ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΗΛΕΚΤΡΟΝΙΚΟ – ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Διπλωματική Εργασία

Του

Χριστοφόρου Β. ΚΟΛΙΟΥ

Θεσσαλονίκη, 2020

ΗΛΕΚΤΡΟΝΙΚΟ – ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Χριστόφορος Β. ΚΟΛΙΟΣ

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ
ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων/ουσα Καθηγητής/τρια Θεοχάρης Ι. Δαλακούρας
Ονοματεπώνυμο Καθηγητή/τριας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την …../…../2020

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
Θεοχάρης Ι. Δαλακούρας	.....	.....

Χριστόφορος Β. ΚΟΛΙΟΣ

Περίληψη

Η διπλωματική εργασία χωρίζεται σε δύο μέρη. Το πρώτο μέρος είναι σχετικό με τα πληροφοριακά συστήματα και τη λειτουργία του διαδικτύου επιχειρώντας να παρουσιάσει την λειτουργία τους καθώς και το πόσο ωφέλησε τον άνθρωπο. Από την άλλη πλευρά γίνεται παρουσίαση των αρνητικών φαινομένων που προκάλεσε η εξάπλωση του διαδικτύου. Γίνεται προσπάθεια ανάπτυξης των δυσχερειών, από τεχνικής άποψης, στην καταπολέμηση του διαδικτυακού εγκλήματος σε σχέση με το παράνομο περιουσιακό όφελος. Η εξέλιξη του φαινομένου αναμένεται μεγάλη, καθ' όσον η ανάγκη χρήσης των πληροφοριακών συστημάτων παρουσιάζεται πλέον ως μια από τις βασικότερες ανάγκες του ανθρώπου. Περαιτέρω γίνεται μια προσπάθεια παρουσίασης του νομικού οπλοστασίου της Ευρώπης και της Ελλάδας σχετικά με την αντιμετώπιση των εγκληματικών αυτών συμπεριφορών. Αναφέρονται τρόποι αντιμετώπισης τόσο από τεχνικής όσο και από νομικής πλευράς.

Ειδικότερα παρατίθεται ανάλυση των άρθρων 292Β, 370Β, 370Γ, 370Δ, 370Ε, $381^{Α}$, 386, $386^{Α}$ Π.Κ, τόσο με βάση τον παλαιό νόμο όσο και με βάση τις αλλαγές που επήλθαν με την κύρωση του νέου Ποινικού Κώδικα (Ν. 4639/2019).

Π Ε Ρ Ι Ε Χ Ο Μ Ε Ν Α

Α φ ι ε ρ ώ ν ε τ α ι,

Στα αγαπημένα μου τέκνα, Βασίλειο, Ευαγγελία, Γεώργιο, καθώς και στη σύζυγό μου, γιατί σε όλη την πορεία μου τους είχα στο πλευρό μου, αλλά και για το χρόνο που τους αποστέρησα για την πραγματοποίηση του Μεταπτυχιακού. Η αγάπη τους, αποτέλεσε εφαλτήριο και συνάμα έμπνευση για να ολοκληρώσω τις σπουδές μου.

Τους ευχαριστώ Θερμά μέσα από την καρδιά μου.!!

Χριστόφορος Β. ΚΟΛΙΟΣ

Η ΣΕΛΙΔΑ ΑΥΤΗ ΕΙΝΑΙ ΣΚΟΠΙΜΑ ΛΕΥΚΗ

Με την ολοκλήρωση της παρούσας διπλωματικής εργασίας, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα **Καθηγητή κ. Θεοχάρη ΔΑΛΑΚΟΥΡΑ** για την ανάθεση του συγκεκριμένου θέματος, την εμπιστοσύνη που μου έδειξε, τις γνώσεις που μου προσέφερε τόσο κατά την διάρκεια φοίτησής μου στο μεταπτυχιακό, όσο και κατά τη διάρκεια της εκπόνησης της διπλωματικής εργασίας καθώς και για τις άκρως χρήσιμες και εποικοδομητικές υποδείξεις κατά τη συγγραφή της.

Επιπλέον, θα ήθελα να ευχαριστήσω θερμά όλους τους διδάσκοντες καθηγητές του Προγράμματος Μεταπτυχιακών Σπουδών (ΠΜΣ) «Δίκαιο και Πληροφορική», αφενός του Τμήματος Νομικής του [Δημοκρίτειου Πανεπιστημίου Θράκης] σφετέρου του Τμήματος Εφαρμοσμένης Πληροφορικής του [Πανεπιστημίου Μακεδονίας], για την χρήσιμη καθοδήγηση και υποστήριξη αλλά και για τις πολύτιμες γνώσεις που μου παρείχαν, καθ' όλη τη διάρκεια φοίτησης μου στο πρόγραμμα.

Η ΣΕΛΙΔΑ ΑΥΤΗ ΕΙΝΑΙ ΣΚΟΠΙΜΑ ΛΕΥΚΗ

1. Εισαγωγή

Την τελευταία δεκαετία η τεχνολογική έκρηξη μας έχει φέρει όλους πιο κοντά στον παγκόσμιο ιστό και στην χρήση του ηλεκτρονικού υπολογιστή, ως εργαλείο που ικανοποιεί τις περισσότερες από τις καθημερινές μας ανάγκες. Στην σημερινή εποχή οι ηλεκτρονικοί υπολογιστές και το Διαδίκτυο (internet) παίζουν σημαντικό ρόλο στη ζωή των ανθρώπων[1].

Οι εγκληματίες δυστυχώς αυτή την τεχνολογική επανάσταση των τελευταίων ετών την αντιλήφθηκαν και άρχισαν να τη χρησιμοποιούν με απώτερο στόχο τη διευκόλυνση των εγκληματικών πράξεων τους.

Πολλά από τα εγκλήματα που διαπράττονται μέσα από τον Κυβερνοχώρο έχουν παραμείνει ίδια, με τη μόνη διαφορά ότι ο τόπος του εγκλήματος αλλάζει από έναν τόπο του πραγματικού κόσμου σε έναν διαδικτυακό. Επιπλέον έχουν αναπτυχθεί και νέες εγκληματικές πράξεις όπως για παράδειγμα η φθορά ψηφιακών δεδομένων κλοπή διαδικτυακής ταυτότητας (identity theft), , επιθέσεις άρνησης υπηρεσιών, online κλοπή κωδικών πιστωτικών καρτών κ.τ.λ.

Καθώς λοιπόν η τεχνολογία προχωράει αναπτύσσεται και ένα νέο είδος εγκληματικότητας με την χρήση της ψηφιακής τεχνολογίας και των ηλεκτρονικών υπολογιστών[2]. Αντικείμενο λοιπόν της παρούσας εργασίας αποτελεί η ανάπτυξη του θέματος - αντικειμένου με θέμα - τίτλο: {**«Ηλεκτρονικό - οικονομικό Έγκλημα στον Κυβερνοχώρο**»} το οποίο σχετίζεται με το έγκλημα στον Κυβερνοχώρο[3].

Το Internet, είναι ένα πλέγμα από εκατομμύρια διασυνδεδεμένους υπολογιστές, που επιτρέπει την ανταλλαγή δεδομένων πέρα από γεωγραφικά και κοινωνικά σύνορα.

---

[1] *Κρανιδώτη Μ.,* (Επιμ.), Νέες τεχνολογίες και ανθρώπινα δικαιώματα, Εκδ. Αντ. Ν. Σάκκουλα, 2008.

[2] Βλαχόπουλος Κ.,, Ηλεκτρονικό έγκλημα: μορφές, πρόληψη, αντιμετώπιση, 2007, σελ.7

[3] Γασπαρινάτου Μ., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΚΟΥΛΑΣ 2016 σελ. 1305 επ.

Οι πληροφορίες που διακινούνται στο Διαδίκτυο είναι σε ψηφιακή μορφή, δηλαδή συστοιχίες από τα δυαδικά ψηφία 0 και 1 και μπορεί να είναι υλικό πολυμέσων όπως βίντεο, ήχο, εικόνα αλλά και απλό κείμενο.

Το Διαδίκτυο αναφέρεται σε ένα σύνολο υπολογιστών και δικτύων που συνδέονται μεταξύ τους σε ένα παγκόσμιο δίκτυο έτσι ώστε να μπορούν να επικοινωνούν και να μοιράζονται πληροφορίες από απόσταση.

Εικόνα 1.- Σύνδεση Υπολογιστών

Το Internet είναι ένα από τα πιο αντιπροσωπευτικά και πιο επιτυχημένα παραδείγματα των ωφελειών που προκύπτουν από τη συνεχή επένδυση και αφοσίωση στην έρευνα και ανάπτυξη της υποδομής της πληροφορικής. Ουσιαστικά δεν ανήκει σε κανέναν και παράλληλα είναι προσβάσιμο σε όλους, χωρίς διακρίσεις. Εταιρείες, κυβερνήσεις, βιομηχανία και ακαδημαϊκή έρευνα κατέχουν ένα κομμάτι αυτής της υποδομής, αλλά δεν υπάρχει κανένας που να το κατέχει εξολοκλήρου[4].

Η τεχνολογία του είναι κυρίως βασισμένη στην διασύνδεση επιμέρους δικτύων ανά τον κόσμο με πολυάριθμα τεχνολογικά πρωτόκολλα, με κύριο το TCP/IP.

Ο αντίστοιχος αγγλικός όρος internet προκύπτει από τη σύνθεση λέξεων inter-network. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιούμενη μορφή του, με τους όρους Διαδίκτυο, Ιντερνέτ περιγράφεται σύνολο των διασυνδεδεμένων υπολογιστών και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του.

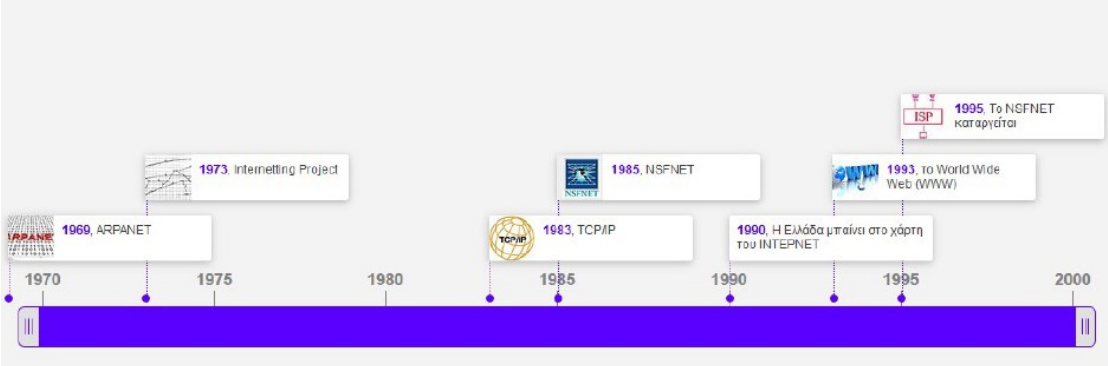
[4] Γασπαρινάτου Μ., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΚΟΥΛΑΣ 2016 σελ. 1305 επ.

Για την αποστολή των δεδομένων χρησιμοποιεί μεταγωγή πακέτων (packet switching) και το πρωτόκολλο TCP/IP.

2. Ιστορική αναδρομή και εξέλιξη του Κυβερνοχώρου

2.1 ARPAnet: ο πρόγονος του Διαδικτύου[5]

Το σημερινό Internet αποτελεί εξέλιξη του ARPANET (Advanced Research Projects Agency Network), ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του '60 στις ΗΠΑ.



Το δίκτυο ARPANET γεννιέται το 1969 με πόρους του προγράμματος ARPA του Υπουργείου Άμυνας, με σκοπό:

-- **να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς** και

-- **να αποτελέσει ένα πείραμα για τη μελέτη της αξιόπιστης λειτουργίας των δικτύων με την τεχνολογία της μεταγωγής πακέτων**.

Στην αρχική του μορφή, το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων (packet switching), σύμφωνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε «πακέτα» έχοντας ως αποτέλεσμα τη χρήση της ίδιας επικοινωνιακής γραμμής από πολλούς χρήστες.

[5] Γασπαρινάτου Μ., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΚΟΥΛΑΣ 2016 σελ. 1305 επ.

Στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων σημείων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας.

Έτσι, ο πρώτος κόμβος του δικτύου ARPANET εγκαταστάθηκε και λειτούργησε για πρώτη φορά το φθινόπωρο του 1969, στο University of California στο Los Angeles. Μέχρι το Δεκέμβριο του 1969, το δίκτυο αποτελούσαν συνολικά (4) τέσσερις κόμβοι, αφού προστέθηκαν τα ερευνητικά κέντρα από το University of Utah, το University of California της Santa Barbara και το ίδρυμα Stanford Research Institute International.

Το δίκτυο αυτό ονομάστηκε ARPAnet, προς τιμήν του στρατιωτικού χορηγού του. Οι υπερ-υπολογιστές των τεσσάρρων Πανεπιστημίων, είχαν τη δυνατότητα να ανταλλάσσουν δεδομένα μέσω ειδικών τηλεπικοινωνιακών γραμμών υψηλής ταχύτητας και μπορούσαν να προγραμματιστούν από απόσταση μέσω άλλων απομακρυσμένων κόμβων. Έτσι, οι επιστήμονες και οι ερευνητές της εποχής εκείνης, μπορούσαν να μοιράζονται ο ένας τους υπολογιστές των άλλων.

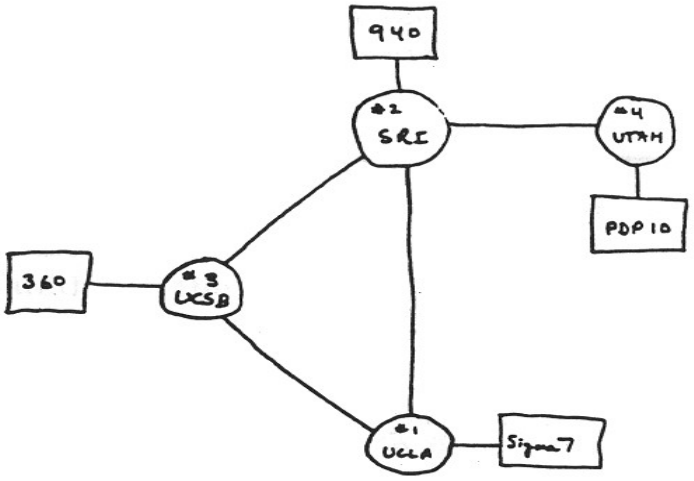


FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)

Εικόνα: Σχηματική παρουσίαση της αρχικής μορφής του ARPANET

Μέσα στη δεκαετία του '70 το ARPAnet αναπτύχθηκε. Περισσότεροι κόμβοι συνδέθηκαν και πλέον μεγαλύτερος αριθμός χρηστών χρησιμοποιούσαν καθημερινά τις υπηρεσίες του δικτύου. Οι χρήστες δεν προέρχονταν πια μόνο από Ακαδημαϊκές κοινότητες και ιδρύματα. Εξαιτίας όμως της δομής του δικτύου, οποιοσδήποτε μπορούσε να συνδεθεί σε αυτό, εφόσον διέθετε έναν υπολογιστή, αλλά κι ένα λογαριασμό (άδεια πρόσβασης) σε κάποιον πανεπιστημιακό υπολογιστή, με σκοπό την επικοινωνία και την ανταλλαγή απόψεων και πληροφοριών.

Επιστήμονες και ερευνητές αποτέλεσαν τους πρώτους χρήστες του δικτύου καθώς μπορούσαν να χρησιμοποιήσουν ο ένας τον υπολογιστή του άλλου από μεγάλη απόσταση και να εκμεταλλευτούν τις δυνατότητες του.

Πιο δημοφιλής εφαρμογή του συστήματος αναδείχτηκε πολύ γρήγορα το e-mail. Έτσι, το ARPAnet μετατράπηκε σε ένα ταχύτατο ηλεκτρονικό ταχυδρομείο, καθώς το χρησιμοποιούσαν για συνεργασία σε ερευνητικά προγράμματα, αλλά και για συζητήσεις πάνω σε θέματα ποικίλου ενδιαφέροντος.

2.2 Από το ARPANET στο INTERNET: TCP/IP6

Το 1973 ξεκίνησε από τους ερευνητές της ARPA, ένα νέο ερευνητικό πρόγραμμα με στόχο την διασύνδεση πιθανώς ανόμοιων δικτύων και την ομοιόμορφη μεταφορά δεδομένων από το ένα δίκτυο στο άλλο. Το πρόγραμμα αυτό ονομάστηκε Internetting Project (Πρόγραμμα Διαδικτύωσης) και από την έρευνα γεννιέται μια νέα τεχνική, το Internet Protocol (IP) (Πρωτόκολλο Διαδικτύωσης), από την οποία θα πάρει αργότερα το όνομά του το Internet[7].

Έναν χρόνο αργότερα, ολοκληρώθηκε η ανάπτυξη μίας κοινής "γλώσσας" που θα επέτρεπε στα διαφορετικά αυτά δίκτυα να επικοινωνούν μεταξύ τους. Η γλώσσα αυτή έγινε γνωστή ως Transmission Control Protocol (TCP) (Πρωτόκολλο Ελέγχου Μετάδοσης) και η ανάπτυξή της σηματοδότησε μία κρίσιμη καμπή στην ανάπτυξη των δικτύων ενώ παράλληλα ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (E-mail).

Το 1983, το πρωτόκολλο TCP/IP (δηλ. ο συνδυασμός των TCP και IP) αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ.

Η έκδοση του λειτουργικού συστήματος Berkeley UNIX, το οποίο περιλαμβάνει το TCP/IP, συντελεί στη γρήγορη εξάπλωση της διαδικτύωσης των υπολογιστών, με αποτέλεσμα εκατοντάδες Πανεπιστήμια να συνδέσουν τους υπολογιστές τους στο ARPANET, το οποίο επιβαρύνεται πολύ. Το 1983, χωρίζεται σε δύο τμήματα:

- στο MILNET (για στρατιωτικές επικοινωνίες) και
- στο νέο ARPANET (για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση)[8].

Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το NSFNET χρησιμοποιώντας το πρωτόκολλο TCP/IP και στα τέλη της δεκαετίας του '80, όλο και περισσότερες χώρες συνδέονται στο NSFNET (Καναδάς, Γαλλία, Σουηδία, Αυστραλία, Γερμανία, Ιταλία, κ.α.).

---

[6] Tanenbaum, A. (2011*) Computer Networks*, 5th Edition, Pearson.
[7] https://www.lifo.gr/articles/technology_articles/168993
[8] https://www.sutori.com/story/e-istoria-tou-internet--zYdjkNDuzTpjB8uamiiuT1Cj

Πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο, το οποίο αρχίζει να γίνεται γνωστό σαν INTERNET και να εξαπλώνεται με ταχύτατους ρυθμούς σε ολόκληρο τον κόσμο. Επακόλουθο ήταν το έτος 1990 να καταργηθεί το ARPANET.

2.3 Παγκόσμιος Ιστός (World Wide Web – WWW) -Ένα παγκόσμιο δίκτυο για όλους

Το 1993 το ερευνητικό ίδρυμα CERN στην Ελβετία παρουσιάζει την υπηρεσία του Παγκόσμιου Ιστού (World Wide Web) που αναπτύχθηκε από τον Tim Berners - Lee .Αυτή είναι ουσιαστικά η "πλατφόρμα", η οποία κάνει εύκολη την πρόσβαση στο Internet, ακόμα και στη μορφή που είναι γνωστό σήμερα[9].

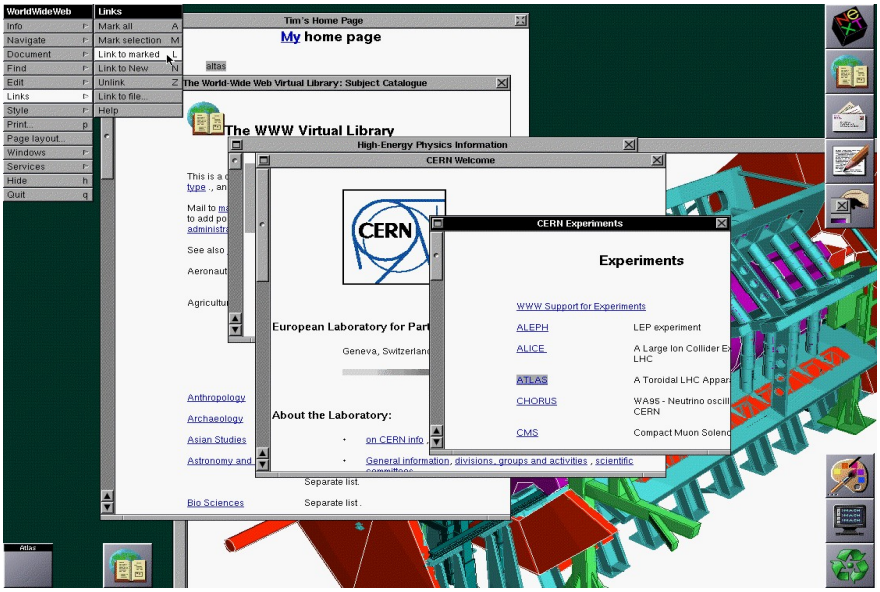
Στόχος της υπηρεσίας του Παγκόσμιου Ιστού ήταν η δημιουργία ενός δικτύου- συστήματος διασύνδεσης πληροφοριών, σε μορφή πολυμέσων (multimedia), που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι και θα επέτρεπαν την αναζήτηση και μεταφορά των πληροφοριών που περιέχουν μέσω ενός ειδικού πρωτοκόλλου που έγινε γνωστό ως Hypertext Transfer Protocol (HTTP).

Έναν χρόνο αργότερα, ο Tim Berners - Lee ανέπτυξε ένα πρόγραμμα "browser / editor", το οποίο ονόμασε World Wide Web.

Το επόμενο βήμα ήταν η ανάπτυξη ενός βελτιωμένου "browser", δηλαδή ενός συστήματος που θα επέτρεπε σε συνδέσμους (links) να "κρύβονται" μέσα στο κείμενο και για το σκοπό αυτό χρησιμοποίησε τη γλώσσα HyperText Markup Language (HTML)[10]. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη.

[9]https://www.retrocomputers.gr/forum/istoria-ypologiston-software-ktl/2104-istoria-tou-internet

[10] http://www.epaggelmaties.com/writer/2001-2003/intemethistory.html



Εικόνα 2.3: Ο πρώτος browser

Η δοκιμαστική έκδοσή του παραχωρήθηκε δωρεάν σε διάφορα πανεπιστήμια και σύντομα γνώρισε τεράστια διάδοση. Έως το 1994 δεκάδες χιλιάδες αντίγραφά του είχαν εγκατασταθεί σε υπολογιστές παγκοσμίως ενώ παράλληλα, εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Internet (Internet Service Providers - ISP) και προσφέρουν πρόσβαση στο Internet για όλους.

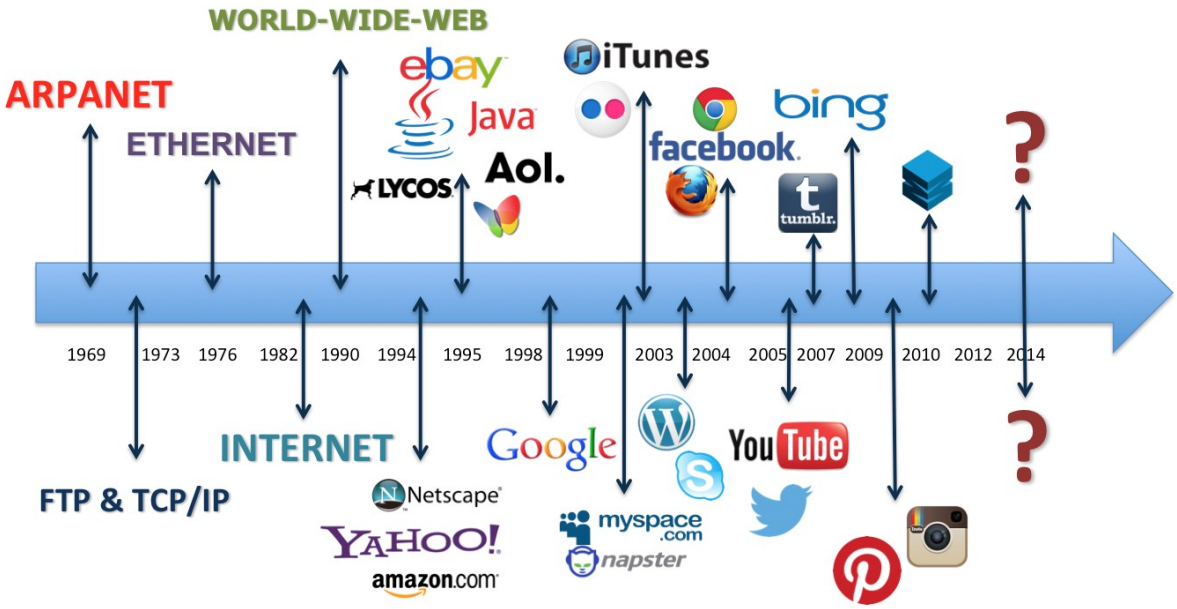
Οι υπηρεσίες που παρείχε το World Wide Web οδήγησαν όχι μόνο στην περαιτέρω ανάπτυξη του, αλλά και στην εξάπλωση των προσωπικών υπολογιστών, καθώς η ευκολία απόκτησης πρόσβασης στο Internet προσέλκυσε ένα μεγάλο αριθμό χρηστών και έφερε την "έκρηξη" των τελευταίων χρόνων.

Σημαντικές στιγμές στην ιστορία του Διαδικτύου

Σύντομη Ιστορική Ανασκόπηση

- **1940:** Σύνδεση δύο υπολογιστών και ανταλλαγή δεδομένων με τηλέτυπο
- **1960 - 1970:** Αναπτύσσονται τα πρώτα δίκτυα υπολογιστών
- **1980 - 1990:** Εκρηκτική διάδοση των δικτύων – Διαδίκτυο
- **1991:** Επινόηση του World Wide Web

Σχηματικά, οι σημαντικότερες εταιρείες / υπηρεσίες και τα προϊόντα τους εμφανίζονται στο ακόλουθο χρονολόγιο[11]:



Εικόνα 2.4: Χρονολόγιο Υπηρεσιών Διαδικτύου

2.4 Η Αρχή της Ουδετερότητας του Διαδικτύου

Το Διαδίκτυο είναι αποκεντρωμένο και αυτοδιαχειριζόμενο. Δεν υπάρχει δηλαδή κάποιος κεντρικός οργανισμός που να το διευθύνει και να παίρνει

[11]https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUKEwjc5bnj__HmAhUSL1AKHaUaD1IQjRx6BAgBEAQ&url=https%3A%2F%2Fmalonemediagroup.com%2Fhistory-of-the-internet-timeline-an-ever-evolving-digital-world%2F&psig=AOvVaw1oDLvcmnF06lHQ7D3ZC2xj&ust=1578503992207802

αποφάσεις σχετικά με το είδος των πληροφοριών που διακινούνται, τις υπηρεσίες που παρέχονται από τους διάφορους υπολογιστές του ή τη διαχείρισή του[12].

Βασική και Θεμελιώδη αρχή που ισχύει στο Διαδίκτυο είναι η Αρχή της Ουδετερότητας του Διαδικτύου (**net neutrality)**, η οποία σημαίνει ότι η πρόσβαση σε όλες τις ιστοσελίδες και τις διαδικτυακές υπηρεσίες θα πρέπει να είναι:

- ίση και
- να μην καταλαμβάνεται από διακρίσεις με βάση τον χρήστη, το περιεχόμενο,τον ιστότοπο, την πλατφόρμα κλπ

2.5 Η ελεύθερη πρόσβαση στο διαδίκτυο ως βασικό ανθρώπινο δικαίωμα

Με πρόσφατο ψήφισμα[13] του ΟΗΕ, αναγνωρίστηκε η ελευθερία πρόσβασης στο Διαδίκτυο ως βασικό ανθρώπινο δικαίωμα.

Η Γενική Συνέλευση του ΟΗΕ στο εν λόγω ψήφισμά της, επικυρώνει ομόφωνα (με κάποιες επιμέρους ενστάσεις από χώρες) τη δέσμευση της διεθνούς κοινότητας στην προστασία της ελεύθερης πρόσβασης στο διαδίκτυο, ως βασικό αγαθό για όλους. Ταυτόχρονα, αναφέρεται ρητά, για πρώτη φορά, στην ανάγκη "προστασίας, προώθησης και άσκησης των ανθρωπίνων δικαιωμάτων στο διαδίκτυο". Επιπλέον, καταδικάζει κάθε χώρα που εκ προθέσεως περιορίζει την ελεύθερη πρόσβαση των πολιτών στο διαδίκτυο.

Το ψήφισμα έρχεται να συμπληρώσει και να αποσαφηνίσει το γενικότερο πλαίσιο της Χάρτας των Δικαιωμάτων του Ανθρώπου στο πλαίσιο του διαδικτύου και των ΤΠΕ, ιδιαίτερα σε ό,τι αφορά:

(α) την ελευθερία έκφρασης,

(β) το δικαίωμα πρόσβασης στην εκπαίδευση,

[12] http://www.uth.gr/main/help/help-desk/internet/internet2.html
[13] https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

(γ) την ελευθερία πρόσβασης στην πληροφορία,

(δ) το δικαίωμα της συνάθροισης και της συνεργασίας μέσω του διαδικτύου,

(ε) το δικαίωμα προστασίας της ιδιωτικότητας,

(στ) το δικαίωμα πρόσβασης στις νέες τεχνολογίες ως μέσο κοινωνικής και οικονομικής ανάπτυξης & ευημερίας.

Η βασική θέση που διατυπώνεται πλέον είναι ότι όλα τα ανθρώπινα δικαιώματα που ισχύουν στον πραγματικό κόσμο πρέπει να προστατεύονται εξίσου και στον ψηφιακό κόσμο. Επίσης, καλεί όλα τα κράτη να συμβάλλουν αποφασιστικά στην τήρηση των διεθνών υποχρεώσεών τους σχετικά με τα ζητήματα ασφάλειας σε ό,τι αφορά την ελευθερία έκφρασης, συνεργασίας και ιδιωτικότητας, ώστε το διαδίκτυο να παραμείνει ανοικτό, παγκόσμιο και διαλειτουργικό μέσο προσβάσιμο σε όλους.

3. Ηλεκτρονικό – Πληροφοριακό έγκλημα

Πώς όμως ορίζεται το «**Κυβερνοέγκλημα**» (Cybercrime) και το «**Ηλεκτρονικό έγκλημα**» (Computer crime);

Για την ακριβής σημασία των όρων υπάρχουν διχογνωμίες. Είναι αλήθεια ότι η χρήση των υπολογιστών και των τεχνολογιών της πληροφορικής κατέστησαν δυνατή τη διάπραξη κάθε εγκληματικής πράξης. Σε πολλές περιπτώσεις η χρήση των υπολογιστών δεν αλλάζει το θεμελιακό χαρακτήρα ενός αδικήματος - μία δωροδοκία παραμένει δωροδοκία ανεξάρτητα εάν τα χρήματα δίνονται με ηλεκτρονικό τρόπο - παρά το γεγονός ότι η χρήση του υπολογιστή μπορεί να επηρεάζει το βαθμό του αδικήματος.[14]

Πρέπει εισαγωγικά να σημειωθεί ότι το «ηλεκτρονικό έγκλημα» προηγείται χρονικά και λογικά της κατηγορίας των κυβερνοεγκλημάτων.

