ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΑΠΑΤΗ ΣΤΑ ΣΥΓΧΡΟΝΑ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ Η ΠΟΙΝΙΚΗ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗ

Διπλωματική Εργασία

του

Χαράλαμπου Α. Μουράτογλου

Θεσσαλονίκη, 02/2024

Η ΑΠΑΤΗ ΣΤΑ ΣΥΓΧΡΟΝΑ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ Η ΠΟΙΝΙΚΗ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗ

Χαράλαμπος Α. Μουράτογλου

Πτυχίο Στρατιωτικής Σχολής Ευελπίδων (ΣΣΕ), 2018

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές

Θεοχάρης Δαλακούρας
Νικόλαος Αποστολίδης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29/02/2024

Θεοχάρης Δαλακούρας	Νικόλαος Αποστολίδης	Γεώργιος Δανιήλ
.....	.....	.....

Χαράλαμπος Α. Μουράτογλου

Περίληψη

Το περιβάλλον των ηλεκτρονικών υπολογιστών και του διαδικτύου, εκτός από τα αδιαμφισβήτητα οφέλη που απλόχερα παρέχει στον κάθε χρήστη τον 21ο αιώνα, εγκυμονεί πλήθος κινδύνων για τα προσωπικά του δικαιώματα, τα οποία αρκετές φορές καταστρατηγούνται. Η ανωνυμία του διαδικτύου, η άγνοια των χρηστών, ο εκμηδενισμός των αποστάσεων, αλλά και η ιλιγγιώδης ταχύτητα με την οποία συντελείται καθετί στο ηλεκτρονικό περιβάλλον, αποτέλεσαν μερικές μόνο από τις αιτίες, στις οποίες αποδίδεται ο φρενήρης ρυθμός πολλαπλασιασμού των ηλεκτρονικών εγκλημάτων σήμερα. Η απάτη, η οποία θα μας απασχολήσει στην παρούσα διπλωματική εργασία, αποτελεί τη συνηθέστερη έκφανση του ηλεκτρονικού εγκλήματος σήμερα, αποτελώντας μία σύγχρονη πρόκληση για το νομοθέτη, ο οποίος καλείται να παρακολουθεί και να συμβαδίζει με τις τεχνολογικές εξελίξεις σε παγκόσμια κλίμακα, προκειμένου να είναι σε θέση να αποκαθιστά τη δικαιική ειρήνη.

Η παρούσα διπλωματική εργασία χωρίζεται σε 3 μέρη. Αρχικά, γίνεται αναφορά στη γένεση και στην εξέλιξη των ηλεκτρονικών υπολογιστών μέχρι και σήμερα. Πραγματοποιείται μία σύντομη εξήγηση του τρόπου λειτουργίας και επικοινωνίας των ηλεκτρονικών υπολογιστών μεταξύ τους, προκειμένου να δημιουργηθεί αυτό που αποκαλούμε «διαδίκτυο» σήμερα.

Στη συνέχεια, γίνεται αναφορά στη λειτουργία των υπολογιστών ως μέσα διάπραξης εγκλημάτων με παράλληλη αναφορά στα δύο βασικότερα άρθρα του ΠΚ (386 και 386Α) που ποινικοποιούν την απάτη.

Τέλος, αναφέρονται ορισμένες σύγχρονες μορφές ηλεκτρονικής απάτης, το phishing, το pharming, η χωρίς δικαίωμα ανάληψη χρημάτων από ΑΤΜ, καθώς και το skimming, οι οποίες απασχολούν τις αρχές σε παγκόσμιο επίπεδο ολοένα και περισσότερο τη σημερινή εποχή.

Λέξεις Κλειδιά: διαδίκτυο, ηλεκτρονικό έγκλημα, κυβερνοέγκλημα, ποινικό δίκαιο, ηλεκτρονική απάτη, απάτη με υπολογιστή, απάτη μέσω υπολογιστή, phishing, pharming, skimming.

Abstract

The environment of computers and the internet, apart from the indisputable benefits that they generously provide to each user in the 21st century, poses a multitude of risks for their personal rights, which are often circumvented. The anonymity of the internet, the ignorance of users, the annihilation of distances, but also the dizzying speed with which everything is done in the electronic environment, were just some of the causes, to which the frenzied rate of proliferation of electronic crimes is attributed today. Fraud, which will concern us in this thesis, is the most common manifestation of electronic crime today, constituting a modern challenge for the legislator, who is called upon to monitor and keep pace with technological developments on a global scale, in order to restore justice.

This thesis is divided into 3 parts. First, reference is made to the genesis and evolution of computers until today. A brief explanation is given of how computers work and communicate with each other to create what we call the "Internet" today.

Then, reference is made to the operation of computers as a means of committing crimes with a parallel reference to the two main articles of the Criminal Code (386 and 386A) which criminalize fraud.

Finally, reference is made to some modern forms of electronic fraud, phishing, pharming, unauthorized withdrawal of money from ATMs, as well as skimming, which concern authorities worldwide more and more nowadays.

Keywords: internet, electronic crime, cybercrime, criminal law, electronic fraud, computer fraud, computer fraud, phishing, pharming, skimming.

ΠΕΡΙΕΧΟΜΕΝΑ

Συμβολισμοί

Ελληνικοί Συμβολισμοί

ΑΠ	Άρειος Πάγος
ΑΤΜ	Αυτόματο Ταμειολογιστικό Μηχάνημα
α.υ.ε	Αντικειμενική Υπόσταση Εγκλήματος
Βλ.	Βλέπετε
ΕΕ	Ευρωπαϊκή Ένωση
Επ.	επόμενα
ΗΥ	Ηλεκτρονικός Υπολογιστής
κ.λπ.	και λοιπά
ν.	Νόμος
ν.π.δ.δ.	Νομικό Πρόσωπο Δημοσίου Δικαίου
ν.π.ι.δ.	Νομικό Πρόσωπο Ιδιωτικού Δικαίου
ΟΤΑ	Οργανισμός Τοπικής Αυτοδιοίκησης
Παρ.	Παράγραφος
ΠΚ	Ποινικός Κώδικας
ΠοινΔικ	Ποινική Δικαιοσύνη
ΠοινΛογ	Ποινικός Λόγος
ΠοινΧρ	Ποινικά Χρονικά
π.χ.	Παραδείγματος Χάριν
σελ.	Σελίδα
ΤρΕφΚακΑθ	Τριμελές Εφετείο Κακουργημάτων Αθηνών
υ.υ.ε	Υποκειμενική Υπόσταση Εγκλήματος

Ξενόγλωσσοι Συμβολισμοί

ARPA	Advanced Research Projects Agency
CIA	Confidentiality Integrity Availability
CPU	Central Processing Unit
DNS	Domain Name System
EMV	Europay Mastercard Visa
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network
p2p	peer-to-peer
PIN	Personal Identification Number
POS	Point of Sale
RFID	Radio Frequency Identification
SMS	Short Message Service
TCP	Transmission Control Protocol
tor	The Onion Routing
URL	Uniform Resource Locator
WAN	Wide Area Network
WLAN	Wide Local Area Network
WWW	World Wide Web

1 Εισαγωγικές Σκέψεις

Ο 21ος αιώνας ακόμη πριν από την αφετηρία του, προμηνύοταν ότι θα αποτελέσει τον αιώνα των τεχνολογικών εξελίξεων και αλλαγών. Διαβιώνουμε σε μία, όπως συχνά ακούμε να αποκαλείται, «Κοινωνία της Πληροφορίας», στην οποία ο τεχνολογικός τομέας διαδραματίζει πρωταρχικό ρόλο. Η πρόσφατη, πρωτόγνωρη και σε παγκόσμια κλίμακα, επιδημιολογική πανδημία του Covid-19, επέβαλλε τη μεταφορά αρκετών πτυχών της καθημερινότητάς μας (π.χ. εκπαίδευση, εργασία, αγορές, διασκέδαση) στο ηλεκτρονικό περιβάλλον, ενώ συγχρόνως αποτέλεσε μία βλέψη στο (ίσως όχι και τόσο μακρινό) μέλλον και στον τρόπο με τον οποίο το διαδίκτυο και οι ηλεκτρονικοί υπολογιστές δύνανται να λειτουργήσουν και να συνδράμουν την ανθρωπότητα. Η αμεσότητα, η ευκολία, καθώς και η καθολικότητα της πρόσβασης στο διαδίκτυο σήμερα, αποτελούν επακόλουθα της αλματώδους ανάπτυξης που έχει σημειώσει ο τεχνολογικός τομέας. Το γεγονός αυτό όμως, έχει λειτουργήσει ευνοϊκά για την γένεση και ευδοκίμηση νέων μορφών κοινωνικών συμπεριφορών[1], μερικές από τις οποίες προσβάλλουν τα έννομα αγαθά ή δικαιώματα τρίτων με αποτέλεσμα να χαρακτηρίζονται ως αξιόποινες.

Η συνδρομή των ηλεκτρονικών υπολογιστών στη βελτίωση της ποιότητας ζωής του ανθρώπου είναι αδιαμφισβήτητη και τα οφέλη αναρίθμητα. Ωστόσο, η μη συνετή χρήση αυτών, είναι ικανή να τους «μεταλλάξει» από πολύτιμα εργαλεία, σε μέσα διάπραξης εγκλημάτων. Ορισμένα από αυτά (τα λεγόμενα γνήσια ηλεκτρονικά εγκλήματα) τελούνται αποκλειστικά σε τεχνολογικό περιβάλλον, με ή χωρίς τη συμβολή του διαδικτύου, ενώ στα υπόλοιπα (μη γνήσια ηλεκτρονικά εγκλήματα) η επιστήμη της πληροφορικής χρησιμοποιείται απλώς για τη μεταφορά των παραδοσιακών μορφών αδικημάτων σε μία καινούργια υπόσταση[2]. Στις περισσότερες περιπτώσεις, παρόλο που το ουσιαστικό περιεχόμενο μίας αξιόποινης πράξης παραμένει αναλλοίωτο συγκριτικά με την «παραδοσιακή» μορφή της, εντούτοις, διαφοροποιούνται και πληθαίνουν σημαντικά οι τρόποι τέλεσής της. Η αναγκαιότητα για φυσική επαφή θύτη – θύματος έχει πλέον εκλείψει και αντικαθίσταται σε μεγάλο βαθμό από την απροσωπία και ανωνυμία που εξασφαλίζουν οι υπολογιστές και το διαδίκτυο.

[1] Κιούπης Δ., Ποινικό δίκαιο και internet, 1999

[2] Αγγελής Ι., Διαδίκτυο και Ποινικό Δίκαιο, ΠοινΧρ Ν/2000

Η απάτη με υπολογιστή, η οποία και ποινικοποιείται με το Άρθρο 386Α ΠΚ, αποτελεί μία από τις συνηθέστερες εκφάνσεις του ηλεκτρονικού εγκλήματος σήμερα. Συνήθως, συνίσταται στην εισαγωγή, αφαίρεση ή αλλοίωση δεδομένων ή/και προγραμμάτων ενός ηλεκτρονικού υπολογιστή[3] και αποσκοπεί στον προσπορισμό παράνομου περιουσιακού οφέλους στον δράστη εις βάρος του θύματος. Η εισαγωγή του διαδικτύου στην επιστήμη των υπολογιστών, άλλαξε ριζικά την μέχρι τότε διαμορφωθείσα κατάσταση και συνέβαλε καθοριστικά στη δημιουργία νέων μορφών ηλεκτρονικής απάτης, με το phishing, το pharming και το skimming να αποτελούν χαρακτηριστικά παραδείγματα αυτών. Το ευρύτατο φάσμα των δυνατοτήτων που παρέχεται από τα σύγχρονα υπολογιστικά συστήματα, σε συνδυασμό με τη σημαντικά μεγάλη ανωνυμία που εξασφαλίζει ο κυβερνοχώρος, έχουν ανάγει την ηλεκτρονική απάτη σε ένα ιδιαίτερα συχνό φαινόμενο, το οποίο μαστίζει ολοένα και μεγαλύτερο τμήμα της σύγχρονης κοινωνίας. Παράλληλα, η ιλιγγιώδης ταχύτητα με την οποία συντελούνται οι «πράξεις» στον κυβερνοχώρο, έχει πολλές φορές ως αποτέλεσμα ο χρήστης να μην αντιλαμβάνεται καν ότι έχει πέσει θύμα διαδικτυακής απάτης.

Η ραγδαία τεχνολογική ανάπτυξη αποτελεί μία σύγχρονη και άνευ προηγουμένου πρόκληση για τη νομική επιστήμη, με την οποία σε αρκετές περιπτώσεις αδυνατεί να συμβαδίσει. Κάτι τέτοιο συμβαίνει διότι, αφενός μεν για την προσέγγιση των νομικών θεμάτων που σχετίζονται με τον κυβερνοχώρο, απαιτείται εξειδικευμένη γνώση των τεχνολογιών επιστήμης και πληροφορικής[4], αφετέρου δε υπάρχει δυσκολία συσχέτισης και ερμηνείας τους, με αποτέλεσμα η θέσπιση των κανόνων δικαίου να έπεται της τέλεσης των αδικημάτων. Η αρχή ότι το διαδίκτυο και οι υπολογιστές, εκτός από τα αδιαμφισβήτητα πλεονεκτήματα που παρέχουν και είναι γνωστά σε όλους, μπορεί να λειτουργήσουν και ως μέσα τέλεσης εγκλημάτων, πρέπει να υιοθετείται από τον κάθε συνετό χρήστη, ενώ η καλύτερη γνώση των κινδύνων που εγκυμονούνται στον Παγκόσμιο Ιστό μπορεί να λειτουργήσει επικουρικά στην πρόληψη των ανεπιθύμητων καταστάσεων.

[3] Μυλωνόπουλος Χρ., Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991

[4] Αγγελής Ι., Διαδίκτυο και Ποινικό Δίκαιο, ΠοινΧρ Ν/2000

2 Το διαδίκτυο από προνόμιο για λίγους, σε αναγκαιότητα

Στις αρχές του 21ου αιώνα, κανένας σχεδόν δε θα μπορούσε να φανταστεί ότι το Διαδίκτυο, το οποίο αποτελούσε ένα προνόμιο που μόλις το 14% του πληθυσμού στη χώρα μας κατείχε, θα έφτανε στο σημείο να αποτελέσει ένα «εργαλείο» πολλαπλής χρησιμότητας[5]. Φυσικά το ιδιαίτερα χαμηλό αυτό ποσοστό δεν οφείλεται αποκλειστικά στην απροθυμία των πολιτών να ενστερνιστούν κάθε είδους καινοτόμο τεχνολογικό επίτευγμα. Ανάμεσα στους παράγοντες που οφείλονται για την καθυστέρηση της εξάπλωσής του, συγκαταλέγονται τόσο το ιδιαίτερα υψηλό κόστος αγοράς ενός ηλεκτρονικού υπολογιστή και των παρελκομένων του, όσο και το κόστος πρόσβασης στο διαδίκτυο τη χρονική περίοδο εκείνη. Έτσι λοιπόν, μόλις δύο δεκαετίες πριν, δε θα αποτελούσε υπερβολή να το χαρακτηρίζαμε ως μια πολυτέλεια για λίγους.

Ωστόσο, τα ολοένα και αυξανόμενα πλεονεκτήματα του διαδικτύου σε συνδυασμό με τη διείσδυσή του στις διάφορες πτυχές της καθημερινότητας των ανθρώπων (εργασία, μελέτη, διασκέδαση, έρευνα, κοινωνική δικτύωση κ.λπ.), οδήγησαν τον κόσμο στην αποβολή του σκεπτικισμού που μπορεί να τον απέτρεπε από τη νέα αυτή τεχνολογία. Σημαντικό ρόλο σε αυτό φυσικά έπαιξε και η απήχηση που είχαν οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο στις νεότερες ηλικίες (περίπου το 50% των νέων 15-25 ετών από τις αρχές ακόμα του 21ου αιώνα είχε αποκτήσει πρόσβαση στον Παγκόσμιο Ιστό).

Μέχρι και σήμερα, ο ρυθμός εξάπλωσης της τεχνολογίας των ηλεκτρονικών υπολογιστών και του διαδικτύου έχει υπάρξει καταιγιστικός, με το 63% πλέον του παγκοσμίου πληθυσμού να έχει πρόσβαση σε αυτό[6] (2021). Μάλιστα, αν αναλογιστεί κανείς ότι το ποσοστό αυτό φτάνει να αγγίζει το 98% και 94% για τις χώρες της Βόρειας και Νότιας Ευρώπης αντίστοιχα[7], συνειδητοποιεί τον καθοριστικό ρόλο που πλέον διαδραματίζει στην καθημερινότητά μας.

Προκειμένου όμως να είναι κάποιος σε θέση να κατανοήσει καλύτερα τη φιλοσοφία του Παγκόσμιου Ιστού, καθώς και τους κίνδυνους που αυτός μπορεί να εγκυμονεί για τους χρήστες του, κρίνεται σκόπιμη η αναφορά του τρόπου λειτουργίας των δικτύων, καθώς και μία αναφορά στην ιστορική εξέλιξη αυτού.

[5] Βλ. Φραγκάκης Δ, Ιστορικά Αρχεία στο Διαδίκτυο, Βιβλιοθήκες και Πληροφόρηση, τεύχος 16, 2003

[6] https://www.statista.com/statistics/209096/share-of-internet-users-in-the-total-world-population-since- 2006/

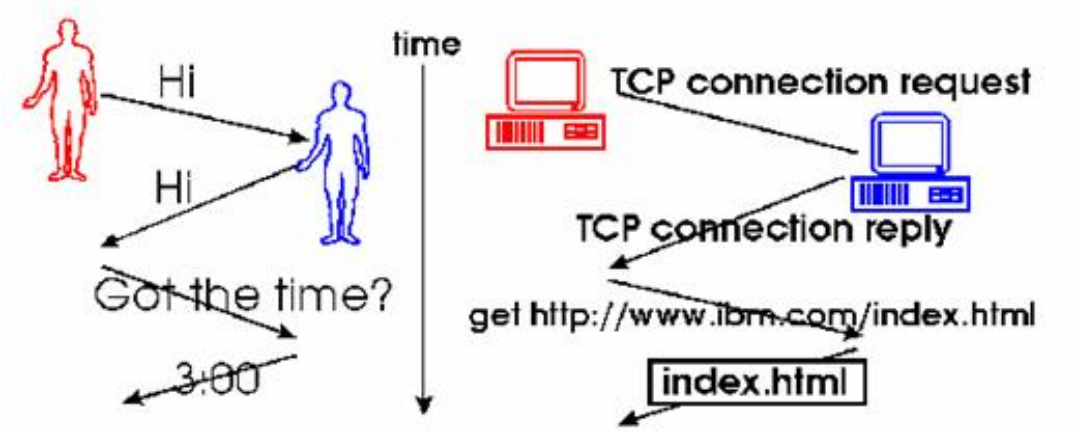
[7] https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/

2.1 Τι ονομάζουμε δίκτυο υπολογιστών

Ο όρος «δίκτυο υπολογιστών» χρησιμοποιείται για να περιγράψει δύο ή περισσότερα υπολογιστικά συστήματα (ηλεκτρονικοί υπολογιστές, «έξυπνα τηλέφωνα», «έξυπνες» ηλεκτρικές συσκευές κ.λπ.) τα οποία επικοινωνούν, δηλαδή ανταλλάσσουν πληροφορίες και δεδομένα μεταξύ τους. Προκειμένου αυτό να καταστεί δυνατό, είναι απαραίτητη η φυσική τους (ενσύρματη ή ασύρματη) διασύνδεση.

Η ανταλλαγή δεδομένων μεταξύ των υπολογιστών διέπεται από ένα σύνολο τυποποιημένων κανόνων[8], που ονομάζονται πρωτόκολλα, τα οποία και καθορίζουν επακριβώς τα βήματα που πρέπει να ακολουθηθούν από τα μέρη, για την επίτευξη της επικοινωνίας μεταξύ τους. Κατά μία διαφορετική προσέγγιση, αποτελούν μία «συμφωνία» μεταξύ των υπολογιστών ως προς τον τρόπο με τον οποίο θα αρχίσει και θα συνεχιστεί η επικοινωνία.

Ο τρόπος επικοινωνίας των υπολογιστών μέσω των πρωτοκόλλων μπορεί να παραλληλιστεί με τον τρόπο λειτουργίας της ανθρώπινης επικοινωνίας. Όταν ένα άτομο θέλει να απευθύνει μια ερώτηση σε ένα άλλο (π.χ. τι ώρα είναι), (συνήθως) ξεκινά τη συζήτηση με ένα σύντομο χαιρετισμό. Αν το αντισυμβαλλόμενο μέρος απαντήσει με τον ανάλογο τρόπο, τότε αυτό εκλαμβάνεται ως ένα θετικό στοιχείο για τη συνέχιση της επικοινωνίας και προβαίνει στην επιθυμητή ερώτηση. Αν όμως, για κάποιο λόγο, δε λάβει ανταπόκριση στο χαιρετισμό του, ή η απάντηση που θα λάβει ο ερωτηθείς υποδηλώνει απροθυμία συνέχισης της συζήτησης, τότε η επικοινωνία περατώνεται.



