**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**

**ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**Π.Μ.Σ «Ασφάλεια Ψηφιακών Συστημάτων»**

# ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

## «Εξιχνίαση Ηλεκτρονικού Εγκλήματος»

**Συντάκτρια: Ελένη Γκύζη – ΜΤΕ 1506**

**Επιβλέπων Καθηγητής: Κ. Λαμπρινουδάκης**

**Αθήνα 28 Φεβρουαρίου 2018**

## *ΕΥΧΑΡΙΣΤΙΕΣ*

*Θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου Κωνσταντίνο Λαμπρινουδάκη και την κυρία Ευαγγελία Μήτρου για την πολύτιμη συμβολή τους για την εκπόνηση της παρούσας Διπλωματικής Εργασίας, αλλά και για τη γενικότερη υποστήριξή της κατά τη διάρκεια των Μεταπτυχιακών σπουδών μου.*

# Περίληψη

Η ψηφιακή επανάσταση, δηλαδή οι σαρωτικές αλλαγές που επέφερε η πληροφορική και η τεχνολογία των επικοινωνιών λόγω της ευρείας χρήσης των ψηφιακών τεχνολογιών, όπως παραδείγματος χάριν ο ηλεκτρονικός υπολογιστής και τα κινητά τηλέφωνα, σηματοδότησε την έναρξη της εποχής της Πληροφορίας.

Οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο αποτελούν πλέον ένα από τα πιο σπουδαιότερα επιτεύγματα της τεχνολογίας καθώς με τη διείσδυσή τους στην καθημερινότητα των ανθρώπων δημιούργησαν τη δυνατότητα να ανταλλάσσονται και να μεταφέρονται πληροφορίες ελεύθερα και να υπάρχει άμεση πρόσβαση σε γνώσεις που θα ήταν δύσκολο ή αδύνατο στο παρελθόν. Είναι γεγονός ότι πλέον έχουν πραγματοποιηθεί ουσιαστικές και παράλληλα θετικές αλλαγές στην οργάνωση της πολιτικής, οικονομικής και κοινωνικής ζωής και στις καθημερινές δραστηριότητες, όπως η επικοινωνία, οι συναλλαγές, η εκπαίδευση, η διασκέδαση, η παραγωγική διαδικασία, ενώ η ουσιαστική συμβολή στην προαγωγή της επιστήμης είναι εξίσου σημαντική. Τα πληροφοριακά συστήματα αποτελούν ένα χρησιμότατο εργαλείο, καθώς προσφέρουν άπειρες δυνατότητες στους χρήστες τους, οι οποίοι καλούνται τόσο να τις ανακαλύψουν και να τις εκμεταλλευτούν, όσο και να συμβάλουν με τον τρόπο τους στη διαρκή μεταβολή και εξέλιξή τους.

Η μετάβαση στην Κοινωνία της Πληροφορίας συνεπάγεται πολλαπλά οφέλη για κάθε πολίτη ατομικά και αλλά και γενικά για το κοινωνικό σύνολο. Παράλληλα όμως δημιουργούνται και οι κατάλληλες συνθήκες και προϋποθέσεις για την ανάπτυξη νέων μορφών εγκληματικότητας και τη δημιουργία νέων κινδύνων. Η χρήση των υπολογιστών και του διαδικτύου αποτελεί μεταφορά πληροφοριών και προσωπικών δεδομένων που συνήθως σχετίζονται με το επάγγελμα, την οικογενειακή κατάσταση, την περιουσιακή κατάσταση, την υγεία και άλλους τομείς της προσωπικής ζωής. Το γεγονός αυτό, σε συνδυασμό με τις απεριόριστες δυνατότητες που προσφέρει το διαδίκτυο αλλά και την

εύκολη και ταχύτατη πρόσβαση του κάθε χρήστη, είναι εύκολο να οδηγήσει σε κάθε είδους παράνομη πράξη.

Τα προηγμένα τεχνολογικά κράτη, αναγνωρίζοντας τους εν λόγω κινδύνους και λαμβάνοντας υπόψη την ανάγκη για προστασία θεμελιωδών δικαιωμάτων του ατόμου οριοθέτησης της χρήση της τεχνολογίας και της πληροφορικής προς το συμφέρον της κοινωνίας, προχώρησαν στη θέσπιση ειδικών νομικών ρυθμίσεων καθώς δεν ήταν δυνατό οι παραδοσιακές γενικές διατάξεις να αντιμετωπίσουν τις νέες αυτές μορφές εγκλήματος, οι οποίες είναι άρρηκτα συνδεδεμένες με τη ραγδαία εξέλιξη της τεχνολογίας και της πληροφορικής.

Στο πλαίσιο αυτής της εργασίας μελετάται το ηλεκτρονικό και διαδικτυακό έγκλημα, οι μορφές του και οι κοινωνικές προεκτάσεις του, όπως επίσης και οι τρόποι αντιμετώπισής του. Περιγράφεται το νομικό πλαίσιο και οι διατάξεις που διέπουν την ποινική αντιμετώπισή του σε Ευρωπαϊκό επίπεδο αρχικά και μετέπειτα στην Ελληνική νομοθεσία και παρουσιάζονται παράλληλα οι πρόσφατες τροποποιήσεις στον Ποινικό Κώδικα.

# Πίνακας Περιεχομένων

## Περιεχόμενα

# Κεφάλαιο 1

# Βασικές Έννοιες Ηλεκτρονικού/Διαδικτυακού Εγκλήματος

## 1.1. Εισαγωγή

Η ραγδαία ανάπτυξη της τεχνολογίας και ειδικότερα της επιστήμης της πληροφορικής, έχει επιφέρει τεράστιες αλλαγές στην καθημερινότητα σχεδόν όλων των ανθρώπων. Η τεχνολογία και η πληροφορική έχει εισβάλει σχεδόν σε όλους τους τομείς και έχει βελτιώσει σημαντικά την ποιότητα της ζωής μας, καθώς διευκολύνονται και εξυπηρετούνται γρηγορότερα οι καθημερινές μας ανάγκες. Παράλληλα όμως, έχουν δημιουργηθεί και οι ιδανικές συνθήκες για την ανάπτυξη νέων μορφών εγκληματικότητας, που σχετίζονται με τα συστήματα πληροφοριών και το διαδίκτυο.

Η εν λόγω εγκληματικότητα μεταβάλλεται με γρήγορους ρυθμούς ακολουθώντας τις τεχνολογικές εξελίξεις και λαμβάνει διάφορες μορφές, όπως: επιθέσεις κατά συστημάτων πληροφοριών, προσβολές της ιδιωτικότητας απάτη, παραβιάσεις πνευματικής ιδιοκτησίας, διάδοση παιδικής πορνογραφίας όπως επίσης υποστήριξη της διάπραξης παραδοσιακών εγκλημάτων. Η ελευθερία της έκφρασης, η οποία αποτελεί αναφαίρετο δικαίωμα των πολιτών κάθε κοινωνίας, σε συνδυασμό με τη διεύρυνση της χρήσης του διαδικτύου οδήγησε στην ενδυνάμωση της ελεύθερης έκφρασης και στην διάδοση νέων ιδεών μέσω νέων πηγών πληροφόρησης. Όμως καθώς ένα βασικό χαρακτηριστικό του διαδικτύου είναι η ανωνυμία, δημιουργούνται οι ιδανικές συνθήκες για τέλεση των ανωτέρω παράνομων ενεργειών και εγκλημάτων, τα οποία καθίσταται δύσκολο να εξιχνιαστούν και να διαλευκανθούν, με αποτέλεσμα η παραβατικότητα να αποτελεί συχνό και με αυξανόμενη ένταση φαινόμενο καθώς ο κυβερνοχώρος δεν μπορεί να ελεγχθεί το ίδιο αποτελεσματικά με τον πραγματικό κόσμο.

Σήμερα, τα πληροφοριακά συστήματα αποτελούν αναπόσπαστο και σημαντικό μέρος της οικονομίας και της κοινωνίας όλων των κρατών. Πολλά πληροφοριακά συστήματα είναι διασυνδεδεμένα μεταξύ πολλών κρατών, ενισχύοντας με αυτόν τον τρόπο τη διασυνοριακή επικοινωνία. Η ανάγκη για την συνεχή και ομαλή λειτουργία τους είναι επιτακτική και αποτελεί σημαντική προτεραιότητα των εμπλεκόμενων μερών. Αυτή η ανάγκη λοιπόν είχε ως αποτέλεσμα την έναρξη διεργασιών για τη θέσπιση νομοθετικού και κανονιστικού πλαισίου για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, τόσο σε διεθνές όσο και σε Ευρωπαϊκό επίπεδο.

## 1.2. Ηλεκτρονικοί Υπολογιστές και Διαδίκτυο

Η ραγδαία ανάπτυξη της τεχνολογίας τον 20$^{ο}$ αιώνα, ο οποίος ήταν η αρχή μεγάλων επιστημονικών ανακαλύψεων, είχε ως συνέπεια να πραγματοποιηθούν επαναστατικές αλλαγές στην καθημερινότητα των ανθρώπων με θετικές και αρνητικές συνέπειες. Η χρήση της τεχνολογίας ξεκίνησε με τη μετατροπή των φυσικών πρώτων υλών σε εργαλεία. Μετέπειτα, μια σειρά τεχνολογικών επιτευγμάτων, όπως το ραδιόφωνο, το αυτοκίνητο, ο υπολογιστής και το διαδίκτυο, συνέβαλλαν στην αλλαγή των καθημερινών δραστηριοτήτων αλλά και στον τρόπο σκέψης του σύγχρονου ανθρώπου.

Σήμερα η χρήση των ηλεκτρονικών υπολογιστών είναι ευρέως διαδεδομένη και ειδικά στις νεαρές ηλικίες, όπου η χρήση τους εκτοξεύεται. Πολλές από τις καθημερινές μας δραστηριότητες υποστηρίζονται από τους υπολογιστές καθώς μπορούμε να γράφουμε, να κάνουμε αριθμητικές πράξεις, να παίζουμε παιχνίδια, να ακούμε μουσική, να ψωνίζουμε και γενικά να δραστηριοποιούμαστε μέσω αυτών.

Η τεχνολογία εξελίσσεται και η χρήση του ηλεκτρονικού υπολογιστή γίνεται ολοένα και περισσότερο αναγκαία, καθώς οι υπολογιστές μπορούν να επεξεργάζονται με μεγάλη ακρίβεια και πολύ γρήγορα τεράστιο όγκο δεδομένων, καθιστώντας τους απαραίτητους σε διάφορους τομείς, ως υποστηρικτικό εργαλείο:

- Στις επιστήμες
- Στην εκπαίδευση
- Στην ιατρική
- Στη δημόσια διοίκηση
- Στις συγκοινωνίες
- Στα διάφορα επαγγέλματα

Όμως το μεγάλο βήμα της τεχνολογίας των υπολογιστών πραγματοποιήθηκε με τη διασύνδεσή τους μέσω του Διαδικτύου. Το Διαδίκτυο αποτελεί ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι βρίσκονται διασκορπισμένοι σε όλον τον πλανήτη και επικοινωνούν μεταξύ τους ανταλλάσσοντας δεδομένα. Η ανταλλαγή μηνυμάτων (πακέτων) είναι εφικτή με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού.

Αποτελεί την κύρια μηχανή με την οποία τα άτομα επικοινωνούν μεταξύ τους ταχύτερα πλέον από ποτέ. Στα σπουδαιότερα πλεονεκτήματά του έχουν περιληφθεί η ταχύτητα και η άνεση. Τα πάντα μπορούν να πραγματοποιηθούν με το πάτημα ενός κουμπιού του πληκτρολογίου ή με ένα κλικ του ποντικιού. Στο διαδίκτυο ο τόπος χάνει τη σημασία του. Η σωστή χρήση του διαδικτύου μπορεί να ανεβάσει το μορφωτικό επίπεδο των χρηστών του, προσφέροντάς τους επίκαιρα στοιχεία από όλους τους τομείς της σύγχρονης γνώσης. Το διαδίκτυο και κατ’ επέκταση οι ηλεκτρονικοί υπολογιστές έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητάς μας, είτε ως μέσα ψυχαγωγίας – ενημέρωσης, είτε ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων.

Ξεκίνησε το 1969 ως ερευνητικό στρατιωτικό πρόγραμμα, με την ονομασία ARPANET, από το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών της Αμερικής. Όλα

πρωτοξεκίνησαν με τη σύνδεση τεσσάρων υπολογιστών, που βρίσκονταν σε διαφορετικές πόλεις της Αμερικής. Οι υπολογιστές συνδέονταν με τέτοιο τρόπο, ώστε, αν διακοπτόταν μια σύνδεση, οι υπόλοιποι να συνέχιζαν απρόσκοπτα την επικοινωνία τους. Αυτή η βασική αρχή σύνδεσης ισχύει ακόμη και σήμερα καθώς όλοι οι επιχειρηματικοί, κυβερνητικοί και ακαδημαϊκοί οργανισμοί διασύνδεουν τον εξοπλισμό επεξεργασίας των δεδομένων τους μέσω μίας ομάδας διασυνδεδεμένων δικτύων, το διαδίκτυο (Stallings W, 2008).

Το διαδίκτυο ήταν η αιτία ώστε ο ηλεκτρονικός υπολογιστής από υποστηρικτικό εργαλείο να μετατραπεί σε μέσο άντλησης πληροφοριών αλλά και σε μέσο επικοινωνίας.

Μέσο άντλησης πληροφοριών, καθώς μέσα σε λίγα δευτερόλεπτα μπορούν να μεταδοθούν με μεγάλη ταχύτητα πληροφορίες απ' όλο τον κόσμο στον υπολογιστή μας. Η εξέλιξη αυτή ανέδειξε ακόμα περισσότερο την αξία της πληροφορίας στις σύγχρονες κοινωνίες, ώστε να μιλάμε πια για Κοινωνία της Πληροφορίας.

Μέσο επικοινωνίας, καθώς έχοντας πρόσβαση στο Διαδίκτυο είναι δυνατή η επικοινωνία με ανθρώπους από όλο τον κόσμο, μέσω διαφόρων υπηρεσιών/εφαρμογών:

- Ηλεκτρονικό Ταχυδρομείο (email)
- Συνομιλία (chat)
- Τηλεδιάσκεψη (Teleconference)
- Ομάδες Συζητήσεων (Newsgroups)

Επίσης επαναστατική θεωρείται και αλλαγή που επήλθε σε διάφορες παραδοσιακές δραστηριότητες, οι οποίες είναι πλέον εφικτό να πραγματοποιούνται από απόσταση:

- Τηλε-εκπαίδευση (e-learning)
- Τηλεργασία (teleworking)

- Ηλεκτρονικό εμπόριο (e-commerce)
- Ηλεκτρονική διακυβέρνηση (e-governance)
- Τηλεϊατρική

Είναι αδιαμφισβήτητο ότι η χρήση των ηλεκτρονικών υπολογιστών και η ανακάλυψη του διαδικτύου επηρέασε σε τεράστιο βαθμό την ανθρωπότητα. Εκατομμύρια χρήστες καθημερινά σε όλο τον κόσμο χρησιμοποιούν τους υπολογιστές και το διαδίκτυο στις καθημερινές τους δραστηριότητες, βελτιώνοντας την ποιότητα της ζωής τους και αλλάζοντας ριζικά τον τρόπο επικοινωνίας και το τρόπο σκέψης τους.

Πάρα ταύτα, η ένταξή τους στη ζωή μας δημιούργησε και μία σειρά από αρνητικές επιπτώσεις, οι οποίες συνδέονται άμεσα με την υπέρμετρη χρήση τους. Μερικά από τα σημαντικά προβλήματα είναι η αποξένωση, η μείωση ελεύθερου χρόνου , η υπερ-πληροφόρηση και η παραβατική συμπεριφορά.

## 1.3. Έγκλημα

Σύμφωνα με τον ορισμό του Ποινικού Κώδικα, στο Δεύτερο Κεφάλαιο – Η αξιόποινη πράξη, άρθρο 14 – Η έννοια της αξιόποινης πράξης, «έγκλημα είναι πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο». Σύμφωνα με το άρθρο 18 – Διαίρεση των αξιόποινων πράξεων, «κάθε πράξη που τιμωρείται με την ποινή του θανάτου ή της κάθειρξης είναι κακούργημα. Κάθε πράξη που τιμωρείται με φυλάκιση ή με χρηματική ποινή ή περιορισμό σε σωφρονιστικό κατάστημα είναι πλημμέλημα. Κάθε πράξη που τιμωρείται με κράτηση ή πρόστιμο είναι πταίσμα.

Το έγκλημα είναι μία σύνθετη έννοια, καθώς σε αυτή συνυπάρχουν από τη μία η κοινωνική, βιολογική και ψυχολογική πραγματικότητα του ανθρώπου και από την άλλη η δεοντολογία που διέπει στο πλαίσιο ορισμένης κοινωνίας την κοινωνική συμπεριφορά του. Το έγκλημα αποτελεί αναμφίβολα αναπόσπαστο κομμάτι της εκάστοτε κοινωνίας

και λειτουργεί ως ένας οργανισμός μέσα στον οποίο μεταβάλλονται οι εκφάνσεις, τα μέσα τέλεσης και το νομικό πλαίσιο που το διέπει (Μαγκάκης, 1984).

Το νόημα του περιεχομένου του εγκλήματος συνίσταται στο ότι αποτελεί μία πράξη η οποία θίγει τις αξίες της κοινωνική ζωής, και που η τέλεση της εκφράζει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται κοινωνικά αναγκαία (Μαγκάκης, 1984).