Κατά τον V. Zur Muhlen εγκληματικότητα δια μέσου των υπολογιστών "*αποτελεί κάθε εγκληματική συμπεριφορά στην οποία ο υπολογιστής είναι εργαλείο ή σκοπός της πράξης*"[15]

Σύμφωνα με τον ορισμό που προτείνει ο Donn Parker[16] ως computer crime μπορεί να θεωρηθεί μία εγκληματική πράξη για την επιτυχή τέλεση της οποίας είναι αναγκαία η γνώση των υπολογιστών.

Η **Interpol** ονομάζει το ηλεκτρονικό έγκλημα ως ψηφιακό (digital crime) και το χωρίζει σε τρεις κατηγορίες :

- στο ηλεκτρονικό έγκλημα, το οποίο περιλαμβάνει την πειρατεία, την κλοπή δεδομένων και την κλοπή χρόνου, το λεγόμενο computer break-ins

[14] Lilian Mitrou , "Cybercrime" and computer crime": Lecture Notes in Postgraduate Programme" Techno-economic Management & Security of Digital Systems", Department of Digital Systems, University of Piraeus

[15] Ορισμοί οι οποίοι έχουν κυριαρχήσει από το 1970 και μετά είναι του Muhlen(1971) Parker (1973) Sieber (1986) Wsik (1991). Παρουσιάζονται αναλυτικά στο Λάζος Γ. (2001): Πληροφορική και Έγκλημα, Αθήνα , Νομική Βιβλιοθήκη

[16] Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual. Technical Report OJP-86-C-002, U.S. Department of Justice, National Institute of Justice, Office of Justice Program. 2nd edition

- στο έγκλημα διαδικτύου, το οποίο περιλαμβάνει την παιδική πορνογραφία, την αγορά και πώληση ναρκωτικών, το ξέπλυμα χρήματος
- στο ηλεκτρονικό έγκλημα, το οποίο σχετίζεται με τραπεζικές απάτες

Σύμφωνα με τον **Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.)** η εγκληματικότητα μέσω των υπολογιστών, σύμφωνα με ορισμό που έδωσε το 1986, ορίζεται ότι: "*πληροφορικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων (data) ή/και τη μετάδοση δεδομένων*"[17]

3.1 Ορισμός του Κυβερνοεγκλήματος[18]

Τι είναι το κυβερνοέγκλημα; Είναι γεγονός ότι δεν υφίσταται ένας γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο[19]. Διαφορετικοί οργανισμοί και φορείς υιοθετούν διαφορετικούς ορισμούς. Για παράδειγμα, ο ορισμός που δίνεται από τις Αρχές επιβολής του Νόμου είναι διαφορετικός από αυτόν που δίνεται από τα CERTs (Computer Emergency Response Teams).

Άλλοι σχετικοί όροι που χρησιμοποιούνται διεθνώς για τα εγκλήματα του κυβερνοχώρου είναι: ηλεκτρονικά εγκλήματα (electronic crimes), online εγκλήματα (online crimes), εγκλήματα Διαδικτύου (internet crimes), ψηφιακά εγκλήματα (digital crimes), εγκλήματα νέων τεχνολογιών (new technology crimes), κυβερνοεγκλήματα (cyber crimes). Το πρόθεμα κυβερνο- (cyber-) συχνά παρατίθεται δίπλα σε λέξεις αδικημάτων, υποδεικνύοντας ότι το έγκλημα αφορά τον ψηφιακό κόσμο: κυβερνο-εκφοβισμός, κυβερνο-εκβιασμός, κυβερνο-τρομοκρατία κ.α.. Είναι σαφές, δηλαδή, ότι υπάρχει δυσκολία ως προς την αποτύπωση των κυβερνοεγκλημάτων σε νομικά κείμενα σε διαφορετικές γλώσσες και σε διαφορετικά Κράτη.

---

[17] Βλ. OECD Computer related crime : An analysis of legal policy, Paris: OECD, 1986

[18] Γασπαρινάτου Μ., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΟΥΛΑΣ 2016 σελ. 1305 επ.

[19] 'Αλλοι σχετικοί όροι που χρησιμοποιούνται διεθνώς είναι: electronic crime, on line crime, digital crime, communication crime, high-tech crime, information technology crime κλπ.

Εικόνα 3.1: Σχηματική αποτύπωση cyber-crime

Η Σύμβαση για τα εγκλήματα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης), του 2001, χρησιμοποιεί έναν ορισμό για το κυβερνοέγκλημα που βασίζεται στο ποια εγκλήματα θα έπρεπε να συμπεριληφθούν σε αυτόν (αντί να δώσει έναν ακριβή ορισμό). Σε αυτόν περιλαμβάνονται:

α) εγκλήματα κατά της **εμπιστευτικότητας** (confidentiality), **ακεραιότητας** (integrity) και **διαθεσιμότητας** (availability) ψηφιακών δεδομένων και συστημάτων υπολογιστών (παράνομη πρόσβαση, υποκλοπή, παρέμβαση σε δεδομένα και συστήματα),

β) εγκλήματα **σχετικά με το περιεχόμενο**, για διακίνηση παιδικής πορνογραφίας

γ) εγκλήματα **σχετιζόμενα με υπολογιστές** (computer related offences) (λ.χ. πλαστογραφία ή απάτη με χρήση υπολογιστή),

δ) εγκλήματα σχετικά με **παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων** (offences related to infringement of Copyright and related rights).

Επειδή πρόκειται για κείμενο που γράφτηκε το 2001, πολλές μορφές κυβερνοεγκλήματος που έχουν εμφανιστεί έκτοτε, δε μπορούν να ενταχθούν στις τέσσερις προαναφερθείσες κατηγορίες.

Τα εγκλήματα του κυβερνοχώρου αποτελούν υποκατηγορία του κυβερνοεγκλήματος και διακρίνονται σε τρεις μεγάλες κατηγορίες[20]:

- Γνήσια-παραδοσιακά εγκλήματα, όπως η απάτη και η πλαστογραφία, που τελούνται μέσω ηλεκτρονικών υπολογιστών και συστημάτων πληροφοριών
- εγκλήματα που τελούνται αποκλειστικά σε ψηφιακό περιβάλλον, όπως επιθέσεις εναντίον πληροφοριακών συστημάτων, επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service) και hacking.
- εγκλήματα με ψηφιακό περιεχόμενο που μεταδίδεται μέσω συστημάτων πληροφοριών (για παράδειγμα υλικό σεξουαλικής εκμετάλλευσης ανηλίκων ή ρατσιστικός λόγος),

3.2 Τύποι-μορφές κυβερνοεγκλημάτων[21]

Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες[22], κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω κατηγορίες[23]:

1. Παρεμπόδιση (κυβερνο) κυκλοφορίας
2. Πλαστογραφία
3. Τροποποίηση και Κλοπή δεδομένων
4. Μη εξουσιοδοτημένη πρόσβαση
5. Εισβολή και Σαμποτάζ σε δίκτυο
6. Υπόθαλψη αδικημάτων
7. Διασπορά ιών
8. Απάτη

Μία περαιτέρω τυπολογία των διαφορετικών μορφών κυβερνοεγκλημάτων που συναντάμε, είναι η ακόλουθη[24]:

[20] Βλαχόπουλος Κ., Ηλεκτρονικό έγκλημα: μορφές, πρόληψη, αντιμετώπιση, 2007, σελ.7
[21] Γασπαρινάτου Μ., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΟΥΛΑΣ 2016 σελ. 1305 επ.
[22] https://www.library.cornell.edu/colldev/mideast/cycrime.pdf,. Νοέμβρ. 2019
[23] Σφακιανάκης Ε., Ο κώδικας του Διαδικτύου, εκδ. All about Internet, Αθήνα 2016, σελ. 32-42

- παράνομη πρόσβαση σε υπολογιστικά συστήματα (hacking & cracking – συχνά με εκμετάλλευση ευπαθειών του συστήματος),
- αποστολή μη ζητηθείσας αλληλογραφίας (spamming), δηλαδή αποστολή πολλαπλών μηνυμάτων ηλεκτρονικού ταχυδρομείου, συνήθως με τη χρήση μολυσμένων υπολογιστών (botnet),
- ανάπτυξη και διασπορά κακόβουλου κώδικα (όπως ιούς και Trojans, που προκαλούν βλάβη σε υπολογιστικά συστήματα, ή χρησιμοποιούνται για τη διάπραξη άλλων εγκλημάτων),
- εγκλήματα σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας (για παράδειγμα βιομηχανική κατασκοπεία ή διαμοιρασμός περιεχομένου που προστατεύεται από τη νομοθεσία περί πνευματικής ιδιοκτησίας, χωρίς σχετική άδεια – εικόνες, μουσική, ταινίες)δορυφορική πειρατεία,
- hacking, με σκοπό την υποκλοπή δεδομένων, τη διασπορά κακόβουλου λογισμικού ή την απόπειρα εκβίασης,
- πειρατεία λογισμικού,
- εγκλήματα βασισμένα στη λειτουργία δικτύων (λόγου χάρη phishing – μια προσπάθεια εξαπάτησης χρηστών μέσω ψεύτικων απεικονίσεων – και υποκλοπή ταυτότητας).
- επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (Distributed Denial of Service - DDoS)[25], ήτοι ένας τρόπος αποστολής υπερβολικά μεγάλου αριθμού αιτημάτων στον εξυπηρετητή, που οδηγεί σε κατάρρευση μιας ιστοσελίδας,
- πρόσβαση σε δίκτυα υπολογιστών, με τη χρήση τεχνικών
- phreaking (μη εξουσιοδοτημένη χρήση συστημάτων τηλεφωνικής επικοινωνίας, είτε για την πραγματοποίηση δωρεάν τηλεφωνικών κλήσεων, είτε για την ανώνυμη επικοινωνία μεταξύ μελλών μιας εγκληματικής οργάνωσης),

---

[24] Σφακιανάκης Ε., Ο κώδικας του Διαδικτύου, εκδ. All about Internet, Αθήνα 2016, σελ. 32-42

[25] **Μαυρίδης** Ι., Ασφάλεια Πληροφοριών στο Διαδίκτυο., Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών . Ελληνικά ακαδημαϊκά Ηλεκτρονικά συγγράμματα και βοηθήματα. Προσπελάσιμο στην https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&ved=2ahUKEwjHzZmSpIrnAhWJwAIHHbEKCS8QFjAOegQIAxAB&url=https%3A%2F%2Frepository.kallipos.gr%2Fbitstream%2F11419%2F1024%2F2%2F00_master_document-KOY.pdf&usg=AOvVaw0KHZe3ZyF3KkxS1jcyeMYu., Νοέμβριος. 2019, σελ. 40 επ.

- κατοχή και διαμοιρασμός υλικού σεξουαλικής εκμετάλλευσης ανηλίκων,

Μια πράξη μπορεί να ανήκει ταυτόχρονα σε πολλές από τις παραπάνω κατηγορίες εγκλημάτων: η πειρατεία λογισμικού συνδυάζεται με τον παράνομο διαμοιρασμό αρχείων ενώ οι επιθέσεις phishing απαιτούν την αποστολή μη ζητηθείσας αλληλογραφίας (spamming)[26].

Στην Ελλάδα συγκεκριμένα έχουν εξιχνιασθεί οι εξής μορφές κυβερνοεγκλημάτων από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος[27]:

1. Παιδική πορνογραφία
2. Παραβίαση προσωπικών δεδομένων
3. Cracking and Hacking
4. Οικονομικά Εγκλήματα (Απάτες μέσω Διαδικτύου κ.τ.λ.)
5. Εγκλήματα που παραβιάζουν την πνευματική ιδιοκτησία
6. Διακίνηση ναρκωτικών-φαρμάκων
7. Κλοπή Διαδικτυακής Ταυτότητας
8. Κοινά/παραδοσιακά εγκλήματα που διαπράττονται με την χρήση του διαδικτύου (εξυβρίσεις, απειλές κ.τ.λ.)

3.3 Χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο

Το έγκλημα στον Κυβερνοχώρο με το συμβατικό έγκλημα διαφοροποιούνται μεταξύ τους από τα ακόλουθα χαρακτηριστικά γνωρίσματα[28]:

✔ Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σε όσους έχουν ροπή ή τάση στην παιδοφιλία ή χρήση παιδικής πορνογραφίας (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο,

[26] Αναστάσιος Παπαθανασίου / Γεώργιος Γέρμανος, «*Αντιμετωπίζοντας το Κυβερνοέγκλημα. Μελλοντικές τάσεις και απειλές*», 1ο Παγκύπριο Συνέδριο Ποινικού Δικαίου και Εγκληματολογίας που διοργανώθηκε από το Τμήμα Νομικής και το Ινστιτούτο Ποινικών Σπουδών και Εγκληματολογίας (ICSC) του Πανεπιστημίου Λευκωσίας (UNic) και το Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών (ΕΠ & ΕΕ) του Εθνικού Καποδιστριακού Πανεπιστημίου Αθηνών (ΕΚΠΑ)

[27] Σφακιανάκης Ε., Ο κώδικας του Διαδικτύου, εκδ. All about Internet, Αθήνα 2016, σελ. 32-42

[28] Σφακιανάκης Ε., Ο κώδικας του Διαδικτύου, εκδ. All about Internet, Αθήνα 2016, σελ. 21-23

χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (News groups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (IRC- Internet Relay Chat),

✔ Το έγκλημα στον κυβερνοχώρο αποτελεί την πιο γρήγορη διάδοση μορφής εγκλήματος καθώς τελείται στιγμιαία, ανώνυμα και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα,

✔ Είναι έγκλημα "χωρίς πατρίδα"[29], παρότι τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους ανεξαρτήτου εδαφικού περιορισμού,

✔ Οι "εγκληματίες του κυβερνοχώρου" πολλές φορές χρησιμοποιούν ψευδή στοιχεία για να προσελκύσουν τα υποψήφια θύματά τους π.χ. αποστέλλουν ηλεκτρονικά μηνύματα ή επιστολές (e- mail) ανωνύμως ή και με ψευδή στοιχεία,

✔ Είναι εύκολο να διαπραχθεί αλλά δύσκολο να εντοπιστεί γιατί συχνά δεν αφήνει ίχνη (όπως στα κοινά εγκλήματα είναι τα δακτυλικά αποτυπώματα)[30],

✔ Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις, και μπορεί να διαπραχθεί χωρίς την φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του,

✔ Κατά κανόνα είναι πολύ δύσκολο να προσδιοριστεί ο (πραγματικός) τόπος τελέσεως του. Από τεχνικής και νομικής άποψης είναι ακόμα πιο δύσκολο να εντοπιστεί ο δράστης[31] και να συγκεντρωθούν όλα τα αποδεικτικά στοιχεία λόγω του διασυνοριακού χαρακτήρα

---

29 http://www.crimetimes.gr/%CE%B4%CE%B9%CE%B5%CF%8D%CE%B8%CF%85%CE%BD%CF%83%CE%B7-%CE%B4%CE%AF%CF%89%CE%BE%CE%B7%CF%82-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%BF%CF%8D-%CE%B5%CE%B3%CE%BA%CE%BB%CE%AE/., προσπελάσιμο Νοέμβρ. 2019

30 https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-4411-2016

31 **Μαυρίδης** Ι., Ασφάλεια Πληροφοριών στο Διαδίκτυο., Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών . Ελληνικά ακαδημαϊκά Ηλεκτρονικά συγγράμματα και βοηθήματα. Προσπελάσιμο στην https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&ved=2ahUKEwjHzZmSpIrnAhWJwAIHHbEKCS8QFjAOegQIAxAB&url=https%3A%2F%2Frepository.kallipos.gr%2Fbitstream%2F11419%2F1024%2F2%2F00_master_document-KOY.pdf&usg=AOvVaw0KHZe3ZyF3KkxS1jcyeMYu., Νοέμβριος. 2019, σελ. 40 επ.

✔ Κατά κανόνα για την διερεύνησή του απαιτείται συνεργασία δύο τουλάχιστον εκείνου που γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και σε εκείνου όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία.

✔ Για την Αστυνομική διερεύνησή γενικότερα, και τις δικαστικές αρχές, απαιτείται άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

✔ Δεν υπάρχουν επαρκή στατιστικά στοιχεία, για το έγκλημα στο Διαδίκτυο καθώς ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου (cyber-crimes) καταγγέλλονται. Και αυτό για να μην αμφισβητείται η αξιοπιστία των θυμάτων που συνήθως είναι εταιρείες.

✔ Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα διότι είναι ελάχιστες οι καταγγελλόμενες υποθέσεις.

3.4 Εύρος του κυβερνοεγκλήματος

Με δεδομένο το πλήθος των διαφορετικών ορισμών του κυβερνοεγκλήματος, είναι αναπόφευκτη η διαφωνία ως προς το πραγματικό εύρος του κυβερνοεγκλήματος τόσο στην Ευρώπη όσο και στον υπόλοιπο κόσμο.

Στα περισσότερα Κράτη, τα σχετικά δεδομένα – όπου υπάρχουν – προέρχονται από καταγεγραμμένα στατιστικά των Αρχών επιβολής του Νόμου. Επιπλέον στοιχεία μπορεί να δημοσιεύονται έπειτα από έρευνες ιδιωτικών οργανισμών και φορέων. Η χρήση των στατιστικών που προέρχονται από τις εισαγγελικές και δικαστικές Αρχές εγείρει προβληματισμούς, καθώς η μεταξύ των κρατών νομοθεσία διαφέρει στα εγκλήματα που τελούνται στον κυβερνοχώρο.

Εξίσου διαφέρουν και οι εκτιμήσεις σχετικά με τις οικονομικές επιπτώσεις του κυβερνοεγκλήματος[32] (σε οργανισμούς, σε Κράτη και σε μεμονωμένα άτομα), διότι:

[32] Προστασία Κρίσιμων Πληροφοριακών και επικοινωνιακών Υποδομών της Δημόσιος Διοίκησης: Στρατηγικός σχεδιασμός,. Επιστημονική επιμέλεια Γκρίτζαλης Δ., Μήτρου

- οι επιχειρήσεις προτιμούν να μη δημοσιοποιήσουν περιστατικά που τους αφορούν,
- τα θύματα δεν καταγγέλλουν ένα έγκλημα, είτε γιατί η απώλεια είναι μικρή, είτε γιατί νιώθουν ντροπή
- είναι δύσκολη η ποσοτικοποίηση ορισμένων μορφών κυβερνοεγκλήματος (π.χ. επιθέσεις DDoS)[33],

Συχνά το φως της δημοσιότητας βλέπουν εκθέσεις ιδιωτικών επιχειρήσεων (π.χ. εταιρείες anti-virus), τα στοιχεία των οποίων, βασίζονται σε δεδομένα που προέρχονται από τους πελάτες. Άρα ούτε σε αυτή την περίπτωση είναι φρόνιμη η γενίκευση των συμπερασμάτων.

Παρ' όλα αυτά, δεν υπάρχει αμφιβολία ότι το κυβερνοέγκλημα γνωρίζει **παγκόσμια αύξηση και διάδοση[34].** Αυτό συμβαίνει διότι:

- από τη φύση του, το κυβερνοέγκλημα είναι διασυνοριακό και έτσι η διερεύνηση υποθέσεων από τις Αρχές επιβολής του Νόμου είναι εξαιρετικά δύσκολη,
- το ρίσκο που παίρνουν οι κυβερνοεγκληματίες είναι σχετικά μικρό, λόγω της ανωνυμίας που μπορούν να χρησιμοποιήσουν στον κυβερνοχώρο,
- ο αριθμός των συσκευών που διασυνδέονται και αποκτούν τη δυνατότητα επικοινωνίας διαρκώς αυξάνεται, άρα μακραίνει και ο κατάλογος των υποψήφιων θυμάτων,
- είναι εξαιρετικά προσοδοφόρο (γιατί να διαπράξει κάποιος μια ληστεία σε τράπεζα, όταν μπορεί να αφαιρέσει ένα ευρώ από λογαριασμούς εκατομμυρίων χρηστών του Διαδικτύου;).

Ν.,Σουλαρίδου Β., Σεπτέμβριος 2008., προσπελάσιμο στην https://www.infosec.aueb.gr/CIS_Reviews/reviews/1580eGovFor_CICIP.pdf

[33] **Μαυρίδης** Ι., Ασφάλεια Πληροφοριών στο Διαδίκτυο., Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών . Ελληνικά ακαδημαϊκά Ηλεκτρονικά συγγράμματα και βοηθήματα. Προσπελάσιμο στην https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&ved=2ahUKEwjHzZmSpIrnAhWJwAIHHbEKCS8QFjAOegQIAxAB&url=https%3A%2F%2Frepository.kallipos.gr%2Fbitstream%2F11419%2F1024%2F2%2F00_master_document-KOY.pdf&usg=AOvVaw0KHZe3ZyF3KkxS1jcyeMYu., Νοέμβριος. 2019, σελ. 40 επ.

[34] Ηλεκτρονικό Έγκλημα -Υπ. Εσωτερικών και Διοικητικής Ανασυγκρότησης - Ελληνική Αστυνομία. (n.d.). προσπελάσιμο Νοέμβριος 2019, από https://repository.kallipos.gr/bitstream/11419/1037/1/05_chapter_13.pdf

3.5 Διερεύνηση Κυβερνοεγκλήματος και Ψηφιακών Εγκλημάτων [35]

Κάθε χρήστης του διαδικτύου (internet) αφήνει κατά την πλοήγησή του σε αυτό ηλεκτρονικά ίχνη τα οποία αποτελούν την ταυτότητά του (ηλεκτρονική) και η οποία είναι **μοναδική στην παγκόσμια διαδικτυακή κοινότητα**[36].

Η μοναδικότητα κάθε ηλεκτρονικού ίχνος απαρτίζεται από τρία (3) μέρη:

α) την **ημεροχρονολογία,**

β) την **διεύθυνση πρωτοκόλλου IP Address** και

γ) τη **ζώνη ώρας**.

Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του ηλεκτρονικού ίχνους του δράστη, το οποίο είναι **μοναδικό για κάθε χρήστη** και αποτελεί **σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο**.

3.6 Το σκοτεινό διαδίκτυο (deep web)

Το σκοτεινό διαδίκτυο (deep web)[37] αποτελεί ένα γιγάντιο μέρος του Διαδικτύου που δεν είναι προσβάσιμο μέσω της τακτικής αναζήτησης από την Google ή από άλλες μηχανές αναζήτησης. Αυτό το περιεχόμενο αναφέρεται και ως ο κρυφός ή αόρατος ιστός[38].

---

[35] http://www.astynomia.gr/images/stories/2015/3prak_syn.pdf

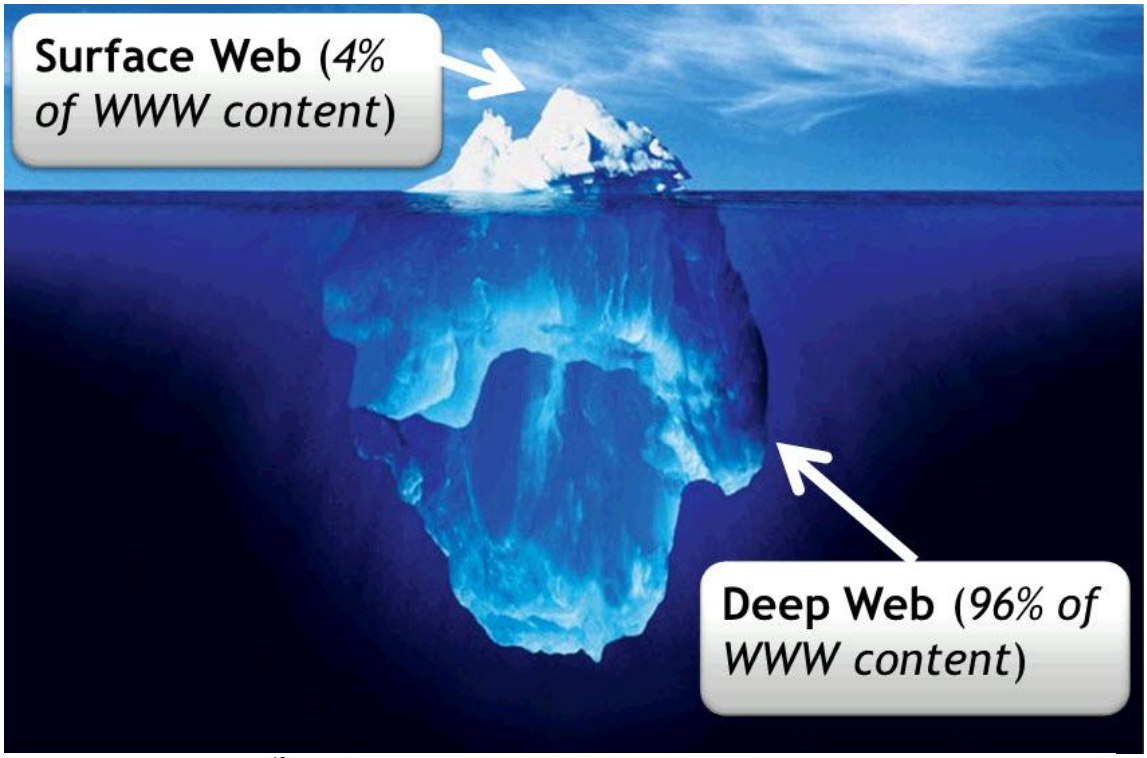
[36] https://el.wikipedia.org/wiki/%CE%99%CF%83%CF%84%CE%BF%CF%81%CE%AF%CE%B1_%CF%84%CE%BF%CF%85_%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85

[37] Europol, 2013, *Strategic Assessment of Commercial Sexual Exploitation of Children Online*, Διαθέσιμο: Europol, 2013, *Strategic Assessment of Commercial Sexual Exploitation of Children Online*, Διαθέσιμο: https://www.europol.europa.eu/sites/default/files/publications/efc_strategic_assessment__public_version.pdf

[38] Δεληγιάννης Κ., Ο κόσμος του σκοτεινού Internet, Η ΚΑΘΗΜΕΡΙΝΗ, https://www.kathimerini.gr/765417/article/texnologia/diadiktyo/o-kosmos-toy-skoteinoy-internet

Η αναζήτηση στο διαδίκτυο σήμερα, μπορεί να συγκριθεί με το να προσπαθήσουμε να απλώσουμε ένα δίχτυ σε όλη την επιφάνεια ενός ωκεανού. Ενώ ένα μεγάλο μέρος μπορεί να πιαστεί στο δίχτυ, εξακολουθεί να υπάρχει ένας πλούτος πληροφοριών που είναι βαθιά, και ως εκ τούτου τον χάσαμε[39]!

Ο λόγος είναι απλός: Οι περισσότερες πληροφορίες του Ιστού είναι θαμμένες πολύ κάτω σε ιστοσελίδες που δημιουργούνται δυναμικά, και οι παραδοσιακές μηχανές αναζήτησης δεν τις βρίσκουν.



Εικόνα 3.6: Dark Web[40]

Εδώ είναι μερικά γεγονότα σχετικά με το Deep Web:

- Οι εξήντα, μόνον, από τις μεγαλύτερες βαθιά κρυμμένες τοποθεσίες Web περιέχουν συνολικά περίπου 750 terabytes πληροφοριών – ήδη, αυτές από μόνες τους, υπερβαίνουν το μέγεθος του «επιφανειακού Web» κατά σαράντα φορές.Η ενημέρωση του κοινού σχετικά με το βαθύ Web είναι

[39] https://www.techne.gr/threads/10351-Deep-Web-%CE%92%CE%B1%CE%B8%CF%8D-%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF!?styleid=21

[40] Ληφθείσα εικόνα από https://www.techne.gr/threads/10351-Deep-Web-%CE%92%CE%B1%CE%B8%CF%8DCE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF!?styleid=21

σήμερα 400 με 550 φορές μεγαλύτερη από ό,τι συνήθως ορίζει το World Wide Web.

- το Deep Web περιέχει 7.500 terabyte πληροφοριών ενώ το «επιφανειακό Web» (εκείνο δηλαδή το Web που βρίσκουμε από τις παραδοσιακές μηχανές αναζήτησης) περιέχει 19 terabyte πληροφοριών.
- Οι Deep ιστοσελίδες τείνουν να είναι πιο περιορισμένες, με βαθύτερο περιεχόμενο, από τους συμβατικούς χώρους του «επιφανειακού Web».
- το «Deep Web» περιέχει περίπου 550 δισεκατομμύρια μεμονωμένα έγγραφα σε σύγκριση με το 1 δισεκατομμύριο που υφίστανται στο «επιφανειακό Web».
- Περισσότερες από 200.000 βαθιά κρυμμένες ιστοσελίδες υπάρχουν σήμερα.
- Το βαθύ Web είναι η μεγαλύτερη αναπτυσσόμενη κατηγορία των νέων πληροφοριών στο Διαδίκτυο.
- Το περιεχόμενο του Deep Web είναι ιδιαίτερα σημαντικό για κάθε ανάγκη πληροφόρησης και αγοράς.
- Η ποιότητα του περιεχομένου του Deep Web είναι 1.000 έως 2.000 φορές μεγαλύτερη από εκείνη του «επιφανειακού Ιστού».
- Ένα πλήρες ενενήντα πέντε τοις εκατό του Deep Web είναι προσβάσιμες στο κοινό πληροφορίες – που δεν υπόκεινται σε τέλη ή συνδρομές.
- Περισσότερο από το ήμισυ του περιεχομένου του Deep Web βρίσκεται σε συγκεκριμένες βάσεις δεδομένων.

3.7 Τι υπάρχει στο Deep Web;

Οι μηχανές αναζήτησης εμφανίζουν αποτελέσματα χρησιμοποιώντας κάποιους αλγόριθμους που «βάζουν σε λίστες» της ιστοσελίδες και λέγονται

crawlers[41]. Οι crawlers όμως δεν βρίσκουν τα πάντα. Υπάρχουν «κρυφοί» πόροι στο διαδίκτυο που χονδρικά, κατατάσσονται στις παρακάτω κατηγορίες.

- Μη συνδεδεμένο περιεχόμενο: σελίδες που δεν συνδέονται με άλλες σελίδες. Έτσι, τα crawlers που χρησιμοποιούν οι μηχανές αναζήτησης, δεν μπορούν να τις «βρουν» από άλλες σελίδες που εξετάζουν.

- Δυναμικό περιεχόμενο: δυναμικές σελίδες στις οποίες έχει κάποιος πρόσβαση μόνο μέσα από φόρμες στις οποίες συμπληρώνει στοιχεία.

- Scripted content: σελίδες που είναι διαθέσιμες μόνο από συνδέσμους που παράγονται από JavaScript καθώς και περιεχόμενο που κατεβάζεται από Web servers μέσω Flash π.χ.

- Private Web: ιστοσελίδες που χρειάζεται να κάνετε login με username και password

- Contextual Web: είναι οι σελίδες εκείνες το περιεχόμενο των οποίων προσαρμόζεται ανάλογα με τον τρόπο που έχει κανείς πρόσβαση σε αυτό. Παραδείγματος χάριν, οι σελίδες εκείνες που, αν έχετε πρόσβαση σε αυτές με μία διεύθυνση IP από την Ελλάδα, βλέπετε διαφορετικό περιεχόμενο από το αν θα επισκεπτόσασταν την ίδια σελίδα από μία IP των ΗΠΑ.

