τα πολλαπλά οφέλη του για την οικονομία μπορούν να συνοψισθούν ως προς την αξία των αγαθών και ως προς τη διαφήμιση τους μέσω διαδικτύου[20].

Αναφορικά με τα μειονεκτήματα που συγκεντρώνει το διαδίκτυο, μπορούμε να πούμε ότι θα μπορούσαν να μην ήταν τόσο επιβλαβή, όσο μπορούν να αποδειχθούν τώρα σε περίπτωση που υπήρχε η σωστή παιδεία των χρηστών. Αρχικά, αξίζει να αναφερθούμε στο γεγονός ότι πλήθος πληροφοριών που διαχέονται καθημερινά στο διαδίκτυο δεν είναι αληθείς και πολλές φορές παραπλανούν τους χρήστες. Για το λόγο αυτό, κάθε πληροφορία που μας ενδιαφέρει πρέπει να ελέγχεται πάντα από πλήθος διαφορετικών πηγών (εν προκειμένω sites), των οποίων έχουμε ελέγξει και στο παρελθόν την ακρίβεια και την αξιοπιστία τους.

Ένα επίσης από τα σημαντικά μειονεκτήματα που συγκεντρώνονται στη χρήση του διαδικτύου είναι ότι μειώνεται πολλές φορές η ανθρώπινη προσωπική επαφή και επικοινωνία και δημιουργείται μια εικονική επικοινωνία, ακόμα και με άτομα του άμεσου οικογενειακού και φιλικού περιβάλλοντος. Κάτι τέτοιο μπορεί πολλές φορές να δημιουργήσει ακόμη και παρεξηγήσεις, καθώς η γραπτή επικοινωνία δεν επιτρέπει στα άτομα που συνομιλούν να γνωρίζουν χαρακτηριστικά της επικοινωνίας (πχ. Γλώσσα του σώματος, όπως κινήσεις χεριών, συσπάσεις, εκφράσεις

[20] Αντωνιάδης και συν. (2012), «Παράγων Διαδίκτυο. Το Διαδίκτυο ως μοχλός της ανάπτυξης της ελληνικής οικονομίας», διαθέσιμο ηλεκτρονικά: http://www.bcg.gr/documents/file101711.pdf

προσώπου, τόνο της φωνής και οτιδήποτε άλλο προσδίδει έμφαση στην επικοινωνία και σε αυτό που λέγεται). Δεν είναι λίγες οι φορές που λόγω της άλογης χρήσης του Διαδικτύου πολλά άτομα έχουν οδηγηθεί στην ανάπτυξη μιας «παράλληλης ζωής», η οποία κάθε άλλο παρά σχετική είναι με την πραγματική τους[21].

Η εκτεταμένη χρήση του διαδικτύου έχει δημιουργήσει στην κοινωνία μιας νέας μορφής εξάρτηση, η οποία «αναγκάζει» τα άτομα να ζουν μέσα από έναν υπολογιστή και να δαπανούν μεγάλο μέρος του καθημερινού τους χρόνου σε δραστηριότητες μέσω αυτού και μόνο. Ο υπολογιστής γίνεται αναπόσπαστο μέρος της ζωής και της καθημερινότητας τους με αποτέλεσμα ο εικονικός κόσμος του Διαδικτύου να ταυτίζεται πολλές φορές με τον πραγματικό και να υπάρχουν παρανοήσεις. Ο εθισμός στο διαδίκτυο έχει οδηγήσει πολλά άτομα και κυρίως άτομα νεαρότερης ηλικίας σε ακραίες πράξεις ακόμη και σε παραμέληση βασικών καθημερινών αναγκών, τόσο επιβίωσης, όσο και κοινωνικοποίησης.

Επιπρόσθετα, ένα κακό χαρακτηριστικό της υπερβολικής εξάπλωσης του διαδικτύου και της αλόγιστης χρήσης αυτού είναι το ότι έχει δημιουργηθεί εδώ και μερικά χρόνια ένα νέο είδους εγκλήματος, το ηλεκτρονικό έγκλημα, φαινόμενο που πραγματεύεται η παρούσα εργασία και θα αναλυθεί εκτενώς στη συνέχεια.

Στο σημείο αυτό σημειώνεται ότι το ηλεκτρονικό έγκλημα δεν περιορίζεται μόνο σε ορισμένες πράξεις, αλλά εκτείνεται σε ένα ευρύ φάσμα πράξεων που πολλές φορές φθάνουν στα όρια του κακουργήματος. Οι ηλεκτρονικές απάτες, οι υποκλοπές προσωπικών δεδομένων, ο διαδικτυακός εκφοβισμός, η πορνογραφία (κυρίως παιδική) είναι μόνο μερικές από τις μορφές που έχει πάρει σήμερα το σύγχρονο ηλεκτρονικό έγκλημα. Οι πράξεις αυτές διώκονται ποινικά και φέρουν ποινές ίσες και μεγαλύτερες πολλές φορές των παραδοσιακών εγκλημάτων.

Όλα τα παραπάνω βέβαια μπορούν να μετριαστούν και στην καλύτερη περίπτωση να αφανιστούν, όταν υπάρχει σωστή διαπαιδαγώγηση των ατόμων που χρησιμοποιούν το Διαδίκτυο και μάλιστα των χρηστών μικρότερων ηλικιών. Από την παιδική ήδη ηλικία θα πρέπει ο χρήστης να μυείται στη σωστή χρήση του διαδικτύου το οποίο θα περιορίσει τα αρνητικά φαινόμενα αυτού και θα επαυξήσει τα οφέλη που μπορεί το άτομο να αποκομίσει από μια εύλογη και ορθή χρήση[22].

---

[21] Βλαχόπουλος Κ (χ.χ.), Υποψήφιος Διδάκτωρ Τμήματος Πληροφορικής Ιονίου Πανεπιστημίου, «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-crime.gr/301.pdf, Ανακτήθηκε στις 23/09/2013

[22] Βλαχόπουλος Κ (χ.χ.), Υποψήφιος Διδάκτωρ Τμήματος Πληροφορικής Ιονίου Πανεπιστημίου, «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-

Το Έγκλημα

2.1 Τι είναι το έγκλημα;

Το έγκλημα μπορεί να είναι οποιαδήποτε ενέργεια είναι ενάντια ή παρεκκλίνει από τους κοινά αποδεκτούς κανόνες μιας κοινωνίας. Εγκλήματα διαπράττονταν σε όλες τις κοινωνίες από αρχαιοτάτων χρόνων με διαφορετικές μορφές, αντιμετώπιση, συνέπειες και εκφάνσεις.

Μπορεί να σημειωθεί ότι το έγκλημα είναι συνισταμένη διαφόρων προϋποθέσεων, χωρίς πάντα να είναι ευκρινές ποιες από όλες αυτές τις προϋποθέσεις επιδρά περισσότερο στην συντέλεση του. Πολλοί είναι εκείνοι που πιστεύουν ότι το έγκλημα προέρχεται κυρίως από ατομική προδιάθεση του ατόμου, πηγάζει από κληρονομικά ζητήματα ή η επιρροή προέρχεται από τον περίγυρο[23].

Σε όλες ανεξαιρέτως τις κοινωνίες υπάρχουν κανόνες τυπικοί ή άτυποι, οι οποίοι σκοπό έχουν να προστατεύσουν τα κοινωνικά αγαθά. Ταυτόχρονα, σε όλες τις κοινωνίες υπάρχουν άνθρωποι οι οποίοι παραβαίνουν τους κανόνες αυτούς. Αποτέλεσμα της προσβολής αυτών των αγαθών είναι η επιβολή διαφόρων κυρώσεων (ποινών) στους εκάστοτε παραβάτες. Οι ποινές αυτές δεν είναι παρά ένας τρόπος αντίδρασης της κοινωνίας στο έγκλημα. Η αντίδραση, καθώς και το είδος της ποινής, βρίσκονται πάντα σε στενή εξάρτηση με την εκάστοτε εποχή και πολιτισμό. Σύμφωνα με τον Durkheim, το έγκλημα υπάρχει σε κάθε κοινωνία, αν και σε καθεμία από

---

crime.gr/301.pdf, Ανακτήθηκε στις 23/09/2013

[23] Ιωαννίδης & Κουτσελίνη, (2002), ««Έγκλημα. Μια γενική θεώρηση ενός διαχρονικού φαινομένου», Αστυνομική Ανασκόπηση, μέρος Α', τεύχος 216, σελ. 680-685

αυτές η μορφή του είναι διαφορετική και οι εγκληματικές πράξεις δεν είναι παντού ίδιες[24].

Γενικότερα, αν εξαιρέσει κανείς ότι το έγκλημα αποτελεί τον πυρήνα του Ποινικού Κώδικα και ορίζεται εξ αυτόν ως πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο (Άρθρο 24 παρ. 1 Ποινικού Κώδικα). Τα στοιχεία της έννοιας του εγκλήματος είναι τα εξής:

Ä Να είναι πράξη, δηλαδή συμπεριφορά ανθρώπινη, εκούσια (πχ όχι κινήσεις επιληπτικού σε κρίση) και εξωτερική (δηλαδή όχι σκέψεις).

Ä Αντικειμενικά και απρόσωπα η πράξη αυτή να βρίσκεται σε αντίθεση προς απαγορευτικό ή επιτακτικό κανόνα δικαίου, ο οποίος την περιγράφει και απειλή ποινή κατά του παραβάτη.

Ä Να μην υπάρχει λόγος που να αποκλείει το άδικο (πχ άμυνα).

Ä Να υπάρχει καταλογισμός: να κριθεί ότι ο δράστης είναι πρόσωπο άξιο μομφής και κατά συνέπεια προσωπικά υπεύθυνο για την πράξη του (πχ ακαταλόγιστα είναι τα άτομα που πάσχουν από ψυχική νόσο).

Ä Να απειλείται από τον νόμο ποινή για την πράξη αυτή.

Σύμφωνα με τον Αλεξιάδη (1996), ο οποίος είναι Καθηγητής της Νομικής Σχολής, έγκλημα είναι κάθε εκδήλωση ανθρώπινης δράσης η οποία είναι επικίνδυνα αντικοινωνική[25]. Αυτό που εν γένει μπορεί να σημειωθεί είναι ότι οι ποινικοί νόμοι παγκοσμίως σχεδόν περιλαμβάνουν την προδοσία, το φόνο, ορισμένα σεξουαλικά παραπτώματα καθώς και σοβαρές περιπτώσεις προσβολής της ιδιοκτησίας ως εγκλήματα, αν και πάλι δεν έχουν την ίδια σοβαρότητα και δεν επιδέχονται την ίδια ποινή σε όλα τα κράτη του κόσμου[26]. Οι κυριότερες διακρίσεις εγκλημάτων, όπως αυτές έχουν ορισθεί από τον Ποινικό Κώδικα είναι:

1. Κακούργημα (πράξη που τιμωρείται με κάθειρξη), πλημμέλημα (πράξη που τιμωρείται με φυλάκιση ή χρηματική ποινή ή περιορισμό σε σωφρονιστικό κατάστημα) και πταίσμα (πράξη που τιμωρείται με κράτηση ή πρόστιμο)
2. Εγκλήματα με δόλο (από πρόθεση) ή εγκλήματα από αμέλεια
3. Εγκλήματα τετελεσμένα ή απόπειρες εγκλημάτων

[24] Τσουραμάνης, (2003), «Σύγχρονα Κοινωνικά Προβλήματα. Η ελληνική πραγματικότητα», Αθήνα, Εκδ. Παπαζήσης

[25] Αλεξιάδης (1996), «Εγχειρίδιο Εγκληματολογίας», Θεσσαλονίκη, Εκδ. Σάκκουλα

[26] Γαρδίκας (1955), «Εγκληματολογία» τεύχος Γ' εκδόσεις Δημ. Ν. Τζάκα – Στ. Δελαγραμμάτικα, Αθήνα

4. Εγκλήματα βασικά (πχ απλή σωματική βλάβη) ή εγκλήματα που αποτελούν παραλλαγές των βασικών (πχ βαριά σωματική βλάβη, σύμφωνα με το Άρθρο 310 του Ποινικού Κώδικα) ή εγκλήματα ιδιώνυμα (δηλαδή όσα δεν αποτελούν απλή παραλλαγή του βασικού, αλλά έχουν εγκληματολογική και κοινωνικοηθική αυτοτέλεια, για παράδειγμα ανθρωποκτονία με συναίνεση, σύμφωνα με το Άρθρο 300 του Ποινικού Κώδικα, ή παιδοκτονία, σύμφωνα με το Άρθρο 303 του Ποινικού Κώδικα)

5. Εγκλήματα βλάβης ή εγκλήματα διακινδύνευσης. Η πρώτη περίπτωση αναφέρεται στα εγκλήματα εκείνα των οποίων η αντικειμενική υπόσταση περιλαμβάνει τη βλάβη ορισμένου αντικειμένου, πχ ανθρωποκτονία, ενώ η δεύτερη περίπτωση, εκείνα των οποίων η αντικειμενική υπόσταση ενέχει διακινδύνευση ορισμένου έννομου αγαθού, δηλαδή αγαθού το οποίο προστατεύει ο νόμος, όπως για παράδειγμα η υγεία, η περιουσία

6. Εγκλήματα στιγμιαία (πχ κλοπή) και εγκλήματα διαρκή (η τέλεση του παρατείνεται χρονικά, πχ παράνομη κράτηση)

7. Εγκλήματα σχετικά με την απονομή της δικαιοσύνης (πχ ψευδορκία) και εγκλήματα κατά της ζωής (ανθρωποκτονία εκ προθέσεως). Εγκλήματα κατά της ιδιοκτησίας, εγκλήματα κατά της τιμής και κοινώς επικίνδυνα εγκλήματα. Εγκλήματα κατά της γενετήσιας ελευθερίας και εγκλήματα οικονομικής εκμετάλλευσης της γενετήσιας ζωής και εγκλήματα κατά των περιουσιακών δικαιωμάτων.

Αναφέρεται ότι εκτός όλων των άλλων, υπάρχει στενή σχέση ανάμεσα στον πολιτισμό του περιβάλλοντος και στην τεχνική του εγκλήματος που χρησιμοποιείται. Για παράδειγμα, οι ληστές των Ινδιών στραγγαλίζουν τα θύματά τους, καθώς οποιαδήποτε άλλη μέθοδος θα ήταν αντίθετη με το έθιμο της ομάδας. Σε άλλες πάλι ομάδες ο δολοφόνος χρησιμοποιεί το δηλητήριο και σε άλλες πάλι, το πιστόλι ή το πολυβόλο[27].

Σύμφωνα με επίσημη έκθεση της Αστυνομίας, στην Ελλάδα το έτος 2005 εξετάσθηκαν 139 περιπτώσεις οργανωμένων εγκλημάτων (διαπράχθηκαν από οργανώσεις), οι οποίες παρουσιάζονται στον παρακάτω πίνακα (Πίνακας 2):

[27] Melossi D., "Η κοινωνική θεωρία και οι μεταβαλλόμενες αναπαραστάσεις του εγκληματία. Εικόνες Εγκλήματος", εισαγωγή – επιμέλεια: Αφρ. Κουκουτσάκη, πρόλογος: Umberto Gatti, Πλέθρον

Πίνακας 2: Υποθέσεις Οργανωμένων Εγκλημάτων 2005

ΕΓΚΛΗΜΑ	ΑΡΙΘΜΟΣ ΥΠΟΘΕΣΕΩΝ
ΠΑΡΑΝΟΜΗ ΜΕΤΑΝΑΣΤΕΥΣΗ	50
ΝΑΡΚΩΤΙΚΑ (διακίνηση)	32
ΕΜΠΟΡΙΟ ΑΝΘΡΩΠΩΝ	21
ΕΜΠΟΡΙΟ ΚΛΑΥΤΟΚΙΝΗΤΩΝ	7
ΑΠΑΤΕΣ	6
ΛΑΘΡΕΜΠΟΡΙΟ ΤΣΙΓΑΡΩΝ	6
ΠΑΡΑΧΑΡΑΞΕΙΣ	4
ΑΡΧΑΙΟΚΑΠΗΛΙΕΣ	3
ΚΛΟΠΕΣ	3
ΠΛΑΣΤΟΓΡΑΦΙΕΣ	3
ΛΗΣΤΕΙΕΣ	3
ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ	1
Άθροισμα	**139**

Πηγή:
http://www.astynomia.gr/images/stories/STATS/Attachment16319_EKTHESI%20ORGANOMENOY%20EGLIMATOS.pdf

Υπενθυμίζεται, ότι από την αρχή του 2010, για πρώτη φορά, η Ελληνική Αστυνομία με ειδικό λογισμικό αποτυπώνει ηλεκτρονικά και σε πραγματικό χρόνο όλα τα αδικήματα και τα συμβάντα αστυνομικού ενδιαφέροντος. Με το νέο αυτό τρόπο καταγράφονται καθημερινά (μέσω του συστήματος Police On Line), αναλυτικά και με πληρότητα όλα τα περιστατικά, σε κάθε αστυνομική Υπηρεσία της χώρας για την ενημέρωση των πολιτών. Σύμφωνα με τα Στατιστικά στοιχεία εγκληματικότητας, εγκλημάτων κατά της οικονομίας, παράνομης διακίνησης μεταναστών, συγκεντρώσεων, αθλητικών εκδηλώσεων, καθώς και απολογισμού της αστυνομικής ανταπόκρισης για το έτος 2012, όπως αυτά δημοσιεύθηκαν στην Ιστοσελίδα της Ελληνικής Αστυνομίας, σημειώνονται τα παρακάτω στοιχεία[28]:

Το έτος 2012 καταγράφηκαν στην επικράτεια οι λιγότερες ανθρωποκτονίες, ληστείες και κλοπές – διαρρήξεις της τελευταίας τριετίας (2010 – 2012). Συγκεκριμένα, συγκριτικά με το 2011, καταγράφηκαν (19) λιγότερες ανθρωποκτονίες, (644) λιγότερες ληστείες, (9.013) λιγότερες κλοπές – διαρρήξεις και (1.076) λιγότερες κλοπές τροχοφόρων. Στο σύνολο της επικράτειας (συγκριτικά πάντα με το 2011) σημειώθηκαν 12% λιγότερες περιπτώσεις εκβιασμών, ενώ οι πλαστογραφίες μειώθηκαν κατά 15%, οι υποθέσεις αρχαιοκαπηλίας μειώθηκαν σε ποσοστό 8% και η κυκλοφορία πλαστών χαρτονομισμάτων κατά 5%. Είναι επίσης αξιοσημείωτο ότι το έτος 2012 συνελήφθησαν συνολικά (184.000) περίπου άτομα για εγκλήματα και αξιόποινες συμπεριφορές, κακουργηματικού και πλημμελητικού

[28] Ιστοσελίδα της Ελληνικής Αστυνομίας «Στατιστικά Στοιχεία», ηλεκτρονικά διαθέσιμο: http://www.astynomia.gr/index.php?option=ozo_content&lang='..'&perform=view&id=24766&Itemid=1058&lang=

χαρακτήρα. Από αυτά, (15.642) άτομα συνελήφθησαν για ληστείες, κλοπές και διαρρήξεις σπιτιών, αυτοκινήτων, καταστημάτων, Τραπεζών κ.λπ., ενώ παράλληλα εξαρθρώθηκαν (455) σημαντικές πολυμελείς εγκληματικές οργανώσεις, που διέπρατταν πράξεις βίας ή σοβαρές μορφές αδικημάτων με μεγάλη κοινωνική απαξία.

Στην Περιφέρεια Αττικής για το α' εξάμηνο του 2014, σύμφωνα με τα στοιχεία της Ελληνικής Αστυνομίας διαπράχθηκαν τα παρακάτω εγκλήματα, όπως αυτά αποτυπώνονται στον Πίνακα

Γ.Α.Δ.ΑΤΤΙΚΗΣ	**2 0 1 3 (Α'6μηνο)** ΕΓΚΛΗΜΑΤΑ			**2 0 1 4 (Α'6μηνο)** ΕΓΚΛΗΜΑΤΑ			**Ποοσοστιαία μεταβολή τελεσμένων εγκλημάτων 2013-2014**
	τελ/να	απόπειρες	εξιχνιάσεις	τελ/να	απόπειρες	εξιχνιάσεις	
ΑΝΘΡΩΠΟΚΤΟΝΙΕΣ	**27**	27	38	**21**	28	42	**-22%**
ΑΠΑΤΕΣ	**844**	67	240	**750**	31	210	**-11%**
ΑΡΧΑΙΟΚΑΠΗΛΕΙΑ	**4**		4	**5**	3	5	**25%**
ΒΙΑΣΜΟΙ	**22**	11	19	**26**	13	25	**18%**
ΕΚΒΙΑΣΕΙΣ	**42**	1	19	**31**		16	**-26%**
ΕΠΑΙΤΕΙΑ	**44**		44	**34**		34	**-23%**
ΖΩΟΚΛΟΠΗ	**69**	1	3	**56**	1	2	**-19%**
ΚΥΚΛΟΦΟΡΙΑ ΠΑΡΑΧΑΡΑΓΜΕΝΩΝ	**738**		216	**1.039**	1	354	**41%**
ΛΑΘΡΕΜΠΟΡΙΟ	**304**	3	279	**294**	9	260	**-3%**
Ν περί ΝΑΡΚΩΤΙΚΩΝ	**1.610**	4	1.519	**1.712**	7	1.587	**6%**
Ν περί ΟΠΛΩΝ	**514**	2	387	**488**	1	326	**-5%**
Ν περί ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ	**43**		42	**43**		31	**0%**
ΠΛΑΣΤΟΓΡΑΦΙΑ	**508**		429	**680**	2	602	**34%**
ΣΕΞΟΥΑΛΙΚΗ ΕΚΜΕΤΑΛΛΕΥΣΗ	**110**		109	**136**		121	**24%**
ΚΛΟΠΕΣ - ΔΙΑΡΡΗΞΕΙΣ	**20.876**	1.346	2.847	**19.996**	1.361	2.323	**-4%**
ΚΛΟΠΕΣ ΤΡΟΧΟΦΟΡΩΝ	**9.226**	141	2.107	**7.498**	142	1.681	**-19%**
ΛΗΣΤΕΙΕΣ	**1.934**	61	471	**1.451**	51	460	**-25%**

Πίνακας 3: Συγκριτικά στοιχεία διαπραχθέντων εγκλημάτων για τα έτη 2013 και 2014 (α' εξάμηνο)

Πηγή: Αρχεία Ελληνικής Αστυνομίας (2014), http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=43803&Itemid=1149&lang=, ανακτήθηκε στις 30/08/2014

Από τα στοιχεία του παραπάνω πίνακα, φαίνεται μια πτωτική τάση, συγκρίνοντας το α' εξάμηνο του 2014 με το αντίστοιχο εξάμηνο του προηγούμενου έτους σε όλα σχεδόν τα εγκλήματα για την Περιφέρεια Αττικής. Βέβαια, η πλαστογραφία, η σεξουαλική εκμετάλλευση, η κυκλοφορία παραχαραγμένων, οι βιασμοί η αρχαιοκαπηλεία είναι ορισμένες μορφές εγκλημάτων που έχουν αυξητική πορεία μεταξύ των δυο περιόδων.