Πηγή: http://www2.ic.uff.br/~michael/kr1999/1-introduction/1_02-protocol.htm

[8]Βλ. http://www2.ic.uff.br/~michael/kr1999/1-introduction/1_02-protocol.htm

Στα δίκτυα υπολογιστών, ο αριθμός των χρησιμοποιούμενων πρωτοκόλλων είναι ιδιαίτερα μεγάλος, καθένα από τα οποία ρυθμίζει τον τρόπο λειτουργίας μίας διαφορετικής διεργασίας.

2.2 Οι κατηγορίες των δικτύων

Τα δίκτυα υπολογιστών διαφέρουν ανάλογα με την έκταση την οποία καλύπτουν, το μέγιστο αριθμό χρηστών που μπορούν να εξυπηρετήσουν, καθώς και το είδος των υπηρεσιών που αυτά προσφέρουν. Οι δύο βασικότερες κατηγορίες δικτύων είναι τα LANs (Local Area Networks) και τα WANs (Wide Area Networks)[9].

- Ένα LAN καλύπτει μια σχετικά μικρή γεωγραφική περιοχή, η οποία μπορεί να είναι ένα σπίτι, ένα σχολείο, ένα γραφείο εργασίας, ένα κτήριο κ.λπ.
- Ένα WAN αποτελείται από την ένωση πολλών διαφορετικών LANs και επεκτείνεται σε μία γεωγραφικά ευρύτερη περιοχή, η οποία μπορεί να είναι μια επιχείρηση, ένα ίδρυμα ή ένας οργανισμός.

Μέχρι πριν μερικά χρόνια, η διασύνδεση ενός υπολογιστή σε ένα δίκτυο μπορούσε να επιτευχθεί μόνο ενσύρματα με τη χρήση καλωδίων. Ωστόσο, η καταιγιστική εξέλιξη της επιστήμης της τεχνολογίας κατόρθωσε να άρει και αυτόν τον περιορισμό, και σήμερα να καθίσταται δυνατή η ασύρματη πρόσβαση ενός υπολογιστή σε ένα δίκτυο, γεγονός στο οποίο έχει τις ρίζες της και η ραγδαία εξάπλωση των έξυπνων κινητών (smartphones), των tablets, καθώς και των υπολοίπων έξυπνων συσκευών. Με αυτόν τον τρόπο γεννιέται μια νέα κατηγορία δικτύων, τα WLANs (Wireless LANs)[10], τα οποία αν και κερδίζουν συνεχώς σε δημοσιότητα, κυρίως λόγω της πρακτικότητάς τους, υστερούν εντούτοις σημαντικά στον τομέα της ασφάλειας.

---

[9] Βλ. https://www.informatique-mania.com/el/linternet/quels-types-de-reseaux-informatiques-existent/

[10] Βλ. A Detailed Study on Wireless LAN Technologies - Vijay Chandramouli,. Department of Computer Science and Engineering, The University of Texas at Arlington, όπου πραγματοποιείται διεξοδικότερη ανάλυση των WLAN δικτύων.

2.3 Τι είναι το διαδίκτυο και πως λειτουργεί

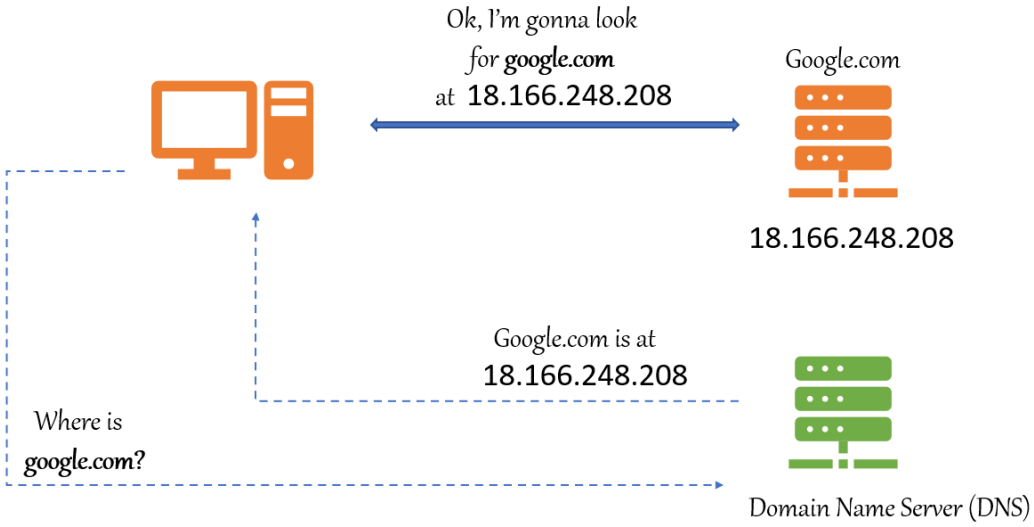
Η επικοινωνία δύο ή περισσοτέρων δικτύων μεταξύ τους, καθίσταται δυνατή μέσω ορισμένων συσκευών που ονομάζονται δρομολογητές (routers). Ο ρόλος των δρομολογητών είναι η σύνδεση των διαφορετικών δικτύων μεταξύ τους, αποτελώντας με αυτόν τον τρόπο, τη «δίοδο» για την επικοινωνία των υπολογιστών, ανεξαρτήτως χιλιομετρικών αποστάσεων και γεωγραφικών περιορισμών. Όλες οι συσκευές οι οποίες βρίσκονται συνδεδεμένες (ενσύρματα ή ασύρματα) στον ίδιο δρομολογητή, δημιουργούν ένα τοπικό δίκτυο (LAN ή WLAN), και στη συνέχεια μέσω του αυτού, αποκτούν πρόσβαση στα υπόλοιπα (εξωτερικά) δίκτυα με τα οποία αυτός είναι συνδεδεμένος. Η συνένωση των χιλιάδων διαφορετικών δικτυών (LANs, WANs ή WLANs) ολόκληρου του πλανήτη συγκροτεί ένα ενιαίο, παγκόσμιο, «κοινό» δίκτυο που ονομάζεται διαδίκτυο (internet – International Network).

Κάθε υπολογιστής, προκειμένου να μπορεί να αναγνωριστεί από τις υπόλοιπες συσκευές του δικτύου στο οποίο αυτός βρίσκεται, αποκτά μέσω του δρομολογητή (router) μία διεύθυνση IP, η οποία είναι μοναδική και λειτουργεί σαν ταυτότητα για την αναγνώριση της συσκευής αυτής. Η δομή της διεύθυνσης IP[11] αποτελείται από τέσσερις δεκαδικούς αριθμούς (από 0 έως 255) οι οποίοι διαχωρίζονται μεταξύ τους με τελείες. Όταν όμως ο ηλεκτρονικός υπολογιστής πρόκειται να συνδεθεί (μέσω του δρομολογητή) στο διαδίκτυο, τότε αποκτά μία διαφορετική (εξωτερική) διεύθυνση IP, η οποία είναι επίσης μοναδική και χρησιμοποιείται για τον εντοπισμό της συσκευής αυτής, κατά ανάλογο τρόπο που λειτουργεί και μία φυσική διεύθυνση.

Προκειμένου να μπορέσει κάποιος να περιηγηθεί στο διαδίκτυο, απαιτείται η χρήση κάποιου φυλλομετρητή ιστού (browser), ενώ για να αποκτήσει πρόσβαση σε έναν ιστότοπο, πρέπει να γνωρίζει τη μοναδική διεύθυνση IP του ιστοχώρου αυτού. Κάτι τέτοιο όμως πρακτικά θα ήταν ανέφικτο, διότι για κάθε ιστοχώρο που επιθυμεί κανείς να επισκεφτεί, θα έπρεπε να γνωρίζει τη μοναδική διεύθυνσή του. Η λύση στο πρόβλημα αυτό έχει δοθεί από μία υπηρεσία που ονομάζεται DNS (Domain Name System -

[11] Η αναφορά αφορά τις IPv4 διευθύνσεις. Το εύρος των διαθέσιμων IPv4 διευθύνσεων ανέρχεται σε 2^{32}, δηλαδή περίπου 4,3 δισεκατομμύρια διευθύνσεις. Παρόλα αυτά, εδώ και αρκετά χρόνια, λόγω του κορεσμού των διαθέσιμων IPv4 διευθύνσεων, για τη διαδικτυακή επικοινωνία χρησιμοποιείται η πιο πρόσφατη έκδοση του πρωτοκόλλου η οποία ονομάζεται IPv6. Η δομή αυτού του είδους των διευθύνσεων αποτελείται από 8 ομάδες των τεσσάρων δεκαεξαδικών ψηφίων, φτάνοντας έτσι τις 2^{128} (3.4×10^{38}) διαθέσιμες.

Σύστημα Ονοματοδοσίας Δικτύου). Σήμερα υπάρχουν εξυπηρετητές (servers), των οποίων η λειτουργία είναι η αντιστοίχιση των ονομάτων που πληκτρολογεί ο χρήστης (π.χ. www.google.com, ή www.amazon.com, κ.λπ.), σε διευθύνσεις IP (π.χ. 8.8.8.8 , 54.192.0.0), τις οποίες και χρησιμοποιεί στη συνέχεια ο υπολογιστής για τη σύνδεσή του, κατά ανάλογο τρόπο λειτουργίας ενός τηλεφωνικού καταλόγου. Αν η διεύθυνση που επιθυμεί να επισκεφτεί ο χρήστης υπάρχει καταχωρημένη στο DNS, τότε αποστέλλεται στον υπολογιστή, διαφορετικά παραπέμπει το χρήστη σε άλλο DNS[12].



Πηγή: https://geekflare.com/change-dns-server/

Κάθε πάροχος υπηρεσιών τηλεπικοινωνίας παρέχει ένα δικό του DNS, χωρίς όμως να αποκλείεται η δυνατότητα επιλογής ενός διαφορετικού. Ο αριθμός των διαφορετικών DNS που υπάρχουν είναι μεγάλος, με τις ταχύτητες ανταπόκρισής τους να αγγίζουν ακόμη και τα 10ms.

2.4 Τα μοντέλα διασύνδεσης

Τα δίκτυα υπολογιστών διακρίνονται σε δύο κατηγορίες όσον αφορά τη δομή και τους τρόπους διασύνδεσης μεταξύ τους.

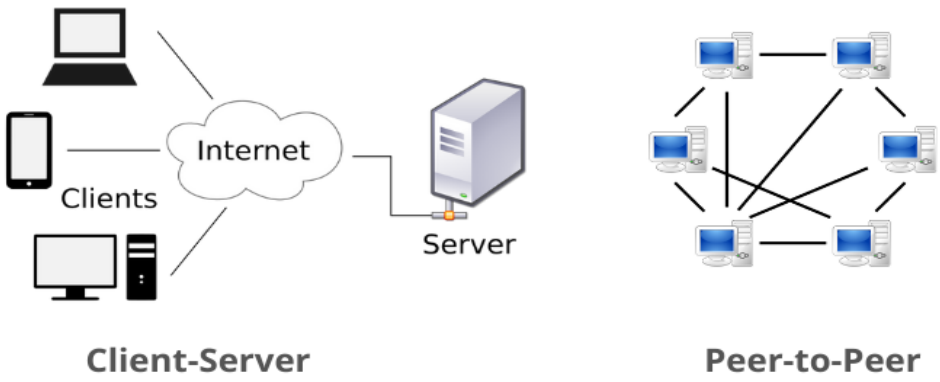
[12] Βλ. https://www.fortinet.com/resources/cyberglossary/what-is-dns για αναλυτικότερη περιγραφή του τρόπου λειτουργίας των DNS.

- Client-Server

Σε αυτήν την περίπτωση, ένας υπολογιστής αναλαμβάνει το ρόλο του διακομιστή, τη διαχείριση δηλαδή των πόρων εντός του δικτύου αυτού. Για παράδειγμα, ένας εξυπηρετητής μπορεί να χρησιμοποιηθεί για την αποθήκευση αρχείων, για την αποστολή και λήψη e-mail, για τη φιλοξενία μίας ιστοσελίδας, για τη διαχείριση εργασιών εκτύπωσης, για τον έλεγχο της πρόσβασης στο δίκτυο κ.α.[13] Προκειμένου να αποκτήσουν πρόσβαση όλοι οι υπόλοιποι υπολογιστές στα μέσα αυτά, υλοποιείται μία διαδικασία επικοινωνίας και αίτησης των πόρων αυτών από το διακομιστή. Η αδυναμία λειτουργίας ή πρόσβασης σε αυτόν, έχει ως συνέπεια τα παρεχόμενα από αυτόν δεδομένα να μην είναι προσβάσιμα από τους υπόλοιπους χρήστες.

- Peer-to-peer (p2p)

Στην περίπτωση ενός peer-to-peer μοντέλου διασύνδεσης, οι υπολογιστές που απαρτίζουν το δίκτυο μπορούν να λειτουργήσουν ταυτόχρονα τόσο ως πελάτες (clients), όσο και ως εξυπηρετητές (servers), λαμβάνοντας και παρέχοντας αντίστοιχα δεδομένα στους υπολοίπους δεδομένα[14]. Αποτελεί μία αποκεντρωτική μορφή δικτύωσης, με την οποία πραγματοποιείται πιο αποδοτική χρησιμοποίηση των πόρων λόγω του επιμερισμού αυτών, ενώ είναι λιγότερο τρωτό σε ευπάθειες και αδυναμίες που μπορεί να οφείλονται στη δυσλειτουργία ενός συστήματος (fault tolerance).



Πηγή: https://www.networkstraining.com/peer-to-peer-vs-client-server-network/

[13] Βλ. https://www.computerhope.com/jargon/s/server.htm για εκτενέστερη ανάλυση καθώς και παραδείγματα λειτουργίας ενός server

[14] Βλ. https://www.britannica.com/technology/P2P

2.5 Η ιστορική εξέλιξη του διαδικτύου

2.5.1 Το ARPANET : Ο πρόγονος του Διαδικτύου

Οι πρώτοι ηλεκτρονικοί υπολογιστές έκαναν την εμφάνισή τους κατά τον Β' Παγκόσμιο Πόλεμο και χρησιμοποιήθηκαν αρχικά για την εξυπηρέτηση στρατιωτικών σκοπών[15]. Αντιλαμβανόμενοι τα σημαντικά πλεονεκτήματα που αυτοί μπορούσαν να παρέχουν, κυρίως λόγω της μεγάλης ταχύτητας εκτέλεσης των ανατιθέμενων σε αυτούς εντολών, οι επιστήμονες επιδίωξαν από νωρίς τη δυνατότητα επικοινωνίας των υπολογιστών μεταξύ τους.

Η πρώτη ολοκληρωμένη μορφή δικτύου, ανακαλύφθηκε από τις ΗΠΑ το 1969, κατά τη διάρκεια του Ψυχρού Πολέμου, ονομάστηκε ARPANET και θεωρείται από πολλούς ως ο πρόγονος του σημερινού διαδικτύου. Η ονομασία αυτή οφείλεται στην Υπηρεσία Έρευνας Προηγμένων Προγραμμάτων (ARPA – Advanced Research Projects Agency) που ιδρύθηκε από τον Αϊζενχάουερ το 1958, με σκοπό την ανάπτυξη και εκμετάλλευση των ερευνητικών προγραμμάτων πέρα από το στρατιωτικό τομέα. Η σύσταση της εταιρείας ήταν η Αμερικανική απάντηση στην εκτόξευση του πυραύλου Σπούτνικ από τη Σοβιετική Ένωση ένα χρόνο νωρίτερα. Σε αντίθεση με την μέχρι τότε διαμορφωθείσα κατάσταση, το ARPANET βασίστηκε σε μία πρωτοποριακή για την εποχή τεχνική η οποία ονομάζεται μεταγωγή πακέτων (packet switching). Αυτή συνίσταται στην διαίρεση των δεδομένων σε μικρότερες μονάδες (πακέτα), τα οποία και στη συνέχεια αποστέλλονται στον παραλήπτη. Τα πλεονεκτήματα που παρουσιάζει η συγκεκριμένη τεχνική αφορούν στην βέλτιστη διαχείριση των κυκλωμάτων επικοινωνίας, ενώ παρέχεται επίσης η δυνατότητα αποστολής των πακέτων μέσω εναλλακτικών οδεύσεων, τόσο για αύξηση της ταχύτητας επικοινωνίας των κυκλωμάτων, όσο και την βελτίωση της αξιοπιστίας του δικτύου. Η εξέλιξη του ARPANET ήταν καθοριστική και ραγδαία, καταφέρνοντας μέχρι το τέλος της δεκαετίας του 80, το υπόψη δίκτυο να περιλαμβάνει περισσότερους από 30.000 ανταποκριτές[16].

---

[15] Βλ https://www.bbvaopenmind.com/en/articles/the-internet-global-evolution-and-challenges/ και https://www.internetsociety.org/internet/history-internet/brief-history-internet/ για την εξέλιξη του διαδικτύου

[16] https://www.livescience.com/internet

2.5.2 Το πρωτόκολλο επικοινωνίας TCP/IP

Το πρωτόκολλο επικοινωνίας TCP/IP (Transmission Control Protocol/Internet Protocol) αποτελεί τη βάση, πάνω στην οποία είναι δομημένο, κατά κύριο λόγο, το διαδίκτυο σήμερα. Αποτελεί σύνθεση διαφόρων επιμέρους πρωτοκόλλων, όμως οφείλει το όνομά του στα δύο σημαντικότερα εξ' αυτών, το TCP και το IP.

Το πρωτόκολλο διαδικτύου (IP) λειτουργεί κατά παρόμοιο τρόπο με την αποστολή ενός γράμματος. Προκειμένου να ξεκινήσει η επικοινωνία μεταξύ των συσκευών, πρέπει πρώτα να αναγνωρίσει η μία την άλλη. Οι διευθύνσεις IP είναι μοναδικές και χρησιμοποιούνται για τον ακριβή προσδιορισμό κάθε συσκευής που είναι συνδεδεμένη στο διαδίκτυο. Όπως αναφέρθηκε προηγουμένως, από την εποχή του ARPANET μέχρι και σήμερα, ο τρόπος επικοινωνίας των υπολογιστών επιτυγχάνεται μέσω της μεταγωγής πακέτων, μέσω δηλαδή του κατακερματισμού των δεδομένων που πρόκειται να αποσταλούν σε μικρότερα τεμάχια που ονομάζονται πακέτα. Σε κάθε πακέτο, προστίθενται δύο διευθύνσεις IP, του παραλήπτη και του αποστολέα, για να εξασφαλίσουν ότι το κάθε πακέτο θα φτάσει στον σωστό προορισμό.

Το πρωτόκολλο ελέγχου μετάδοσης (TCP)[17] χρησιμοποιείται παράλληλα με το πρωτόκολλο διαδικτύου, για τη μεταφορά των δεδομένων μεταξύ των χρηστών. Το TCP εγγυάται την αξιόπιστη διαβίβαση των πακέτων δεδομένων, περιλαμβάνοντας μηχανισμούς, οι οποίοι σε αρχικό στάδιο εξασφαλίζουν ότι έχει επιτευχθεί η ζεύξη μεταξύ των δύο ανταποκριτών, μέσω μιας διαδικασίας που ονομάζεται τριπλή χειραψία (three-way handshake). Στη συνέχεια και μόλις αυτή ολοκληρωθεί επιτυχώς, ξεκινάει ο αποστολέας τη μετάδοση των πακέτων, ακολουθώντας μία συγκεκριμένη αλληλουχία. Με αυτόν τον τρόπο, μόλις παραλαμβάνει το κάθε πακέτο, ο παραλήπτης γνωρίζει το επόμενο πακέτο που θα ακολουθήσει και ενημερώνει αντίστοιχα τον αποστολέα για επαναπροώθησή του σε περίπτωση που αυτό δεν παραληφθεί. Τέλος, μόλις ολοκληρωθεί η διαβίβαση του συνόλου των πακέτων, το πρωτόκολλο TCP τερματίζει τη σύνδεση και αυτά ταξινομούνται και επανασυντίθενται με τη σειρά που είχαν αποσταλεί.

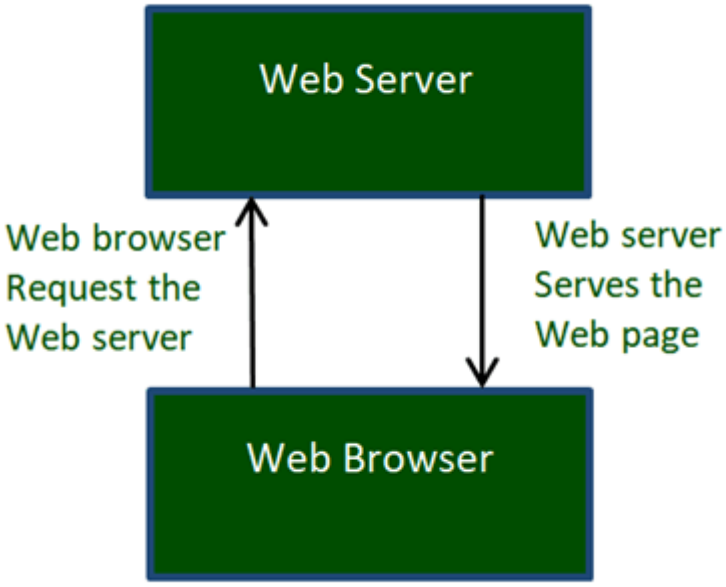
[17] Βλ. https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission-control-protocol--tcp

2.5.3 Από το ARPANET στον Παγκόσμιο Ιστό

Το 1989 ο βρετανός επιστήμονας του CERN Tim Berners-Lee, δημιούργησε τον Παγκόσμιο Ιστό (World Wide Web)[18] , γεγονός που αποτέλεσε κομβικό σημείο στη μέχρι σήμερα εξέλιξη του διαδικτύου. Η ανάγκη της επικοινωνίας και ανταλλαγής πληροφοριών μεταξύ των επιστημόνων του CERN, καθώς και όλου του πλανήτη, ήταν η αιτία που επέβαλε τη δημιουργία του Ιστού. Η ιδέα πίσω από τον Παγκόσμιο Ιστό, ήταν η δυνατότητα προβολής εγγράφων υπερκειμένων (hypertext) μέσω ενός φυλλομετρητή ιστού (browser), χρησιμοποιώντας 3 βασικές τεχνολογίες (HTML, URL και HTTP).