- Περιεχόμενο περιορισμένης πρόσβασης: ιστοσελίδες που περιορίζουν την πρόσβαση στο περιεχόμενό τους με τεχνικούς τρόπους (Robots Exclusion Standards, CAPTCHAS και άλλα)

- Non - HTML/text content: περιεχόμενο κειμένου που είναι κωδικοποιημένο σε αρχεία multimedia ή συγκεκριμένα formats που δεν μπορούν να διαβάσουν οι μηχανές αναζήτησης,

- Οτιδήποτε δεν ακολουθεί το πρότυπο HTTP/HTTPS.

[41] Βλ. πτυχιακή εργασία Μηλιώνη Ελένη, Τμήμα Μηχανικών πληροφορικής ΤΕΙ Δυτικής Ελλάδας, 2017. http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/5723/CIED%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20.pdf?sequence=1

3.8 Σχέση Κυβερνοεγκλήματος και Οικονομικού Εγκλήματος

Το έγκλημα στον κυβερνοχώρο, σύμφωνα με πολλούς μελετητές και ερευνητές του αντικειμένου, αποτελεί μία **ειδικότερη μορφή του εγκλήματος του «λευκού περιλαίμιου» (white-collar crime),** αφού προϋποθέτει:

- **γνώσεις και επιδεξιότητα**,
- **ιδιαίτερες ικανότητες**,
- όπως και τα απαραίτητα **τεχνικά και οικονομικά μέσα**.[42]

Έχει παρατηρηθεί ότι το έγκλημα λευκού περιλαιμίου αποτελεί περισσότερο μια κοινωνική παρά νομική έννοια, η οποία αρχικά χρησιμοποιήθηκε και από δικηγόρους και από κοινωνικούς επιστήμονες. Δεν υπάρχει καμία συγκεκριμένη παράβαση ή ομάδα παραβάσεων που μπορούν να προσδιοριστούν ως έγκλημα λευκού περιλαιμίου.

Οι τεχνολογικές εξελίξεις των τελευταίων ετών έχουν δημιουργήσει περαιτέρω περιπλοκές που περιβάλλουν τους τύπους προσώπων που είναι σε θέση να διαπράξουν το έγκλημα του λευκού περιλαιμίου. Ο δράστης μιας διαδικτυακής απάτης, παραδείγματος χάριν, μπορεί το ίδιο εύκολα να είναι ένας αυτοδίδακτος έφηβος που χρησιμοποιεί έναν προσωπικό υπολογιστή στο σπίτι όπως και ένας μορφωμένος επαγγελματίας στον εργασιακό του χώρο.[43]

Μεταξύ του κυβερνο-εγκλήματος και του οικονομικού εγκλήματος υφίσταται μια **αλληλεξάρτηση** η οποία δημιουργεί δύσκολα εννοιολογικά ερωτήματα. Αυτό οφείλεται εν μέρει στο ότι τα τελευταία χρόνια τα περισσότερα εγκλήματα ιδιοκτησίας έχουν διαπραχτεί με τη χρήση των υπολογιστών, αλλά και στο γεγονός ότι όλες οι σύγχρονες επιχειρήσεις στηρίζονται πλέον σε μεγάλο βαθμό στην ψηφιακή τεχνολογία.

Το παρακάτω σχήμα των Smith R. & Grabosky P. παρέχει μια απεικόνιση της **αλληλεξάρτησης** μεταξύ των εννοιών του εγκλήματος του **λευκού**

[42] Γασπαρινάτου Μ., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΟΥΛΑΣ 2016
[43]Περπέρης Απόστολος, Το Ηλεκτρονικο–οικονομικό έγκλημα: Ερευνητική προσέγγιση, Διδακτορική Διατριβή, Πάντειο Πανεπιστήμιο, Αθήνα, 2015

περιλαιμίου, του **οικονομικού εγκλήματος** και του **κυβερνο-εγκλήματος**.[44]

Εικόνα 3.7: Σχηματική αποτύπωση Εγκλημάτων

Μπορούμε λοιπόν να δούμε οτι το κυβερνο-έγκλημα έχει κοινά σημεία τόσο με το έγκλημα λευκού περιλαιμίου όσο και με το οικονομικό έγκλημα. Υπάρχει και μια ομάδα των κυβερνο - εγκλημάτων που δεν έχει κανένα οικονομικό χαρακτηριστικό από την άποψη του οικονομικού οφέλους και περιλαμβάνονται οι περιπτώσεις της κυβερνο-παρενόχλησης (cyberbullying παραδείγματος χάριν) και του κυβερνο-βανδαλισμού κατά τις οποίες χρησιμοποιούνται οι υπολογιστές για να πραγματοποιηθούν οι απειλές. Η διάδοση επιβλαβούς περιεχομένου συχνά έχει οικονομικά κίνητρα, όπως οι διαδικτυακές επιχειρήσεις που διαδίδουν παιδική πορνογραφία έναντι αμοιβής, ενώ άλλο περιεχόμενο όπως το ρατσιστικό υλικό γενικά δεν παρακινείται από οικονομικά κίνητρα.[45]

Έτσι, σε σχέση με το έγκλημα του λευκού περιλαιμίου, μπορούμε να διακρίνουμε το ηλεκτρονικό έγκλημα σε:

[44] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σσ. 27-30
[45] Smith Russell, Grabosky Peter & Urbas Gregor (2004), ό.π.

3.8.1 Κυβερνοέγκλημα που δεν αποτελεί μορφή του εγκλήματος λευκού περιλαίμιου

Μεγάλο κομμάτι του ηλεκτρονικού εγκλήματος δεν μπορεί να συμπεριληφθεί στην έννοια του εγκλήματος λευκού περιλαιμίου που διαπράττεται από άτομα υψηλού κύρους η που εκμεταλλεύονται την επαγγελματικής τους θέση. Ωστόσο υπάρχουν και εγκλήματα λευκού περιλαιμίου που δεν τελούνται με τη χρήση των ψηφιακών τεχνολογιών.

Η εισβολή σε υπολογιστικά συστήματα (το γνωστό hacking) αποτελεί την κατεξοχήν μορφή ηλεκτρονικού εγκλήματος που δεν αποτελεί μορφή του εγκλήματος λευκού περιλαιμίου.[46]

Αυτό όμως δεν αποκλείει το γεγονός ότι μια εισβολή σε ένα σύστημα υπολογιστή ή τηλεπικοινωνιών (hacking) να αποτελέσει το μέσο-εργαλείο για την τέλεση περαιτέρω εγκλημάτων οικονομικής φύσεως (πχ για εκβίαση).

3.8.2 Κυβερνοέγκλημα που αποτελεί μορφή του εγκλήματος λευκού περιλαιμίου

Το Διαδίκτυο και τα πληροφοριακά συστήματα γίνονται συχνά το κύριο εργαλείο για τη διάπραξη απάτης, φοροδιαφυγής, ακόμα και για επιθέσεις σε άλλες επιχειρήσεις με παράνομη πρόσβαση σε αρχεία και δίκτυα ή υποκλοπή επικοινωνιών για διενέργεια βιομηχανικής κατασκοπείας και άλλων παραβιάσεων οικονομικού χαρακτήρα.

Οργανισμοί και επιχειρήσεις χρησιμοποιούν τη σύγχρονη ψηφιακή τεχνολογία σαν εργαλείο εγκληματικών δραστηριοτήτων. Η χρήση λοιπον της τεχνολογίας της πληροφορικής στην τήρηση οικονομικών στοιχείων, τιμολογίων, μισθολογικών στοιχείων των εργαζομένων και άλλων πληρωμών

[46] Grabosky Peter & Walkley Sascha, (2007), σσ. 358-375

καθιστά και τις επιχειρήσεις άμεσα εξαρτώμενες από αυτή[47].

Εκτός από τις επιχειρήσεις, τους οργανισμούς, τα υψηλόβαθμα στελέχη με υψηλό κύρος, αλλά και απλοί εργαζόμενοι σε σύγχρονες επιχειρήσεις και οργανισμούς μπορούν να εκμεταλλεύονται τις εγκληματικές ευκαιρίες που προσφέρουν οι νέες τεχνολογίες.

Στις περιπτώσεις, όπως αυτές που ο ρόλος της είναι συμπτωματικός ή περιστασιακός για την τέλεση του εγκλήματος, η ψηφιακή τεχνολογία δημιουργεί έναν σημαντικά κοινό τόπο μεταξύ του ηλεκτρονικού και του οικονομικού εγκλήματος (ειδικά για τις περιπτώσεις των στελεχών που ενεργούν για λογαριασμό της επιχείρησης).[48]

Όλα σχεδόν τα αρχεία των επιχειρήσεων και οργανισμών καταχωρούνται σε ψηφιακή μορφή, έχοντας ως φυσικό επακόλουθο το σύγχρονο επιχειρηματικό έγκλημα να λαμβάνει ψηφιακή μορφή και περιεχόμενο και να συνιστά μια μεγάλης κλίμακας αλληλοεπικάλυψη του επιχειρησιακού εγκλήματος (του λευκού περιλαιμίου) με το ηλεκτρονικό.[49]

Μεγάλο μέρος των σύγχρονων οικονομικών εγκλημάτων με στόχο ή μέσο τον ηλεκτρονικό υπολογιστή, σύμφωνα με τον D.Parker, τελούνται από τους λεγόμενους insiders (εσωτερικούς ως προς την επιχείρηση) οι οποίοι διαθέτουν ιδιαίτερα προσόντα, γνώση, πρόσβαση, ευκαιρίες και δυνατότητες, αναπτύσσοντας εκλεπτυσμένες μεθόδους για να προκαλέσουν απώλειες πληροφοριακών δεδομένων στην επιχείρηση όπου εργάζονται ως έμπιστοι υπάλληλοι ή ανώτερα στελέχη.[50]

Το 2018 η Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα της PwC (Price Waterhouse Coopers)[51] ως προς τους υπαιτίους του οικονομικού εγκλήματος, αναφέρει οτι σχεδόν στο 50% των περιστατικών οικονομικής απάτης, ο δράστης ήταν εργαζόμενος του οργανισμού εις βάρος του οποίου διαπράχθηκε

[47]Γασπαρινάτου Μ., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΚΟΥΛΑΣ 2016

[48]Περπέρης Απόστολος, Το Ηλεκτρονικο–οικονομικό έγκλημα: Ερευνητική προσέγγιση, Διδακτορική Διατριβή, Πάντειο Πανεπιστήμιο, Αθήνα, 2015

[49] Grabosky Peter & Walkley Sascha (2007), ό.π.

[50]Parker Donn (1997), "Computer abuse", στο Hollinger Richard C. (editor), *Crime, deviance and the computer*, Aldershot Hants, England: Dartmouth, σελ.23-33

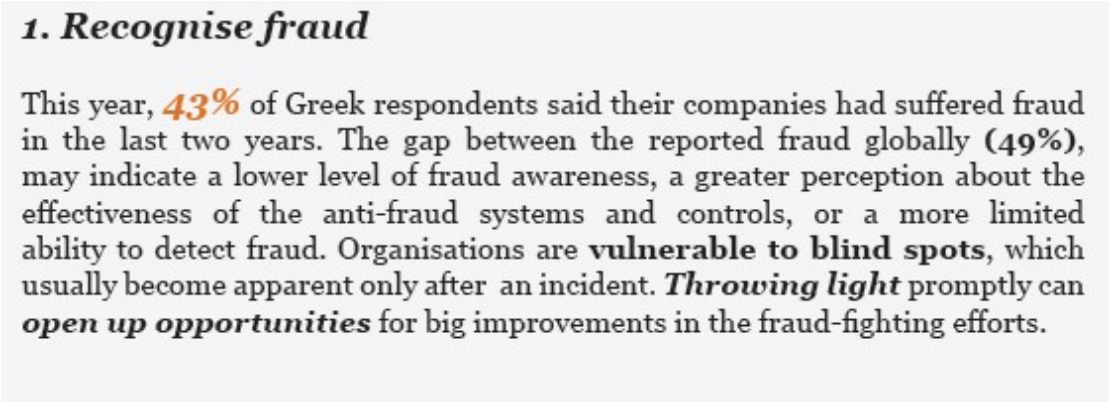
[51] https://www.pwc.com/gr/en/publications/assets/economic%20crime%20fraud%20survey-gr.pdf

η απάτη.

Εικόνα 3.8.2: Αποτελέσματα έρευνας

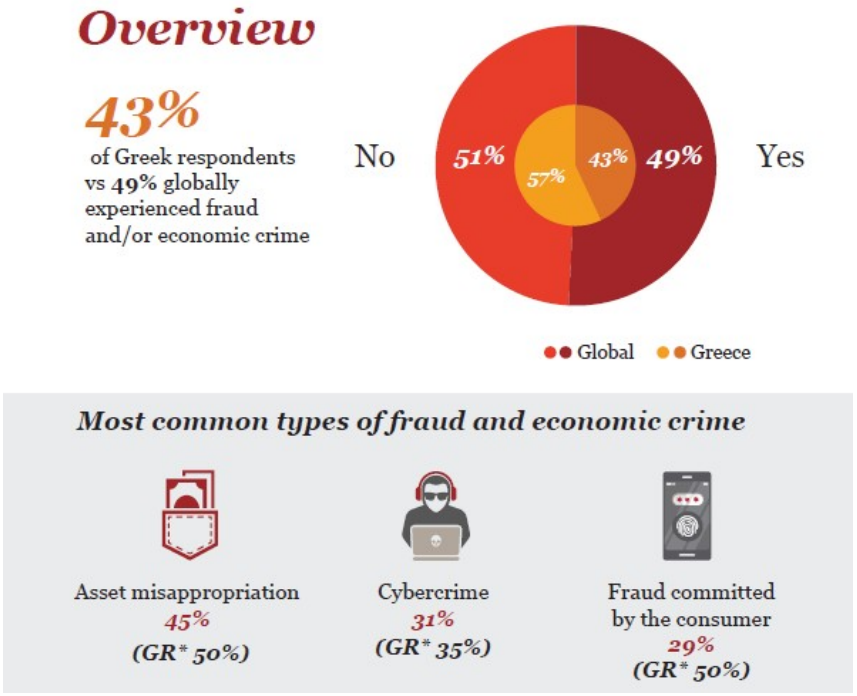
Οι εσωτερικοί δράστες είναι στην πλειοψηφία τους άνδρες απόφοιτοι πανεπιστημίου με εργασιακή εμπειρία από 3 έως 5 χρόνια, ηλικίας μεταξύ 31 40 ετών που καταλαμβάνουν μεσαίες/ανώτερες διοικητικές θέσεις.[52]

Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα[53]



Εικόνα 3.8.3: Αποτελέσματα έρευνας

[52] https://www.pwc.com/gr/en/media-centre/assets/global-economic-crime-pr-gr.pdf
[53]https://www.pwc.com/gr/en/publications/assets/economic%20crime%20fraud%20survey-gr.pdf



Εικόνα 3.8.4: Αποτελέσματα έρευνας

Εκτός από τους εργαζόμενους στην επιχείρηση και τους χάκερ, πλέον και οι επαγγελματίες εγκληματίες θα έχουν τη δυνατότητα να εισέρχονται στο πεδίο του ηλεκτρονικού εγκλήματος. Εφόσον το παραδοσιακό περιβάλλον στο οποίο δραστηριοποιούνται μετατρέπεται σε ηλεκτρονικό και αυτοματοποιημένο, αναγνωρίζουν πλέον και την δική τους ανάγκη για γνώση της πληροφορικής τεχνολογίας. Η πληροφορική δίνει τη δυνατότητα σε επαγγελματίες εγκληματίες και τα δίκτυα οργανωμένου εγκλήματος να καταστρώνουν ευρείας κλίμακας εγκληματικές επιχειρήσεις σε τομείς όπως λαθρεμπόριο ναρκωτικών, πορνεία, τζόγο και εκβιασμό.

Η ανάπτυξη της πληροφορικής και των ψηφιακών τηλεπικοινωνιών έχει αποσυνδέσει την εγκληματική δραστηριότητα από την ανάγκη της γεωγραφικής εγγύτητας ως προς το στόχο. Έχει μάλιστα εκτιμηθεί ότι, ακριβώς λόγω των αλλαγών στις μορφές της πληροφορίας, τις μεθόδους και τους πόρους των εγκληματιών, ο συνολικός αριθμός περιστατικών επιχειρηματικού εγκλήματος θα μειωθεί κατά τα επόμενα χρόνια, ενώ το μέγεθος των απωλειών θα αυξηθεί δραματικά. Η αυξανόμενη διάδοση, η πολυπλοκότητα της τεχνολογίας και αποτελεσματικότητα των μέτρων ασφαλείας από τη μια και η αυξανόμενη ποσότητα, αλλά και η οικονομική αξία, των αποθηκευμένων σε πληροφοριακά συστήματα ψηφιακών

πληροφοριών, δεδομένων από την άλλη, οδηγούν στην επαύξηση των ζημιών. Ο D. Parker εκτιμά ότι παράλληλα θα μειώνεται ολοένα και περισσότερο ο αριθμός των χρηστών που θα έχουν τη δυνατότητα διάπραξης τέτοιων εγκλημάτων, επειδή θα απαιτούνται ιδιαίτερα προσόντα, γνώσεις, πληροφορίες, πρόσβαση και πόροι.[54]

3.9 Συμπέρασμα για την σχέση

Το έγκλημα στον Κυβερνοχώρο παρουσιάζει πολλά κοινά χαρακτηριστικά στοιχεία, με το οικονομικό έγκλημα.

Τα σημαντικότερα από αυτά τα κοινά χαρακτηριστικά, που συγκροτούν και το εγκληματικό πρότυπο του ηλεκτρονικο-οικονομικού εγκλήματος, συνοψίζονται στο ότι και τα δύο είδη εγκλήματος διαπράττονται:

- **χωρίς τη χρήση βίας**,
- **με προσπάθεια εξαπάτησης ή απόκρυψης της νόμιμης φύσης της δράσης, στο πλαίσιο μιας κατά τα άλλα νόμιμης ενασχόλησης** (στην εργασία ή τον ελεύθερο χρόνο), την οποία ο δράστης εκμεταλλεύεται δρώντας παρασιτικά.[55]

Η συνέργεια του οικονομικού με το ηλεκτρονικό στοιχείο του εγκλήματος είναι σε βαθμό τέτοιο που συχνά **δεν μπορούμε να διακρίνουμε αν πρόκειται για απλό οικονομικό ή απλό ηλεκτρονικό έγκλημα οπότε μιλάμε για «ηλεκτρονικο-οικονομικό» έγκλημα**.[56]

[54] Parker Donn (1987) ο.π.
[55] Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013), φ.π.
[56] Περπέρης Απόστολος,, 2015 ο.π.

4. Οικονομική Κυβερνοεγκληματικότητα.

4.1 Κατηγορίες των οικονομικών εγκλημάτων στον Κυβερνοχώρο

Σύμφωνα με την Shinder[57], τα οικονομικά εγκλήματα του λευκού περιλαιμίου στον κυβερνοχώρο περιλαμβάνουν διάφορες κατηγορίες όπως:

1. Η **μη εξουσιοδοτημένη απόκτηση εμπιστευτικών πληροφοριών** για την αγορά μετοχών ή άλλων επενδυτικών προϊόντων.
2. Η **μη εξουσιοδοτημένη πρόσβαση στα αρχεία μια επιχείρησης** με σκοπό την αλλαγή τους προς όφελος του εγκληματία, π.χ. να του δοθεί αύξηση μισθού
3. Η **αλλοίωση των ηλεκτρονικών λογαριασμών** της επιχείρησης ή των πελατών της προς όφελος του εγκληματία.
4. Η **πώληση πληροφοριών της επιχείρησης** σε τρίτους, συνεργάτες ή ανταγωνιστές με σκοπό τον εκβιασμό ή τη δωροληψία.
5. Η **αλλοίωση των λογιστικών βιβλίων ή των δηλώσεων** της επιχείρησης για τη παροχή εσφαλμένων πληροφοριών σε τρίτους, όπως επενδυτές, εφορία κλπ με σκοπό τη κάλυψη άλλων εγκλημάτων.

4.2 Τα κίνητρα των οικονομικών εγκληματιών στον Κυβερνοχώρο

Σε σχέση με τα κίνητρά τους οι εγκληματίες των οικονομικών εγκλημάτων στον Κυβερνοχώρο, σύμφωνα με την Shinder[58], εμπίπτουν στις εξής **κατηγορίες**:

- **Ο «υπολογιστικός» τύπος** ευφυούς εγκληματία βάσει προγραμματισμένου σχεδίου με χρονική ακρίβεια για οικονομικό όφελος και χωρίς ηθικούς ενδοιασμού βρίσκει την κατάλληλη ευκαιρία θα

[57]Shinder Debra Littlejohn, Tittel Ed. (2002), Scene of cybercrime Computer Forensics Handbook, Syngress Publishing

[58] Shinder Debra Littlejohn, Tittel Ed. (2002), Scene of cybercrime Computer Forensics Handbook, Syngress Publishing, σελ 121

διαπράξει το έγκλημα και αποσύρεται από τη δράση μετά από κάποιο διάστημα ή αφότου έχει συγκεντρώσει το χρηματικό ποσό που είχε υπολογίσει.

- Ο **«δυσαρεστημένος» εγκληματίας** που αισθάνεται προδομένος από την επιχείρηση στην οποία εργάζεται επειδή δεν πήρε την αύξηση ή τη θέση που προσδοκούσε ή έλαβε μια αδίκως αρνητική αξιολόγηση.
- **Ο «απελπισμένος»,** διαπράττει εγκληματικές πράξεις ως απάντηση σε σοβαρά οικονομικά προβλήματα που αντιμετωπίζει λόγω υγείας, οικογενειακής κρίσης, κακών επενδυτικών επιλογών ή λόγω εμπλοκής του σε προβλήματα με το νόμο, ναρκωτικών, αλκοόλ, τζόγο κλπ.

4.3 Χαρακτηριστικά γνωρίσματα της οικονομικής εγκληματικότητας στον Κυβερνοχώρο[59]

Το **ηλεκτρονικό έγκλημα με οικονομική διάσταση** παρουσιάζει κάποια γενικά χαρακτηριστικά τα οποία συνάμα πολλές φορές είναι και προβλήματα – πρακτικές δυσχέρειες στην διερεύνηση, διαλεύκανση και αντιμετώπιση του.
Αυτά είναι:

- Παρουσιάζει **διάχυση της θυματοποίησης**. Συχνά δεν υπάρχει συγκεκριμένο και προσδιορίσιμο θύμα, καθώς θύματα μπορεί να είναι το Κράτος , μια εταιρεία η πολλά άτομα.
- Παρουσιάζει **περιορισμένη θέαση**. Τα ηλεκτρονικά τους ίχνη καλύπτονται εύκολα, ενώ τα θύματα συχνά δεν γνωρίζουν καν ότι έπεσαν θύματα.
- Παρουσιάζει **διάχυση της ευθύνης**. Στα εγκλήματα αυτά εμπλέκονται πολλά άτομα μέσω Η/Υ από διαφορετικές εταιρείες και χώρες με αποτέλεσμα να είναι δύσκολο για τις αρχές να αποδείξουν και να αποδώσουν την ευθύνη.
- **Επιεικείς ποινές**. Λόγω διασυνδέσεων, οικονομικής ευχέρειας για

[59] Περπέρης Απόστολος, 2015 ο.π.

καλό συνήγορο πολλοί εγκληματίες του λευκού κολάρου επιτυγχάνουν είτε απαλλαγή είτε βραχύχρονη φυλάκιση.

❖ **Δυσκολία ανίχνευσης**, **προσαγωγής στη δικαιοσύνη** και **απόδειξης της ευθύνης στο δικαστήριο** λόγω μη επαρκούς συνεργασίας των θυμάτων με τις αρχές επειδή αυτά δεν επιθυμούν να λάβουν αρνητική φήμη αν γίνει γνωστή η υπόθεση.

❖ Διέπονται από **ασαφή νομοθεσία,** η οποία δεν περιγράφει με ακρίβεια τα στοιχεία του εγκλήματος. Οι δράστες εφευρίσκουν συχνά νέες μεθόδους και τεχνικές διάπραξης με αποτέλεσμα οι εγκληματικές τους πράξεις, είτε να μην καλύπτονται από τις υπάρχουσες αντικειμενικές υποστάσεις εγκληματικών συμπεριφορών είτε να καλύπτονται προβληματικά.

❖ **Πολυπλοκότητα**, από πλευράς **νόμων, χωρών** που εμπλέκονται στη δικαιοδοσία και **τεχνικών** εξαπάτησης που χρησιμοποιούνται.

❖ **Εξειδικευμένες γνώσεις επίσης απαιτούνται** και από όσους ασχολούνται με αυτή τη μορφή εγκληματικότητας όπως είναι οι εισαγγελείς, αστυνομικοί δικαστές, δικηγόροι, επιστήμονες.

❖ Εμφανίζει **πολυπλοκότητα** κατά την τέλεση του, απαιτεί εξειδικευμένες **γνώσεις, εμπειρία, εξοικείωση και πληροφορικό εξοπλισμό**, καθιστώντας δύσκολη την τέλεση του από κάποιον που δεν διαθέτει τα παραπάνω «προσόντα» όπως θα μπορούσε να γίνει με τα εγκλήματα «του δρόμου».

❖ Οι δράστες του διαθέτουν **υψηλό επίπεδο εκπαίδευσης ή ειδίκευσης στην πληροφορική τεχνολογία**, ανήκουν στα μεσαία ή ανώτερα στρώματα, διαπράττουν τα εγκλήματα τους κυρίως κατά τη διάρκεια της επαγγελματικής τους ενασχόλησης.

❖ Η διερεύνηση και δίωξη του από τις αρχές είναι πολύ δύσκολη καθώς απαιτούνται εξειδικευμένες γνώσεις και υψηλό επίπεδο εκπαίδευσης.

❖ Οι δράστες σε πολλές περιπτώσεις τυγχάνουν **εξωδικαστικής αντιμετώπισης,** π.χ. με διοικητικά μέτρα στο πλαίσιο των επιχειρήσεων.

❖ Εμφανίζει **μεγάλο «σκοτεινό αριθμό»,** συνήθως μεγαλύτερο από αυτόν του κοινού εγκλήματος.

❖ Πολλά από τα σύγχρονα οικονομικά εγκλήματα (διαφόρων ειδών

απάτες, ξέπλυμα χρήματος κλπ.) πλέον τελούνται με ή και απαιτούν τη σύμπραξη της πληροφορικής και ψηφιακής τεχνολογίας εφόσον το περιβάλλον στο οποίο διαδραματίζονται είναι πλέον ψηφιακό και δικτυακό.

- Ακόμα και οι περιπτώσεις των ηλεκτρονικών εγκλημάτων που προβλέπονται στο ποινικό δίκαιο αντιμετωπίζονται είτε από ήδη υπάρχουσες ρυθμίσεις που ισχύουν και για τα οικονομικά εγκλήματα είτε από ειδικά για το ηλεκτρονικό έγκλημα νομοθετήματα.
- Η πράξη δεν στοχεύει κυρίως στη κάλυψη βιοτικών αναγκών επιβίωσης του δράστη, αλλά στην επίτευξη ανώτερου επίπεδου ανέσεως και ευμάρειας εναντίον του οικονομικού συμφέροντος των θυμάτων.
- Είναι έγκλημα που συνήθως διαπράττεται χωρίς τη χρήση φυσικής βίας,.
- Τέλος συχνά διαπράττεται στο πλαίσιο της νόμιμης απασχόλησης του δράστη από:

α) επιχειρήσεις εναντίον άλλων επιχειρήσεων (όπως η βιομηχανική κατασκοπία) για απόκτηση συγκριτικού πλεονεκτήματος.

β) υπαλλήλους μιας επιχείρησης στο πλαίσιο της νόμιμης απασχόλησης τους, όπου ο απασχολούμενος, καταχράται την ιδιότητα του ή εξ αφορμής της, εκτελεί την παράνομη πράξη.[60]

γ) τρίτους οι οποίοι αποκτούν μη εξουσιοδοτημένη πρόσβαση και διαπράττουν διάφορες πράξεις κακοχρησίας υπολογιστών.[61]

Συνοψίζοντας οι Newman Graeme & Clarke Roland[62] πολύ εύστοχα εισήγαγαν το ακρωνύμιο SCAREM (Stealth, Challenge, Anonymity, Reconnaissance, Escape, Multiplicity)[63] για να περιγράψουν τα **χαρακτηριστικά του ηλεκτρονικού εγκλήματος στον τομέα του ηλεκτρονικού εμπορίου**:

---

[60]Ιωαννίδης Χ., Νομικά Ζητήματα αναφορικά με Εγκλήματα Λευκού Κολάρου, (Σάκκουλας, Αθήνα-Κομοτηνή), 2001 σελ. 157-173

[61] Περπέρης Απόστολος, 2015 ο.π.

[62] Newman Graeme R., & Clarke Ronald V. (2003), Super-highway Robbery: Preventing ECommerce Crime. Cullompton, Devon, Willan, N.Y., σ.17

[63] Καπαρδής Α.,, Μαρία Κραμβιά-Καπαρδή και Νέστωρας Κουράκης, *Οικονομικά Εγκλήματα στην Κύπρο: Μια Πολυθεματική Προσέγγιση* (Α. Σάκκουλας, Αθήνα-Κομοτηνή, 2001) 353

- **Ανωνυμία** (Anonymity). Το διαδίκτυο προσφέρει τη δυνατότητα στο δράστη να διαφεύγει, εκμεταλλευόμενος τη διακριτικότητα και ανωνυμία που προσφέρουν οι ηλεκτρονικές επιχειρήσεις για συναλλαγές των πελατών τους.
- **Απόκρυψη** (Stealth), το διαδίκτυο προσφέρει μεγαλύτερη δυνατότητα απόκρυψης της τέλεσης του εγκλήματος. Για παράδειγμα ο δράστης (hacker) μπορεί να μπει κρυφά στα αρχεία μιας τράπεζας, να πάρει αυτό που θέλει και να βγει χωρίς να αφήσει ίχνη.
- **Πρόκληση** (Challenge) για τους hackers να παραβιάσουν το σύστημα, ώστε να καυχώνται ότι το κατάφεραν.

Εικόνα 4.3: Internet surfing and anonymity

- **Διαφυγή** (Escape), η ικανότητα του δράστη να καλύπτει τα ίχνη του για να αποφύγει την σύλληψη χρησιμοποιώντας τις IP ή τον υπολογιστή κάποιου άλλου χρήστη, επιχείρησης ή πανεπιστημίου.
- **Αναγνώριση**, η γνώση του κατάλληλου στόχου (Reconnaissance) από την καθημερινή ρουτίνα του δράστη. Ο δράστης μπορεί να εγκαταστήσει προγράμματα (spyware) παρακολούθησης των δραστηριοτήτων του στόχου του.
- **Πολλαπλότητα** (Multiplicity), δυνατότητα στον δράστη να πλήξει περισσότερο από έναν στόχους ταυτόχρονα.

5. Το προφίλ και τα Χαρακτηριστικά των Δραστών

5.1 Πως επιδρούν οι παράγοντες: κίνητρο, εκλογίκευση, ευκαιρία στην τέλεση του ηλεκτρονικο-οικονομικού εγκλήματος[64]

Οι εγκληματικές δυνατότητες που προσφέρονται από την ευρύτατη διάδοση του διαδικτύου είναι πλέον προσβάσιμες όχι μόνο από τα προνομιούχα κοινωνικά στρώματα αλλά και από τις ευρύτερες μάζες πληθυσμού (εκδημοκρατισμός του διαδικτύου).