Αντίστοιχα είναι τα στοιχεία για την άλλη μεγάλη περιφέρεια της Ελλάδας, καθώς στη Θεσσαλονίκη, ναι μεν παρατηρείται επί του συνόλου των εγκλημάτων μια πτωτική πορεία (11.131 εγκλήματα που σημειώθηκαν συνολικά το α' εξάμηνο του 2013, το αντίστοιχο εξάμηνο του 2014 σημειώθηκαν 9.976 εγκλήματα) με το ποσοστό μείωσης τους να αγγίζει το 10%, αλλά ορισμένες κατηγορίες εγκλημάτων παρουσίασαν αύξηση. Ενδεικτικά, αναφέρεται ότι στη Θεσσαλονίκη για τις δυο εξεταζόμενες περιόδους σημειώθηκε αύξηση στο ποσοστό των εγκλημάτων που αφορούσαν περιπτώσεις εκβιασμών (αύξηση 9%), κυκλοφορία παραχαραγμένων (αύξηση 6%), λαθρεμπόριο (αύξηση 63%), παραβάσεις του Ν. περί Ναρκωτικών (αύξηση 23%) και οι παραβάσεις του Ν. περί όπλων υπερδιπλασιάστηκαν[29].

[29] Αρχεία Ελληνικής Αστυνομίας (2014), http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=43803&Itemid=1149&lang=, ανακτήθηκε στις 30/08/2014

Τέλος, όσον αφορά στο σύνολο της επικράτειας (πίνακας 4) φαίνεται μια πτωτική τάση της εγκληματικότητας της τάξης του 9%.

Πίνακας 4: Συγκριτικά στοιχεία εγκληματικότητας στο σύνολο της Ελληνικής επικράτειας για το 2013-2014 (α' εξαμηνο)

ΕΠΙΚΡΑΤΕΙΑ	2013 (Α'6μηνο)			2014 (Α'6μηνο)		
	ΕΓΚΛΗΜΑΤΑ			ΕΓΚΛΗΜΑΤΑ		
	τελ/να	απόπειρες	εξιχνιάσεις	τελ/να	απόπειρες	εξιχνιάσεις
ΑΝΘΡΩΠΟΚΤΟΝΙΕΣ	**70**	72	114	**52**	76	121
ΑΠΑΤΕΣ	**1.416**	92	547	**1.344**	73	671
ΑΡΧΑΙΟΚΑΠΗΛΕΙΑ	**24**		22	**34**	3	32
ΒΙΑΣΜΟΙ	**64**	33	73	**63**	27	74
ΕΚΒΙΑΣΕΙΣ	**80**	6	60	**79**	1	64
ΕΠΑΙΤΕΙΑ	**1.184**		1.089	**1.042**	4	1.039
ΖΩΟΚΛΟΠΗ	**486**	9	70	**403**	5	82
ΚΥΚΛΟΦΟΡΙΑ ΠΑΡΑΧΑΡΑΓΜΕΝΩΝ	**2.704**	3	432	**3.115**	1	566
ΛΑΘΡΕΜΠΟΡΙΟ	**583**	3	515	**819**	9	715
Ν περί ΝΑΡΚΩΤΙΚΩΝ	**4.803**	5	4.607	**5.374**	36	5.124
Ν περί ΟΠΛΩΝ	**2.920**	7	2.597	**3.080**	3	2.619
Ν περί ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ	**228**		220	**175**		161
ΠΛΑΣΤΟΓΡΑΦΙΑ	**1.100**	1	981	**1.325**	2	1.222
ΣΕΞΟΥΑΛΙΚΗ ΕΚΜΕΤΑΛΛΕΥΣΗ	**263**		260	**213**		196
ΚΛΟΠΕΣ - ΔΙΑΡΡΗΞΕΙΣ	**38.370**	2.434	8.161	**34.458**	2.413	6.889
ΚΛΟΠΕΣ ΤΡΟΧΟΦΟΡΩΝ	**15.352**	199	4.720	**12.025**	400	3.877
ΛΗΣΤΕΙΕΣ	**2.555**	121	856	**1.902**	99	724
ΣΥΝΟΛΟ	**72.202**	**2.985**	**25.324**	**65.503**	**3.152**	**24.176**

Πηγή: Αρχεία Ελληνικής Αστυνομίας (2014), http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=43803&Itemid=1149&lang=, ανακτήθηκε στις 30/08/2014

Η αρχαιοκαπηλία, οι παραβάσεις του Ν. περί Ναρκωτικών, οι παραβάσεις του Ν. περί όπλων, η κυκλοφορία παραχαραγμένων, οι περιπτώσεις πλαστογραφίας είναι και στο σύνολο της περιφέρειας εκείνες οι μορφές εγκλημάτων που συνεχίζουν να αυξάνονται μεταξύ των δυο περιόδων.

Οι κλιμακούμενες αυτές μειώσεις, συνδέονται άμεσα με την επιχειρησιακή δυναμική που έχει αναπτύξει η Ελληνική Αστυνομία, στο πλαίσιο του γενικότερου στρατηγικού σχεδιασμού, τόσο στον τομέα της πρόληψης και αποτροπής, όσο και στον τομέα της συνολικής αστυνομικής ανταπόκρισης και των εξιχνιάσεων, κυρίως σοβαρών εγκληματικών συμπεριφορών[30].

2.2 Ιστορική αναδρομή εγκλήματος

Εγκλήματα συναντά κανείς στα βάθη της ιστορίας από την αρχή της ανθρωπότητας, αν και παλαιότερα δεν είχαν τη μορφή που έχουν σήμερα ή δε θεωρούνταν πάντα ως αξιόποινες πράξεις. Στην πρωτόγονη κοινωνία, η συμπεριφορά που καταδικάζονταν αυστηρότερα μεταξύ όλων ήταν εκείνη που προσέβαλλε τις υπερφυσικές και θεϊκές δυνάμεις, ακόμη και στην περίπτωση που οι πράξεις ήταν σχετικά ασήμαντες (πχ. η παράβαση των κυνηγετικών κανόνων), οι οποίες όμως σχετίζονταν με υπερφυσικές δοξασίες ή με θρησκευτικές αντιλήψεις[31].

Εγκλήματα λοιπόν συναντάμε από την αρχαιότητα σε όλους τους πολιτισμούς. Στην αρχαία Ελλάδα η πορνεία χαρακτηρίστηκε το «αρχαιότερο επάγγελμα» στον κόσμο και μάλιστα στην αρχαία Αθήνα αποτελούσε έναν θεσμό μεταξύ νομιμότητας και παρανομίας. Εκτός από την πορνεία βέβαια, το έγκλημα στην αρχαία Ελλάδα διανθιζόταν υπό διάφορες μορφές. Συγκεκριμένα, η αθηναϊκή νομοθεσία περιελάμβανε πέντε κατηγορίες κακοποιών: τους κλέφτες, τους κλέφτες μανδυών, τους λαφυραγωγούς, τους διαρρήκτες και τους πορτοφολάδες. Η κλοπή όμως και η λεηλασία δεν εμφανίζονται μόνο στον κόσμο των ανθρώπων αλλά και στον κόσμο των θεών. Μάλιστα, ο Ερμής ήταν ο προστάτης των κλεφτών. Στην κωμωδία Όρνιθες του Αριστοφάνη συναντάμε την περίπτωση κάποιου που

[30] Δελτίο Τύπου ΕΛ.ΑΣ. (2014), Μείωση των βασικών δεικτών εγκληματικότητας, ηλεκτρονικά διαθέσιμη αναδημοσίευση: http://www.eglimatikotita.gr/2014/05/2014_15.html, ανακτήθηκε στις 02/09/2014

[31] Ιωαννίδη, Β., & Κουτσελίνη, Α. (2002). Έγκλημα. Μια γενική θεώρηση ενός διαχρονικού φαινομένου. *Αστυνομική Ανασκόπηση.* Μέρος Α'. Τεύχος 216, σς. 680-685

καταληστεύτηκε.

Συγκεκριμένα, ο Αριστοφάνης περιγράφει την κλοπή του μανδύα ενός καλεσμένου σε μια γιορτή, όταν αυτός αργά το βράδυ ξεκίνησε να επιστρέψει στο σπίτι του. Επίσης, πέρα από τις κάθε είδους κλοπές και υπεξαιρέσεις υπήρχαν και επεισόδια βίας με τραυματισμούς ή και θανάτους. Οι αναμετρήσεις ανάμεσα στις αθηναϊκές φατρίες κάποιες φορές αποδείχτηκαν πολύ σκληρές με θύματα και τραυματίες ακόμη και επιφανείς Αθηναίους[32].

Τα εγκλήματα στην Αρχαία Ελλάδα τιμωρούνταν, ίσως πολύ αυστηρά, για την εποχή εκείνη και τα δεδομένα της. Στην αρχαία Ελλάδα, τα είδη των ποινών ήταν τρία: εξορία, επιβολή προστίμου, ακόμα και θανατική ποινή. Μεταξύ των παραπάνω, η πλέον ατιμωτική ποινή θεωρούνταν η εξορία, καθώς εκείνος που διωχνόταν από την πόλη, δεν είχε πλέον πατρίδα για την υπόλοιπη ζωή του. Αναφορικά με τη θανατική ποινή ήταν αρκετά διαδεδομένη ως τιμωρία στην αρχαία Ελλάδα και μάλιστα εφαρμόζονταν με πολλούς διαφορετικούς τρόπους, κυρίως για να αποφευχθούν οι βεντέτες μεταξύ των οικογενειών και οι αυτοδικείς πράξεις[33]. Εγκλήματα αναφέρονται ακόμη στην Παλαιά Διαθήκη στον κώδικα Χαμουραμπί και στον Όμηρο. Στη Ρωμαϊκή εποχή τα εγκλήματα ήταν επίσης κάτι σύνηθες και μάλιστα τα περισσότερα συντελούνταν με φρικτούς τρόπους και έπειτα από εντολές υψηλά ιστάμενων προσώπων, ακόμα και αυτοκρατόρων.

Εγκλήματα συναντάμε σε όλες τις εποχές, στο Βυζάντιο, στο Μεσαίωνα, αλλά και στους νεότερους χρόνους με την εγκληματικότητα να αυξάνεται συνεχώς και να προστίθενται στα ήδη υπάρχοντα εγκλήματα νέα, τα οποία έως τώρα δεν είχαν απασχολήσει τις Αρχές και την Κοινωνία. Μερικά από τα αξιοσημείωτα εγκλήματα του 20^{ου} αιώνα είναι τα εξής:

- Η κλοπή της Μόνα Λίζα (1911) από το μουσείο του Λούβρο και η μεταφορά της στη Φλωρεντία
- Ο φόνος της Ελίζαμπεθ Σορτ («Η Μαύρη Ντάλια», 1947), ο οποίος παραμένει ανεξιχνίαστος ακόμη και σήμερα.
- Η υπόθεση Μάνσον (1969)
- Η υπόθεση του Αντρέι Τσικατίλο (1978)
- Η υπόθεση Τζον Γουέιν Γκέισι (1978)

[32] Παπαγεωργίου Ε (χ.χ.), «Ο υπόκοσμος στην Αρχαία Ελλάδα», διαθέσιμο ηλεκτρονικά: http://www.apologitis.com/gr/ancient/ypokosmos.htm,

[33] Ηλεκτρονικό άρθρο (24/05/2009), με θέμα: «Θανατική ποινή», διαθέσιμο: http://thanatikipoini.blogspot.gr/2009/05/blog-post_24.html

- Η υπόθεση του Τεντ Μπάντι (1978)
- Η κατάρρευση της Τράπεζας Μπάρινγκς (1995)
- Η σφαγή στο Κολούμπαιν (1999)

Παρόλα αυτά το περιεχόμενο της έννοιας του εγκλήματος δεν ήταν ποτέ ίδιο σε όλες τις εποχές. Βέβαια, ούτε και σήμερα είναι ίδιο σε όλες τις χώρες. Στην Αγγλία και τις ΗΠΑ του 19ου αιώνα, η μαγεία αποτελούσε έγκλημα και οι παραβάτες καταδικάζονταν σε θάνατο. Δε συνέβαινε όμως το ίδιο στην Ελλάδα της περιόδου εκείνης. Στην Ελλάδα, μετά το 1982, η μοιχεία δεν αποτελεί εγκληματική πράξη, κάτι όμως που δε συμβαίνει σε άλλες χώρες, όπου η μοιχεία τιμωρείται ακόμη και σήμερα με θανατική ποινή. Επομένως, η έννοια του εγκλήματος διαμορφώνεται από διάφορους παράγοντες και κυρίως από τις κοινωνικές, πολιτικές, πολιτιστικές ή πολιτισμικές συνθήκες που επικρατούν στην κάθε εποχή και την κάθε περιοχή.

Το έγκλημα στις μέρες μας τείνει να γίνεται ολοένα και περισσότερο οργανωμένο και να ακολουθεί την πορεία της παγκοσμιοποίησης. Οι δράστες του έχουν το έγκλημα ως κύρια ή και αποκλειστική δραστηριότητα και ενεργούν με σκοπό την επίτευξη μεγάλου οικονομικού οφέλους. Στις δραστηριότητές τους αυτές, οι οργανωμένοι εγκληματίες διευκολύνονται από τη βαθμιαία κατάργηση των συνόρων και την εύκολη και γρήγορη πλέον μετακίνηση ανθρώπων, κεφαλαίων και αγαθών παγκοσμίως. Στην σύγχρονη εγκληματικότητα αξίζει να αναφερθεί ότι μεγάλο ρόλο παίζει και η εξέλιξη της τεχνολογίας της οποίας η συμβολή είναι τεράστια προς αυτή την κατεύθυνση με αποτέλεσμα πολλοί να είναι εκείνοι που τη χρησιμοποιούν σε εγκληματικές διεξόδους[34].

Σήμερα, οι ποινικοί νόμοι[35] όλου σχεδόν του κόσμου περιλαμβάνουν την προδοσία, το φόνο, ορισμένα σεξουαλικά παραπτώματα καθώς και σοβαρές περιπτώσεις προσβολής της ιδιοκτησίας και δίνουν στα αδικήματα αυτά τον ίδιο περίπου ορισμό. Στην περίπτωση ορισμένων από τα αδικήματα αυτά -κακουργήματα, εγκλήματα- ο ποινικός νόμος δίνει μια αρκετά ακριβή εικόνα των κριτηρίων αντικοινωνικής συμπεριφοράς που επικρατούν στην ομάδα. Το κράτος, όμως, αναγκάζεται, όταν η κοινωνική ζωή γίνει εξαιρετικά περίπλοκη, να προσθέσει στα αδικήματα του ποινικού νόμου και πράξεις άλλες, οι οποίες αποτελούν ιδιαίτερα

[34] Κουράκης (2001), «Το Έγκλημα και οι εγκληματολογικές επιστήμες στον 21ο αιώνα», Ποινικός Λόγος, 801-803

[35] Γαρδίκας (1955), Εγκληματολογία, τ. Γ', Σωφρονιστική, εκδ. Δημ. Ν. Τζάκα - Στ. Δελαγραμμάτικα, Αθήναι

χαρακτηριστικά ορισμένων τύπων κοινωνικής οργάνωσης.

Κατ' ακολουθία, ο προοδευτικά όλο και συχνότερος χαρακτηρισμός πράξεων ως εγκλημάτων είναι αποτέλεσμα της κοινωνικής ανάπτυξης και διαφοροποίησης του βιομηχανικού πολιτισμού. Από μεγάλες ομάδες μέσα στα κράτη, τα εγκλήματα αυτά δεν θεωρούνται πράξεις αντικοινωνικές· π.χ. η πώληση οινοπνευματωδών ποτών χαρακτηρίσθηκε ως έγκλημα για τη νομοθεσία των Ηνωμένων Πολιτειών σε μία ορισμένη περίοδο, δεν την έκριναν όμως όλοι ως αντικοινωνική. Στην περίπτωση τέτοιων παραβάσεων, ο ποινικός νόμος δεν μπορεί να χρησιμεύσει ως δείκτης των αντιλήψεων της ομάδας για την αντικοινωνική συμπεριφορά[36].

2.2 Ποινικό Δίκαιο

Το ποινικό δίκαιο αποτελεί έναν από τους κλάδους του δικαίου με αντικείμενο του το έγκλημα, το οποίο συνδέεται με ανθρώπινα πάθη, εντάσεις και ανυπέρβλητα διλήμματα. Το ποινικό δίκαιο είναι εκείνο που διαφυλάσσει τη σπουδαιότητα των ατομικών ελευθεριών, την αξία του ανθρώπου και τις αρχές του κράτους δικαίου. Ορίζει τις προϋποθέσεις κάτω από τις οποίες η Πολιτεία επιβάλλει ποινικές κυρώσεις σε εκείνους που έχουν προβεί σε μια αξιόποινη πράξη. Κυριότερη πηγή του ποινικού δικαίου είναι ο ποινικός κώδικας, ο οποίος χωρίζεται σε δυο μέρη, τον γενικό και τον ειδικό[37].

[36] Παπαθεοδώρου, (1992). Ο κοινωνικός έλεγχος του εγκλήματος. *Χρονικά Εργαστηρίου Εγκληματολογίας και Δικαστικής Ψυχιατρικής*, Τμήματος Νομικής, Πανεπιστημίου Θράκης, τχ. 4, Ιαν. 1992, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, σσ. 55-67.

[37] Μυλωνόπουλος (2010), «Ποινικό Δίκαιο», διαθέσιμο: http://www.poinikachronika.gr/assets/Mylonopoulos-PoinDik-CenikoM%20I-10%20first%20p..pdf

Η αποστολή του ποινικού δικαίου είναι διττή, αφού από τη μια προστατεύει τα έννομα αγαθά και από την άλλη εξασφαλίζει τις ατομικές ελευθερίες από την κρατική αυθαιρεσία[38].

Το ποινικό δίκαιο αναφέρεται ως:

· Ουσιαστικό ποινικό δίκαιο (ή κυρίως ποινικό δίκαιο), όταν η ποινική εξουσία, την οποία ρυθμίζει αφορά στις προϋποθέσεις και την έκταση του ποινικού κολασμού, δηλαδή τον προσδιορισμό των αξιόποινων πράξεων και της ποινικής κύρωσης τους και ως

· Δικονομικό ποινικό Δίκαιο ή Δικονομία, όταν η εν λόγω ποινική εξουσία αφορά στις προϋποθέσεις και στους τύπους (όργανα και διαδικασία) για τη βεβαίωση της ενοχής του φερόμενου ως δράστη (κατηγορούμενου) ενός εγκλήματος για την επιβολή της προβλεπόμενης από τον νόμο ποινικής κύρωσης (ποινής, μέτρου ασφάλειας ή μέτρου για ανήλικους).

Το έγκλημα και η ποινική κύρωση αποτελούν δυο κεντρικές έννοιες για το ποινικό δίκαιο και ο αντίστοιχος ορισμός τους των εννοιών αυτών, προσδίδει αντίστοιχο περιεχόμενο και στο εν λόγω δίκαιο. Το Ποινικό Δίκαιο αποτελεί σήμερα ειδική Νομική επιστήμη στην οποία περιλαμβάνονται:

- αυτή καθαυτή η Νομική Ποινική Επιστήμη,
- η Εγκληματολογία και
- η Ποινολογία ή Ποινικολογία

Επίσης συμβάλλουν συμπληρωματικά οι εξής επιστήμες:

- η Φιλοσοφία,
- η Ιατροδικαστική,
- η Ψυχιατρική,
- η Δικαστική Ψυχολογία, και
- η Εγκληματολογική Στατιστική.