Το 1991, ο Tim Berners-Lee χρησιμοποιώντας τον υπολογιστή όπου πειραματιζόταν, δημιούργησε τον πρώτο web server (εξυπηρετητή), και την πρώτη ιστοσελίδα (info.cern.ch), η οποία παρείχε υπερσυνδέσμους για πληροφορίες σχετικά με το έργο αυτό. Αρχικά, ήταν δυνατή η πρόσβαση μόνο από ερευνητές του δικτύου του CERN, ωστόσο στα τέλη του ίδιου κιόλας έτους έγινε ευρέως προσβάσιμο από όλους.

Ο πρώτος εμπορικός Web server δημιουργήθηκε στις ΗΠΑ το Δεκέμβρη του 1991 και μέσα σε 2 χρόνια, περισσότεροι από 500 όμοιοι βρίσκονταν σε λειτουργία, αποτελώντας έτσι το 1% της ροής των δεδομένων στο διαδίκτυο.



Πηγή: https://www.javatpoint.com/what-is-world-wide-web

[18] https://www.javatpoint.com/what-is-world-wide-web

Η φιλοσοφία πίσω από τη δομή του Παγκόσμιου Ιστού είναι αρκετά απλή. Οποιοσδήποτε χρήστης που αναζητά πληροφορίες και δεδομένα, μπορεί να έχει πρόσβαση διά μέσω του υπολογιστή του και χρησιμοποιώντας ένα φυλλομετρητή ιστού, στις πληροφορίες που κάποιος άλλος χρήστης παρέχει μέσω του δικού του υπολογιστή ή εξυπηρετητή στο κοινό. Έτσι, όλες οι ιστοσελίδες «φιλοξενούνται» σε web servers, κατά ανάλογο τρόπο με ένα άτομο το οποίο μένει σε ένα διαμέρισμα.

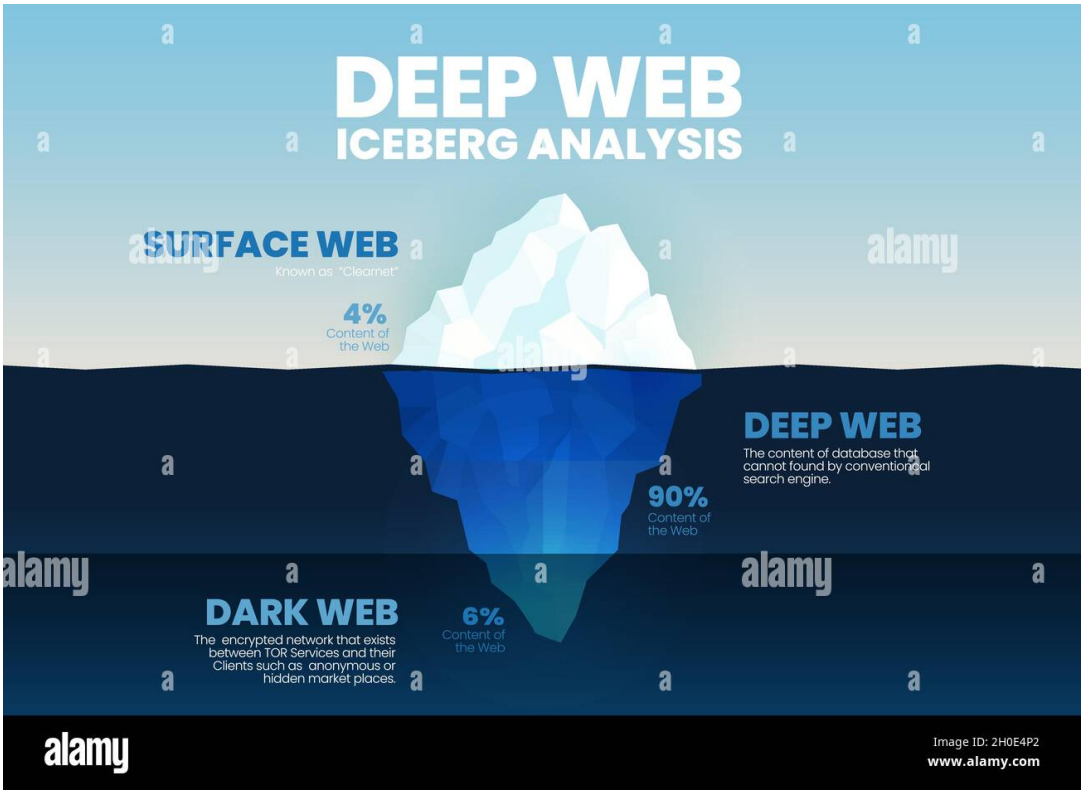
Η βασική γλώσσα προγραμματισμού που χρησιμοποιείται για τη δομή μιας ιστοσελίδας είναι η HTML (Hyper Text Markup Language), ενώ για τη διαβίβασή της μέσω του διαδικτύου χρησιμοποιείται το πρωτόκολλο HTTP (Hyper Text Transfer Protocol). Σήμερα το πρωτόκολλο http έχει αντικατασταθεί σχεδόν εξ΄ ολοκλήρου από το https (secure) το οποίο, σε αντίθεση με τον προκάτοχό του, παρέχει κρυπτογράφηση και κατ' επέκταση εγγυάται μεγαλύτερη ασφάλεια των δεδομένων κατά τη μεταφορά τους.

Για να έχουμε πρόσβαση σε μία ιστοσελίδα ή ένα αρχείο στο διαδίκτυο, είναι απαραίτητη η γνώση του URL (Uniform Resource Locator)[19]. Το URL είναι μοναδικό, αποτελεί τη διεύθυνση του αρχείου στο διαδίκτυο και απαρτίζεται από 3 μέρη. Το πρώτο συμβολίζει το πρωτόκολλο που χρησιμοποιείται για την πρόσβαση στο μέσο (π.χ. https), το δεύτερο τον κόμβο στον οποίο είναι τοποθετημένο το μέσο (π.χ.www.google.gr) και το τρίτο τη θέση και το όνομα του αρχείου στον εξυπηρετητή.

2.6 Οι κατηγορίες του Παγκόσμιου Ιστού (World Wide Web)

Το περιβάλλον του Παγκόσμιου Ιστού δεν αποτελεί έναν ενιαίο, μεμονωμένο χώρο όπου μπορούν να αλληλοεπιδρούν όλοι οι χρήστες. Αντιθέτως, υπάρχουν διαβαθμίσεις ανάλογα με το ποιες πληροφορίες και με ποιο τρόπο αυτές είναι προσβάσιμες στο κάθε χρήστη, κατ' ανάλογο τρόπο όπως ένα παγόβουνο δεν είναι πλήρως ορατό από κάποιον που βρίσκεται στην επιφάνεια της θάλασσας. Οι 3 βασικές κατηγορίες του Παγκόσμιου Ιστού είναι ο επιφανειακός, ο βαθύς και ο σκοτεινός ιστός.

[19] Βλ. http://www.eeei.gr/odhgos/netsc404/whaturl.htm για το URL και τα είδη



Πηγή: https://www.alamy.com/blue-vector-presentation-iceberg-deep-web-concept-is-3-elements-analyze-4-is-the-clearest-surface-web-90-is-deep-web-cannot-search-and-dark-web-is-image447780650.html

2.6.1 Ο Επιφανειακός Ιστός (Surface Web)

Ο επιφανειακός ιστός είναι το μέρος του διαδικτύου το οποίο είναι ελεύθερα προσβάσιμο από το σύνολο των χρηστών του διαδικτύου και θα μπορούσε να παρομοιαστεί με το τμήμα εκείνο του παγόβουνου, το οποίο είναι ορατό από την επιφάνεια της θάλασσας. Παρόλο που σε αυτόν ανήκουν οι πιο γνωστές ιστοσελίδες που χρησιμοποιούνται για την ενημέρωση, την επικοινωνία, τη διασκέδαση, την ψυχαγωγία, καθώς το σύνολο των σελίδων που μπορεί να επισκεφτεί κανείς μέσω των διαφόρων μηχανών αναζήτησης (google, bing, yahoo κ.λπ.), εντούτοις αποτελεί μόλις το 4% του συνολικού διαδικτύου.

2.6.2 Ο Βαθύς Ιστός (Deep Web)

Ο βαθύς ιστός συνιστά περίπου το 90% του συνόλου των διαδικτυακών ιστοτόπων και είναι το κομμάτι εκείνο του Παγκόσμιου Ιστού, το οποίο δεν καθίσταται προσβάσιμο μέσω των μηχανών αναζήτησης. Μπορεί να παραλληλιστεί με το μεγαλύτερο τμήμα του παγόβουνου που βρίσκεται κάτω από την επιφάνεια του νερού. Σε αυτόν περιέχονται βάσεις δεδομένων ιατρικών, επιστημονικών και οικονομικών αρχείων, καθώς και ιδιωτικά στοιχεία, όπως λογαριασμοί e-mail, προφίλ μέσων κοινωνικής δικτύωσης κ.λπ. Στο βαθύ ιστό ανήκουν επίσης και όλα τα διαχειριστικά περιβάλλοντα όλων των ιστοσελίδων[20], τα δεδομένα που βρίσκονται αποθηκευμένα στο υπολογιστικό νέφος (cloud), αλλά και παράνομο περιεχόμενο. Αν και το deep web είναι προσβάσιμο από τους κοινούς περιηγητές ιστών μέσω των διευθύνσεων IP ή των URL των ιστοτόπων, συνήθως απαιτείται είσοδος με τη μορφή διαπιστευτηρίων (όνομα και κωδικός χρήστη) για την προσπέλαση στα δεδομένα αυτά[21].

2.6.3 Ο Σκοτεινός Ιστός (Dark Web)

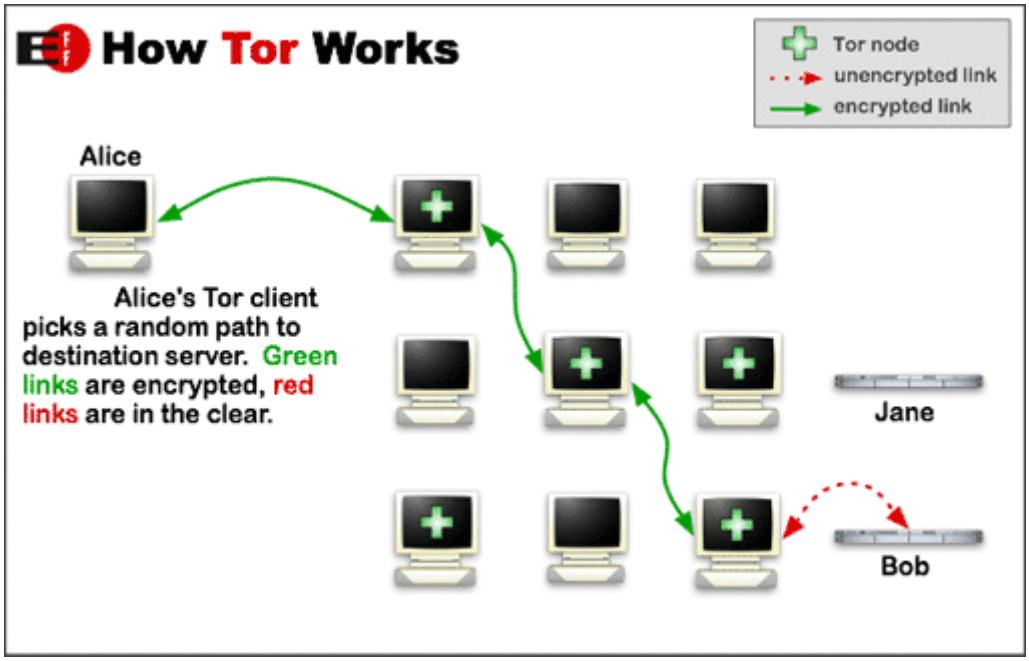
Ο σκοτεινός ιστός παρομοιάζεται με το τελικό και βαθύτερο τμήμα του παγόβουνου, καλύπτει σχεδόν το 6% των συνολικών ιστοτόπων, ενώ είναι συχνά συνυφασμένος με παράνομο περιεχόμενο και δραστηριότητες. Επειδή η πλειοψηφία του περιεχομένου του dark web είναι κρυπτογραφημένη, η πρόσβαση σε αυτό μπορεί να γίνει αποκλειστικά μέσω ειδικών φυλλομετρητών ιστού που καθιστούν ανώνυμη την περιήγηση, με τον γνωστότερο από τους οποίους να είναι ο tor (The Onion Routing). Οι ιστοσελίδες που φιλοξενούνται στο σκοτεινό ιστό έχουν την κατάληξη .onion σε αντίθεση με τις συνηθισμένες .com, .edu, και .gr που συναντά κανείς στο surface και στο deep web.

Ο φυλλομετρητής tor δημιουργήθηκε στα μέσα της δεκαετίας του 90 από το αμερικανικό ναυτικό, προκειμένου να διασφαλίζεται η ασφαλής και προστατευμένη επικοινωνίας του προσωπικού. του Ο τρόπος λειτουργίας του είναι να κρυπτογραφεί τα δεδομένα πριν αυτά αποσταλούν στο διαδίκτυο. Σε αντίθεση με τα συνηθισμένα

[20] Βλ. https://www.lab.com.gr/deep-web-%CE%BA%CE%B1%CE%B9-dark-web-%CF%84%CE%BF-%CE%AC%CE%B3%CE%BD%CF%89%CF%83%CF%84%CE%BF-internet/

[21] https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different

προγράμματα περιήγησης ιστού, τα οποία επιλέγουν το πιο σύντομο (από χρονικής άποψης) δρόμο για την αποστολή των δεδομένων, ο tor χρησιμοποιεί μία τυχαία διαδρομή κρυπτογραφημένων διακομιστών, που ονομάζονται κόμβοι[22]. Ο κάθε ενδιάμεσος κόμβος στον οποίο αυτά περιέρχονται, μπορεί να αποκρυπτογραφήσει μόνο το τμήμα εκείνο των δεδομένων, που περιέχει πληροφορίες σχετικά με τον επόμενο κόμβο στον οποίο αυτά πρόκειται να διαβιβαστούν, και σε καμία περίπτωση το σύνολο αυτών. Με αυτόν τον τρόπο αποφεύγεται να γίνει ορατή η τοποθεσία και η δραστηριότητα που διεξάγει ένας χρήστης στο διαδίκτυο. Η διαμόρφωση αυτή της κρυπτογράφησης σε πολυάριθμα και ξεχωριστά στρώματα, μπορεί να συγκριθεί με τη δομή ενός κρεμμυδιού, στο οποίο οφείλει και το όνομά του.



Πηγή: https://el.wikipedia.org/wiki/Tor

Η αδυναμία εντοπισμού των χρηστών, έχει ανάγει το σκοτεινό ιστό σε ιδανικό περιβάλλον δράσης για παράνομες δραστηριότητες, όπως την αγοροπωλησία ναρκωτικών ουσιών, όπλων, σπάνιων έργων τέχνης, σχεδίων διάσημων κτηρίων, τη διάθεση υλικού παιδικής πορνογραφίας ή και γυμνών φωτογραφιών διάσημων προσώπων. Οι πληρωμές γίνονται συνήθως μέσω κρυπτονομισμάτων (bitcoins) τα οποία δεν παρέχουν τη δυνατότητα ανίχνευσης. Παράλληλα, οι κίνδυνοι μόλυνσης από

[22] Βλ. https://www.youtube.com/watch?v=xHeOUd4E9As&ab_channel=SecNewsTV για τη διάκριση surface, deep και dark web και τους κινδύνους που ελλοχεύονται και https://www.the-sun.com/lifestyle/tech-old/271948/what-dark-web-how-work/

κακόβουλο λογισμικό ή να πέσει κανείς θύμα απάτης, αυξάνονται κατακόρυφα σε περιβάλλον του σκοτεινού ιστού. Ωστόσο, είναι βασικό να κατανοήσει κανείς ότι τόσο η απλή πρόσβαση στο dark web, όσο και η χρήση των υπηρεσιών tor αυτές καθαυτές, δεν μπορούν σε καμία περίπτωση να θεωρηθούν ως παράνομες και να ποινικοποιηθούν αν δεν συνοδεύονται από περαιτέρω αξιόποινες ενέργειες.

2.7 Το Διαδίκτυο των Πραγμάτων (Internet of Things)

Ο όρος διαδίκτυο των πραγμάτων [Internet of Things (IoT)] χρησιμοποιήθηκε πρώτη φορά το μακρινό 1999, από τον Άγγλο επιστήμονα Kevin Ashton, ο οποίος οραματιζόταν ένα περιβάλλον, όπου οι διάφορες ηλεκτρικές συσκευές θα μπορούν να επικοινωνούν μεταξύ τους και να ελέγχονται μέσω του διαδικτύου[23]. Το γεγονός αυτό, μπορεί τότε να ανήκε αποκλειστικά στη σφαίρα της επιστημονικής φαντασίας, ωστόσο, εδώ και μερικά χρόνια η μετουσίωσή του προχωράει με γοργούς ρυθμούς.

Με τον όρο διαδίκτυο των πραγμάτων, σήμερα αναφερόμαστε στο σύνολο των ηλεκτρονικών συσκευών με δυνατότητα σύνδεσης στο Διαδίκτυο[24]. Το έναυσμα για τη συγκεκριμένη ιδέα δόθηκε από την χρησιμοποίηση της RFID (Radio Frequency Identification) τεχνολογίας από ανεφοδιαστικές αλυσίδες για τον εντοπισμό των αγαθών, χωρίς την απαίτηση της ανθρώπινης παρέμβασης. Κατά ανάλογο τρόπο, θα μπορούσε να γίνει χρήση του IP πρωτοκόλλου ούτως ώστε να είναι σε θέση οι ηλεκτρονικές («έξυπνες») συσκευές να συνδεθούν στο διαδίκτυο.

Η φιλοσοφία πίσω από τη γενική ιδέα του Διαδικτύου των πραγμάτων, είναι η πρόσβαση και ο απομακρυσμένος έλεγχος της οποιαδήποτε ηλεκτρονικής συσκευής, από τον κάθε χρήστη, οποιαδήποτε χρονική στιγμή και από οποιοδήποτε μέρος αυτός επιθυμεί.[25] Για το σκοπό αυτό, υπήρξε απαραίτητη η υιοθέτηση ενός αριθμού κοινών πρωτοκόλλων επικοινωνίας μεταξύ των συσκευών, τα οποία και εξελίσσονται διαρκώς.

[23] Βλ. The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World, Vivek Singhania, Internet Society, October 2015

[24] Βλ. Κάτος Β., Ψηφιακά Πειστήρια, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

[25] Internet of Things Applications, Challenges and Related Future Technologies, World Scientific News 67(2) (2017) 126-148

Η πρώτη IoT συσκευή παρουσιάστηκε το 1990 από τον John Romkey και ήταν μία τοστιέρα[26], η οποία μπορούσε να συνδεθεί με έναν υπολογιστή, μέσω του πρωτοκόλλου TCP/IP. Ακολούθησαν κι άλλες ηλεκτρικές συσκευές, όπως φορητές κάμερες και ψυγεία με δυνατότητα διασύνδεσης στο διαδίκτυο, για να φτάσουμε στον 21ο αιώνα και την σχεδόν καθολική εφαρμογή του Internet Of Things στα αντικείμενα της καθημερινότητάς μας. Μέχρι το 2025 μάλιστα, οι ειδικοί εκτιμούν ότι ο συνολικός αριθμός των IoT συσκευών θα έχει ξεπεράσει τα 75 δισεκατομμύρια[27].

Εκτός από τον τομέα της διασκέδασης, το Διαδίκτυο των Πραγμάτων, έχει επεκταθεί σε πολυάριθμες ακόμα πτυχές της καθημερινότητάς μας, όπως η υγεία, οι μετακινήσεις, η ασφάλεια, η ενέργεια, οι κτηριακές υποδομές κ.λπ.