Όσον αφορά το ηλεκτρονικο-οικονομικό έγκλημα οι Grabosky και Walkley θεωρούν την εξάπλωση της πληροφορικής τεχνολογίας ως βασικό παράγοντα της αύξησης των δραστών με κίνητρο. **Η ανάπτυξη των διαδικτυακών συναλλαγών, του ηλεκτρονικού εμπορίου, των ηλεκτρονικών δημοπρασιών, των χρηματιστηριακών συναλλαγών, των υπηρεσιών διαδικτυακής αποθήκευσης αρχείων και δεδομένων (τύπου cloud) έχουν δημιουργήσει ελκυστικούς στόχους και εγκληματικές ευκαιρίες σε δράστες με κίνητρο.**

Ο Coleman ασχολήθηκε, όπως είδαμε παραπάνω, με την εξήγηση της εγκληματικής συμπεριφοράς ως ένα σύνθετο συνδυασμό κινήτρων και ευκαιριών.

Εκτός από τα κίνητρα θα πρέπει να υπάρχει και η ανάλογη ευκαιρία, καθώς χωρίς αυτή δεν μπορεί να υπάρξει έγκλημα ανεξάρτητα από τη δύναμη που μπορεί να ασκεί το κίνητρο στο άτομο. Κανένα κίνητρο δεν είναι αρκετό για να εξηγήσει μια συμπεριφορά παρά μόνο σε συνδυασμό με τη μελέτη των ευκαιριών που είναι διαθέσιμες σε άτομα που κατέχουν θέσεις ισχύος. Η δομή του βιομηχανικού καπιταλισμού και η φύση του ανταγωνισμού

---

[64] Περπέρης Α., «Ο ρόλος των κινήτρων και των ευκαιριών στη δόμηση του προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος», http://crime-in-crisis.com/%CE%BF-%CF%81%CF%8C%CE%BB%CE%BF%CF%82-%CF%84%CF%89%CE%BD-%CE%BA%CE%B9%CE%BD%CE%AE%CF%84%CF%81%CF%89%CE%BD-%CE%BA%CE%B1%CE%B9-%CF%84%CF%89%CE%BD-%CE%B5%CF%85%CE%BA%CE%B1%CE%B9%CF%81%CE%B9%CF%8E%CE%BD/#

των επιχειρήσεων επιτρέπουν στα στελέχη τους τη δικαιολόγηση και εκλογίκευση των παράνομων συμπεριφορών και τους καθιστά δύσκολο να αντισταθούν στα οφέλη που αναμένονται από αυτές όταν τους παρουσιάζονται ελκυστικές ευκαιρίες για κέρδη.

Η Shapiro διέκρινε διάφορες τεχνικές που χρησιμοποιούν οι δράστες για να αποκτήσουν και να εκμεταλλευτούν την εμπιστοσύνη των θυμάτων τους κατά την διαμόρφωση της εγκληματικής τους ευκαιρίας.

Παρόμοιες τεχνικές κατάχρησης εμπιστοσύνης σύμφωνα με τους Grabosky και Walkley εφαρμόζονται και στον ψηφιακό χώρο.

Η διαφορά είναι ότι ενώ στον πραγματικό κόσμο η εμπιστοσύνη βασίζεται στην φυσική επαφή δράστη και θύματος, στον ψηφιακό αυτό πραγματοποιείται μέσω των δικτύων επικοινωνίας.

Τα στοιχεία που χαρακτηρίζουν τη διαμόρφωση του μοτίβου εμπιστοσύνης στον ψηφιακό χώρο είναι η **απουσία φυσικής επικοινωνίας και αλληλεπίδρασης, με εξ αποστάσεως επικοινωνία και η ανωνυμία.** Για παράδειγμα οι phishers, για να προσεγγίσουν και να αποκτήσουν την εμπιστοσύνη θυμάτων προκειμένου να τους αποσπάσουν εμπιστευτικές πληροφορίες σχετικά με τους τραπεζικούς λογαριασμούς τους, χρησιμοποιούν το όνομα γνωστών και καταξιωμένων εταιρειών. **Η οικοδόμηση εμπιστοσύνης γίνεται μέσω email, συμμετοχής σε δωμάτια συνομιλίας (chat rooms), αποστολής ενημερωτικών φυλλαδίων κλπ.**

Η εξαπάτηση και παραπλάνηση των θυμάτων σχετικά με την πραγματική ταυτότητα του δράστη και των προθέσεών του στηρίζεται σε μεγάλο βαθμό και στην ανωνυμία που παρέχει το ψηφιακό περιβάλλον. Η ανωνυμία στον κυβερνοχώρο δίνει τη δυνατότητα στους ψηφιακούς δράστες να παρέχουν παραπλανητικά στοιχεία για την ταυτότητά τους, τη φύση της συναλλαγής ή τις αληθινές προθέσεις τους, προκειμένου να πείσουν τα υποψήφια θύματα τους, όπως παιδιά για να τους συναντήσουν, αγοραστές προϊόντων μέσω διαδικτυακών δημοπρασιών, επενδυτές μετοχών, κάτοχους τραπεζικών λογαριασμών, άτομα για να παρενοχλήσουν, να εκβιάσουν κλπ.

Ένα ακόμα σημαντικό στοιχείο για τη δόμηση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος αποτελεί η **έλλειψη «ικανών φυλάκων»[65], δηλ. εμπόδια** που να αποτρέπουν τη δημιουργία των εγκληματικών ευκαιριών η οποία παρουσιάζεται και στον παγκόσμιο ψηφιακό ιστό, όπως και στο παραδοσιακό έγκλημα του λευκού περιλαιμίου. Η έλλειψη «ικανών φυλάκων» όσον αφορά τον χώρο του διαδικτύου εμφανίζεται με την μορφή αδυναμίας επιβολής του νόμου από πλευράς διωκτικών αρχών, έλλειψη ενημέρωσης των χρηστών για την ανάγκη λήψης μέτρων ασφάλειας και άμυνας έναντι των διαδικτυακών κινδύνων, ευάλωτα συστήματα υπολογιστών και δικτύων όπως και έλλειψη προθυμίας καταγγελίας των εγκλημάτων στις αρχές.

Σημαντικό παράγοντα στη διαμόρφωση του εγκληματικού προτύπου και τη δημιουργία της εγκληματικής ευκαιρίας για τον ψηφιακό δράστη όπως και για τον παραδοσιακό, αποτελεί η κατάχρηση της εμπιστοσύνης του θύματος από τον δράστη και η έλλειψη «ικανών φυλάκων»

Συμπερασματικά, το ηλεκτρονικο-οικονομικό έγκλημα ευνοείται από τη συνύπαρξη τριών παραγόντων: ***κίνητρο, εκλογίκευση, ευκαιρία***. Το έγκλημα αυτού του είδους είναι πιο πιθανό να τελεστεί όταν διαθέτει ευκολία διάπραξης, κίνητρο για το δράστη το υψηλό αναμενόμενο όφελος, χαμηλό κίνδυνο επισήμανσης, δικαιολογία και ευνοείται από τις ευκαιρίες που παρουσιάζονται περιστασιακά.

Τα κίνητρα είναι σημαντικά για τη διάπραξη του ηλεκτρονικο-οικονομικού εγκλήματος και αφορούν κυρίως την ικανοποίηση προσωπικών αναγκών όπως απόκτηση χρήματος, φήμης, ατομικής επιτυχίας. Ο δράστης υπολογίζει ορθολογικά τα οφέλη και τα κόστη, με βάση την προσπάθεια που απαιτείται και τους πιθανούς κινδύνους που συνεπάγεται η διάπραξη του εγκλήματος, τις ανταμοιβές, τις ευκαιρίες που ευνοούν τη δράση και τις εκλογικεύσεις που κάνει πριν προβεί στην τέλεση του εγκλήματος.

Τα στοιχεία που δομούν την εγκληματική ευκαιρία αποτελούν η εγγύτητα του στόχου στον δράστη, η ύπαρξη ευάλωτου στόχου που δεν

[65] Περπέρης Απόστολος, 2015 ο.π.

διαθέτει επαρκή φύλαξη, το υψηλό αναμενόμενο όφελος και ο χαμηλός κίνδυνος σύλληψης και επιβολής ποινής. Το ψηφιακό περιβάλλον διαθέτει τα συγκεκριμένα χαρακτηριστικά ή τουλάχιστον δημιουργεί στον πιθανό δράστη την αίσθηση ότι τα διαθέτει.

Εικόνα 5.1: Περιορισμός πρόσβασης - κρυπτογραφία

5.2 Το προφίλ του κυβερνο-εγκληματία που επιδιώκει οικονομικό όφελος[66]

Το προφίλ του κυβερνο-εγκληματία που επιδιώκει οικονομικό όφελος περιλαμβάνει τα παρακάτω γενικά χαρακτηριστικά[67]:

[66] Μαυρίδης Ι., Ασφάλεια Πληροφοριών στο Διαδίκτυο., Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών . Ελληνικά ακαδημαϊκά Ηλεκτρονικά συγγράμματα και βοηθήματα. Προσπελάσιμο στην https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&ved=2ahUKEwjHzZmSpIrnAhWJwAIHHbEKCS8QFjAOegQIAxAB&url=https%3A%2F%2Frepository.kallipos.gr%2Fbitstream%2F11419%2F1024%2F2%2F00_master_document-KOY.pdf&usg=AOvVaw0KHZe3ZyF3KkxS1jcyeMYu., Νοέμβριος. 2019

1. **Διαθέτει βασικές τουλάχιστον τεχνικές γνώσεις σχετικά με τη χρήση των Η/Υ, του Διαδικτύου και κατάλληλων τεχνολογικών εργαλείων και μεθόδων**. Κάτι που ένας απλός χρήστης των ηλεκτρονικών μέσων δεν χρειάζεται για τις καθημερινές δραστηριότητες του στο διαδίκτυο, π.χ. να πλοηγηθεί στις ιστοσελίδες, να στείλει ηλεκτρονικά μηνύματα κλπ.,
2. **Δημιουργία εικονικής προσωπικότητας και ζωής**. Πολλοί δράστες στον κυβερνοχώρο δημιουργούν καινούριες, ψεύτικες ταυτότητες (προσωπικότητες) που, εκτός του ότι τους ευχαριστεί να υποδύονται κάποιον «άλλο», τις χρησιμοποιούν για να ξεγελάσουν θύματα, να κρύβονται και να αποφεύγουν τον εντοπισμό και τη σύλληψη.
3. Ο δράστης έχει **ισχυρό κίνητρο για οικονομικό όφελος και αθέμιτο κέρδος**
4. Υποτίμηση του νόμου ή αίσθηση ότι βρίσκεται υπεράνω του νόμου. Σχεδόν κανείς δεν θεωρεί ότι οι πράξεις του είναι κακές αλλά τις δικαιολογεί. ...Μερικές φορές μάλιστα, λόγω των ικανοτήτων, εμπειρίας, της θέσης ή των περιστάσεων πιστεύει ότι είναι υπεράνω του νόμου ή ότι ο νόμος δεν ισχύει στον κυβερνοχώρο.
5. Ριψοκίνδυνη προσωπικότητα που επιδιώκει να έχει τον έλεγχο των καταστάσεων. Για κάποιους εγκληματίες η αίσθηση του κινδύνου τους συναρπάζει, τους ελκύει και τους κάνει να αφιερώνουν μεγαλύτερες προσπάθειες σε ριψοκίνδυνες και παράνομες συμπεριφορές παρά σε νόμιμες.

5.3 Το Προφίλ θυμάτων και οι διαδικτυακές ασχολίες των χρηστών του Διαδικτύου ως υποψήφια θύματα/στόχοι.

5.3.1 Ριψοκίνδυνες διαδικτυακές συμπεριφορές που εκθέτουν τους χρήστες του Διαδικτύου σε διαδικτυακά οικονομικά εγκλήματα

Το δίκτυο αποτελεί τον κοινό «χώρο» συνάντησης των πιθανών δραστών των ηλεκτρονικο-οικονομικών εγκλημάτων, και τα υποψήφιων θυμάτων - πιθανών στόχων. Οι δύο πλευρές αποτελούν χρήστες του ίδιου δικτύου το

[67] Shinder Debra Littlejohn, Tittel Ed. (2002), Scene of cybercrime Computer Forensics Handbook, Syngress Publishing, σσ. 113-118

οποίο αποτελεί την «δεξαμενή» άντλησης τόσο πιθανών δραστών όσο και ελκυστικών στόχων.

Μια ***ριψοκίνδυνη διαδικτυακή συμπεριφορά*** που εκθέτει τους χρήστες, τους καθιστά ευάλωτους και κατάλληλους στόχους φέρνοντάς τους σε εγγύτητα με πιθανούς δράστες μπορεί να συνιστούν διάφορες καθημερινές συνήθειες στο διαδίκτυο όπως[68]:

- **συχνή χρήση του e-banking,**
- **αποδοχή αγνώστων ως «φίλους» στα μέσα κοινωνικής δικτύωσης,**
- **συμμετοχή των χρηστών σε «δωμάτια» επικοινωνίας (chat rooms) με άλλους χρήστες,**
- **συχνή πραγματοποίηση διαδικτυακών συναλλαγών για αγορά προϊόντων μέσω δημοπρασιών ή ηλεκτρονικών καταστημάτων,**
- **εμπλοκή του ίδιου του θύματος σε παράνομες διαδικτυακές δραστηριότητες όπως χρήση ευρυζωνικής σύνδεσης για κατέβασμα δωρεάν ή πειρατικού λογισμικού ή αρχείων, συμμετοχή σε δραστηριότητες hacking, επίσκεψη άγνωστων ιστοσελίδων με αμφιλεγόμενο περιεχόμενο και θέαση απαγορευμένου υλικού όπως πορνογραφικό υλικό.**
- **κοινοποίηση προσωπικών πληροφοριών και δεδομένων,**
- **κλικάρισμα σε εικόνες,**
- **άνοιγμα ύποπτων emails (spam) κλπ.**

Η καθημερινή αυτή ρουτίνα των χρηστών του διαδικτύου, όσο συχνότερα επιδεικνύεται τόσο περισσότερο τους εκθέτουν και τους φέρνουν σε «εγγύτητα» με δράστες που έχουν κίνητρο να τους θυματοποιήσουν.[69]

---

[68] Choi Kyung-shick (2008b), «Computer Crime Victimization and Integrated Theory: An Empirical Assessment», *International Journal of Cyber Criminology* (IJCC) ISSN: 0974 – 2891 January-June 2008, 2 (1), ςς . 308–333 ανακτικθκε από http://www.cybercrimejournal.com/Choiijccjan2008.htm, Μαρτ. 2014 και Bossler Adam & Holt Thomas (2009), "On-line Activities, Guardianship, & Malware Infection: An Examination of Routine Activities Theory," *International Journal of Cyber Criminology*, 3, ςς. 400–420

[69] Περπέρης Α., 2015 ο.π.

5.4 Η «ελκυστικότητα» ή καταλληλότητα του στόχου

Για το θέμα της ελκυστικότητας ή καταλληλότητας του στόχου για τους πιθανούς δράστες οι Cohen και Felson, χρησιμοποίησαν τα αρχικά VIVA (value, inertia, visibility, accessibility)[70] για να περιγράψουν ως κατάλληλο τον στόχο-θύμα που διαθέτει μεγαλύτερη «αξία», «φορητότητα» (ευκολία μεταφοράς), «θεατότητα» και «προσβασιμότητα» σε σχέση με άλλους.

Στην περίπτωση των ηλεκτρονικών εγκλημάτων τα στοιχεία ή πληροφορίες που καθιστούν το στόχο-θύμα πιο επιθυμητό σε πιθανούς δράστες αποτελούν:

- **διευθύνσεις του ηλεκτρονικού του ταχυδρομείου,**
- **το πλήρες όνομα του θύματος,**
- **βίντεο,**
- **προσωπικές φωτογραφίες,**
- **πληροφορίες για ενδιαφέροντα και δραστηριότητες στο χώρο και το χρόνο που δημοσιοποιούνται σε ιστοσελίδες (κοινωνικής δικτύωσης κυρίως) και**
- **άλλα προσωπικά στοιχεία που προσελκύουν το ενδιαφέρον των δραστών.[71]**

Άλλοι ελκυστικοί, από άποψη φορητότητας και προσβασιμότητας, στόχοι μπορεί να είναι διάφορα αρχεία μουσικής, εικόνων, ταινιών και προγράμματα που μπορεί κανείς εύκολα και «δωρεάν» να κατεβάσει από το διαδίκτυο.

Από έρευνες που πραγματοποιήθηκαν για τα δημογραφικά χαρακτηριστικά της ελκυστικότητας του στόχου οι έρευνες διαπιστώθηκε ότι το γυναικείο φύλο είναι σε μεγαλύτερο κίνδυνο θυματοποίησης από ψηφιακές επιθέσεις, γεγονός που μπορεί να οφείλεται στο ότι οι άνδρες διαθέτουν πιο πολλές δεξιότητες για τη χρήση των ψηφιακών τεχνολογιών[72]. Όσον αφορά το

---

[70] Cohen Lawrence & Felson Marcus (1979), "Social change and crime rate trends: a routine **activity approach*", American Sociological Review*, 44, σ. 590**

[71] Reyns Bradford W., Henson Billy & Fisher Bonnie S. (2011), «Being Pursued Online: Applying
Cyber-Lifestyle-Routine Activities Theory To Cyberstalking Victimization», *Criminal Justice and Behavior*, 38, ςς. 1149-1169.

[72] Bossler Adam, & Holt Thomas J. (2009)

επίπεδο της απασχόλησης όσοι διαθέτουν πλήρη απασχόληση είναι πιο πιθανοί στόχοι επιθέσεων.

Σύμφωνα με έρευνα του Παντείου Πανεπιστημίου για την θυματοποίηση και τον φόβο του εγκλήματος στο διαδίκτυο βρέθηκε ότι η πλειονότητα των θυμάτων έχει θυματοποιηθεί επανειλημμένα (πάνω από 5 φορές) πράγμα που επιβεβαιώνει την άποψη ότι οι δράστες χρησιμοποιούν «οδούς» και προτιμούν στόχους που ήδη έχουν δοκιμάσει και γνωρίζουν.[73]

[73] Zarafonitou Christina & Koumentaki Evangelia (2014), *Victimisation and insecurity of undergraduate students while using internet*, 14th Annual Conference of the ESC, Prague, 10-13 September 2014, ανακτήθηκε από http://criminology.panteion.gr, Νοέμβριος 2014

6. Συνεργασίες σε διεθνές και Ευρωπαϊκό επίπεδο

6.1 Το διεθνές οργανωμένο έγκλημα και η σύνοδος των G8

Τα οκτώ περισσότερο βιομηχανικά αναπτυγμένα κράτη, ανέπτυξαν πρωτοβουλία για την αύξηση της αποτελεσματικότητας της συνεργασίας μεταξύ των κρατών για την καταπολέμηση του Διεθνούς εγκλήματος. Η συνεισφορά των κρατών αυτών υιοθετήθηκε από πάνω από 50 κράτη[74], τα οποία έδωσαν προτεραιότητα στην διασυνοριακή υποστήριξη, την αμοιβαία νομική βοήθεια, την συνεργασία των αστυνομικών αρχών, καθώς και την έκδοση των κρατουμένων. Το 2004, με την έναρξη της ισχύος των αποφάσεων της συνθήκης του Ευρωπαϊκού Συμβουλίου προτάθηκε και η αύξηση των εθνικών νομοθετημάτων που θα ποινικοποιούσαν τις περιπτώσεις ηλεκτρονικού εγκλήματος, αλλά και τον συντονισμό των αρμοδίων αρχών επιβολής του νόμου, στην προσπάθεια αντιμετώπισης των εγκλημάτων υψηλής τεχνολογίας.

6.2 Η Ευρωπαϊκή Ένωση, η europol και η Cepol.

Από την αρχή ακόμη της συνθήκης του Μάαστριχτ, χώρες κράτη μέλη, της Ευρωπαϊκής Ένωσης, περιέλαβαν τη δημιουργία υπερεθνικών οργανισμών που θα αντιμετώπιζαν τις εγκληματικές δραστηριότητες που θα αφορούσαν το διακρατικό έγκλημα. Η συνεργασία τους θα βασίζονταν στις αποφάσεις του Ευρωπαϊκού Συμβουλίου για το κυβερνοέγκλημα καθώς και στις συνθήκες της Ευρωπαϊκής Ένωσης, για τη συνδυασμένη δράση και υποστήριξη σε νομικά θέματα μεταξύ των χωρών κρατών μελών.

Η Ευρωπαϊκή Αστυνομία γνωστή και ως europol, ένας θεσμός της Ευρωπαϊκής Ένωσης, προσπαθεί να βελτιώσει τη συνεργασία των αστυνομικών αρχών για την καταπολέμηση του κυβερνοεγκλήματος. Η

[74]Περπέρης Α., Το ηλεκτρονικο-οικονομικό έγκλημα. Διδακτορική Διατριβή, Πάντειο Πανεπιστήμιο, Αθήνα, 2015

συνεργασία αυτή περιλαμβάνει διατάξεις που επικουρούν και προάγουν την ανταλλαγή πληροφοριών και αποδεικτικών στοιχείων μεταξύ των κρατών μελών, τη δημιουργία εκθέσεων σχετικά με τις διεθνείς τάσεις εγκληματικότητας, αλλά και την παροχή τεχνικής υποστήριξης για έρευνες πού διεξάγονται στο πλαίσιο αυτό. Ως παράδειγμα μπορούμε να αναφέρουμε τη μεγάλη επιχείρηση που διεξήχθη σε συνεργασία με το ομοσπονδιακό γραφείο ερευνών της Αμερικής (FBI) και είχε ως αποτέλεσμα τη διακοπή λειτουργίας τετρακοσίων παράνομων ιστοσελίδων και την κατ επέκταση σύλληψη δεκαεπτά δραστών. Οι παράνομες αυτές ιστοσελίδες είχαν σχέση με πωλήσεις ναρκωτικών, όπλων, υλικού παιδικής πορνογραφίας, ενώ μεταξύ των επισκεπτών των ιστοσελίδων αυτών, ήταν και πλήθος εξτρεμιστικών οργανώσεων, που δεν εμφανίζονταν στις κλασικές μηχανές αναζήτησης αλλά σε μηχανές αναζήτησης το ονομαζόμενου "σκοτεινού" διαδικτύου [75].

Από την 1η Ιουλίου του 2016, ιδρύθηκε κι ο οργανισμός της Ευρωπαϊκής Ένωσης με την ονομασία CEPOL[76], πού έχει έδρα τη Βουδαπέστη της Ουγγαρίας. Η CEPOL, συγκροτεί ένα δίκτυο το οποίο περιλαμβάνει τα ιδρύματα κατάρτισης των λειτουργών επιβολής του νόμου στα κράτη-μέλη της Ευρωπαϊκής Ένωσης και τα στηρίζει, παρέχοντας κατάρτιση και εκπαίδευση, σχετικά με τις προτεραιότητες στον τομέα της ασφάλειας, της συνεργασίας για την επιβολή του νόμου αλλά και την ανταλλαγή πληροφοριών. Η CEPOL συνεργάζεται με τα όργανα της Ευρωπαϊκής Ένωσης, με διεθνείς οργανισμούς και Τρίτες χώρες, ώστε να διασφαλίσει ότι οι σοβαρές απειλές για την ασφάλεια θα έχουν συλλογική και ενιαία αντιμετώπιση. Πέραν της εκπαίδευσης που παρέχεται στα στελέχη των κρατών-μελών στις διάφορες αστυνομικές ακαδημίες, διατηρεί και ειδική πλατφόρμα όπου παρέχει, μέσω αυτής, διαδικτυακή κατάρτιση στα πρόσωπα των αρχών επιβολής του νόμου. (Web seminars and Courses)[77].

[75] Περπέρης Α., ό. π., σελ. 195
[76] https://www.cepol.europa.eu/el., Νοέμβρ., 2019
[77] Βλ. https://www.cepol.europa.eu/el.

6.3 Ο οργανισμός οικονομικής συνεργασίας και ανάπτυξης

Από το 1997 και ο Ο.Ο.Α.Σ.Α εξέδωσε κατευθυντήριες γραμμές σχετικά τα μέσα που τα κράτη-μέλη οφείλουν να συντονίζουν την πολιτική τους στον τομέα της κρυπτογράφησης ώστε να επιτυγχάνουν την ισορροπία μεταξύ του κοινωνικού ελέγχου και της ιδιωτικότητας. Οι κατευθυντήριες αυτές γραμμές μετά το περιστατικό της 11ης Σεπτεμβρίου, εστίασαν στην αντιμετώπιση της κυβερνοτρομοκρατίας, του Hacking και αναλόγου είδους άλλων επιθέσεων. Η πρωτοβουλία αυτή ήταν ενδεικτική και υποδεικνύει την πρόθεση των κρατών-μελών, όσον αφορά τη συναίνεση για την αντιμετώπιση θεμάτων διαδικτυακής ασφάλειας. Στο σημείο αυτό, το κείμενο δεν αποτελούσε κάποιας μορφής νομικής δέσμευσης. Ανάλογου είδους δράση αναπτύχθηκε και από την ομάδα οικονομικής δράσης, που ιδρύθηκε από τη Σύνοδο των G7 στο Παρίσι, η οποία εξέδωσε κατευθύνσεις για την καταπολέμηση του ξεπλύματος μαύρου χρήματος, από άποψη ποινικής νομοθεσίας, Διεθνούς συνεργασίας και νομοθεσίας στις χρηματιστηριακές συναλλαγές. Μεταγενέστερα το 2014 στο Βερολίνο υπογράφτηκε από 52 κράτη, συμφωνία για την αυτόματη ανταλλαγή χρηματοοικονομικών πληροφοριών μεταξύ των μελών, με στόχο την καταπολέμηση της φορολογικής απάτης καθώς και της φοροδιαφυγής[78]. Οι χώρες-μέλη δεσμεύτηκαν για την πρώτη ανταλλαγή πληροφοριών το 2017. Η συμφωνία προβλέπει ότι οι τράπεζες θα πρέπει να κοινοποιούν αυτόματα[79] τα στοιχεία του προσώπου, τη διεύθυνσή του, το ποσό του εμβάσματος, το ύψος των τόκων και την πληρωμή μερισμάτων στη Χώρα που ο κάτοχος ενός λογαριασμού καταβάλει τους φόρους του.

6.4 Η Διεθνής Αστυνομική συνεργασία (Interpol)

Η Διεθνής αστυνομία με έδρα τη Λυών της Γαλλίας συντονίζει τη δράση των αστυνομικών αρχών των κρατών μελών, στον τομέα της ανταλλαγής των πληροφοριών, της ανάπτυξης κοινής δράσης, καθώς και στην ανταλλαγή

[78] Περπέρης Α., ό.π.,

[79] Κουπαράνης Π, (2014), «Η φοροδιαφυγή το στόχαστρο του ΟΟΣΑ», http://www.dw.de , 2014

μεθόδων και πρακτικών για την αντιμετώπιση των εγκλημάτων. Η Interpol παρέχει διεθνή εκπαιδευτικά σεμινάρια για την εκπαίδευση των στελεχών και παρέχει ειδικές τεχνικές γνώσεις, όσον αφορά την πληροφορική τεχνολογία, στους αστυνομικούς ερευνητές που ασχολούνται με το ηλεκτρονικό έγκλημα. Στην κατεύθυνση αυτή θετικά προσμετράται και η δημιουργία ομάδων εργασίας ειδικών προσώπων που ασχολούνται σε τοπικό επίπεδο με την ανταλλαγή καλών πρακτικών. Έμφαση δόθηκε στη δημιουργία ιστοσελίδας, που αφορά ένα παγκόσμιο σύστημα καταχώρησης πλαστογραφημένων καρτών, η οποία παρέχει στους ειδικούς τη δυνατότητα να ενημερώνονται άμεσα και να αποκτούν πληροφορίες προκειμένου να τους συνδράμουν στην διεξαγωγή των ερευνών. Πρόσβαση στην ιστοσελίδα αυτή έχουν και στελέχη του τραπεζικού συστήματος που είναι αρμόδια για την ανταλλαγή πληροφοριών με τους αρμόδιους δίωξης των εγκλημάτων και απατών.

7. Το Ελληνικό νομικό καθεστώς για την αντιμετώπιση του ηλεκτρονικού εγκλήματος

7.1 Το αδίκημα του άρθρου 370Γ παρ. 1 του Π.Κ

Σύμφωνα με τον προσφάτως θεσπισθέντα Ποινικό κώδικα, το πρώην άρθρο 370Β παρ. 1 Π.Κ, αναριθμήθηκε σε 370Γ παρ.1 Π.Κ και η διάταξή του παραμένει ώς είχε, χωρίς να τροποποιηθεί. Έτσι, " *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 δημόσιου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχος τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους*".

Ως ανωτέρω αναγράφεται, η εν λόγω πρόβλεψη τιμωρεί το δράστη που προβαίνει σε αντιγραφή, αποτύπωση, χρησιμοποίηση, γνωστοποίηση ή με οποιοδήποτε άλλο τρόπο παρέμβαση σε κρατικά, επαγγελματικά, επιστημονικά, απόρρητα, ή απόρρητα του δημοσίου ή απόρρητα του ιδιωτικού τομέα[80]. Το προστατευόμενο έννομο αγαθό απαρτίζουν ***τα απόρρητα*** υπό τη μορφή των στοιχείων ή προγραμμάτων υπολογιστών[81].

---

[80] **Μαυρίδης** Ι., Ασφάλεια Πληροφοριών στο Διαδίκτυο., Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών . Ελληνικά ακαδημαϊκά Ηλεκτρονικά συγγράμματα και βοηθήματα. Προσπελάσιμο στην https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&ved=2ahUKEwjHzZmSpIrnAhWJwAIHHbEKCS8QFjAOegQIAxAB&url=https%3A%2F%2Frepository.kallipos.gr%2Fbitstream%2F11419%2F1024%2F2%2F00_master_document-KOY.pdf&usg=AOvVaw0KHZe3ZyF3KkxS1jcyeMYu., Νοέμβριος. 2019, σελ. 255 επ.

[81] **Βασιλάκη Ε.**, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών Υπολογιστών. Η αντιμετώπιση του προβλήματος ιδιαίτερα μετα την εισαγωγή του ν. 1805/1988 Α.Ν Σάκκουλας, Αθήνα 1993, σελ. 159-163. Κωνσταντινίδη, Α., Η διακεκριμένη παραβίαση απορρήτων στοιχείων (πρώην άρθρο 370Β παρ.2 περ. β΄Π.Κ), ΠοινΧρ1997, σελ. 1216, όπου υποστηρίζεται ότι το προστατευόμενο έννομο αγαθό είναι η περιουσία ως σύνολο. Η ως άνω μόμως άποψη δεν λαμβάνει υπόψη ότι το άρθρο 370Β Π.Κ δεν αναφέρει ως απαραίτητο στοιχείο της αντικειμενικής υπόστασης του εγκλήματος την αποτίμηση σε οικονομική αξία των απορρήτων και συνεπώς δεν συνδέει τα απόρρητα με την περιουσιακή τους ιδιότητα.