Το ποινικό δίκαιο έχοντας ως αντικείμενο την άσκηση της ποινικής εξουσίας

[38] Μαγκάκη (1989), ΣυστΕρμΠΚ αρθρ.1 αρ 2, Χωραφά 5, Ανδρουλάκη Ι, 95 «Η αιτιολόγηση των αποφάσεων των ποινικών δικαστηρίων», τ. Α’

από την Πολιτεία (και όχι τη ρύθμιση σχέσεων μεταξύ των μερών) ανήκει στο Δημόσιο Δίκαιο και αποτελεί στη λαϊκή συνείδηση τον πλέον αντιπροσωπευτικό και άμεσα αισθητό κλάδου Δικαίου, καθώς ασχολείται με πράξεις που θίγουν κατά τον πλέον οδυνηρό τρόπο τα σημαντικότερα ίσως αγαθά του ατόμου.

2.3 Εγκληματολογία

Η συστηματική πολύπλευρη μελέτη του εγκλήματος και των μεθόδων πρόληψης και καταστολής του αφορούν με λίγα λόγια το αντικείμενο της Εγκληματολογίας, η οποία αποτελεί έναν ιδιαίτερο κλάδο γνώσης, όπου χρησιμοποιεί πορίσματα ή μεθόδους της Κοινωνιολογίας, της ψυχολογίας, της Ανθρωπολογίας, της ψυχιατρικής, της στατιστικής, της βιολογίας και άλλων επιστημών, προκειμένου να εξαχθούν τα απαραίτητα συμπεράσματα. Παρότι η διδασκαλία της Εγκληματολογίας ξεκίνησε στην Ελλάδα πριν από το Β΄ Παγκόσμιο Πόλεμο, από τον Κωνσταντίνο Γαρδίκα, η εξέλιξη της συγκεκριμένης επιστήμης δεν ακολούθησε τη θεαματική ανάπτυξη που σημειώθηκε μεταπολεμικά σε διεθνές επίπεδο.

Ο Κωνσταντίνος Γαρδίκας (1966) όρισε την εγκληματολογία ως την επιστήμη που *«σπουδάζει το έγκλημα ως πραγματικόν (ψυχικόν και φυσικόν) γεγονός και τα μέσα της κατ' αυτού πάλης»*, ενώ παρόμοιοι είναι οι ορισμοί που έχουν δοθεί από διαφορετικούς κατά καιρούς επιστήμονες της[39].

Η εγκληματολογία άρχισε να αναπτύσσεται γύρω στα 1880, όταν το έγκλημα έπαψε να αποδίδεται στην αμαρτία ή τα δαιμόνια και άρχισε να μελετάται θεωρητικά από τον Garofalo και εμπειρικά από τον Λομπρόζο. Οι μελέτες του δεύτερου συσχετίζουν ορισμένες σωματικές, αλλά και ψυχικές ιδιομορφίες με την εγκληματική ροπή και άνοιξαν το δρόμο σε έρευνες που αναζητούσαν τη μόνη ή κύρια αιτία του εγκλήματος στην κληρονομικότητα, σε εγκεφαλικές βλάβες, στη σωματική διάπλαση, στη δυσλειτουργία ενδοκρινών αδένων, στη γενετική ανωμαλία του συνδρόμου XYY κ.α.

Ένας αρκετά λακωνικός, αλλά ταυτόχρονα ιδιαίτερα ενδιαφέρον ορισμός είναι ο εξής: *Εγκληματολογία είναι η συζήτηση για το έγκλημα και τις μεθόδους με τις οποίες η κοινωνία το αντιμετωπίζει*[40].

---

[39] Γαρδίκα (1966), «Εγκληματολογία» τόμος Α', «Τα γενικά και ατομικά αίτια των εγκλημάτων» 5η Έκδοση, Αθήνα

[40] Morrison (1995), "Theoretical Criminology: from modernity to post-modernity" Great Britain

Η ποικιλία ορισμών που έχουν δοθεί για τη συγκεκριμένη επιστήμη συνάδουν στο ότι η εγκληματολογία αποτελεί τη συνισταμένη τμημάτων ορισμένων κλάδων, όπως η ψυχολογία, η κοινωνιολογία, η ανθρωπολογία, η εθνογραφία, η ψυχιατρική, το ποινικό δίκαιο κλπ., οι οποίοι περιλαμβάνουν στο αντικείμενό τους, σε κάποιο βαθμό, και τη σπουδή του εγκλήματος, του εγκληματία ή της συμπεριφοράς. Η εγκληματολογική επιστήμη στην ευρύτερη έννοια περιλαμβάνει τα εξής:

· Κυρίως εγκληματολογία, που εξετάζει την ιστορική και κοινωνιολογική εξέλιξη των γεγονότων – εγκλημάτων, την περιγραφή τους (πόσα και ποια τελέσθηκαν, αιτίες και παράγοντες τους κτλ)

· Σωφρονιστική ή ποινολογία με αντικείμενο την επίσημη αντίδραση της Πολιτείας στο έγκλημα. Δηλαδή, περιλαμβάνονται οι διάφορες ποινές και η αποτελεσματικότητα τους.

· Ανακριτική ή επιστημονική αστυνομική, που περιλαμβάνει την πολύπλευρη έρευνα (εξέταση μαρτύρων, ανάκριση, συλλογή και αξιολόγηση ιχνών εγκλήματος κτλ) σχετικά με τη διάπραξη κάποιου εγκλήματος και την αποκάλυψη ταυτότητας του δράστη. Τα πορίσματα της παραπάνω έρευνας αξιοποιεί η ποινική δικαιοσύνη.

· Δικαστική ψυχολογία. Σε αυτήν περιλαμβάνονται η έρευνα ψυχικών φαινομένων και γεγονότων τα οποία επιδρούν στην ανεύρεση της αλήθειας και στην απόφαση του δικαστή.

· Δικαστική ψυχιατρική (μελέτη περιπτώσεων ψυχικής ασθένειας, διαταραχής ή άλλης ιδιαιτερότητας της προσωπικότητας του κατηγορούμενου στην έκβαση της δίκης)

· Εγκληματοπροληπτική πολιτική, όπου αποτελείται από το σύνολο των ενεργειών και των μέσων τα οποία αναφέρονται στην αντιμετώπιση των εγκλημάτων.

Έτσι, σημειώνεται με απλά λόγια ότι αντικείμενο της εγκληματολογίας και των επιστημόνων / επαγγελματιών αυτής είναι η καταγραφή, η διερεύνηση και η ανάλυση του σύγχρονου εγκλήματος, το οποίο ερευνάται ως ανθρώπινη πράξη αλλά ταυτόχρονα και ως κοινωνικό φαινόμενο, ενώ παράλληλα αναζητούνται οι παράγοντες εκδήλωσης της εγκληματικότητας. Επίσης, η επιστήμη της εγκληματολογίας μελετά το δράστη των εγκληματικών πράξεων, αναζητώντας παράλληλα τις σχέσεις μεταξύ ποινικής πράξης και ποινικής κύρωσης.

Το Ηλεκτρονικό Έγκλημα

3.1 Ορισμός ηλεκτρονικού εγκλήματος

Η ραγδαία εξάπλωση της τεχνολογίας και η διείσδυση του διαδικτύου στην καθημερινή ζωή των ανθρώπων έχει επιφέρει πλήθος αλλαγών στη ζωή και τις συνήθειες τους, επηρεάζοντας πολλούς διαφορετικούς τομείς, από τις διαπροσωπικές τους σχέσεις, έως τις καθημερινές τους συναλλαγές με τις επιχειρήσεις (πχ. Ηλεκτρονικό εμπόριο) αλλά ακόμα και το κράτος. Η χρήση των ηλεκτρονικών υπολογιστών, η οποία αυξάνεται συνεχώς δε διαμόρφωσε μόνο νέες συνθήκες στην καθημερινή ζωή των ατόμων, στο χώρο και τις συνθήκες εργασίας τους, στην επικοινωνία τους και στην καθημερινή τους ψυχαγωγία, προσθέτοντας νέες μορφές διασκέδασης, αλλά ταυτόχρονα δημιούργησε νέους τρόπους στα δεδομένα των μέχρι σήμερα συναλλαγών, αφού οι ηλεκτρονικοί υπολογιστές χρησιμοποιούνται εκτεταμένα και στις επιχειρήσεις, στις δημόσιες και ιδιωτικές υπηρεσίες, αλλά και στους κρατικούς φορείς.

Βέβαια, οι συγκεκριμένες εξελίξεις ναι μεν έχουν επηρεάσει θετικά τη ζωή των ατόμων διότι τους εξασφαλίζουν αμέτρητες πληροφορίες απ' όπου κι αν βρίσκονται (αρκεί να έχουν πρόσβαση στον ηλεκτρονικό τους υπολογιστή) και εξοικονομούν σημαντικό χρόνο, αλλά από την άλλη δεν μπορούσαν παρά να έχουν και κάποιες αρνητικές επιπτώσεις τόσο για τα ίδια τα άτομα όσο και για την κοινωνία στο σύνολο της. Οι επιπτώσεις σε ατομικό επίπεδο εστιάζουν κυρίως στον εθισμό

που μπορεί να προκληθεί από τη συνεχόμενη και πολύωρη χρήση των ηλεκτρονικών υπολογιστών και του διαδικτύου, ο οποίος με τη σειρά του γίνεται επιβλαβής ως προς το άτομο με διάφορους τρόπους (αντικοινωνική συμπεριφορά, εικονική πραγματικότητα, κλπ).

Αναφορικά με τις αρνητικές συνέπειες ως προς το κοινωνικό σύνολο σε αυτές συμπεριλαμβάνονται διάφορες μορφές και παράγοντες που ευνοούν νέες αντικοινωνικές συμπεριφορές σε σημείο εγκληματικότητας. Οι νέες αυτές μορφές εγκληματικότητας στο σύνολο τους συντελούν στη θεσμοθέτηση ενός σχετικά νέου όρου, αυτού του «Ηλεκτρονικού Εγκλήματος».

Κατά καιρούς, έχουν γίνει πολλές προσπάθειες να ορισθεί επακριβώς το ηλεκτρονικό έγκλημα.

Σύμφωνα με τον ορισμό της ίδιας της Ελληνικής Αστυνομίας, ηλεκτρονικό έγκλημα θεωρούνται:

«*οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία*».

Ανάλογα με τον τρόπο τέλεσης, τα ηλεκτρονικά εγκλήματα διαχωρίζονται στις εξής κατηγορίες[41]:

- Εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και
- Κυβερνοεγκλήματα (cyber crime), εάν τελεσθούν μέσω του Διαδικτύου.

Ένας άλλος ορισμός του έχει δοθεί από τους Forester & Morrison (1994), όπου το ηλεκτρονικό έγκλημα ορίζεται ως:

«μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της».

[41]Ιστοσελίδα Ελληνικής Αστυνομίας (2013), «Ηλεκτρονικό Έγκλημα», διαθέσιμη: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

Παρόλα αυτά όμως το ηλεκτρονικό έγκλημα δεν είναι τόσο απλό και μπορεί να δεχθεί μια τριπλή προσέγγιση, η οποία τείνει να επικρατήσει σήμερα. Σύμφωνα με αυτήν, το ηλεκτρονικό έγκλημα μπορεί να θεωρηθεί ως[42]:

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

Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες, μερικές εκ των οποίων θα αναλυθούν παρακάτω και σύμφωνα με την Ελληνική Αστυνομία διακρίνονται στις εξής κατηγορίες:

1. Απάτες μέσω Διαδικτύου
2. Παιδική πορνογραφία
3. Cracking και hacking
4. Διακίνηση-πειρατεία λογισμικού
5. Πιστωτικές κάρτες
6. Διακίνηση ναρκωτικών
7. Έγκλημα στα chat rooms

Γενικότερα, ένα από τα σημαντικότερα σημεία αναφορικά με το έγκλημα στο διαδίκτυο είναι ότι είναι γρήγορο και διαπράττεται μέσα σε δευτερόλεπτα και πολλές φορές δε γίνεται αντιληπτό από το θύμα. Τα ίχνη που αφήνει είναι ψηφιακά και πολλές φορές δύσκολα ανιχνεύσιμα, καθώς πολλά από τα εγκλήματα απαιτούν εξειδικευμένες γνώσεις, οι οποίες εκλείπουν πολλές φορές και από τις ίδιες τις Αρχές δίωξης. Το ηλεκτρονικό έγκλημα δίνει τη δυνατότητα σε άτομα με ιδιαιτερότητες όπως οι παιδόφιλοι (child pornography) να επικοινωνούν γρήγορα και άμεσα σε πραγματικό χρόνο και να δημιουργούν ομάδες συζητήσεων μέσα στις οποίες ανταλλάσουν απόψεις και πληροφορίες και προβαίνουν στις εγκληματικές τους πράξεις πολλές φορές έπειτα από μεταξύ τους συνεννόηση[43].

[42] 1. Αγγελής Ι. (2000), «Διαδίκτυο (Διαδίκτυο) και ποινικό δίκαιο. Έγκλημα στον κυβερνοχώρο», Ποινικά Χρονικά, σελ. 675

[43] Ιστοσελίδα Ελληνικής Αστυνομίας (2013), «Ηλεκτρονικό Έγκλημα», διαθέσιμη: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

Η ψηφιακή πραγματικότητα και η δημιουργία σε αυτήν του ψηφιακού εγκλήματος στο Διαδίκτυο πλέον, στο οποίο συνδέονται καθημερινά εκατομμύρια άνθρωποι ανά τον κόσμο και ανταλλάσουν πληροφορίες και δεδομένα έχει δυστυχώς αναπόφευκτα μετατρέψει το χώρο αυτόν σε ένα πεδίο πολλές φορές ανεξέλεγκτης εγκληματικής δράσης, η οποία καθημερινά διογκώνεται και αναζητούνται συνεχώς τρόποι για την αποφυγή ή έστω τον περιορισμό αυτής.

3.2 Το «πρώτο» ηλεκτρονικό έγκλημα

Γενικότερα, η εμφάνιση του ηλεκτρονικού εγκλήματος μπορεί να τοποθετηθεί την ίδια χρονική περίοδο με αυτή των ηλεκτρονικών υπολογιστών. Οι «ηλεκτρονικοί εγκληματίες» προσπάθησαν από την εμφάνιση των ηλεκτρονικών υπολογιστών να βρουν τρόπους μέσα από τις νέες τεχνολογίες και να εκμεταλλευτούν προς όφελος των εγκληματικών τους σκοπών τα νέα μέσα που τους προσφέρονταν. Βέβαια, λόγω του ότι η τεχνολογία τα πρώτα χρόνια των ηλεκτρονικών υπολογιστών δεν ήταν τόσο αναπτυγμένη και απαιτούνταν εξειδικευμένες γνώσεις για τη χρήση τους, γεγονός που έκανε τους ηλεκτρονικούς υπολογιστές είδος πολυτελείας, το ηλεκτρονικό έγκλημα δεν είχε σε καμία περίπτωση τις σημερινές του διαστάσεις και μορφές[44].

Η εξάπλωση του Διαδικτύου και η μετατροπή του υπολογιστή σε εργαλείο του καθενός, αλλά και η απλοποίηση των χρησιμοποιούμενων συστημάτων συνέβαλε στη ραγδαία εξάπλωση του ηλεκτρονικού εγκλήματος. Βέβαια, το πρώτο καταγεγραμμένο ως ηλεκτρονικό έγκλημα είχε διαπραχθεί πολύ νωρίτερα, όταν ο Joseph – Marie Jacquard κατασκεύασε τον αργαλειό και χρονολογείται περί το 1820[45]. Η συσκευή επέτρεπε την επανάληψη μιας συγκεκριμένης ακολουθίας βημάτων, όμοιων μεταξύ τους κατά την ύφανση, κάτι το οποίο προκάλεσε ανησυχία στους υπαλλήλους του Jacquard οι οποίοι φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία και προκαλούσαν δολιοφθορές στο μηχάνημα για να αποθαρρύνουν τη χρήση της νέας τεχνολογίας[46]. Το παραπάνω αν και δε συμπεριλαμβάνει τη χρήση υπολογιστή, κατατάσσεται ως το πρώτο ηλεκτρονικό έγκλημα, λόγω της χρήσης μιας νέας τεχνολογίας.

---

[44] Βλαχόπουλος (2007), «Ηλεκτρονικό Έγκλημα», Εκδόσεις Νομικής Βιβλιοθήκης

[45] Βλαχόπουλος (2007), «Ηλεκτρονικό Έγκλημα», Εκδόσεις Νομικής Βιβλιοθήκης

[46] Βλαχόπουλος (2007), «Ηλεκτρονικό Έγκλημα», Εκδόσεις Νομικής Βιβλιοθήκης

3.3 Βασικές μορφές ηλεκτρονικού εγκλήματος

Η αυξανόμενη χρήση των υπολογιστών δε διαμόρφωσε απλά νέες συνθήκες καθημερινότητας, αλλά δημιούργησε πλήθος νέων μορφών αντικοινωνικής συμπεριφοράς, μετατρέποντας πολλές φορές τον υπολογιστή σε ένα νέο μέσο τέλεσης εγκλημάτων. Σύμφωνα με έκθεση του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) το ηλεκτρονικό έγκλημα ταξινομείται σε 5 βασικές κατηγορίες, οι οποίες είναι οι εξής:

1. Μη επιτρεπόμενη αντιγραφή ή χρήση προϊόντων Software και παραβίαση αποκλειστικών δικαιωμάτων του δημιουργού/νόμιμου κατόχου αυτών. Η συγκεκριμένη ενέργεια ονομάζεται «πειρατεία στο Software» και παραβιάζει τους κανόνες της πνευματικής ιδιοκτησίας
2. Εισαγωγή δεδομένων χωρίς εξουσιοδότηση ή καταστροφή δεδομένων στο/από το υπολογιστικό σύστημα
3. Αλλοίωση ή μείωση της αξιοπιστίας δεδομένων υπολογιστικού συστήματος
4. Παρεμπόδιση της λειτουργίας υπολογιστικού συστήματος
5. Εισβολή χωρίς της απαραίτητη άδεια σε υπολογιστικά συστήματα

Σε αυτά προστέθηκαν ακόμη τρεις κατηγορίες ηλεκτρονικού εγκλήματος, οι οποίες είναι οι εξής:

1. Ηλεκτρονικά οικονομικά εγκλήματα (απάτη, πλαστογραφία, ηλεκτρονικό σαμποτάζ)
2. Ηλεκτρονικά εγκλήματα κατά των ατομικών δικαιωμάτων
3. Εγκλήματα κατά της Εθνικής ασφάλειας και του ελέγχου, διασυνοριακή ροή πληροφοριών, κατά της δημοκρατικής νομιμότητας και της ακεραιότητας των κοινωνικών διαδικασιών κ.α. Η συγκεκριμένη κατηγορία γενικότερα περιλαμβάνει όλα τα «υπερατομικά» όπως ονομάζονται ηλεκτρονικά εγκλήματα.

3.3.1 Παιδική πορνογραφία

Η παιδική εκμετάλλευση υπήρξε από τα αρχαία ήδη χρόνια, συχνό φαινόμενο, ενώ τα δίκτυα παραβατών που επικοινωνούσαν πριν την ανακάλυψη των προσωπικών υπολογιστών και του Διαδικτύου ήταν μέρος της καθημερινής ζωής αν και χρειαζόταν μεγαλύτερη προσπάθεια να βρει κανείς και να εισάγει ένα δίκτυο εκμετάλλευσης των ανηλίκων.

Σήμερα, στην εποχή του Διαδικτύου, ένα από τα βασικότερα εγκλήματα που διαπράττονται μέσω αυτού, το οποίο τείνει να εξελιχθεί σε ένα φαινόμενο που δεν μπορεί να περιορισθεί είναι η διακίνηση παιδικού πορνογραφικού υλικού σε αυτό. Η διαφορά με το παγκόσμιο γίγνεσθαι, όπου υπάρχει οργανωμένη δράση, συγκριτικά με την Ελλάδα είναι το γεγονός ότι εντός της χώρας οι δράστες δρουν μεμονωμένα.

Η Παιδική πορνογραφία ορίζεται ως οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή. Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Σύμφωνα με το τμήμα της Δίωξης Ηλεκτρονικού Εγκλήματος Ελλάδος, παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση με οποιαδήποτε μέσο, ενός παιδιού που συμμετέχει σε πραγματικές η προσομοιωμένες σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών του για σεξουαλικούς σκοπούς. Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης, η παιδική πορνογραφία έχει τις εξής μορφές[47]:

- Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.
- Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.
- Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Το έγκλημα δηλαδή αυτό διαπράττεται όταν κάποιος από πρόθεση και προμελετημένα παράγει, διανέμει και μεταδίδει παιδικό πορνογραφικό υλικό μέσω Ηλεκτρονικού υπολογιστή. Σημειώνεται ότι το συγκεκριμένο αποτελεί ίσως τη

[47] Υπουργείο Παιδείας και Πολιτισμού Κύπρου (2014). Κίνδυνος: Παιδική Πορνογραφία. Ηλεκτρονικά διαθέσιμο: http://www.pi.ac.cy/InternetSafety/sec_kindinoi_pornografia.html, ανακτήθηκε στις 03/09/2014

μεγαλύτερη βιομηχανία στο χώρο του διαδικτύου, καθώς η ταχύτατη εξάπλωση, τα γενικά χαρακτηριστικά και οι ευκολίες τις οποίες παρέχει το διαδίκτυο έχουν ως αποτέλεσμα την ραγδαία αύξηση των κρουσμάτων online εκμετάλλευσης και πορνογραφίας ανηλίκων τα τελευταία χρόνια.