Το φαινόμενο του εγκλήματος διέπεται από διαχρονικότητα, καθώς ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Καμιά κοινωνία δεν έχει απαλλαχθεί από αυτό, και σε κάθε έγκλημα (προσβολή), υπήρχε, υπάρχει και θα υπάρχει ποινή (αντίδραση). Αντίθετα αυτό που παρατηρείται είναι μια αύξηση του εγκληματικού φαινομένου και συγχρόνως εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς (Μαγκάκης, 1984).

Από πολύ παλαιά, επίσης, είχε υποστηριχθεί ότι το έγκλημα είναι στην πραγματικότητα η συνισταμένη αιτίων ατομικών, που εκπορεύονται δηλαδή από το ίδιο το άτομο, αλλά και επιδράσεων περιβαλλοντικών, χωρίς να είναι δυνατόν να προσδιοριστεί ποια συμβάλλουν περισσότερο (Βλ. και Α. Γιωτοπούλου-Μαραγκοπούλου, 1979).

Παρά το γεγονός της συνεχούς εξέλιξης του εγκληματικού φαινομένου τα βασικά στοιχεία που το συνθέτουν παραμένουν τρία (Φαρσεδάκης Ι, 1996):

- Ο κανόνας – δηλαδή η έκφραση της κοινωνίας έναντι κάποιας συμπεριφοράς
- η παραβίαση – δηλαδή η ενέργεια που αθετεί το όριο της συμπεριφοράς
- η κύρωση – δηλαδή η ποινή

Είναι προφανές ότι δεν θα υπήρχε κύρωση αν δεν υπήρχε το έγκλημα, όπως και δεν θα υπήρχε έγκλημα αν δεν υπήρχε κανόνας συμπεριφοράς για να τον παραβεί κάποιος. Συμπεραίνουμε λοιπόν, ότι ένα από τα βασικά χαρακτηριστικά του εγκλήματος είναι η αλληλεπίδραση μεταξύ των τριών παραπάνω βασικών στοιχείων που το συνθέτουν.

Εν κατακλείδι, το έγκλημα αποτελεί αναπόσπαστο κομμάτι κάθε κοινωνίας, το οποίο εξελίσσεται και μεταβάλλεται, παίρνοντας νέες μορφές όπως επίσης μεταβάλλονται και τα μέσα τέλεσης και το εκάστοτε νομικό πλαίσιο που το καθορίζει. Το εγκληματικό φαινόμενο αποτελεί κοινωνικό φαινόμενο που ακολουθεί την εξέλιξη της ανθρώπινης κοινωνίας.

## 1.4. Ηλεκτρονικό και Διαδικτυακό Έγκλημα

Η παραβατική συμπεριφορά των χρηστών του διαδικτύου, οδήγησε στη δημιουργία μίας νέας μορφής εγκλήματος, το «ηλεκτρονικό έγκλημα». Το 1994 οι Forester και Morrison όρισαν το Ηλεκτρονικό Έγκλημα (Computer Crime) σαν «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης της». Δηλαδή, υφίσταται μία νέα μορφή εγκλήματος, η οποία διαφοροποιείται από την συμβατική μορφή, καθώς η τέλεση πραγματοποιείται μέσω ενός ηλεκτρονικού υπολογιστή.

Γενικά είναι αρκετά δύσκολο να δώσουμε έναν ακριβή ορισμό στο «ηλεκτρονικό έγκλημα» και κυρίως να το διαχωρίσουμε από το «κυβερνοέγκλημα». Καταρχήν, πρέπει να σημειωθεί ότι το «ηλεκτρονικό έγκλημα» αποτελεί ειδικότερη μορφή του κοινού εγκλήματος ενώ προηγείται χρονικά και λογικά του κυβερνοεγκλημάτος. Όπως παρατηρεί ο Αγγελής δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο ούτε στη διεθνή νομοθεσία, ούτε στη διεθνή νομολογία. Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) η εγκληματικότητα μέσω των υπολογιστών "αφορά κάθε παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που έχει σχέση με την αυτόματη επεξεργασία και μεταφορά στοιχείων" (Αγγελής Ι, 2000).

Σύμφωνα με τον Don Parker «το διαδικτυακό έγκλημα λοιπόν ή αλλιώς το κυβερνοέγκλημα (cybercrime), είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος,

αυτό για την τέλεση του οποίου ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο. Σχετίζεται με οποιαδήποτε μορφή κατάχρησης των δυνατοτήτων που προσφέρει το διαδίκτυο (Furnell, 2006).

Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, 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 διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου. Το ηλεκτρονικό έγκλημα προηγείται χρονικά του κυβερνοεγκλήματος (ΕΛ.ΑΣ - Δίωξη Ηλεκτρονικού Εγκλήματος).

Με τον όρο «κυβερνοέγκλημα» [cybercrime] νοούνται τρεις κατηγορίες ποινικών αδικημάτων :

- Γνήσια πληροφορικά εγκλήματα – Κλασικά ποινικά αδικήματα, που τελούνται μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών (πχ. απάτη, πλαστογραφία).

- Εγκλήματα σε σχέση με ψηφιακό περιεχόμενο – Ποινικά αδικήματα, που σχετίζονται με την διακίνηση παράνομου περιεχομένου μέσω συστημάτων πληροφοριών (πχ παιδική πορνογραφία).

- Εγκλήματα κατά πληροφοριακών συστημάτων – Ποινικά αδικήματα, που διαπράττονται κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων.

Σύμφωνα με τον Αργυρόπουλο (2001), θα διακρίνουμε τα παρακάτω ηλεκτρονικά εγκλήματα:

- Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Σε αυτήν την κατηγορία έχουμε εγκλήματα όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον (ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο). Εδώ το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος.

- Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς την ύπαρξη δικτύωσης. Τέτοιο έγκλημα θεωρείται η παράνομη αντιγραφή λογισμικού.

- Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο (τα λεγόμενα διαδικτυακά εγκλήματα). Η χρήση του διαδικτύου είναι απαραίτητο στοιχείο για την εγκληματική συμπεριφορά του δράστη. Εδώ εντάσσουμε τη διασπορά κακόβουλου λογισμικού.

Σύμφωνα με τον Neil Barrett (1997) τα ηλεκτρονικά εγκλήματα διακρίνονται σε δύο (2) κατηγορίες :

- Σε εκείνα που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ , η εισβολή σε ηλεκτρονικά αρχεία και ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών

- Σε εκείνα που υποστηρίζονται από Η/Υ και οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα μαύρου χρήματος που γίνονται ηλεκτρονικά

Σύμφωνα με τον Donald Pipkin (2003) τα ηλεκτρονικά εγκλήματα διακρίνονται σε τέσσερις (4) κατηγορίες :

- Στην πρώτη κατηγορία ανήκουν τα παραδοσιακά εγκλήματα τα οποία τελούνται με χρήση Η/Υ και ως τέτοια αναφέρει την απάτη, την κλοπή στοιχείων ιδιοκτητών πιστωτικών καρτών και την κλοπή της ηλεκτρονικής ταυτότητας.

- Στην δεύτερη κατηγορία υπάγονται τα ειδικά εγκλήματα των Η/Υ και σαν τέτοια ο συγγραφέας θεωρεί την επίθεση της άρνησης παροχής υπηρεσίων, την άρνηση πρόσβασης σε πληροφορίες και τη διασπορά καταστρεπτικών ιών.

- Στην τρίτη κατηγορία τοποθετεί τα αδικήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία και καταστροφή πληροφοριών που έχουν κλαπεί.

- Στην τέταρτη κατηγορία ανήκουν τα εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου.

Μια άλλη οπτική είναι η κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων που προτάθηκε από την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα που από την ίδρυση του στις αρχές της δεκαετία του 1980, διενήργησε έρευνες με

στόχο να εξακριβώσει την έκταση του εγκλήματος μέσω Η/Υ σε δημόσιο και ιδιωτικό τομέα. Οι κατηγορίες είναι (Furnell, 2006):

- Απάτη: Για προσωπική ωφέλεια (αλλοίωση των εισαγόμενων με νόμιμο τρόπο, καταστροφή /συμπίεση/ ακαταλληλότητα εκροών, αλλοίωση των δεδομένων του Η/Υ, αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρούμενων των προσβολών από τους ιούς)

- Κλοπή: των δεδομένων, του λογισμικού

- Χρήση λογισμικού χωρίς άδεια: χρήση παράνομων αντιγράφων λογισμικού

- Ιδιωτική εργασία: μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκομιδή κέρδους ή για ίδιον όφελος

- Χάκινγκ: :ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας

- Σαμποτάζ: η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή εξοπλισμό

- Εισαγωγή πορνογραφικού υλικού

- Ιοί: διάχυση ενός προγράμματος με σκοπό την ματαίωση της τρέχουσας εφαρμογής

Τα ηλεκτρονικά εγκλήματα μπορούν να διακριθούν σε τρεις κατηγορίες ανάλογα με τον τρόπο και το περιβάλλον τέλεσής τους:

- **Εγκλήματα που διαπράττονται τόσο σε κοινό περιβάλλον όσο και στο διαδίκτυο**

Η εξέλιξη της τεχνολογίας και η χρήση των ηλεκτρονικών υπολογιστών διευκολύνει την σύγχρονη εγκληματικότητα, η οποία λαμβάνει συνεχώς νέες διαστάσεις, καθώς οι δράστες συνεχώς προσαρμόζονται στα νέα δεδομένα και εξελίσσουν τους τρόπους τέλεσης των εγκλημάτων. Τα μέσα τέλεσης των εν λόγω εγκλημάτων αποτελούν ο ηλεκτρονικός υπολογιστής και η σύνδεση στο διαδίκτυο.

Όταν ένα «κοινό» έγκλημα τελείται σε ηλεκτρονικό περιβάλλον, δεν έχουμε ένα πρόσθετο στοιχείο στην αντικειμενική υπόσταση του αδικήματος, αλλά έναν εναλλακτικό τρόπο τέλεσης του αδικήματος. Στη συγκεκριμένη περίπτωση, η χρήση του Η/Υ και η σύνδεση με το διαδίκτυο είναι δηλαδή το μέσο τέλεσης της εγκληματικής συμπεριφοράς, το modus operandi. Οι δράστες διαπράττουν κοινά αδικήματα με τη διαφορά ότι ενεργούν στο ιδιόμορφο περιβάλλον του διαδικτύου.

Παραδείγματα εγκλημάτων που διαπράττονται τόσο σε κοινό περιβάλλον όσο και στο διαδίκτυο είναι τα αδικήματα της συκοφαντικής δυσφήμησης, της απειλής, της εκβίασης, της εξύβρισης, της απάτης, της πλαστογραφίας και της παραβίασης της πνευματικής ιδιοκτησίας.

- **Σε εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (Computer Crimes)**

Στην κατηγορία αυτή εντάσσονται τα εγκλήματα που τελούνται αποκλειστικά σε ηλεκτρονικό περιβάλλον εν ευρεία έννοια. Απαιτείται δηλαδή η χρήση ηλεκτρονικού

υπολογιστή, προκειμένου να πληρωθεί η αντικειμενική υπόσταση του εγκλήματος. Η σύνδεση του Η/Υ με το διαδίκτυο δεν αποτελεί προαπαιτούμενο για την τέλεσή τους, σε αντιδιαστολή με την περίπτωση των διαδικτυακών εγκλημάτων, τέλεση των οποίων νοείται μόνο στο ηλεκτρονικό περιβάλλον του διαδικτύου. Ειδοποιός διαφορά αυτής της κατηγορίας εγκλημάτων με την κατηγορία εκείνων που τελούνται τόσο σε κοινό όσο και σε ηλεκτρονικό περιβάλλον είναι ότι στα πρώτα απαραίτητο στοιχείο της αντικειμενικής υπόστασής τους αποτελεί η χρήση Η/Υ, χωρίς την οποία δεν υφίσταται τέλεσή τους, ενώ στα δεύτερα η χρήση του Η/Υ με ή χωρίς σύνδεση με το διαδίκτυο είναι ένα μέσο τέλεσης των εγκλημάτων αυτών (Αγγελής, 2000).

Ενδεικτικά, στην κατηγορία αυτή υπάγονται τα αδικήματα που προβλέπονται στο άρθρα 370Β και 370Γ του ελληνικού ποινικού δικαίου και σύμφωνα με τα οποία αξιόποινη πράξη είναι η αθέμιτη πρόσβαση σε δεδομένα ηλεκτρονικών υπολογιστών.

- **Σε γνήσια εγκλήματα του Κυβερνοχώρου με την έννοια της ποινικοποίησης συμπεριφοράς που έχει σχέση αποκλειστικά με τον Κυβερνοχώρο (Cybercrimes)**

Τα διαδικτυακά εγκλήματα περιλαμβάνουν τα ηλεκτρονικά εγκλήματα, όμως αποτελούν μία ευρύτερη έννοια. Για τη διάπραξή τους είναι απαραίτητος ένας ηλεκτρονικός υπολογιστής και σύνδεση στο διαδίκτυο, καθώς τελούνται αποκλειστικά σε διαδικτυακό περιβάλλον.

Παραδείγματα εγκλημάτων που διαπράττονται στον κυβερνοχώρο είναι η μεταβίβαση αποκρυπτογραφημένων κειμένων χωρίς σχετική άδεια, η μη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφοριών και η μόλυνση συστήματος πληροφοριών με ιούς.

Ανάλογα με το περιεχόμενο τα εγκλήματα διακρίνονται

- Εγκλήματα κατά της προσωπικότητας και ιδιωτικότητας
- Εγκλήματα κατά της περιουσίας
- Παράνομο και αθέμιτο/επιβλαβές περιεχόμενο

**Το πρώτο καταγεγραμμένο ηλεκτρονικό έγκλημα**

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

Συμπεραίνουμε λοιπόν ότι οι εγκληματικές πράξεις στηρίζονται πλέον σε πιο περίπλοκη και διαρκώς εξελισσόμενη τεχνολογία, χωρίς αυτό να σημαίνει ότι το συμβατικό - παραδοσιακό έγκλημα και τα μέσα διάπραξής του έπαψαν να υπάρχουν.

## 1.5. Κατηγορίες Ηλεκτρονικών-Διαδικτυακών Εγκλημάτων

Τα πιο διαδεδομένα ηλεκτρονικά/διαδικτυακά εγκλήματα είναι τα παρακάτω:

### 1.5.1 Κακόβουλες εισβολές σε δίκτυα

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

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

### 1.5.2 Ανεπιθύμητη αλληλογραφία

- **Spamming:** είναι η μαζική αποστολή ηλεκτρονικών μηνυμάτων ή άλλων, σε μια προσπάθεια προώθησης προϊόντων ή ιδεών. Λόγω του χαμηλού κόστους αποστολής, η αποστολή γίνεται σε μεγάλο αριθμό αποδεκτών. Η ταυτότητα του αποστολέα είναι συνήθως πλαστογραφημένη ή μεταμφιεσμένη, δηλαδή δεν είναι έγκυρη, καθώς ο βασικός στόχος είναι η απόκρυψη της πραγματικής ταυτότητας του αποστολέα.

Τα κυριότερα χαρακτηριστικά του spamming είναι:

- Απρόκλητο: Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα, η οποία θα δημιουργούσε ή θα προκαλούσε τη σχέση αυτή.

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

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

### 1.5.3 Ηλεκτρονικό ψάρεμα

- **Phising:** είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-'θύματος', με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί. Ο όρος ηλεκτρονικό ψάρεμα χρησιμοποιείται γιατί ο θύτης παρουσιάζεται μία αξιόπιστη οντότητα ώστε να προσελκύσει χρήστες, διαδικασία που παραλληλίζεται με τη διαδικασία του δολώματος στο ψάρεμα. Ένα ευρέως γνωστό παράδειγμα είναι η αποστολή email σε χρήστες internet banking με απώτερο σκοπό τη διαρροή προσωπικών δεδομένων όπως στοιχεία τραπεζικών λογαριασμών, πιστωτικών καρτών κτλ. Στο εν λόγω email αποστολέας φαίνεται μία τράπεζα η οποία ζητάει επιβεβαίωση username & password στο internet banking, επισημαίνοντας ότι η μη αποστολή θα οδηγήσει σε προσωρινή παύση λειτουργίας της εν λόγω υπηρεσίας.

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

- **Pharming:** είναι μια επίθεση που αποσκοπεί στην ανακατεύθυνση της επισκεψιμότητας ενός ιστότοπου σε έναν άλλο, πλαστό ιστότοπο. Οι δράστες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστοχώρο όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών.

### 1.5.4 Επιθέσεις άρνησης εξυπηρέτησης – DDoS

Αποτρέπει ή παρεμποδίζει την κανονική χρήση ή τη διαχείριση επικοινωνιακών δομών. Αυτή η επίθεση μπορεί να έχει συγκεκριμένο σκοπό: για παράδειγμα μια οντότητα μπορεί να συγκρατεί όλα τα μηνύματα που κατευθύνονται προς ένα συγκεκριμένο προορισμό. Μία άλλη μορφή άρνησης εξυπηρέτησης είναι η προσωρινή διακοπή της λειτουργίας ενός ολόκληρου δικτύου, είτε με αχρήστευσή του είτε με υπερφόρτωσή του με μηνύματα ώστε να μειωθεί σημαντικά η απόδοσή του. (William Stallings)

### 1.5.5 Κακόβουλο λογισμικό – Malware

Είναι λογισμικό που δημιουργήθηκε με την πρόθεση να τοποθετηθεί σε ένα σύστημα και να προκαλέσει βλάβες. Μπορεί να χωριστεί σε δύο κατηγορίες: αυτό που χρειάζεται ένα πρόγραμμα ξενιστή, και αυτό που είναι ανεξάρτητο. Η πρώτη κατηγορία αποτελείται κυρίως από τμήματα προγραμμάτων που δε μπορούν να υπάρξουν ανεξάρτητα από κάποιο πραγματικό πρόγραμμα εφαρμογής, βοηθητικό πρόγραμμα ή πρόγραμμα συστήματος. Τέτοια προγράμματα είναι οι ιοί, οι λογικές βόμβες, οι κερκόπορτες και ο δούρειος ίππος.