[26] Βλ. https://hqsoftwarelab.com/blog/the-history-of-iot-a-comprehensive-timeline-of-major-events- infographic/

[27] https://www.nccoe.nist.gov/iot

3 Το διαδίκτυο ως μέσο τέλεσης εγκλημάτων

Η ολοκληρωτική εγκαθίδρυση της επιστήμης της τεχνολογίας και πληροφορικής στην καθημερινή μας ζωή, αφενός μεν έχει συνεισφέρει στην αυτοματοποίηση πολλών διαδικασιών της καθημερινότητάς μας, αφετέρου δε έχει συμβάλλει στην εμφάνιση νέων μορφών κοινωνικών συμπεριφορών σε όλους τους τομείς της κοινωνικής ζωής[28]. Ολοένα και μεγαλύτερο μέρος της κοινωνικής μας δραστηριότητας διεξάγεται πλέον στο διαδίκτυο[29], με τομείς όπως η επικοινωνία και η εργασία να αποτελούν χαρακτηριστικά παραδείγματα. Παράλληλα, αξιοσημείωτη είναι και η συνεισφορά της τεχνολογίας στην επιστήμη της υγείας, βελτιώνοντας καθοριστικά τις παρεχόμενες υγειονομικές υπηρεσίες και παρέχοντας νέες δυνατότητες, οι οποίες μέχρι πρότινος φάνταζαν αδύνατες. Παράλληλα, και σε άλλους τομείς της καθημερινής ζωής όπως οι μεταφορές, η έρευνα, το περιβάλλον, η διασκέδαση κ.λπ. έχει γίνει αισθητή η διείσδυση της τεχνολογίας και μάλιστα σε τόσο ουσιώδη βαθμό, ώστε να μπορούμε να πούμε, ότι τον 21ο αιώνα η τεχνολογική πρόοδος ενός κράτους είναι σε θέση να αποτελεί καθρέφτη της ισχύος και της «κατάταξής» του στην παγκόσμια κλίμακα.

Παράλληλα όμως με τη εδραίωση της τεχνολογίας σε όλους τους παραπάνω κλάδους της κοινωνικής ζωής, έχουν εκδηλωθεί αξιόποινες συμπεριφορές οι οποίες προσβάλλουν την έννομη τάξη και τα προστατευόμενα από το Δίκαιο ατομικά, αλλά και υπερατομικά αγαθά.

Διερευνώντας τον αντίκτυπο που έχει επιφέρει η νέα αυτή μορφή κοινωνικής πραγματικότητας από τη σκοπιά του νομοθέτη, διαπιστώνουμε ότι ο τελευταίος βρίσκεται αντιμέτωπος με μία ισχυρή πρόκληση, όχι μόνο επειδή καλείται να αντιστοιχίσει (στο βαθμό που αυτό είναι δυνατό) τις νέες αξιόποινες κοινωνικές συμπεριφορές με τις ήδη υπάρχουσες του «φυσικού» κόσμου, αλλά και επειδή, πολλές φορές (εξαιτίας κυρίως της πρωτοτυπίας τους), η παραπάνω αντιστοίχιση καθίσταται αδύνατη.

Η νομική επιστήμη και κατ' επέκταση το Δίκαιο του κάθε κράτους, είναι δομημένα πάνω στην απτή πραγματικότητα της καθημερινότητας και του φυσικού κόσμου. Η σταδιακή μεταφορά των κοινωνικών πτυχών στο ηλεκτρονικό περιβάλλον, σε

[28] Βλ. Αγγελής Ι., Διαδίκτυο και Ποινικό Δίκαιο, ΠοινΧρ Ν/2000

[29] Βλ. Κιούπης Δ., Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

συνδυασμό με την τέλεση παλαιών και νέων μορφών ποινικών αδικημάτων, τόνισαν την επιτακτική ανάγκη για προσαρμογή της Ευρωπαϊκής και Ελληνικής νομοθεσίας στη νέα αυτή πραγματικότητα, με την τροποποίηση των υπαρχουσών διατάξεων ή και τη θέσπιση νέων όπου και όποτε αυτό κρίνεται απαραίτητο. Η μεν παγκοσμιότητα των δεδομένων που παρέχεται με τις υπηρεσίες του διαδικτύου, διαφοροποιεί το ηλεκτρονικό έγκλημα ως μία ιδιότυπη μορφή ποινικού αδικήματος, επιβάλλει δε, την διασυνοριακή συνεργασία των δικαστικών αλλά και αστυνομικών αρχών για την αποτελεσματική αντιμετώπισή του, μέσα από τη θέσπιση ενός διακρατικού ποινικού πλαισίου[30].

3.1 Από τι αποτελείται ένας Ηλεκτρονικός Υπολογιστής και πως αυτός λειτουργεί

Από τη γένεσή τους, τα υπολογιστικά συστήματα αποτελούνται από δύο κύρια μέρη, το υλικό και το λογισμικό, τα οποία αν και ανεξάρτητα, αλληλοεπιδρούν μεταξύ τους προκειμένου να καταστεί δυνατή η εύρυθμη λειτουργία του υπολογιστή.

Το υλικό (hardware) περιλαμβάνει όλα τα φυσικά-μηχανικά μέρη του υπολογιστή που έχουν δηλαδή υλική υπόσταση, τα οποία μπορεί δηλαδή κανείς να δει και αγγίξει. Το υλικό διακρίνεται στην Κεντρική Μονάδα (CPU – Central Processing Unit), τις περιφερειακές συσκευές (πληκτρολόγιο, ποντίκι, οθόνη κ.λπ.) και τα αποθηκευτικά μέσα (μνήμη RAM, σκληρός δίσκος, μνήμη ROM).

Το λογισμικό (software) απεναντίας, χαρακτηρίζεται ως το σύνολο των προγραμμάτων, των διαδικασιών και των οδηγιών που καθορίζουν στο υλικό τις ενέργειες που αυτό πρέπει να κάνει, καθώς και τον τρόπο με τον οποίο αυτές πρέπει να γίνουν[31]. Δεν έχει υλική υπόσταση και δεν είναι ορατό ή αντιληπτό από τον άνθρωπο ενώ χωρίς αυτό, το υλικό δεν θα ήταν σε θέση να λειτουργήσει και να παράγει τα επιδιωκόμενα αποτελέσματά του.

Η βάση ενός προγράμματος ηλεκτρονικού υπολογιστή ονομάζεται αλγόριθμος και ορίζεται ως μία σειρά αυστηρά καθορισμένων ενεργειών (εντολών) και εκτελέσιμων

[30] Βλ. Δαλακούρας Θ., Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

[31] https://edu.gcfglobal.org/en/computer-science/hardware-and-software/1/#

σε συγκεκριμένο χρόνο, με τις οποίες επιδιώκεται η λύση ενός προβλήματος[32]. Για την επικοινωνία μεταξύ τους, οι ηλεκτρονικοί υπολογιστές χρησιμοποιούν το δυαδικό σύστημα, δηλαδή μία αλληλουχία των αριθμών 0 και 1. Συνεπώς, ο κάθε αλγόριθμος θα πρέπει να μεταφραστεί σε μία ακολουθία του δυαδικού συστήματος. Επειδή κάτι τέτοιο όμως θα ήταν εξαιρετικά δύσχρηστο και πρακτικά αδύνατο, χρησιμοποιούνται ορισμένα «βοηθήματα» που ονομάζονται γλώσσες προγραμματισμού και με τα οποία μπορεί ο χρήστης να ορίζει τις εντολές που επιθυμεί να εκτελέσει ο υπολογιστής[33]. Σήμερα υπάρχουν εκατοντάδες γλώσσες προγραμματισμού μερικές από τις οποίες είναι η Python, η C++, η C, η HTML, η JAVA κλπ.

Το κείμενο, δηλαδή η ακολουθία των εντολών που δίνεται από τον προγραμματιστή μέσω μίας γλώσσας προγραμματισμού, ονομάζεται πηγαίο πρόγραμμα (source code) ή πηγαίος κώδικας[34]. Το πηγαίο πρόγραμμα μπορεί να τροποποιηθεί από το χρήστη μέσω ενός διορθωτή κειμένου (editor) και είναι γραμμένο σε γλώσσα προγραμματισμού υψηλού επιπέδου, η οποία όμως δεν είναι απευθείας κατανοητή από τον ηλεκτρονικό υπολογιστή. Προκειμένου να επιτευχθεί αυτό, πρέπει το πηγαίο πρόγραμμα να μεταφραστεί σε αντικειμενικό πρόγραμμα (object code), δηλαδή σε γλώσσα μηχανής με τη βοήθεια ενός προγράμματος μεταγλώττισης (compiler). Ο compiler ελέγχει επίσης τυχόν ορθογραφικά ή συντακτικά λάθη του πηγαίου προγράμματος, προκειμένου να εξασφαλιστεί με τον τρόπο αυτό η απρόσκοπτη λειτουργία και εκτέλεση του αντικειμενικού προγράμματος από τον υπολογιστή.

3.2 Τι είναι το ηλεκτρονικό έγκλημα

Ο πρώτος ορισμός του ηλεκτρονικού εγκλήματος δόθηκε το 1994 από τους Forester και Morrison, οι οποίοι το περιέγραψαν ως «μία εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο». Κατά καιρούς, έχουν γίνει διάφορες διατυπώσεις, χωρίς ωστόσο να υπάρχει ένας κοινά αποδεκτός ορισμός του ηλεκτρονικού εγκλήματος μέχρι σήμερα. Ως ηλεκτρονικό έγκλημα, θα

[32]https://el.wikipedia.org/wiki/%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CF%82

[33] https://stigma.host/programming-languages/

[34] http://karakos.gr/apospasma.pdf

μπορούσαν να οριστούν οι κακόβουλες πράξεις, που έχουν σαν σκοπό να πλήξουν τα συστήματα πληροφοριών, δηλαδή έναν ηλεκτρονικό υπολογιστή, τα προγράμματά του ή και τα δίκτυα επικοινωνίας του με άλλους υπολογιστές[35]. Επίσης, μπορεί να περιγραφεί και ως τις αξιόποινες πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών καθώς και άλλων συστημάτων επεξεργασίας δεδομένων.[36]

Η έννοια του ηλεκτρονικού εγκλήματος (e-crime) δεν πρέπει να συγχέεται με εκείνη του δικτυακού ή κυβερνοεγκλήματος (cybercrime), καθώς η δεύτερη αποτελεί μία υποκατηγορία της πρώτης που προϋποθέτει ως απαραίτητο όρο το στοιχείο της δικτύωσης [37]. Με άλλα λόγια, ο ηλεκτρονικός υπολογιστής ή συσκευή (π.χ. smartphone, tablet κλπ.) που χρησιμοποιείται ως μέσο της προσβολής ή κατά τη διάπραξη αυτής, πρέπει προηγουμένως να βρίσκεται διασυνδεδεμένος σε κάποιο τοπικό δίκτυο ή στο διαδίκτυο.

Το διαφορετικό περιβάλλον τέλεσης δεν αποτελεί το μοναδικό στοιχείο που διαφοροποιεί το ηλεκτρονικό από το «κοινό» έγκλημα. Γενικότερα και στην πλειοψηφία τους, οι διάφορες εκφάνσεις του ηλεκτρονικού εγκλήματος μπορούν να καταταχθούν στις εξής τρεις κατηγορίες[38]:

Α) Σε εκείνα που τελούνται τόσο στο «φυσικό» κόσμο, όσο και στο περιβάλλον του διαδικτύου. Μερικά από αυτά είναι η απάτη, η εξύβριση, η συκοφαντική δυσφήμιση, ο εκφοβισμός κ.λπ.

Β) Σε εκείνα που τελούνται αποκλειστικά σε ηλεκτρονικό περιβάλλον, χωρίς ωστόσο ο ηλεκτρονικός υπολογιστής να έχει αποκτήσει πρόσβαση στο διαδίκτυο. Ο εγκληματίας στην περίπτωση αυτή ενεργεί αυτοτελώς και το έγκλημα που διαπράττεται χαρακτηρίζεται ως έγκλημα με ηλεκτρονικό υπολογιστή (computer crime). Ορισμένα χαρακτηριστικά παραδείγματα αποτελούν η παράνομη πρόσβαση σε σύστημα πληροφοριών ή δεδομένα (370Β ΠΚ), καθώς και η παράνομη πρόσβαση και διάθεση περιεχομένου απορρήτων προγραμμάτων (370Γ ΠΚ).

---

[35] Βλ. Νούσκαλης Γ., Απάτη με ΗΥ – Παρελθόν και Μέλλον του άρθρου 386Α ΠΚ υπό το πρίσμα των εξελίξεων στην ΕΕ, ΠοινΔικ 2/2003.

[36] Βλ. Κάτος Β., Ψηφιακά Πειστήρια, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

[37] Βλ. Δαλακούρας Θ., Έννοια, διακρίσεις και χαρακτηριστικά των εγκλημάτων στον κυβερνοχώρο, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

[38] Βλ. Αγγελής Ι., Διαδίκτυο (Internet) και ποινικό δίκαιο, ΠοινΧρ Ν/2000.

Γ) Σε εκείνα που τελούνται αποκλειστικά σε διαδικτυακό περιβάλλον. Τα τελευταία αποτελούν τα λεγόμενα «γνήσια εγκλήματα κυβερνοχώρου» (cybercrimes).

3.3 Τα χαρακτηριστικά του ηλεκτρονικού εγκλήματος

Παρόλο που το ηλεκτρονικό έγκλημα μοιράζεται αρκετά κοινά χαρακτηριστικά με το «συμβατικό» έγκλημα, εντούτοις υπάρχουν ορισμένα στοιχεία του που το αναγορεύουν ως μια ιδιότυπη μορφή αυτού. Ειδικότερα:

- Το διαφορετικό περιβάλλον τέλεσης

Το ηλεκτρονικό έγκλημα, είτε αυτό τελείται σε περιβάλλον κυβερνοχώρου είτε όχι, αποτελεί μία παντελώς διαφορετική εκδοχή παραβατικότητας, η οποία ήταν άγνωστη στην ανθρωπότητα μέχρι πριν μερικές δεκαετίες. Η ελλιπής ενημέρωση των χρηστών για τον τρόπο λειτουργίας των ηλεκτρονικών υπολογιστών και του διαδικτύου, η άγνοια των κινδύνων που ελλοχεύουν στο περιβάλλον του Παγκόσμιου Ιστού, η αλματώδης τεχνολογική πρόοδος που σημειώνει καθημερινά η επιστήμη των υπολογιστών καθιστώντας πρακτικά σχεδόν ακατόρθωτη τη διατήρηση ενός ικανοποιητικού γνωστικού επιπέδου, η ραγδαία εξάπλωση των προϊόντων τεχνολογίας στις μικρές ηλικίες και η δυνατότητα εκμηδενισμού των αποστάσεων που παρέχει η τεχνολογία, αποτελούν μερικά μόνο από τα αίτια που έχουν συμβάλλει καθοριστικά στην έξαρση των ηλεκτρονικών εγκλημάτων σήμερα. Η ευμεταβλητότητα που χαρακτηρίζει τον τεχνολογικό τομέα, ως απόρροια της διαρκούς τάσης για εξέλιξη, έθετε και εξακολουθεί να θέτει μία σημαντική πρόκληση για την έννομη τάξη και τις αρχές, οι οποίες καλούνταν να αντιμετωπίσουν αξιόποινες συμπεριφορές πρωτόγνωρες για τα μέχρι σήμερα γνωστά δεδομένα τους. Παρόλο που σε ορισμένα εγκλήματα η νομική βάση μπορεί να παρέμενε η ίδια, το στοιχείο του διαφορετικού περιβάλλοντος τέλεσης ήταν αυτό που επέβαλλε τη θέσπιση νέων ποινικών διατάξεων.

- Η απαίτηση εξειδικευμένων τεχνικών γνώσεων για την τέλεσή του

Η διάπραξη ενός ηλεκτρονικού εγκλήματος πολλές φορές προαπαιτεί ο δράστης να κατέχει ειδικές γνώσεις σχετικά με την επιστήμη και τον τρόπο λειτουργίας των ηλεκτρονικών υπολογιστών. Οι γνώσεις αυτές μπορεί να αφορούν τόσο στη δομή και λειτουργία, όσο και στον τρόπο επικοινωνίας των ηλεκτρονικών υπολογιστών, προκειμένου να είναι σε θέση ο δράστης να εκμεταλλευτεί τυχόν κενά ασφαλείας τα

οποία υπάρχουν ή μπορεί να προκύψουν. Αυτό έχει ως αποτέλεσμα να τίθεται ένας σημαντικός περιορισμός στον αριθμό και στην ταυτότητα των εγκληματιών, σε αντίθεση με τις περισσότερες «κλασικές» μορφές εγκλημάτων, όπου η πλειοψηφία του πληθυσμού είναι σε θέση να πληροί την αντικειμενική υπόσταση αυτών. Παράλληλα, το ηλεκτρονικό έγκλημα κατά κύριο λόγο, χαρακτηρίζεται από το στοιχείο της πρόθεσης και σκοπιμότητας, αφού ο δράστης δεν μπορεί να ισχυριστεί ότι ενήργησε παρορμητικά ή «από ανάγκη».

- Τα ίχνη του εντοπίζονται δυσκολότερα (Μεγαλύτερη Ανωνυμία)

Κατά αναλογία με τα φυσικά εγκλήματα, κάθε πράξη που γίνεται σε ηλεκτρονικό περιβάλλον, αφήνει αντίστοιχα τα δικά της «δακτυλικά αποτυπώματα». Κάθε μορφής δραστηριότητα που εκτελεί κάποιος στο διαδίκτυο αφήνει ίχνη, δεδομένα δηλαδή σε ηλεκτρονική μορφή. Ο ισχυρισμός ότι το διαδίκτυο εγγυάται πλήρη ανωνυμία και η δραστηριότητα που εκτελεί κάποιος στο περιβάλλον αυτό δεν δύναται να εντοπισθεί, είναι απολύτως αναληθής. Πολλές φορές μάλιστα, οι ενέργειες ενός ατόμου στο φυσικό κόσμο, μπορεί να αφήνουν ίχνη και στον κυβερνοχώρο, όπως π.χ. γίνεται με το στίγμα που λαμβάνεται από τη θέση ενός κινητού τηλεφώνου. Ιδιαίτερα σε περίπτωση σχηματισμού ποινικής δικογραφίας, το κέντρο βάρους της δικονομικής διαδικασίας μεταφέρεται στη συλλογή των ψηφιακών πειστηρίων. Ως ψηφιακά πειστήρια ορίζονται τα δεδομένα που εντοπίζονται, συλλέγονται, αναλύονται και ερμηνεύονται, έπειτα από μία επιστημονικά αποδεκτή διαδικασία, προκειμένου να λειτουργήσουν ως αποδεικτικά μέσα στην ποινική διαδικασία[39]. Η συλλογή των ψηφιακών πειστηρίων μπορεί πολλές φορές βέβαια να συνεπάγεται μία εξαιρετικά απαιτητική, από άποψη χρόνου και κόστους, διαδικασία, ενώ για τα δεδομένα τα οποία αποκτώνται, πρέπει να έχει διασφαλιστεί η ακεραιότητά τους προκειμένου να μπορούν να χρησιμοποιηθούν. Δεν είναι λίγες οι φορές κατά τις οποίες οι δράστες, με πρόθεση να εξαφανίσουν τυχόν ενοχοποιητικά γι' αυτούς στοιχεία, προβαίνουν σε συνειδητή απόπειρα καταστροφής των δεδομένων, δυσχεραίνοντας με τον τρόπο αυτό, την περαιτέρω αξιοποίησή τους από τις αρχές.

- Η ιλιγγιώδης ταχύτητα σχετικά με τον χρόνο τέλεσής τους

Το απειροελάχιστο χρονικό διάστημα εντός του οποίου πολλές φορές συντελείται η διάπραξη ενός ηλεκτρονικού εγκλήματος, έχει ως αποτέλεσμα οι περισσότεροι χρήστες

[39] Βλ. Κάτος Β., Η φύση των ψηφιακών πειστηρίων, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

να μην συνειδητοποιούν ότι έχουν πέσει θύματα, ενώ δεν είναι λίγες και οι φορές κατά τις οποίες οι παράνομες αυτές πράξεις δεν καταγράφονται καν ως περιστατικά. Η συνειδητοποίηση από το θύμα ότι ο δράστης έχει προβεί στην τέλεση κάποιας εγκληματικής ενέργειας εις βάρος του επέρχεται συνήθως εκ των υστέρων, καθιστώντας την ποινικοποίηση της εγκληματικής συμπεριφοράς δυσχερέστερη[40].