Η παιδική πορνογραφία συνδέεται άμεσα με την πραγματική και ηλεκτρονική σεξουαλική κακοποίηση ανηλίκων, την εμπορία παιδιών και τον σεξουαλικό τουρισμό. Οι δράστες των διαδικτυακών σεξουαλικών εγκλημάτων σε βάρος ανηλίκων, στην συντριπτική τους πλειονότητα τους άρρενες, δύναται να προέρχονται από οποιοδήποτε οικογενειακό, κοινωνικό, οικονομικό και επαγγελματικό περιβάλλον και να ανήκουν σε οποιαδήποτε ηλικιακή ομάδα, ή φυλή με μοναδικό κοινό τους χαρακτηριστικό την εντατική τους ενασχόληση με το διαδίκτυο. Τα ανήλικα θύματα ανήκουν επίσης σε όλες τις ηλικίες, από τη βρεφική μέχρι την εφηβική και προέρχονται κυρίως από προβληματικά οικογενειακά και κοινωνικά περιβάλλοντα με τις συνέπειες της κακοποίησης, διαδικτυακής ή/και πραγματικής να αποδεικνύονται τραυματικές τόσο βραχυπρόθεσμα, όσο και μακροπρόθεσμα[48].

Το πρόβλημα της παιδικής πορνογραφίας μπορεί να προσεγγισθεί από δυο πλευρές, αναφορικά με τη διάθεση του δράστη. Αρχικά, η όρεξη του δράστη για παράνομες πράξεις επί του συγκεκριμένου μπορεί να εκτονωθεί μέσω της εισόδου του σε μια πορνογραφική ιστοσελίδα, και να μην εκδηλωθούν διαστροφικές τάσεις στο υπόλοιπο πραγματικό κοινωνικό περιβάλλον. Βέβαια, πιθανό είναι τέτοιου είδους θεάματα να δημιουργήσουν ψύχωση και εμμονή στο δράστη με αποτέλεσμα η συμπεριφορά του να εκτονωθεί εις βάρος κάποιου ανήλικου ατόμου στον κοινωνικό τους περίγυρο[49].

Σημαντικό είναι να σημειωθεί ότι τα συγκεκριμένα κυκλώματα έχουν εδραιωθεί σε τέτοιο βαθμό που οι πορνογραφικές διευθύνσεις ανακοινώνονται πλέον ιδιωτικά και κάτω από συγκεκριμένη κωδικοποίηση, μέσω email στους ενδιαφερόμενους ή διαφημίζονται σε ιδιωτικές ομάδες συζητήσεων υπό παραπλανητικούς τίτλους, ενώ οι μηχανές αναζήτησης δεν καταδεικνύουν σε μια απλή έρευνα σελίδες τέτοιου περιεχομένου.

Ο σημαντικός ρόλος, τον οποίο καλείται να διαδραματίσει η επιστήμη της

[48] Φαρσεδάκης, Ι.Ι. (2007). Πορνογραφία και εκμετάλλευση ανηλίκων στο διαδίκτυο. Πανδημος. Παντειακές εκδόσεις

[49] Δήμου (2002), «Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων», Αθήνα

εγκληματολογίας για την κατανόηση και την αποτελεσματικότερη αντιμετώπιση του κενού αυτού φαινομένου, επιβάλει την επανεξέταση και τον επαναπροσδιορισμό των αρχών της, προκειμένου να μπορέσει να αγκαλιάσει θεωρητικά την νεοδημιουργηθείσα σεξουαλική κυβερνό-εγκληματικότητα, στην οποία υπάγεται και η εκμετάλλευση και η πορνογραφία των ανηλίκων στο διαδίκτυο ειδικότερα. Προκειμένου να προληφθεί επιτυχώς και να αντιμετωπιστεί αποτελεσματικά το φαινόμενο αυτό, έχουν υπάρξει σημαντικές πρωτοβουλίες, τόσο ήπιες– μη δικαιικές όσο και κατασταλτικές- δικαιικές σε διεθνές, ευρωπαϊκό αλλά και ελληνικό επίπεδο. Μόνες οι δικαιικές ρυθμίσεις ωστόσο, δεν είναι απόλυτα αποτελεσματικές, ενώ και οι νομοθετικές δράσεις δεν έχουν την αναμενόμενη επιτυχία, μιας και συνήθως οι τεχνολογικές εξελίξεις προηγούνται των δικαιικών ρυθμίσεων[50]

3.3.2 Πειρατεία λογισμικού

Το λογισμικό είναι μια πολύτιμη τεχνολογία στην σύγχρονη πληροφορική και χρησιμοποιείται καθημερινά στον ηλεκτρονικό υπολογιστή. Η ανάπτυξη του είναι ο συνδυασμός δημιουργικών ιδεών και γνώσεων προγραμματιστών, συγγραφέων και επιστημόνων της πληροφορικής. Πειρατεία λογισμικού ονομάζεται η παράνομη λήψη, αντιγραφή, και κοινοποίηση πνευματικών δικαιωμάτων των οποίων ο δημιουργός έχει εργαστεί επίμονα και σκληρά για να τα δημιουργήσει. Οι παραβάτες

[50] Φαρσεδάκης, Ι.Ι. (2007). Πορνογραφία και εκμετάλλευση ανηλίκων στο διαδίκτυο. Πανδημος. Παντειακές εκδόσεις

ονομάζονται πειρατές[51].

Το Διαδίκτυο βοηθά στην αύξηση των ευκαιριών για την πώληση προϊόντων και υπηρεσιών αλλά παράλληλα δημιουργεί ευκαιρίες για την κλοπή λογισμικού με αποτέλεσμα τα τελευταία χρόνια η παράνομη αναπαραγωγή και χρήση προγραμμάτων να έχει λάβει τεράστιες διαστάσεις λόγω της μεγάλης ευκολίας που μας προσφέρουν οι αντιγραφικές μηχανές. Αναφορικά με τα μέτρα που έχει πάρει το ελληνικό κράτος για την παράνομη αυτή δραστηριότητα, εκτός από την Ευρωπαϊκή Οδηγία για την Πνευματική Ιδιοκτησία με την οποία το ελληνικό κράτος έχει εναρμονισθεί από το 2004, το 2007 ψήφισε ένα νομοσχέδιο (ν. 3524/07) που προβλέπει την επιβολή διοικητικού προστίμου €1,000 για κάθε παράνομο/πειρατικό πρόγραμμα λογισμικού που εντοπίζεται σε έναν Η/Υ. Παράλληλα και άλλοι κρατικοί φορείς έχουν ενσωματώσει την προστασία της πνευματικής ιδιοκτησίας στους πρωταρχικούς τους στόχους[52]. Οι περιπτώσεις πειρατείας λογισμικού είναι οι ακόλουθες[53]:

1. Η δημιουργία παράνομων αντιγράφων προγράμματος από το αυθεντικό και η χρήση τους.

2.Η παράνομη εγκατάσταση προγραμμάτων χωρίς την άδεια του δημιουργού.

3.Η παράνομη αναπαραγωγή και διάθεση αντιγράφων προγραμμάτων με κίνητρο το οικονομικό όφελος.

Το ποσοστό πειρατείας λογισμικού στην Ελλάδα αγγίζει το 61% και είναι το υψηλότερο ποσοστό στην Ευρώπη των 27 κρατών-μελών (μέσος όρος 36%), ενώ η αξία του παράνομα εγκατεστημένου λογισμικού στη χώρα μας εκτιμάται στο 128 εκατομμύρια ευρώ. Στην προηγούμενη έρευνα της BSA το 2005 για το ποσοστό πειρατείας το αντίστοιχο ποσοστό ήταν 64% (On-line κοινότητα των φοιτητών

[51] Βλαχόπουλος (2007), «Ηλεκτρονικό Έγκλημα», Εκδόσεις Νομικής Βιβλιοθήκης

[52]Business Software Alliance (2010), «Η πειρατεία λογισμικού», διαθέσιμο ηλεκτρονικά: http://webcache.googleusercontent.com/search?q=cache:ojwxCrgwJeAJ:blogs.sch.gr/plinetfk/files/2009/05/sw-piracy.pdf+&cd=2&hl=el&ct=clnk&gl=gr

[53]Βλασσόπουλος Γ. (2012), «Πειρατεία Λογισμικού», διαθέσιμο ηλεκτρονικά: http://7gym-perist.att.sch.gr/autosch/joomla15/attachments/article/18/%CE%A0%CE%B5%CE%B9%CF%81%CE%B1%CF%84%CE%B5%CE%AF%CE%B1%20%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%BF%CF%8D%20-%20Giannis%20Vlassopoulos.pdf

Πληροφορικής του Ο.Π.Α, 2007), ενώ η Πειρατεία Λογισμικού στην Ελλάδα μειώθηκε κατά 1 ποσοστιαία μονάδα το 2008 φθάνοντας στο 57%, και σημειώνοντας συνολική πτώση 7 ποσοστιαίων μονάδων την τριετία 2005-2008[54]. Τα τελευταία χρόνια, το ελληνικό κράτος έχει πραγματοποιήσει αξιόλογα βήματα για την προστασία της πνευματικής ιδιοκτησίας με τη θεσμοθέτηση πρωτοποριακών νόμων που στοχεύουν στην καταπολέμηση της πειρατείας των έργων διανοητικής ιδιοκτησίας. Εάν η δράση των στελεχών του ΣΔΟΕ και της αρμόδιας υπηρεσίας του συνεχίσει με ακόμα πιο εντατικό ρυθμό και το 2012, υπάρχει έντονη αισιοδοξία ότι η Ελλάδα θα καταφέρει να μειώσει το ποσοστό της πειρατείας λογισμικού που αυτή τη στιγμή ανέρχεται στο 59%[55].

Για το έτος 2013 συνεχίζονται οι έλεγχοι του ΣΔΟΕ για τα παραπάνω με εντατικό ρυθμό και τα αποτελέσματα αυτών κοινοποιούνται στους δικαιούχους μέσω του Οργανισμού Πνευματικής Ιδιοκτησίας, ενώ οι κυρώσεις που συνεπάγεται η χρήση παράνομου λογισμικού είναι τριών ειδών:

- διοικητικές
- αστικές και
- ποινικές

Οι διοικητικές κυρώσεις αφορούν στην επιβολή διοικητικού προστίμου από το ΣΔΟΕ, το οποίο ανέρχεται στα 1.000€ για κάθε παράνομο αντίτυπο που εντοπίζεται κατά τον έλεγχο. Από το 2011 μέχρι και σήμερα έχει επιβληθεί διοικητικό πρόστιμο συνολικού ύψους 9,000,000 ευρώ, κατά προσέγγιση, εις βάρος επιχειρήσεων που έχουν ελεγχθεί. Μέχρι σήμερα το 93,2 % των παραβατών έχει προβεί στην ανεπιφύλακτη καταβολή του επιβληθέντος διοικητικού προστίμου, ενώ μόνο 6,8% των περιπτώσεων έχει αχθεί ενώπιον των ποινικών δικαστηρίων. Όσον

[54] Business Software Alliance (2010), «Η πειρατεία λογισμικού», διαθέσιμο ηλεκτρονικά: http://webcache.googleusercontent.com/search?q=cache:ojwxCrgwJeAJ:blogs.sch.gr/plinetfk/files/2009/05/sw-piracy.pdf+&cd=2&hl=el&ct=clnk&gl=gr

[55] 19. Μίμης (2011) «ΣΔΟΕ: Πρόστιμα για παράνομο λογισμικό», διαθέσιμο ηλεκτρονικά: http://www.star-fm.gr/2011/11/02/%CE%A3%CE%94%CE%9F%CE%95-%CE%A0%CF%81%CF%8C%CF%83%CF%84%CE%B9%CE%BC%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%80%CE%B1%CF%81%CE%AC%CE%BD%CE%BF%CE%BC%CE%BF-%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C/

αφορά τις αστικές κυρώσεις, αυτές συντρέχουν ταυτόχρονα με τις διοικητικές και συνακόλουθα οι παραβάτες υποχρεούνται τόσο στην καταβολή του διοικητικού προστίμου, όσο και στην καταβολή αποζημίωσης στους εκάστοτε δικαιούχους, η οποία ισούται τουλάχιστον με το διπλάσιο της αγοραίας αξίας των προγραμμάτων που βρέθηκαν να είναι εγκατεστημένα χωρίς άδεια[56].

Το πειρατικό λογισμικό δεν αποτελεί μονάχα οικονομικό ρίσκο στην περίπτωση οικονομικών κυρώσεων, αλλά εγκυμονεί κινδύνους από ιούς και παγίδες ασφαλείας στο δίκτυο των υπολογιστών, όπως η απώλεια αρχείων, ενώ οι αρνητικές συνέπειες της Πειρατείας Λογισμικού εκτείνονται πέραν των οικονομικών και των συνεπειών της βιομηχανίας πληροφορικής. Αγγίζουν ταυτόχρονα την αγορά εργασίας στερώντας χιλιάδες θέσεις εργασίας σε ταλαντούχους και πτυχιούχους Έλληνες[57].

3.3.3 Οικονομικό Έγκλημα

Τα πληροφοριακά οικονομικά εγκλήματα είναι εκείνα που διαπιστωμένα απασχολούν τους διάφορους ερευνητές που ασχολούνται με τα ηλεκτρονικά εγκλήματα. Μάλιστα η συγκεκριμένη μορφή είναι κι αυτή που συναντάμε πολύ περισσότερο συγκριτικά με τις υπόλοιπες κατηγορίες. Το οικονομικό έγκλημα είναι μια μορφή που γίνεται εύκολα αντιληπτό από τους ενδιαφερόμενους σε σχετικά μικρό

[56]Δελτίο Τύπου ΣΔΟΕ (2013), «ΣΔΟΕ πειρατεία λογισμικού», διαθέσιμο ηλεκτρονικά: http://web.opi.gr/portal/page/portal/opi/newsall/press/sdoe_el

[57]Business Software Alliance (2010), «Η πειρατεία λογισμικού», διαθέσιμο ηλεκτρονικά: http://webcache.googleusercontent.com/search?q=cache:ojwxCrgwJeAJ:blogs.sch.gr/plinetfk/files/2009/05/sw-piracy.pdf+&cd=2&hl=el&ct=clnk&gl=gr; On-line κοινότητα των φοιτητών Πληροφορικής του Ο.Π.Α (2007), ««Πειρατές» λογισμικού 6 στους 10 Έλληνες χρήστες Η/Υ», διαθέσιμο ηλεκτρονικά: http://t-h.wikispaces.com/file/view/%C2%AB%CE%A0%CE%B5%CE%B9%CF%81%CE%B1%CF%84%CE%AD%CF%82%C2%BB+%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%BF%CF%8D+6+%CF%83%CF%84%CE%BF%CF%85%CF%82+10+%CE%88%CE%BB%CE%BB%CE%B7%CE%BD%CE%B5%CF%82+%CF%87%CF%81%CE%AE%CF%83%CF%84%CE%B5%CF%82+%CE%97%CE%A5.pdf/32305559/%C2%AB%CE%A0%CE%B5%CE%B9%CF%81%CE%B1%CF%84%CE%AD%CF%82%C2%BB%20%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%BF%CF%8D%206%20%CF%83%CF%84%CE%BF%CF%85%CF%82%2010%20%CE%88%CE%BB%CE%BB%CE%B7%CE%BD%CE%B5%CF%82%20%CF%87%CF%81%CE%AE%CF%83%CF%84%CE%B5%CF%82%20%CE%97%CE%A5.pdf

χρονικό διάστημα από την τέλεση του, ενώ είναι και μετρήσιμο επίσης εύκολα και γρήγορα από τις διωκτικές αρχές[58].

Στο πλαίσιο του συγκεκριμένου εγκλήματος περιλαμβάνονται η παραποίηση δεδομένων ή πληροφοριών που βρίσκονται σε βάσεις δεδομένων ή προγράμματα οικονομικού κέρδους και οφέλους. Αφορά συνήθως και κατά κύριο λόγο την κλοπή, τη διαγραφή, την αλλοίωση ή την προσθήκη δεδομένων ή πληροφοριών με απώτερο σκοπό το οικονομικό όφελος κάποιου σε βάρους κάποιου άλλου (ιδιώτη ή επιχείρησης συνήθως).

3.3.4 Online Κοινωνικά Δίκτυα και Ηλεκτρονικό Έγκλημα

Τα online κοινωνικά δίκτυα (ιστότοποι κοινωνικής δικτύωσης) είναι κοινότητες του Διαδικτύου, όπου τα άτομα αλληλεπιδρούν μέσω των προφίλ που έχουν δημιουργήσει και παρουσιάζουν δημόσια την εικόνα τους. Αν και η έννοια της αυτών των κοινοτήτων χρονολογείται από τις απαρχές σχεδόν της δημιουργίας των δικτύων υπολογιστών, οι δραστηριότητες αυτών γνώρισαν μεγάλη επιτυχία και αναγνωρίσθηκαν, χρησιμοποιήθηκαν από το ευρύ κοινό, μόνο μετά την έλευση του Διαδικτύου[59]. Οι ιστότοποι κοινωνικής δικτύωσης διακρίνονται σε διάφορες κατηγορίες ανάλογα με ορισμένα χαρακτηριστικά τους στοιχεία, όπως[60]:

- το αντικείμενό τους (το στόχο της δικτύωσης),
- τον τρόπο εγγραφής και συμμετοχής μελών (ελεύθερη ή περιορισμένη),
- τον τρόπο επικοινωνίας μεταξύ των μελών τους και
- το είδος του περιεχομένου που ανταλλάσσουν οι χρήστες μεταξύ τους.

Όποια και αν είναι η μορφή της ή τα χαρακτηριστικά τους, τα online κοινωνικά δίκτυα έχουν στην πλειονότητα τους ένα βασικό χαρακτηριστικό, το οποίο δεν είναι άλλο από τα ορατά προφίλ των χρηστών, στα οποία συνδέεται ένας αριθμός «φίλων», «ακολούθων» ή όπως αλλιώς ονομάζονται οι χρήστες που συνδέονται

[58]Λάζος Γ. (2001), «Πληροφορική και έγκλημα», Νομική Βιβλιοθήκη

[59]Acquisti A &. Gross R. (2006), "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook"

[60]Jagatic, T., Johnson, N., Jakobsson, M., Menczer, F. (2007). "Social phishing". Communications of the ACM, 5 (10), 94-100

μεταξύ τους. Για να δημιουργήσει κάποιος ένα προφίλ σε ένα online κοινωνικό δίκτυο απαντά σε μια σειρά ερωτήσεων σχετικών με τα χαρακτηριστικά των χρηστών, όπως είναι η ηλικία τους, το επάγγελμά τους, η εκπαίδευση και τα ενδιαφέροντα τους[61]. Η διαφάνεια και η προσβασιμότητα ενός προφίλ διαφέρει από δίκτυο σε δίκτυο ανάλογα με την ιστοσελίδα και τα αιτήματα των χρηστών ως προς την ιδιωτικότητα (privacy) των στοιχείων τους. Τα δημοφιλέστερα online κοινωνικά δίκτυα (Social Media) παγκοσμίως είναι τα εξής:

- Twitter, το οποίο δημιουργήθηκε το 2006, το οποίο είναι αρκετά απλό και εύχρηστο με μικρότερο όγκο πληροφοριών σχετικών με τους χρήστες. Αποτελεί κατ' ουσία μια εφαρμογή micro-blogging και κερδίζει καθημερινά όλο και μεγαλύτερη δημοτικότητα.
- Facebook. Το Facebook, λανσαρίστηκε το 2004, από έναν φοιτητή του Harvard, τον γνωστό πλέον σε όλους Mark Zuckerberg και άνοιξε την πρόσβαση στο ευρύ κοινό το 2006. Αυτή τη στιγμή ο ιδρυτής του είναι ένας από τους πλουσιότερους ανθρώπους στον κόσμο και αν το Facebook σήμερα ήταν χώρα, σύμφωνα με τους καταγεγραμμένους αριθμούς χρηστών θα ήταν θα ήταν η τρίτη μεγαλύτερη σε πληθυσμό χώρα στον πλανήτη.
- Google Plus. Τον Ιούνιο του 2011, η εταιρεία Google ανακοίνωσε μια δοκιμαστική έκδοση μιας νέας σελίδας κοινωνικής δικτύωσης με το όνομα Google Plus (Google+), η οποία αποτελεί την πιο πρόσφατη προσπάθεια να δημιουργηθεί ένα κοινωνικό δίκτυο που θα ανταγωνίζεται επάξια το Facebook. Το Google Plus δίνει τη δυνατότητα στους χρήστες του να ανταλλάξουν πληροφορίες και να μοιραστούν με τους υπόλοιπους χρήστες που εκείνοι θα έχουν επιλέξει να βρεθούν στο διαδικτυακό τους χώρο (circles) εικόνες, βίντεο κ.α.
- LinkedIn. Πρόκειται για ένα κοινωνικό δίκτυο, το οποίο αναφέρεται σε κάθε μορφής επιστήμονα και επαγγελματία και γνωρίζει το τελευταίο διάστημα μεγάλη απήχηση από το επιστημονικό και ερευνητικό κοινό όλων των χωρών. Το Φεβρουάριο του 2012, το LinkedIn αποτελούσε το μεγαλύτερο επαγγελματικό social networking site παγκοσμίως με 150 εκατομμύρια χρήστες σε πάνω από 200 χώρες[62].
- YouTube. Το YouTube ξεκίνησε τη λειτουργία του τον Φεβρουάριο

[61]Boyd D., Ellison N., (2007), "Social Network Sites: Definition, History and Scholarship", Journal of Computer-Mediated Communication, Vol. 13, No.1

[62] About LinkedIn, Διαθέσιμο Ηλεκτρονικά: http://press.linkedin.com/about

του 2005 και αποτελεί ένα πασίγνωστο πλέον social networking site, το οποίο επιτρέπει στους χρήστες να αναρτούν ή απλά να βλέπουν βίντεο. Ο κάθε χρήστης μπορεί να δημιουργήσει προσωπικό προφίλ και να κάνει «φιλίες» με άλλους χρήστες. Σήμερα εμφανίζεται το τρίτο σε κατάταξη των δημοφιλέστερων ιστοσελίδων πίσω από Google και το Facebook. Το Δεκέμβριο του 2010, το YouTube αριθμούσε στους 500 εκ. χρήστες παγκοσμίως με την πλειοψηφία αυτών να βρίσκονται μεταξύ 25-54 ετών με ένα ποσοστό που άγγιζε το 46%. Σύμφωνα με τα επίσημα στοιχεία της εταιρεία το έτος 2011, το YouTube είχε περισσότερες από 1 τρισεκατομμύριο προβολές, δηλαδή σε κάθε άτομο πάνω στη γη αντιστοιχούσαν περίπου ετησίων 140 προβολές.