**Ιός (virus):** είναι ένα μικρό πρόγραμμα που μπορεί να μολύνει άλλα προγράμματα τροποποιώντας τα. Η τροποποίηση περιλαμβάνει τη δημιουργία ενός αντιγράφου του ιού, που με τη σειρά του θα μολύνει άλλα προγράμματα.

**Λογική βόμβα (logic bomb):** είναι ένα από τα παλαιότερα είδη προγραμμάτων απειλής, προγενέστερο από τους ιούς και τα σκουλήκια. Είναι κώδικας ενσωματομένος σε κάποιο κανονικό πρόγραμμα που είναι προγραμματισμένος να εκραγεί όταν ικανοποιούνται συγκεκριμένες συνθήκες. Παραδείγματα συνθηκών που μπορούν να χρησιμοποιηθούν για την πυροδότηση μιας λογικής βομβας είναι η παρουσία ή η απουσία συγκεκριμένων αρχείων, μία συγκεκριμένη ημέρα της εβδομάδας ή ημερομηνία, ή η εκτέλεση της εφαρμογής από κάποιο συγκεκριμένο χρήστη. Μετά την πυροδότησή της, η βόμβα μπορεί να τροποποιήσει ή να διαγράψει δεδομένα ή ολόκληρα αρχεία, να προκαλέσει το «πάγωμα» ενός μηχανήματος, ή να προκαλέσει κάποια άλλη ζημιά.

**Κερκόπορτες (backdoor or trap door):** είναι ένα μυστικό σημείο εισόδου σε ένα πρόγραμμα, το οποίο επιτρέπει σε κάποιον που είναι ενήμερος γι αυτό να αποκτήσει πρόσβαση χωρίς να περάσει από τις συνηθισμένες διαδικασίες ασφάλειας. Χρησιμοποιούνται νόμιμα εδώ και πολλά χρόνια από τους προγραμματιστές για τη διόρθωση και τον έλεγχο προγραμμάτων. Αυτό γίνεται συνήθως όταν ο προγραμματιστής αναπτύσσει μία εφαρμογή που περιέχει κάποια διαδικασία πιστοποίησης ή κάποια μακροσκελή διαδικασία διευθέτησης, που απαιτούν από το χρήστη να εισαγάγει πολλές τιμές προκειμένου να ξεκινήσει την εκτέλεση της εφαρμογής. Κατά την αποσφαλμάτωση (debug) του προγράμματος ο προγραμματιστής ενδεχομένως να επιθυμεί να αποκτήσει ειδικά προνόμια στην απαιτούμενη διαδικασία διευθέτησης και πιστοποίησης ή να επιθυμεί να διασφαλίσει ότι θα υπάρχει μια μέθοδος για την ενεργοποίηση του προγράμματος στην περίπτωση που υπάρχει κάποιο σφάλμα στην ενσωματωμένη διαδικασία πιστοποίησης της εφαρμογής. Η κερκόπορτα είναι ο κώδικας που αναγνωρίζει κάποια ειδική ακολουθία εισόδου ή ο οποίος ενεργοποιείται όταν εκτελείται από έναν συγκεκριμένο αναγνωριστικό χρήστη ή από μια απίθανη ακολουθία συμβάντων. Οι κερκόπορτες γίνονται απειλές όταν χρησιμοποιούνται από ασυνείδητους προγραμματιστές για την απόκτηση μη εξουσιοδοτημένης πρόσβασης.

**Δούρειος ίππος (Trojan horse):** είναι ένα χρήσιμο ή φιανομενικά χρήσιμο πρόγραμμα ή διαδικασία εντολών, πο περιέχει κρυφό κώδικα ο οποίος όταν καλείτα πραγματοποιεί κάποια ανεπιθύμητη ή επιβλαβή λειτουργία. Τα προγράμματα δούρειου ίππου μπορούν να χρησιμοποιηθούν για την έμμεση εκτέλεση λειτουργιών, τις οποίες ένας μη εξουσιοδοτημένος χρήστης δε θα μπορούσε να εκτελέσει άμεσα. Για παράδειγμα, για να αποκτήσει κάποιος χρήστης πρόσβαση στα αρχεία ενός άλλου χρήστη σε ένα κοινόχρηστο σύστημα, θα μπορούσε να δημιουργήσει ένα δούρειο ίππο ο οποίος όταν εκτελείται θα αλλάζει τα δικαιώματα πρόσβασης για τα αρχεία του άλλου χρήστη που τον ενεργοποίησε, έτσι ώστε τα αρχεία να είναι αναγνώσιμα από όλους τους χρήστες. Ο

δημιουργός του δούρειου ίππου θα μπορούσε να παρακινήσει τους χρήστες να εκτελέσουν το πρόγραμμα τοποθετώντας σε ένα κοινόχρηστο φάκελο και δίνοντας του ένα τέτοιο όνομα ώστε να φαίνεται ότι πρόκειται για μία χρήσιμη εφαρμογή

**Σκουλίκια (warms):** είναι ένα πρόγραμμα που μπορεί να δημιουργεί αντίγραφα του εαυτού του και να τα στέλνει από υπολογιστή σε υπολογιστή μέσω διαδικτύου. Κατά την άφιξή του το σκουλήκι μπορεί να ενεργοποιηθεί και να συνεχίσει να αναπαράγεται και να μεταδίδεται. Εκτός από τη διάδοσή του συνήθως πραγματοποιεί και κάποιες ανεπιθύμητες ενέργειες. Ψάχνει ενεργητικά για άλλα συστήματα προκειμένου να διαδοθεί και να τα μολύνει και αυτά με τη σειρά τους γίνονται αυτόματα το σημείο εκκίνησης για νέες επιθέσεις σε άλλα συστήματα.

**Άλλα είδη κακόβουλου λογισμικού:** rootkits, ransomeware, scareware, bacteria

### 1.5.6 Οικονομικό έγκλημα

Σκοπός των οικονομικών εγκλημάτων είναι το μεγάλο οικονομικό όφελος μέσω διάπραξης παρανομιών. Μορφές του οικονομικού εγκλήματος:

**Ξέπλυμα χρήματος**: ο όρος «ξέπλυμα χρήματος» χρησιμοποιείται για να περιγράψει τις διαδικασίες μέσω των οποίων τα κέρδη των εγκλημάτων (βρώμικο χρήμα) υπόκεινται σε μια σειρά διαδικασιών, οι οποίες καλύπτουν τις παράνομες ρίζες τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές/καθαρό χρήμα (Λάζος 2001).

**Νιγηριανή απάτη:** Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντάς τους με τεράστια κέρδη. Ο αποστολέας – απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρείας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητάει τη βοήθεια του θύματος – παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια, το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφθεί με προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψηφίου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχθεί. Ξεκινάει λοιπόν μια διαδικασία ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν (Τσουραμάνης 2005).

### 1.5.7 Διακίνηση παιδικού πορνογραφικού υλικού

Αποτελεί αδιαμφισβήτητα μια ειδεχθή εγκληματική δραστηριότητα, η οποία τα τελευταία χρόνια λαμβάνει έντονη δραστηριότητα και στη χώρα μας εντείνοντας την προσπάθεια των διωκτικών αρχών για τον περιορισμό του φαινομένου. Το υλικό πορνογραφίας ανηλίκων, που διακινείται μέσω του Διαδικτύου, μπορεί να είναι σε μορφή φωτογραφιών, βίντεο ή και οποιασδήποτε άλλης μορφής πολυμέσων.

Οι πιο διαδεδομένοι τρόποι προμήθειας - διακίνησης του συγκεκριμένου υλικού είναι οι εξής:

- Με την χρήση ειδικών Peer-to-Peer (P2P) προγραμμάτων τα οποία καθιστούν δυνατή την ανταλλαγή αρχείων μέσω διαδικτύου.

- Αποστολή σεσημασμένου υλικού πορνογραφίας ανηλίκων μέσω ηλεκτρονικής αλληλογραφίας (email), ως επισυναπτόμενα αρχεία.

- Τέτοιου είδος υλικό φιλοξενείται και σε διάφορους δικτυακούς ιστοτόπους (forum) περιορισμένης πρόσβασης καθόσον απαιτείται συνήθως από τον εκάστοτε χρήστη η δημιουργία λογαριασμού για να εισέλθει.

- Με την χρήση ειδικών πλατφόρμων που εξυπηρετούν τον διαμοιρασμό αρχείων, μεταξύ υπολογιστών.

Κάθε χρήστης διαδικτύου κατά την προμήθεια - διακίνηση υλικού πορνογραφίας ανηλίκων μέσω διαδικτύου, αφήνει το ψηφιακό του στίγμα με την μορφή της IP διεύθυνσης, προσδιορίζοντας έτσι μοναδικά την ταυτότητα του, ενώ τελευταίο διάστημα παρατηρούνται φαινόμενα τεχνικής απόκρυψης της ψηφιακής ταυτότητας των χρηστών με την χρήση εξειδικευμένων προγραμμάτων.

Στην ελληνική έννομη τάξη, ως υλικό πορνογραφίας ανηλίκων νοείται η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση, σε ηλεκτρονικό ή άλλο υλικό φορέα, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.

Σε βάρος των δραστών της συγκεκριμένης παραβατικής συμπεριφοράς στη Χώρα μας, τυγχάνουν εφαρμογής οι γενικές διατάξεις του Π.Κ., ήτοι τα άρθρα 337 «Προσβολή της γενετήσιας αξιοπρέπειας», 339 «Αποπλάνηση παιδιών», 342 «Κατάχρηση ανηλίκων σε ασέλγεια», 348Α «Πορνογραφία ανηλίκων», 348Β «Προσέλκυση παιδιών για γενετήσιους λόγους», 348Γ «Πορνογραφικές παραστάσεις ανηλίκων» και 351Α Π.Κ. «Ασέλγεια με ανήλικο έναντι αμοιβής» στα πλαίσια της αντιμετώπισης της εν γένει εγκληματικότητας.

### 1.5.8 Διαδικτυακή τρομοκρατία – Cyber terrorism

Είναι η χρήση των ηλεκτρονικών υπολογιστών και δικτύων για την πραγματοποίηση μίας τρομοκρατικής επίθεσης. Το FBI ορίζει «Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) «ως την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες». Η χρήση του διαδικτύου παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα:

- Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.

- Οι ενέργειες τους δύσκολα εντοπίζονται.

- Μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.

- Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρόντας την ανωνυμία του. Με τη χρήση λοιπόν του Διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων.

### 1.5.9 Επιθέσεις παρενόχλησης – Cyberbulling:

Ο όρος Cyberbullying είναι συνώνυμος του κυβερνό - εκφοβισμού ή της ηλεκτρονικής παρενόχλησης και αναφέρεται στην εσκεμμένη προσβολή, απειλή ή παρενόχληση άλλων με τη χρήση των σύγχρονων μέσων επικοινωνίας, συνήθως για μεγάλο διάστημα. Ο διαδικτυακός εκφοβισμός γίνεται είτε μέσω του Διαδικτύου (π.χ. E-Mail, instant messengers όπως ICQ, κοινωνικά δίκτυα, βίντεο, διαδικτυακές πύλες) ή μέσω του κινητού τηλεφώνου (π.χ. SMS ή ενοχλητικές κλήσεις). Συχνά, ο ένοχος είναι ανώνυμος έτσι ώστε το θύμα δεν γνωρίζει από που προέρχονται οι επιθέσεις. Ειδικά με παρενοχλήσεις μεταξύ παιδιών και εφήβων τα θύματα και οι δράστες συνήθως γνωρίζονται στον «πραγματικό» κόσμο». Τα θύματα έχουν σχεδόν πάντα μια ιδέα για το πρόσωπο που θα μπορούσε να είναι πίσω από τις επιθέσεις. Ο διαδικτυακός εκφοβισμός γίνεται συνήθως από ανθρώπους από το δικό τους περιβάλλον (το σχολείο, τη γειτονιά, το χωριό κλπ.). Περιπτώσεις στις οποίες αλλοδαποί ή ξένοι συμμετέχουν ομαδικά, δεν είναι ευρέως διαδεδομένες. (cyberhelp.eu)

## 1.6. Ψηφιακοί Εγκληματίες

Από την εμφάνιση κιόλας των ηλεκτρονικών υπολογιστών εμφανίστηκαν και οι πρώτοι επίδοξοι «ηλεκτρονικοί εγκληματίες», οι οποίοι προσπάθησαν με διάφορους τρόπους να εκμεταλλευτούν τις νέες τεχνολογίες προς όφελός τους. Εξάλλου η ταχύτατη εξέλιξή τους, προσέφερε διαρκώς νέες ευκαιρίες για εύκολη διάπραξη πλήθους εγκλημάτων. Ωστόσο, οι πρώτοι ηλεκτρονικοί υπολογιστές χρησιμοποιούσαν γλώσσα μηχανής, οπότε για τη διάπραξη των εγκλημάτων απαιτούνταν οι απαραίτητες γνώσεις αλλά και ο κατάλληλος εξοπλισμός. Ο ηλεκτρονικός υπολογιστής αποτελούσε είδος πολυτελείας και κατά συνέπεια το ηλεκτρονικό έγκλημα μπορούσε να διαπραχθεί από λίγους και ήταν περιορισμένο. (Βλαχόπουλος Κ, 2007).

Ο ψηφιακός εγκληματίας δραστηριοποιείται αποκλειστικά στον κυβερνοχώρο και χρησιμοποιεί αποκλειστικά και μόνο την ψηφιακή τεχνολογία για να παραβεί το νόμο. Είναι γνωστός τόσο στο ευρύ κοινό όσο και στη βιβλιογραφία αλλά και στα ΜΜΕ κυρίως ως Hacker αλλά και ως Cracker.

Ο Donn Parker (1998), ειδικός σε θέματα ασφάλειας Η/Υ υποστηρίζει για τους ψηφιακούς εγκληματίες τις ακόλουθες απόψεις:

- Οι άνθρωποι αυτοί διαφέρουν μεταξύ τους ανάλογα με τις δεξιότητες, τη γνώση, τους πόρους και τα κίνητρά τους.

- Οι ψηφιακοί εγκληματίες μπορούν να έχουν διαφορετικά επίπεδα ικανοτήτων που στηρίζονται στη βασική τους εκπαίδευση, τις κοινωνικές τους αλληλεπιδράσεις και στην εμπειρία τους στη χρήση των ηλεκτρονικών υπολογιστών.

- Υπάρχουν τρεις κατηγορίες ψηφιακών εγκληματιών:
    - οι κατασκευαστές εργαλείων
    - οι χρήστες εργαλείων και
    - οι συγγραφείς προγραμμάτων.

- Τα κίνητρά τους περιλαμβάνουν την πλεονεξία, την ανάγκη (για να λύσουν τα προσωπικά τους προβλήματα, όπως η πληρωμή χρεών από τυχερά παιχνίδια), την αδυναμία να κατανοήσουν τη ζημιά που προξενούν σε άλλους, την προσωποποίηση των υπολογιστών (τους θεωρούν ως αντιπάλους τους σε ένα παιχνίδι) και το σύνδρομο του Robin Hood (που τους κάνει να βλέπουν τις εταιρίες τόσο πλούσιες ώστε η οικονομικές ζημιές που τους προκαλούν να δικαιολογούνται ηθικά).

- Πολλοί από αυτούς θεωρούν ότι η απλή εισβολή σε συστήματα Η/Υ, ο βανδαλισμός τους ή η προφανής παραβίαση της εμπιστευτικότητάς τους είναι ένα αβλαβές και ηθικά αποδεκτό χόμπι.

- Μερικοί πάλι θεωρούν ότι η εισβολή σε συστήματα Η/Υ έχει και τη θετική της πλευρά με την έννοια ότι με τον τρόπο αυτό συμβάλλουν στη βελτίωση της ασφάλειάς τους.

- Οι περισσότεροι ενεργοί ψηφιακοί εγκληματίες είναι νέοι άνδρες, ηλικίας 12 έως 24 ετών.

- Πολλοί γονείς ανήλικων ψηφιακών εγκληματιών δεν έχουν καμία ιδέα για το τι κάνουν τα παιδιά τους με τον ακριβό εξοπλισμό υπολογιστών που τους έχουν κάνει δώρο

- Μερικοί υποστηρικτές των ψηφιακών εγκληματιών κατηγορούν τα θύματα τους για τα ανεπαρκή μέτρα ασφάλειας που έχουν λάβει και ελαχιστοποιούν τα ηθικά ζητήματα που τυχόν προκύπτουν.

- Μερικοί τέλος, υποστηρικτές των χάκερ περιγράφουν τις επιθέσεις τους ως δικαιολογημένες διαμαρτυρίες ή ως άμεση δράση ενάντια στους εχθρούς του περιβάλλοντος ή της κοινωνίας γενικά.