- Ο διασυνοριακός χαρακτήρας σε σχέση με τον τόπο τέλεσής του

Το ηλεκτρονικό έγκλημα συχνά αποκαλείται και υπερεθνικό, καθώς η έναρξη, η πρόληψη ή/και οι συνέπειές του αφορούν ή και επεκτείνονται πέρα από τα σύνορα ενός κράτους[41]. Κάθε ηλεκτρονικός υπολογιστής ο οποίος αποκτά (μέσω του τηλεπικοινωνιακού παρόχου) πρόσβαση στο διαδίκτυο, είναι σε θέση να ανταλλάζει πληροφορίες, σε αμελητέο χρόνο, με κάθε άλλο διασυνδεδεμένο στο διαδίκτυο υπολογιστή σε οποιοδήποτε μέρος του πλανήτη. Για την επίτευξη της επικοινωνίας αυτής, οι πληροφορίες (που έχουν τη μορφή πακέτων) πρέπει να ταξιδέψουν μέσα από διάφορους δρομολογητές ή πύλες (gateways) προκειμένου να φτάσουν στον τελικό αποδέκτη, εκτελώντας έτσι πολλαπλά άλματα (hops). Ακόμα και στην περίπτωση όπου οι δύο ανταποκριτές βρίσκονται στο ίδιο γεωγραφικό κράτος, η δρομολόγηση των πακέτων που ανταλλάσσονται μεταξύ τους μπορεί να επιτυγχάνεται διά μέσω πυλών ή δρομολογητών που είναι εγκατεστημένοι σε άλλα κράτη. Επομένως ο εδαφικός προσδιορισμός και περιορισμός της χρήσης του διαδικτύου είναι ανέφικτος.

Παράλληλα, οι δράστες ορισμένες φορές, σκοπίμως επιδιώκουν να μην κάνουν γνωστή ή να δηλώσουν μια διαφορετική τοποθεσία από αυτήν στην οποία βρίσκονται, γεγονός που δυσχεραίνει περαιτέρω την αποκάλυψη του πραγματικού τόπου δράσης ή τέλεσης του εγκλήματος.

- Η απροθυμία καταγγελιών και η διακρατική συνεργασία των διωκτικών αρχών σε σχέση με την απόδειξη τέλεσής τους

Αποτελεί αρκετά συχνό φαινόμενο η αποσιώπηση ενός ηλεκτρονικού συμβάντος εξαιτίας της απροθυμίας καταγγελίας του από το θύμα. Συνήθως, τα φυσικά πρόσωπα, δεν προβαίνουν σε καταγγελία, είτε επειδή μπορεί να μην έχουν συνειδητοποιήσει καν ότι έχουν πέσει θύματα, αλλά κυρίως επειδή ο φόβος και η άγνοια που τους διακατέχουν

[40] Βλ. Δαλακούρας Θ., Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης (Ν 4411/2016) , Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

[41] Βλ. Γ. Χλούπης, Υπερεθνικό Έγκλημα με τη χρήση Η/Υ, 1999, σελ.647

(τόσο ως προς τη διαδικασία της καταγγελίας, όσο και από τις ενδεχόμενες συνέπειες της πράξης τους αυτής), λειτουργούν ως αποτρεπτικοί παράγοντες.

Όσον αφορά τα νομικά πρόσωπα, το ζήτημα της καταγγελίας του ηλεκτρονικού εγκλήματος λειτουργεί διαφορετικά και «κινείται» συνήθως σε άλλες διαστάσεις. Η παραδοχή για ένα νομικό πρόσωπο ότι έχει πέσει θύμα ηλεκτρονικού εγκλήματος, μεταφράζεται συνήθως σε κλονισμό της αξιοπιστίας του προς το κοινό και της φήμης που αυτό έχει κατοχυρώσει, γεγονός που με τη σειρά του δύναται να επισύρει σφοδρές οικονομικές (κυρίως) επιπτώσεις γι' αυτό. Για το έτος 2022, περίπου το 71% των εταιρειών σε παγκόσμια κλίμακα[42] έχει πέσει θύμα κακόβουλου λογισμικού λύτρων (ransomware)[43]. Μάλιστα, η ίδια έρευνα αναφέρει ότι το 72% των θυμάτων, δέχτηκαν να πληρώσουν τα λύτρα προκειμένου να εξασφαλίσουν ξανά την πρόσβαση στα δεδομένα τους, γεγονός που υποδηλώνει εμφανώς αφενός μεν την απροθυμία τους για την καταγγελία του περιστατικού στις διωκτικές αρχές, αφετέρου δε τονίζει την αναγκαιότητα για ένα νομικό πρόσωπο διασφάλισης της θέσης που αυτό έχει εδραιώσει στον επιχειρηματικό τομέα.

3.4 Οι νομοθετικές προκλήσεις του ηλεκτρονικού εγκλήματος

Όσον αφορά τη νομική προσέγγιση του κυβερνοχώρου, αυτός διέπεται από τις ίδιες Συνταγματικές Αρχές που επικρατούν και στο «φυσικό» κόσμο[44]. Ο σεβασμός της προσωπικότητας του άλλου, η ισότητα μεταξύ των ατόμων, η ελεύθερη έκφραση και διακίνηση των απόψεων, η διασφάλιση της ιδιωτικότητας και του απορρήτου της ελεύθερης ανταπόκρισης και επικοινωνίας, είναι μερικές μόνο από τις προαναφερόμενες αρχές, οι οποίες όμως ουκ ολίγες φορές καταστρατηγούνται ιδίως στο περιβάλλον του κυβερνοχώρου.

Η βασική πρόκληση που αντιμετωπίζει ο νομοθέτης δεν οφείλεται πουθενά αλλού, παρά στην ίδια τη φύση του κυβερνοχώρου. Η απουσία του στοιχείου του

[42] Πηγή: https://www.statista.com/statistics/700894/global-ransom-payers-rate/

[43] Σε αυτή τη μορφή ηλεκτρονικού εγκλήματος, ο δράστης αποκτά πρόσβαση σε δεδομένα του θύματος, τα οποία και κρυπτογραφεί, με αποτέλεσμα να στερεί από το χρήστη τη δυνατότητα πρόσβασης σε αυτά, αν προηγουμένως δεν ικανοποιήσει τις (χρηματικές συνήθως) απαιτήσεις του δράστη

[44] Βλ. Αγγελής Ι., Διαδίκτυο και Ποινικό Δίκαιο, ΠοινΧρ Ν/2000

πραγματικού που αποτελεί χαρακτηριστικό γνώρισμα του διαδικτύου, σε συνδυασμό με την αδυναμία προσδιορισμού του μεγέθους και των ορίων εντός των οποίων αυτό εκτείνεται, αποτελούν σχεδόν ανυπέρβλητα εμπόδια στο έργο του νομοθέτη.

Όπως αναφέρθηκε προηγουμένως, πρωταγωνιστικό ρόλο στην αποδεικτική διαδικασία, διαδραματίζει η συλλογή των ψηφιακών πειστηρίων. Τα τελευταία είναι εκείνα που μπορούν να οδηγήσουν στον εντοπισμό του δράστη, υπό την προϋπόθεση όμως να έχει διατηρηθεί η ακεραιότητά τους, ώστε αυτά να μπορούν να αξιοποιηθούν στην ποινική δικονομία. Η εξασφάλιση της ακεραιότητας των ψηφιακών πειστηρίων αποτελεί άλλοτε μια σχετικά απλή διαδικασία και άλλες φορές απαιτεί εξειδίκευση και τεχνογνωσία πάνω στον τομέα αυτόν[45], γεγονός που μπορεί να αποτελέσει μια σημαντική πρόκληση για τις αρχές.

Ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος επιτάσσει τη συνεργασία των διωκτικών αρχών των κρατών για την αποτελεσματική του αντιμετώπιση. Κάτι τέτοιο δεν επιτυγχάνεται αποκλειστικά και μόνο με τη συνεργασία μεταξύ των αστυνομικών αρχών των κρατών για την πρόληψη, καταστολή και σύλληψη των φερόμενων ως δραστών. Βασικές προϋποθέσεις για να επιτευχθεί αυτό, αποτελεί η θέσπιση ενός κοινού νομοθετικού πλαισίου, σύμφωνα με το οποίο θα ποινικοποιούνται οι παράνομες συμπεριφορές του κυβερνοχώρου, καθώς και η μετέπειτα καθολική ενσωμάτωσή του στο εθνικό δίκαιο κάθε χώρας. Κάτι τέτοιο κρίνεται απαραίτητο, αρχικά επειδή στο περιβάλλον του διαδικτύου δεν μπορούν να εφαρμοστούν εδαφικοί ή κρατικοί περιορισμοί, αλλά πρέπει αυτό να αντιμετωπίζεται ως μία ενιαία οντότητα. Επιπλέον, η ύπαρξη διαφορετικής ποινικής αντιμετώπισης ορισμένων παραβατικών συμπεριφορών (κυρίως με την ελαφρύτερη ποινική τους αντιμετώπιση ή ακόμα και την μη ποινικοποίησή τους), ενδεχομένως να οδηγούσε σε έξαρση των περιστατικών αυτών, ενώ το κράτος θα λειτουργούσε ευνοϊκά για την υπόθαλψη των παραβατών.

Το περιεχόμενο της επικοινωνίας ή οι ενέργειες που πραγματοποιούνται από ένα χρήστη, μπορεί μεν να μην αντιβαίνουν στη νομική τάξη της χώρας από όπου αυτός ενεργεί, μπορεί να θεωρούνται όμως αντίθετες προς το Δίκαιο του κράτους όπου βρίσκεται ο πιθανός αποδέκτης της επίθεσης[46]. Κατά ανάλογο τρόπο, γεννιούνται

[45] Βλ. Κάτος Β., Η φύση των ψηφιακών πειστηρίων, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

[46] Βλ. Δαλακούρας Θ., Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης (Ν 4411/2016) , Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

προβληματισμοί αναφορικά με τη σημαντικότητα του ρόλου που διαδραματίζει η κρατική έννομη τάξη της χώρας όπου βρίσκονται αποθηκευμένα τα δεδομένα και οι βάσεις δεδομένων μίας δραστηριότητας.

Ορόσημο στην προσπάθεια ενσωμάτωσης των νέων μορφών αξιόποινων συμπεριφορών του διαδικτύου στην ευρωπαϊκή ποινική νομοθεσία, αποτέλεσε η Σύμβαση της Βουδαπέστης[47], η οποία υπογράφηκε στις 23.11.2001 και ενσωματώθηκε από πλήθος κρατών σε παγκόσμιο επίπεδο. Η Σύμβαση αυτή[48] καθώς και η Οδηγία 2013/40/ΕΕ κυρώθηκαν στη χώρα μας με το ν.4411/2016 και περιλαμβάνει 4 γενικότερες κατηγορίες εγκλημάτων που σχετίζονται με υπολογιστές[49]:

- Εγκλήματα κατά της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων η/υ (τα οποία περιλαμβάνουν την παράνομη πρόσβαση, την παράνομη υποκλοπή δεδομένων, την παρέμβαση σε δεδομένα, την παρέμβαση σε σύστημα και τη κακή χρήση συσκευών)
- Εγκλήματα σχετικά με η/υ (στα οποία συγκαταλέγονται η πλαστογραφία σε σχέση με η/υ και η απάτη με η/υ)
- Εγκλήματα σχετικά με το περιεχόμενο
- Εγκλήματα σχετικά με παραβιάσεις των δικαιωμάτων πνευματικής ιδιοκτησίας και των σχετικών δικαιωμάτων

3.5 Hacking - Cracking

Ως επί το πλείστον, οι χρήστες των υπολογιστών και του κυβερνοχώρου οι οποίοι προβαίνουν σε παράνομες και εγκληματικές συμπεριφορές, ταξινομούνται σε δύο κύριες κατηγορίες : τους χάκερς (hackers) και τους κράκερς (crackers).

Με τον όρο «hacking» αναφερόμαστε στην άνευ αδείας πρόσβαση (συνήθως μέσω του διαδικτύου, χωρίς αυτό ωστόσο να είναι προαπαιτούμενο), σε ευαίσθητα ή μη δεδομένα, από μη εξουσιοδοτημένα προς αυτό άτομα. Τις περισσότερες των

[47] Βλ. Δαλακούρας Θ., Οι ειδικότερες διατάξεις της Σύμβασης για το έγκλημα στον κυβερνοχώρο, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη

[48] Αναφέρεται και ως σύμβαση 189

[49] Βλ. Ιγγλεζάκης Ι., Έγκλημα πληροφορικής, Κυβερνοέγκλημα και κυβερνοασφάλεια, Δίκαιο Πληροφορικής, 2021, Δ εκδ., εκδ. Σάκκουλα

περιπτώσεων, η παράνομη αυτή εισβολή δεν συνοδεύεται από εκμετάλλευση ή καταστροφή των πόρων αυτών προς όφελος του επιτιθέμενου, αλλά απεναντίας εκτελείται για την προσωπική ικανοποίησή του, για την παράκαμψη των συστημάτων ασφαλείας, δηλαδή ως ένα μέσο απόδειξης της τεχνολογικής υπεροχής του δράστη σε σχέση με τα υφιστάμενα αποτρεπτικά μέτρα ασφαλείας. Επιπλέον, ένας hacker μπορεί να χρησιμοποιεί τις εξειδικευμένες γνώσεις του με σκοπό να ανακαλύψει ή να εμφανίσει τυχόν αδυναμίες στην ασφάλεια του ηλεκτρονικού συστήματος οι οποίες μπορούν να εκθέσουν τα δεδομένα σε κίνδυνο.

Ο όρος «cracking» χρησιμοποιείται για να περιγράψει την παράνομη είσοδο σε ένα ηλεκτρονικό σύστημα ή βάση δεδομένων, παρακάμπτοντας τους περιορισμούς ασφαλείας που έχουν τεθεί, με σκοπό την πρόκληση σοβαρής ζημιάς, ενεργώντας (συνήθως) με κίνητρο το οικονομικό όφελος.

Συχνά βέβαια, ο όρος hacker χρησιμοποιείται για να περιγράψει τους χρήστες που δρουν είτε μεμονωμένα, είτε σε ομάδες με σκοπό να πλήξουν υπολογιστικά συστήματα και βάσεις δεδομένων ή να αποκτήσουν παράνομη πρόσβαση σε διαβαθμισμένα δεδομένα, καλύπτοντας έτσι και τις δύο προαναφερθείσες κατηγορίες.

Με γνώμονα τις προθέσεις τους, οι hackers διακρίνονται στις εξής βασικές κατηγορίες[50]:

- White Hat Hackers

Αυτοί αντιπροσωπεύουν την «ηθική» πλευρά του hacking (ethical hacking). Διεισδύουν σε δίκτυα υπολογιστών μόνο μετά από συναίνεση του αρμοδίου οργάνου, με σκοπό να αποκαλύψουν τα κενά ασφαλείας που υπάρχουν στο σύστημα και να τα αντιμετωπίσουν. Αρκετές φορές, εταιρείες ή νομικά πρόσωπα τους προσλαμβάνουν με σκοπό να έχουν μία σαφέστερη εικόνα του επιπέδου ασφαλείας που βρίσκονται τα ηλεκτρονικά τους συστήματα.

- Black Hat Hackers

Οι black hat hackers είναι οι εγκληματίες του διαδικτύου, οι οποίοι κακοπροαίρετα εισβάλλουν σε υπολογιστικά συστήματα, χωρίς προηγούμενη έγκριση από το νόμιμο δικαιούχο. Συνήθως εντοπίζοντας ένα κενό ασφαλείας, το εκμεταλλεύονται εμφυτεύοντας στο σύστημα κάποιο κακόβουλο λογισμικό, όπως ιούς ή δούρειους ίππους, τα οποία στη συνέχεια ενεργούν ποικιλοτρόπως και προκαλούν καταστροφές.

[50] https://www.avast.com/c-hacker-types

- Gray Hat Hackers

Οι Gray Hat Hackers δρουν συνήθως διεισδύοντας σε δίκτυα ή υπολογιστές χωρίς προηγούμενη έγκριση του αρμοδίου προσώπου, χωρίς ωστόσο οι προθέσεις τους να χαρακτηρίζονται απαραίτητα ως κακόβουλες. Μόλις εντοπίσουν αδυναμίες στα συστήματα ασφαλείας, ενημερώνουν τους χρήστες, ζητώντας πολλές φορές χρηματικά ποσά προκειμένου να προσδιορίσουν επακριβώς τις ατέλειες στην ασφάλεια.

Οι κακόβουλες επιθέσεις δίκτυα υπολογιστών μπορεί να οδηγήσουν σε μεγάλες απώλειες χρημάτων και χρόνου, εξαιτίας της καταστροφής ή κλοπής σημαντικών για τους χρήστες δεδομένων ή περιουσιακών στοιχείων. Ένας δράστης για να αποκτήσει πρόσβαση σε ένα δίκτυο, εκμεταλλεύεται ευπάθειες τόσο στο λογισμικό (software) όσο και στο υλικό (hardware), ενώ επίσης αυτό μπορεί να συντελεστεί και με την παραβίαση των διαπιστευτηρίων του χρήστη (username και password).

Μόλις ένας εισβολέας αποκτήσει πρόσβαση σε έναν ή και περισσότερους υπολογιστές, τότε μπορεί να προβεί στις εξής ενέργειες[51]:

- Κλοπή Πληροφοριών

Στην περίπτωση αυτή, ο hacker αποκτά πρόσβαση προκειμένου να αποσπάσει από το χρήστη σημαντικές πληροφορίες με σκοπό να τις χρησιμοποιήσει ο ίδιος, να τις μεταβιβάσει έναντι ανταλλάγματος σε τρίτους, ή ακόμα και να τις στερήσει από τον κάτοχο.

- Απώλεια και Παραποίηση Δεδομένων

Ο hacker εισβάλλει με σκοπό να καταστρέψει ή να αλλοιώσει τα δεδομένα του χρήστη, προκειμένου να παραχθεί ένα διαφορετικό αποτέλεσμα. Η αποστολή σε ένα χρήστη κακόβουλου λογισμικού, το οποίο κατακερματίζει το σκληρό δίσκο, με αποτέλεσμα την απώλεια των δεδομένων μπορεί να αναφερθεί ως ένα παράδειγμα της εγκληματικής αυτής συμπεριφοράς.

- Κλοπή Ταυτότητας

Υπό τον όρο «κλοπή ταυτότητας[52]» (identity theft) περιγράφεται η παράνομη οικειοποίηση από κάποιον τρίτο, με ποικίλες μεθόδους, διαφόρων προσωπικών

[51] http://cisco.num.edu.mn/CCNA_R&S1/course/module11/11.2.1.1/11.2.1.1.html

[52] Στην Οδηγία 2013/40/ΕΕ επισημαίνεται η ανάγκη θέσπισης ικανών μέτρων αντιμετώπισης του φαινομένου.

στοιχείων του νόμιμου δικαιούχου, όπως αριθμών τραπεζικών καρτών ή λογαριασμών, διαπιστευτηρίων εισόδου σε πλατφόρμες κ.λπ.[53]

- Διακοπή Παρεχόμενων Υπηρεσιών

Εδώ ο εισβολέας αποστερεί από το χρήστη τη δυνατότητα πρόσβασης σε υπηρεσίες [π.χ. ιστοσελίδες, υπολογιστικό νέφος (cloud), διαδικτυακές πλατφόρμες κ.λπ.]. Στις περιπτώσεις όπου οι επιθέσεις αυτές διενεργούνται εναντίον εξυπηρετητών (servers), τότε το σύνολο των χρηστών στερείται την πρόσβαση στις παρεχόμενες από τον εξυπηρετητή υπηρεσίες. Χαρακτηριστικό παράδειγμα αποτελούν οι επιθέσεις DoS (Denial of Service) εναντίον εξυπηρετητών, που έχουν ως συνέπεια το περιεχόμενό τους να μην είναι προσβάσιμο στους χρήστες[54].

3.6 Η ανάγκη προστασίας στο διαδίκτυο

Τα ιδιότυπα χαρακτηριστικά των ηλεκτρονικών εγκλημάτων και κυρίως ο διασυνοριακός τους χαρακτήρας επιβάλλουν τόσο τη συνεργασία μεταξύ Δημοσίου και Ιδιωτικού τομέα, όσο και μεταξύ των διαφόρων κρατών, προκειμένου να διασφαλισθεί η προστασία των ατομικών αλλά και υπερατομικών αγαθών.

Στην καθημερινότητά μας, ο όρος προστασία αναφέρεται στην φροντίδα που παρέχεται με σκοπό να προφυλαχθεί κάποιος/κάτι από υπαρκτούς ή διαφόρους πιθανούς κινδύνους[55]. Όσον αφορά το περιβάλλον των ηλεκτρονικών υπολογιστών, η προστασία αυτή επεκτείνεται και καλύπτει τα δύο βασικά μέρη ενός υπολογιστικού συστήματος, δηλαδή το υλικό και το λογισμικό. Έτσι λοιπόν, η προστασία μπορεί να περιλαμβάνει τόσο τη διασφάλιση της ακεραιότητας ενός συστήματος από φυσικούς κινδύνους του εξωτερικού κόσμου (π.χ. αντίξοες καιρικές συνθήκες, υπερτάσεις ρεύματος, συνθήκες υγρασίας κ.λπ.), όσο και την εξασφάλιση της εμπιστευτικότητας (Confidentiality), ακεραιότητας (Integrity) και διαθεσιμότητας (Availability) των ψηφιακών δεδομένων.