Γενικότερα, αυτό που παρατηρείται τα τελευταία χρόνια είναι ότι οι χρήστες του Διαδικτύου χρησιμοποιούν όλο και περισσότερο τα κοινωνικά δίκτυα στην καθημερινότητα τους και υπάρχουν πολλοί που εξαρτώνται από αυτά. Το συγκεκριμένο, σε συνδυασμό με τα όσα αναφέρθηκαν παραπάνω έχει δώσει τη δυνατότητα σε διάφορους παραβάτες να υιοθετούν αντικοινωνικές συμπεριφορές μέσα από αυτά τα δίκτυα. Δεν είναι λίγοι οι χρήστες εκείνοι που έχουν εξαπατηθεί μέσω κάποιου τρίτου ατόμου στο πεδίο των κοινωνικών δικτύων.

Στην προκειμένη περίπτωση, η «επίθεση» ξεκινά συνήθως από κάποιο μήνυμα ή αίτημα φιλίας του θύτη προς το θύμα ή ακόμη και μέσω φαινομενικά «αθώων» link τα οποία παραπέμπουν σε κάποιο βίντεο, φωτογραφία, εφαρμογή κλπ. Έπειτα, ο θύτης αποσπά πληροφορίες και προσωπικά στοιχεία από το θύμα και τα χειρίζεται αναλόγως των προθέσεων του. Σύμφωνα με άρθρο που δημοσιεύτηκε στην εφημερίδα *Καθημερινή* παρουσιάζεται εντυπωσιακή αύξηση στον αριθμό των επιτήδειων που στοχεύουν τα online κοινωνικά δίκτυα τα οποία μάλιστα χαρακτηρίζονται ως «χρυσορυχεία» προσωπικών πληροφοριών. Σύμφωνα με στοιχεία από το FBI από το 2006, περίπου 3.200 λογαριασμοί χρηστών έχουν δεχτεί κάποιας μορφής επίθεση. Αυτό που παρατηρείται είναι ότι η εξαπάτηση μέσω αυτών των δικτύων στην πλειονότητα τους έχει σκοπό το κέρδος. Χαρακτηριστικό μάλιστα παράδειγμα αποτελεί το Twitter, όπου υπήρξαν δεκάδες επιθέσεις ψεύτικης ιστοσελίδας, πανομοιότυπης με αυτήν γνωστής υπηρεσίας, όπου παρότρυνε τους χρήστες να εισάγουν στοιχεία τους, τα οποία στη συνέχεια και χρησιμοποιούσε προς εξαπάτηση τους[63]. Σημαντικός είναι και ο αριθμός επιθέσεων των hackers εν γένει

[63] 3. Άρθρο από την Ηλεκτρονική Έκδοση της Εφημερίδας Καθημερινή (2009) με θέμα: «Στόχος εξαπάτησης τα Social Media», Διαθέσιμο ηλεκτρονικά: http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_21/10/2009_303476

προς χρήστες των Social Media, όπου προσβάλλουν τον υπολογιστή τους με κάποιας μορφής ιό και καταστρέφουν τα αρχεία και τις βάσεις δεδομένων τους.

Για το λόγο αυτό τα ίδια τα Social Media προσπαθούν να εισάγουν ρυθμίσεις και να ενημερώσουν τους χρήστες τους για τους διάφορους κινδύνους που ενέχει η αλόγιστη και χωρίς προσοχή χρήση τους. Μάλιστα το Facebook ενημερώνει μέσα από ειδικό λογαριασμό τους χρήστες του για το Ηλεκτρονικό Έγκλημα και το πώς αυτό μπορεί να καταπολεμηθεί από τους ίδιους τους χρήστες οι οποίοι προτρέπονται να μην πέσουν θύματα εξαπάτησης από επίδοξους διαδικτυακούς εγκληματίες.

3.3.5 Διαδικτυακή τρομοκρατία

Σύμφωνα με το FBI, ως διαδικτυακή τρομοκρατία ή όπως είναι γνωστό στην αγγλική: cyber terrorism, ορίζεται *η προσχεδιασμένη και πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες*[64].

Η μορφή αυτή του εγκλήματος είναι ιδιαίτερη εύκολη, καθώς οι ενέργειες εντοπίζονται δύσκολα και μπορούν να έχουν πολλαπλούς στόχους ταυτόχρονα. Άλλωστε, το Διαδίκτυο είναι ένας χώρος που μπορεί ο καθένας να αποκρύψει την πραγματική του εικόνα και να διατηρήσει την ανωνυμία του με αποτέλεσμα να είναι δύσκολα προσβάσιμα τα πραγματικά του στοιχεία. Επομένως, οι διαδικτυακοί τρομοκράτες έχουν περισσότερο χρόνο στη διάθεση τους για να εξαπολύσουν τις επιθέσεις τους και το ενδεχόμενο να μη γίνει ποτέ γνωστή η πραγματική τους ταυτότητα, αφού έχουν παρακάμψει όλες τις ασφαλιστικές δικλείδες, είναι αρκετά σημαντικό.

Αξίζει να σημειωθεί ότι οι φόβοι των αρχών περί του συγκεκριμένου θέματος έχουν αυξηθεί, καθώς ήρθαν στο φως της δημοσιότητας στοιχεία σχετικά με ορισμένες κακόβουλες πράξεις, οι οποίες συνέβαλαν στην επιδείνωση της οικονομικής κρίσης στα τέλη του 2008. Μία έκθεση για τους οικονομικούς πολέμους που συντάχθηκε το 2009 για λογαριασμό του Πενταγώνου και δημοσιεύθηκε το 2011, ανέφερε χαρακτηριστικά ότι υπάρχουν ενδείξεις περί ύπαρξης ανώνυμων

[64] Ιστοσελίδα FBI (2013), http://www.fbi.gov/

επιχειρηματιών, οι οποίοι προειδοποίησαν τις Αρχές για περίεργα εμπορικά πρότυπα την περίοδο που «κατέρρευσε» η Lehman Brothers[65].

Επίσης, ένα άλλο παράδειγμα σχετικά με την ηλεκτρονική τρομοκρατία, αυτή τη φορά όμως χωρίς να περιέχονται στοιχεία «οικονομικών πολέμων» και παρεμφερών επιθέσεων, είναι το παράδειγμα του δεκαπεντάχρονου Αμερικανού που λειτουργούσε με το όνομα «Chameleon». Ο συγκεκριμένος νεαρός βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Τότε, ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, και θεωρήθηκε ύποπτος ότι για τον βομβαρδισμό των Αμερικανικών βάσεων στην Ανατολική Αφρική το 1998 και συνεπώς στην κορυφή του καταλόγου των καταζητούμενων του FBI. Στον Chameleon δόθηκαν 1000 $ προκαταβολικά για την ανταλλαγή με το software και θα έπαιρνε επιπλέον 10.000 $ με την πρόοδο της εργασίας. Ευτυχώς το FBI τον συνέλαβε προτού να έχει την ευκαιρία να διανέμει τα στοιχεία[66].

3.3.6 Hacking

Το Hacking αφορά τη μη εξουσιοδοτημένη πρόσβαση και χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας καταρχήν δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους από την εν λόγω «επίθεση, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας εισβολής σε ένα υπολογιστικό σύστημα. Η έννοια του hacking είναι ευρεία και μπορεί να αφορά από το νομικό και έγκριτο πληροφορικό προγραμματισμό έως μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να οριστούν ως παράνομες και

[65] Εφημερίδα ΚΑΘΗΜΕΡΙΝΗ (2012), «Η «διαδικτυακή τρομοκρατία» απειλεί τη διεθνή οικονομία», διαθέσιμο ηλεκτρονικά: http://portal.kathimerini.gr/4dcgi/_w_articles_kathextra_7_14/01/2012_422676

[66] Ιστοσελίδα FBI (2013), http://www.fbi.gov/

εγκληματικές[67].

Ο επιτιθέμενός ή αλλιώς hacker, εισχωρώντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του συγκεκριμένου, εντοπίζει πιθανά αδύνατα σημεία του και έτσι μπορεί στη συνέχεια αν θέλει να διαπράξει κακόβουλη επίθεση ή ακόμα και να διαθέσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει στην επίθεση. Η δράση των hackers δεν είναι πάντα καταστροφική και συνδεδεμένη με εγκληματικές πράξεις βανδαλισμού. Οι τεχνικές που χρησιμοποιούν οι hackers είναι οι εξής:

· Εκμετάλλευση των Cookies. Τα Cookies είναι μικρά αρχεία τα οποία τοποθετούνται σε κάθε Η/Υ από διάφορες δικτυακές τοποθεσίες που επισκέπτεται ο χρήστης. Στα εν λόγω αρχεία περιέχονται πληροφορίες που αφορούν το χρήστη, όπως τα προσωπικά του στοιχεία ή δραστηριότητες του. Ο hacker λοιπόν έχει τη δυνατότητα να ανακτήσει αυτά τα χρήσιμα για το χρήστη δεδομένα (όνομα και κωδικό πρόσβασης για κάποια υπηρεσία), εφόσον ως «ειδικός» έχει αρχικά εντοπίσει πιθανή ευπάθεια να πλήττει το ηλεκτρονικό σύστημα.

· Ανίχνευση δικτυακών υπηρεσιών συστημάτων. Ο σκοπός του hacker σε αυτή την περίπτωση είναι η συγκέντρωση πληροφοριών σχετικά με το σύστημα το οποίο στοχεύει. Η τεχνική που χρησιμοποιεί είναι αυτή της σάρωσης των θυρών (port scanning). Το port scanning είναι επιτρεπτό εντός τοπικών δικτύων, αποτελεί όμως κακόβουλη ενέργεια σε περίπτωση που κάποιος αναζητά αδυναμίες σε ένα σύστημα. Η ανίχνευση ενεργειών port scanning είναι δύσκολη αν και υπάρχουν προγράμματα λογισμικού με τη χρήση των οποίων μπορεί να επιβεβαιωθεί η ύπαρξη απόπειρας πρόσβασης σε δεδομένα του συστήματος του χρήστη. Τα συγκεκριμένα προειδοποιούν κάθε φορά που γίνεται επίθεση στο σύστημα και καταγράφουν την IP διεύθυνση με την οποία ήταν συνδεδεμένος ο επιτιθέμενος.

· Ανίχνευση δικτυακών πακέτων. Το παραπάνω πραγματοποιείται με τις εφαρμογές λογισμικού packet sniffers. Ο packet sniffer «συλλαμβάνει» τα μηνύματα που ανταλλάσει ο χρήστης (αποστέλλει ή λαμβάνει). Εφόσον τα μηνύματα δεν είναι κρυπτογραφημένα, είναι δυνατή η απόσπαση πληροφοριών τους, όπως κωδικοί πρόσβασης πιστωτικών καρτών. Ο packet sniffer επίσης αποθηκεύει και απεικονίζει τα περιεχόμενα διάφορων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που συλλαμβάνει. Ακόμα, ο packet sniffer έχει δυνατότητες λήψης

[67] Λάζος (2001), «Πληροφορική και έγκλημα», Νομική Βιβλιοθήκη

πληροφοριών σχετικά με την τοπολογία ενός δικτύου, του αριθμού των συνδεδεμένων στο δίκτυο υπολογιστών κλπ.

Η Ελληνική Νομοθεσία

4.1 Τι συμβαίνει στην ελληνική νομοθεσία

Οι νομοθετικές ρυθμίσεις που αφορούν τα ψηφιακά εγκλήματα παρουσιάζουν αδυναμίες τόσο στην ελληνική, όσο και στην παγκόσμια νομοθεσία, καθώς οι εξελίξεις είναι συνεχείς και ο νομοθέτης είναι αναγκασμένος να ενημερώνεται συνεχώς. Η ψηφιακή εγκληματικότητα αποτελεί δραστηριότητα εξειδικευμένης και ανεπτυγμένης τεχνολογίας και ο κάθε νομοθέτης πρέπει να είναι πλήρως ενημερωμένος για την τεχνολογία που χρησιμοποιείται και κατ' επέκταση ποια μορφή μπορεί αυτή να πάρει και να χρησιμοποιηθεί με κακόβουλους σκοπούς.

Ένα σημαντικό πρόβλημα ως προς την υιοθέτηση νομοθεσίας σχετικά με το έγκλημα, είναι ακριβώς ο παγκόσμιος χαρακτήρας του, καθώς ο γεωγραφικός τόπος που διαπράττεται ένα «παραδοσιακό» έγκλημα είναι προσδιοριστικό στοιχείο αυτού και αντιμετωπίζεται ανάλογα στην κάθε περιοχή. Στην περίπτωση του ηλεκτρονικού εγκλήματος είναι αρκετά δύσκολο να εντοπισθεί ο πραγματικός τόπος διάπραξης του και να αντιμετωπισθεί κατάλληλα σε αυτόν. Επίσης, οι συνέπειες του μπορεί ταυτόχρονα να εμφανιστούν σε περισσότερες από μια χώρες, όπου σε καθεμία εξ αυτών ισχύει διαφορετικό νομικό καθεστώς.

Στις ΗΠΑ, ο πρώτος νόμος για το ηλεκτρονικό έγκλημα θεσπίστηκε το 1984 και παρουσιάστηκε έλλειψη ορολογίας σχετιζόμενης με αυτό, αλλά και με τους ηλεκτρονικούς υπολογιστές. Τροποποιήθηκε το 1986, χρησιμοποιώντας πλέον νέα ορολογία. Στη Μεγάλη Βρετανία ο πρώτος νόμος για το Ηλεκτρονικό έγκλημα υιοθετήθηκε το 1990 σύμφωνα με τις οδηγίες του Καναδά και της Ιρλανδίας[68] και ονομάστηκε Computer Misuse Act.

Έκτοτε έχουν γίνει πολλές διεθνείς προσπάθειες για την πάταξη του Ηλεκτρονικού εγκλήματος, κυρίως μέσω των οποίων έχει θεσπιστεί και η ανάλογη Ελληνική Νομοθεσία. Συγκεκριμένα, η ελληνική νομοθεσία περιλαμβάνει πολλά διαφορετικά σημεία στα οποία αναφέρεται το Ηλεκτρονικό έγκλημα, οι μορφές τους

[68]WIKIPEDIA (2o13), «Computer Misuse Act 1990», διαθέσιμο ηλεκτρονικά: http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990#The_Computer_Misuse_Act

και πως αυτά αντιμετωπίζονται. Αναφορικά με τα άρθρα που αναφέρονται στο Ηλεκτρονικό έγκλημα στον Ποινικό Κώδικα, αυτά είναι τα εξής[69]:

· Άρθρο 337 - Προσβολή της γενετήσιας αξιοπρέπειας. Το συγκεκριμένο αναφέρεται σε όποιον 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.

· Άρθρο 348 - Διευκόλυνση ακολασίας άλλων. Το παρόν άρθρο αναφέρει ότι όποιος διευκολύνει την ασέλγεια μεταξύ άλλων χρησιμοποιώντας απατηλά μέσα τιμωρείται με φυλάκιση μέχρι τριών ετών και με χρηματική ποινή.

· Άρθρο 348Α - Πορνογραφία ανηλίκων. Στη συγκεκριμένη περίπτωση αναφέρεται ότι 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, ενώ η τέλεση των παραπάνω μέσω ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

· Άρθρο 348Β - Προσέλκυση παιδιών για γενετήσιους λόγους. 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.

· Άρθρο 370Β - Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα. Στη συγκεκριμένη περίπτωση 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,

[69] Άρθρα Ποινικού Κώδικα, ηλεκτρονικά διαθέσιμα: http://www.e-crime.gr/nomothesia/PoinKod.pdf

τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών.

Πέρα από τα παραπάνω άρθρα η ελληνική πολιτεία έχει θεσπίσει διάφορους κανονισμούς και έχει υιοθετήσει και ευρωπαϊκά μέτρα για την πάταξη του συγκεκριμένου εγκλήματος, αν και σύμφωνα με στοιχεία της Ελληνικής Αστυνομίας, δεν υπάρχει ελληνικός νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Για το λόγο αυτό, όπως και προαναφέρθηκε η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και διεθνείς οργανισμούς για να αντιμετωπίσει τέτοιου είδους θέματα[70].

Αναφορικά με τους Νόμους που σχετίζονται με το Ηλεκτρονικό Έγκλημα, είναι όλοι ιδιαίτερα πρόσφατοι με τον παλαιότερο να πρόκειται για το Ν. 2472/1997, ο οποίος αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επίσης, υπάρχουν οι εξής νόμοι του Ελληνικού Κράτους σχετικά με τις μορφές του Ηλεκτρονικού Εγκλήματος[71]:

Ä Ν. 3471/2006, περί προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής του ατόμου στον τομέα των ηλεκτρονικών επικοινωνιών. Ο συγκεκριμένος αφορά κατ' ουσία τροποποίηση του Ν. 2472/1997

Ä Ν. 3917/2011. Ο συγκεκριμένος αφορά τη 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.

Ο προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος της Δ/νσης Ασφάλειας Αττικής, Αστυνόμος Α' κ. Εμμανουήλ Σφακιανάκης παρατηρεί ότι[72]:

«οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες, τόσο στην Ελλάδα όσο και στις υπόλοιπες χώρες. Αυτό συμβαίνει διότι το Ηλεκτρονικό Έγκλημα αποτελεί εγκληματική δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται

[70]Ιστοσελίδα Ελληνικής Αστυνομίας (2013), «Ηλεκτρονικό Έγκλημα», διαθέσιμη: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

[71] Άρθρα Ποινικού Κώδικα, ηλεκτρονικά διαθέσιμα: http://www.e-crime.gr/nomothesia/PoinKod.pdf

[72] Internet και Ηλεκτρονικό Έγκλημα (2007), Διαθέσιμο ηλεκτρονικά: http://dide.flo.sch.gr/Plinet/Tutorials/Internet-ElectronicCrime-LionHeart.pdf, ανακτήθηκε στις 28/08/2014

προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον, οι νομοθέτες είναι αναγκασμένοι να ενημερώνονται διαρκώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθούν με τον τρόπο διάπραξης αδικημάτων μέσω αυτών».

4.2 Υπηρεσία δίωξης ηλεκτρονικού εγκλήματος

Η Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος αποτελεί μέρος της Ελληνικής Αστυνομίας και αναφέρεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας. Η αποστολή της συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας[73]. 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, η δομή της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος είναι[74]:

- 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.

[73]Ιστοσελίδα Ελληνικής Αστυνομίας (2013), «Ηλεκτρονικό Έγκλημα», διαθέσιμη: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

[74] 15. Ιστοσελίδα Ελληνικής Αστυνομίας (2013), «Ηλεκτρονικό Έγκλημα», διαθέσιμη: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite

Στα παραπάνω πλαίσια και έχοντας ως μοναδικό σκοπό τη φύλαξη των ατόμων από επιβλαβείς συμπεριφορές εις βάρος τους η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος πέρα από οποιαδήποτε άλλη δράση της επιτελεί και κοινωνικό έργο, μέσω των δράσεων της. Συγκεκριμένα, όπως χαρακτηριστικά αναφέρεται στον επίσημο διαδικτυακό τόπο της Ελληνικής Αστυνομίας, η υπηρεσία αναπτύσσει έντονη δραστηριότητα για την ενημέρωση χρηστών του διαδικτύου όλων των ηλικιών και οργανώνει ημερίδες για την ενημέρωση του κοινού ως προς την ασφαλή πλοήγηση του. Οι παραπάνω δράσεις λαμβάνουν χώρα σε όλη τη Ελλάδα, έχοντας ως βασικό στόχο την ενδελεχή ενημέρωση των Ελλήνων πολιτών ως προς τη χρήση των νέων τεχνολογιών και των κινδύνων που αυτοί ελλοχεύουν.

Επίσης, η Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος διατηρεί ιστοσελίδα γνωστή ως CyberKids (http://www.cyberkid.gov.gr/main.html), στην οποία γονείς, παιδιά αλλά και ο οποιοσδήποτε χρήστης του Διαδικτύου μπορεί να έχει πρόσβαση και να ενημερωθεί για ποικίλα θέματα που άπτονται της χρήσης του Διαδικτύου, των ωφελειών αυτής σε περίπτωση που είναι ορθή και των κινδύνων που κρύβονται πίσω από την αλόγιστη χρήση, αλλά και πως μπορεί να γίνει η οποιαδήποτε πρόληψη τους, χωρίς τα αποτελέσματα να είναι ζημιογόνα και ανεπανόρθωτα.