# Κεφάλαιο 2

# Οι επιθέσεις κατά πληροφοριακών συστημάτων

## 2.1 Εισαγωγή

Σύμφωνα με το άρθρο 2§α της Οδηγίας 2013/40/ΕΕ 3 , σύστημα πληροφοριών είναι «*η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους*».

Επιπλέον, σύμφωνα με το άρθρο 2§β της ως άνω Οδηγίας ορίζεται πως ηλεκτρονικά δεδομένα είναι «*η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο σύστημα να εκτελεί μια λειτουργία*».

## 2.2 Επιθέσεις κατά των συστημάτων πληροφοριών

Οι επιθέσεις κατά των συστημάτων πληροφοριών είναι οι αξιόποινες πράξεις που στρέφονται άμεσα κατά των ίδιων των συστημάτων πληροφοριών, ως αυτοτελών εννόμων αγαθών, θίγοντας κάποια από τις βασικές τους ιδιότητες, δηλαδή την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητά τους.

Οι πράξεις αυτές διακρίνονται με τη σειρά τους σειρά τους σε τρεις βασικές κατηγορίες:

- Στην πρώτη κατηγόρια ανήκουν ενέργειες μέσω των οποίων επιχειρείται παρέμβαση στο ίδιο το σύστημα πληροφοριών, όπως η παράνομη πρόσβαση σε αυτό, με την οποία προσβάλλεται η εμπιστευτικότητα του, η καταστροφή ή αδρανοποίηση της λειτουργίας ενός συστήματος πληροφοριών, μέσω της οποίας θίγεται η ακεραιότητα και η διαθεσιμότητα του συστήματος και ο παράνομος αποκλεισμός από το σύστημα πληροφοριών, οπού θίγεται και εδώ το έννομο αγαθό της διαθεσιμότητας.

- Στη δεύτερη κατηγορία ανήκουν πράξεις μέσω των οποίων προκαλείται παρέμβαση επάνω στις πληροφορίες ή διαφορετικά στα ηλεκτρονικά δεδομένα. Εδώ εντάσσονται ενέργειες όπως η καταστροφή ή αλλοίωση των δεδομένων που διακινούνται καθώς και η παράνομη αφαίρεση των δεδομένων.

- Σε μια τρίτη κατηγορία ανήκουν τέλος πράξεις προπαρασκευαστικές των επιθέσεων όπως η παραγωγή, η πώληση και η διανομή εργαλείων, ή προγραμμάτων η/υ μέσω των οποίων μπορούν να τελεστούν τα προαναφερόμενα αδικήματα.

### 2.2.1 Επιθέσεις άρνησης εξυπηρέτησης (Denial of Service-DoS)

Οι επιθέσεις άρνησης εξυπηρέτησης – DOS έχουν ως σκοπό την αδυναμία εξυπηρέτησης νόμιμων χρηστών. Ως τρόποι με τους οποίους μπορεί τεχνικά να επιτευχθεί αυτό είναι:

- Με πρόκληση διακοπής επικοινωνίας μεταξύ φυσικών συσκευών
- με εξάντληση των υπολογιστικών πόρων (εύρος δικτύου, αποθηκευτικός χώρος κτλ)

Παρακάτω παραθέτονται τα πιο διαδεδομένα είδη επιθέσεων DDos:

- “Smurf”
- “Fraggle”
- “Ping Flood”
- “Ping of Death”
- “LAND”
- “SYN Flood”
- “Teardrop”
- “Slow HTTP DoS”

### 2.2.2 Επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης (Distributed Denial of Service-DDoS)

Οι επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης (DDoS) έχουν την ίδια φιλοσοφία με τις επιθέσεις άρνησης εξυπηρέτησης (DoS), με τη διαφορά όμως ότι πραγματοποιούνται όχι από έναν μόνο επιτιθέμενο υπολογιστή, αλλά από πολλούς, οι οποίοι αποκαλούνται «υπολογιστές-ζόμπι» (zombie computers),και εντάσσονται σε ένα δίκτυο υπολογιστών που αποκαλείται «botnet». (Sérgio S.C. Silva, Rodrigo M.P. Silva, Raquel C.G. Pinto and Ronaldo M. Salles “Botnets: A survey”, Computer Networks 2013)

### 2.2.3 Άλλες επιθέσεις

**Επίθεση "Man-in-the-middle"**

Αυτή η μορφή επίθεσης υποκλέπτει δεδομένα σε συνεχή βάση για όσο διάστημα διαρκεί μια συγκεκριμένη επικοινωνία.

**Επίθεση "ARP spoofing" ή "ARP poisoning"**

Αυτή η μορφή επίθεσης περιλαμβάνει την αποστολή «ψεύτικων» μηνυμάτων ARP (Address Resolution Protocol) σε ένα τοπικό δίκτυο, προκαλώντας την ανακατεύθυνση των δεδομένων προς διαφορετικό μέρος από αυτό που θα έπρεπε κανονικά να βρεθούν.

**Επίθεση "Port Scan"**

Αυτή η μορφή επίθεσης έχει βασικό σκοπό να «ελέγχονται οι αδυναμίες ενός διακομιστή με την αποστολή «εξερευνητικών αιτημάτων».

### 2.2.4 Επιπτώσεις των επιθέσεων κατά των συστημάτων πληροφοριών

Η ασφάλεια και η αξιοπιστία των πληροφοριακών συστημάτων έχει καίρια σημασία, καθώς υπάρχει αλληλεξάρτηση με διάφορους τομείς της κοινωνίας, όπως παραδείγματος χάριν με την οικονομία, με τη διοίκηση, τη διακυβέρνηση, την υγεία, την παιδεία, και γενικά με όλους τους σημαντικούς τομείς κρατικών και κοινωνικών δραστηριοτήτων. Αντιλαμβανόμαστε ότι τα πληροφοριακά συστήματα αποτελούν κρίσιμες υποδομές ζωτικής σημασίας, οι οποίες χρήζουν προστασία.

Με βάση την Οδηγία 2008/114 ΕΚ της 08/12/08 «σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και σχετικά με την

αξιολόγηση της ανάγκης βελτίωσης προστασίας τους» ως Υποδομές Ζωτικής Σημασίας νοούνται «τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών». Παραδείγματος χάριν η ηλεκτροδότηση, η υδροδότηση, οι μεταφορές, ο τραπεζικός τομέας, οι υγειονομικές υπηρεσίες έκτακτης ανάγκης, τα σώματα ασφαλείας, το σύστημα διαχείρισης κυκλοφορίας, το χρηματιστήριο κ.α.

Οι κυβερνοεπιθέσεις επίσης μπορεί να αποσκοπούν, στην αφαίρεση δεδομένων, απόρρητων πληροφοριών και δικαιωμάτων σε χρήματα (τραπεζικός τομέας), στην εκβίαση για την πληρωμή λύτρων με την απειλή αχρήστευσης των συστημάτων πληροφοριών ή του περιεχομένου των δεδομένων τους, καθώς και στην καταστροφή συστημάτων και δεδομένων υπολογιστών, είτε για να διευκολυνθεί κάποιο έγκλημα (ή η απόκρυψη του) ή για λόγους τρομοκρατίας. Τέλος, στόχοι των επιθέσεων μπορεί να αποτελούν επιχειρήσεις ή βιομηχανίες με σκοπό την καταστροφή των συστημάτων τους και τη δυσφήμισή τους για λόγους ανταγωνισμού.

# Κεφάλαιο 3

# Μέθοδοι Αντιμετώπισης

## 3.1 Βασικές Έννοιες της Ασφάλειας

Κοινωνία της πληροφορίας ονομάζεται μία κοινωνία όπου η παραγωγή, διανομή, χρήση, ενσωμάτωση και διαχείριση πληροφοριών αποτελεί σημαντική οικονομική, πολιτική και πολιτιστική δραστηριότητα. Σκοπός μιας κοινωνίας της πληροφορίας είναι να κερδίσει ανταγωνιστικό πλεονέκτημα διεθνώς, δια μέσου της χρήσης της πληροφορικής (IT) με δημιουργικό και παραγωγικό τρόπο. Η οικονομία της γνώσης είναι η αντίστοιχη έννοια σε οικονομικό επίπεδο, σύμφωνα με την οποία ο πλούτος δημιουργείται μέσα από την οικονομική εκμετάλλευση της κατανόησης. Οι άνθρωποι που έχουν τα μέσα να συμμετέχουν σε αυτή τη μορφή κοινωνίας ορισμένες φορές ονομάζονται «ψηφιακοί πολίτες». Αυτή αποτελεί και μια από τις δεκάδες ετικέτες που υποδηλώνουν ότι οι σύγχρονοι άνθρωποι μπαίνουν σε μία νέα μορφή κοινωνίας (Beniger, James R. 1986)

Αντιλαμβανόμαστε πόσο σημαντική είναι σήμερα στη συνεχώς αναπτυσσόμενη Κοινωνία της Πληροφορίας, η πρόσβαση σε δεδομένα και πληροφορίες. Οι ποσότητες πληροφοριών-δεδομένων που καθημερινά μεταδίδονται, διαδίδονται και επεξεργάζονται είναι ανυπολόγιστες σε όγκο αλλά και σε αριθμό. Η πληροφορία αποτελεί ένα αυτόνομο αγαθό, και οι χρήστες της πληροφορίας είναι υπεύθυνοι για την πληρότητά της (completeness) και τη ακρίβεια (accuracy).

**Ιδιότητες των πληροφοριών:**

- **Ακεραιότητα (integrity):** η προστασία των δεδομένων από μη εξουσιοδοτημένη τροποποίηση, συμπτωματική ή συνειδητή

- **Εμπιστευτικότητα (confidentiality):** η απόκρυψη δεδομένων από μη εξουσιοδοτημένη ανάγνωση
- **Αυθεντικότητα (authenticity):** κάθε χρήστης ή διασυνδεδεμένη συσκευή αναγνωρίζεται μοναδικά για τις διεργασίες που εκτελεί και τα δεδομένα που χρησιμοποιεί
- **Διαθεσιμότητα (availability):** η πλήρης και σωστή εξυπηρέτηση χρηστών και εφαρμογών για το μεγαλύτερο δυνατό χρονικό διάστημα

## 3.2 Μηχανισμοί Ασφάλειας

### 3.2.1 Λογισμικό Ασφάλειας – Antivirus

Ιδανική λύση για την απειλή των ιών είναι η αποτροπή. Δεν πρέπει εξαρχής να επιτραπεί στον ιό η είσοδος μέσα στο σύστημα. Αυτός ο στόχος είναι γενικά αδύνατον να επιτευχτεί αν και η αποτροπή μπορεί να μειώσει τον αριθμό των επιτυχημένων επιθέσεων από ιούς. Η καλύτερη προσέγγιση είναι:

- Ανίχνευση – αφού συμβεί η μόλυνση διαπιστώνεται ότι έχει συμβεί μόλυνση και εντοπίζεται ο ιός
- Αναγνώριση – αφού έχει επιτευχθεί η ανίχνευση, αναγνωρίζεται ο συγκεκριμένος ιός που έχει προσβάλει το πρόγραμμα
- Κατάργηση – αφού έχει αναγνωριστεί ο συγκεκριμένος ιός, αφαιρούνται όλα τα ίχνη του ιού από το μολυσμένο πρόγραμμα και έτσι αυτό επανέρχεται στην κανονική του κατάσταση. Καταργείται ο ιός από όλα τα μολυσμένα συστήματα έτσι ώστε να μην μπορεί να διαδοθεί περαιτέρω η μόλυνση (Stallings W, 2008).

### 3.2.2 Firewalls

Η αντιπυρική ζώνη είναι ένα φράγμα μέσα από το οποίο πρέπει να περάσει όλη η δικτυακή κυκλοφορία και προς τις δυο κατευθύνσεις. Η πολιτική που εφαρμόζεται στην αντιπυρική ζώνη ορίζει ποια κίνηση μπορεί να περνάει από αυτή προς την κάθε κατεύθυνση. Μπορεί να λειτουργεί ως φίλτρο σε επίπεδο πακέτων IP ή να λειτουργεί σε πρωτόκολλο ανωτέρου επιπέδου. Έμπιστο σύστημα είναι ο υπολογιστής και το λειτουργικό σύστημα που μπορεί να πιστοποιηθεί ότι εφαρμόζει μία συγκεκριμένη πολιτική ασφάλειας. Το έμπιστο σύστημα συνήθως ασχολείται με τον έλεγχο πρόσβασης. Η πολιτική που εφαρμόζεται ορίζει ποιοι θα έχουν πρόσβαση και σε ποιά αντικείμενα. Τα συνηθισμένα κριτήρια αξιολόγησης για την ασφάλεια της τεχνολογίας πληροφορικής είναι μία διεθνής πρωτοβουλία προτυποποίησης με στόχο τον ορισμό ενός κοινού συνόλου απαιτήσεων ασφάλειας, αλλά και ενός συστηματικού τρόπου για την αξιολόγηση προϊόντων με βάση αυτά τα κριτήρια. Οι αντιπυρικές ζώνες μπορούν να είναι ένα αποτελεσματικό μέσο προστασίας ενός τοπικού συστήματος από διαδικτυακές απειλές, ενώ ταυτόχρονα επιτρέπουν την πρόσβαση στον έξω κόσμο μέσω δικτύων ευρείας περιοχής και του Διαδικτύου (Stallings W, 2008).

### 3.2.3 Πιστοποίηση χρήστη

Η δημιουργία και η χρήση συνθηματικών λέξεων ή συμβόλων αποτελεί την πιο συνηθισμένη τεχνική πιστοποίησης ταυτότητας χρήστη. Για να επιτραπεί η είσοδος ενός πιστοποιημένου χρήστη σε ένα πληροφοριακό σύστημα, είναι απαραίτητη η χρήση ενός «ονόματος χρήστη – username» και ο «κωδικός πρόσβασης – password». Η χρήση τους εξασφαλίζει μεγάλη ασφάλεια και αποτελεί την πιο συνηθισμένη τεχνική.

### 3.2.4 Κρυπτογραφία και Ασφάλεια

Η κρυπτογράφηση είναι με διαφορά το σημαντικότερο αυτοματοποιημένο εργαλείο για την ασφάλεια δικτύων και επικοινωνιών. Χρησιμοποιούνται κατά κύριο λόγο δύο μορφές κρυπτογράφησης: η συμβατική ή συμμετρική κρυπτογράφηση και η κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρη κρυπτογράφηση. Η ασφάλεια της συμμετρικής κρυπτογράφησης βασίζεται στη μυστικότητα του κλειδιού και όχι στη μυστικότητα του αλγόριθμου που χρησιμοποιείται. Άρα δε χρειάζεται να κρατάμε μυστικό τον αλγόριθμο κρυπτογράφησης αλλά θα πρέπει να μένει μυστικό μόνο το κλειδί. Η ασύμμετρη κρυπτογράφηση περιλαμβάνει τη χρήση δύο ξεχωριστών κλειδιών, ένα δημόσιο που κοινοποιείται ώστε να χρησιμοποιείται από τους άλλους και ένα ιδιωτικό που είναι γνωστό μόνο στον ιδιοκτήτη του. Ένας γενικός αλγόριθμος δημοσίου κλειδιού βασίζεται σε ένα κλειδί για την κρυπτογράφηση και σε ένα διαφορετικό αλλά συσχετιζόμενο κλειδί για την αποκρυπτογράφηση. Το κλειδί που χρησιμοποιείται στη συμβατική κρυπτογράφηση αναφέρεται συνήθως ως μυστικό κλειδί ενώ τα δύο κλειδιά που χρησιμοποιούνται στην ασύμμετρη κρυπτογράφηση αναφέρονται ως δημόσιο και ιδιωτικό. (Stallings W, 2008).

# Κεφάλαιο 4

# Νομικό Πλαίσιο Ηλεκτρονικού Εγκλήματος

## 4.1 Νομική Προσέγγιση

Με την παγκοσμιοποίηση και την ολοένα αυξανόμενη χρήση των ηλεκτρονικών υπολογιστών αλλά και του διαδικτύου, καθώς τα οφέλη που αποκομίζουν οι χρήστες είναι αναρίθμητα και οι δυνατότητες που προσφέρονται τεράστιες, ελλοχεύει τον κίνδυνος της κακόβουλης χρήσης αλλά και της κατάχρησης, όσον αφορά το διαδίκτυο και την ηλεκτρονική επεξεργασία δεδομένων και πληροφοριών.

Λόγω της ραγδαίας εξέλιξης της τεχνολογίας, το ηλεκτρονικό & διαδικτυακό έγκλημα αποτελεί ένα νέο αντικείμενο που λαμβάνει συνεχώς νέες μορφές, απειλώντας από απλούς χρήστες του διαδικτύου μέχρι πολυεθνικές εταιρίες, κρατικές υπηρεσίες κτλ. Για την καταπολέμηση της αυξανόμενης εγκληματικότητας στον κυβερνοχώρο είναι απαραίτητη η συνεργασία σε επίπεδο κρατών, ώστε να υπάρξει αποτελεσματική αντιμετώπισή του. Επίσης είναι απαραίτητος ο συνδυασμός νομικών και των τεχνικών γνώσεων για την κατανόησή του και την αντιμετώπισή του. Η τεχνολογία προχωρά πολύ πιο γρήγορα από τη νομοθεσία, οπότε απαιτείται η συνεχής ενημέρωση βασιζόμενη στις εκάστοτε τεχνολογικές εξελίξεις.

Οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν αδυναμίες τόσο στην Ελλάδα όσο και σε άλλες χώρες. Η ιδιαίτερη φύση των ψηφιακών εγκλημάτων υποχρεώνει τον νομοθέτη να ενημερώνεται συνεχώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να κατορθώσει να εξοικειωθεί με τον τρόπο διάπραξης των σχετικών αξιόποινων πράξεων, καθώς οι νομικές γνώσεις μόνο δεν είναι αρκετές. Είναι γεγονός εξάλλου ότι η ψηφιακή εγκληματικότητα αποτελεί μια δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα

να παρουσιάζονται σοβαρές δυσχέρειες στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. (Τσουραμάνης Χρ. 2005)

## 4.2 Διαδίκτυο και Ποινική Νομοθεσία

Το νομοθετικό πλαίσιο γύρω από το Ηλεκτρονικό Έγκλημα παραμένει μέχρι σήμερα ένα πολύπλοκο και αμφιλεγόμενο θέμα, τόσο σε διεθνές όσο και σε εθνικό επίπεδο, καθώς ένα από τα σημαντικά προβλήματα που προκύπτουν στην αντιμετώπιση του είναι η δυσκολία οριοθέτησης των πράξεων που θα πρέπει να διώκονται ποινικά, όπως επίσης και η αδυναμία της συνεχούς παρακολούθησης των εξελίξεων στον τομέα της τεχνολογίας και της πληροφορικής ώστε να υπάρχει πολλή καλή γνώση και εξειδίκευση αναφορικά με τη φύση των εγκλημάτων, των μέσων που χρησιμοποιούνται και τον τρόπο με τον οποίο τελούνται τα αδικήματα αυτά. Επίσης, εξίσου βασικό πρόβλημα αποτελεί το γεγονός ότι το ηλεκτρονικό έγκλημα έχει παγκόσμιο χαρακτήρα και όχι συγκεκριμένο γεωγραφικό χώρο, λόγω του διασυνοριακού – διεθνοποιημένου χαρακτήρα του. Εν αντιθέσει με το συμβατικό έγκλημα, το οποίο μπορεί να οριοθετηθεί χωρο-χρονικά, το ηλεκτρονικό έγκλημα μπορεί να τελεσθεί σε μία χώρα, ενώ οι συνέπειές του να είναι ολέθριες για μία άλλη. Συχνά οι διωκτικές αρχές δυσκολεύονται να δράσουν καθώς δε μπορούν να εντοπίσουν εύκολα ή και καθόλου τη χώρα τέλεσης του ηλεκτρονικού εγκλήματος και λόγω της «ευχέρειας τέλεσης», δηλαδή ότι μπορεί να πραγματοποιηθεί από τον καθένα και να πλήξει τον καθένα, δυσκολεύει το έργο τους.

### Δίκαιο

Το δίκαιο αποτελούν οι κανόνες και οι αρχές που ρυθμίζουν σε συγκεκριμένο χώρο και χρόνο, με τρόπο υποχρεωτικό, εξαναγκαστικό και ετερόνομο τη συμπεριφορά των ανθρώπων που συναποτελούν τα μέλη μιας κοινωνίας.

Χαρακτηριστικά του με την έννοια αυτή είναι:

- ο κανονιστικός χαρακτήρας του δικαίου, αφού οι κανόνες του αναφέρονται στο δέον, σε αυτό που πρέπει να γίνεται και όχι στο ον, σε αυτό δηλαδή που υπάρχει,

- ο ρυθμιστικός χαρακτήρας του δικαίου, το οποίο αποβλέπει στη ρύθμιση της συμβίωσης μεταξύ των μελών μιας κοινωνίας,

- ο υποχρεωτικός και εξαναγκαστικός χαρακτήρας του δικαίου, το οποίο απαιτεί τη συμμόρφωση μεταξύ των μελών μιας κοινωνίας μέσω της απειλής κυρώσεων για τη μη εφαρμογή των κανόνων δικαίου που προβλέπει,

- ο ετερόνομος χαρακτήρας του που συνίσταται στο ότι δεν προέρχεται ή πηγάζει από την ιδιωτική αυτονομία ή την αυτοδέσμευση των ιδιωτών αλλά από το κράτος ή την κοινωνία. Το δίκαιο, χαρακτηρίζεται ως θετό, είναι ισχύον και η νομική του ισχύς εξαρτάται από την τυπική και ουσιαστική ισχύ του. Έτσι, η τυπική ισχύς των νόμων εκκινεί από τη δημοσίευσή τους στο Φύλλο της Εφημερίδας της Κυβερνήσεως, ενώ η ουσιαστική ισχύ τους εκκινεί δέκα ημέρες μετά. Η πραγματική ισχύς του δικαίου εξαρτάται από την πρακτική εφαρμογή και αποτελεσματικότητά του, χωρίς η ανυπαρξία της να επιδρά στην τυπική ισχύ του. Το θετό δίκαιο διακρίνεται από το φυσικό δίκαιο, για το οποίο η πρώτη αναφορά γίνεται στην τραγωδία του Σοφοκλή, Αντιγόνη. Το φυσικό δίκαιο περιέχει κανόνες δικαίου που υφίστανται ανεξάρτητα, πριν και πέρα από το θετικό δίκαιο, χαρακτηρίζονται υπερθετικοί κανόνες δικαίου και αποτυπώνουν γενικές, διαχρονικές και πανανθρώπινες αξίες και ιδέες και κυρίως την έννοια της δικαιοσύνης. Στην ιστορία του δικαίου, το φυσικό δίκαιο επανήλθε στη σύγχρονη περί δικαίου συζήτηση αρχικά τον 19ο αιώνα μέσα από την ανάπτυξη του κινήματος του ιδεαλισμού και υποχώρησε μέσα από την επικράτηση του νομικού θετικισμού, ενός ρεύματος που δέχεται την ύπαρξη αποκλειστικά και μόνο του τυπικού, ισχύοντος, θετού δικαίου (Zippelious, 2008). Ωστόσο, η θεωρία του φυσικού δικαίου, παρά το γεγονός ότι δεν υποστηρίζεται καθεαυτή έχει ασκήσει

πολύ θετική επιρροή στην ανάπτυξη της διεθνούς προστασίας των ανθρωπίνων δικαιωμάτων αλλά και στην ανάδειξη της σημασίας των γενικών αρχών για τη λειτουργία και την δυναμική και εξελικτική ερμηνεία του δικαίου (Σούρλας, 1995).

## Η εξέλιξη του δικαίου

Το νομικό πλαίσιο και η εξέλιξη των σχετικών κανόνων χαρακτηρίζεται από τέσσερα στάδια:

- Προστασία προσωπικότητας – ιδιωτικότητας – προσωπικών δεδομένων. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών
- Καταστολή οικονομικού ηλεκτρονικού εγκλήματος
- Προστασία πνευματικής ιδιοκτησίας
- Παράνομο και αθέμιτο περιεχόμενο όπως το αδίκημα της παιδικής πορνογραφίας

Για να στοιχειοθετηθεί ένα ηλεκτρονικό έγκλημα, το οποίο είναι μία αρκετά περίπλοκη διαδικασία, οι αρμόδιες διωκτικές αρχές θα πρέπει να να διερευνήσουν την εγκληματική συμπεριφορά και τα αρμόδια δικαστήρια να δικάσουν την εν λόγω υπόθεση.

Απαραίτητη προϋπόθεση είναι η συλλογή των στοιχείων που παραθέτουμε παρακάτω:

- Αντικειμενική υπόσταση: περιγραφή πράξης/παράλειψης η οποία συνιστά ποινικά κολάσιμη συμπεριφορά
- Χρόνος τέλεσης
- Τόπος τέλεσης

- Ο τόπος που ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη πράξη ή παράλειψη
- Ο τόπος που επήλθε ή έπρεπε σύμφωνα με την πρόθεση του υπαιτίου να επέλθει το αξιόποινο αποτέλεσμα

- Εμπλεκόμενα πρόσωπα (προσδιορισμός παραβάτη και θύματος)
- Θεωρία του βαρύνοντος τόπου: το κράτος στο οποίο εκδηλώθηκε το έγκλημα κατά την κύρια σημασία του.

## 4.3 Νομική Αντιμετώπιση – Ευρωπαϊκό Δίκαιο

Στην Ευρωπαϊκή Ένωση έχουν πραγματοποιηθεί μεγάλες προσπάθειες για την αντιμετώπιση των ηλεκτρονικών και διαδικτυακών εγκλημάτων. Ενδεικτικά παρακάτω είναι οι σημαντικότερες ενέργειες για την καταπολέμησή τους:

Ενδεικτικές ενέργειες των δράσεων της Ευρωπαϊκής Ένωσης για την καταπολέμηση του ηλεκτρονικού/διαδικτυακού εγκλήματος είναι οι παρακάτω:

- Η απόφαση πλαίσιο 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας, που αφορούν τα μέσα πληρωμής πλην των μετρητών

(http://eur-lex.europa.eu/legal-ontent/EL/TXT/PDF/?uri=CELEX:32001F0413&from=EL)

- Η οδηγία 2011/93/ΕΕ 10 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011 σχετικά με την καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και την αντικατάσταση της απόφασης-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου

(http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32011L0093)

- Η οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου, της 25ης Νοεμβρίου 2009, για την τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Επίσημη Εφημερίδα Ευρωπαϊκής Ένωσης-18.12.2009)

- Η οδηγία 2002/58/ΕΚ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (Επίσημη Εφημερίδα Ευρωπαϊκής Ένωσης-31.07.2002)

Επιπλέον

- Η Σύμβαση της Βουδαπέστης στις 23.11.2001 για «μία ασφαλέστερη κοινωνία της πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος της πληροφορικής».

- Πρόσθετο Πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον κυβερνοχώρο»

- Η Επιτροπή των Ευρωπαϊκών Κοινοτήτων το 2001 εξέδωσε την ανακοίνωση «για μια ασφαλέστερη κοινωνία της πληροφορίας με τη βελτίωση της ασφάλειας

των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής»

- Η Απόφαση-Πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της 24ης Φεβρουαρίου 2005 για τις επιθέσεις κατά των συστημάτων πληροφοριών (Βρυξέλλες, 2005). στο προοίμιο της ανωτέρω Απόφασης-Πλαισίου την εξής φράση : «*Ο στόχος της παρούσας απόφασης-πλαίσιο είναι η βελτίωση της συνεργασίας μεταξύ των δικαστικών και άλλων αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, μέσω της προσέγγισης των κανόνων του ποινικού δικαίου των κρατών μελών που αφορούν επιθέσεις κατά συστημάτων πληροφοριών*».

- Η υπ' αριθ. 2013/40/ΕΕ Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της ως άνω απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, στοχεύοντας στην εναρμόνιση της ποινικής νομοθεσίας των κρατών-μελών της Ευρωπαϊκής Ένωσης σε θέματα επιθέσεων κατά συστημάτων πληροφοριών, με τη θέσπιση ελάχιστων κανόνων για τον ορισμό των ποινικών αδικημάτων και των σχετικά προβλεπόμενων κυρώσεων, τη βελτίωση της συνεργασίας των αρμόδιων αρχών των κρατών-μελών, συμπεριλαμβανομένων των αστυνομικών ή άλλων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου, καθώς και των αρμόδιων ειδικευμένων οργανισμών και φορέων της Ευρωπαϊκής Ένωσης.

### 4.3.1 Συστάσεις του Συμβουλίου της Ευρώπης

Το Συμβούλιο της Ευρώπης, με δεδομένη τη ραγδαία εξέλιξη της πληροφορικής επιστήμης καθώς και την εμφάνιση νέων μορφών αδικημάτων που αυτή προκάλεσε, επιχείρησε να αντιμετωπίσει τα προβλήματα που εμφανίστηκαν. Αρχικά προχώρησε με

μία ουσιαστική προσέγγιση ως προς τη νομική αντιμετώπιση του ηλεκτρονικού εγκλήματος εκδίδοντας συστάσεις – recommendations για τα κράτη-μέλη, χωρίς όμως δεσμευτική ισχύ μεν, αλλά υποδεικνύοντας δε μία συγκεκριμένη γραμμή ως προς την αντιμετώπιση των εν λόγω εγκλημάτων.

1. **Σύσταση της Επιτροπής Υπουργών No. R (85) 10** σχετικά με την πρακτική εφαρμογή της Ευρωπαϊκής Σύμβασης για την αμοιβαία συνδρομή σε ποινικές υποθέσεις όσον αφορά τις αιτήσεις δικαστικής συνδρομής για την άρση απορρήτου τηλεπικοινωνιών – "*Recommendation No. R (85) 10 of the Committee of Ministers to Members States concerning the practical application of the European Convention on mutual assistance in criminal matters in respect of letters rogatory for the interception of telecommunications. (Adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers' Deputies)".*

2. **Σύσταση της Επιτροπής Υπουργών No. R (88) 2** σχετικά με την πειρατεία στον τομέα των πνευματικών και συγγενικών δικαιωμάτων – "*Recommendation No. R (88) 2 of the Committee of Ministers to Members States on measures to combat piracy in the field of copyright and neighbouring rights (Adopted by the Committee of Ministers on 18 January 1988 at the 414th meeting of the Ministers' Deputies)".*

3. **Σύσταση της Επιτροπής Υπουργών No. R (87) 15** που ρυθμίζει την χρήση προσωπικών δεδομένων στον αστυνομικό τομέα – *"Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies)*

4. **Σύσταση της Επιτροπής Υπουργών No. R (89) 9** σχετικά με έγκλημα που σχετίζεται με ηλεκτρονικούς υπολογιστές όπου υπάρχουν οδηγίες για τις εθνικές νομοθεσίες σχετικά με τους ορισμούς ορισμένων εγκλημάτων σχετιζόμενων με υπολογιστές - *"Recommendation No. R (89) 9 of the Committee of Ministers to member states on computer-related crime (Adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies)*

   Στη Σύσταση αυτή αναγνωρίζεται η ανάγκη ύπαρξης ενός επαρκούς και γρήγορου μηχανισμού αντιμετώπισης του ηλεκτρονικού εγκλήματος, στη διασυνοριακή φύση τους και στην επιτακτική ανάγκη εναρμόνισης των εθνικών νομοθεσιών στο τομέα αυτό, καθώς και στη βελτίωση της διεθνούς νομικής συνεργασίας. Δημιουργήθηκε επίσης κατάλογος αξιόποινων εγκληματικών συμπεριφορών που πρέπει να ποινικοποιηθούν, όπως ηλεκτρονική απάτη και πλαστογραφία, φθορά σε δεδομένα και προγράμματα υπολογιστή, σαμποτάζ σε ηλεκτρονικό υπολογιστή, μη εξουσιοδοτημένη πρόσβαση και υποκλοπή, καθώς και μη εξουσιοδοτημένη αναπαραγωγή λογισμικού η/υ.

5. **Σύσταση της Επιτροπής Υπουργών No. R (95) 13** που αφορά προβλήματα της ποινικής δικονομίας σε σχέση με την τεχνολογία της πληροφορικής - *"Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology* (*Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies)*

   Στη Σύσταση αυτή καθιερώνονται σε διεθνές κείμενο οι γενικές δικονομικές αρχές που θα πρέπει να ισχύουν κατά την έρευνα των εγκλημάτων στο χώρο της τεχνολογίας των πληροφοριών. Στις αρχές αυτές περιλαμβάνονται η έρευνα και η κατάσχεση, η κρυπτογράφηση, η διερεύνηση, η τήρηση στατιστικών στοιχείων, η

εκπαίδευση και η διεθνής συνεργασία. Τα ζητήματα αυτά καλύπτουν τις περιπτώσεις της ποινικής έρευνας τόσο των κυβερνοεγκλημάτων όσο και των εγκλημάτων του κοινού ποινικού δικαίου, των οποίων τα αποδεικτικά στοιχεία μπορεί να βρεθούν ή να μεταδοθούν σε ηλεκτρονική μορφή.

6. **Σύσταση της Επιτροπής Υπουργών No. R (95) 4** σχετικά με την προστασία των προσωπικών δεδομένων στον τομέα των τηλεπικοινωνιακών υπηρεσιών, με ιδιαίτερη αναφορά στις τηλεφωνικές υπηρεσίες

## 3.3.2 Η Σύμβαση της Βουδαπέστης

Οι παραπάνω συστάσεις όμως του Συμβουλίου της Ευρώπης, έχοντας μη δεσμευτική ισχύ αλλά μόνο συμβουλευτική, δεν είχαν τα αναμενόμενα δραστικά αποτελέσματα, και ως εκ τούτου αναγνωρίστηκε η ανάγκη για διεθνή συνεργασία στον ποινικό τομέα, ανάγκη για μία αντεγκληματική πολιτική για την προστασία της κοινωνίας από το έγκλημα στον κυβερνοχώρο και την υιοθέτηση αποτελεσματικότερων μέτρων.