Οι τρεις αυτές αρχές [56] αποτελούν το τρίπτυχο της ασφάλειας των υπολογιστικών συστημάτων. Ο όρος εμπιστευτικότητα αναφέρεται στην προστασία των υπολογιστικών

[53] Τζαννετής Αρ., Το πλαστό έγγραφο, ΠοινΧρ, 2021, εκδ. Σάκκουλα, σελ. 226

[54] Βλ. Άρθρο 4 της Οδηγίας 2013/40/ΕΕ

[55] Μπαμπινιώτης Γ., Λεξικό της Νέας Ελληνικής Γλώσσας, 2002

[56] Επίσης γνωστές και ως CIA (εκ των Confidentiality, Integrity, Availability)

συστημάτων και των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, δηλαδή από αναρμόδια για το σκοπό αυτό πρόσωπα. Η ακεραιότητα περιγράφει την αυθεντικότητα των δεδομένων, ότι δηλαδή τα δεδομένα προέρχονται από το συγκεκριμένο αποστολέα και απευθύνονται στον καθορισμένο παραλήπτη, χωρίς να έχουν υποστεί αλλοίωση ή οποιουδήποτε άλλου είδους τροποποίηση. Επίσης, η ακεραιότητα εξασφαλίζει ότι τα ψηφιακά δεδομένα τροποποιούνται αποκλειστικά από εξουσιοδοτημένους χρήστες. Τέλος, διαθεσιμότητα σημαίνει ότι οι αρμόδιοι χρήστες έχουν ανά πάσα στιγμή δυνατότητα πρόσβασης στα υπολογιστικά τους μέσα ή στους ψηφιακούς τους πόρους, χωρίς αυτή να παρακωλύεται για οποιοδήποτε λόγο.

Η αδυναμία καθορισμού εδαφικών περιορισμών στο περιβάλλον του διαδικτύου, συνεπάγεται ότι ο κάθε χρήστης μπορεί να πέσει θύμα ηλεκτρονικού εγκλήματος από οποιονδήποτε άλλο χρήστη του διαδικτύου. Η τάση προς ψηφιοποίηση και μεταφορά στο ηλεκτρονικό περιβάλλον της πλειοψηφίας των καθημερινών δραστηριοτήτων μας, επιτείνει την ανάγκη συνειδητοποίησης των αναρίθμητων κινδύνων, στους οποίους βρίσκεται κανείς εκτεθειμένος καθημερινά. Η προστασία στο διαδίκτυο είναι ένα θέμα το οποίο δεν πρέπει να απασχολεί μόνο τις αστυνομικές αρχές, αλλά και τον καθένα μας ξεχωριστά.

Η ελευθερία ανταλλαγής και μετάδοσης πληροφοριών μεταξύ όλων των διασυνδεδεμένων στο διαδίκτυο υπολογιστών και μάλιστα σε μηδενικό χρόνο, αποτέλεσε το βασικότερο πλεονέκτημα της ταχείας εξάπλωσής του. Παρόλα αυτά όμως, συνάμα δημιουργούνται και οι προϋποθέσεις παράνομης διείσδυσης τρίτων στο υπολογιστικό σύστημα ενός χρήστη[57].

Εκτός από τους διαρκείς κινδύνους που ακούν στο όνομα hacking και cracking, δεν θα πρέπει να θεωρούνται ως απειλές ήσσονος σημασίας οι ενέργειες των ιδίων των χρηστών. Πολλές φορές ο κίνδυνος μπορεί να πηγάζει από τους ίδιους τους χρήστες ή τους εργαζομένους σε μία επιχείρηση. Αυτό μπορεί να μεταφράζεται είτε σε αφέλεια που πηγάζει από την άγνοια των χρηστών ή ακόμα και σε συνειδητές κακόβουλες ενέργειες από μέλη μίας επιχείρησης. Μερικά παραδείγματα που μπορούν να αναφερθούν είναι η καταστροφή και απώλεια δεδομένων, η μη τήρηση των πρωτοκόλλων ασφαλείας υλικού και λογισμικού (π.χ. χρήση ευπαθών κωδικών πρόσβασης, εργασία σε περιβάλλον που δεν έχει τις απαραίτητες συνθήκες θερμοκρασίας ή υγρασίας), η μη εξουσιοδοτημένη

[57] Βλ. Κιούπης Δ., Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, 2000

πρόσβαση σε ευαίσθητα δεδομένα ή πληροφορίες καθώς και η κλοπή πνευματικής ιδιοκτησίας ή απορρήτων επιχειρήσεων.

4 Η απάτη ως ηλεκτρονικό έγκλημα

Όπως αναφέρθηκε προηγουμένως, η καθολική εισχώρηση και εγκαθίδρυση της τεχνολογίας και της επιστήμης των ηλεκτρονικών υπολογιστών στην ζωή μας τον 21ο αιώνα, έχει συντελέσει στη δυνατότητα χρησιμοποίησης των τελευταίων, σε πληθώρα δραστηριοτήτων της καθημερινότητας, αλλά παράλληλα και ως μέσα διάπραξης εγκλημάτων. Οι νέες μορφές αξιόποινων πράξεων που συντελούνται μέσω των ηλεκτρονικών υπολογιστών τόσο σε περιβάλλον κυβερνοχώρου όσο και εκτός, πολλές φορές δεν μπορούν να υπαχθούν στις υπάρχουσες διατάξεις του ΠΚ, αφού δεν πληρούν εξ' ολοκλήρου την αντικειμενική υπόσταση αυτών. Το γεγονός αυτό, έχει αναγκάσει τον ποινικό νομοθέτη να προβεί στην θέσπιση νέων διατάξεων, ή στην συμπλήρωση των υπαρχουσών, προκειμένου να μπορέσει να επιτευχθεί η βέλτιστη ποινικοποίηση των περιπτώσεων αυτών. Μερικά από τα άρθρα του ΠΚ τα οποία θεσπίστηκαν ειδικά για την εξυπηρέτηση του παραπάνω σκοπού είναι το 348Α (Προσέλκυση παιδιών για γενετήσιους λόγους), το 370Β (Παράνομη αντιγραφή και χρήση απόρρητων δεδομένων) το 370Γ (Παράνομη πρόσβαση σε πληροφοριακό σύστημα), το 381Α (Φθορά ηλεκτρονικών δεδομένων) και το 386Α (Απάτη με υπολογιστή).

Η απάτη στα σύγχρονα υπολογιστικά συστήματα εμφανίζεται κατά κύριο λόγο με δύο μορφές, την απάτη μέσω υπολογιστή (386 ΠΚ) και την απάτη με υπολογιστή (386Α ΠΚ). Οι δύο αυτές παραλλαγές, αν και εκ πρώτης όψεως μπορεί να εμφανίζουν αρκετές ομοιότητες, νομικά αποκλίνουν μεταξύ τους, με αποτέλεσμα ο ποινικός νομοθέτης να τις αντιμετωπίζει ως δύο ξεχωριστές περιπτώσεις.

Το περιβάλλον τέλεσης τόσο στην απάτη μέσω υπολογιστή, όσο και στην απάτη με υπολογιστή δύναται να διαφέρει. Και τα δύο ηλεκτρονικά εγκλήματα μπορούν να λάβουν χώρα είτε ένα πληροφοριακό σύστημα δεν βρίσκεται συνδεδεμένο σε κάποιο δίκτυο (offline), είτε βρίσκεται σε κάποιο τοπικό δίκτυο, είτε ακόμα και στο περιβάλλον του διαδικτύου (online). Στην τελευταία περίπτωση έχουμε την κλασική μορφή ενός κυβερνοεγκλήματος (e-crime), ενώ είναι αυτή που συναντάται και στην πλειοψηφία των περιπτώσεων.

4.1 Η απάτη μέσω υπολογιστή (386 ΠΚ)

Η απάτη μέσω υπολογιστή αποτελεί μία άλλη έκφανση της κοινής απάτης, «μεταφερόμενη» σε ηλεκτρονικό περιβάλλον. Ο ηλεκτρονικός υπολογιστής ή το πληροφοριακό σύστημα χρησιμοποιείται από το δράστη **ως ένα απλό μέσο για τη διάπραξη του εγκλήματος της απάτης**. Για το λόγο αυτό, κατατάσσεται στα «μη γνήσια» κυβερνοεγκλήματα, καθώς αποτελεί ένα συμβατικό έγκλημα, το οποίο δεν τελείται αποκλειστικά με τη χρήση ενός ηλεκτρονικού υπολογιστή, αλλά δύναται να τελεστεί και χωρίς αυτόν[58]. Η απάτη μέσω υπολογιστή ποινικοποιείται από το νομοθέτη με το άρθρο 386 ΠΚ, σύμφωνα με το οποίο:

«1. Όποιος με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή.

2. Αν η απάτη στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημιά που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1000) ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά από είκοσι (20) έτη».

Σύμφωνα με τα άρθρα 18 ΠΚ («Οι αξιόποινες πράξεις διακρίνονται σε κακουργήματα και πλημμελήματα. Κάθε πράξη που τιμωρείται με κάθειρξη ισόβια ή πρόσκαιρη είναι κακούργημα. Κάθε πράξη που τιμωρείται με φυλάκιση ή περιορισμό σε ειδικό κατάστημα κράτησης νέων ή μόνο με χρηματική ποινή ή παροχή κοινωφελούς εργασίας είναι πλημμέλημα.») και 19 ΠΚ [«Αν μια πράξη που εκδικάστηκε είναι κακούργημα ή πλημμέλημα, κρίνεται με βάση τη βαρύτερη ποινή που καθορίζεται από τον νόμο γι' αυτή και όχι με βάση την τυχόν ελαφρότερη ποινή που επέβαλε ο δικαστής λόγω ελαφρυντικών περιστάσεων (άρθρο 84) ή για οποιονδήποτε άλλο λόγο μείωσης της

[58] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ.482-483

ποινής σύμφωνα με το άρθρο 83.»], η απάτη μέσω υπολογιστή αποτελεί ένα έγκλημα το οποίο από πλευράς ποινικής βαρύτητας μπορεί να αποτελέσει τόσο πλημμέλημα, όσο και κακούργημα. Βασικό κριτήριο για την διάκρισή του στις δύο παραπάνω κατηγορίες δεν είναι άλλο, από την αποτίμηση του μεγέθους της προκληθείσας ζημίας. Αν αυτή ξεπερνάει τις 120.000 ευρώ και κατ' επέκταση εμπίπτει στις περιπτώσεις όπου ποινικοποιείται με κάθειρξη, τότε αντιμετωπίζεται ως κακούργημα, ενώ σε κάθε άλλη διαφορετική περίπτωση η απάτη που στοιχειοθετείται αντιμετωπίζεται ως πλημμέλημα. Επιπλέον, μεταξύ των διακεκριμένων μορφών των κακουργημάτων (άνω των 120.000 ευρώ), ο νομοθέτης πραγματοποιεί μία ακόμη διάκριση, η οποία σχετίζεται με το πρόσωπο του αποδέκτη της εγκληματικής πράξης. Συγκεκριμένα, αν αυτή τελείται εναντίον του Δημοσίου, ν.π.δ.δ. ή κάποιου ΟΤΑ, τότε η επιβαλλόμενη ποινή της κάθειρξης αυξάνεται από έως δέκα (10), σε τουλάχιστον δέκα (10) έτη, ενώ παράλληλα επιβάλλεται και χρηματική ποινή ύψους έως χίλιες (1000) ημερήσιες μονάδες.

Οι ανωτέρω διακρίσεις διαδραματίζουν σημαντικό ρόλο και όσον αφορά τη διάρκεια του χρόνου παραγραφής. Σύμφωνα με το 111§2 ΠΚ, «Τα κακουργήματα παραγράφονται μετά είκοσι έτη αν ο νόμος προβλέπει γι' αυτά την ποινή της ισόβιας κάθειρξης και μετά δέκα πέντε έτη σε κάθε άλλη περίπτωση, εκτός αν ο νόμος προβλέπει διαφορετικά», ενώ το 111§3 ΠΚ ορίζει ότι «Τα πλημμελήματα παραγράφονται μετά πέντε έτη». Έτσι λοιπόν, στην περίπτωση που η απάτη μέσω υπολογιστή χαρακτηριστεί ως πλημμέλημα (δηλ. το συνολικό ποσό της ζημιάς που προκαλείται δεν υπερβαίνει τις 120.000 ευρώ), τότε ο χρόνος παραγραφής ανέρχεται σε 5 χρόνια. Εάν η απάτη αντιθέτως κριθεί ως κακούργημα (συνολική ζημία άνω των 120.000 ευρώ) διακρίνεται ως προς το θύμα αυτής. Αν ο αποδέκτης της ζημίας είναι κάποιο φυσικό πρόσωπο ή ν.π.ι.δ., ο χρόνος παραγραφής ανέρχεται σε 15 έτη (111§2 ΠΚ), ενώ στην πλέον διακεκριμένη μορφή απάτης κατά την οποία ο αποδέκτης είναι το Δημόσιο, ν.π.δ.δ. ή ΟΤΑ, τότε ο χρόνος παραγραφής ανέρχεται στη μεγαλύτερη διάρκεια, ήτοι στα 20 έτη (386§2 ΠΚ).

4.1.1 Αντικειμενική Υπόσταση

Στην περίπτωση της κοινής απάτης (άρα και στην απάτη μέσω υπολογιστή), η αντικειμενική υπόσταση ορίζεται συνήθως από μία αλληλουχία αιτιωδών πράξεων, κάθε μία από τις οποίες αποσκοπεί στην επίτευξη ενός αυτοτελούς αποτελέσματος.

Σε πρώτο στάδιο, επιχειρείται από το δράστη η παραπλάνηση του θύματος με το οποίο αυτός έρχεται σε επαφή (αυτή μπορεί να επιτευχθεί με δύο τρόπους όπως θα αναλυθεί στη συνέχεια). Όπως και σε όλα τα ηλεκτρονικά εγκλήματα, η «επαφή» δράστη και θύματος δεν νοείται με την έννοια της φυσικής επαφής, της συνύπαρξης δηλαδή στον ίδιο χώρο των ατόμων αυτών, αλλά κατά κανόνα προϋποθέτει εδαφική απόσταση μεταξύ τους, η οποία πολλές φορές μάλιστα υπερβαίνει και τα όρια ενός κράτους. Παράλληλα, το ηλεκτρονικό περιβάλλον εξαλείφει και την απαίτηση της χρονικής συνύπαρξης δράστη και θύματος για την επίτευξη του εγκληματικού αποτελέσματος, καθώς οι παραπλανητικές ενέργειες του δράστη μπορούν να επιφέρουν το επιδιωκόμενο αποτέλεσμα σε μεταγενέστερο χρόνο (όταν π.χ. το θύμα συνδεθεί στο πληροφοριακό του σύστημα ή όταν «τρέξει» το πρόγραμμα που του έχει αποσταλεί).

Η παραπλάνηση του θύματος, μόλις αυτή επιτευχθεί, συντελεί με τη σειρά της στο δεύτερο αποτέλεσμα, που είναι η περιουσιακή διάθεση μέσω της πράξης, παράλειψης ή ανοχής. Ο δράστης έχοντας πλέον κερδίσει την εμπιστοσύνη του χρήστη αποφεύγοντας οποιαδήποτε υποψία μπορούσε να δημιουργηθεί, πείθει τον τελευταίο στην εμπράγματη μεταβίβαση των περιουσιακών του στοιχείων (με το στοιχείο του συνειδητού να απουσιάζει). Πολλές φορές αυτή μπορεί να μη συμβαίνει άμεσα (π.χ. με μεταφορά χρηματικού ποσού σε λογαριασμό του δράστη ή τρίτου) αλλά έμμεσα, όπως στην περίπτωση της αποκάλυψης στο δράστη των προσωπικών στοιχείων e-banking του θύματος. Ο κακόβουλος χρήστης στη συνέχεια θα προβεί ο ίδιος σε δεύτερο χρόνο στη μεταβίβαση, οπότε και τότε θα πραγματοποιηθεί η ουσιαστική αποπεράτωση του εγκλήματος της απάτης μέσω υπολογιστή, μιας και η περιουσιακή μεταβίβαση αποτελεί αναπόσπαστο στοιχείο της α.υ. του. Η βλάβη της περιουσίας του θύματος είναι η τρίτη και τελευταία πράξη που ολοκληρώνει την εγκληματική συμπεριφορά[59].

Δράστης, δηλαδή **υποκείμενο** της απάτης μέσω υπολογιστή μπορεί να είναι οποιοσδήποτε κατέχει ορισμένες βασικές γνώσεις που απαιτούνται για την τέλεση της υπόψη πράξης, χωρίς να απαιτείται η συγκέντρωση στο πρόσωπό του άλλων ιδιαιτέρων

[59] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, Άρθρα 385-406 ΠΚ, Εγκλήματα Περιουσιακής μετάθεσης, 2000, εκδ. Σάκκουλα

χαρακτηριστικών («Όποιος…»). Για το λόγο αυτό, η απάτη χαρακτηρίζεται ως **κοινό** και όχι ιδιαίτερο έγκλημα.

Αντικείμενο της πράξης αυτής είναι το σύνολο των περιουσιακών αγαθών, τα οποία ο δράστης επιθυμεί παράνομα να αποκτήσει προς όφελος ιδίου ή τρίτου («ξένη περιουσία»). Καθώς τα περιουσιακά αγαθά δεν έχουν κάποια ατομικότητα κατά τη στιγμή της προσβολής, η περιουσιακή βλάβη στην πράξη της απάτης νοείται με την μορφή της μείωσης του συνόλου της περιουσίας.

Οι πράξεις της απάτης (**εγκληματική συμπεριφορά**) μπορεί να περιλαμβάνουν: i) την αθέμιτη παράσταση αναληθών γεγονότων ως αληθινών ή/και την σκόπιμη αποσιώπηση των πραγματικών γεγονότων, ii) τη βλάβη της ξένης περιουσίας με απώτερο σκοπό τον παράνομο προσπορισμό του περιουσιακού οφέλους προς όφελος του δράστη ή ορισμένου τρίτου, και iii) την έμμεση παραπλάνηση του θύματος με την παρότρυνσή του να προβεί, σε ακούσια εκ μέρους του, περιουσιακή διάθεση μέσω πράξης, παράληψης ή ανοχής.

4.1.2 Υποκειμενική Υπόσταση

Για την τέλεση της απάτης μέσω υπολογιστή, απαιτείται ο δόλος εκ μέρους του δράστη και κατά συνέπεια δεν μπορεί να γίνει λόγος για απάτη εξ' αμελείας. Ο δόλος του δράστη συνίσταται στη βούλησή του για εξαπάτηση του ανυποψίαστου θύματος, ενώ για τη στοιχειοθέτηση της υποκειμενικής υπόστασης, υπάρχει και η επιπλέον απαίτηση ύπαρξης πρόσθετου σκοπού προσπορισμού της ξένης περιουσίας προς όφελος του δράστη ή τρίτου. Για το λόγο αυτό, κατατάσσεται στα εγκλήματα **υπερχειλούς υποκειμενικής υπόστασης**. Με την συντέλεση της περιουσιακής βλάβης ολοκληρώνεται το έγκλημα της απάτης, ενώ η ουσιαστική αποπεράτωση επέρχεται με τον προσπορισμό της παράνομης ξένης περιουσίας[60].

[60] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, Άρθρα 385-406 ΠΚ, Εγκλήματα Περιουσιακής μετάθεσης, 2000, εκδ. Σάκκουλα

4.1.3 Οι τρόποι τέλεσης της απάτης μέσω υπολογιστή

4.1.3.1 Η εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών

Στην περίπτωση αυτή, ο δράστης σκοπίμως παρουσιάζει ορισμένα γεγονότα στο χρήστη, τα οποία όμως δεν αντικατοπτρίζουν την πραγματικότητα. Το θύμα βασιζόμενο στα στοιχεία αυτά, οδηγείται τελικά σε ανεπιθύμητη περιουσιακή διάθεση. Ως γεγονότα ορίζονται ορισμένες καταστάσεις του εξωτερικού κόσμου, οι οποίες είναι άμεσα και εύκολα αντιληπτές από το μέσο άνθρωπο. Βασικό στοιχείο ενός γεγονότος είναι ότι πρέπει να είναι συντελεσμένο, να αφορά δηλαδή είτε το παρελθόν, είτε το παρόν. Επομένως περιστάσεις που αφορούν μελλοντικές καταστάσεις οι οποίες εμπεριέχουν το στοιχείο της αβεβαιότητας (βλ. π.χ. αιρέσεις, προθεσμίες κ.λπ.) δεν μπορούν να θεωρηθούν ως γεγονότα. Ειδικότερα, τα γεγονότα που συνεπάγονται έννομες συνέπειες, ονομάζονται νομικά. Επίσης, ως γεγονότα δεν μπορούν να χαρακτηριστούν οι καταστάσεις του εσωτερικού κόσμου ενός ατόμου, καθώς επίσης και οι προσωπικές απόψεις ή εκτιμήσεις του, καθώς ενσωματώνουν το στοιχείο της υποκειμενικής του κρίσης. Ο δράστης πολλές φορές μάλιστα, επιδιώκει να επιτύχει τον εγκληματικό του σκοπό γνωρίζοντας και εκμεταλλευόμενος την απειρία ή/και κουφότητα του θύματος. Χαρακτηριστικό παράδειγμα της τακτικής αυτής μπορεί να αποτελέσει ένα ανεπιθύμητο (spam) μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail) το οποίο αποστέλλεται σε πολλούς χρήστες και τους ενημερώνει ότι ο τραπεζικός τους λογαριασμός έχει προσβληθεί από hackers, χωρίς ωστόσο κάτι τέτοιο να συμβαίνει στην πραγματικότητα.