4.3 Η δικαστική των Η/Υ

Με την εξάπλωση του Διαδικτύου στη ζωή μας έχει αρθεί τα τελευταία χρόνια και πολλαπλασιάζεται με γεωμετρικούς ρυθμούς συνεχώς το ενδιαφέρον των αρχών περί προστασίας των προσωπικών δεδομένων των χρηστών στο διαδίκτυο και η διασφάλιση αυτών από τυχόν αλλοιώσεις και οποιεσδήποτε άλλες ενέργειες. Η διασφάλιση των προσωπικών δεδομένων των χρηστών στο Διαδίκτυο πρόκειται για τη λεγόμενη δικαστική των υπολογιστών και υπάρχει συγκεκριμένος Νόμος στο Σύνταγμα που ορίζει το δικαίωμα του καθενός για το απόρρητο των προσωπικών του δεδομένων και επικοινωνιών. Συγκεκριμένα, στο Άρθρο 19 του Συντάγματος, *«Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο»*. Το απόρρητο της επικοινωνίας κατοχυρώνεται επίσης στο άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου, στο άρθρο 17 του Διεθνούς Συμφώνου περί Ατομικών και Πολιτικών Δικαιωμάτων της 19-12-1966 (ήδη ν.2462/1997), στο άρθρο 12 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου (Ο.Η.Ε.), στο άρθρο 17 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Στις ρυθμίσεις του άρθρου 19 του Συντάγματος, αντιτίθεται κάθε μορφή παρακολούθησης, ελέγχου και αποτύπωσης της ανταπόκρισης ή επικοινωνίας, κάθε μορφή παρεμπόδισης της επικοινωνίας, καθώς και κάθε μορφή χρησιμοποίησης αποδεικτικών μέσων, τα οποία αποκτήθηκαν κατά παράβαση της συνταγματικής προστασίας του απορρήτου. Επίσης, σύμφωνα με το Άρθρο 19 του Συντάγματος, η Αρχή Προστασίας Προσωπικών Δεδομένων (ανεξάρτητη αρχή εποπτείας της εφαρμογής του Ν. 2472/1997 και άλλων ρυθμίσεων περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα), ασκεί μια σειρά αρμοδιοτήτων ρυθμιστικές, αλλά και ελεγκτικές.

Η διείσδυση των υπολογιστών και του Διαδικτύου στη ζωή μας και η εξάπλωση εγκληματικών ενεργειών με τη χρήση των παραπάνω μέτρων, έχει ως αποτέλεσμα να κρίνεται πολλές φορές αναγκαία η άρση του απορρήτου της επικοινωνίας, προκειμένου να συλλεχθούν στοιχεία και αποδείξεις για τη διερεύνηση εγκλημάτων. Με τις αποδείξεις αυτές, ασχολείται ένας νέος και ιδιαίτερα ανερχόμενος κλάδος, αυτός της Δικαστικής των Ηλεκτρονικών Υπολογιστών, όπως αποδίδεται στα ελληνικά (Computer Forensics)[75].

Η άρση του απορρήτου των επικοινωνιών μπορεί να γίνει σε εξαιρετικές περιπτώσεις και περιπτώσεις υψίστης ανάγκης και σημασίας, όπως σε ζητήματα εθνικής ασφάλειας ή για τη διακρίβωση σοβαρών εγκλημάτων. Στην πρώτη περίπτωση, δηλαδή σε ζητήματα εθνικής ασφάλειας, περιλαμβάνεται ότι αποκλειστικά αναφέρεται στην προάσπιση της χώρας έναντι εξωτερικών κινδύνων και διακρίνεται από τις έννοιες της δημόσιας ασφάλειας και της δημόσιας τάξης. Η πρώτη αφορά την προστασία του πολιτεύματος και των εξουσιών που δίδει το σύνταγμα εν γένει, ενώ η δεύτερη προασπίζει το έννομο αγαθό της «κοινής ειρήνης». Για την άρση απορρήτου σε αυτήν την περίπτωση και τη συλλογή αποδείξεων, θα πρέπει να υπάρχουν σαφή κριτήρια, όπου θα καθοδηγήσουν τους δικαστές στη διάγνωση των λόγων εθνικής ασφάλειας, οι οποίο θίγονται[76].

---

[75] Μανιάτης (2011), «Δικαστική των Ηλεκτρονικών Υπολογιστών», ΔιΜΕΕ, Τεύχος 4, ηλεκτρονικά διαθέσιμο: http://www.infomm.teipat.gr/eclass/modules/document/file.php/TMG116/FORUM_MANIATHS%20(2).pdf

[76] Δαγτόγλου (2005), «Συνταγματικό Δίκαιο – ατομικά δικαιώματα», Τόμος Α, δεύτερη αναθεωρημένη έκδοση, Εκδόσεις Αντ, Ν. Σάκκουλα, Αθήνα – Κομοτηνή; Χρυσογόνος (2002), «Ατομικά και κοινωνικά Δικαιώματα», 2η Έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή; Αλιβιζάτος «Η Συνταγματική θέση των ενόπλων δυνάμεων» Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 1987

Στη δεύτερη περίπτωση που ορίζεται άρση απορρήτου, συγκαταλέγονται οι διακριβώσεις σοβαρών εγκλημάτων. Το Σύνταγμα σε αυτή την περίπτωση δεν εννοεί οποιαδήποτε αξιόποινη πράξη[77]. Η έννοια των «ιδιαίτερα σοβαρών εγκλημάτων» πρέπει να εκλαμβάνεται στενότερη από εκείνη του κακουργήματος και σαφώς να περιλαμβάνει τετελεσμένα εγκλήματα και όχι προπαρασκευαστικές πράξεις[78]. Αν σύμφωνα λοιπόν με τους παραπάνω λόγους κριθεί αναγκαία η άρση του απορρήτου για λόγους εθνικής ασφάλειας, αυτή γίνεται σύμφωνα με τις Παραγράφους 1 και 2 του Άρθρου 3 του Ν. 2225/1994 μόνο από δικαστική ή άλλη πολιτική, στρατιωτική ή αστυνομική δημόσια αρχή στην αρμοδιότητα της οποίας υπάγεται το θέμα που επιβάλλει την άρση.

Άρση απορρήτου γίνεται πλέον και για την εξακρίβωση ηλεκτρονικών εγκλημάτων που υπάγονται στις παραπάνω διατάξεις. Το παραπάνω υπάγεται στον κλάδο της Δικαστικής των Υπολογιστών, όπως αναφέρθηκε προηγουμένως, ο οποίος έχει διαμορφωθεί μέσα από διάφορες τάσεις που έχουν προκύψει κατά τη διάρκεια της ιστορίας των υπολογιστών[79]. Παρακάτω αναφέρονται διάφορες κοινές τεχνικές σχετικά με τη Δικαστική των Ηλεκτρονικών Υπολογιστών[80]:

Αρχικά γίνεται κατάσχεση του εξοπλισμού πληροφορικής, υπό συγκεκριμένες κατευθυντήριες οδηγίες. Ο υπολογιστής απενεργοποιείται και έπειτα φωτογραφίζεται, ενώ ο εξοπλισμός του καταγράφεται λεπτομερώς. Καθώς οι ανακριτικές ενέργειες έχουν ως αντικείμενο και σημείο αναφοράς τους τον υπολογιστή, ο χρόνος απενεργοποίησης δηλώνεται όχι σύμφωνα με τα δεδομένα των διωκτικών αρχών αλλά όπως είναι καταγεγραμμένος στο εσωτερικό ρολόι του υπολογιστή. Τέλος, δημιουργείται ένα ακριβές αντίγραφο κάθε σκληρού δίσκου (νομική αναπαράσταση ή legal imaging) διαδικασία η οποία πρέπει να πραγματοποιείται όσο το δυνατόν πιο σύντομα από τη στιγμή κατάσχεσης του

[77] Δαγτόγλου (2005), Συνταγματικό Δίκαιο – ατομικά δικαιώματα», Τόμος Α, δεύτερη αναθεωρημένη έκδοση, Εκδόσεις Αντ, Ν. Σάκκουλα, Αθήνα – Κομοτηνή

[78] Παυλόπουλος (1987), «Τεχνολογική εξέλιξη και συνταγματικά δικαιώματα», ΝοΒ

[79] Μανιάτης (2011), «Δικαστική των Ηλεκτρονικών Υπολογιστών», ΔιΜΕΕ, Τεύχος 4, ηλεκτρονικά διαθέσιμο: http://www.infomm.teipat.gr/eclass/modules/document/file.php/TMG116/FORUM_MANIATHS%20(2).pdf

[80] Μανιάτης (2011), «Δικαστική των Ηλεκτρονικών Υπολογιστών», ΔιΜΕΕ, Τεύχος 4, ηλεκτρονικά διαθέσιμο: http://www.infomm.teipat.gr/eclass/modules/document/file.php/TMG116/FORUM_MANIATHS%20(2).pdf

υπολογιστή.

Οι προσωπικοί υπολογιστές διατηρούν αρχεία που καταγράφουν τη δραστηριότητα του εκάστοτε χρήστη στο Διαδίκτυο. Για παράδειγμα, τηρούνται αρχεία εισερχόμενης και εξερχόμενης ηλεκτρονικής αλληλογραφίας, συνδρομές σε ομάδες συζητήσεων και πιθανώς πρόσβαση σε καταγεγραμμένες ιδιωτικές συνομιλίες στο Διαδίκτυο. Επιπλέον, οι υπολογιστές θέτουν σε «κρυφή μνήμη» (κρύπτη) προσφάτως χρησιμοποιημένα δεδομένα, σε περίπτωση που χρειαστεί να επαναχρησιμοποιηθούν σε σύντομο χρονικό διάστημα. Επομένως, οι αρχές έχουν πρόσβαση στο υλικό που «διακινήθηκε» μέσω του Υπολογιστή πριν το διάστημα της κατάσχεσης.

Μια άλλη τεχνική που χρησιμοποιείται στη δίωξη του ηλεκτρονικού εγκλήματος είναι η λεγόμενη τεχνική «μύρισμα». Με τη μέθοδο αυτή συλλέγονται αποδεικτικά στοιχεία, καθώς οι ερευνητές «οσφραίνονται, την κυκλοφορία στο Διαδίκτυο κατά τη διαμετακόμιση στοιχείων. Η διαδικασία αυτή είναι αρκετά δύσκολη, καθώς διέπεται από την έννοια των επικοινωνιών πάνω στην οποία βασίζεται το Διαδίκτυο, δηλαδή στην «ανταλλαγή πακέτων» δεδομένων. Αυτό συνίσταται στη διαδικασία που ακολουθούν τα μηνύματα προτού να σταλούν στον κυβερνοχώρο, κατά την οποία σπάνε σε κομμάτια, τα λεγόμενα «πακέτα». Τα «πακέτα» έπειτα συναρμολογούνται εκ νέου και μεταφέρονται στον προορισμό τους. Για να γίνει λοιπόν η διαδικασία «μύρισμα» απαιτούνται γνώσεις σχετικά με την κτήση δεδομένων, αλλά και για την επανασυναρμολόγηση τους.

Η έρευνα στο Διαδίκτυο είναι μια άλλη τεχνική η οποία χρησιμοποιείται για την εξακρίβωση ηλεκτρονικών εγκλημάτων, αν και είναι δύσκολη η προσκόμιση αποδείξεων στις συγκεκριμένες περιπτώσεις, καθώς οι χρήστες χρησιμοποιούν συνήθως πλαστά στοιχεία και διευθύνσεις κατά την εισβολή τους σε ένα σύστημα. 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 υπαλλήλων. Είναι αναγκαία η διεπιστημονική προσέγγιση του ζητήματος αυτού λοιπόν προκειμένου να εξακριβώνονται τα εγκλήματα που τελούνται με τη χρήση των Ηλεκτρονικών Υπολογιστών και του Διαδικτύου, αλλά και να δημιουργηθούν ασφαλιστικές δικλείδες για την αποφυγή και τον περιορισμό τους.

Προτάσεις για προστασία στο Διαδίκτυο

5.1 Βασικές Έννοιες Ασφάλειας

Ο Παγκόσμιος Ιστός (World Wide Web) είναι μια από τις σημαντικότερες υπηρεσίες του διαδικτύου και προσφέρει στους χρήστες του τη δυνατότητα πρόσβασης στη μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο. Πρόκειται για μια τεράστια συλλογή εγγράφων, τα οποία είναι αποθηκευμένα σε εκατομμύρια υπολογιστές στον κόσμο και η οποία εμπλουτίζεται συνεχώς από όλους τους χρήστες οι οποίοι αποφασίζουν να ανεβάσουν στο χώρο του τις σελίδες τους. Η πλοήγηση στις σελίδες του παγκοσμίου ιστού πραγματοποιείται μέσω ειδικών προγραμμάτων πλοήγησης -browsers- (π.χ. Internet Explorer, Mozilla Firefox κ.λπ.) και απαιτεί ιδιαίτερη προσοχή από τον χρήστη, διότι εγκυμονεί πολλαπλούς κινδύνους, τόσο για την ασφάλεια του υπολογιστή του, όσο και για την ασφάλεια των προσωπικών του δεδομένων[81].

Στην ενότητα αυτή θα προσπαθήσουμε, να προσεγγίσουμε και να διερευνήσουμε τους τρόπους με τους οποίους οι χρήστες μπορούν να προστατευθούν και να μη βρεθούν θύματα εξαπάτησης διαδικτυακών εγκληματιών. Σύμφωνα με τον Τσουραμάνη (2005) τρεις είναι οι βασικές έννοιες της Ασφάλειας[82]:

1. **Εμπιστευτικότητα.** Η συγκεκριμένη έννοια αναφέρεται στην προστασία των προσωπικών δεδομένων από την πρόσβαση σε αυτά μη εξουσιοδοτημένων χρηστών. Για την επίτευξη της απαιτείται περιορισμός της πρόσβασης σε συστήματα και δεδομένα μόνο στους νόμιμους χρήστες τους.

2. **Ακεραιότητα**. Η έννοια της ακεραιότητας και η διατήρηση αυτής συνδέεται με την προστασία των δεδομένων από τυχόν τροποποίηση (προσθήκη, διαγραφή). Η αλλοίωση της παραπάνω έννοιας καθοιονδήποτε τρόπο μπορεί να προκύψει εξαιτίας κάποιου λάθους στο σύστημα ή ακόμα να είναι αποτέλεσμα δόλιας ενέργειας.

3. **Διαθεσιμότητα.** Η διαθεσιμότητα σχετίζεται με τη δυνατότητα

[81] Υπουργείο Παιδείας και Θρησκευμάτων (2014). Ασφάλεια στο Διαδίκτυο. Ηλεκτρονικά διαθέσιμο: http://www.e-yliko.gr/htmls/pc_use/snav.aspx, ανακτήθηκε στις 03/09/2014

[82] Τσουραμάνης (2005), «Ψηφιακή Εγκληματικότητα - Η (αν)ασφαλής όψη του διαδικτύου», Αθήνα, Εκδ.Β.Ν. Κατσαρού

άμεσης προσπέλασης των συστημάτων και των δεδομένων, όταν ή όποτε απαιτείται. Στις επιθέσεις άρνησης εξυπηρέτησης υπάρχει παραβίαση της διαθεσιμότητας, όταν δεν επιτρέπεται στους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στους πόρους του συστήματος.

5.2 Τα συνηθέστερα μέτρα πρόληψης των χρηστών

Υπάρχουν διάφορες ενέργειες, οι οποίες πρέπει να γίνονται από τους χρήστες, προκειμένου να προβαίνουν σε ασφαλείς ενέργειες κατά την πλοήγηση στο διαδίκτυο και την αναζήτηση πληροφοριών.

Ειδικότερα, όταν διενεργείται μια αναζήτηση, για παράδειγμα, με την χρήση ενός συνόλου από λέξεις-κλειδιά, ερευνάται πρώτα η βάση δεδομένων και ακολούθως συγκεντρώνονται όλες οι διευθύνσεις που περιέχουν αυτές τις λέξεις. Τα αποτελέσματα αναζήτησης, έτσι όπως εμφανίζονται στον χρήστη, συνήθως περιέχουν την διεύθυνση της ιστοσελίδας, ένα δείγμα του κειμένου μέσα στο οποίο υπάρχουν οι λέξεις που αναζητήθηκαν, μια σύντομη περιγραφή και την κατηγορία στην οποία έχει καταγραφεί η ιστοσελίδα στην δεδομένη μηχανή αναζήτησης. Ο τρόπος σωστής αναζήτησης μέσα από τις μηχανές αναζήτησης, τους θεματικούς καταλόγους και τις μηχανές αναζήτησης είναι από τις πλέον βασικές δεξιότητες που πρέπει να διαθέτει ο χρήστης, τόσο για να μη χαθεί στις λεωφόρους των πληροφοριών του Διαδικτύου, όσο και για να βρίσκει ταχύτερα τις πληροφορίες που αναζητά. Είναι επομένως βασικός στόχος της εκπαίδευσης των νέων ανθρώπων, πολιτών της κοινωνίας της πληροφορίας[83].

Σημειώνεται ότι το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική, ταχύτατη και αξιόπιστη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου. Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Μερικά από τα προβλήματα που μπορεί να αντιμετωπίσει ένας χρήστης ηλεκτρονικού

[83] Υπουργείο Παιδείας και Θρησκευμάτων (2014). Ασφάλεια στο Διαδίκτυο. Ηλεκτρονικά διαθέσιμο: http://www.e-yliko.gr/htmls/pc_use/snav.aspx, ανακτήθηκε στις 03/09/2014

ταχυδρομείου είναι τα εξής[84]:

- Μετάδοση ιών
- Ενοχλητική αλληλογραφία (spam mail)
- Μηνύματα απατηλού περιεχομένου (hoaxes)
- Προστασία προσωπικών δεδομένων.

Οι χρήστες μπορούν να υιοθετήσουν διάφορα μέτρα με τα οποία να προστατεύσουν τα προσωπικά τους δεδομένα από ενδεχόμενη κακόβουλη χρήση. Αυτά μπορούν να είναι τα εξής:

α) Χρήση Λογισμικού Ασφαλείας -Λογισμικό Antivirus

Μέσω του Διαδικτύου εξαπλώνονται πολλές φορές, όπως αναφέρθηκε και παραπάνω διάφοροι ιοί, οι οποίοι μπορούν να προκαλέσουν μερική ή ακόμη και συνολική καταστροφή του υπολογιστή. Η χρήση λογισμικού «αντιβιοτικού» ή όπως είναι ευρύτερα γνωστή η χρήση Antivirus είναι η πιο συνηθισμένη μέθοδος αντιμετώπισης επιθέσεων στο λογισμικό του υπολογιστή. Ένα πρόγραμμα Antivirus έχει τρείς βασικές λειτουργίες

[84] Υπουργείο Παιδείας και Θρησκευμάτων (2014). Ασφάλεια στο Διαδίκτυο. Ηλεκτρονικά διαθέσιμο: http://www.e-yliko.gr/htmls/pc_use/snav.aspx, ανακτήθηκε στις 03/09/2014

1. Ανίχνευση των ιών : Η λειτουργία αυτή πραγματοποιείται κατόπιν ενέργειας του χρήστη. Το λογισμικό Antivirus ελέγχει το σκληρό δίσκο του υπολογιστή ή τη μνήμη RAM αυτού προκειμένου να εμφανισθεί η «μόλυνση» ή η ενδεχόμενη ύπαρξη ιού στο σύστημα.

2. Προσδιορισμός ταυτότητας ιών: Στην περίπτωση που το σύστημα έχει προσβληθεί από κάποιον ιό, το λογισμικό ενημερώνει το χρήστη για την ταυτότητα του και πιθανόν το από πού αυτός προήλθε.

3. Καθαρισμός των ιών : Με τη λειτουργία αυτή το εγκατεστημένο «αντιβιοτικό» λογισμικό επιδιορθώνει το μολυσμένο από τον ιό αρχείο ή ακόμα μπορεί και να το διαγράψει.

β) Χρήση πιστοποίησης

Μια από τις συνηθέστερες μορφές και τεχνικές πρόληψης και ασφάλειας των χρηστών είναι η χρήση της πιστοποίησης της ταυτότητας τους με τη δημιουργία συνθηματικών. Το όνομα του χρήστη και ο κωδικός πρόσβασης του είναι τα στοιχεία που συνήθως ζητά και το πιο απλό σύστημα υπολογιστή για να πιστοποιήσει ότι πρόκειται για την είσοδο σε αυτό ενός πιστοποιημένου χρήστη. Ο χρήστης εισάγει τα στοιχεία που του ζητούνται και το σύστημα ελέγχει αυτά και έπειτα επιτρέπει την πρόσβαση στο χρήστη. Η διαδικασία αυτή είναι η συνηθέστερη και η πιο ικανοποιητική λύση για την πιστοποίηση των χρηστών, χωρίς όμως αυτό να είναι απόλυτα ασφαλές, καθώς υπάρχουν και σε αυτήν την περίπτωση αρκετοί κίνδυνοι εναντίον αυτού.

γ) Firewalls

Ο όρος firewall ή τείχος προστασίας διαφορετικά χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που έχει τις κατάλληλες ρυθμίσεις προκειμένου να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο. Η κύρια λειτουργία, δηλαδή ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δίκτυα υπολογιστών. Συνήθως δε, τα δίκτυα αυτά είναι δυο και συγκεκριμένα το διαδίκτυο και το τοπικό/εταιρικό δίκτυο που χρησιμοποιεί ο κάθε χρήστης.