Έτσι, στις 23 Νοεμβρίου 2001, υπογράφηκε στη Βουδαπέστη από 26 χώρες κράτη – μέλη του Συμβουλίου της Ευρώπης (Αλβανία, Αρμενία, Αυστρία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρος, Εσθονία, Φιλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιταλία, Μολδαβία, Ολλανδία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Ισπανία, Σουηδία, Ελβετία, πρώην Γιουγκοσλαβική Δημοκρατία της Μακεδονίας, Ουκρανία, Ηνωμένο Βασίλειο) και από 4 χώρες – παρατηρητές (Καναδάς, Ιαπωνία, Νότιος Αφρική και ΗΠΑ) διεθνής σύμβαση με αντικείμενο την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η εν λόγω σύμβαση έχει τεθεί σε εφαρμογή, καθώς έχει κυρωθεί από 5 μέλη, τρία εκ των οποίων είναι μέλη του Συμβουλίου της Ευρώπης (άρθρο 36). Τα κράτη – μέλη αναλαμβάνουν την υποχρέωση της συμμόρφωσής τους με τις διατάξεις της. Και τούτο πραγματώνεται με την εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των κρατών-μελών στον τομέα της εγκληματικότητας στον κυβερνοχώρο, με τη θέσπιση

εσωτερικών δικονομικών διατάξεων για την έρευνα, τη δίωξη και την εκδίκαση των εγκλημάτων του κυβερνοχώρου, καθώς και τη θέσπιση κανόνων αναφορικά με τη διεθνή συνεργασία. (Αγγελή Ι)

Επομένως, σκοπός της Σύμβασης είναι η προστασία της διεθνούς κοινότητας αναφορικά με την εγκληματικότητα που εκδηλώνεται στο διαδίκτυο μέσω της θεμελίωσης κοινών ουσιαστικών και δικονομικών ποινικών αρχών, της θέσπισης της κατάλληλης νομοθεσίας από τα κράτη μέλη, καθώς και μέσω της επίτευξης της ανάλογης δικαστικής συνεργασίας μεταξύ των κρατών μελών.

**Σκοπός της Σύμβασης**

- Η εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των κρατών μελών στο τομέα της εγκληματικότητας στον κυβερνοχώρο.
- Η θέσπιση εσωτερικών ποινικών διατάξεων
- Η θέσπιση γρήγορων και αποτελεσματικών κανόνων στον τομέα της διεθνούς συνεργασίας.

**Η Σύμβαση περιλαμβάνει:**

- **Διατάξεις ουσιαστικού ποινικού δικαίου**

1. Διατάξεις για τη διαφύλαξη των αποθηκευμένων δεδομένων σε έναν υπολογιστή
2. Διατάξεις για τη διαφύλαξη και γνωστοποίηση των μεταδιδόμενων δεδομένων
3. Διατάξεις για την παροχή πληροφοριών
4. Διατάξεις έρευνας και κατάσχεσης αποθηκευμένων στοιχείων
5. Διατάξεις σχετικά με την πραγματικού χρόνου συλλογή διακινουμένων δεδομένων

6. Διατάξεις σχετικά με την παρακολούθηση – υποκλοπή του περιεχομένου δεδομένων

- **Διατάξεις ποινικού δικονομικού δικαίου**

1. Διατάξεις για τη διαφύλαξη των αποθηκευμένων δεδομένων σε έναν υπολογιστή
2. Διατάξεις για τη διαφύλαξη και γνωστοποίηση των μεταδιδόμενων δεδομένων
3. Διατάξεις για την παροχή πληροφοριών
4. Διατάξεις έρευνας και κατάσχεσης αποθηκευμένων στοιχείων
5. Διατάξεις σχετικά με την πραγματικού χρόνου συλλογή διακινουμένων δεδομένων
6. Διατάξεις σχετικά με την παρακολούθηση – υποκλοπή του περιεχομένου δεδομένων

- **Διατάξεις διεθνούς δικαστικής συνεργασίας**

1. Διατάξεις για την έκδοση καταζητούμενων
2. Γενικές αρχές σχετικές με την αμοιβαία συνδρομή
3. Διατάξεις αυτεπάγγελτης πληροφόρησης
4. Διατάξεις σχετικά με την δημοσιοποίηση αποθηκευμένων δεδομένων σε ένα υπολογιστικό σύστημα
5. Διατάξεις σχετικά με τη γνωστοποίηση των δεδομένων κίνησης

Η σύμβαση περιέχει ρυθμίσεις για τη συνέργεια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. (Ε.Μήτρου 2012)

### 4.3.3 Πρόσθετο Πρωτόκολλο της Σύμβασης του Συμβουλίου της Ευρώπης για το Έγκλημα στον Κυβερνοχώρο σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσεως

Στο Στρασβούργο, στις 28.1.2003 υπογράφηκε Πρόσθετο Πρωτόκολλο σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών.

Ο ορισμός του ρατσιστικού και ξενοφοβικού υλικού παρατίθεται στο άρθρο 2 του Πρόσθετου Πρωτοκόλλου:

*«**Ρατσιστικό και ξενοφοβικό υλικό**: κάθε γραπτό υλικό, εικόνα ή οποιαδήποτε άλλη εκπροσώπηση των ιδεών ή θεωριών, που υποστηρίζει, προωθεί ή εξωθεί μίσος, διακρίσεις ή βία, κατά οποιουδήποτε ατόμου ή ομάδας ατόμων, με βάση τη φυλή, το χρώμα, την καταγωγή ή εθνική ή εθνοτική καταγωγή, τη θρησκεία, καθώς και αν χρησιμοποιείται ως πρόσχημα για οποιονδήποτε από αυτούς τους παράγοντες" (Άρθρο 2 – Ορισμός).»*

Ο σκοπός του Προσθέτου Πρωτοκόλλου:

Σύμφωνα με το άρθρο 1 του Κεφαλαίου Ι, είναι τα Συμβαλλόμενα στο Πρόσθετο Πρωτόκολλο Μέρη να συμπληρώσουν - διευρύνουν τις διατάξεις της Σύμβασης της Βουδαπέστης όσον αφορά την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, οι οποίες διαπράττονται μέσω συστημάτων υπολογιστών. Το διαδίκτυο, αποτελώντας ένα ισχυρό μέσο παγκόσμιας επικοινωνίας, μπορεί εύκολα να αποτελέσει τον χώρο όπου μεμονωμένα άτομα ή ομάδες ατόμων θα εκφράσουν ρατσιστικές ή ξενοφοβικές ιδέες, προωθώντας μέσω αυτού αντίστοιχο υλικό,το οποίο μπορεί να παροτρύνει ή να παρακινεί άλλους στη διάπραξη ρατσιστικών ή ξενοφοβικής φύσης ενεργειών.

Στο Κεφάλαιο ΙΙ στα άρθρα 3 έως 7 γίνεται αναφορά στις τιμωρητέες πράξεις καθώς και στα μέτρα που πρέπει να ληφθούν από τα Συμβαλλόμενα Μέρη, όταν οι πράξεις αυτές διαπράττονται από πρόθεση και χωρίς δικαίωμα. Ειδικότερα, στο άρθρο 3 ποινικοποιείται η διανομή και η διάθεση γενικότερα ρατσιστικού και ξενοφοβικού υλικού μέσω συστήματος υπολογιστή.

Στα άρθρα 4 και 5 τιμωρούνται αντίστοιχα η απειλή και η προσβολή, μέσω συστήματος υπολογιστή, οι οποίες έχουν ρατσιστικό ή ξενοφοβικό περιεχόμενο.

Στο άρθρο 6 τιμωρείται η διανομή ή γενικότερα η διάθεση, μέσω συστήματος υπολογιστή, υλικού που αρνείται, υποβαθμίζει τη σημασία, εγκρίνει ή δικαιολογεί γενοκτονία ή εγκλήματα κατά της ανθρωπότητας.

Στο άρθρο 7 τιμωρείται η συνέργεια και η ηθική αυτουργία στα προαναφερθέντα στα άρθρα 3-6 αδικήματα.

Στο Κεφάλαιο ΙΙΙ ρυθμίζεται η σχέση του Πρόσθετου Πρωτοκόλλου με τη Σύμβαση της Βουδαπέστης.

Τέλος, στο Κεφάλαιο IV ρυθμίζονται θέματα όπως η έναρξη ισχύος του Πρόσθετου Πρωτοκόλλου (άρθρο 10), η προσχώρηση (άρθρο 11), η διατύπωση επιφυλάξεων και η ανάκληση αυτών (άρθρα 12, 13), η εδαφική εφαρμογή (άρθρο 14), η καταγγελία (άρθρο 15) και η κοινοποίηση (άρθρο 16).

(https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/prostheto-protokollo-tis-symvasis-gia-egklima-ston )

### 4.3.4 Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

Η οδηγία της ΕΕ για το έγκλημα στον κυβερνοχώρο αποσκοπεί στην καταπολέμηση του ηλεκτρονικού εγκλήματος και την προώθηση της ασφάλειας των πληροφοριών μέσω ισχυρότερων εθνικών νόμων, αυστηρότερων ποινικών κυρώσεων και περισσότερης συνεργασίας μεταξύ των αρμόδιων αρχών.

ΠΡΑΞΗ

Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.

ΣΥΝΟΨΗ

Η παρούσα οδηγία προβλέπει νέους κανόνες που εναρμονίζουν την ποινικοποίηση και τις ποινές για σειρά αδικημάτων που στρέφονται κατά των συστημάτων πληροφοριών. Οι κανόνες αυτοί περιλαμβάνουν την απαγόρευση χρήσης των αποκαλούμενων«botnets» -κακόβουλου λογισμικού που έχει σχεδιαστεί για να αποκτά εξ αποστάσεως τον έλεγχο ενός δικτύου υπολογιστών. Καλεί, επίσης, τις χώρες της ΕΕ να χρησιμοποιούν τα ίδια σημεία επαφής που χρησιμοποιούνται από το Συμβούλιο της Ευρώπης και τους G8 προκειμένου να αντιδρούν γρήγορα στις απειλές που συνδέονται με προηγμένη τεχνολογία.

Τα κύρια είδη ποινικών αδικημάτων που καλύπτονται από την παρούσα οδηγία είναι οι επιθέσεις κατά των συστημάτων πληροφοριών, που περιλαμβάνουν επιθέσεις άρνησης υπηρεσιών με σκοπό να τεθεί εκτός λειτουργίας ένας εξυπηρετητής, αλλά και υποκλοπή δεδομένων και επιθέσεις«botnet».

Το έγκλημα στον κυβερνοχώρο πρέπει να καταπολεμηθεί αποτελεσματικά, όχι μόνο εντός ενός δεδομένου κράτους μέλους αλλά και στο σύνολο των κρατών μελών. Τούτο απαιτεί:

- τη διασφάλιση ότι τα ίδια αδικήματα ποινικοποιούνται σε όλα τα κράτη μέλη· και
- την εξασφάλιση στις αρχές επιβολής του νόμου των μέσων για δράση και συνεργασία μεταξύ τους.

Για τον σκοπό αυτό, η παρούσα οδηγία απαιτεί την προσέγγιση των συστημάτων ποινικού δικαίου μεταξύ των χωρών της ΕΕ και την ενίσχυση της συνεργασίας μεταξύ των δικαστικών αρχών όσον αφορά:

- την παράνομη πρόσβαση σε συστήματα πληροφοριών,
- την παράνομη παρεμβολή σε σύστημα,
- την παράνομη παρεμβολή σε δεδομένα,
- την παράνομη υποκλοπή.

Σε όλες τις περιπτώσεις, η εγκληματική πράξη πρέπει να διαπράττεται εκ προθέσεως.

Τιμωρείται η ηθική αυτουργία, η υποβοήθηση, η συνέργεια και η απόπειρα διάπραξης για οποιοδήποτε από τα παραπάνω αδικήματα.

Τα κράτη μέλη πρέπει να προβλέψουν ότι τέτοιου είδους αδικήματα τιμωρούνται με αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις.

Σε περίπτωση που το αδίκημα διαπράττεται στο πλαίσιο εγκληματικής οργάνωσης κατά την έννοια της παρούσας οδηγίας, και προκαλεί σημαντική ζημία ή θίγει ζωτικά συμφέροντα, αυτό θα θεωρείται επιβαρυντική περίσταση. Το ίδιο ισχύει αν το αδίκημα διαπράττεται χρησιμοποιώντας την ταυτότητα άλλου προσώπου και προκαλεί βλάβη στον εν λόγω πρόσωπο.

Η οδηγία εισάγει επίσης την ευθύνη «νομικών προσώπων» και καθορίζει τις κυρώσεις που μπορούν να εφαρμοστούν σε περίπτωση νομικής ευθύνης.

Κάθε χώρα της ΕΕ ασκεί δικαιοδοσία στο ελάχιστο για τα αδικήματα που διαπράττονται στο έδαφός της ή από κάποιον από τους υπηκόους της εκτός του εδάφους της. Σε περίπτωση που πολλές χώρες έχουν δικαιοδοσία για κάποιο αδίκημα, οφείλουν να συνεργαστούν, προκειμένου να αποφασιστεί ποια χώρα θα διεξάγει τη δίωξη κατά του δράστη του εν λόγω αδικήματος.

Βελτίωση της συνεργασίας

Για την καλύτερη καταπολέμηση του εγκλήματος στον κυβερνοχώρο, η οδηγία κάνει έκκληση για περισσότερη διεθνή συνεργασία μεταξύ των δικαστικών αρχών και των αρχών επιβολής του νόμου.

Προς επίτευξη αυτού του σκοπού, οι χώρες της ΕΕ θα πρέπει:

- να έχουν ένα λειτουργικό εθνικό σημείο επαφής,
- να χρησιμοποιούν το υπάρχον δίκτυο των σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας,
- να ανταποκρίνονται σε επείγοντα αιτήματα για βοήθεια εντός 8 ωρών προκειμένου να δηλώσουν αν και πότε θα μπορέσουν να απαντήσουν,
- να συλλέγουν στατιστικά δεδομένα σχετικά με το έγκλημα στον κυβερνοχώρο.

Η παρούσα οδηγία βασίζεται και αντικαθιστά την απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών. Στηρίζεται επίσης στη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο του 2001 η οποία χρησιμεύει ως πρότυπο για την εθνική και την περιφερειακή νομοθεσία για το έγκλημα στον κυβερνοχώρο και δημιουργεί κοινή βάση συνεργασίας εντός της ΕΕ, αλλά και πέραν αυτής. (http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:l33193)

Τα άρθρα της Σύμβασης:

- Το άρθρο 1 παραθέτει το ***αντικείμενο της Σύμβασης*.**
- Το άρθρο 2 παραθέτει τους ***βασικούς ορισμούς:***

*Για τους σκοπούς της παρούσας οδηγίας, εφαρμόζονται οι ακόλουθοι ορισμοί:*

*α) «σύστημα πληροφοριών»: η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισ σότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επε ξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργα σίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους·*

*β) «ηλεκτρονικά δεδομένα»: η παρουσίαση γεγονότων, πληροφο ριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτε λέσει μια λειτουργία·*

*γ) «νομικό πρόσωπο»: κάθε οντότητα που έχει το καθεστώς του νομικού προσώπου βάσει του εφαρμοστέου δικαίου, αλλά δεν περιλαμβάνει κράτη, ή δημόσιους φορείς κατά την άσκηση της εξουσίας τους ή δημόσιους διεθνείς οργανισμούς·*

*δ) «χωρίς δικαίωμα»: η αναφερόμενη στην παρούσα οδηγία συμπε ριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου.*

- Το άρθρο 3 αναφέρεται σε ***Παράνομη πρόσβαση σε συστήματα πληροφοριών***

*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος*

*πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφα λείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περι πτώσεις.*

- Το άρθρο 4 αναφέρεται σε ***Παράνομη παρεμβολή σε σύστημα***

*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομέ νων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.*

- Το άρθρο 5 αναφέρεται σε ***Παράνομη παρεμβολή σε δεδομένα***

*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.*

- Το άρθρο 6 αναφέρεται σε ***Παράνομη υποκλοπή***

*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλε κτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφο ριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδο μένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.*

- Το άρθρο 7 αναφέρεται σε ***Εργαλεία που χρησιμοποιούνται για τη διάπραξη των αδικημάτων***

*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλου θων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποι ηθούν προς διάπραξη οποιουδήποτε εκ των αδικημάτων που ανα φέρονται στα άρθρα 3 έως 6, τιμωρείται ως ποινικό αδίκημα, του λάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις: α) πρόγραμμα υπολογιστή, που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6· β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών*

- Το άρθρο 8 αναφέρεται σε ***Ηθική αυτουργία, υποβοήθηση και συνέργεια και απόπειρα***

*1. Τα κράτη μέλη εξασφαλίζουν ότι η ηθική αυτουργία, ή η υποβοήθηση και η συνέργεια, προς διάπραξη αδικήματος που ανα φέρεται στα άρθρα 3 έως 7 τιμωρείται ως ποινικό αδίκημα.*

*2. Τα κράτη μέλη εξασφαλίζουν ότι η απόπειρα διάπραξης αδι κήματος που αναφέρεται στα άρθρα 4 και 5 να τιμωρείται ως ποινικό αδίκημα.*

- Το άρθρο 9 αναφέρεται σε ***Κυρώσεις***

*1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξα σφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8 τιμωρούνται με αποτελεσματικές, αναλογικές και αποτρεπτικές ποι νικές κυρώσεις.*

*2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξα σφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7 τιμωρούνται με στερητική της ελευθερίας ποινή, το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον δύο έτη, τουλάχιστον για περιπτώσεις που δεν είναι ήσσονος σημασίας.*

*3. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξα σφαλίσουν ότι, οσάκις τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται εκ προθέσεως, και εφόσον έχει πληγεί σημα ντικός αριθμός συστημάτων πληροφοριών μέσω της χρήσης εργα λείου αναφερομένου στο άρθρο 7, το οποίο έχει σχεδιασθεί ή προσαρμοσθεί πρωτίστως για τον σκοπό αυτό, τιμωρούνται με στε ρητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον τρία έτη.*