4.1.3.2 Η αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων

Μορφή απάτης μέσω υπολογιστή έχουμε και στην περίπτωση όπου ο δράστης γνωρίζει την αλήθεια ορισμένων γεγονότων και παρόλα αυτά σκοπίμως τα αποκρύπτει από το θύμα, ωθώντας το έμμεσα με τον τρόπο αυτό, στη λήψη μίας δυσμενούς για τα συμφέροντά του απόφασης ή ενισχύοντας με τον τρόπο αυτό την πλάνη στην οποία αυτό μπορεί να βρίσκεται.

4.2 Η απάτη με υπολογιστή (386Α ΠΚ)

Το άρθρο 386Α ΠΚ βασίστηκε στα άρθρα 263a και 148a του Γερμανικού και Αυστριακού Δικαίου αντίστοιχα και ορίζει ότι:

«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 σε πληροφοριακό σύστημα, γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης της ταυτότητας, ή ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή.

2. Όποιος κατασκευάζει, διαθέτει ή κατέχει πρόγραμμα ή πληροφοριακό σύστημα που προορίζεται για τη διάπραξη του εγκλήματος της παρ. 1 τιμωρείται με φυλάκιση έως δύο (2) έτη και χρηματική ποινή. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή πληροφοριακό σύστημα πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παρ. 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 ζημιά που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά από είκοσι (20) έτη.»

Όσον αφορά τη διάταξη του άρθρου 386Α ΠΚ, εντοπίζονται αρκετές ομοιότητες με αυτή του 386 ΠΚ. Οι ομοιότητες αυτές δεν είναι τυχαίες, αλλά σκοπίμως έχουν

εφαρμοστεί από το νομοθέτη προκειμένου να μπορέσει να αποτελέσει ένα σημαντικό βοήθημα για τον ερμηνευτή[61].

Η ηλεκτρονική απάτη θα μπορούσε να ορισθεί ως η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας μέσω της α) εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή ή/και β) της παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο[62].

Στην απάτη με υπολογιστή, ο δράστης χρησιμοποιεί τον υπολογιστή ως ένα **απαραίτητο μέσο προκειμένου να διαμορφώσει κατάλληλα τις συνθήκες εξαπάτησης του θύματος**[63]. Οι συνθήκες αυτές μπορεί να αφορούν τόσο στην δημιουργία μη ορθού προγράμματος η/υ, όσο και στην μη ορθή παρέμβαση κατά τη λειτουργία αυτού, με χρήση ή όχι ελλιπών δεδομένων αναγνώρισης ταυτότητας. Οι συνθήκες αυτές δημιουργούν στο χρήστη εσφαλμένη επίγνωση της πραγματικότητας, με αποτέλεσμα ο τελευταίος να προβαίνει στη διάθεση των περιουσιακών του στοιχείων. Για το λόγο αυτό, η απάτη με υπολογιστή συγκαταλέγεται στα «γνήσια» κυβερνοεγκλήματα, καθώς τελείται εναντίον ηλεκτρονικών συστημάτων πληροφοριών και δικτύων επικοινωνιών ή μπορεί να τελεστεί αποκλειστικά με χρήση αυτών[64].

Ως περιουσιακά στοιχεία θα πρέπει να αντιμετωπίζονται, εκτός από τα χρηματικά κεφάλαια στην φυσική και ηλεκτρονική τους μορφή, και τα προσωπικά στοιχεία του χρήστη (όπως διαπιστευτήρια εισόδου σε ιστοτόπους), δεδομένα του χρήστη τα οποία βρίσκονται αποθηκευμένα στον ηλεκτρονικό του υπολογιστή ή σε υπολογιστικό νέφος (cloud) ή διακινούνται στο διαδίκτυο, δεδομένα πνευματικής ιδιοκτησίας του χρήστη, καθώς και κάθε άλλο ηλεκτρονικό δεδομένο το οποίο ανήκει στην κυριότητά του.

Το άρθρο 386Α ενσωματώθηκε στον ΠΚ με το άρθρο 5 του νόμου 1805/1988, με σκοπό να καλύψει τα οποιαδήποτε κενά δημιουργούσε η εισαγωγή της ηλεκτρονικής τεχνολογίας και αδυνατούσαν να καλυφθούν από τη διάταξη του άρθρου 386 ΠΚ περί

---

[61] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 484

[62] Άρθρο 8 της Σύμβασης της Βουδαπέστης.

[63] Βλ. Κουράκης Ν., Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001

[64] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 482

απάτης[65]. Σύμφωνα με την Εισηγητική Έκθεση, σκοπός του συγκεκριμένου άρθρου αποτελεί «η θέσπιση ειδικών ποινικών διατάξεων για τη διασφάλιση της γνησιότητας των στοιχείων, που εγγράφονται και αποθηκεύονται στους ηλεκτρονικούς υπολογιστές ή παράγονται και αναπαράγονται από αυτούς (ύστερα από την εισαγωγή της πληροφορικής στη χώρα μας)». Παράλληλα, κρίθηκε αναγκαία η θέσπιση ειδικών διατάξεων «γιατί η αξιόποινη δραστηριότητα, η οποία μπορεί να αναπτυχθεί στον τομέα της πληροφορικής, δεν καλύπτεται πλήρως από την υπάρχουσα ποινική νομοθεσία ενώ η νέα αυτή μορφή τεχνολογίας μπορεί να ανοίξει δρόμους σε νέες, άγνωστες και με εφαρμογές αντίστοιχης τεχνολογίας μεθόδους εγκληματικής δράσης, οι οποίες δεν προβλέπονται από τον Ποινικό Κώδικα και τους ισχύοντες ειδικούς ποινικούς νόμους». Με την ψήφιση του νόμου αυτού, η Ελλάδα έγινε μία από τις πρώτες χώρες σε ευρωπαϊκό επίπεδο που επιχείρησαν να αντιμετωπίσουν τις νέες εκφάνσεις των ηλεκτρονικών εγκλημάτων και ιδιαίτερα του παράνομου προσπορισμού ξένης περιουσίας μέσω της ηλεκτρονικής απάτης. Το γεγονός αυτό αποκτά ακόμα μεγαλύτερη βαρύτητα αν αναλογιστεί κανείς ότι την εποχή εκείνη, η χώρα μας δεν κατείχε εξέχουσα θέση στην παγκόσμια κλίμακα των τεχνολογικών εξελίξεων και υποδομών.[66]

Με το Ν 4411/2016, η χώρα μας ενσωμάτωσε την Οδηγία 2013/40/ΕΕ για το έγκλημα στον κυβερνοχώρο, ενώ παράλληλα, υπήρξε αναδιατύπωση του αρ. 386Α ΠΚ, στο οποίο προστέθηκαν οι περιπτώσεις της «χωρίς δικαίωμα χρήσης δεδομένων» και της «χωρίς δικαίωμα παρέμβασης σε πληροφοριακό σύστημα» (προς αντικατάσταση της παλαιάς διατύπωσης «επέμβαση κατά την εφαρμογή του προγράμματος»), ενώ αφαιρέθηκε και η παλαιά αόριστη διατύπωση «με οποιονδήποτε άλλο τρόπο». Συνάμα προστέθηκαν στο αρ. 13 ΠΚ οι ορισμοί του «πληροφοριακού συστήματος» και των «ψηφιακών δεδομένων»[67]. Η τροποποίηση αυτή της διάταξης του αρ. 386Α ΠΚ, φάνηκε να επιλύει το, επί πολλά έτη, ζήτημα αντικρουόμενων απόψεων σε θεωρία και νομολογία σχετικά με την ποινικοποίηση της χωρίς δικαίωμα μεταφοράς χρημάτων[68]. Πιο συγκεκριμένα, η αιτιολογική έκθεση του Ν 4411/2016 αναφέρει «κατά τη βούληση του

[65] Βλ. Κουράκης Ν., Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001

[66] Βλ. Σάμιος Θ., Η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων ως τρόπος τελέσεως της απάτης με υπολογιστή (άρθρο 386Α' ΠΚ), 2003

[67] Βλ. Μοροζίνης Ι., Η μεταφορά χρημάτων «χωρίς δικαίωμα» ως προσβολή της περιουσίας, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη, σελ.170 επ.

[68] Βλ. ΑΠ 742/2012, ΑΠ 65/2016, ΑΠ 96/2017

ιστορικού νομοθέτη οποιαδήποτε μεταφορά χρημάτων γίνεται με υποκλοπή και χρήση ξένων (ορθών) κωδικών ή με παράνομη διείσδυση του δράστη στα πληροφοριακά συστήματα τραπεζών ή χρηματιστηριακών εταιρειών συνιστά απάτη με υπολογιστή κατ' άρθρο 386Α ΠΚ».

Όπως αναφέρθηκε και στην περίπτωση της απάτης μέσω υπολογιστή (386 ΠΚ), με βάση τα αρ. 18 ΠΚ και 19 ΠΚ, κριτήριο αξιολόγησης της απάτης με υπολογιστή από πλευράς βαρύτητας σε πλημμέλημα ή κακούργημα (διακεκριμένη μορφή εγκλήματος), θα αποτελέσει σε πρώτο χρόνο το ύψος της ζημιάς που προκαλείται (αν υπερβαίνει τις 120.000 ευρώ τότε αντιμετωπίζεται ως κακούργημα), αλλά σε δεύτερο χρόνο και η ταυτότητα του θύματος για την περαιτέρω διάκριση και αυστηρότερη μεταχείριση των κακουργημάτων.

Κατ' αντιστοιχία, στην περίπτωση που θεωρείται κακούργημα, ο χρόνος παραγραφής ορίζεται στα 20 έτη αν ο αποδέκτης της εγκληματικής ενέργειας είναι το Δημόσιο, ν.π.δ.δ. ή ΟΤΑ, όπως ορίζει και το 386Α §3 ΠΚ, ενώ σε άλλη περίπτωση ο χρόνος ορίζεται στα 15 έτη (111§2 ΠΚ). Στην περίπτωση στοιχειοθέτησης πλημμελήματος ανέρχεται στα 5 έτη, σύμφωνα με το 111§3 ΠΚ.

4.2.1 Αντικειμενική Υπόσταση

Κατά τη θέσπιση του άρθρου 386Α το 1988, γινόταν λόγος για επηρεασμό των στοιχείων υπολογιστή. Σήμερα και σε προσπάθεια της νομικής επιστήμης για συμπόρευση με τις διαρκείς εξελίξεις του τεχνολογικού τομέα, γίνεται αναφορά για πληροφοριακά συστήματα, εννοώντας με τον τρόπο αυτό τόσο τους ίδιους τους ηλεκτρονικούς υπολογιστές ως υλικές συσκευές, τα προγράμματά τους καθώς και τα δίκτυα επικοινωνίας μεταξύ τους.

Υποκείμενο της απάτης με υπολογιστή μπορεί να είναι οποιοσδήποτε («όποιος…»), άρα και η απάτη με υπολογιστή κατατάσσεται στα κοινά και όχι στα ιδιαίτερα εγκλήματα.

Αντικείμενο της πράξης αποτελεί η περιουσία του ατόμου ή των ατόμων αυτών που δέχονται την προσβολή («ξένη περιουσία…»). Ένα βασικό χαρακτηριστικό της απάτης με υπολογιστή είναι ότι η περιουσιακή βλάβη που προκαλείται με την εγκληματική πράξη δεν απαιτείται να ταυτίζεται απαραίτητα με το πρόσωπο ενός θύματος (μπορεί να βλάπτεται η περιουσία μεγάλου ή αγνώστου αριθμού ατόμων). Το

υποκείμενο της απάτης συνήθως ενεργεί όχι για την προσβολή αποκλειστικά ενός θύματος, αλλά ενός ευρύτερου αριθμού ατόμων και για το σκοπό αυτό ως περιουσία είναι ορθότερο να λογίζεται το σύνολο των επί μέρους ζημιών που έχουν προκληθεί ως απόρροια της συγκεκριμένης πράξης του δράστη[69]. Έτσι, η διάκρισή της με βάση το όριο των 120.000 ευρώ δεν πρέπει να προσδιορίζεται με βάση την ατομική περιουσιακή βλάβη, αλλά με βάση τη συνολική, ακόμη κι αν αυτό συνεπάγεται ότι η περιουσιακή ζημιά που έχει υποστεί το καθένα άτομο ξεχωριστά είναι αμελητέα. Για καταδικαστική δε απόφαση, σε αντίθεση με την περίπτωση της κοινής απάτης, αυτή δεν κρίνεται ως αναιτιολόγητη αν δεν αναφέρει συγκεκριμένα το πρόσωπο του θύματος (καθώς αυτό μπορεί να μην είναι καν γνωστό)[70].

Οι πράξεις του δράστη που στοιχειοθετούν την **εγκληματική συμπεριφορά** στην απάτη με υπολογιστή αφορούν στον επηρεασμό των στοιχείων λειτουργίας του ηλεκτρονικού υπολογιστή και μπορούν να αντιπαραβληθούν με την παράπειση του θύματος σε περιουσιακή διάθεση[71] στην περίπτωση της κοινής απάτης του 386 ΠΚ. Βασικό χαρακτηριστικό της εγκληματικής συμπεριφοράς στην απάτη με υπολογιστή είναι ότι η περιουσιακή βλάβη που υπόκειται το θύμα, έρχεται ως επακόλουθο όχι του λανθασμένου από την επεξεργασία αποτελέσματος, αλλά της πλάνης που το τελευταίο του δημιουργεί. Δεν μπορεί να γίνει λόγος για πλάνη ενός υπολογιστικού μηχανήματος, καθώς αυτό εκτελεί τις προγραμματισμένες από το χρήστη του εντολές και δεν είναι αυτό το οποίο θα οδηγήσει το ανυποψίαστο θύμα σε περιουσιακή διάθεση.

Ένα ακόμη βασικό στοιχείο της απάτης με υπολογιστή είναι η σχέση που αναγκαία πρέπει να υφίσταται μεταξύ της βλάβης του θύματος και του οφέλους του υποκειμένου. Έτσι λοιπόν, δεν συντελείται απάτη με υπολογιστή στην περίπτωση κατά την οποία ο δράστης ενεργεί προκαλώντας περιουσιακή βλάβη στο θύμα, από την οποία όμως αυτός δεν αποκομίζει κάποιο οικονομικό όφελος. Παράλληλα δεν στοιχειοθετείται απάτη με υπολογιστή ούτε στην περίπτωση όπου το υποκείμενο αποκτά μέσω επηρεασμού των στοιχείων υπολογιστή πρόσβαση σε διαπιστευτήρια ή κωδικούς

---

[69] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, Άρθρα 385-406 ΠΚ, Εγκλήματα Περιουσιακής μετάθεσης, 2000, εκδ. Σάκκουλα

[70] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 491

[71] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, Άρθρα 385-406 ΠΚ, Εγκλήματα Περιουσιακής μετάθεσης, 2000, εκδ. Σάκκουλα

πρόσβασης του θύματος, τα οποία όμως δεν χρησιμοποιεί εν συνεχεία για την πρόκληση οικονομικής ζημίας.

Ως κατ' εξακολούθηση έγκλημα, όπως ορίζεται και στο 98§2 ΠΚ, αντιμετωπίζεται η απάτη με υπολογιστή (λαμβάνοντας υπόψη αντίστοιχα τη συνολική περιουσιακή ζημία) στις περιπτώσεις εκείνες κατά τις οποίες ο δράστης με τις επιμέρους πράξεις του απόβλεπε στο αποτέλεσμα αυτό[72]. Στις περιπτώσεις αυτές, ο ποινικός χαρακτηρισμός της πράξης θα προσδιοριστεί από τη συνολική αξία της προκληθείσας βλάβης.

4.2.2 Υποκειμενική Υπόσταση

Κατ' αντιστοιχία και με την περίπτωση της κοινής απάτης (ή απάτης μέσω υπολογιστή) του 386 ΠΚ, έτσι και στην απάτη με υπολογιστή προαπαιτούμενο στοιχείο είναι ο δόλος (πρόθεση) από την πλευρά του δράστη. Όπως και η απάτη μέσω υπολογιστή, κατατάσσεται στα εγκλήματα υπερχειλούς υποκειμενικής υπόστασης, καθώς εκτός από την πλήρωση των απαιτούμενων από την α.υ. στοιχείων, απαιτείται και ο πρόσθετος σκοπός του παράνομου προσπορισμού ξένου περιουσιακού οφέλους. Επιπροσθέτως, εξαιτίας της πρόσθετης αυτής επιδίωξης («με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος») ίσως είναι ορθότερο να γίνεται αναφορά αποκλειστικά για άμεσο δόλο α΄ βαθμού (δόλο σκοπού). Έτσι, ένας δράστης ο οποίος προβαίνει π.χ. σε μη ορθή διαμόρφωση ενός προγράμματος η/υ ή παρεμβαίνει χωρίς δικαίωμα σε πληροφοριακό σύστημα, στερούμενος την επιδίωξη για προσπορισμό παρανόμου περιουσιακού οφέλους για τον εαυτό του ή τρίτο, δεν μπορεί να θεωρηθεί ότι πληροί την υ.υ.ε της απάτης με υπολογιστή.

[72] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 495

4.2.3 Οι τρόποι τέλεσης της απάτης με υπολογιστή

Η απάτη με υπολογιστή αποτελεί ένα πολύτροπο ή υπαλλακτικώς μικτό έγκλημα (όσοι τρόποι και να τελεστούν, υπάρχει ένα έγκλημα[73]). Συγκεκριμένα, το άρθρο 386Α ΠΚ προβλέπει 5 συγκεκριμένους τρόπους επέμβασης σε ένα πρόγραμμα με σκοπό τη διεξαγωγή ηλεκτρονικής απάτης, οι οποίοι μπορεί να εφαρμόζονται είτε ξεχωριστά, είτε επικουρικά[74] και αναλύονται στη συνέχεια:

4.2.3.1 Η μη ορθή διαμόρφωση προγράμματος υπολογιστή

Ένα υπολογιστικό πρόγραμμα βασίζεται σε μία σειρά διαδοχικών εντολών, οι οποίες ορίζονται από το δημιουργό του (προγραμματιστή) και τις οποίες ο υπολογιστής εκτελεί πιστά, παράγοντας με τον τρόπο αυτό το επιθυμητό αποτέλεσμα. Η μη ορθή διαμόρφωση προγράμματος εμπεριέχει τόσο την περίπτωση δημιουργίας ενός νέου (ολικά ή μερικά) προγράμματος με τον επηρεασμό ή την αλλοίωση ενός ήδη υπάρχοντος προγράμματος, όσο και την περίπτωση απόκρυψης δεδομένων (holding back)[75]. Και στις δύο περιπτώσεις, η παρέμβαση στην ακολουθία των λογικών βημάτων του προγράμματος έχει ως συνέπεια το αποτέλεσμα που προκύπτει να είναι διαφορετικό από το αρχικά επιδιωκόμενο από τον προγραμματιστή.

Παραδειγματικά μπορεί να αναφερθεί ένα υπολογιστικό πρόγραμμα το οποίο έχει διαμορφωθεί κατά τρόπο τέτοιο, ώστε με κάθε συναλλαγή που πραγματοποιεί ο χρήστης του, να παρακρατεί μεγαλύτερο ποσό από αυτό που υπό φυσιολογικές συνθήκες επιβαρύνει τον πελάτη. Είναι καίριο να αναφερθεί ότι βασικό ρόλο στην αξιολόγηση της ορθότητας και νομιμότητας ή μη ενός προγράμματος, διαδραματίζει η αρχική πρόθεση του προγραμματιστή (δημιουργού του).

---

[73] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 484

[74] Βλ. Κουράκης Ν., Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001

[75] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 485

4.2.3.2 Η χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα

Αυτός ο τρόπος τέλεσης της απάτης με υπολογιστή βρίσκει εφαρμογή με διάφορους τρόπους, μερικοί από τους οποίους είναι οι εξής: με την επέμβαση στα μηχανικά μέρη (π.χ. πληκτρολόγιο ή ποντίκι) του ηλεκτρονικού υπολογιστή (Hardwaremanipulation), με την επεξεργασία των δεδομένων από το πληκτρολόγιο (Konsolmanipulation), με την αθέμιτη εισαγωγή δεδομένων στον υπολογιστή (Inputmanipulation) και με την επέμβαση κατά την εξαγωγή των δεδομένων από τον ηλεκτρονικό υπολογιστή (Outputmanipulation)[76].

Η σειρά των εντολών στα περισσότερα προγράμματα ενός υπολογιστή είναι αυστηρά καθορισμένη. Αυτό πρακτικά σημαίνει ότι η παρέμβαση με τροποποίηση των εντολών του προγράμματος, μπορεί να οδηγήσει είτε στην μη ολοκλήρωσή του, είτε στη δημιουργία ενός νέου, διαφορετικού από το αρχικό, αποτελέσματος.

Ένα παράδειγμα αυτού του τρόπου τέλεσης απάτης είναι η παρέμβαση σε ένα διακομιστή (server) συνδρομητικού τηλεοπτικού καναλιού και η εγκατάσταση σε αυτό ενός προγράμματος, το οποίο θα διαμοιράζει το τηλεοπτικό σήμα σε αριθμό μη εξουσιοδοτημένων συνδρομητών.