Θεμελιώδη έννοια της αντικειμενικής υπόστασης που προβλέπεται στην εν λόγω διάταξη, **αποτελεί το απόρρητο**. Για την έννοια του απορρήτου έχουν διατυπωθεί διάφορες θεωρίες. Η κρατούσα στην επιστημονική κοινότητα θεωρία[82], για την έννοια του απορρήτου, προσδιορίζεται με δύο στοιχεία, ένα αντικειμενικό και ένα υποκειμενικό. Η υποστηριζόμενη αυτή μικτή θεωρία, αντικειμενικά προστατεύει την πληροφορία η οποία δεν πρέπει να είναι γνωστή σε ένα ευρύ κύκλο προσώπων και υποκειμενικά την θέληση και το ενδιαφέρον του κατόχου της να τη διατηρήσει μυστική. Όσον αφορά τα προγράμματα των ηλεκτρονικών Υπολογιστών θα πρέπει και αυτά με τη σειρά τους να είναι περιορισμένης προσβασιμοτητας αλλά και να διαφαίνεται το συμφέρον του κατόχου τους να διατηρηθούν ως απόρρητα. Το γεγονός αυτό στηρίζει τη δικαιολογητική του βάση στα μεγάλα ποσά που δαπανώνται για την κατασκευή των προγραμμάτων και εξωτερικεύεται απο τα μέτρα προστασίας που παίρνει ο εκάστοτε νόμιμος κάτοχος.

Εκείνο που θα πρέπει να διευκρινίσουμε κατα την ανάλυση της παραγράφου αυτής είναι ο όρος ***αθέμιτα***. Ως όρος γενικού περιεχομένου προκάλεσε το ενδιαφέρον της θεωρίας αλλά και της νομολογίας σχετικά με την ερμηνεία και ένταξή του στο ποινικό σύστημα. Επιπροσθέτως, για το αν αποτελεί ειδικό στοιχείο του αδίκου ή στοιχείο της αντικειμενικής υπόστασης του εγκλήματος[83].

Αθέμιτα ενεργεί κάποιος αφενός όταν η πράξη του δεν στηρίζεται σε κάποιο κανόνα δικαίου που προβλέπει αυτή ως νόμιμη και αφετέρου όταν κάποιος δεν έχει δικαίωμα να πράξει κατ' αυτόν τον τρόπο[84]. Στην αιτιολογική έκθεση του σχεδίου του Π.Κ του 1933 αναφέρεται ο όρος "αθέμιτα" υπο την έννοια[85] της, "*άνευ δικαιώματος χορηγούντος την προς τοιαύτην ενέργειαν εξουσίαν*". Απο την νομολογία του ανωτάτου Ακυρωτικού Δικαστηρίου, η έννοια αθέμιτα έχει

[82]**Βασιλάκη Ε.**, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών Υπολογιστών. Η αντιμετώπιση του προβλήματος ιδιαίτερα μετα την εισαγωγή του ν. 1805/1988 Α.Ν Σάκκουλας, Αθήνα 1993, σελ. 162-178, Λαμπάκη ρ., σε Χαραλαμπάκη, Αρ., Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο, 2η έκδοση, Νομική Βιβλιοθήκη, σελ. 2977 επ., Μυλωνόπουλου,. Χρ., ό.π., σελ. 72-73

[83]Λαμπάκη Χ., σε Χαραλαμπάκη Αρ., ό.π., σελ. 2960 επ.

[84]Λαμπάκη Χ., σε Χαραλαμπάκη Αρ., ό.π., σελ. 2960 επ., Μανωλεδάκη, Ι., Ερμηνεία κατ' άρθρο των όρων του Ειδικού μέρους του Π.Κ, 1996, σελ. 134

[85] Αιτιολογική Έκθεση Σχεδίου Ποινικού κώδικα 1933, σελ. 549-550

προσδιοριστεί ως "χωρίς σχετικό δικαίωμα ή χωρίς τη συναίνεση του ομιλούντος"[86].

Όσον αφορά το ζήτημα το όρου αθέμιτα υπο την έννοια ένταξής του ως στοιχείου της αντικειμενικής υπόστασης του εγκλήματος ή ως ειδικού στοιχείου του αδίκου, η νομολογία του Α.Π[87] μας επιλύει το ζήτημα υπέρ της δεύτερης περίπτωσης. Ωστόσο το ίδιο δεν συμβαίνει κι από τη θεωρία, που έχει κατατείνει στην άποψη[88] ότι "*η συναίνεση του ομιλούντος*" απο τη στιγμή που καταργεί την έννοια "παγίδευση ή παρέμβαση" συνιστά στοιχείο της αντικειμενικής υπόστασης του εγκλήματος μιας και διαπραγματευόμαστε ένα έννομο αγαθό που ο φορέας του έχει πλήρη εξουσία διαθέσεως[89]. Απο τη θεωρία του γενικού μέρους του ποινικού δικαίου η διάκριση αυτή έχει μεγάλη σημασία αφού ανάλογα μη την επιλογή του "στοιχείου" επηρεάζεται η θέση του κατηγορουμένου από την άποψη π.χ μιας πλάνης[90]. Έτσι αν θεωρήσουμε ότι ο όρος αθέμιτα αποτελεί στοιχείο της αντικειμενικής υπόστασης του εγκλήματος, η τυχόν πλάνη του δράστη ως προς το στοιχείο αυτό, θα είναι πραγματική με αποτέλεσμα την μη πλήρωση της αντικειμενικής υπόστασης του εγκλήματος, ενώ αν θεωρήσουμε τον ορό "αθέμιτα" ως ειδικό στοιχείο του αδίκου, η επερχόμενη πλάνη του δράστη θα είναι νομική[91] και θα πρέπει περαιτέρω να δικαιολογηθεί το συγγνωστό ή μη αυτής, προκειμένου ο δράστης να κριθεί ακαταλόγιστος.

Η αντικειμενική υπόστασή του εν λόγω αδικήματος πραγματώνεται με διαφορετικούς τρόπους τέλεσης. Οι τρόποι αυτοί είναι ***η αντιγραφή, η αποτύπωση, η χρησιμοποίηση, η αποκάλυψη σε τρίτον και η οπωσδήποτε παραβίαση στοιχείων*** ή προγραμμάτων υπολογιστών. Ως ***αντιγραφή*** θα μπορούσαμε να θεωρήσουμε την τοποθέτηση του στοιχείου ή του προγράμματος σε έναν υλικό φορέα χωρίς κατ' αποκλειστικότητα να

[86]Α.Π 1026/2008, ΠοινΧρ ΝΟ, σελ. 343 και Α.Π 2270/2009, σε www.areiospagos.gr/nomologia/apofaseis_result.asp?S=1

[87] Α.Π 1607/2007 Ποιν.Δικ 2008, σελ. 831

[88] Ανδρουλάκη Ν., Ποινικό Δίκαιο - Γενικό Μέρος (Θεωρία για το έγκλημα), 2η εκδ., σελ. 355,

[89] Μανωλεδάκη Ι., Ποινικό Δίκαιο - Γενική Θεωρία, 2004, σελ. 851.

[90] Άρθρο 30 παρ. 1 Π.Κ : Δεν πράττει με δόλο όποιος κατά το χρόνο τέλεσης της πράξης αγνοεί τα περιστατικά που τη συνιστούν. (πραγματική πλάνη).

[91] Άρθρο 31 παρ. 2 Π.Κ : Η πράξη όμως δεν καταλογίζεται σε εκείνον που την τελεί αν αυτός δεν είχε συνείδηση του άδικου χαρακτήρα της λόγω πλάνης που δεν μπορούσε να αποφύγει, μολονότι κατέβαλε την οφειλόμενη από τις περιστάσεις και δυνατή για αυτόν επιμέλεια (συγγνωστή νομική πλάνη). Αν ο υπαίτιος μπορούσε να αποφύγει την πλάνη η πράξη καταλογίζεται σε αυτόν, αλλά το δικαστήριο μπορεί να του επιβάλλει μειωμένη ποινή.

γίνεται χρήση τεχνικών μέσων, δηλαδή θα μπορούσαμε να στοιχειοθετήσουμε αντιγραφή και σε ένα συμβατικό έγγραφο - έντυπο με την μορφή της γραφής ή ακόμη και σχεδίασης. Η ***αποτύπωση*** περαιτέρω θα μπορούσε να αφορά την αναπαραγωγή ενός αντιγράφου προγράμματος ή δεδομένων από το πρωτότυπο[92] (π.χ. φωτοτυπία). Η ***αποκάλυψη σε τρίτο***, μπορεί να περιλαμβάνει την γνωστοποίηση του λογισμικού ή των στοιχείων που επιτρέπει την περαιτέρω εκμετάλλευσή τους[93]. Τέλος, ο τελευταίος τρόπος τέλεσης ***της οπωσδήποτε παραβίασης*** των απορρήτων έχει επικριθεί από τη θεωρία καθόσον η γενικότητά του, διευρύνει υπερβολικά το αξιόποινο[94]. Σύμφωνα με τη θεωρία ο συγκεκριμένος τρόπος τέλεσης θα πρέπει να αντιμετωπιστεί περιοριστικά, ώστε να αποδίδεται μόνο σε πράξεις ίσης απαξίας και βαρύτητας, με εκείνες των ανωτέρω τεσσάρων τρόπων τέλεσης του εγκλήματος, οι οποίοι το ανεβάζουν μια κλίμακα σε σχέση με την απλή πρόσβαση σε δεδομένα[95]. Το ίδιο είχε επικριθεί και η διάταξη του άρθρου 386Α όπως ίσχυε πριν την τροποποίησή της με το νόμο 4411/2016, αφού προβλέπονταν η τιμωρία του δράστη ακόμη κι αν το αδίκημα τελούνταν με οποιονδήποτε άλλο τρόπο, γεγονός που αποτελούσε μία αόριστη πρόβλεψη με αυξημένα όρια του τρόπου τέλεσης. Η προϊσχύουσα διάταξη του άρθρου 386Α τροποποιήθηκε τελικά, όπως πρέπει να τροποποιηθεί και η διάταξη του άρθρου 370Γ παρ. 1 ώστε να είναι οριοθετημένη και να πληροί τη συνταγματικά κατοχυρωμένη αρχή του Ποινικού δικαίου "nullum crimen nulla poena sine lege certra"[96]. Περαιτέρω, προκειμένου να πληρείται η αντικειμενική υπόσταση του άρθρου και ειδικότερα της παραγράφου 1 απαιτείται τα απόρρητα να είναι στοιχεία αποθηκευμένα σε υπολογιστή είτε να είναι προγράμματα υπολογιστή[97]. Η συγκεκριμένη διάταξη προστατεύει και τις

[92] Βασιλάκη Ε, ο.π., σελ. 178
[93] Ανδρέου., Ποινικός Κώδικας, σελ. 1505
[94] Καϊάφα - Γκμπάντι Μ., Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, σελ. 1071
[95] Κιούπη Δ., Ποινικό Δίκαιο και internet., σελ. 129
[96] Μανωλεδάκη Ι., Ποινικό Δίκαιο, ζ΄ έκδοση, Σάκκουλας Αθήνα - Θεσσαλονίκη 2005, σελ. 24 επ.
[97] Μυλωνόπουλος Χ., Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Α. Ν. Σάκκουλας, Αθήνα 1991, σελ.82

προσβολές που αφορούν το λογισμικό του ηλεκτρονικού υπολογιστή αλλά και όλα τα είδη προγραμμάτων μαζί με το συνοδευτικό υλικό τους[98].

Αξίζει να επισημάνουμε όσον αφορά το στοιχείο αυτό της αντικειμενικής υπόστασης του άρθρου 370Γ παρ.1 παρά τα προβλεπόμενα στο άρθρο 13 του Ποινικού Κώδικα στο οποίο προστέθηκαν οι όροι "πληροφοριακό σύστημα" και "ψηφιακά δεδομένα", με το νόμο 4411 /2016, δεν αντικαταστάθηκαν οι όροι κατ' αντιστοιχία με τις τροποποιήσεις που πραγματοποιήθηκαν στο άρθρο 370Δ παρ. 2 του Ποινικού Κώδικα. Στο άρθρο 370Δ παράγραφος 2 του Ποινικού Κώδικα, ο χρησιμοποιηθείς όρος "στοιχεία υπολογιστή" καθώς και ο όρος "στοιχεία περιφερειακής μνήμης υπολογιστή", αντικαταστάθηκαν με τον όρο "σύνολο ή τμήμα πληροφοριακού συστήματος". Η αντικατάσταση αυτή έλαβε χώρα καθόσον η διάταξη έπρεπε να συμβαδίζει με τις τεχνολογικές εξελίξεις αφενός και αφετέρου με την ενωσιακή νομοθεσία, ώστε να είναι δυνατή η τιμωρία της παράνομης πρόσβασης όχι μόνο σε βάρος ενός συστήματος ηλεκτρονικού υπολογιστή αλλά και σε οποιαδήποτε συσκευή που είναι ικανή να επεξεργάζεται αυτόματα τα ψηφιακά δεδομένα σύμφωνα με ένα πρόγραμμα, όπως π.χ tablets, smartphones και λοιπές συσκευές. Τελικά η διάταξη του άρθρου 370Γ παρ. 1 παρέμεινε ως είχε και μετά την ψήφιση του νέου κώδικα, χωρίς να αντικατασταθούν οι όροι "στοιχεία ή προγράμματα υπολογιστών" με τους νέους όρους που ήδη είχαν προστεθεί στο άρθρο 370Δ παρ. 2 και στο άρθρο 13 του Ποινικού Κώδικα, ως ψηφιακά δεδομένα "συνόλου ή τμήματος πληροφοριακού συστήματος". Αυτό σημαίνει ότι, αν έχουμε μία αντιγραφή, αποτύπωση η χρησιμοποίηση ενός κρατικού, επιστημονικού ή επαγγελματικού απορρήτου, ως στοιχείου η προγράμματος υπολογιστή, που υπάρχει σε μία διαφορετική συσκευή από εκείνο του ηλεκτρονικού υπολογιστή, όπως για παράδειγμα σε ένα Smartphone, παραμένει ατιμώρητη καθόσον δεν προστατεύεται από το άρθρο 370Γ παρ. 2 του Ποινικού Κώδικα. Με την αλματώδη τεχνολογική εξέλιξη είναι μαθηματικά βέβαιο ότι αυτό θα συμβεί στην πράξη αφού οι επαγγελματίες έχουν σταδιακά και στο πέρασμα του χρόνου αντικαταστήσει τους ηλεκτρονικούς υπολογιστές με άλλες συσκευές πιο εύχρηστες που έχουν τη δυνατότητα να

[98] **Βασιλάκη Ε.**, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών Υπολογιστών. Η αντιμετώπιση του προβλήματος ιδιαίτερα μετα την εισαγωγή του ν. 1805/1988 Α.Ν Σάκκουλας, Αθήνα 1993, σελ. 222 και ΠοινΔικ 2004, σελ. 1110

προσομοιάζουν με έναν ηλεκτρονικό υπολογιστή και να διεκπεραιώνουν τις εργασίες του. Έτσι η διάταξη του άρθρου 370Γ παρ. 2 πρέπει να τροποποιηθεί ως προς τον όρο "**στοιχεία ή προγράμματα υπολογιστών**" και να αντικατασταθούν οι όροι με τους "**ψηφιακά δεδομένα συνόλου ή τμήματος πληροφοριακού συστήματος**" προκειμένου, ως ανωτέρω αναγράφηκε, να συμβαδίζει η πράξη με τις προβλέψεις του ενωσιακού δίκαιου ώστε να μην βρίσκονται οι πράξεις αυτές στη σφαίρα το απυρόβλητου.

Η διάταξη του άρθρου 370Γ του Ποινικού Κώδικα προβλέπει την τιμωρία για την παραβίαση συγκεκριμένων μορφών απορρήτου. Γίνεται λόγος, για προστασία κρατικών απορρήτων, εκείνων δηλαδή που έχουν σημασία για την υπόστασή του Κράτους καθώς και εκείνων, που εξαιτίας της φύσης τους, η θέληση της Κυβέρνησης έγκειται στη μη γνωστοποίηση σε τρίτα πρόσωπα που βρίσκονται έξω από το Κυβερνητικό σχήμα, αφού η αποκάλυψή τους μπορεί να βλάψει τα συμφέροντα του Ελληνικού κράτους[99]. Η έννοια Κρατικό απόρρητο βρίσκεται στο δεύτερο κεφάλαιο του ειδικού μέρους του Ποινικού Κώδικα και τιτλοφορείται ως παραβίαση μυστικών της πολιτείας. Εκεί προστατεύεται το Κρατικό μυστικό - απόρρητο, αφού η τυχόν διάρρευσή του σε άλλους θα έθετε σε κίνδυνο την ασφάλεια και τα συμφέροντα της πολιτείας. Το **Κρατικό μυστικό-απόρρητο** ορίζεται ώς ένα γεγονός, αντικείμενο ή πληροφορία, που η πρόσβαση είναι δυνατή σε ένα προσδιορισμένο κύκλο προσώπων για να αποφευχθεί ο κίνδυνος προσβολής της εδαφικής ακεραιότητας, της αμυντικής ικανότητας, των διεθνών σχέσεων, ή των οικονομικών συμφερόντων του Ελληνικού κράτους και της διεθνούς ειρήνης[100]. Ως ***επιστημονικά απόρρητα*** θεωρούνται αυτά που περιέχουν γνώσεις αφορώσες γνωστικά αντικείμενα υπαγόμενα σε συγκεκριμένη συστηματική-μεθοδολογική κατάταξη όπως π.χ. μία αδημοσίευτη επιστημονική εργασία, μία μελέτη, ή ένα άρθρο, κ.τ.λ.[101]. Ως **επαγγελματικά απόρρητα**, η απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα

[99] Χαραλαμπάκη, Α., Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο, 2η έκδοση Νομική Βιβλιοθήκη 2014., σελ. 2980

[100] Βλ. Αιτιολογική Έκθεση του ν. 4619/2019 για την καινούργια προσθήκη του άρθρου 149 Π.Κ που αφορά την επεξήγηση του όρου κρατικό απόρρητο προς άρση των υπαρχουσών αμφισβητήσεων.

[101] Χαραλαμπάκη Α., Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο, 2η έκδοση Νομική Βιβλιοθήκη 2014., σελ. 2980

θεωρούνται αυτά που βρίσκονται στην κατοχή της επιχείρησης και τα οποία αποτελούν όπως έχει ήδη κριθεί από τη νομολογία, τα στοιχεία που αφορούν συναλλαγές μιας εταιρείας με άλλες εταιρείες ή αφορούν μετοχικό κεφάλαιο που απεικονίζει ξένους ή και Έλληνες επενδυτές ή αναφέρονται σε ισοζύγια ή καταστάσεις που αφορούν επιταγές ή καρτέλες λογαριασμών που περιέχουν επιταγές και αφορούν συναλλαγές της εταιρείας[102]. Περαιτέρω, ως απόρρητα θεωρούνται και αυτά που ο νόμιμος κάτοχος θα μεταχειρίζεται ως απόρρητα σύμφωνα με την πρόβλεψη του άρθρου 370Γ παρ. 2 εδάφιο β΄ του Ποινικού Κώδικα. Η έννοια της κατοχής στη συγκεκριμένη περίπτωση είναι διαφορετική σε σχέση με την έννοια που βρίσκουμε στα εγκλήματα κατά της ιδιοκτησίας, αφενός γιατί πραγματεύεται ένα διαφορετικό αντικείμενο και αφετέρου γιατί προσδιορίζεται ως μία κατάσταση στηριζόμενη στο νόμο. Σύμφωνα με τη νομολογία[103], η κατοχή είναι η δυνατότητα εξουσίας των στοιχείων ενός προγράμματος δεν είναι απαραίτητο να στηρίζεται σε πραγματική κατοχή αλλά αντίθετα να στηρίζεται σε κάποιο νόμιμο δικαίωμα.

7.2 Η παράγραφος 2 του άρθρου 370Γ ως προς τη διακεκριμένη μορφή.

Σύμφωνα με την παράγραφο 2 του άρθρου 370Γ, η οποία προβλέπει ότι "*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*". Ο νομοθέτης εδώ θεσπίζει διακεκριμένη μορφή του βασικού εγκλήματος της παραγράφου 1 στις δύο κατωτέρω περιπτώσεις, αφενός όταν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων και αφετέρου όταν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας. Στις περιπτώσεις αυτές, επιβάλλεται ποινή τουλάχιστον ενός έτους. Θα μπορούσαμε να πούμε ότι ο δράστης βρίσκεται στην υπηρεσία του κατόχου όταν παραδείγματος χάρη, συνδέεται με αυτόν με σχέση εξαρτημένης ή ανεξάρτητης εργασίας. Ο λόγος που οδηγεί τον νομοθέτη στην

[102] ΣυμβΑΠ 1294/2007, Τ.Ν.Π "Νόμος"
[103] Χαραλαμπάκη Α., Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο, 2η έκδοση Νομική Βιβλιοθήκη 2014., σελ. 2980 και ΣυμβΕφΑθ 2949/2003 ΠοινΔικ 2004, σελ. 1110

επαύξηση των ορίων της ποινής, έχει να κάνει αφενός με την ευκολία προσβολής του εννόμου αγαθού από το δράστη, αλλά και με την ενδεχόμενα γνώση των στοιχείων που ήδη μπορεί να μεταχειρίζεται, ενώ αφετέρου στην οικονομική αξιολόγηση της ζημίας, είτε στην περιουσία του θύματος, είτε της ωφέλειας που αποφέρει στο δράστη. Άξιο μνείας είναι ότι κατά την ψήφιση του νέου ποινικού κώδικα (νομος 4619/2019) απαλείφθηκε η παράγραφος 3, η οποία αναφέρονταν σε παραβίαση στρατιωτικών και διπλωματικών απόρρητων. Το πρόβλημα που δημιουργούνταν με την προϊσχύσασα διάταξη είχε να κάνει με την τιμωρία των δραστών όταν προσβάλλονται τα στρατιωτικά και διπλωματικά απόρρητα κάτι που θα μπορούσε να λυθεί και με τους κανόνες περί αληθινής συρροής. Οι προϊσχύουσες διατάξεις, έτσι όπως είχαν θεσπιστεί, άφηναν ατιμώρητο τον δράστη για το άδικο που περιέχονταν στην διάταξη του πρώην άρθρου 370Β του Ποινικού Κώδικα, ενώ ακόμη προκαλούσε σύγχυση ως προς το προστατευόμενο έννομο αγαθό αφού τιμωρούνταν ένα ατομικό αγαθό με μία διάταξη που προστάτευε ένα κρατικό έννομο αγαθό, (της Ασφάλειας του Κράτους).

7.3 Η παράνομη πρόσβαση σε πληροφοριακό σύστημα. (άρθρα 370Β παρ. 1 και 370Δ παρ. 2)

Η χωρίς δικαίωμα πρόσβαση σε σύστημα ηλεκτρονικού υπολογιστή, δηλαδή το κοινώς λεγόμενο hacking, ποινικοποιήθηκε για πρώτη φορά με το άρθρο 4 του νόμου 1805 / 1988 που προσέθεσε το άρθρο 370Γ παρ. 2 στον Ποινικό μας κώδικα. Υποστηρίχθηκαν πολλές απόψεις σχετικά με το έννομο αγαθό που προστατεύεται με το άρθρο 370Γ παρ. 2 του Ποινικού Κώδικα με περισσότερο επικρατέστερη την άποψη[104] ότι αναφέρεται στο απόρρητο υπό τυπική έννοια δηλαδή το δικαίωμα του νόμιμου κατόχου των δεδομένων να τηρεί αυτά ως απόρρητα και κατ' επέκταση να αποκλείει την πρόσβαση οιουδήποτε τρίτου σε αυτά[105]. Στην προκειμένη περίπτωση το περιεχόμενο

[104] Ιγγλεζάκη Ι., Δίκαιο της πληροφορικής, β΄ έκδοση Σάκκουλα, Αθήνα - Θεσσαλονίκη, 2008, σελ. 279,

[105] Ως προς την τυπική και ουσιαστική έννοια του απορρήτου, βλ ΠοινΧρ ΝΔ/2004 σελ. 75,. που αναφέρει ότι η διάταξη του 370Γ παρ. 2 ΠΚ αποσκοπεί στην τιμωρία της παραβιάσεως

του απορρήτου ταυτίζεται με την εμπιστευτικότητα (confidentiality) ως μία έκφανση της ασφάλειας των δεδομένων και στοιχείων, δηλαδή την ιδιότητα των στοιχείων ενός ηλεκτρονικού συστήματος να καθίστανται προσπελάσιμα μόνο από χρήστες που έχουν εξουσιοδοτηθεί προς τούτο. Το έννομο αγαθό, είναι ατομικό, αφού για το αδίκημα του άρθρου αυτού απαιτείται έγκληση του παθόντα. Για την πραγμάτωση της αντικειμενικής υπόστασης του εγκλήματος αυτού, απαιτείται πρόσβαση σε δεδομένα ή στοιχεία. Η πρόσβαση εδώ αναφέρεται στην ενέργεια του δράστη που κατατείνει στην ανάγνωση, απόκτηση, ή αλλοίωση των στοιχείων του υπολογιστή που λαμβάνει χώρα είτε μέσω τηλεπικοινωνιών, είτε όχι. Περαιτέρω είναι αδιάφορο αν ο δράστης έλαβε γνώση των στοιχείων ή όχι. Χαρακτηριστικά παραδείγματα από τη νομολογία, που εντάχθηκαν στον τιμωρητικό χαρακτήρα του άρθρου 370Γ παρ. 2, είναι η παραβίαση τραπεζικών δεδομένων, το pharming, και το hacking[106], ενώ κρίθηκε ότι το φαινόμενο των "ιών - viruses", δεν εντάσσεται στο πεδίο εφαρμογής του άρθρου 370Γ του Ποινικού Κώδικα, αλλά στο άρθρο 381 Π.Κ αφού πλήττει την ιδιοκτησία και όχι το απόρρητο. Όσον αφορά την παραβίαση των μέτρων ασφαλείας ένα ενδεικτικό παράδειγμα αποτελεί η παραβίαση του ειδικού κωδικού πρόσβασης password, ενώ ο νομοθέτης χρησιμοποίησε τότε, τη λέξη **ιδίως**, που σημαίνει ότι η παραβίαση των μέτρων ασφαλείας δεν είναι απαραίτητη για να θεμελιωθεί το αξιόποινο του άρθρου 370Γ παρ.2 Π.Κ., αφού αρκεί η βούληση του νόμιμου κατόχου να έχει τα στοιχεία σε κάποιο ιδιωτικό χώρο[107].

Όσον αφορά τον όρο "στοιχεία", εννοούνται εκείνα που έχουν εισαχθεί σε ηλεκτρονικό Υπολογιστή ή περιφερειακή μνήμη π.χ usb sticks, thumb drives, hard drives, κτλ και όχι όσα "στοιχεία" δεν έχουν αποθηκευτεί σε αυτά τα μέσα, γιατί δεν μπορούσαν να υπαχθούν σε αυτή τη διάταξη[108]. Η έννοια χωρίς δικαίωμα πρέπει να επεξηγηθεί με γνώμονα το προστατευόμενο έννομο

μυστικών που έχουν να κάνουν με προγράμματα ηλεκτρονικών υπολογιστών και εξ' αυτού, προστατεύεται το ουσιαστικό απόρρητο των προγραμμάτων.

[106] Βασιλάκη Ε., Τα φαινόμενα pharming, phishing και η ποινική τους αξιολόγηση, ΠοινΧρ2007, σελ. 861 επ.

[107] Σπυρόπουλος Φ., Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (Hacking), Ποινική και εγκληματολογική προσέγγιση - Αξιολόγηση της Ελληνικής Ποινικής Νομοθεσίας - Έρευνα σε δείγμα νομικών, επιστημόνων πληροφορικής και hackers, Σειρά: ΠΟΙΝΙΚΑ, Α. Ν. Σάκκουλας, Αθήνα 2016., σελ. 191.

[108] Μυλωνόπουλος Χ., Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Σειρά: ΠΟΙΝΙΚΑ, Α. Ν. Σάκκουλας, Αθήνα 1991

αγαθό. Η έννοια χωρίς δικαίωμα αποκλείει την πλήρωση της αντικειμενικής υπόστασης του εγκλήματος και αυτή δεν αναφέρεται μόνο ως ένα ειδικό στοιχείο του αδίκου. Σε περίπτωση που δοθεί η σχετική εξουσιοδότηση δεν έχουμε καν προσβολή του εννόμου αγαθού[109].

Με τη μεταφορά της Οδηγίας 2013/40 ΕΕ το άρθρο 370Γ παρ. 2 τροποποιήθηκε ως εξής: "*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 κάτοχος του, τιμωρείται με φυλάκιση*".

Η ίδια διάταξη, με τα προβλήματα που θα δούμε ευθύς αμέσως, μεταφέρθηκε και στο νέο Ποινικό Κώδικα και εναριθμήθηκε σε άρθρο 370Δ παρ. 2. Παράλληλα όμως στο άρθρο 370Β παρ. 1 του νέου ποινικού κώδικα υφίσταται παρόμοια διάταξη, νομοτεχνικά σαφώς βελτιωμένη, που όμως απο την αιτιολογική έκθεση[110], δεν προκύπτει καθαρά η αιτιολογική βάση ύπαρξης δύο παρόμοιων διατάξεων σε δύο ξεχωριστά άρθρα, πλην της επισήμανσης ότι στο νέο ποινικό κώδικα και ειδικότερα στο άρθρο 370Β εντάχθηκε το έγκλημα που τυποποιούνταν, έως σήμερα, στο άρθρο 370Γ, νομοτεχνικά βελτιωμένο με τους όρους "πληροφοριακό σύστημα" και "ηλεκτρονικά δεδομένα[111]".

Αν προσπαθήσουμε να συγκρίνουμε τις δύο αναφερόμενες διατάξεις σε σχέση με το προηγούμενο καθεστώς μπορούμε να σταθούμε σε τρείς επισημάνσεις. Σύμφωνα με το άρθρο 3 της οδηγίας 2013/40/ΕΕ, ο όρος που χρησιμοποιείται εκεί είναι το "σύστημα πληροφοριών" και όχι "πληροφορικό σύστημα" και αντί των "ηλεκτρονικών δεδομένων" ο όρος των "ψηφιακών δεδομένων". Καταργείται ο όρος στοιχεία που είναι αποθηκευμένα σε υπολογιστή ή περιφερειακή μνήμη αφού καλύπτεται από την έννοια του πληροφοριακού συστήματος, παρόλα αυτά όμως η νέα διάταξη περιλαμβάνει ξανά τον όρο "στοιχεία" αντί της έννοιας "ψηφιακά δεδομένα". Η ίδια διάταξη όμως περιλαμβάνεται εκτός του άρθρου 370Δ παρ. 2 και στο άρθρο 370Β

[109] Σπυρόπουλος Φ., Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (Hacking), Ποινική και εγκληματολογική προσέγγιση - Αξιολόγηση της Ελληνικής Ποινικής Νομοθεσίας - Έρευνα σε δείγμα νομικών, επιστημόνων πληροφορικής και hackers, Σειρά: ΠΟΙΝΙΚΑ, Α. Ν. Σάκκουλας, Αθήνα 2016., σελ. 195 επ.
[110] Βλ. Αιτιολογική Έκθεση ν. 4619/2019 σελ. 71 επ.
[111] Βλ. Αιτιολογική Έκθεση ν. 4619/2019 σελ. 71 επ.

παρ. 1 σαφώς νομοτεχνικά βελτιωμένη ώστε να συμβαδίζει με τις διατάξεις του ενωσιακού δικαίου, με τους όρους "σύστημα πληροφοριών" και "ηλεκτρονικά δεδομένα". Είναι φυσικό για την ασφάλεια και την εφαρμογή του δικαίου να τεθούν σαφείς διατάξεις που θα τυγχάνουν εφαρμογής σε κάθε περίπτωση, οι οποίες να μην παρουσιάζουν "apriori" ερμηνευτικά προβλήματα ή να προκαλούν σύγχυση. Οι όροι "σύστημα πληροφοριών" και "ψηφιακά δεδομένα" ερμηνεύονται και αναλύονταιι στο άρθρο 13 του νέου Π.Κ και ανέμενε κανείς αυτοί οι όροι να χρησιμοποιηθούν στα αντίστοιχα άρθρα περί ηλεκτρονικών παραβιάσεων, κάτι που επιτυγχάνεται τώρα, μόνο κατα μέρος.