*4. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξα σφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον πέντε έτη, εφόσον: α) διαπράττονται στο πλαίσιο εγκληματικής οργάνωσης κατά την έννοια της απόφασης-πλαισίου 2008/841/ΔΕΥ, ανεξαρτήτως της κύρωσης που ορίζεται σε αυτή· β) προκαλούν σημαντικές ζημίες, ή γ) διαπράττονται κατά συστήματος πληροφοριών που αποτελεί μέρος ζωτικής σημασίας υποδομής.*

*5. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να δια σφαλίσουν ότι εφόσον τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται με υφαρπαγή δεδομένων προσωπικού χαρα κτήρα άλλου προσώπου, προκειμένου να αποκτηθεί η εμπιστοσύνη τρίτων, και, ως εκ τούτου, προκαλούν ζημία στον νόμιμο δικαιούχο της ταυτότητας, το γεγονός αυτό μπορεί, σύμφωνα με το εθνικό δίκαιο, να εκλαμβάνεται ως επιβαρυντική περίσταση, εκτός εάν οι εν λόγω περιστάσεις καλύπτονται ήδη από άλλο αδίκημα που τιμωρεί ται σύμφωνα με το εθνικό δίκαιο.*

- Το άρθρο 10 αναφέρεται σε ***Ευθύνη νομικών προσώπων***

*1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι νομικά πρόσωπα είναι δυνατόν να υπέχουν ευθύνη για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8 τα οποία έχουν τελεσθεί προς όφελός τους από οιοδήποτε πρόσω πο, ενεργώντας είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου και το οποίο κατέχει ιθύνουσα θέση εντός του νομικού αυτού προσώπου, βάσει μιας από τις ακόλουθες εξουσίες: α) εξουσία εκπροσώπησης του νομικού προσώπου· β) εξουσία λήψης αποφάσεων για λογαριασμό του νομικού προσώ που· γ) εξουσία άσκησης ελέγχου εντός του νομικού προσώπου.*

*2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι νομικά πρόσωπα μπορούν να θεωρούνται υπεύ θυνα οσάκις η έλλειψη εποπτείας ή ελέγχου εκ μέρους ενός από τα πρόσωπα που αναφέρονται στην παράγραφο 1 έχει επιτρέψει τη διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 8 προς όφελος του εν λόγω νομικού προσώπου από πρόσωπο που τελεί υπό την εξουσία του.*

*3. Η ευθύνη των νομικών προσώπων δυνάμει των παραγράφων 1 και 2 δεν αποκλείει την ποινική δίωξη φυσικών προσώπων που είναι αυτουργοί ή ηθικοί αυτουργοί ή συνεργοί στη διάπραξη αδικημά των που αναφέρονται στα άρθρα 3 έως 8*

- Το άρθρο 11 αναφέρεται σε ***Κυρώσεις κατά νομικών προσώπων***

*1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι το νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 10 παράγραφος 1 τιμωρείται με αποτελεσμα τικές, αναλογικές και αποτρεπτικές κυρώσεις, στις οποίες περιλαμβάνονται χρηματικές ποινές ή πρόστιμα και οι οποίες μπορούν να περιλαμβάνουν και άλλες κυρώσεις, όπως: α) αποκλεισμό από δημόσιες παροχές ή ενισχύσεις· β) προσωρινή ή οριστική απαγόρευση της άσκησης εμπορικών δρα στηριοτήτων· γ) θέση υπό δικαστική εποπτεία· δ) δικαστική εκκαθάριση· ε) προσωρινό ή οριστικό κλείσιμο των εγκαταστάσεων που χρησι μοποιήθηκαν για τη διάπραξη του αδικήματος.*

*2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι το νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 10 παράγραφος 2 τιμωρείται με αποτελεσμα τικές, αναλογικές και αποτρεπτικές κυρώσεις ή άλλα μέτρα.*

- Το άρθρο 12 αναφέρεται σε ***Δικαιοδοσία***

*1. Τα κράτη μέλη θεμελιώνουν τη δικαιοδοσία τους για τα αδι κήματα που αναφέρονται στα άρθρα 3 έως 8, εφόσον το αδίκημα έχει διαπραχθεί: α) εν όλω ή εν μέρει στο έδαφος*

*τους· ή β) από υπήκοό τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται αδίκημα στον τόπο όπου έχει διαπραχθεί.*

*2. Κράτος μέλος, κατά τη θεμελίωση της δικαιοδοσίας του σύμ φωνα με την παράγραφο 1 στοιχείο α), εξασφαλίζει ότι διαθέτει δικαιοδοσία, οσάκις: α) ο δράστης διέπραξε το αδίκημα, όταν ευρίσκετο στο έδαφός του, ανεξάρτητα από το εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός του· ή β) το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδα φός του ανεξάρτητα από το εάν όταν ο δράστης διέπραξε το αδίκημα ευρίσκετο στο έδαφός του.*

*3. Το κράτος μέλος ενημερώνει σχετικά την Επιτροπή οσάκις αποφασίζει να θεμελιώσει δικαιοδοσία για αδίκημα που αναφέρεται στα άρθρα 3 έως 8, το οποίο διαπράττεται εκτός του εδάφους του, οσάκις, μεταξύ άλλων: α) ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφος του, ή β) το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκα τεστημένου στο έδαφος του.*

- Το άρθρο 13 αναφέρεται σε ***Ανταλλαγή πληροφοριών***

*1. Για τους σκοπούς της ανταλλαγής πληροφοριών σχετικά με τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8, τα κράτη μέλη εξασφαλίζουν ότι διαθέτουν ένα λειτουργικό εθνικό σημείο επαφής και κάνουν χρήση του υφιστάμενου δικτύου επιχειρησιακών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας. Τα κράτη μέλη εξασφαλίζουν επίσης ότι διαθέτουν διαδικασίες ώστε, σε περιπτώσεις επειγουσών αιτήσεων συνδρομής, η αρμόδια αρχή να μπορεί να δηλώσει, εντός οκτώ ωρών από την παραλαβή, τουλάχιστον εάν θα απαντήσει στην αίτηση, καθώς και τη μορφή και τον εκτιμώμενο χρόνο της απάντησης αυτής.*

*2. Τα κράτη μέλη ενημερώνουν την Επιτροπή για το σημείο επαφής που έχουν ορίσει κατά τα αναφερόμενα στην παράγραφο 1. Η Επιτροπή διαβιβάζει αυτές τις πληροφορίες στα άλλα κράτη μέλη και τους αρμόδιους ειδικευμένους οργανισμούς και φορείς της Ένωσης. 3. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα ώστε να εξα σφαλίσουν ότι διατίθενται οι κατάλληλοι δίαυλοι αναφοράς προκει μένου να διευκολυνθεί η υποβολή αναφορών χωρίς αδικαιολόγητη καθυστέρηση σχετικά με αδικήματα που αναφέρονται στα άρθρα 3 έως 6 στις αρμόδιες εθνικές τους αρχές*

Το άρθρο 14 αναφέρεται σε ***Παρακολούθηση και στατιστικές***

*1. Τα κράτη μέλη εξασφαλίζουν ότι ένα σύστημα ευρίσκεται σε ετοιμότητα για την καταγραφή, την παραγωγή και την παροχή στατιστικών στοιχείων για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7.*

*2. Τα αναφερόμενα στην παράγραφο 1 στατιστικά στοιχεία καλύπτουν κατ' ελάχιστον τα υφιστάμενα δεδομένα ως προς τον αριθμό των αδικημάτων που αναφέρονται στα άρθρα 3 έως 7, τα οποία καταγράφονται από τα κράτη μέλη, καθώς και τον αριθμό των*

*προσώπων τα οποία διώχθηκαν και καταδικάστηκαν για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7.*

*3. Τα κράτη μέλη διαβιβάζουν στην Επιτροπή τα στοιχεία που συγκεντρώνουν σύμφωνα με το παρόν άρθρο. Η Επιτροπή μεριμνά ώστε να δημοσιεύεται και να υποβάλλεται στους αρμόδιους ειδι κευμένους οργανισμούς και φορείς της Ένωσης συγκεντρωτική επι σκόπηση αυτών των στατιστικών εκθέσεων.*

Το άρθρο 15 αναφέρεται σε *Αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ*

*Η απόφαση-πλαίσιο 2005/222/ΔΕΥαντικαθίσταται όσον αφορά τα κράτη μέλη που συμμετέχουν στην έκδοση της παρούσας οδηγίας, με την επιφύλαξη των υποχρεώσεων των κρατών μελών ως προς τις προθεσμίες μεταφοράς της απόφασης-πλαισίου στο εθνικό τους δίκαιο. Όσον αφορά τα κράτη μέλη που συμμετέχουν στην έκδοση της παρούσας οδηγίας, οι παραπομπές στην απόφαση-πλαίσιο 2005/222/ΔΕΥ θεωρούνται ως παραπομπές στην παρούσα οδηγία.*

Το άρθρο 16 αναφέρεται σε ***Μεταφορά στο εθνικό δίκαιο***

*1. Τα κράτη μέλη θέτουν σε ισχύ τις αναγκαίες νομοθετικές, κανονιστικές και διοικητικές διατάξεις για συμμορφωθούν με την παρούσα οδηγία έως τις 4 Σεπτεμβρίου 2015*

*2. Τα κράτη μέλη διαβιβάζουν στην Επιτροπή το κείμενο των μέτρων με τα οποία μεταφέρουν στο εθνικό τους δίκαιο τις υπο χρεώσεις που υπέχουν δυνάμει της παρούσας οδηγίας. 3. Τα εν λόγω μέτρα, όταν θεσπίζονται από τα κράτη μέλη, περιέχουν αναφορά στην παρούσα οδηγία ή συνοδεύονται από παρόμοια αναφορά κατά την επίσημη δημοσίευσή τους. Ο τρόπος πραγματοποίησης της αναφοράς αυτής καθορίζεται από τα κράτη μέλη.*

Το άρθρο 17 αναφέρεται *σε* ***Υποβολή εκθέσεων***

*Η Επιτροπή υποβάλλει, μέχρι τις 4 Σεπτεμβρίου 2017, έκθεση στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο με την οποία αξιολογεί ται κατά πόσον τα κράτη μέλη έχουν λάβει τα αναγκαία μέτρα για να συμμορφωθούν προς την παρούσα οδηγία, συνοδευόμενη, εφό σον απαιτείται, από νομοθετικές προτάσεις. Η Επιτροπή λαμβάνει επίσης υπόψη τις τεχνικές και νομικές εξελίξεις στον τομέα του εγκλήματος στον κυβερνοχώρο, ιδίως σε σχέση με το πεδίο εφαρ μογής της παρούσας οδηγίας.*

Το άρθρο 18 αναφέρεται *στην* ***Εναρξη Ισχύος***

Το άρθρο 17 αναφέρεται *στους* ***Αποδέκτες***

(Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 14.08.2013)

## 4.4 Ελλάδα – Νομικό καθεστώς

Τα ηλεκτρονικά εγκλήματα και τα κυβερνοεγκλήματα στο παρελθόν τιμωρούνταν με βάση τον Ν.1805/1988 «Εκσυγχρονισμός του θεσμού του ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων» (ΦΕΚ 199/Α/31.08.1988), ο οποίος επέφερε με τα άρθρα 2-5 τροποποιήσεις, στα τότε ισχύοντα άρθρα 13, 370 και 386 του Ποινικού Κώδικα. Για 28 έτη οι παρακάτω διατάξεις ήταν αμετάβλητες παρόλο που η εξέλιξη της τεχνολογίας ήταν ραγδαία και η φύση των ηλεκτρονικών/διαδικτυακών εγκλημάτων εξελισσόταν με γρήγορους ρυθμούς, ενώ παράλληλα αυξάνονταν και ο αριθμός των εν λόγω επιθέσεων. Αυτό είχε ως συνέπεια να δημιουργούνται προβλήματα ως προς τη δίωξη των εν λόγω εγκλημάτων.

στην περίπτωση γ' του άρθρου 13 ΠΚ προστέθηκε εδάφιο, το οποίο ορίζει πως *«Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία» .*

- **Παράνομη πρόσβαση σε απόρρητα (370 Β)**

Μετά το άρθρο 370 Α προστέθηκε το άρθρο 370 Β, το οποίο ορίζει *«1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών.* Ως *απόρρητα*

*θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους. 2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους. 3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147. 4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση».*

- **Ποινική προστασία πνευματικής ιδιοκτησίας(370Γ §1)/ 1**
- **Διείσδυση σε συστήματα και επικοινωνίες (hacking)- 370Γ§2**

Μετά το άρθρο 370Β προστέθηκε το άρθρο 370Γ το οποίο όριζε ότι *« 1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ. 2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα (29) ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. 3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του. 4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση» .*

- **Απάτη με υπολογιστή (386Α ΠΚ)**

Μετά το άρθρο 386 προστέθηκε το άρθρο 386Α το οποίο όριζε ότι *«Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα»*. (Λ.Καρατζά)

- **Ποινική Προστασία των προσωπικών δεδομένων (22 ν. 2472/97)**

Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και σκοπός του η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Ο νομοθέτης με το άρθρο 22 ν. 2472/97 για την προστασία του αοριοθετεί με ουσιαστικούς, οργανωτικούς, διαδικαστικούς και κυρωτικούς κανόνες τη συνταγματικά ανεκτή επεξεργασία προσωπικών δεδομένων και με τον τρόπο αυτό ρυθμίζει τη ροή των προσωπικών δεδομένων στο πλαίσιο του κράτους, της οικονομίας και της κοινωνίας και οργανώνει τις πληροφοριακές σχέσεις μεταξύ των προσώπων. Ο νόμος αντιμετωπίζει το δημόσιο και τον ιδιωτικό τομέα ως ισοδύναμες πηγές διακινδύνευσης για τα δικαιώματα των προσώπων, λαμβάνοντας υπόψη την χρησιμοποίηση ιδιωτικών βάσεων δεδομένων για δημόσιους σκοπούς, την αύξουσα “ιδιωτικοποίηση” λειτουργιών και υπηρεσιών που ως τώρα ανήκαν στη σφαίρα της δημόσιας εξουσίας, και κυρίως την αύξουσα εμπορευματοποίηση των προσωπικών δεδομένων. Οι διατάξεις και επιταγές του καταλαμβάνουν, χωρίς διαφοροποιήσεις, την αυτοματοποιημένη αλλά και την κλασική, με συμβατικές μεθόδους διεξαγόμενη, επεξεργασία και αυτό όχι μόνο για να αποτραπεί κίνδυνος περιγραφής των επιταγών και απαγορεύσεων αλλά και επειδή ελήφθη υπόψη ότι σημαντικός αριθμός αρχείων εξακολουθεί να τηρείται με παραδοσιακές μεθόδους. (Μήτρου Ε. 2012)

- **Διατάραξη οικιακής ειρήνης (334ΠΚ)**

Η παράνομη πρόσβαση σε δεδομένα παρουσιάζει αναλογία προς το έγκλημα της διατάραξης οικιακής ειρήνη που περιγράφεται στο άρθρο 334 του ποινικού κώδικα, καθώς, όπως παρατηρείται, παραβιάζεται ένας χώρος «ηλεκτρονικής εξουσίασης», όπου το κάθε νομικό η φυσικό πρόσωπο αξιώνει να αυτοπροσδιορίζεται και να μπορεί ελεύθερα, χωρίς «παρεμβολές» και «παραβιάσεις» να αναπτύσσει τις δραστηριότητές του. (Ποινικός Κώδικας) (Μήτρου Ε, 2002)

**Ειδικοί Ποινικοί Νόμοι**

- Ν.2225/1994 «Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»
- Ν. 2246/1994 «Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών»
- Ν.2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
- Ν. 2672/1998 «Διακίνηση εγγράφων με ηλεκτρονικά μέσα»
- Ν.2774/1999 «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»
- Ν.2867/2000 «Οργάνωση και λειτουργία των τηλεπικοινωνιών»
- Ν .3115/2003 «Αρχή διασφάλισης του απορρήτου των επικοινωνιών»
- Ν.3431/2006 «Περί ηλεκτρονικών επικοινωνιών»
- Ν. 3471/2006 «Προστασία Δεδομένων Προσωπικού Χαρακτήρα»

### 4.4.1 Επικαιροποίηση της ελληνικής νομοθεσίας - Νόμος 4411/2016

Στο ΦΕΚ 142/Α/3-8-2016 δημοσιεύθηκε ο Νόμος 4411/2016, με το οποίο γίνεται γίνεται επικαιροποίηση της ποινικής νομοθεσίας στον τομέα της «κυβερνοεγκληματικότητας» («cybercriminality»). Ειδικότερα, κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, το Προσθέτο Πρωτοκόλλο, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών που υπογράφηκε στο Στρασβούργο στις 28 Ιανουαρίου 2003 και ενσωματώθηκε την Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Με το νόμο τιμωρούνται ενέργειες που στρέφονται κατά των δικτύων πληροφοριών, δηλαδή πράξεις που αποσκοπούν στην από πρόθεση πρόκληση βλάβης στα δίκτυα και στρέφονται κατά της ακεραιότητας, της διαθεσιμότητας των δεδομένων ή των συστημάτων πληροφορικής. Επιπλέον τιμωρούνται πράξεις που αφορούν την παράνομη πρόσβαση, την υποκλοπή, την παρεμβολή σε δεδομένα και τις παρεμβολές σε συστήματα. (www.e-nomothesia.gr)

Η επικαιροποίηση της ποινικής νομοθεσίας και η αλλαγή του νομικού πλαισίου ήταν αναγκαία για τον εκσυγχρονισμό και την ορθή καταπολέμηση του ηλεκτρονικού/διαδικτυακού εγκλήματος, όπως επίσης και για να συμβαδίσει η Ελλάδα με τις υπόλοιπες Ευρωπαϊκές χώρες και με το διεθνές νομικό πλαίσιο.