Το επίπεδο εμπιστοσύνης το δυο δικτύων είναι αυτό που κατ' ουσία ενεργοποιεί το Firewall. Συγκεκριμένα και αναφορικά με τα παραπάνω, το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτει για το χρήστη τον μέγιστο βαθμό εμπιστοσύνης. Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπιση τους. Η σωστή πρακτική είναι το firewall να ρυθμίζεται έτσι ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου. Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall έτσι ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει. Το παραπάνω όμως καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

Τα Firewalls μπορεί να είναι λογισμικό που εγκαθίσταται σε έναν υπολογιστή (πχ. το windows firewall), λογισμικό που προστατεύει το δίκτυο (πχ. Microsoft ISA Server) ή ακόμη και συσκευή hardware συνδεμένη στο δίκτυο. Τα firewalls φιλτράρουν την πληροφορία που εισέρχεται στο δίκτυο ή εξέρχεται από αυτό, με βάση κανόνες τους οποίους έχουμε θέσει. Με τον τρόπο αυτό προστατεύεται το δίκτυο από εισβολείς (hackers, ορισμένους ιούς κλπ). Επιπλέον, απαγορεύεται η αποστολή πληροφορίας από τους υπολογιστές του δικτύου, όπως π.χ. ποιοί τύποι αρχείων επιτρέπεται να αποστέλλονται.Παρόλη τη θετική τους λειτουργία τα Firewalls έχουν υψηλό οικονομικό κόστος και οι χρήστες συναντούν μεγάλη δυσκολία στις ρυθμίσεις τους προκειμένου αυτές να είναι αποτελεσματικές ως προς την εκπλήρωση της αποστολής τους.

Από μόνο του ένα Firewall δεν μπορεί να προσφέρει τη μέγιστη δυνατή προστασία. Ένα firewall είναι ένα επιπλέον επίπεδο προστασίας, ένας «φράχτης» τοποθετημένος γύρω από ένα δίκτυο ή από μια συγκεκριμένη εφαρμογή. Όταν ένα πακέτο φτάνει στον δρομολογητή του firewall, αυτός το επεξεργάζεται και αποφασίσει αν θα το αφήσει να περάσει στο δίκτυο που προστατεύει ή όχι.

5.3 Παιδιά και Ασφάλεια

Τα παιδιά και γενικότερα τα άτομα μικρών ηλικιών είναι εκείνα που κινδυνεύουν περισσότερο, όσον αφορά την έκθεση τους στο Διαδίκτυο και μάλιστα είναι αρκετά συχνοί χρήστες αυτού, με αποτέλεσμα καθημερινά να αναζητούνται τρόποι για να προστατευθούν από τους κινδύνους τους οποίους εγκυμονεί το Διαδίκτυο. Σύμφωνα με την επίσημη ανακοίνωση της Ελληνικής Αστυνομίας τα παιδιά πρέπει να παροτρύνονται από τους γονείς, ώστε να τους εξηγούν τις εμπειρίες τους κατά την περιπλάνησή τους στο Διαδίκτυο. Οι γονείς θα πρέπει να μιλάνε με τα παιδιά τους με τρόπο διαλεκτικό και διαλλακτικό, και να τα ενημερώνουν για εικόνες ή κείμενα τα οποία μπορεί να συναντήσουν κατά την περιήγηση τους στο Διαδίκτυο καθως η φύση τους μπορεί να είναι εκφοβιστική ή περίεργη.

Τα παιδιά, αλλά και οι ενήλικες θα πρέπει με κάθε τρόπο να διαφυλάσσουν τις προσωπικές τους πληροφορίες και να μη δίνουν τα προσωπικά τους στοιχεία, όπως, όνομα, διεύθυνση, τηλέφωνο ή και φωτογραφίες σε αγνώστους που συναντούν στο Διαδίκτυο ακόμη και αν τους ζητηθεί. Ο κωδικός εισόδου στον ηλεκτρονικό υπολογιστή θα πρέπει να παραμένει μυστικός και να μη δανείζεται σε κανένα, ούτε φίλο, ούτε γνωστό. Καλό θα ήταν βέβαια, τα παιδιά να περιηγούνται στο Διαδίκτυο έπειτα από την άδεια και κατά την παρουσία των γονιών τους, οι οποίοι θα τους καθοδηγούν ανάλογα και θα τους αποτρέπουν από την περιήγηση σε sites αμφίβολου περιεχομένου. Επίσης, καλό θα ήταν τα παιδιά να αποφεύγουν τις συνομιλίες σε ομάδες συζητήσεων και chat rooms στα οποία δεν υπάρχει κάποιο συγκεκριμένο εκπαιδευτικό για παράδειγμα ενδιαφέρον και θα πρέπει να αποκτήσουν τέτοια παιδεία από τον οικογενειακό τους περίγυρο, κατά την οποία θα εγκαταλείπουν μια συζήτηση αν αυτή τους φέρνει σε δύσκολη θέση.

Επίσης, τα παιδιά θα πρέπει να διαπαιδαγωγούνται κατά τέτοιο τρόπο, ώστε να μην εμπιστεύονται όχι μόνο άτομα μέσω Διαδικτύου, ακόμα και ότι διαβάζουν. Ότι υπάρχει στο Διαδίκτυο δεν είναι κατ΄ανάγκη αληθινό. Θα πρέπει λοιπόν με διάφορους τρόπους να ελέγχουν αν αυτό που διαβάζουν είναι κάτι πραγματικό ή έχει δημιουργηθεί για να παραπλανήσει ή εξαπατήσει τον αναγνώστη. Οι παραπάνω «οδηγίες» ισχύουν για όλες τις ηλικίες παιδιών και νέων. Αντίστοιχα, οι γονείς καλούνται να έχουν τον ηλεκτρονικό υπολογιστή σε χώρους όπως το σαλόνι ή γενικότερα σε κοινόχρηστους από την οικογένεια χώρους και όχι σε υπνοδωμάτια, προκειμένου να μπορούν να ελέγχουν τις δραστηριότητες των παιδιών τους στο Διαδίκτυο. Προτείνεται στους γονείς να ασχολούνται με τα παιδιά τους και να τα

καθοδηγούν σχετικά με τον τρόπο που δουλεύει το Διαδίκτυο, ενώ παράλληλα να αφιερώνουν χρόνο για να περιηγηθούν μαζί τους σε αυτό.

Καλό θα ήταν οι γονείς μέσα από συζητήσεις με τα παιδιά τους να μαθαίνουν τις δραστηριότητες αυτών στο Διαδίκτυο και ταυτόχρονα να τα ενθαρρύνουν να προτιμούν τις ιστοσελίδες που εκείνοι ήδη γνωρίζουν και εμπιστεύονται και όχι αυτές που θεωρούν ανάρμοστες. Στον υπολογιστή θα πρέπει να υπάρχει εγκατεστημένο κάποιο λογισμικό φίλτρο που θα απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου (πχ περιεχομένου για ενήλικες). Προτείνεται δε, η συζήτηση με τα παιδιά για την ασφάλεια στο Διαδίκτυο, όπως συζητούν μαζί τους για την ασφάλεια στην καθημερινή τους ζωή. Τέλος, οι γονείς θα πρέπει να ενημερώνονται για το που θα πρέπει να απευθυνθούν σε περίπτωση που συναντήσουν κάτι βλαβερό ή παράνομο στο Διαδίκτυο.

5.4 Ασφαλείς Συναλλαγές[85]

Σήμερα, μέσω Διαδικτύου πραγματοποιούνται ολοένα και περισσότερες οικονομικές συναλλαγές, με επιχειρήσεις και υπηρεσίες ιδιωτικού και δημόσιου χαρακτήρα, με κρατικές υπηρεσίες κα. Σημαντικές είναι οι ασφαλιστικές δικλείδες που έχουν τεθεί για την ασφάλεια των συναλλασσόμενων, αν και ακόμα υπάρχουν αρκετοί που δεν εμπιστεύονται τις Διαδικτυακές συναλλαγές και ανησυχούν για την ασφάλεια των προσωπικών τους δεδομένων και των οικονομικών τους στοιχείων. Προτείνεται λοιπόν στους χρήστες να προστατευθούν οι ίδιοι μέσα από απλές ενέργειες από το να πέσουν θύματα κακόβουλων ενεργειών. Μια απλή ενέργεια είναι να μην πραγματοποιούνται οικονομικές συναλλαγές μέσω Διαδικτύου από Internet Café, δημόσιες βιβλιοθήκες και άλλους δημόσιους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές. Σχετικά με τους κωδικούς πρόσβασης που χρησιμοποιούνται κατά τις τις διαδικτυακές συναλλαγές προτείνονται τα εξής:

- Συχνή αλλαγή των κωδικών πρόσβασης
- Αποφυγή χρήσης κωδικών πρόσβασης που περιέχουν στοιχείς όπως:

[85] Βλαχόπουλος (2007), «Ηλεκτρονικό Έγκλημα», Εκδόσεις Νομικής Βιβλιοθήκης; Βλαχόπουλος (χ.χ.), «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-crime.gr/301.pdf

ημερομηνία γέννησης, αριθμό τηλεφώνου ή άλλα προσωπικά στοιχεία του χρήστη

· Αποφυγή ύπαρξης κωδικών πρόσβασης σε ηλεκτρονικές συναλλαγές μέσα σε τσάντες, πορτοφόλια, κινητά τηλέφωνα κτλ, διότι σε μια ενδεχόμενη κλοπή των παραπάνω αντικειμένων, ο κωδικός γίνεται έρμαιο των επίδοξων εγκληματιών

· Χρήση διαφορετικών κωδικών σε διαφορετικές συναλλαγές.

Καλό και χρήσιμο είναι να απενεργοποιείται η λειτουργία «Αυτόματης Καταχώρησης» του κωδικού του προγράμματος περιήγησης Web Banking κυρίως των τραπεζών. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους. Αν ο χρήστης πραγματοποιεί ηλεκτρονικές αγορές, καλό θα ήταν αυτές να πραγματοποιούνται από γνωστές εταιρίες , οι οποίες παρέχουν εγγυήσεις ασφάλειας. Σε περίπτωση ηλεκτρονικών συναλλαγών για εμπορικούς λόγους προτείνεται η χρήση μιας και μόνο κάρτας, η οποία καλό θα ήταν να μην είναι πιστωτική, αλλά να έχει ένα συγκεκριμένο χρεωστικό υπόλοιπο για την κάθε συναλλαγή.

Κάθε υπολογιστής θα πρέπει να έχει εγκατεστημένο ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και ο χρήστης πρέπει να φροντίζει να λαμβάνει τακτικά τις ενημερωμένες εκδόσεις τους, καθώς οι ιοί εξελίσσονται συνεχώς και οι εξελίξεις της τεχνολογίας δεν επιτρέπουν καθυστερήσεις. Επίσης, ο χρήστης δε θα πρέπει να ανοίγει τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν είναι βέβαιος. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επιπλέον, προτείνεται να μην απαντάνε οι χρήστες σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά στοιχεία. Επίσης, προσωπικά στοιχεία ή στοιχεία συναλλαγών δε θα πρέπει να αποστέλλονται μέσω μιας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail) καθώς είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα.

Από τη στιγμή που οι χρήστες κάνουν συναλλαγές μέσω Διαδικτύου καλό θα ήταν να ελέγχουν τακτικά τους τραπεζικούς τους λογαριασμούς και τους λογαριασμούς των πιστωτικών τους καρτών που ενδεχομένως χρησιμοποιούν στις συναλλαγές για οποιαδήποτε ασυνήθιστη κατάθεση ή ανάληψη και να ειδοποιούν αμέσως την τράπεζα σε περίπτωση που διαπιστωθεί η οποιαδήποτε διαφορά.

ΕΠΙΛΟΓΟΣ

Η τεχνολογία έχει σημειώσει θεαματική ανάπτυξη τα τελευταία χρόνια και έχει διεισδύσει με ταχείς ρυθμούς στην καθημερινή πραγματικότητα του ατόμου. Ο καθένας σχεδόν ανά την υφήλιο σε αναπτυγμένες χώρες χρησιμοποιεί καθημερινά έναν ηλεκτρονικό υπολογιστή και έχει πρόσβαση στο Διαδίκτυο. Το πλήθος των πληροφοριών και η ταχύτητα μετάδοσης τους, η γρήγορη επικοινωνία και οι ποικίλες δυνατότητες που προσφέρει, είναι μερικοί μόνο από τους λόγους που έχουν μετατρέψει το Διαδίκτυο σε ένα ιδιαίτερα δημοφιλές εργαλείο στα χέρια του σύγχρονου ανθρώπου. Βέβαια, πέρα από τα πλεονεκτήματα και τις δυνατότητες που προσφέρει το Διαδίκτυο στο άτομο, έχει φέρει και ορισμένες αρνητικές επιπτώσεις στη ζωή του, όπως είναι η κοινωνική αποξένωση, λόγω εθισμού σε αυτό. Μια από τις σημαντικότερες αρνητικές επιπτώσεις του Διαδικτύου στη σύγχρονη κοινωνία δεν είναι άλλη από την εκμετάλλευση αυτού και της τεχνολογίας γενικότερα για την διάπραξη εγκλημάτων, τα επονομαζόμενα ηλεκτρονικά εγκλήματα.

Η διάπραξη ηλεκτρονικών εγκλημάτων είναι ένα λεπτό ζήτημα που απαιτεί μία ειδικευμένη προσέγγιση. Το ηλεκτρονικό έγκλημα σε σοβαρότερες ή όχι μορφές έχει γίνει μια καθημερινή πραγματικότητα στις Παγκόσμιες διωκτικές αρχές και η εξακρίβωση του απαιτεί όχι μόνο νομοθετικές ή παρεμφερείς με αυτές γνώσεις, αλλά και εξειδικευμένες γνώσεις πληροφορικής και τεχνολογίας. Αυτό που έχει παρατηρηθεί και καταγραφεί τα τελευταία χρόνια είναι ότι περιπτώσεις του ηλεκτρονικού εγκλήματος αυξάνονται με θεαματικούς ρυθμούς και οι παράγοντες διάπραξης τους διαφέρουν κατά περίπτωση. Το ηλεκτρονικό έγκλημα εξελίσσεται συνεχώς, ακολουθώντας αναλογικά, την εξέλιξη της τεχνολογίας.

Ο ηλεκτρονικός εγκληματίας, λειτουργώντας στην αφάνεια και αφήνοντας ελάχιστα ίχνη και με σύμμαχο την έλλειψη τεχνογνωσίας, καταφέρνει καθημερινά να εισβάλει ακόμα σε συστήματα υψηλής ασφαλείας έχοντας σχεδόν πάντα σαν σκοπό την απολαβή οικονομικού οφέλους. Παράλληλα, οι μορφές των εγκληματικών ενεργειών του καλύπτουν σχεδόν όλο το φάσμα του ποινικού κώδικα, αλλά και των αναφερθέντων νομικών κενών. Για την αντιμετώπιση αυτού του φαινομένου, τα μέτρα προστασίας οφείλουν να είναι συνολικά.

Ο καθένας ξεχωριστά, αλλά και ο κάθε οργανισμός πρέπει να λάβει τα μέτρα του κατά της εκδήλωσης αυτών των επιθέσεων, αλλά ταυτόχρονα να είναι σε θέση να αποκαταστήσει τη ζημιά που προκλήθηκε με όσο το δυνατότερο λιγότερες οικονομικές απώλειες, εφόσον αυτός είναι ο πρωτεύων σκοπός του εγκληματία. Απαραίτητη καθίσταται η θέσπιση «νέων εγκλημάτων», που να θέτουν όρια στην συμπεριφορά όσον χρησιμοποιούν το διαδίκτυο. Τα εγκλήματα θα πρέπει να διέπονται από Ρυθμιστικές Διατάξεις (νόμους και κανόνες του συντάγματος) κατά την θέσπιση των οποίων πρέπει να ληφθούν υπόψη η ελεύθερη διακίνηση ιδεών, η ελευθερία της έκφρασης και οι λοιπές συνταγματικές αρχές. Τέλος, απαραίτητη καθίσταται και η εκπαίδευση όλων των εμπλεκόμενων φορέων σε θέματα, πληροφορικής, νέων τεχνολογιών και Διαδικτύου καθώς και η ενημέρωση των πολιτών στην χρήση αυτού, προκειμένου να περιοριστεί το ηλεκτρονικό έγκλημα με όλους τους δυνατούς τρόπους και να σταματήσει να βλάπτει την κοινωνία και την οικονομία της κάθε χώρας.

Αναφορικά με τον όρο Computer Forensics στις μέρες μας στην ηλεκτρονική εγκληματικότητα και τις προφυλάξεις που θα μπορούσαν να παρθούν, θα λέγαμε πως αν αποφασισθεί να γίνει μια έρευνα για την συλλογή αποδεικτικών στοιχείων είναι συνήθως απαραίτητο να πάρουμε μια εγκληματολογική εικόνα των υπολογιστών που περιλαμβάνονται στο συμβάν. Γι’ αυτό τον σκοπό υπάρχουν τόσο εμπορικά όσο και μη εμπορικά εργαλεία που έχουν αντέξει το βάρος του νομικού συστήματος. Απ’ τη στιγμή που θα γίνει το συμβάν θα πρέπει να ακολουθούμε συγκεκριμένα βήματα με τα οποία θα πρέπει να αντιμετωπίσουμε το περιστατικό.

Η εγκληματολογική έρευνα λοιπόν περιλαμβάνει τα εξής στάδια:

- Άμεση απόκριση
- Αντιγραφή για εγκληματολογική έρευνα
- Εγκληματολογική ανάλυση
- Αναφορά
- Περιεχόμενο
- Πρόληψη

Επειδή τα εργαλεία αυτά είναι ανοικτού κώδικα και το αποτέλεσμα της αντιγραφής που παρέχουν μπορεί να εισαχθεί σχεδόν σε οποιοδήποτε εργαλείο ανάλυσης εγκληματολογικής έρευνας ίσως είναι προτιμότερο να καταφύγουμε σε αυτά. Το εργαλείο dd χρησιμοποιείται για να αντιγράφει bit, από ένα αρχείο σε ένα άλλο. Η αντιγραφή με αυτόν τον τρόπο, είναι η βάση για όλα τα εργαλεία αντιγραφής για εγκληματολογική έρευνα. Το dd είναι ευέλικτο και ο κώδικας προέλευσης είναι ελεύθερα διαθέσιμος. Επιπλέον το dd μπορεί να μεταγλωτιστεί σχεδόν σε οποιοδήποτε πλατφόρμα Unix. Οι επιλογές της γραμμής εντολών σχετικά με την αντιγραφή που κάνει το dd, είναι οι εξής:

- if Καθορίζει το αρχείο εισόδου που θα διαβαστεί
- of Καθορίζει το αρχείο εξόδου που θα γραφτεί
- bs Καθορίζει το μέγεθος του block, σε byte, που θα διαβαστεί και θα γραφτεί
- count Καθορίζει τον αριθμό των block που θα αντιγραφούν από το αρχείο εισόδου, στο αρχείο εξόδου
- skip Καθορίζει τον αριθμό των block που θα αγνοηθούν από την αρχή, πριν το διάβασμα του αρχείου εισόδου
- conv

Επιτρέπει να καθοριστούν επιπλέον ορίσματα, κάποια από τα οποία είναι τα εξής:

- notrunc Δεν θα επιτρέψει να αποκοπεί η έξοδος στην περίπτωση λάθους
- noerror Δεν θα σταματήσει το διάβασμα του αρχείου εισόδου στην περίπτωση λάθους (δηλαδή, αν διαβάστηκαν λανθασμένα μπλοκ, η διαδικασία θα συνεχισθεί).
- sync Θα γεμίσει τα αντίστοιχα bit εξόδου με μηδενικά, όταν συμβεί ένα λάθος εισόδου. Αυτό συμβαίνει μόνο αν χρησιμοποιείται σε συνδυασμό με την επιλογή notrunc.

Πρέπει να είναι προφανές ότι το dd λειτουργεί με αρχεία και όχι κατευθείαν με φυσικές συσκευές. Ωστόσο τα λειτουργικά συστήματα Unix ανοικτού κώδικα, όπως το Linux και το FreeBSD, χειρίζονται τις συσκευές ως αρχεία. Αυτά τα ειδικά αρχεία, που βρίσκονται στον κατάλογο /dev, επιτρέπουν άμεση πρόσβαση σε συσκευές που χειρίζεται το λειτουργικό σύστημα. Συνεπώς, τα αρχεία εισόδου στο dd μπορεί να είναι ολόκληροι σκληροί δίσκοι, διαμερίσματα σκληρών δίσκων ή άλλες συσκευές. Για να δημιουργήσουμε μια αντιγραφή για εγκληματολογική έρευνα ενός σκληρού δίσκου (δηλαδή, το /dev/hdb στο Linux ή το /dev/ad1 στο FreeBSD) θα είναι το αρχείο εισόδου. Για να δημιουργήσουμε μια αντιγραφή ενός διαμερίσματος, το αρχείο εισόδου θα είναι το αρχείο διαμερίσματος, (δηλαδή, το /dev/hdb1στο Linux ή το /dev/ad1s1 στο FreeBSD).