Περαιτέρω και σε σχέση με την απειλούμενη ποινή, το μεν άρθρο 370Β παρ. 1 τιμωρεί το δράστη με φυλάκιση έως δύο έτη και χρηματική ποινή, το δε άρθρο 370Δ παρ. 2 τιμωρεί το δράστη με φυλάκιση από 10 ημέρες μέχρι πέντε 5 έτη ήτοι με φυλάκιση. Η επιταγή της Οδηγίας 2013/40/ΕΕ (άρθρο 9) για τη θέσπιση ανωτάτου ορίου ποινής φυλάκισης τουλάχιστον δύο ετών, επιτυγχάνεται μόνο στο άρθρο 370Δ παρ. 2. βάσει της οποίας τιμωρείται ο δράστης που πληροί την αντικειμενική υπόσταση του άρθρου αυτού, με όριο ποινής 10 ημέρες μέχρι 5 έτη, χωρίς να γίνεται διάκριση περι ήσσονος σημασίας παραβιάσεις. Αντιθέτως στο άρθρο 370Β παρ.1, λαμβάνει χώρα διάκριση περι των ήσσονος σημασίας παραβιάσεων αφού κρίνονται αυτές ατιμώρητες, πλην όμως το ανώτατο όριο ποινής έχει τεθεί η φυλάκιση έως το πολύ δύο έτη.

Στις ως άνω δυο προβλέψεις, ήτοι άρθρα 370Β παρ. 1 και 370Δ παρ. 2, τιμωρείται η πρόσβαση, μόνο εφόσον γίνεται κατα παράβαση των μέτρων ασφαλείας και απαγορεύσεων που έχει θέσει ο νόμιμος κάτοχος. Φαίνεται δηλαδή ότι τα δεδομένα δεν προστατεύονται όταν ο νόμιμος κάτοχος έχει βούληση στο να διατηρήσει αυτά απόρρητα πλην όμως δεν έχει λάβει κάποια μέτρα ασφαλείας.

Τέλος, από τη σύγχυση που προκαλουν οι θεσπισθείσες διατάξεις υπο το νέο ποινικό κώδικα πρόβλημα δημιουργείται και στο τρόπο δίωξης των συναφών εγκλημάτων. Έτσι, στην μεν 370Β παρ. 1 η δίωξη του εγκλήματος λαμβάνει χώρα μόνο κατ᾽ έγκληση του παθόντα, ενώ στην 370Δ παρ. 2

αυτεπαγγέλτως[112]. Το πρόβλημα που δημιουργείται εδώ, από τις δύο εν λόγω διατάξεις, είναι προφανές πλην όμως καταλείπεται η περαιτέρω ανάλυσή του, αφού δεν πληροί το σκοπό της παρούσης εργασίας.

Συνοπτικά, θα λέγαμε ότι αν συγκεράσουμε τις δύο διατάξεις ο σκοπός του νομοθέτη ήταν η όσο το δυνατόν καλύτερη συμμόρφωση του τελευταίου στις επιταγές του Ενωσιακού ομοίου, αλλά και της Σύμβασης για το Κυβερνοέγκλημα. Η προστασία της εμπιστευτικότητας των συστημάτων πληροφοριών ως ειδικότερη έκφανση του απορρήτου, παρέχει τη δυνατότητα στο νόμιμο κάτοχό τους να ορίζει το ποιός μπορεί να έχει πρόσβαση στα δεδομένα. Τότε μόνο συμβαδίζει το προστατευόμενο έννομο αγαθό με το έννομο αγαθό που ορίζεται στη Σύμβαση του Συμβουλίου. Από την άλλη πλευρά για την αποτελεσματική δίωξη των πράξεων αυτών, δεν χωρεί αμφιβολία ότι, οι θεσπισμένες διατάξεις θα πρέπει να είναι απαλλαγμένες, όσο το δυνατόν, από κάθε είδους προβλήματα που γεννούν περαιτέρω ερμηνείες και συγκρούσεις.

7.4 Η υποκλοπή των δεδομένων ή ηλεκτρομαγνητικών εκπομπών (αρ. 370Ε Π.Κ).

Στο άρθρο 370Ε παρ. 1 ορίζεται ότι: "όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς η εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους τιμωρείται με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή".

Η διάταξη αυτή ενσωματώνει το άρθρο 3 της σύμβασης για το κυβερνοέγκλημα καθώς και το άρθρο 6 της οδηγίας της Ευρώπης και τιμωρείται πλέον η παραβίαση του απορρήτου των Επικοινωνιών, μέσω Πληροφοριακών Συστημάτων, αλλά και η χρήση των πληροφοριών[113]. Με το

[112] Βλ. παρακάτω το συγκριτικό πίνακα διατάξεων. σελ. 88-89

[113] Βαγενά Ε., Το νέο θεσμικό Πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος, ΔιΜΕΕ 2017, σελ. 35, όπου αναφέρεται ότι μέχρι σήμερα οι αντίστοιχες πράξεις διώκονταν σύμφωνα

άρθρο αυτό του νέου Ποινικού Κώδικα προστατεύεται η υποκλοπή ηλεκτρονικής επικοινωνίας email που αποστέλλεται μέσω ταχυδρομείου αλλά και η παραβίαση κάθε διαδικτυακής επικοινωνίας. Σύμφωνα με τη νομολογία[114] η παραβίαση αυτή δεν μπορούσε να υπαχθεί στην πρόβλεψη του άρθρου 370Α Π.Κ.. Η δυνατότητα του νόμιμου χρήστη των δεδομένων να επιλέγει τα πρόσωπα που θα γνωστοποιήσει τα δεδομένα αυτά, αλλά και η προστασία της ιδιωτικότητάς τους, αποτελεί και το έννομο αγαθό που προστατεύεται από τη διάταξη αυτή. Στην ουσία προστατεύεται το απόρρητο της επικοινωνίας, μέσω των Πληροφοριακών Συστημάτων, η λεγόμενη δηλαδή εμπιστευτικότητα (confidentiality) των δεδομένων.

Η αντικειμενική υπόσταση του αδικήματος αυτού μπορεί να τελεστεί με διάφορους τρόπους, με πρώτο αυτόν της **παρακολούθησης**, της **αποτύπωσης** σε υλικό φορέα, καθώς και της **παρέμβασης** σε διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικών εκπομπών. Το άρθρο 6 της οδηγίας αναφέρεται σε παράνομη υποκλοπή δημοσίων διαβιβάσεων χωρίς όμως περαιτέρω να γίνεται ανάλυση του ορισμού της υποκλοπής. Στην υπ΄ αριθμό 9 σκέψη της οδηγίας αναφέρεται ενδεικτικά, σε τι μπορεί να συνίσταται η αναφερόμενη υποκλοπή και ειδικότερα αναφέρει την ακρόαση, τον έλεγχο και την επιτήρηση του περιεχομένου των επικοινωνιών. Ο εθνικός νομοθέτης εισήγαγε διαφορετικές λέξεις στον Ποινικό Κώδικα αφού η οδηγία ανέφερε ενδεικτικούς τρόπους και όχι εξαντλητικούς. Ο πρώτος τρόπος τέλεσης, αυτός δηλαδή της "**παρακολούθησης**" μοιάζει με τον όρο της "παγίδευσης" του εγκλήματος της υποκλοπής των τηλεφωνικών επικοινωνιών όπου μέσω ενός τεχνικού μέσου (κοριού) παρακολουθείται μία τηλεφωνική συνομιλία. Αυτό βέβαια μπορεί να επιτευχθεί και από απόσταση με τη χρήση παραδείγματος χάρη κάποιου κακόβουλου λογισμικού. Ο δεύτερος τρόπος τέλεσης που αφορά την "**αποτύπωση**" αποτελεί εδώ στοιχείο της αντικειμενικής υπόστασης του αδικήματος και όχι σκοπό του δράστη όπως προβλέπει το άρθρο 370Α παρ. 1[115]. Τέλος **η παρέμβαση,** αποτελεί μία γενικότερη έννοια

με το νόμο 3115/2003 για την παραβίαση του απορρήτου των επικοινωνιών, με το νόμο 2472/1997 σχετικά με τα δεδομένα προσωπικού χαρακτήρα καθώς και με το νόμο 3471/2006.

[114] ΕφΑθ 9099/2005, ΔιΜΕΕ 2005, σελ. 561

[115] Χαραλαμπάκη Α., Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο, 2η έκδοση Νομική Βιβλιοθήκη 2014., σελ. 2962 επ.

που ετέθη προφανώς για να καλυφθεί η οποιαδήποτε παρεμβολή στη διαβίβαση δεδομένων, από, προς, ή εντός πληροφοριακού συστήματος.

Στην αιτιολογική σκέψη 54 της σύμβασης για το κυβερνοέγκλημα, ορίζεται ότι η έννοια της μη δημόσιας διαβίβασης των δεδομένων δεν θα πρέπει να λαμβάνει υπόψη τη φύση των δεδομένων που μεταδίδονται, αλλά τη καθαυτή διαβίβαση, ώστε να διαφαίνεται η πρόθεση εμπιστευτικής επικοινωνίας. Η επικοινωνία μπορεί να γίνει ανάμεσα σε δύο υπολογιστές που ενδεχομένως ανήκουν στο ίδιο πρόσωπο ή μεταξύ υπολογιστών που βρίσκονται σε διαφορετική τοποθεσία. Ο ορισμός της μη δημόσιας διαβίβασης από τη Σύμβαση, είναι σύμφωνος και με τη θεωρία η οποία αναφέρει ότι **μη δημόσιες** πράξεις είναι αυτές που δεν μπορούν να γίνουν αντιληπτές από αόριστο αριθμό προσώπων.

Όσον αφορά την υποκειμενική υπόσταση του εγκλήματος αυτό κατατάσσεται στα υπερχείλους υποκειμενικής υπόστασης, αφού απαιτείται σκοπός του δράστη προκειμένου να πληροφορηθεί αυτός ή άλλος το περιεχόμενο των δεδομένων καθώς και των ηλεκτρομαγνητικών εκπομπών των Πληροφοριακών Συστημάτων. Η μόνη διαφορά που παρατηρούμε σε σχέση με το άρθρο 370Α παρ. 1 του Ποινικού Κώδικα είναι ότι, η αποτύπωση σε υλικό φορέα στο άρθρο 370Ε παρ. 1 αποτελεί τρόπο τέλεσης του αδικήματος, δηλαδή είναι στοιχείο της αντικειμενικής υπόστασης του εγκλήματος και όχι στοιχείο της υποκειμενικής υπόστασης του δράστη. Όσον αφορά το πλαίσιο της ποινής η παραβίαση του άρθρου αυτού καθώς και του άρθρου 370Α παρ. 1, επισύρει φυλάκιση με σαφώς αυστηρότερο όριο για το πρώτο εκ των αναφερομένων άρθρο, αφού προβλέπεται ποινή φυλάκισης τουλάχιστον τριών ετών. Το σημαντικότερο εδώ είναι ότι ο εθνικός νομοθέτης τροποποίησε το είδος της προγενέστερης ποινής που προβλέπονταν με το προηγούμενο καθεστώς, από κάθειρξη σε φυλάκιση, συμφωνώντας θα λέγαμε με τις κυρώσεις που προέβλεπε η οδηγία της Ευρωπαϊκής Ένωσης, πλην όμως δεν θα μπορούσε να μείνει απαρατήρητη η διαφορετικότητα αντιμετώπισης περιστατικών που αφορά π.χ μια ίδιας φύσεως υποκλοπή από σύνδεση ή δίκτυο σταθερής - κινητής τηλεφωνίας, σε σχέση με την ίδια υποκλοπή δεδομένων πληροφοριακού συστήματος, αφού το δεύτερο και τελευταίο τιμωρείται με αυστηρότερο πλαίσιο ποινής. Περαιτέρω τυποποιείται αυτοτελώς

η χρησιμοποίηση μιας πληροφορίας ή του υλικού στο οποίο αποτυπώθηκε κατόπιν υποκλοπής μη δημόσιων διαβιβάσεων μεταξύ πληροφοριακού συστήματος. Σύμφωνα με τη νομολογία ως χρήση θεωρείται η αποστολή ηλεκτρονικής επιστολής όπου εμπεριέχονται συνημμένα διάφορα αρχεία με απόρρητα δεδομένα που ανταλλάσσονταν μεταξύ πληροφοριακού συστήματος, ή η διαρροή προσωπικής ηλεκτρονικής αλληλογραφίας στα μέσα κοινωνικής δικτύωσης. Ο καινούργιος ποινικός κώδικας[116], καταργεί την παράγραφο 3 του άρθρου 370Ε αφού η επιλογή της παραπομπής των υποκλοπών που αφορούν στρατιωτικά ή διπλωματικά απορρήτα αναφέρεται σε άλλο κεφάλαιο, όπου το έννομο αγαθό αφορά την ασφάλεια του Κράτους και επιλύει πλέον τα προβλήματα που παρουσιάζονταν με την προηγούμενη πρόβλεψη.

7.5 Η παρακώλυση λειτουργίας Πληροφοριακών Συστημάτων (Άρθρο 292 Β του Π.Κ)

Το έγκλημα του άρθρου αυτού τελείται από εκείνον που 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. Η διάταξη αυτή προστατεύει την ακεραιότητα του πληροφοριακού συστήματος, τη λειτουργία αυτού, την ορθή επεξεργασία ενός μεγάλου όγκου πληροφοριών, καθώς και την παροχή διαφόρων υπηρεσιών. Πρόκειται για ένα κοινωνικό έννομο αγαθό αφού πλέον ρητά, περιγράφεται στην αιτιολογική έκθεση ότι αφορά έναν ευρύτερο αριθμό ατόμων και για το λόγο αυτό η πράξη διώκεται πλέον αυτεπάγγελτα. Όπως φαίνεται εδώ ο νομοθέτης έλαβε υπόψη του τις επισημάνσεις και τις παρατηρήσεις που θεμελιώθηκαν κατά την θεωρητική ανάλυση του εγκλήματος αυτού[117]. Περαιτέρω είναι ένα έγκλημα διαζευκτικά

[116] Βλ,. Νόμο 4619/2019 "Νέος Ποινικός Κώδικας"

[117]Χατζηνικολάου Ν., Ποινικό Δίκαιο - Ειδικό Μέρος, Εγκλήματα κατα τις ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών, των κοινωφελών εγκαταστάσεων, της λειτουργίας πληροφοριακών συστημάτων (άρθρα 290-298 Π.Κ), Π.Ν. Σάκκουλας, Αθήνα 2017, σελ. 184.

μικτό με διάφορους τρόπους[118] τέλεσης, οι οποίοι μπορούν να εναλλάσσονται. Συγκεκριμένα προβλέπεται η εισαγωγή, η διαβίβαση, η διαγραφή, η καταστροφή, η αλλοίωση ψηφιακών δεδομένων και ο αποκλεισμός της πρόσβασης σε αυτά. Ως εισαγωγή θεωρείται η είσοδος νέων δεδομένων ενώ ως διαβίβαση θεωρείται η αποστολή από απόσταση ηλεκτρονικών μηνυμάτων ή ακόμη και η χειροκίνητη μεταφορά μέσω κινητών μέσων αποθήκευσης[119]. Όσον αφορά τον αποκλεισμό της πρόσβασης στα δεδομένα ενός συστήματος πληροφοριών, αυτός μπορεί να συντελεστεί είτε με την επέμβαση στα δεδομένα όπως π.χ με την αλλαγή ενός κωδικού πρόσβασης είτε με την παρέμβαση σε κάποιο υλικό του μέρος. Το τελευταίο φαίνεται ιδιαίτερα προβληματικό, αφού στη θεωρία γίνεται λόγος για το αν μπορεί να υπαχθεί στην διάταξη αυτή ή θα πρέπει, μια τέτοια υλική παρέμβαση, να αντιμετωπιστεί σύμφωνα με τις διατάξεις περί κοινής φθοράς. Το δεύτερο φαίνεται κατα τη γνώμη μου επικρατέστερο αφού και στο άρθρο 5 της Σύμβασης για το Κυβερνοέγκλημα αναφέρεται ρητά η ποινικοποίηση της παρεμβολής σε συστήματα πληροφοριών με τη χρήση ή επιρροή δεδομένων υπολογιστών[120]. Περαιτέρω ζητήματα προκαλούν οι έννοιες που έχουν εισαχθεί στο άρθρο 292Β και αφορούν τη σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών. Η έννοια ειδικά της σοβαρής "παρεμπόδισης" δεν μπορεί να συγκριθεί με την έννοια της σοβαρής "παρακώλυσης" που συναντάται σε άλλη διάταξη του Π.Κ. Η "παρακώλυση ή παρεμπόδιση" κατα τον Π.Κ έχει την έννοια του αποκλεισμού μια υπηρεσίας. Στο άρθρο 292 Π.Κ η έννοια της παρεμπόδισης της λειτουργίας των κοινόχρηστων συγκοινωνιακών μέσων, είναι ταυτόσημη με τη διακοπή. Ο σκοπός του νομοθέτη πάντως αποκλείει το αξιόποινο για την απλή "δυσχέρανση"[121]. Στο άρθρο 290 Π.Κ η διατάραξη της ασφάλειας των συγκοινωνιών εξιδικεύεται περαιτέρω χωρίς να διακόπτεται η κυκλοφορία στους δρόμους, αλλά λαμβάνει χώρα με την πρόκληση προβλημάτων που τίθενται απο το δράστη και θέτουν σε κίνδυνο την ασφάλεια των

[118] Χατζηνικολάου Ν., ό.π. σελ. 186
[119] Χατζηνικολάου Ν., ό.π. σελ. 187
[120] Αιτιολογική έκθεση της Σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα, σκέψη 65. - https://rm.coe.int/16800cce5b.
[121] Αιτιολογική έκθεση 4619/2019

συγκοινωνιών[122]. Γενικότερα η έννοια της διατάραξης είναι ηπιότερη στον Ελληνικό ποινικό κώδικα σε αντίθεση με την έννοια της παρακώλυσης που σημαίνει την διακοπή λειτουργίας μιας υπηρεσίας. Στο άρθρο 292Β όμως η έννοια της διατάραξης έχει βαρύτερη σημασία αφού χρησιμοποιείται για να περιγράψει πράξεις που προβλέπονται στο άρθρο 292Β παρ.2, ενώ η παρεμπόδιση και η διακοπή διαφαίνεται να έχουν ταυτόσημες έννοιες. Εδω παρατηρείται για άλλη μια φορά ότι κατα την μεταφορά διατάξεων του Ενωσιακού δικαίου στο εσωτερικό, δεν ελήφθη μέριμνα για την ερμηνεία και τη σωστή απόδοση - ένταξη της ενωσιακής ορολογίας, σε ένα ενιαίο και διαφορετικό κείμενο όπως αυτό του Ποινικού μας Κώδικα, προκειμένου η ενσωμάτωση να είναι επιτυχής[123]. Είναι λογικό οι έννοιες διακοπή και σοβαρή παρεμπόδιση να έχουν μια διαφορετικότητα και να μην αντιμετωπίζονται ως ίσης βαρυτικής αξίας. Επίσης είναι σημαντικό να περιγράψουμε και τη σοβαρότητα της διακοπής, αφού αυτή δεν μπορεί να καθίσταται σοβαρή, όπως π.χ, έχουμε στη περίπτωση μιας μερικών δευτερολέπτων διακοπής λειτουργίας ενός συστήματος, που λαμβάνει χώρα με μαζική αποστολή spamming mails, η οποία θα έπρεπε να θεωρείται ως ήσσονος σημασίας και να μένει ατιμώρητη όπως προβλέπεται στο άρθρο 4 της οδηγίας. Τέλος η έννοια "χωρίς δικαίωμα" όπως αναλύθηκε στα προηγούμενα άρθρα φαίνεται να ανήκει στην αντικειμενική υπόσταση του εγκλήματος, αποκλείοντας την πλήρωση των στοιχείων του αδικήματος στην περίπτωση που γίνεται η προσβολή με δικαίωμα, αφού δεν προσβάλλεται το έννομο αγαθό της ακεραιότητας ενός συστήματος[124].

7.6 Η παρακώλυση λειτουργίας και η επαύξηση του αξιοποίνου (παρ. 2 του 292Β Π.Κ)

[122] Άρθρο 290 παρ.1 Π.Κ :1." Όποιος διαταράσσει την ασφάλεια της συγκοινωνίας στους δρόμους: α) με καταστροφή, βλάβη ή μετακίνηση εγκαταστάσεων ή οχημάτων, β) με τοποθέτηση ή διατήρηση εμποδίων, γ) με αλλοίωση σημείων ή σημάτων ή με τοποθέτηση ή διατήρηση εσφαλμένων σημείων ή σημάτων, ή δ) με άλλες, εξίσου επικίνδυνες για την ασφάλεια της συγκοινωνίας πράξεις, τιμωρείται.."

[123] Χατζηνικολάου Ν., ό.π. σελ. 188,

[124] Χατζηνικολάου Ν., ό.π. σελ. 191 επ., για την αντίθετη άποψη, που υποστηρίζει το αρχικό άδικο της πράξης το οποίο αίρεται με τη συναίνεση του ιδιοκτήτη ή του κατόχου.

Στις παραγράφους 2 και 3 του άρθρου 292Β Π.Κ προβλέπονται συνολικά τρεις περιπτώσεις τέλεσης του εγκλήματος στη διακεκριμένη του μορφή ήτοι α) *με τη χρήση εργαλείου που έχει σχεδιαστεί κατα κύριο λόγο* για την πραγματοποίηση μαζικών επιθέσεων (π.χ botnet), β) *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,* καθώς και *γ) αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες,* ενώ περαιτέρω αναφέρονται με τη λέξη, *ιδίως,* ενδεικτικά, αναφερόμενες περιπτώσεις ζωτικής σημασίας σε αγαθά και υπηρεσίες. Θα μπορούσαμε εδώ να σχολιάσουμε τη χρήση της έννοιας σχεδιασμός κατα "*κύριο λόγο" ενός εργαλείου* μαζικών επιθέσεων. Απο τη μια πλευρά έχουμε μια υπερβολική διεύρυνση του αξιοποίνου. Απο την άλλη, τέθηκε αντικειμενικά για να ενταχθούν εκεί όλα τα προγράμματα που apriori έχουν την δυνατότητα να πραγματοποιούν μαζικές επιθέσεις, ακόμη και τα νόμιμα, ως μια προσπάθεια να παρακαμφθούν οι αποδεικτικές δυσχέρειες. Πυροσβεστικά όμως έρχεται ο υπερχειλής σκοπός του δράστη για να καλύψει το μεγάλο χάσμα της διεύρυνσης του αξιοποίνου[125], αφού απαιτούνται περαιτέρω επιθέσεις που επηρεάζουν μεγάλο αριθμό συστημάτων. Προβληματικοί είναι και οι όροι της δεύτερης διακεκριμένης περίπτωσης, αφού κι αυτοί διακρίνονται απο μια γενικότητα και ασάφεια η οποία έχει επικριθεί από μερίδα θεωρητικών[126]. Τέλος, η τρίτη διακεκριμένη μορφή αφορά προσβολές σε πληροφοριακά συστήματα που παρέχουν ζωτικής σημασίας αγαθά ή υπηρεσίες (π.χ ύδρευση, Δ.Ε.Η, κ.τ.λ.,).

Στον νέο κώδικα δεν περιλήφθηκε η ισχύουσα διάταξη της παρ. 3, που αφορούσε μια οργανωμένη δραστηριότητα, καθώς έγινε δεκτό ότι πρέπει στις περιπτώσεις αυτές να "*λειτουργούν οι κανόνες της συρροής*"[127]. Δεν προβλέφθηκε επίσης διάταξη για την κατ' έγκληση δίωξη της πράξης, καθώς

[125] Χατζηνικολάου Ν., ό.π. σελ. 195 επ.
[126] Χατζηνικολάου Ν., ό.π. σελ. 195 επ.
[127] Αιτιολογική έκθεση ν. 4619/2019, σελ. 59

πρόκειται για έγκλημα που αφορά ένα "*ευρύτερο αριθμό ατόμων*" και για το λόγο αυτό "*η πράξη πρέπει να διώκεται αυτεπαγγέλτως*"[128].

7.7 Οι προπαρασκευαστικές πράξεις του άρθρου 292Γ Π.Κ

Η διάταξη αυτή αποτελεί ενσωμάτωση του άρθρου 7 της οδηγίας 2013/40/ΕΕ που επιβάλλει την ποινικοποίηση των προπαρασκευαστικών ενεργειών των αδικημάτων της παράνομης πρόσβασης και της παρεμβολής στα ψηφιακά δεδομένα ενος συστήματος πληροφοριών. Ποινικοποιείται *η παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή , κατοχή, διανομή, ή με άλλο τρόπο διακίνηση συσκευών ή προγραμμάτων υπολογιστή, αλλά και κωδικών που μπορεί να χρησιμοποιηθούν* για την διάπραξη της πρόσβασης, με σκοπό τη διάπραξη των αδικημάτων που προβλέπονται στο άρθρο 292Β Π.Κ. Ήταν φυσικό και επόμενο η αντιγραφή των προβλέψεων της σχετικής οδηγίας να οδηγήσει σε υπερβολική διεύρυνση του αξιοποίνου ως ανωτέρω προαναφέρθηκε. Ο περιορισμός του αξιοποίνου έγκειται σε δύσκολα διαγνωστικά στοιχεία υποκειμενικής υποστάσεως, αφού βασίζεται στον υπερχειλή σκοπό του δράστη να χρησιμοποιήσει τα επίμαχα προγράμματα με δόλο διάπραξης των αδικημάτων που προβλέπονται από το άρθρο 292Β Π.Κ. Εδώ θα μπορούσαμε να κάνουμε λόγο ότι ο περιορισμός του αξιοποίνου λαμβάνει χώρα και στην περίπτωση που διάφορες συσκευές ή προγράμματα έχουν αδειοδοτηθεί από κάποια αρμόδια Αρχή, έτσι ώστε να μην εντάσσονται στο απαγορευτικό πλαίσιο της "apriori τιμωρίας" αξιοποιώντας και το στοιχείο, "*χωρίς δικαίωμα" ως στοιχείο αντικειμενικής υποστάσεως του εγκλήματος.*

[128] Αιτιολογική έκθεση ν. 4619/2019, σελ. 59

7.8 Η φθορά των ψηφιακών δεδομένων κατά το πρώην άρθρο 381Α Π.Κ

Κατα τη διάρκεια συγγραφής της παρούσας εργασίας, η θέσπιση του νέου ποινικού κώδικα ήρθε να καταργήσει το άρθρο 381Α Π.Κ. Στο εν λόγω άρθρο είχε ενσωματωθεί η πρόβλεψη του άρθρου 5 της οδηγίας 2013/40/ΕΕ. Κατα περίοδο που αυτό ήταν σε ισχύ, καλύπτοταν ένα κενό της Ελληνικής νομοθεσίας αφού με αυτό προστατεύονταν ρητώς οι φθορές στα ψηφιακά δεδομένα και όχι όταν αυτές συνοδεύονταν μόνο με φθορές υλικών μερών. Η προστασία που παρείχε το άρθρο αυτό είχε να κάνει με την προστασία του εννόμου αγαθού της ακεραιότητας και τη διαθεσιμότητας των ψηφιακών δεδομένων. Ένα ατομικό αγαθό, κατ' έγκληση διωκόμενο, που τιμωρούσε το δράστη όταν αυτός κατέστρεφε ή απέκλειε τη χρήση των ψηφιακών δεδομένων από το νόμιμο κάτοχό τους. Παρ' όλα αυτά το άρθρο καταργήθηκε, χωρίς να γίνεται οποιασδήποτε μορφής νύξη, στην αιτιολογική έκθεση του νόμου σχετικά με το λόγο της κατάργησης.

Από την μια πλευρά, μέρος των αξιόποινων προβλέψεων του καταργηθέντος άρθρου 381Α μπορεί κανείς να συναντήσει σε άλλες διατάξεις του Π.Κ, όπως είναι τα νύν άρθρα 292Β και 378 Π.Κ, από την άλλη όμως πλευρά κατα τη γνώμη μου, δεν είναι δυνατή πλέον η τιμωρία του δράστη που προβαίνει μόνο σε καταστροφή, αλλοίωση ή απόκρυψη ψηφιακών δεδομένων από κάποια συσκευή ή υπολογιστή που περιήλθε στην κατοχή του (π.χ διαγραφή δεδομένων από usb stick, drive, κ.τ.λ), χωρίς αυτός να προκαλέσει ζημία στο υλικό μέρος αυτών.

7.9 Το άρθρο 386Α Π.Κ

Η εξέλιξη της τεχνολογίας επέβαλε τη ρύθμιση των συμπεριφορών που εντάχθηκαν πλέον στο άρθρο 386Α του Ποινικού Κώδικα οι οποίες προκάλεσαν δυσχέρειες στον Έλληνα ποινικό εφαρμοστή του νόμου. Πρόβλημα δημιουργούνταν με τις περιπτώσεις αναλήψεις μετρητών από ΑΤΜ.

Η μόνη περίπτωση που είχε κριθεί από τη νομολογία[129] ήταν η ανάληψη μετρητών από ΑΤΜ, καθ' υπέρβαση του πιστωτικού υπολοίπου του λογαριασμού του κατόχου η οποία κρίθηκε και αντιμετωπίστηκε ως κοινή κλοπή. Στη θεωρία εκφράστηκε η άποψη ότι δεν μπορεί να γίνει δίωξη στο δράστη που έχει υπεξαιρέσει ή κλέψει κάρτα ανάληψης μετρητών, γνωρίζοντας τον προσωπικό αριθμό pin του κατόχου με αποτέλεσμα να πετυχαίνει την ανάληψη χρημάτων από λογαριασμό πραγματικού δικαιούχου[130]. Έτσι ο Έλληνας νομοθέτης αποφάσισε με την ψήφιση του νόμου 1805/1988[131] την εισαγωγή του άρθρου 386Α μετά το άρθρο 386 περί απάτης, διάταξης η οποία θα αντιμετώπιζε τις περιπτώσεις αυτές. Το άρθρο 386Α αποτέλεσε μία ειδική ποινική υπόσταση που εφαρμόστηκε για τις χωρίς δικαίωμα συναλλαγές που λάμβαναν χώρα μέσω ΑΤΜ, αφού οι περιπτώσεις αυτές δεν μπορούσαν να ενταχθούν στο άρθρο 386[132] του Ποινικού Κώδικα διότι η διάταξη αυτή αναφέρεται σε πρόκληση πλάνης σε φυσικό πρόσωπο και όχι σε ηλεκτρονικό υπολογιστή. Το κενό που είχε δημιουργηθεί ήταν μεγάλο, καθόσον σε πάρα πολλές συναλλαγές ο ηλεκτρονικός υπολογιστής αντικατέστησε τον άνθρωπο με μηχανικές διαδικασίες και κατ' επέκταση η έλλειψη δηλώσεως βουλήσεως, ως στοιχείο πλήρωσης της αντικειμενικής υπόστασης του άρθρου 386 Π.Κ ήταν φανερή. Περαιτέρω το άρθρο αυτό τελειοποιήθηκε με το νόμο 4411/2016 και ειδικότερα με το άρθρο 2, όπου το 386Α του Ποινικού Κώδικα αντικαταστάθηκε ως εξής: "*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 τη 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*

[129] Συμβ.Διαρκ.Στρ.Αθ. 401/1986., ΠοινΧρ. ΛΣΤ΄776
[130] Γιαννόπουλος Θ., ΝΟΒ. 34 (1986), 173
[131] Με το νόμο αυτό εισήχθησαν οι περισσότερες διατάξεις που αφορούν τα πληροφοριακά συστήματα ενώ παράλληλα διευρύνθηκε και η έννοια του εγγράφου στο άρθρο 13 Π.Κ
[132] Μυλωνόπουλος Χ., Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ. 54

την υπέστησαν ήταν άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα πρόσωπα.