## Οι αλλαγές στον Ποινικό Κώδικα

Στο άρθρο δεύτερο του Νόμου 4411/2016 παρατίθενται οι διατάξεις ουσιαστικού ποινικού δικαίου, οι οποίες είναι απαραίτητες για την προσαρμογή της ελληνικής νομοθεσίας στη Σύμβαση για το έγκλημα στον Κυβερνοχώρο και την εναρμόνιση της ελληνικής νομοθεσίας με την Οδηγία 2013/40/ΕΕ.

Ειδικότερα:

**1. Στο άρθρο 13 του Ποινικού Κώδικα προστίθενται περιπτώσεις η΄ και θ΄ ως εξής:**

«*η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.*

*θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».*

**2. Μετά το άρθρο 292Α του Ποινικού Κώδικα προστίθεται άρθρο 292Β ως εξής:**

*Άρθρο 292Β*
*Παρακώλυση λειτουργίας πληροφοριακών συστημάτων*
*1. Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών*

*δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών.*
*2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.*
*3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.*
*4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».*

<u>Εγκλήματα σε Σχέση με Εργαλεία για την Τέλεση Κυβερνοεγκλημάτων – Παρακώλυση λειτουργίας πληροφοριακών συστημάτων</u>

Μετά το άρθρο 292Α του Ποινικού Κώδικα προστίθεται νέο άρθρο 292Β για την Παρακώλυση λειτουργίας πληροφοριακών συστημάτων με το οποίο προσαρμόζεται η ποινική προστασία λαμβάνοντας κατ' αρχήν υπόψη την αντίστοιχη ποινική πρόβλεψη για τις επιθέσεις που εκδηλώνονται κατά συστημάτων τηλεφωνικών επικοινωνιών (άρθρο 292Α Π.Κ.), στα πλαίσια όμως των ποινών που η Οδηγία προβλέπει και με γνώμονα την τήρηση της αρχής της αναλογικότητας ανάλογα με το είδος και την ένταση

της προσβολής που οι πράξεις αυτές επιφέρουν. Σύμφωνα με τα οριζόμενα στην Οδηγία προβλέπεται αυστηρότερο πλαίσιο ποινής στις περιπτώσεις, όπου η αξιόποινη συμπεριφορά προκαλεί ζημία σε σημαντικό αριθμό πληροφοριακών συστημάτων μέσω της χρήσης εργαλείων που έχουν σχεδιαστεί κυρίως για τον σκοπό αυτόν, τελείται στο πλαίσιο δράσης εγκληματικής οργάνωσης, σε αντιστοιχία με τον ορισμό αυτής στο άρθρο 187 Π.Κ., προκαλεί ιδιαίτερα μεγάλη ζημία ή πλήττει πληροφοριακά συστήματα τα οποία αποτελούν μέρος υποδομής που παρέχει ζωτικής σημασίας αγαθά ή υπηρεσίες για την κοινωνία και το κράτος.

**3. Μετά το άρθρο 292Β του Ποινικού Κώδικα προστίθεται άρθρο 292Γ ως εξής:**

*Άρθρο 292Γ*
*Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί:*
*α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκλημάτων του άρθρου 292Β,*
*β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».*

Ποινικοποίηση αυτοτελών συμπεριφορών

Μετά το άρθρο 292Β του Ποινικού Κώδικα προστίθεται νέο άρθρο 292Γ σύμφωνα και με το άρθρο 7 της Οδηγίας, ποινικοποιούνται αυτοτελώς συμπεριφορές που κατατείνουν στην τέλεση των εγκλημάτων του άρθρου 292Β Π.Κ. και ειδικότερα παραγωγή, πώληση, διανομή, εισαγωγή, κατοχή κ.λπ. προγραμμάτων ή συσκευών σχεδιασμένων ή προσαρμοσμένων για την τέλεση των πράξεων του άρθρου αυτού.

**4. Οι παράγραφοι 2 και 5 του άρθρου 348Α του Ποινικού Κώδικα αντικαθίστανται ως εξής:**

*«2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.*
*5. Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους».*

**5. Το άρθρο 348Β του Ποινικού Κώδικα αντικαθίσταται ως εξής:**

*«Άρθρο 348Β*
*Προσέλκυση παιδιών για γενετήσιους λόγους*
*Όποιος με πρόθεση, μέσω πληροφοριακών συστημάτων, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαπέντε έτη, να συναντήσει τον ίδιο ή τρίτο, με σκοπό τη διάπραξη σε βάρος του ανηλίκου των αδικημάτων των άρθρων 339 παράγραφοι 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ».*

<u>Πορνογραφία</u>

Το άρθρο 348Β του Ποινικού Κώδικα «Προσέλκυση παιδιών για γενετήσιους λόγους» τροποποιήθηκε και πάλι (έχει ήδη τροποποιηθεί από τον Έλληνα Νομοθέτη, την τελευταία φορά με το ν. 4267/2014, που εναρμόνισε την ελληνική νομοθεσία με την Οδηγία 2011/93/ΕΕ.) και την παρούσα τροποποίηση εισάγεται στις παραγράφους 2 και 5 ο όρος του πληροφοριακού συστήματος, όπως ορίζεται στο άρθρο 13 Π.Κ. προκειμένου να αποφευχθεί η ορολογική ανομοιογένεια στις διάφορες διατάξεις του Ποινικού Κώδικα. Για τους ίδιους λόγους τροποποιείται και το άρθρο 348Β Π.Κ. με την εισαγωγή του όρου « πληροφοριακά συστήματα».

**6. Το άρθρο 370Γ του Ποινικού Κώδικα αντικαθίσταται ως εξής:**

*«Άρθρο 370Γ*
*Παράνομη πρόσβαση σε πληροφοριακό σύστημα*
*1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.*
*2. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.*
*3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.*
*4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση».Βλέπε επίσης: Ευθύνη νομικών προσώπων (Άρθρο 11 της Οδηγίας)*

Παράνομη πρόσβαση σε πληροφοριακό σύστημα

Τροποποιείται το άρθρο 370Γ Π.Κ. και με τη νέα διατύπωση της διάταξης στην δεύτερη παράγραφο τιμωρείται και η χωρίς δικαίωμα πρόσβαση στο σύνολο ή σε τμήμα ενός πληροφοριακού συστήματος, δηλαδή το αποκαλούμενο στην γλώσσα των δραστών hacking.

**7. Μετά το άρθρο 370Γ του Ποινικού Κώδικα προστίθεται άρθρο 370Δ ως εξής:**

*«Άρθρο 370Δ*

*1. Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.*
*2. Με την ποινή της παραγράφου 1 τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπεται στην παράγραφο 1.*
*3. Αν οι πράξεις των παραγράφων 1 και 2 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146».*

<u>Παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων</u>
Με τη νέα διάταξη του άρθρου 370Δ Π.Κ. τιμωρείται αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων και η χρήση των πληροφοριών με ποινές αντίστοιχες της παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών που προβλέπονται στη διάταξη του άρθρου 370Α Π.Κ. (κάθειρξη μέχρι δέκα ετών). Αν οι πράξεις αυτές συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146 Π.Κ..

**8. Μετά το άρθρο 370Δ του Ποινικού Κώδικα προστίθεται άρθρο 370Ε ως εξής:**

*«Άρθρο 370Ε*
*Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα*

*παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».*

Παρεμβολές σε δεδομένα - Παράνομη Υποκλοπή Ψηφιακών Δεδομένων

Με τη νέα διάταξη του άρθρου 370Ε Π.Κ. τιμωρείται αυτοτελώς η εισαγωγή, διανομή κατοχή και διάθεση προγραμμάτων, συσκευών ή τεχνικών μέσων, με τα οποία θα ήταν δυνατή η πρόσβαση σε πληροφοριακό σύστημα, προκειμένου να διαπραχθούν τα εγκλήματα που αναφέρονται στα άρθρα 370Α μέχρι 370Δ Π.Κ. Με το νέο άρθρο 38ΙΑ Π.Κ. εναρμονίζεται η ελληνική νομοθεσία με τα άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας. Με τη νέα διάταξη αυτή καλύπτεται ένα κενό της ελληνικής νομοθεσίας και προστατεύονται πλέον αυτοτελώς τα ψηφιακά δεδομένα από πράξεις καταστροφής, διαγραφής αλλοίωσής τους κ.λπ. Έτσι αποφεύγεται το άτοπο τα ψηφιακά δεδομένα να προστατεύονται αντανακλαστικά μόνο στον βαθμό και την έκταση που πλήττεται ο υλικός τους φορέας (σκληρός δίσκος, φορητή μνήμη κ.λπ.) Στις παραγράφους 2 και 3 προβλέπονται διακεκριμένες παραλλαγές σύμφωνα με τις ρυθμίσεις της Οδηγίας, ενώ στην παρ. 4 προβλέπεται ότι το βασικό έγκλημα της παρ. 1 διώκεται κατ' έγκληση.

**9. Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται άρθρο 381Α ως εξής**

*«Άρθρο 381Α*

*Φθορά ηλεκτρονικών δεδομένων*

*1. Όποιος χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.*

*2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρί α (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν*

*μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.*
*3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.*
*4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».*

<u>Παράνομη Παρεμβολή σε Ψηφιακά Δεδομένα -Φθορά ηλεκτρονικών δεδομένων</u>

Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται νέο άρθρο 381Α Φθορά ηλεκτρονικών δεδομένων με το οποίο η ελληνική νομοθεσία εναρμονίζεται με το άρθρο 7 της Οδηγίας, που προβλέπει την ποινική ευθύνη προσώπων για πράξεις αγοράς, πώλησης, προμήθειας, κατοχής κ.λπ. προγραμμάτων ή κωδικών που μπορούν να χρησιμοποιηθούν για την τέλεση διάφορων αξιόποινων πράξεων μεταξύ των οποίων και οι προβλεπόμενες πλέον στο άρθρο 38ΙΑ Π.Κ..

**10. Μετά το άρθρο 381Α του Ποινικού Κώδικα προστίθεται άρθρο 381Β ως εξής:**

*«Άρθρο 381Β*
*Με φυλάκιση μέχρι δύο (2) ετών, τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα του άρθρου 381Α παράγραφοι 1, 2 και 3 παράγει,*

*πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».*

**11. Το άρθρο 386Α του Ποινικού Κώδικα αντικαθίσταται ως εξής:**

*«Άρθρο 386Α*
*Απάτη με υπολογιστή*
*Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα».*

Απάτη σχετική με υπολογιστές

Τροποποιείται το άρθρο 386Α Π.Κ. (απάτη υπολογιστή) κατά τα οριζόμενα στο άρθρο 8 της Σύμβασης. Σύμφωνα με τη νέα διάταξη περιλαμβάνεται πλέον ρητά στις περιπτώσεις απάτης με υπολογιστή και η χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα, όπως π.χ. στην περίπτωση του δράστη που έχει αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου.

*(https://www.lawspot.gr/nomika-nea/oles-oi-allages-se-poiniko-kodika-kai-kodika-poinikis-dikonomias-me-nomo-4411-2016)*

# Επίλογος – Συμπεράσματα

Η εξέλιξη της τεχνολογίας και της πληροφορικής και η εισβολή των ηλεκτρονικών υπολογιστών και του διαδικτύου στην κοινωνία, οδήγησε στη δημιουργία ιδανικών συνθηκών για τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων. Παράλληλα, αναδείχθηκε η ανάγκη της αντιμετώπισης των εν λόγω εγκλημάτων και της προστασίας των πληροφοριακών συστημάτων από κακόβουλες επιθέσεις.

Για την αντιμετώπιση του κινδύνου αυτού είναι απαραίτητη η διακρατική συνεργασία και η ύπαρξη κοινής και αποτελεσματικής στρατηγικής. Στην Ευρωπαϊκή ένωση έχουμε δει ότι έχουν γίνει σημαντικές δράσεις, όμως κάθε χώρα ξεχωριστά θα πρέπει να ενσωματώνει αυτές τις δράσεις στη δική της νομοθεσία και να λαμβάνει αποτελεσματικά μέτρα. Στην Ελλάδα, η επικαιροποίηση του Ποινικού Κώδικα αποτέλεσε ένα πολύ σημαντικό βήμα, για να συμβαδίσει η χώρα μας με τις αλλαγές που είχαν επέλθει εδώ και καιρό σε ευρωπαϊκό και διεθνές επίπεδο, καθώς το κυβερνοέγκλημα αποτελεί έναν ταχύτατα εξελισσόμενο χώρο.

Εκτός από την ανάγκη για την αντιμετώπιση των νέων μορφών εγκληματικότητας, πολή σημαντική είναι η πρόληψη και η ενημέρωση του κοινού, ώστε να περιοριστεί η τέλεση των εν λόγω εγκλημάτων.

# **Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α**


Furnell St. «Κυβερνοέγκλημα – Καταστρέφοντας την Κοινωνία της Πληροφορίας», (μετάφραση: Φ. Μηλιώνη), Αθήνα Εκδόσεις Παπαζήσης, 2006

Stallings W (2008), Βασικές Αρχές Ασφάλειας Δικτύων, Εφαρμογές και Πρότυπα. Αθήνα: Κλειδάριθμος

Α. Γιωτοπούλου-Μαραγκοπούλου (1979), Παραδόσεις Εγκληματολογίας, Αθήνα-Κομοτηνή: εκδ. Αντ. Ν. Σάκκουλα

Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία, «Ζητήματα από το Δίκαιο της Πληροφορικής», Εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 2002

Αργυρόπουλος Α.Δ., «Ηλεκτρονική Εγκληματικότητα», Εγκληματολογικά 19, Εκδ. Αντ. Ν. Σάκκουλα, 2001.

Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα: Μορφές, Πρόληψη, Αντιμετώπιση», Νομική Βιβλιοθήκη, Αθήνα, 2007, σ. 7-8.

Γκρίτζαλη Δ., (2004) "Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση" Αθήνα

Ζάννη Αν. «Το διαδικτυακό έγκλημα», Αθήνα, Αντ. Ν. Σάκκουλας, 2005

Κιούπης Δημήτρης, «Ποινικό Δίκαιο και Internet», Εκδ. Αντ. Ν. Σάκκουλα, 1999

Κριθαράς Θ. «Ποινικό Δίκαιο και Διαδίκτυο», Αθήνα Νομική Βιβλιοθήκη, 2009

Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα, 2001.

Μαγκάκης Γ.Α., «Ποινικό Δίκαιο», έκδοση γ΄ βελτιωμένη, Εκδ. Παπαζήση, 1984.

Μήτρου Λ., (2001) Προστασία Προσωπικών Δεδομένων: ένα νέο δικαίωμα; σε Δ. Τσάτσου/Ε. Βενιζέλου/Ξ. Κοντιάδη (επιμ.), Το Νέο Σύνταγμα – Πρακτικά συνεδρίου για το αναθεωρημένο Σύνταγμα 1975/1986/2001, Αθήνα – Κομοτηνή, σελ. 83 επ.

Μυλωνόπουλος Χρήστος, «Ποινικό Δίκαιο – Ειδικό Μέρος», Εκδ. Π.Ν.Σάκκουλας, 2001.

Παπακωνσταντίνου Ευάγγελος «Δίκαιο Πληροφορικής», Εκδόσεις Σάκκουλα 2010.

Σούρλας Π. (1995), Μία εισαγωγή στην επιστήμη του Δικαίαου, Αθήνα Σάκκουλας

Συμεωνίδου – Καστανίδου, «Εγκλήματα κατά προσωπικών αγαθών», Νομική Βιβλιοθήκη 2006.

Τσουραμάνης Χρ., «Ψηφιακή Εγκληματικότητα – Η (αν)ασφαλής όψη του διαδικτύου», Εκδ. Β. Ν. Κατσαρού, Αθήνα 2005.

Φαρσεδάκης Ι., «Στοιχεία Εγκληματικότητας» Νομική Βιβλιοθήκη, Αθήνα, 1996

**ΆΡΘΡΑ – ΜΕΛΕΤΕΣ**

Αγγελής Ι., «Διαδίκτυο (Internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο (Cybercrime – Internet Crime)», ΠοινΧρ Ν/2000, σελ. 675.

-Αγγελής Ι., «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», ΠοινΔικ 12/2001, σελ. 1218.

-Αγγελής Ι., «Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», ΠοινΔικ 12/2001, σελ. 1293.

- (Επίσημη Εφημερίδα Ευρωπαϊκής Ένωσης-31.07.2002)

- (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 14.08.2013)


**ΙΣΤΟΣΕΛΙΔΕΣ**


http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=135&Itemid=128&lang=

cyberhelp.eu

(http://eur-lex.europa.eu/legal-ontent/EL/TXT/PDF/?uri=CELEX:32001F0413&from=EL)

(http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32011L0093)

(https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/prostheto-protokollo-tis-symvasis-gia-egklima-ston )

(http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:l33193)

(www.e-nomothesia.gr)

http://www.saferinternet.gr

http://www.e-crime.gr

http://www.astynomia.gr

http://www.en.wikipedia.org

http://www.pharming-fishing.gr

http://el.wikibooks.org

http://electroniccrime.wordpress.com

https://sites.google.com/site/elektronikoenklema2012