Φυσικά, το επόμενο θέμα είναι ποιος θα είναι ο προορισμός της αντιγραφής. Ο προορισμός θα πρέπει να είναι ένας άλλος σκληρός δίσκος (χρησιμοποιώντας τα αρχεία συσκευών που αναφέρθηκαν), που ονομάζεται αντιγραφή bit προς bit του σκληρού δίσκου προέλευσης. Θα μπορούσαμε να επεκτείνουμε αυτή την ιδέα και πέρα από την χρήση σκληρών δίσκων ως μέσων προορισμού, να χρησιμοποιήσουμε αντίθετα μια ταινία, κάτι που είναι μια πολύ πιο αργή μέθοδος. Ο προορισμός θα πρέπει επίσης να είναι ένα κανονικό αρχείο (το οποίο δηλώνεται ως ένα αρχείο αποδεικτικών στοιχείων), που αποθηκεύεται σε οποιοδήποτε σύστημα αρχείων ως ένα λογικό αρχείο.

Αυτός γενικά είναι ο τρόπος που αποθηκεύονται οι περισσότερες μοντέρνες αντιγραφές για εγκληματολογική έρευνα, εξ αιτίας της ευκολίας αυτού του χειρισμού όταν μετακινείται το αρχείο με τα αποδεικτικά στοιχεία μεταξύ των συσκευών. Τέλος, ο προορισμός θα μπορούσε να είναι η τυπική έξοδος (οθόνη).

Για παράδειγμα, αν είναι δυνατόν να αφαιρέσουμε το σκληρό δίσκο από τον υπολογιστή προέλευσης στην διάρκεια μιας αντιγραφής και δεν υπάρχουν άλλες συνδέσεις διαθέσιμες για να συνδεθεί μια επιπλέον συσκευή δίσκου, θα είναι δύσκολο να αποθηκεύσετε τα περιεχόμενα του σκληρού δίσκου κατευθείαν σε έναν άλλο σκληρό δίσκο. Παρόμοια, θα μπορούσαμε να μην αποθηκεύσουμε το αντίγραφο σε ένα κανονικό αρχείο, επειδή θα πρέπει να αντιγραφεί σε μέσα που να είναι ήδη στον υπολογιστή προέλευσης, επικαλύπτοντας συνεπώς πιθανά αποδεικτικά στοιχεία.

Η μόνη επιλογή σε αυτή την περίπτωση είναι να κάνουμε μια εικόνα μέσω δικτύου. Πολλές επιλογές στο dd κάνουν την αντιγραφή πιο αποτελεσματική. Για παράδειγμα, μπορείτε να χειριστείτε το μέγεθος του μπλοκ που αντιγράφεται, για να κάνετε τη διαδικασία γρηγορότερη για τον κύριο υπολογιστή στον οποίο τρέχει το dd, όπου ο διακόπτης bs γενικά επιλέγεται να είναι ο διακόπτης conv, που επιτρέπει επιπλέον προαιρετικές παραμέτρους που υποστηρίζουν την διαδικασία αντιγραφής.

Τέλος, δυο πολύ προτεινόμενες επιλογές είναι οι παράμετροι noerror και η notrunc. Αυτοί οι διακόπτες θα αγνοήσουν τα χαλασμένα μπλοκ της προέλευσης, ώστε η αντιγραφή να συνεχίσει χωρίς να αποκοπεί η έξοδος στο μέσον με τα αποδεικτικά στοιχεία. Μια επιπλέον επιλογή του sync που χρησιμοποιείται με το noerror, κάνει αυτά τα χαλασμένα μπλοκ να μετατραπούν σε μηδενικά στην έξοδο.

Παράδειγμα προστασίας μέσω των παραπάνω μέσων από σχετικές κακόβουλες ενέργειες ηλεκτρονικής εγκληματικότητας, αποτελεί η μυστική ιστοσελίδα Silk Road η οποία λειτουργούσε στο λαθραίο Δίκτυο Tor και εμπορευόταν ποινικά «κολάσιμα» αγαθά μέσω του ψηφιακού χρήματος bitcoin. Το Δίκτυο Tor κατευθύνει τους χρήστες μέσω ενός ελεύθερου, παγκοσμίου και εθελοντικού δικτύου που αποτελείται από 3.000 και περισσότερους διαμοιραστές, οι οποίοι συγκαλύπτουν την τοποθεσία του επισκέπτη σε όποιον προσπαθήσει να παρακολουθήσει τα ηλεκτρονικά του ίχνη. Σύμφωνα με το κατηγορητήριο που οδήγησε στο ένταλμα σύλληψης του Ulbricht: στις 23 Ιουλίου 2013, υπήρχαν περίπου 957.079 εγγεγραμμένοι λογαριασμοί χρηστών. Αυτό βέβαια δεν σημαίνει ότι οι πραγματικοί χρήστες φτάνουν όντως στον αριθμό αυτό, καθώς τίποτα δεν αποτρέπει έναν επισκέπτη από το να δημιουργήσει πολλαπλές εγγραφές. Όποιος κι αν είναι ο πραγματικός αριθμός των χρηστών, πρόκειται πάντως για εκατοντάδες χιλιάδες χρήστες. Η ιστοσελίδα διευκόλυνε την πώληση ναρκωτικών ουσιών και παράνομων υπηρεσιών.

Το μεγαλύτερο κεφάλαιο της ιστοσελίδας Silk Road ήταν η απόλυτη ανωνυμία που παρείχε στους χρήστες αλλά και τους πωλητές. Και σε αυτό συνέβαλε φυσικά, ότι η online αγορά λειτουργούσε αποκλειστικά με bitcoins, διασφαλίζοντας το απόρρητο των συναλλαγών. Από το κατηγορητήριο μαθαίνουμε για το ψηφιακό νόμισμα πως τα bitcoins είναι μια ανώνυμη και αποκεντρωμένη μορφή ηλεκτρονικού χρήματος που υπάρχει αποκλειστικά στο Ίντερνετ και σε καμία φυσική μορφή.

Το νόμισμα παράγεται και ελέγχεται αυτόματα μέσω λογισμικού που τρέχει σε δίκτυο peer-to-peer. Οι συναλλαγές με bitcoins διαχειρίζονται συνολικά από τους υπολογιστές που αποτελούν το δίκτυο. Παρά το γεγονός ότι όλες οι συναλλαγές με bitcoins καταγράφονται σε μια κεντρική εγγραφή γνωστή ως Blockchain, είναι σχεδόν αδύνατο να εντοπιστούν οι χρήστες που τα χρησιμοποιούν, λόγω της ίδιας της φύσης του δικτύου αλλά και της προστασίας που παρέχει το λογισμικό. Και αυτό ακριβώς το απόρθητο -μέχρι πρόσφατα τουλάχιστον- επίπεδο προστασίας ήταν ο ακρογωνιαίος λίθος του κόσμου της online μαύρης αγοράς: σε μόλις δύο χρόνια, η ιστοσελίδα συγκέντρωσε έσοδα κάπου 9,5 εκατομμυρίων bitcoins, ή 1,2 δισ. δολάρια σε πραγματικό χρήμα, χαρίζοντας προμήθεια 80 εκατομμυρίων δολαρίων στον ιδιοκτήτη της.

Βιβλιογραφία

Ελληνόγλωσση

- Αγγελής Ι. (2000), «Διαδίκτυο (Διαδίκτυο) και ποινικό δίκαιο. Έγκλημα στον κυβερνοχώρο», Ποινικά Χρονικά, σελ. 675 επ., Εκδ. Δίκαιο και Οικονομία, Π.Ν. Σάκκουλας·
- Αλεξιάδης Σ. (1996), «Εγχειρίδιο Εγκληματολογίας», Θεσσαλονίκη, Εκδ. Σάκκουλα
- Αλιβιζάτος Ν. (1987) «Η Συνταγματική θέση των ενόπλων δυνάμεων» Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή
- Βλαχόπουλος Κ (2007), «Ηλεκτρονικό Έγκλημα», Εκδόσεις Νομικής Βιβλιοθήκης
- Γαρδίκα Κ.Γ. (1966), «Εγκληματολογία» τόμος Α', «Τα γενικά και ατομικά αίτια των εγκλημάτων» 5η Έκδοση, Αθήνα
- Γαρδίκας Κ. Γ. (1955), «Εγκληματολογία» τεύχος Γ' εκδόσεις Δημ. Ν. Τζάκα – Στ. Δελαγραμμάτικα, Αθήνα
- Δαγτόγλου Π. (2005), «Συνταγματικό Δίκαιο – ατομικά δικαιώματα», Τόμος Α, δεύτερη αναθεωρημένη έκδοση, Εκδόσεις Αντ, Ν. Σάκκουλα, Αθήνα – Κομοτηνή
- Δήμου Γ. (2002), «Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων», Αθήνα
- Ζάννη Αν.(2005), «Το διαδικτυακό έγκλημα, Αθήνα», Αντ. Ν. Σάκκουλας
- Ζαραφωνίτου Χ. (2009), «Τάσεις και Εξελίξεις στη Διδασκαλία, την Έρευνα και την επαγγελματική άσκηση της Εγκληματολογίας στην Ελλάδα», ΠοινΔικ & Εγκληματολογία 2/2009 (Ετος 1ο)
- Ιωαννίδης Β. και Κουτσελίνη Α.(2002), «Έγκλημα. Μια γενική θεώρηση ενός διαχρονικού φαινομένου», Αστυνομική Ανασκόπηση, μέρος Α', τεύχος 216, σελ. 680-685
- Κουράκης Ν. (2001), «Το Έγκλημα και οι εγκληματολογικές επιστήμες στον 21ο αιώνα», Ποινικός Λόγος, 801-803
- Λάζος Γ. (2001), «Πληροφορική και έγκλημα», Νομική Βιβλιοθήκη
- Λέανδρος, Ν. (2005), «Το διαδίκτυο: ανάπτυξη και αλλαγή». Αθήνα, Εκδόσεις Καστανιώτης.

- Μαγκάκη (1989), ΣυστΕρμΠΚ αρθρ.1 αρ 2, Χωραφά 5, Ανδρουλάκη Ι, 95 «Η αιτιολόγηση των αποφάσεων των ποινικών δικαστηρίων», τ. Α'
- Μανιάτης Α. (2012), «Δίκαιο ΜΜΕ», Πανεπιστημιακές σημειώσεις
- Melossi D., "Η κοινωνική θεωρία και οι μεταβαλλόμενες αναπαραστάσεις του εγκληματία. Εικόνες Εγκλήματος", εισαγωγή – επιμέλεια: Αφρ. Κουκουτσάκη, πρόλογος: Umberto Gatti, Πλέθρον
- Παρατηρητήριο για την Κοινωνία της πληροφορίας (2011), «Η χρήση του διαδικτύου από του Έλληνες»
- Παυλόπουλος Π. (1987), «Τεχνολογική Εξέλιξη και Ατομικά Δικαιώματα», NoB
- Τσουραμάνης Χ. (2003), «Σύγχρονα Κοινωνικά Προβλήματα. Η ελληνική πραγματικότητα», Αθήνα, Εκδ. Παπαζήσης
- Τσουραμάνης Χρ. (2005), «Ψηφιακή Εγκληματικότητα - Η (αν)ασφαλής όψη του διαδικτύου», Αθήνα, Εκδ.Β.Ν. Κατσαρού.
- Χρυσογόνος Κ. (2002), «Ατομικά και κοινωνικά Δικαιώματα», 2η Έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή

Ξενόγλωσση

- Acquisti A &. Gross R. (2006), “Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook”, PET 2006
- Boyd D., Ellison N., (2007), “Social Network Sites: Definition, History and Scholarship”, Journal of Computer-Mediated Communication, Vol. 13, No.1
- Forester T. and Morrison P. (1994), “Computer Ethics: Cautionar F Tales and Ethical Dilemmas in Computing”. 2nd ed. Cambridge, MA: MIT Press
- Jagatic, T., Johnson, N., Jakobsson, M., Menczer, F. (2007). “Social phishing”. Communications of the ACM, 5 (10), 94-100
- Morrison W. (1995), “Theoretical Criminology: from modernity to post-modernity” Great Britain
- Newman R (2004), “Identity Theft” US Department of Justice, διαθέσιμο ηλεκτρονικά: https://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf, ανακτήθηκε στις 13/10/2013

Ηλεκτρονικές πηγές

- About LinkedIn, Διαθέσιμο Ηλεκτρονικά: http://press.linkedin.com/about, Ανακτήθηκε 05/10/2013
- Άρθρο από την Ηλεκτρονική Έκδοση της Εφημερίδας Καθημερινή (2009) με θέμα: «Στόχος εξαπάτησης τα Social Media», Διαθέσιμο ηλεκτρονικά: http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_21/10/2009_303476, ανακτήθηκε 20/10/2013
- Άρθρα Ποινικού Κώδικα, ηλεκτρονικά διαθέσιμα: http://www.e-crime.gr/nomothesia/PoinKod.pdf, ανακτήθηκε στις 12/10/2013
- Αρχεία Ελληνικής Αστυνομίας (2014), http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=43803&Itemid=1149&lang=, ανακτήθηκε στις 30/08/2014
- Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα (2013), ηλεκτρονική ιστοσελίδα: http://www.dpa.gr/portal/page?_pageid=33,170929&_dad=portal&_schema=PORTAL, Ανακτήθηκε στις 12/10/2013
- Βικιπαίδεια (2013), «Το Διαδίκτυο», διαθέσιμο ηλεκτρονικά: http://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF, Ανακτήθηκε: 01/08/2013
- Βλασσόπουλος Γ. (2012), «Πειρατεία Λογισμικού», διαθέσιμο ηλεκτρονικά: http://7gym-perist.att.sch.gr/autosch/joomla15/attachments/article/18/%CE%A0%CE%B5%CE%B9%CF%81%CE%B1%CF%84%CE%B5%CE%AF%CE%B1%20%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%BF%CF%8D%20-%20Giannis%20Vlassopoulos.pdf, Ανακτήθηκε στις 04/10/2013
- Βλαχόπουλος Κ (χ.χ.), Υποψήφιος Διδάκτωρ Τμήματος Πληροφορικής Ιονίου Πανεπιστημίου, «Ηλεκτρονικό Έγκλημα. E-crime», παρουσίαση διαθέσιμη ηλεκτρονικά: http://www.e-crime.gr/301.pdf, Ανακτήθηκε στις 23/09/2013
- Business Software Alliance (2010), «Η πειρατεία λογισμικού», διαθέσιμο ηλεκτρονικά: http://webcache.googleusercontent.com/search?q=cache:ojwxCrgwJeAJ:blogs.sch.gr/plinetfk/files/2009/05/sw-piracy.pdf+&cd=2&hl=el&ct=clnk&gl=gr, Ανακτήθηκε στις 13/10/2013

- Cyberthetics (2013), «Τι είναι το Διαδίκτυο», Διαθέσιμο ηλεκτρονικά: http://www.cyberethics.info/cyethics1/index.php?option=com_content&view=article&id=158&Itemid=66&lang=el, Ανακτήθηκε 01/08/2013
- Δελτίο Τύπου ΣΔΟΕ (2013), «ΣΔΟΕ πειρατεία λογισμικού», διαθέσιμο ηλεκτρονικά: http://web.opi.gr/portal/page/portal/opi/newsall/press/sdoe_el, Ανακτήθηκε στις 13/10/2013
- Δελτίο Τύπου ΕΛ.ΑΣ. (2014), Μείωση των βασικών δεικτών εγκληματικότητας, ηλεκτρονικά διαθέσιμη αναδημοσίευση: http://www.eglimatikotita.gr/2014/05/2014_15.html, ανακτήθηκε στις 02/09/2014
- ΕΕΤΤ, Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, «Το Διαδίκτυο και Εγώ», διαθέσιμο ηλεκτρονικά: http://www.eett.gr/opencms/export/sites/default/admin/downloads/Informative_Documentation/Διαδίκτυο_and_Me.pdf, Ανακτήθηκε 01/08/2013
- Εφημερίδα ΚΑΘΗΜΕΡΙΝΗ (2012), «Η «διαδικτυακή τρομοκρατία» απειλεί τη διεθνή οικονομία», διαθέσιμο ηλεκτρονικά: http://portal.kathimerini.gr/4dcgi/_w_articles_kathextra_7_14/01/2012_422676, ανακτήθηκε στις 08/10/2013
- Ηλεκτρονικό άρθρο (24/05/2009), με θέμα: «Θανατική ποινή», διαθέσιμο: http://thanatikipoini.blogspot.gr/2009/05/blog-post_24.html, Ανακτήθηκε στις 20/09/2013
- Ιστοσελίδα Ελληνικής Αστυνομίας (2013), «Ηλεκτρονικό Έγκλημα», διαθέσιμη: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Ite, Ανακτήθηκε στις 22/09/2013
- Internet και Ηλεκτρονικό Έγκλημα (2007), Διαθέσιμο ηλεκτρονικά: http://dide.flo.sch.gr/Plinet/Tutorials/Internet-ElectronicCrime-LionHeart.pdf, ανακτήθηκε στις 28/08/2014
- Ιστοσελίδα FBI (2013), http://www.fbi.gov/, ανακτήθηκε στις 18/10/2013
- Κοινή Εποπτική Αρχής της Ευρωπόλ (2012), «Πέμπτη Έκθεση Δραστηριοτήτων της Κοινής Εποπτικής Αρχής, 2008-2012», διαθεσιμό ηλεκτρονικά: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2012/JSB%20EUROPOL%20ACTIVITY%20REPORT%202008-2012.EL.1.DEFJPG.PDF, Ανακτήθηκε στις 08/10/2013
- Μίμης Χ. (2011) «ΣΔΟΕ: Πρόστιμα για παράνομο λογισμικό», διαθέσιμο ηλεκτρονικά: http://www.star-fm.gr/2011/11/02/%CE%A3%CE%94%CE%9F%CE%95-

%CE%A0%CF%81%CF%8C%CF%83%CF%84%CE%B9%CE%BC%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%80%CE%B1%CF%81%CE%AC%CE%BD%CE%BF%CE%BC%CE%BF-%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C/, ανακτήθηκε στις 09/10/2013

- Μυλωνόπουλος (2010), «Ποινικό Δίκαιο», διαθέσιμο: http://www.poinikachronika.gr/assets/Mylonopoulos-PoinDik-CenikoM%20I-10%20first%20p..pdf, Ανακτήθηκε στις 20/09/2013
- neolaia.grTeam (2013), «Ελλάδα. Στις τελευταίες θέσεις στη χρήση Διαδίκτυο», διαθέσιμο ηλεκτρονικά: http://www.neolaia.gr/2013/01/29/iove-Διαδίκτυο/#.UhH-5NLHYcY, Ανακτήθηκε στις 13/08/2013
- On-line κοινότητα των φοιτητών Πληροφορικής του Ο.Π.Α (2007), ««Πειρατές» λογισμικού 6 στους 10 Έλληνες χρήστες Η/Υ», διαθέσιμο ηλεκτρονικά: http://t-h.wikispaces.com/file/view/%C2%AB%CE%A0%CE%B5%CE%B9%CF%81%CE%B1%CF%84%CE%AD%CF%82%C2%BB+%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%BF%CF%8D+6+%CF%83%CF%84%CE%BF%CF%85%CF%82+10+%CE%88%CE%BB%CE%BB%CE%B7%CE%BD%CE%B5%CF%82+%CF%87%CF%81%CE%AE%CF%83%CF%84%CE%B5%CF%82+%CE%97%CE%A5.pdf/32305559/%C2%AB%CE%A0%CE%B5%CE%B9%CF%81%CE%B1%CF%84%CE%AD%CF%82%C2%BB%20%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%BF%CF%8D%206%20%CF%83%CF%84%CE%BF%CF%85%CF%82%2010%20%CE%88%CE%BB%CE%BB%CE%B7%CE%BD%CE%B5%CF%82%20%CF%87%CF%81%CE%AE%CF%83%CF%84%CE%B5%CF%82%20%CE%97%CE%A5.pdf, Ανακτήθηκε στις 10/10/2013
- Πανελλήνιο Σχολικό Δίκτυο (2013), ηλεκτρονική ιστοσελίδα: http://www.sch.gr/, ανακτήθηκε στις 11/10/2013
- Παπαγεωργίου Ε (χ.χ.), «Ο υπόκοσμος στην Αρχαία Ελλάδα», διαθέσιμο ηλεκτρονικά: http://www.apologitis.com/gr/ancient/ypokosmos.htm, Ανακτήθηκε στις 18/09/2013
- ΣΚΑΙ (2011), «Κοινωνία της Πληροφορίας: Αυξάνεται η διείσδυση του Διαδικτύου», Διαθέσιμο ηλεκτρονικά: http://www.skai.gr/news/technology/article/170570/koinonia-tis-pliroforias-auxanetai-i-dieisdusi-tou-idernet/, Ανακτήθηκε 13/08/2013

- Στεργίου Ε. (2007), «Χρήσιμες συμβουλές για ασφαλή πλοήγηση στο Διαδίκτυο», διαθέσιμο ηλεκτρονικά: http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_1_26/09/2007_180860, Ανακτήθηκε στις 9/10/2013
- Τσακανίκας Α. (2013), «Το Διαδίκτυο στην Ελλάδα: Εμπόδια και Προοπτικές», διαθέσιμο ηλεκτρονικά: http://www.iobe.gr/media/Hmerides/iobeGooglepresentationfinal.pdf, Ανακτήθηκε στις 10/08/2013
- WIKIPEDIA (2o13), «Computer Misuse Act 1990», διαθέσιμο ηλεκτρονικά: http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990#The_Computer_Misuse_Act, ανακτήθηκε στις 10/10/2013