Είναι φανερό πλέον, ότι η νέα διάταξη περιλαμβάνει και τις περιπτώσεις απάτης με ηλεκτρονικό υπολογιστή, όταν λαμβάνει χώρα χρήση ορθών δεδομένων που γίνεται χωρίς δικαίωμα, όπως για παράδειγμα στην περίπτωση ενός δράστη που απέκτησε παράνομα το όνομα χρήστη και τον κωδικό πρόσβασης σε λογαριασμό του δικαιούχου.

Από τη γραμματική διατύπωση του άρθρου προκύπτει και το προστατευόμενο έννομο αγαθό, που δεν είναι άλλο από το έννομο αγαθό της περιουσίας[133]. Η ίδια διάταξη δείχνει ότι η απάτη με ηλεκτρονικό υπολογιστή συμβάλλει στην προστασία της περιουσίας ως οικονομικό σύνολο. Στο άρθρο αυτό υπάγεται και η περιουσία που αφορά Λογιστικό και ηλεκτρονικό χρήμα, καθώς και τα δικαιώματα που προέρχονται από την επεξεργασία στοιχείων του ηλεκτρονικού υπολογιστή. Στη θεωρία διατυπώθηκαν και απόψεις που μιλούσαν για την προστασία της ασφάλειας του υπολογιστή και των προγραμμάτων αυτού ως μέσο διακίνησης και διασφάλισης της περιουσίας, οι οποίες όμως δεν μπορούν να γίνουν δεκτές γιατί δεν πληρούν τη γραμματική διατύπωση του νόμου.

Η αντικειμενική υπόσταση του εγκλήματος τελείται με τους κάτωθι 4 τρόπους :

α) Με τη μη ορθή διαμόρφωση του προγράμματος υπολογιστή. Ώς πρόγραμμα ορίζεται το σύνολο δεδομένων με το οποίο δίνονται εντολές στον υπολογιστή. στην μη ορθή διαμόρφωση του προγράμματος περιλαμβάνονται η επανεγγραφή, η τροποποίηση, η διαγραφή ολόκληρου του προγράμματος ή τμήματος αυτού. Συμπεριλαμβάνεται επίσης η πρόσθεση, η μεταβίβαση δεδομένων καθώς και η εισαγωγή νέων τμημάτων στο πρόγραμμα. Μη ορθότητα υφίσταται όταν ένα πρόγραμμα δεν ανταποκρίνεται στη βούληση και στις παραστάσεις του κατόχου. Βάση της θεωρίας ένα πρόγραμμα είναι μη ορθό όταν παρουσιάζει μία απόκλιση από την πραγματικότητα.

β) Με τη χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων. Στον τρόπο τέλεσης αυτό περιλαμβάνεται είτε η εισαγωγή μη ορθών δεδομένων, είτε ελλιπών δεδομένων. Παράδειγμα εδώ υπάρχει όταν ο δράστης εισάγει στον

[133] Βασιλάκη Ε., ό.π., σελ. 201

ηλεκτρονικό υπολογιστή στοιχεία που αφορούν ανύπαρκτα τέκνα, με σκοπό να εισπράξει κρατικά επιδόματα.

γ) Με τη χωρίς δικαίωμα χρήση δεδομένων. Σύμφωνα με τη διάταξη του άρθρου 386Α του Ποινικού Κώδικα, η οποία τροποποιήθηκε με το νόμο 4411/2016, περιλαμβάνεται πλέον ρητά και αυτός ο τρόπος απάτης. Εδώ προβλέπεται ρητά η ποινικοποίηση της χρήσης ορθών δεδομένων που γίνεται χωρίς δικαίωμα. Για παράδειγμα στην περίπτωση που ο δράστης χρησιμοποίησε κάρτα ηλεκτρονικής ανάληψης χρημάτων κάποιου άλλου, αφού τα δεδομένα που εισάγει στο πρόγραμμα της τράπεζας, **είναι ορθά και μη ελλιπή**, αλλά κάποιου άλλου πραγματικού δικαιούχου.

δ) Με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα. *Πληροφοριακό σύστημα είναι η συσκευή ή η ομάδα συνδεδεμένων 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 την συντήρηση των συσκευών αυτών*[134].

Η υποκειμενική υπόσταση του άρθρου 386Α του Ποινικού Κώδικα κατατάσσει αυτό στα ιδιώνυμα εγκλήματα. Αποτελεί έγκλημα υπερχειλούς υποκειμενικής υπόστασης και απαιτείται δόλος πρώτου βαθμού, συμπεριλαμβανομένου και του ενδεχόμενου δόλου, δηλαδή τη γνώση και τη βούληση του δράστη για την πραγματοποίηση των πραγματικών περιστατικών της αντικειμενικής υπόστασης του εγκλήματος.

7.10 Η σχέση της απάτης 386 Π.Κ με την απάτη με ηλεκτρονικό υπολογιστή, 386Α Π.Κ

Προϋπόθεση για την κοινή απάτη αποτελεί η περιουσιακή βλάβη ως αποτέλεσμα μιας παραπλάνησης ενός φυσικού προσώπου. Η απάτη με ηλεκτρονικό υπολογιστή απαιτεί περιουσιακή βλάβη ως αποτέλεσμα επηρεασμού της διαδικασίας επεξεργασίας ψηφιακών δεδομένων. Εδώ πρέπει

[134] Άρθρο 13 Π.Κ όπως τροποποιήθηκε με το άθρρο 2 του ν. 4411/2016.

με πούμε ότι ο χρήστης εξαπατάται στο διαδίκτυο με κοινά εγκλήματα οικονομικής φύσεως. Τα εγκλήματα αυτά έχουν σχέση με κοινά εγκλήματα που χρησιμοποιούν την πληροφορική ως μέσο τέλεσης. Όταν ο ηλεκτρονικός υπολογιστής χρησιμοποιείται μόνο ως μέσο τέλεσης τότε εφαρμόζονται οι διατάξεις περί κοινής απάτης. Έτσι δημιουργείται το φαινόμενο ενός αμοιβαίου αποκλεισμού των άρθρων, ενώ οι δικαστές πρέπει να αιτιολογούν επαρκώς ποια μορφή απάτης τελείται, καθόσον σε διαφορετική περίπτωση η απόφασή τους, πάσχει από έλλειψη αιτιολογίας και καθίσταται αναιρετέα[135].

7.10.1 Το φαινόμενο phishing και η ποινική αντιμετώπιση του στην Ελλάδα.

Λόγω της ανάπτυξης της τεχνολογίας και της κρυπτογράφησης των δεδομένων που διακινούνται με πληροφοριακά συστήματα, οι δράστες δεν προτιμούν την δαπανηρή και χρονοβόρα διαδικασία παραβίασης (σπάσιμο) των κωδικών που χρησιμοποιεί ο εκάστοτε χρήστης, αλλά την αλίευση των κωδικών αυτών με διάφορους τρόπους. Ένας από τους τρόπους αυτούς είναι και η αποστολή, μέσω ηλεκτρονικής αλληλογραφίας, μηνυμάτων τα οποία υποτίθεται ότι προέρχονται από μεγάλα χρηματοπιστωτικά ιδρύματα. Στην ηλεκτρονική αυτή αλληλογραφία ζητούνται π.χ λόγω κάποιου προβλήματος ασφαλείας του συστήματος, να αποσταλούν από τους πελάτες οι κωδικοί πρόσβασης προς επιβεβαίωση[136]. Αφού ο δράστης τελικώς επιτύχει την λήψη των προσωπικών κωδικών τότε προβαίνει σε χρήση αυτών με σκοπό την αφαίρεση χρημάτων από το λογαριασμό του θύματος. Το φαινόμενο αυτό αντιμετωπίζεται στην Ελλάδα με την βασική διάταξη της απάτης διότι η βλάβη είναι μεν αποτέλεσμα διαδικασίας επεξεργασίας ψηφιακών δεδομένων πλην όμως αποτελεί παραπλάνηση φυσικού προσώπου με τη χρήση ηλεκτρονικού υπολογιστή ως αναγκαίου μέσου για την τέλεση του εγκλήματος. Ο δράστης εδώ διαμορφώνει ένα ψευδές περιστατικό και το ανακοινώνει σε κάποιον ως πραγματικό, πείθοντάς τον να προβεί σε πράξη ώστε μεταγενέστερα να

[135] Καιάφα Γκπάντι, Εμβάθυνση στην ποινική νομολογία, 504
[136] Βλαχόπουλος Κ., Ηλεκτρονικό έγκλημα, 2007, σελ. 58 επ.

μετατεθούν τα περιουσιακά του στοιχεία. Στις περισσότερες περιπτώσεις η μετάθεση των περιουσιακών στοιχείων του θύματος λαμβάνει χώρα εταιροχρονολογημένα και όχι άμεσα. Το phishing δηλαδή έχει την έννοια ενός εγκλήματος κοινής απάτης, που χρησιμοποιεί ως μέσο τον ηλεκτρονικό υπολογιστή, αφού οι πράξεις που ενεργεί ο δράστης συνίστανται σε παράνομη ιδιοποίηση με απατηλά μέσα, στοιχείων ταυτότητας ή κωδικών του θύματος έχοντας ως σκοπό τη βλάβη της περιουσίας του.

7.10.2 Το φαινόμενο των πολυμεσικών μηνυμάτων ως μια ειδικότερη έκφανση εγκλήματος μέσω του διαδικτύου.

Τα τελευταία χρόνια απασχόλησε την κοινή γνώμη και όχι μόνο, μια ειδικότερη μορφή απάτης η οποία σχετίζεται με την παροχή υπηρεσιών πολυμεσικής πληροφόρησης και κατ' επέκταση, την μη ηθελημένη χρέωση συνδρομητών κινητής τηλεφωνίας. Ενδεικτικά αναφέρονται δύο τρόποι με τους οποίους επιτυγχάνεται η χρέωση των συνδρομητών κινητής τηλεφωνίας.

Ο πρώτος τρόπος είναι τα λεγόμενα αναδυόμενα παράθυρα POP UP. Στη περίπτωση που κάποιος μπει στο διαδίκτυο και παρακολουθήσει μία ιστοσελίδα μπορεί ξαφνικά να οδηγηθεί σε μία διαφήμιση ή ένα υποτιθέμενο διαγωνισμό που προσκαλεί το άτομο να συμμετάσχει προκειμένου να κερδίσει διάφορα δώρα όπως π.χ δωροεπιταγές, αεροπορικά εισιτήρια, κουπόνια super Market και λοιπά[137]. Για να επιτευχθεί αυτό θα πρέπει, «το θύμα», να ακολουθήσει κάποια στάδια ενεργειών. Το πρώτο στάδιο είναι να απαντήσει σε μερικές ερωτήσεις, το δεύτερο στάδιο είναι να επιλέξει το δώρο που επιθυμεί και το τρίτο στάδιο είναι να εισάγει τον αριθμό του κινητού του τηλεφώνου, αποδεχόμενος παράλληλα τους όρους χρήσης των παρεχόμενων υπηρεσιών. Εδώ πρέπει να σημειωθεί ότι σε αρκετές περιπτώσεις, έχει παρατηρηθεί ότι η διαδικασία συνεχίζεται ακόμη και αν κάποιος δεν αποδεχθεί τους όρους χρήσης των παρεχόμενων υπηρεσιών. Ακολούθως, ο ενδιαφερόμενος, το θύμα, ουσιαστικά μπορεί να λάβει, (μπορεί όμως και όχι), ένα sms στο κινητό του, που σε αυτό το sms περιέχει ένα pin που πρέπει να

[137] https://youtu.be/8pZ6CY6Txng?t=202,. Δηλώσεις της Αναπληρώτριας συνηγόρου του καταναλωτή Αθηνάς Κοντογιάννη. Προσβ., Νοεμβρ. 2019

καταχωρηθεί στην ιστοσελίδα, ώστε με αυτό τον τρόπο να επιβεβαιωθεί και να ταυτοποιηθεί ο χρήστης. Εάν ο ενδιαφερόμενος το πράξει τελικά, τότε ξεκινάει η αποστολή των παρεχομένων υπηρεσιών, δηλαδή των μηνυμάτων, όπου οι χρεώσεις είναι πολύ υψηλότερες από τις συνηθισμένες. Εδώ έχουμε να κάνουμε με την λεγόμενη παραπλάνηση του χρήστη με την «παράσταση ψευδών γεγονότων ως αληθινών», προκειμένου να τον οδηγήσουν σε αποδοχή των όρων των παρεχόμενων Υπηρεσιών.

Ο δεύτερος τρόπος είναι τα λεγόμενα απρόσμενα sms που λαμβάνει κάποιος στο κινητό του. Υπάρχει περίπτωση να λάβει κάποιος στο κινητό του ένα sms στο οποίο να αναφέρεται ότι είναι εγγεγραμμένος σε μία παρόμοιου είδους υπηρεσία, ακόμη κι αν δεν γνωρίζει τίποτα ή δεν έχει κάνει κάποιου είδους εγγραφή. Σε αυτή την περίπτωση η παράνομη χρέωση ξεκινάει άμεσα. Υπάρχει επίσης περίπτωση να ληφθεί και ένα δεύτερο μήνυμα που να λέει ότι θα πρέπει να καταχωρηθεί ο αριθμός του κινητού τηλεφώνου για επιβεβαίωση σε κάποια ιστοσελίδα. Τέλος υπάρχει και η περίπτωση να ληφθή κι ένα τρίτο μήνυμα στο κινητό του θύματος, που να λέει ότι αν επιθυμεί να σταματήσει την εγγραφή θα πρέπει να αποστείλει την λέξη stop σε sms. Σε αυτές τις περιπτώσεις όταν τα θύματα απαντούν σε αυτά τα μηνύματα οι χρεώσεις είναι πάρα πολύ μεγάλες σε σχέση με τα κοινά sms.

Τα τελευταία χρόνια σύμφωνα με τους αξιωματικούς της δίωξης ηλεκτρονικού εγκλήματος, έχουν σχηματιστεί πάνω από 2.000 δικογραφίες ανάλογου περιεχομένου. Υπάρχουν όμως και οι περιπτώσεις που ο χρήστης χωρίς να έχει διαβάσει τους όρους χρήσης των πολυμεσικών υπηρεσιών καταχωρεί με ένα είδος ***επιπολαιότητας*** τον αριθμό του κινητού τηλεφώνου αλλά και μετέπειτα το pin[138]. Υπάρχουν όμως και οι περιπτώσεις κάποιοι πολίτες να έχουν λάβει τέτοια μηνύματα χωρίς να έχουν καταχωρήσει το κινητό τους τηλέφωνο και αυτό φαίνεται, καθόσουν η επιλογή των αριθμών κινητής τηλεφωνίας γίνεται τυχαία.

Όσον αφορά τη διαγραφή των χρηστών από τέτοιου είδους υπηρεσίες μη ηθελημένες υπάρχουν δύο τρόποι:

138

https://www.newsit.gr/ellada/apates-sms-katapeltis-i-dioksi-ilektronikou-egklimatos/2842365/

α) ο πρώτος τρόπος είναι να επικοινωνήσουν με την υπηρεσία πολυμεσικής πληροφόρησης που φαίνονται ότι είναι εγγεγραμμένοι και

β) ο δεύτερος τρόπος είναι να απευθυνθούν στην εταιρεία κινητής τηλεφωνίας να αναφέρουν το πρόβλημα και μέσω της εταιρείας να προσπαθήσουν να φράξουν τις υπηρεσίες αυτές.

Τέτοιες καταγγελίες λαμβάνονται από τις υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος που σχηματίζουν δικογραφίες για το αδίκημα της ***απάτης***

Περαιτέρω, η Ελληνική Αστυνομία μέσω της εκπροσώπου τύπου, εξέδωσε κάποιες συμβουλές σχετικά με την πρόληψη τέτοιων φαινομένων προς τους πολίτες. Πρώτα από όλα δεν θα πρέπει οι πολίτες να ελκύονται από τέτοιου είδους διαγωνισμούς που είναι "υπερβολικά καλοί για να είναι αληθινοί"[139]. Δεύτερον να μην απαντούν στα μηνύματα τέτοιου περιεχομένου. Τρίτον να μην καταχωρούν τον αριθμό του κινητού τους τηλεφώνου σε κάποιο δικτυακό τόπο αν προηγουμένως δεν έχουν διαβάσει τους όρους και τις προϋποθέσεις που αφορούν την υπηρεσία που τους παρέχεται. Πολλές φορές οι διαφημίσεις που συνοδεύουν προσφορές ή συμμετοχή σε τέτοιες κληρώσεις ενδέχεται να είναι συνδρομητικές. Τέλος σε οποιαδήποτε περίπτωση συνιστάται στους πολίτες να απευθύνονται στη διεύθυνση δίωξης ηλεκτρονικού εγκλήματος, (στο τηλ. 11188) για να καταγγείλουν αυτές τις πράξεις σε αστυνομικό επίπεδο. Περαιτέρω μπορούν να απευθύνονται και στην εθνική επιτροπή τηλεπικοινωνιών και ταχυδρομείων όπως και στο συνήγορο του καταναλωτή[140].

Ο συνήγορος του καταναλωτή ασχολήθηκε εκτενώς με το θέμα[141], όσο δυνατόν θα ήταν να ασχοληθεί, αφού τα στοιχεία που είχε στη διάθεσή του προέρχονταν αφενός από τις καταγγελίες των πολιτών, αφετέρου από τις απόψεις των τηλεπικοινωνιακών παρόχων, που είχαν και τα τεχνικής φύσεως δεδομένα. Παρ᾽ όλα αυτά, προχώρησε σε συστάσεις προς τις εταιρείες αυτές, επισημαίνοντας ότι οι χρεώσεις είναι παράνομες, διότι αντίκεινται στον κώδικα δεοντολογίας για τις υπηρεσίες πολυμεσικών πληροφοριών, καθώς και στο

[139]Βλ. https://www.youtube.com/embed/cEkpSEyfxLE., Δηλώσεις εκπροσώπου τύπου της ΕΛ.ΑΣ., Νοεμβ. 2019

[140]https://www.newsit.gr/ellada/apates-sms-katapeltis-i-dioksi-ilektronikou-egklimatos/2842365

[141]https://www.lawspot.gr/nomika-nea/paremvasi-synigoroy-toy-katanaloti-gia-tis-hreoseis-minymaton-apo-5psifia-noymera-sta

νομό 2251/1994 άρθρο 9 παρ. 5, 9ζ παρ. 1 και 9η παρ. γ για την "προστασία των Καταναλωτών"[142]. Ο συνήγορος έκανε λόγο και για συνευθύνη των παρόχων κινητής τηλεφωνίας αφού αυτές λαμβάνουν οικονομικό αντάλλαγμα που ορίζεται στη σύμβαση με τους παρόχους υπηρεσιών πολυμεσικής πληροφόρησης. Τέλος σε άλλες περιπτώσεις έκανε λόγο για παραβίαση του Κανονισμού προσωπικών δεδομένων[143], αφού οι εταιρείες παρείχαν αυτοματοποιημένα τον αριθμό κινητής τηλεφωνίας του χρήστη στις εταιρείες παροχής πολυμεσικών πληροφοριών προκειμένου γίνει η ταυτοποίηση του χρήστη στη συγκεκριμένη ιστοσελίδα[144]. Επίσης απέστειλε σε πολλές περιπτώσεις τους σχετικούς φακέλους στις αρμόδιες υπηρεσίες δίωξης καθ' όσον παρουσιάζονταν στοιχεία του εγκλήματος της απάτης.

Εδώ στην περίπτωση που ισχύουν τα καταγγελλόμενα, τίθενται περαιτέρω φραγμοί στα στάδια της απόδειξης του τυχόν διαπραττόμενου εγκλήματος κατά της περιουσίας. Αφενός ως μεμονωμένα περιστατικά (κατ' άτομο), η οικονομική ζημία είναι ευτελούς αξίας κι αφετέρου, η πίστωση των χρημάτων που αφαιρέθηκαν από τον χρήστη (καρτοκινητή) ή η ανάκληση της χρέωσης που εμφαίνεται στο λογαριασμό (συμβόλαιο) αποτελεί λόγο απαλλαγής από την ποινή. Η νομιμότητα γνωστοποίησης των απαραίτητων τεχνικών στοιχείων (ενδείξεις – αποδείξεις, IP, ταυτοποίηση) που απαιτούνται στο πλαίσιο της συγκέντρωσης αποδεικτικού υλικού από τις αρμόδιες υπηρεσίες, είναι ιδιαίτερα προβληματική και έχει απασχολήσει θεωρία και νομολογία ουκ ολίγες φορές[145].

[142]http://www.synigoroskatanaloti.gr/docs/announce/2017-09-22.Epistoli-EETT.pdf
[143]http://www.synigoroskatanaloti.gr/docs/reports/2017-12-22.%CE%A3%CF%85%CF%83%CF%84%CE%B1%CF%83%CE%B7-%CE%A5%CE%A0%CE%A0.pdf
[144]http://www.synigoroskatanaloti.gr/docs/reports/2017-12-22.%CE%A3%CF%85%CF%83%CF%84%CE%B1%CF%83%CE%B7-%CE%A5%CE%A0%CE%A0.pdf
[145] Βλέπε αντίστοιχες γνωμοδοτήσεις Εισαγγελέων Α.Π., 9/2009, 12/2009, 9/2011 και αντίθετη γνώμη της ΑΠΔΠΧ 1/2005, στο http://www.adae.gr/fileadmin/docs/nomoi/893-2005.pdf

8. Δυσχέρειες στη Νομική αντιμετώπιση του κυβερνοεγκλήματος

Παρά τις προσπάθειες αυτές, νομικές και μή, τόσο σε διεθνές επίπεδο όσο και σε Ευρωπαϊκό η δίωξη ενός ηλεκτρονικού εγκλήματος καθίσταται ιδιαίτερα δυσχερής. Τα προβλήματα ξεκινούν από την ανυπαρξία ενός σαφούς και ενιαίου ορισμού για την έννοια του ηλεκτρονικού εγκλήματος. Οι νόμοι καθίστανται ανεπαρκείς για να περιγράψουν ενιαία το ηλεκτρονικό έγκλημα και να καλύψουν με σαφήνεια τα εγκλήματα που διαπράττονται. Υπάρχουν ακόμη χώρες που δεν έχουν κυρώσει διεθνείς συνθήκες για την αντιμετώπιση των ψηφιακών εγκλημάτων με αποτέλεσμα την μη ικανοποιητική δίωξη. Πολλά θύματα δεν καταγγέλλουν εύκολα τις παραβιάσεις που γίνονται είτε για λόγους δυσφήμισης είτε λόγω δυσκολίας αποδειξης, είτε ελλείψεις αρμοδίων υπαλλήλων που θα φέρουν εις πέρας μία τέτοια καταγγελία. Ακόμη και όταν καταγγέλλονται τέτοια εγκλήματα οι στατιστικές απεικονίζουν περισσότερο τις προτεραιότητες της αστυνομίας και λιγότερο την πραγματική έκταση του εγκλήματος.

Από άποψη των διαδίκων οι ενάγοντες συχνά δεν γνωρίζουν από ηλεκτρονικούς υπολογιστές, οι δικαστές δεν έχουν χρήσιμα παραδείγματα από τη νομολογία, οι δικηγόροι δεν έχουν σχετική γνώση και εμπειρία, ενώ μέσα σε όλα αυτά έρχονται να προστεθούν και τα προβλήματα της νομοθεσίας αφού πολλές χώρες είναι ιδιαίτερα "χαλαρές" στην αντιμετώπιση του ηλεκτρονικού εγκλήματος, όπως π.χ η Ανατολική Ευρώπη, η Ασία η Ρωσία.

Ο εντοπισμός του εγκλήματος, η ποινική δίωξη, η σύλληψη και η καταδίκη των δραστών καθίστανται κατά αυτόν τον τρόπο ιδιαίτερα δυσχερείς. Εξ᾽ υπαρχής δυσκολία αποτελεί και ο καθορισμός της χώρας (τόπος τέλεσης εγκλήματος)[146] που είναι αρμόδια για την άσκηση της δίωξης. Στις περιπτώσεις δε που αυτό διευκρινιστεί, απαιτείται διακρατική συνεργασία ώστε να συγκεντρωθούν οι αποδείξεις για την έκδοση του δράστη. Προφανής είναι εδώ και η δυσκολία που αντιμετωπίζει η αρμόδια διωκτική αρχή, όσον

[146] Δαλακούρας Θ., Ηλεκτρονικό έγκλημα, με παρατηρήσεις Κιούπη Δ., όσον αφορά τον τόπο τέλεσης του ηλεκτρονικού εγκλήματος. Ν.Β 2019, σελ. 41 επ.

αφορά τον εντοπισμό και την αναγνώριση του δράστη, αφού τεχνολογικά υπάρχουν πολλοί τρόποι απόκρυψης της πραγματικής ταυτότητας, όπως λ.χ μέσω κρυπτογράφησης, μέσω διακομιστών μεσολάβησης, ή χρήσης ψεύτικων ονομάτων και email.

Ένα άλλο μελανό σημείο αποτελεί η συγκέντρωση των αποδεικτικών στοιχείων. Τα αποδεικτικά στοιχεία μπορεί να βρίσκονται είτε αποθηκευμένα σε πολλούς υπολογιστές που βρίσκονται σε διαφορετικές χώρες, είτε σε αποθηκευτικούς χώρους νέφους (cloud storage). Ακόμη πιο δύσκολη γίνεται η έρευνα όταν τα αποδεικτικά στοιχεία είναι κατατμημένα και διαμοιρασμένα σε διάφορες περιοχές της γης. Ακόμη κι αν η συγκέντρωση αυτών των δεδομένων καταστεί εφικτή, το μέγεθος των συγκεντρωθέντων αρχείων απαιτεί ατελείωτες δυνάμεις και μέσα, ώστε να διεκπεραιωθεί.

Ακόμη όμως κι όταν εντοπιστεί διαδικτυακά το ίχνος ενός δράστη, απαιτείται η στάθμιση των ατομικών δικαιωμάτων σε σχέση με το φερόμενο έγκλημα. Οι πιο συχνές δυσκολίες που αντιμετωπίζουν οι δικαστικές αρχές έγκεινται, στην έλλειψη αρκετών αποδεικτικών στοιχείων, στην αδυναμία τεκμηρίωσης του δόλου, στην έλλειψη αρμοδιότητας, στην έλλειψη μαρτύρων ή στην ανηλικότητα των δραστών.

Αλήθεια, πόσο εύκολο είναι να ταξιδέψει ένας μάρτυρας σε ένα άλλο κράτος και να παραστεί σε δικαστήριο; Πόσο εύκολη καθίσταται, δικονομικά, η εξάρθρωση μιας εγκληματικής ομάδας που διαπράττει ηλεκτρονικές απάτες μικρών ποσών προσβάλλοντας αόριστο αριθμό θυμάτων ανά τον κόσμο, αποκομίζοντας στο σύνολο τεράστια κέρδη;

Σήμερα πολλές διαδικτυακές απάτες έχουν να κάνουν με μικρό αριθμό ποσού χρημάτων. Αυτό γίνεται για δύο κυρίως λόγους, είτε γιατί το θύμα δεν θα το αντιληφθεί καθόλου, είτε γιατί και να το αντιληφθεί, δεν θα προβεί σε οποιουδήποτε είδους αναγγελία εγκλήματος αφού η διεκπεραίωσή του είναι δαπανηρή και χρονοβόρα.

Οι αξιωματικοί της Διεύθυνσης Δίωξης Ηλεκτρονικού εγκλήματος[147], αναφέρουν ότι οι δυσκολίες στη δίωξη τέτοιων εγκλημάτων οφείλονται στις κάτωθι αιτίες:

α) Διαφορετική νομοθεσία μεταξύ κρατών,

[147] http://www.astynomia.gr/images/stories/2015/2prak_syn.pdf,.

β) Ελλιπείς γνώσεις χρηστών σε θέματα ασφάλειας,

γ)Το διαδίκτυο είναι αχανές,

δ) ελλιπή μέτρα ασφαλείας,

ε) εύκολη διάπραξη εγκλήματος,

στ) ανωνυμία του δράστη,

ζ) σκοτεινός αριθμός θυμάτων (μη καταγγελία πράξης)

η) εύκολη απόκρυψη των στοιχείων του δράστη,

θ) δύσκολος ο εντοπισμός του δράστη από τις διωκτικές αρχές, (Πολλές υποθέσεις, δυσκολία εντοπισμού και εξέτασης ψηφιακών πειστηρίων).

9. Μέτρα αντιμετώπισης για τη δίωξη ηλεκτρονικού Εγκλήματος

9.1 Θωράκιση του υπολογιστή στόχου.

Η περιορισμένη ικανότητα των κρατών - μελών να ελέγξουν τα εγκλήματα που συμβαίνουν στον κυβερνοχώρο είναι προφανής[148]. Η πρώτη γραμμή άμυνας εντοπίζεται στη συνετή συμπεριφορά από το πιθανό θύμα. Στην πραγματικότητα το διαδικτυακό έγκλημα δεν διαφέρει σε πάρα πολλά σημεία από το πραγματικό κοινό έγκλημα. Έτσι όπως και ο ιδιοκτήτης ενός σπιτιού για να προστατεύσει την περιουσία του κλειδώνει τις πόρτες και τα παράθυρα προκειμένου να μετριάσει την πιθανότητα διάρρηξης, έτσι και ο χρήστης του διαδικτύου θα πρέπει να λάβει μέτρα ώστε να μην αποτελεί τον εύκολο στόχο.

Οι χρήστες των διαδικτυακών υπηρεσιών θα πρέπει να ενημερώνουν τα προγράμματα προστασίας των υπολογιστών τους, να ελέγχουν ότι τα προγράμματα αυτά λειτουργούν, όπως επίσης να αλλάζουν και σε τακτικά χρονικά διαστήματα τους κωδικούς πρόσβασης. Μερικά από τα μέτρα που κρίνονται χρήσιμα για την ασφάλεια του κάθε χρήστη στο διαδίκτυο είναι:

α) Η **χρήση ενημερωμένων προγραμμάτων** antispyware, antivirus και firewall που προστατεύουν τον χρήστη από επιθέσεις μη εξουσιοδοτημένης πρόσβασης σε αρχεία και δεδομένα.

β) η **αποφυγή του ανοίγματος των επισυναπτόμενων αρχείων** ηλεκτρονικών μηνυμάτων από αγνώστους αποστολείς είτε μέσω ηλεκτρονικής αλληλογραφίας είτε μέσω άλλων μέσων,

γ) **συχνή ενημέρωση του λειτουργικού συστήματος** του ηλεκτρονικού υπολογιστή ώστε να καλύπτονται τα κενά ασφαλείας,

δ) τακτική **τήρηση ενημερωμένων αντιγράφων ασφαλείας αρχείων** σε άλλο δίσκο ή χώρο νέφους για την αποφυγή ζημιών από ιούς,

[148]Περπέρης Α, Το Ηλεκτρονικο–οικονομικό έγκλημα: Ερευνητική προσέγγιση, Διδακτορική Διατριβή, Πάντειο Πανεπιστήμιο, Αθήνα, 2015

ε) **απενεργοποίηση των επιλογών που επιτρέπουν την αυτόματη εκτέλεση προγραμμάτων** και αρχείων που αποστέλλονται μέσω λογισμικού διαμοιρασμού αρχείων,

στ) **ενεργοποίηση των φίλτρων spam**, για τον έλεγχο της ηλεκτρονικής αλληλογραφίας.

Οι δράστες του χώρου προσπαθούν να εισαγάγουν, είτε μέσω ηλεκτρονικού ταχυδρομείου είτε μέσω άλλης μορφής επικοινωνίας, στον υπολογιστή του θύματος κακόβουλο λογισμικό ή προγράμματα, ώστε να υποκλέψουν προσωπικά στοιχεία και κωδικούς και γενικότερα να βλάψουν την λειτουργία του υπολογιστή[149].

Τα χρηματοπιστωτικά ιδρύματα ενημερώνουν τους πολίτες που χρησιμοποιούν τις υπηρεσίες τους, για τους κινδύνους που εγκυμονεί η χρήση των διαδικτυακών υπηρεσιών, προκειμένου να τους βοηθήσουν στην ασφαλέστερη πραγματοποίηση των συναλλαγών. Στην κατεύθυνση αυτή η Ευρωπαϊκή ένωση θέσπισε Κανονισμό για τις συναλλαγές που λαμβάνουν χώρα ανέπαφα με χρεωστική ή πιστωτική κάρτα, ώστε να απαιτείται πλέον η χρήση κωδικού όταν συμπληρωθεί ένα ποσό ανέπαφων συναλλαγών[150].

9.2 Προστασία του θύματος από τις απάτες μέσω Υπολογιστή.

Οι απάτες που λαμβάνουν χώρα με τη χρήση των Πληροφοριακών Συστημάτων προσομοιάζουν στα κάτωθι χαρακτηριστικά:

α) Ο δράστης ενημερώνει το υποψήφιο θύμα για κάποια ευκαιρία ή δελεαστική προσφορά ενός προϊόντος.

β) Ακολούθως προσπαθεί να πείσει το θύμα ότι η ευκαιρία είναι μοναδική,

γ) Τέλος αφού ξεγελάσει το θύμα θα προσπαθήσει να του αποσπάσει χρήματα με τη συναίνεσή του.

Το θύμα σε αυτές τις περιπτώσεις μπορεί να ενισχύσει την αμυντική του δυνατότητα εάν είναι ενημερωμένο και εκπαιδευμένο σχετικά με τους

[149]Περπέρης Απόστολος, Το Ηλεκτρονικο–οικονομικό έγκλημα: Ερευνητική προσέγγιση, Διδακτορική Διατριβή, Πάντειο Πανεπιστήμιο, Αθήνα, 2015

[150] https://www.hba.gr/Media/Details/397., Νοέμβρ. 2019

κινδύνους που αυτό διατρέχει στο πλαίσιο της εκάστοτε, καταναλωτικής ή επαγγελματικής, διαδικτυακής συμπεριφοράς.

Σημαντικό ρόλο διαδραματίζει η ενημέρωση των χρηστών και η εκπαίδευσή τους σχετικά με τις νέες τεχνολογίες. Οι καμπάνιες ενημέρωσης πρέπει να αφορούν πιθανούς κινδύνους από την επίδειξη επικίνδυνης διαδικτυακής συμπεριφοράς, όπως είναι λ.χ. το παράνομο κατέβασμα αρχείων, ή η θέαση πορνογραφικού υλικού, κ.λ.π,. Με την απόφαση 276/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου δημιουργήθηκε ένα κοινοτικό πρόγραμμα δράσης για την προώθηση της ασφαλούς χρήσης του διαδικτύου μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα. Το πρόγραμμα δράσης "safer internet" στόχευε στην ανάπτυξη των εμπορικών δραστηριοτήτων μέσω της ασφαλούς χρήσης του διαδικτύου. Βάσει του προγράμματος αυτού,:

α) δημιουργήθηκαν δομές για την λήψη των καταγγελιών του κοινού σχετικά με ιστοσελίδες παράνομου περιεχομένου. Οι καταγγελίες έπειτα από διερεύνηση διαβιβάζονταν στις αρμόδιες υπηρεσίες για τον περαιτέρω χειρισμό της υπόθεσης.

β) αναπτύχθηκαν συστήματα φιλτραρίσματος ως τεχνικά μέσα άσκησης γονικού ελέγχου,

γ) Αναπτύχθηκαν δράσεις και ευαισθητοποίησης των γονέων και εκπαιδευτικών για την αλματώδη αύξηση των χρηστών του διαδικτύου σε μία προσπάθεια αποτελεσματικότερης προστασίας των ανηλίκων από την έκθεσή τους στο διαδίκτυο.

Με την απόφαση 854/2005/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου καθιερώθηκε ένα πολυετές κοινοτικό πρόγραμμα[151] για την προαγωγή της ασφαλέστερης χρήσης του διαδικτύου. Δημιουργήθηκαν γραμμές επικοινωνίας, ώστε οι πολίτες να έχουν τη δυνατότητα να επισημαίνουν παράνομες ιστοσελίδες ή πληροφορίες οι οποίες να διαβιβάζονται στα αρμόδια όργανα. Δημιουργήθηκαν δράσεις ευαισθητοποίησης για την προστασία των χρηστών του διαδικτύου[152].

[151] Περπέρης Α, Το Ηλεκτρονικο–οικονομικό έγκλημα: Ερευνητική προσέγγιση, Διδακτορική Διατριβή, Πάντειο Πανεπιστήμιο, Αθήνα, 2015

[152]https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32005D0854&qid=1448710668577&from=EL

9.3 Οι διωκτικές Αρχές.

Σημαντικά βήματα για την πρόληψη του ηλεκτρονικού-οικονομικού εγκλήματος, στο επίπεδο δίωξης, έχουν κάνει πολλά κράτη μέλη. Ειδικότερα προβαίνουν σε προμήθειες ακριβού τεχνολογικού εξοπλισμού, λαμβάνουν μέριμνα για την εκπαίδευση των στελεχών τους και προωθούν καμπάνιες ενημέρωσης του κοινού για την ποιοτικότερη καταπολέμηση του εγκλήματος[153]. Στην Ελλάδα δημιουργήθηκε η Διεύθυνση Δίωξης Ηλεκτρονικού εγκλήματος[154] η οποία στελεχώνεται από προσωπικό που διαθέτει πλέον πολύτιμες γνώσεις και εμπειρία, τόσο στα ηλεκτρονικο-οικονομικά όσο και στα νομικά θέματα. Έγινε προμήθεια κατάλληλου εξοπλισμού και ελήφθη μέριμνα για την συνεχή επιμόρφωση των στελεχών που υπηρετούν στη Δίωξη Ηλεκτρονικού Εγκλήματος με συμμετοχή σε σεμινάρια και διεθνή Forum. Τέλος καταβλήθηκε προσπάθεια συστηματοποίησης της εθνικής νομοθεσίας, κάλυψης των κενών αυτής, αλλά και εναρμόνισή της με τις νομοθεσίες των κρατών μελών της Ευρώπης.

Σύμφωνα με τους ειδικούς της δίωξης ηλεκτρονικού εγκλήματος, παρά τις δυσκολίες εντοπισμού των δραστών η ανωνυμία στο διαδίκτυο δεν ισχύει σε μεγάλο βαθμό. Στις περισσότερες μορφές εγκλήματος διαφαίνεται το μοντέλο πελάτης-πάροχος μία λειτουργία που θεσπίζει τον έλεγχο της πληροφορίας σε όλες τις διαδικτυακές επικοινωνίες, καθιστώντας, τρόπον τινά, δυνατή την ανίχνευση και τον εντοπισμό (trackback). Αυτό συμβαίνει γιατί προκειμένου οποιοσδήποτε να αποκτήσει πρόσβαση στο ίντερνετ θα πρέπει να καταχωρηθούν τα πραγματικά του στοιχεία σε έναν πάροχο διαδικτυακών υπηρεσιών. Στην συνέχεια ο πάροχος διαδικτυακών υπηρεσιών είναι υποχρεωμένος να τηρεί (log files) αρχεία, με το σημείο σύνδεσης του χρήστη, τη διεύθυνση IP, τη διάρκεια σύνδεσης, το μέγεθος των δεδομένων, κ.λ.π,. Τα στοιχεία αυτά διατίθενται σε οποιαδήποτε αρχή εφόσον ζητηθούν νόμιμα. Ακόμη και στις μορφές διαδικτυακής ανταλλαγής αρχείων, peer-to-peer - file sharing, υπάρχει ένα κομβικό σημείο ελέγχου, που δεν είναι άλλο, από τον

[153]https://www.youtube.com/playlist?reload=9&list=PLtnblhL7y4SZ2HLpamu-edW1_IzIsMdF3
[154] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194.

πάροχο της διαδικτυακής υπηρεσίας. Καθ' όλη τη διάρκεια διαδικτυακής σύνδεσης στο ίντερνετ αφήνονται ίχνη. Συνεπώς, το trackback (εντοπισμός) είναι εύκολη υπόθεση για τους "τεχνικούς" διώκτες των εγκλημάτων. Άλλωστε οι τελευταίες επιτυχίες της Δίωξης Ηλεκτρονικού εγκλήματος μαρτυρούν από μόνες τους[155].

[155]https://sputniknews.gr/ellada/201911015086742-diethnis-astynomikh-epixeirhsh-hlektronikes-apates-ellhnas-syllhpseis/

10. Επιλογικές σκέψεις – Συμπεράσματα.

Είναι αδιαμφισβήτητο ότι, η νέα τάση εγκληματικότητας τόσο στην Ελλάδα, όσο και στις υπόλοιπες χώρες της Ευρώπης, έχει ως βάση το διαδίκτυο καθώς και τη χρήση τερματικών συσκευών (υπολογιστής, Tablet, smartphones.) Είναι λογικό δε, λόγω των δυσχερειών στην απόδειξη, στην μη άμεση σύλληψη των δραστών, στη χρονοβόρα και επίπονη πολλές φορές διαδικασία απονομής δικαιοσύνης, καθώς και άλλων αιτιών που αναπτύχθηκαν στη παρούσα εργασία, να μην μπορεί να καταγραφεί ο ακριβής αριθμός των θυμάτων και των εγκληματικών πράξεων που τελέστηκαν διαμέσου του ηλεκτρονικού υπολογιστή ώστε να εξαχθούν ασφαλή συμπεράσματα για μια ολοκληρωμένη μελέτη. Καθημερινώς, δυστυχώς, γινόμαστε μάρτυρες εγκλημάτων που έχουν ως βάση το διαδίκτυο και τον τερματικό υπολογιστή γενικότερα. Απειλές, διαρροή προσωπικών δεδομένων, εκβιασμοί, εξυβρίσεις, δυσφημήσεις, απάτες, επιθέσεις Hacking – Cracking σε Κρατικές Υπηρεσίες κ.α, συνθέτουν μια γκάμα αδικημάτων που προσβάλλουν όχι μόνο το έννομο αγαθό τις περιουσίας, αλλά και πολλών άλλων.

Μέσα από τις συνεχείς παρεμβάσεις στην εθνική μας νομοθεσία και τη μελέτη του φαινομένου, διαφαίνεται καθαρά η βούληση των εθνικών κυβερνήσεων αφενός στο να εισάγουν ένα νέο νομοθετικό πλαίσιο που να συμβαδίζει με το ευρωπαϊκό κι αφετέρου να είναι ικανό να τιμωρεί το δράστη ώστε να επιτυγχάνεται η αντεγκληματική πολιτική και η προστασία άλλων εξίσου σημαντικών έννομων αγαθών. Άλλες φορές αυτό επιτυγχάνεται ικανοποιητικά, άλλες όμως φορές εισάγεται και «εσφαλμένως» γεγονός που καταστρέφει τόνους συνταχθέντων εγγράφων και εργατοωρών[156].

Περαιτέρω, το μοντέλο δίωξης των αδικημάτων αυτών και προστασίας των θυμάτων, από ποινικοδικονομικής άποψης, μέσω των δύο κατά κύριο λόγο αρμόδιων Υπηρεσιών της Δίωξης Ηλεκτρονικού Εγκλήματος (μια της Αθήνας

[156] Αναφερόμαστε εδώ στις μεταβολές της εθνικής μας νομοθεσίας που έχουν να κάνουν με τις υποβαθμίσεις των αδικημάτων (από κακούργημα σε πλημμέλημα) ή την αύξηση του ορίου της κακουργηματικής απάτης που οδηγεί σε ίδια αποτελέσματα όσον αφορά την τελική τιμωρία των υπαιτίων.

και μια της Θεσσαλονίκης) δεν μπορεί να θεωρηθεί ικανοποιητικό. Το εύρος του αντικειμένου, η πολυπλοκότητα και ο αριθμός των υποθέσεων, η έλλειψη ηλεκτρονικής επικοινωνίας μέσω των Υπηρεσιών, οι τόποι τέλεσης και δίωξης, αποτελούν ανασχετικό παράγοντα στον πολίτη, ο οποίος αποθαρρύνεται στην για την υποβολή μιας καταγγελίας, μη επιδιώκοντας την περαιτέρω ζημία του (μάρτυρες, δικαστήρια, αναβολές, κτλ). Η δίωξη, βέβαια, ενός εγκλήματος στα πλαίσια του ποινικού δικαίου καθίσταται πολλές φορές εντελώς αδιάφορη για τον πολίτη, που έχει ως κύριο στόχο μόνο την ανακάλυψη του δράστη για την αστική αποζημίωσή του από τις προκληθείσες βλάβες που υπέστη, μέσω τέτοιου είδους εγκλημάτων.

Άξιο μνείας, όσον αφορά τη διερεύνηση των εγκλημάτων μέσω διαδικτύου και ηλεκτρονικού υπολογιστή είναι και η διάσταση της Θεωρίας από την Πράξη. Έτσι κι ενώ κατ᾽ επιταγήν της νομοθεσίας περί άρσεως απορρήτου, (και θεωρίας), απαιτούνται συγκεκριμένες διαδικασίες και προϋποθέσεις για τη λήψη στοιχείων και δεδομένων επικοινωνιών, από τις ανακριτικές Αρχές, στη πράξη όλα αυτά «αλλάζουν» με τρείς εκδοθείσες μέχρι σήμερα γνωμοδοτήσεις εισαγγελέων Αρείου Πάγου[157].

Εν κατακλείδι, πολλά ακόμη απομένουν να γίνουν όσον αφορά τον τομέα της δίωξης του ηλεκτρονικού - οικονομικού εγκλήματος, τόσο ως προς την κατεύθυνση της βελτίωσης των εισαγόμενων ρυθμίσεων, όσο και στην ποιοτικότερη διεξαγωγή της ανακριτικής διαδικασίας μέσω μιας νόμιμης και ταχείας οδού συγκέντρωσης των αποδεικτικών στοιχείων.

[157] Βλέπε αντίστοιχες γνωμοδοτήσεις Εισαγγελέων Α.Π., 9/2009, 12/2009, 9/2011, που αφορούν τη λήψη στοιχείων – δεδομένων από τις Ανακριτικές Αρχές σχετικά με τα δεδομένα που φέρεται ότι προστατεύει ο νόμος περί άρσεως απορρήτου.

Π Ι Ν Α Κ Α Σ Α Ν Τ Ι Σ Τ Ο Ι Χ Ι Α Σ

ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ - Π.Δ 283/1985	ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ - Ν. 4619/2019
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	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 και χρηματική ποινή. 2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση τουλάχιστον ενός και χρηματική ποινή, 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 δύο ετών, 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 τριών (3) ετών, 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.

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.	
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.	Άρθρο 292Γ Με φυλάκιση έως δύο έτη ή χρηματική ποινή 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.
Άρθρο 370Β Παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα 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	Άρθρο 370Β Παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα 1. Όποιος κατά παράβαση μέτρου προστασίας και χωρίς δικαίωμα αποκτά πρόσβαση σε μέρος ή στο σύνολο συστήματος πληροφοριών ή σε ηλεκτρονικά δεδομένα τιμωρείται με φυλάκιση έως δύο έτη ή χρηματική ποινή. Σε ιδιαίτερα ελαφρές περιπτώσεις η πράξη μένει ατιμώρητη. 2. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του συστήματος πληροφοριών ή των δεδομένων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του. 3. Αν η πράξη της παραγράφου 1 αναφέρεται σε επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή. 4. Αν ο δράστης είναι στην υπηρεσία του

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.	νόμιμου κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής αξίας, επιβάλλεται φυλάκιση και χρηματική ποινή. 5. Για την ποινική δίωξη των πράξεων των παραγράφων 1 και 4 απαιτείται έγκληση.
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.	Άρθρο 370Γ 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 κάτοχος 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. Οι πράξεις που προβλέπονται στο άρθρο αυτό διώκονται με έγκληση.
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.	Άρθρο 370Δ 1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας. 2. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα

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.	ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του, τιμωρείται με φυλάκιση. 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.
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.	Άρθρο 370Ε 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 περιεχόμενο τους, τιμωρείται με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή. 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.
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.	
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.	
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.	Άρθρο 386Α Απάτη με υπολογιστή 1. Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή: α) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή, β) με τη χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή, γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, ή ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων τιμωρείται με φυλάκιση και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000 ευρώ, επιβάλλεται κάθειρξη έως δέκα έτη και χρηματική ποινή. 2. Όποιος κατασκευάζει, διαθέτει ή κατέχει πρόγραμμα ή σύστημα υπολογιστή που προορίζεται για τη διάπραξη του εγκλήματος της παραγράφου 1 τιμωρείται με φυλάκιση έως δύο έτη και χρηματική ποινή. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή σύστημα υπολογιστή πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παραγράφου 1. 3. Αν η απάτη με υπολογιστή στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000

	ευρώ επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή έως χίλιες ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά είκοσι έτη.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α Ε Λ Λ Η Ν Ι Κ Η

1. **Αγγελής Ι.** Διαδίκτυο (internet) και Ποινικό Δίκαιο. Έγκλημα στον κυβερνοχώρο (cybercrime-internet crime), Ποιν. Χρ Ν,675
2. **Ανδρέου Φ.,** Ποινικός Κώδικας, 2005
3. **Ανδρουλάκη Ν.,** Ποινικό Δίκαιο - Γενικό Μέρος (Θεωρία για το έγκλημα), Π.Ν Σάκκουλας
4. **Αργυρόπουλος Α.,** «Ηλεκτρονική εγκληματικότητα» 2001,
5. **Βαγενά Ε.,** Το νέο θεσμικό Πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος, ΔιΜΕΕ 2017 ΕφΑθ 9099/2005, ΔιΜΕΕ
6. **Βασιλάκη Ε.,** Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών Υπολογιστών. Η αντιμετώπιση του προβλήματος ιδιαίτερα μετα την εισαγωγή του ν. 1805/1988 Α.Ν Σάκκουλας, Αθήνα 1993,
7. **Βασιλάκη Ε.,** Τα φαινόμενα pharming, phishing και η ποινική τους αξιολόγηση, ΠοινΧρ2007,
8. **Βλαχόπουλος Κ.,** Ηλεκτρονικό έγκλημα, 2007,.
9. **Γασπαρινάτου Μ**., Έγκλημα και ποινική καταστολή σε εποχή κρίσης, Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη, Α.Ν ΣΑΚΚΚΟΥΛΑΣ 2016.
10. **Γέρμανος Γ. – Παπαθανασίου Α.,** Νομοθεσία για το έγκλημα στον Κυβερνοχώρο και την Ψηφιακή εγκληματικότητα, Α.Ν Σάκκουλα Ε.Ε, 2017
11. **Γιαννόπουλος Θ.,** ΝΟΒ. 34 (1986).
12. **Δαλακούρας Θ.,** Ηλεκτρονικό έγκλημα, με παρατηρήσεις Κιούπη Δ., όσον αφορά τον τόπο τέλεσης του ηλεκτρονικού εγκλήματος. Ν.Β 2019,
13. **Ιγγλεζάκη Ι.,** Δίκαιο της πληροφορικής, β΄ έκδοση Σάκκουλα, Αθήνα - Θεσσαλονίκη, 2008,
14. **Ιωαννίδης Χ.,** Νομικά Ζητήματα αναφορικά με Εγκλήματα Λευκού Κολάρου, (Σάκκουλας, Αθήνα-Κομοτηνή), 2001
15. **Καϊάφα - Γκμπάντι Μ.,** Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής,
16. **Καιάφα Γκπάντι,** Εμβάθυνση στην ποινική νομολογία,
17. **Καπαρδής Α.,,** Μαρία Κραμβιά-Καπαρδή και Νέστωρας Κουράκης, *Οικονομικά Εγκλήματα στην Κύπρο: Μια Πολυθεματική Προσέγγιση* (Α. Σάκκουλας, Αθήνα-Κομοτηνή, 2001)
18. **Κιούπη Δ.,** Ποινικό Δίκαιο και internet.
19. **Κουπαράνης Π,** (2014), «Η φοροδιαφυγή το στόχαστρο του ΟΟΣΑ», http://www.dw.de , 2014
20. **Κωνσταντινίδη, Α.,** Η διακεκριμένη παραβίαση απορρήτων στοιχείων (πρώην άρθρο 370Β παρ.2 περ. β΄Π.Κ), ΠοινΧρ1997, σελ. 1216, Αιτιολογική Έκθεση Σχεδίου Ποινικού κώδικα 1933, Α.Π 1026/2008, ΠοινΧρ ΝΟ, σελ. 343 και Α.Π 2270/2009, σε www.areiospagos.gr/nomologia/apofaseis_result.asp?S=1 Α.Π 1607/2007 Ποιν.Δικ 2008,
21. **Λάζος Γ. (2001):** Πληροφορική και Έγκλημα, Αθήνα , Νομική Βιβλιοθήκη
22. **Μαργαρίτης Μ.**, Ποινικός Κώδικας, Ερμηνεία – Εφαρμογή, 2η έκδοση 2009
23. **Μανωλεδάκη Ι.,** Ποινικό Δίκαιο, ζ΄ έκδοση, Σάκκουλας Αθήνα - Θεσσαλονίκη 2005
24. **Μανωλεδάκη Ι.,** Ποινικό Δίκαιο - Γενική Θεωρία, 2004

25. **Μυλωνόπουλος Χ.,** Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Α. Ν. Σάκκουλας, Αθήνα 1991,
26. **Μυλωνόπουλος Χ.,** Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991,
27. **Περπέρης Α.**, Το Ηλεκτρονικο–οικονομικό έγκλημα: Ερευνητική προσέγγιση, Διδακτορική Διατριβή, Πάντειο Πανεπιστήμιο, Αθήνα, 2015
28. **Σπυρόπουλος Φ.,** Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (Hacking), Ποινική και εγκληματολογική προσέγγιση - Αξιολόγηση της Ελληνικής Ποινικής Νομοθεσίας - Έρευνα σε δείγμα νομικών, επιστημόνων πληροφορικής και hackers, Σειρά: ΠΟΙΝΙΚΑ, Α. Ν. Σάκκουλας, Αθήνα 2016.,
29. **Σφακιανάκης Ε.**, Ο κώδικας του Διαδικτύου, εκδ. All about Internet, Αθήνα 2016,
30. **Χατζηνικολάου Ν.,** Ποινικό Δίκαιο - Ειδικό Μέρος, Εγκλήματα κατα τις ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών, των κοινωφελών εγκαταστάσεων, της λειτουργίας πληροφοριακών συστημάτων. Σάκκουλας, Αθήνα 2017 Συμβ.Διαρκ.Στρ.Αθ. 401/1986., ΠοινΧρ. ΛΣΤ΄77
31. **Χαραλαμπάκη Α.,** Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο, 2η έκδοση Νομική Βιβλιοθήκη 2014.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α Ξ Ε Ν Ο Γ Λ Ω Σ Σ Η

1. **Tanenbaum, A.** (2011*) Computer Networks*, 5th Edition,
2. **Pearson.Lilian Mitrou ,** "Cybercrime" and computer crime": Lecture Notes in Postgraduate Programme" Techno-economic Management & Security of Digital Systems", Department of Digital Systems, University of Piraeus
3. **Lambrinoudakis, C.,** Mitrou, L., Gritzalis, S., Katsikas, S. K., (2010). Privacy Enhancing Technologies: A review. In Lambrinoudakis, C., Gritzalis, S., and Katsikas, S. K., editors, Privacy Protection and Information and Communication Technologies: Technical and Legal Issues. Papasotiriou Pubs, Athens, Greece. In Greek
4. **Parker, D. B. (1989).** Computer Crime: Criminal Justice Resource Manual. Technical Report OJP-86-C-002, U.S. Department of Justice, National Institute of Justice, Office of Justice Program. 2nd edition
5. **James F. Kurose, University of Massachusetts, Amherst, Keith W. Ross, Polytechnic University, Brooklyn,. Computer Networking: A Top-Down Approach, 6th Edition**
6. OECD Computer related crime : An analysis of legal policy, Paris: OECD, 1986
7. **Smith Russell**, Grabosky Peter & Urbas Gregor (2004),
8. **Grabosky Peter** & Walkley Sascha, (2007),
9. **Parker Donn (1997),** "Computer abuse", στο Hollinger Richard C. (editor), *Crime, deviance and the computer*, Aldershot Hants, England: Dartmouth,
10. **Gibbs Carole,** Cassidy Michael B., & Rivers Louie (2013),
11. **Shinder Debra Littlejohn**, Tittel Ed. (2002), Scene of cybercrime Computer Forensics Handbook, Syngress Publishing Newman Graeme R., & Clarke Ronald V. (2003), Super-highway Robbery: Preventing ECommerce Crime. Cullompton, Devon, Willan, N.Y.,
12. **Choi Kyung-shick (2008b),** «Computer Crime Victimization and Integrated Theory: An Empirical Assessment», *International Journal of Cyber Criminology* (IJCC) ISSN: 0974 – 2891 January-June 2008,
13. **Cohen Lawrence & Felson Marcus (1979),** "Social change and crime rate trends: a routine **activity approach*", American Sociological Review*, 44,**
14. **Reyns Bradford W.,** Henson Billy & Fisher Bonnie S. (2011), «Being Pursued Online: Applying Cyber-Lifestyle-Routine Activities Theory To Cyberstalking Victimization», *Criminal Justice and Behavior*,
15. **Bossler Adam**, & Holt Thomas J. (2009)
16. **Sieber, Computer crimes**, cyber - terrorism, child pornography and financial crimes, in D. Spinellis (ed.), Computer crimes, cyber - terrorism, child pornography and financial crimes, 2004,.

Διαδικτυακές Πηγές, Παραπομπές και Αποφάσεις

1. https://www.newsit.gr/ellada/apates-sms-katapeltis-i-dioksi-ilektronikou-egklimatos/2842365
2. https://www.lawspot.gr/nomika-nea/paremvasi-synigoroy-toy-katanaloti-gia-tis-hreoseis-minymaton-apo-5psifia-noymera-sta
3. http://www.synigoroskatanaloti.gr/docs/announce/2017-09-22.Epistoli-EETT.pdf
4. http://www.synigoroskatanaloti.gr/docs/reports/2017-12-22.%CE%A3%CF%85%CF%83%CF%84%CE%B1%CF%83%CE%B7-%CE%A5%CE%A0%CE%A0.pdf
5. http://www.synigoroskatanaloti.gr/docs/reports/2017-12-22.%CE%A3%CF%85%CF%83%CF%84%CE%B1%CF%83%CE%B7-%CE%A5%CE%A0%CE%A0.pdf
6. Δεληγιάννης Κ., Ο κόσμος του σκοτεινού Internet, Η ΚΑΘΗΜΕΡΙΝΗ http://www.astynomia.gr/images/stories/2015/2prak_syn.pdf,. https://www.hba.gr/Media/Details/397., Νοέμβρ. 2019
7. https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32005D0854&qid=1448710668577&from=EL
8. https://sputniknews.gr/ellada/201911015086742-diethnis-astynomikh-epixeirhsh-hlektronikes-apates-ellhnas-syllhpseis
9. https://www.lifo.gr/articles/technology_articles/168993
10. https://www.sutori.com/story/e-istoria-tou-internet--zYdjkNDuzTpjB8uamiiuT1Cj
11. https://www.retrocomputers.gr/forum/istoria-ypologiston-software-ktl/2104-istoria-tou-internet
12. http://www.epaggelmaties.com/writer/2001-2003/internethistory.html
13. https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=2ahUKEwjc5bnj__HmAhUSL1AKHaUaD1IQjRx6BAgBEAQ&url=https%3A%2F%2Fmalonemediagroup.com%2Fhistory-of-the-internet-timeline-an-ever-evolving-digital-world%2F&psig=AOvVaw1oDLvcmnF06lHQ7D3ZC2xj&ust=1578503992207802
14. http://www.uth.gr/main/help/help-desk/internet/internet2.html
15. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf
16. https://www.kathimerini.gr/765417/article/texnologia/diadiktyo/o-kosmos-toy-skoteinoy-internet
17. http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/5723/CIED%20%20%20%20%20%20%20%20%20%20%20%20%20%20.pdf?sequence=1
18. https://www.pwc.com/gr/en/media-centre/assets/global-economic-crime-pr-gr.pdf
19. https://www.pwc.com/gr/en/publications/assets/economic%20crime%20fraud%20survey-gr.pdf

20. http://www.cybercrimejournal.com/Choiijccjan2008.htm, Μαρτ. 2014 και Bossler Adam & Holt Thomas (2009), "On-line Activities, Guardianship, & Malware Infection: An Examination of Routine Activities Theory," *International Journal of Cyber Criminology*, 3,
21. https://rm.coe.int/16800cce5b.
22. https://youtu.be/8pZ6CY6Txng?t=202,. Δηλώσεις της Αναπληρώτριας συνήγορο του καταναλωτή Αθηνάς Κοντογιάννη.
23. https://www.newsit.gr/ellada/apates-sms-katapeltis-i-dioksi-ilektronikou-egklimatos/2842365/
24. Βλ. https://www.youtube.com/embed/cEkpSEyfxLE., Δηλώσεις εκρποσώπου τύπου της ΕΛ.ΑΣ., Νοεμβ. 2019
25. http://criminology.panteion.gr, Νοέμβριος 2014Zarafonitou Christina & Koumentaki Evangelia (2014), *Victimisation and insecurity of undergraduate students while using internet*, 14th Annual Conference of the ESC, Prague, 10-13 September 2014, ανακτήθηκε από
26. https://www.cepol.europa.eu/el., Νοέμβρ., 2019
27. Περπέρης Α., «Ο ρόλος των κινήτρων και των ευκαιριών στη δόμηση του προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος», http://crime-in-crisis.com/%CE%BF-%CF%81%CF%8C%CE%BB%CE%BF%CF%82-%CF%84%CF%89%CE%BD-%CE%BA%CE%B9%CE%BD%CE%AE%CF%84%CF%81%CF%89%CE%BD-%CE%BA%CE%B1%CE%B9-%CF%84%CF%89%CE%BD-%CE%B5%CF%85%CE%BA%CE%B1%CE%B9%CF%81%CE%B9%CF%8E%CE%BD/#
28. https://www.cepol.europa.eu/el.
29. Cybercrime, The Parliamentary Assembly-Reactions and Conclusions, στην η.δ.http://www.coe.int/T/T/Communication_and_Research/Press/Theme_Files/Cybercrime.
30. Cybercrime, the law moves on, στην η.δ. http://www.coe.int/T/T/Communication_and_Research/Press/Theme_Files/Cybercrime.