4.2.3.3 Η χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας

Σύμφωνα με το αρ. 13§ζ' ΠΚ, «ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μία λειτουργία». Παρόλο που δεν ορίζεται ρητά στο νόμο, είναι γενικά αποδεκτό, ότι ως «μη ορθά» χαρακτηρίζονται τα δεδομένα εκείνα στα οποία η πληροφορία που εμπεριέχεται δεν αντικατοπτρίζει καθόλου την πραγματικότητα, ενώ ως «ελλιπή» εκείνα, που δεν την εκφράζουν πλήρως, καθώς παραλείπονται επιμέρους κρίσιμες δηλώσεις, οι οποίες ενδεχομένως να επηρεάζουν τη συνολική σύλληψη της πραγματικότητας. Έτσι ως μη ορθά θεωρούνται τα δεδομένα που εισάγονται σε έναν υπολογιστή και προσδίδουν στο χρήστη τη φοιτητική ιδιότητα (χωρίς

[76] Βλ. Σάμιος Θ., Η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων ως τρόπος τελέσεως της απάτης με υπολογιστή (άρθρο 386Α' ΠΚ), 2003.

αυτό να ισχύει στην πραγματικότητα), ενώ ως ελλιπή θεωρείται η μη ενημέρωση του υπολογιστικού συστήματος για τη λήξη της φοιτητικής ιδιότητας ενός, μέχρι πρότινος, δικαιούχου. Τα στοιχεία πρέπει να αναφέρονται σε αντικειμενικά γεγονότα και όχι σε προσωπικές κρίσεις ή εκτιμήσεις, ενώ θα πρέπει τα ίδια να οδηγούν σε δημιουργία ψευδών παραστάσεων[77].

Ο όρος της χρησιμοποίησης δεδομένων δεν αναφέρεται αποκλειστικά στην άμεση εισαγωγή και εγγραφή από την πλευρά του δράστη σε έναν υπολογιστή των μη ορθών ή ελλιπών δεδομένων, αλλά αφορά και στην τροφοδοσία-αποστολή αυτών, με σκοπό όταν αυτά γίνουν αντικείμενο επεξεργασίας, να επηρεάσουν την ομαλή λειτουργία ενός προγράμματος του υπολογιστή και να οδηγηθεί με αυτόν τον τρόπο το ανυποψίαστο θύμα σε περιουσιακή διάθεση[78].

Είναι νομικά αδιάφορο αν η παρέμβαση με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων πραγματοποιείται σε μία διαδικασία η οποία ήδη βρίσκεται σε εξέλιξη ή αν αυτό συμβαίνει πριν ξεκινήσει η διεργασία.

Κριτήριο τόσο για την ορθότητα όσο και για την πληρότητα των στοιχείων ενός προγράμματος αποτελεί το κατά πόσο η απεικόνιση μιας πληροφορίας στον ηλεκτρονικό υπολογιστή συνάδει με την αποτύπωσή της στον κώδικα εντολών ενός συγκεκριμένου προγράμματος. Επομένως, η ορθότητα και η πληρότητα των δεδομένων εξαρτάται από την ορθότητα και πληρότητα αντίστοιχα, της κωδικοποιημένης πληροφορίας.

4.2.3.4 Η χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης της ταυτότητας

Σύμφωνα με τη συνήθη διατύπωση της νομολογίας ο όρος «χωρίς δικαίωμα» χρησιμοποιείται για να περιγράψει κάτι που λαμβάνει χώρα «χωρίς τη συναίνεση του ιδιοκτήτη ή χωρίς την ύπαρξη άλλου νόμιμου δικαιολογητικού λόγου». Εξειδικεύοντας την άποψη αυτή της πάγια νομολογίας στην υποπερίπτωση του αρ. 386Α, καταλήγουμε

[77] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, Άρθρα 385-406 ΠΚ, Εγκλήματα Περιουσιακής μετάθεσης, 2000, εκδ. Σάκκουλα

[78] Βλ. Μπουρμάς Γ., Στοιχεία Απάτης με ΗΥ κατ' άρθρο 386Α ΠΚ και διάκριση από την Κοινή Απάτη του 386 ΠΚ, 2001.

ότι «η χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή» είναι αυτή που πραγματοποιείται «χωρίς τη συναίνεση του νόμιμου δικαιούχου ή χωρίς την ύπαρξη άλλου δικαιώματος που παρέχει στο δράστη ο νόμος (είτε πηγάζει από τον ίδιο το νόμο, από σύμβαση ή από τη βούληση/συγκατάθεση του δικαιούχου)»[79].

Σε πολλές από τις περιπτώσεις που κατά καιρούς έχουν απασχολήσει τη νομολογία, γεννάται το εξής ερώτημα: ποια είναι η ποινική αξιολόγηση στην περίπτωση κατά την οποία ο δράστης έχοντας αποκτήσει με νόμιμο τρόπο τα διαπιστευτήρια του χρήστη, προβαίνει σε ενέργειες τις οποίες ο δικαιούχος δεν εγκρίνει. Σύμφωνα όσα αναφέρθηκαν παραπάνω σχετικά με τη διατύπωση του όρου «χωρίς δικαίωμα», αυτή δεν αναφέρεται αποκλειστικά στον τρόπο απόκτησης του username και password του χρήστη. Αντιθέτως, επεκτείνεται και καλύπτει και όλες τις μετέπειτα ενέργειες στις οποίες αυτός προβαίνει. Έτσι, χωρίς δικαίωμα εξακολουθεί να πράττει ο δράστης ο οποίος έχει αποκτήσει μεν με σύννομο τρόπο τα διαπιστευτήρια του δικαιούχου, αλλά τα χρησιμοποιεί κατά τρόπο αντίθετο με τη βούληση ή τα συμφέροντα αυτού. Το έγκλημα που διαπράττεται και σε αυτήν την περίπτωση δεν είναι άλλο από εκείνο της απάτης με υπολογιστή του αρ. 386Α ΠΚ.

Υπάρχουν δύο τρόποι με τους οποίους ένας κακόβουλος χρήστης μπορεί να εξασφαλίσει παράνομη πρόσβαση στα δεδομένα ενός υπολογιστή[80]

- Όταν τα δεδομένα διαβιβάζονται στο διαδίκτυο μεταξύ υπολογιστών

Η περίπτωση αυτή, ποινικά θα μπορούσε να αξιολογηθεί ως παραβίαση του απορρήτου της επικοινωνίας (370 ΠΚ), αφού ο χρήστης ουσιαστικά αποκτά αθέμιτη πρόσβαση παρεμβαίνοντας στο περιεχόμενο της επικοινωνίας μεταξύ των ανταποκριτών.

- Όταν ο χρήστης αποκτήσει πρόσβαση στον ηλεκτρονικό υπολογιστή και κατ' επέκταση και στο σύνολο των δεδομένων που είναι αποθηκευμένα στην μνήμη του υπολογιστή ή σε περιφερειακή μνήμη αυτού.

Στην περίπτωση αυτή, η παράνομη εισχώρηση στα δεδομένα που βρίσκονται αποθηκευμένα στον ηλεκτρονικό υπολογιστή, εμφανίζει αρκετές ομοιότητες με τη διατάραξη της οικιακής ειρήνης του 334 ΠΚ. Κατά αντιστοιχία με την «κλασική» μορφή

[79] Βλ. Μοροζίνης Ι., Η μεταφορά χρημάτων «χωρίς δικαίωμα» ως προσβολή της περιουσίας, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη, σελ.174 επ.

[80] Βλ. Κιούπης Δ., Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, 2000

του εγκλήματος, έτσι και στον ηλεκτρονικό χώρο, ο δράστης παράνομα εισέρχεται στον «προσωπικό» ιδιωτικό χώρο του θύματος (περικλεισμένος χώρος που αυτός κατέχει) ή στον οποίο αυτός μπορεί να χρησιμοποιεί για την εργασία του.

Σε αυτόν τον τρόπο απάτης με υπολογιστή υπάγεται η περίπτωση της ανάληψης χρημάτων από ΑΤΜ με κλεμμένη μαγνητική κάρτα, καθώς και η περίπτωση του skimming που θα αναφερθεί στη συνέχεια.

4.2.3.5 Η χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας

Η διείσδυση της επιστήμης των ηλεκτρονικών υπολογιστών και του διαδικτύου στον οικονομικό τομέα στις αρχές της δεκαετίας του 1970, εισήγαγε τον όρο του internet banking (ηλεκτρονική τραπεζική), ενώ αποτέλεσε σημείο αναφοράς στην εξέλιξη των τραπεζικών συναλλαγών και στη διαμόρφωση της κατάστασης όπως τη γνωρίζουμε σήμερα. Αρχικά η δυνατότητα της απομακρυσμένης διαχείρισης των τραπεζικών λογαριασμών παρεχόταν μέσω των Αυτόματων Ταμειολογιστικών Μηχανημάτων (ΑΤΜ), τα οποία συνδέονταν διαδικτυακά με το κεντρικό υπολογιστικό σύστημα της κάθε τράπεζας, ενημερώνοντάς το σε πραγματικό χρόνο για κάθε μεταβολή που πραγματοποιούταν στο λογαριασμό του κάθε χρήστη. Με την πάροδο του χρόνου, αυτό κατέστη δυνατό τόσο μέσω δημιουργίας διαδικτυακών ιστοτόπων, στους οποίους ο καθένας μπορεί να αποκτήσει πρόσβαση με τα προσωπικά του διαπιστευτήρια, όσο και με την ανάπτυξη εφαρμογών λογισμικού προορισμένων για τις φορητές συσκευές (smartphones, tablets, laptops).

Με την προσθήκη στο άρθρο 386Α ΠΚ της υποπερίπτωσης αυτής, ο νομοθέτης κατέστησε πλέον σαφές ότι η πρακτική της παράνομης μεταφοράς χρημάτων μέσω λογισμικού σε ηλεκτρονικό περιβάλλον (web banking) συνιστά περίπτωση απάτης με υπολογιστή, αίροντας με τον τρόπο αυτό παλαιότερες αντικρουόμενες απόψεις της νομολογίας σχετικά με το αν αυτή πρέπει να αντιμετωπισθεί ως περίπτωση κλοπής ή απάτης.

4.2.4 Ο τόπος και ο χρόνος τέλεσης της απάτης με υπολογιστή

Το άρθρο 16 του Νέου Ποινικού Κώδικα ορίζει ότι: «Τόπος τέλεσης της πράξης θεωρείται ο τόπος, όπου ο υπαίτιος διέπραξε ολικά ή μερικά την αξιόποινη ενέργεια ή παράλειψη, καθώς και ο τόπος όπου επήλθε ή, σε περίπτωση απόπειρας, έπρεπε σύμφωνα με την πρόθεση του υπαιτίου να επέλθει το αξιόποινο αποτέλεσμα».

Όπως ισχύει και με την πλειοψηφία των εγκλημάτων του κυβερνοχώρου, έτσι και η ηλεκτρονική απάτη χαρακτηρίζεται συνήθως από την φυσική απόσταση μεταξύ δράστη και θύματος, γεγονός που δυσχεραίνει τον ακριβή προσδιορισμό του τόπου τέλεσης της αξιόποινης πράξης. Σύμφωνα με την κρατούσα και ορθότερη άποψη, ως τόπος τέλεσης ενός ηλεκτρονικού εγκλήματος θα πρέπει να θεωρηθεί τόσο ο τόπος στον οποίο ενήργησε ο δράστης, όσο και αυτός/-οί όπου επήλθε/-αν τα αποτελέσματα των πράξεών του. Αντίστοιχα, στην κατ' εξακολούθηση απάτη, θα πρέπει να συνυπολογιστούν και όλοι οι επιμέρους τοποθεσίες στις οποίες ενήργησε ο δράστης.

Αναφορικά με το χρόνο τέλεσης της απάτης με υπολογιστή, σύμφωνα με το 17 ΠΚ, αυτός ορίζεται ως τη χρονική στιγμή κατά την οποία ο δράστης ενήργησε την εγκληματική του συμπεριφορά, ενώ ο χρόνος κατά τον οποίο επήλθε το αποτέλεσμα είναι αδιάφορος. Όπως αναφέρθηκε προηγουμένως, στην ηλεκτρονική απάτη δεν απαιτείται οι ενέργειες του δράστη, η εξαπάτηση του θύματος και η πράξη της περιουσιακής μεταβίβασης να συμπίπτουν χρονικά. Ως εκ τούτου, ορθότερο είναι ως χρόνος τέλεσης της απάτης να θεωρείται αποκλειστικά ο χρόνος ολοκλήρωσης των ενεργειών του δράστη, υπό την προϋπόθεση φυσικά να έχει επέλθει και η ουσιαστική αποπεράτωση του εγκλήματος, καθώς χωρίς αυτή, δε νοείται έγκλημα.

4.3 Η διάκριση της απάτης μέσω υπολογιστή από την απάτη με υπολογιστή - Ομοιότητες και διαφορές των Άρθρων 386 ΠΚ και 386Α ΠΚ

Τόσο η κοινή απάτη του Άρθρου 386, όσο και η ηλεκτρονική απάτη του Άρθρου 386Α, αποτελούν εγκλήματα βλάβης της περιουσίας. Και στις δύο ανωτέρω μορφές, ο δράστης αποσκοπεί είτε στον προσπορισμό παρανόμου περιουσιακού οφέλους για τον ίδιο ή άλλο πρόσωπο, είτε στην πρόκληση περιουσιακής βλάβης στο ανυποψίαστο θύμα.

Μία ακόμα ομοιότητα των δύο μορφών απάτης έγκειται στην υπαιτιότητα του δράστη. Όπως αναφέρθηκε προηγουμένως, τόσο στην περίπτωση της κοινής απάτης του άρθρου 386 (με σκοπό από τη βλάβη αυτή…), όσο και στην απάτη με υπολογιστή του άρθρου 386Α ΠΚ (με σκοπό να προσπορίσει…), απαιτείται από το δράστη η ύπαρξη του στοιχείου του δόλου. Ο δόλος που απαιτείται για τη στοιχειοθέτηση της υ.υ.ε είναι άμεσος δόλος α' βαθμού (δόλος σκοπού), αφού ο δράστης έχει πλήρες γνωστικό (γνώση από πλευράς του των στοιχείων που απαρτίζουν την α.υ.ε), καθώς και πλήρες βουλητικό στοιχείο (αποδοχή από πλευράς του της πλήρωσης της α.υ.ε).

Στο Ελληνικό Δίκαιο, οι διατάξεις των άρθρων περί κοινής και ηλεκτρονικής απάτης, έχουν κοινές εννοιολογικές ρίζες και ο νομοθέτης επιβάλλει σε αυτές κοινό πλαίσιο ποινών, τουλάχιστον 3 μηνών φυλάκιση παράλληλα με χρηματική ποινή. Παράλληλα, και τα δύο άρθρα προβλέπουν και περιπτώσεις τέλεσης διακεκριμένων εγκλημάτων, εάν το συνολικό ποσό της προκληθείσας ζημίας υπερβαίνει τα 120.000 ευρώ ή/ και αν αυτά τελούνται εις βάρος του δημοσίου, ν.π.δ.δ. και ΟΤΑ[81]. Ωστόσο, η ηλεκτρονική απάτη πρέπει να αντιμετωπίζεται ως ένα ιδιώνυμο (sui generis) έγκλημα και όχι ως μία ειδικότερη μορφή της κοινής απάτης[82].

Η βασική διαφορά μεταξύ των δύο άρθρων, η οποία και τόνισε την ανάγκη διάκρισής τους και ως εκ τούτου επέβαλλε την προσθήκη του άρθρου 386Α στον ΠΚ, αφορά σε ένα από τα βασικά στοιχεία του εγκλήματος, την πράξη. Η ΑΠ 1152/1999 αποτέλεσε μία από τις πρώτες αποφάσεις στο ελληνικό Ποινικό Δίκαιο που έθιξαν το θέμα της διάκρισης της κοινής απάτης του άρθρου 386 ΠΚ, από την αντίστοιχη παρεμφερή διάταξη του άρθρου 386Α[83].

Το 386 ΠΚ προϋποθέτει την άμεση εξαπάτηση ενός φυσικού προσώπου («πείθοντας κάποιον») προς δημιουργία περιουσιακής βλάβης σε αυτό. Αντιθέτως, στην περίπτωση της απάτης με υπολογιστή, η «θετική» ενέργεια από την πλευρά του δράστη συνίσταται στην αθέμιτη παρέμβαση σε κάποιο πρόγραμμα ή στη διαδικασία

[81] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ.483

[82] Βλ. Κουράκης Ν., Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001, αλλά και Αδ. Παπαδαμάκης, «Τα περιουσιακά Εγκλήματα. Άρθρα 385-406 ΠΚ», σελ.82, 2000, εκδ. Σάκκουλα

[83] Βλ. Μπουρμάς Γ., Στοιχεία Απάτης με ΗΥ κατ' άρθρο 386Α ΠΚ και διάκριση από την Κοινή Απάτη του 386 ΠΚ, 2001

επεξεργασίας των δεδομένων ενός ηλεκτρονικού υπολογιστή, επιδιώκοντας να προκαλέσει διαφορετικό αποτέλεσμα από εκείνο που θα πρόκυπτε υπό φυσιολογικές συνθήκες και αν δεν είχε λάβει χώρα η εν λόγω παρέμβαση,[84], με την περιουσιακή ζημία να έρχεται ως φυσικό επακόλουθο της πράξης αυτής. Έτσι λοιπόν, ο δηλωτικός όρος της πλάνης «πείθοντας κάποιον», έχει αντικατασταθεί με τον όρο «επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή», στον οποίο εκτός από την πράξη εξαπάτησης, συμπεριλαμβάνεται και το άμεσο αποτέλεσμα (η πλάνη), αλλά και το αποτέλεσμα της πλάνης (η περιουσιακή διάθεση)[85]. Για το λόγο αυτό, η απάτη με υπολογιστή δεν αποτελεί ειδικότερή μορφή απάτης, αλλά ένα ιδιώνυμο (sui generis) έγκλημα[86]. Απεναντίας, θεωρείται ότι στοιχειοθετείται κοινή απάτη του άρθρου 386 ΠΚ στις περιπτώσεις εκείνες όπου ο υπολογιστής χρησιμοποιείται ως μέσο (όργανο), με την πληκτρολόγηση μη ορθών ποσών, προς παραπλάνηση τρίτου, ο οποίος και προβαίνει με πράξη, παράλειψη ή ανοχή σε περιουσιακή διάθεση και βλάβη εκ μέρους του. Βασική αναφορά που πρέπει να γίνει είναι ότι για τη στοιχειοθέτηση απλής απάτης, πρέπει να μην πραγματοποιείται επέμβαση στη διαμόρφωση του προγράμματος ή στην εφαρμογή του.

Σύμφωνα με τα παραπάνω και όπως προαναφέρθηκε προηγουμένως, η απάτη μέσω υπολογιστή αποτελεί μία μορφή «μη γνήσιου» κυβερνοεγκλήματος, καθώς αποτελεί ένα συμβατικό έγκλημα το οποίο όμως μπορεί να τελεστεί και με τη χρήση ενός ηλεκτρονικού υπολογιστή. Αντιθέτως, απαραίτητο στοιχείο της απάτης με υπολογιστή είναι η ύπαρξη ενός (τουλάχιστον) πληροφοριακού συστήματος ή δικτύου επικοινωνιών εναντίον ή με τη χρήση του οποίου αυτή τελείται, αποτελώντας έτσι ένα «γνήσιο» κυβερνοέγκλημα[87].

Βασική προϋπόθεση για να χαρακτηριστεί η καταδικαστική απόφαση αιτιολογημένη στην περίπτωση της απάτης μέσω υπολογιστή, είναι ο προσδιορισμός του

---

[84] Βλ. ΤρΕφΚακΑθ 4689/2018

[85] Βλ. Μπουρμάς Γ., Στοιχεία Απάτης με ΗΥ κατ' άρθρο 386Α ΠΚ και διάκριση από την Κοινή Απάτη του 386 ΠΚ, 2001

[86] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, Άρθρα 385-406 ΠΚ, Εγκλήματα Περιουσιακής μετάθεσης, 2000, εκδ. Σάκκουλα

[87] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 482-483

προσώπου του παθόντος, το οποίο πρέπει να είναι γνωστό, κάτι το οποίο δεν απαιτείται για την περίπτωση της απάτης με υπολογιστή[88].

Τέλος, αντιπαραβάλλοντας τα δύο αυτά άρθρα του νέου ΠΚ, διαπιστώνουμε ότι στην περίπτωση της απάτης με υπολογιστή του 386Α ΠΚ, υπάρχει διεύρυνση του αξιόποινου (§2), περιλαμβάνοντας και τις περιπτώσεις εκείνες κατά τις οποίες ένα άτομο προβαίνει στην κατασκευή, διάθεση ή κατοχή προγράμματος ή πληροφοριακού συστήματος για τη διάπραξη του υπόψη εγκλήματος, χωρίς να απαιτείται η χρησιμοποίηση από πλευράς του.

[88] Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη, σελ. 491

5 Σύγχρονες μορφές ηλεκτρονικής απάτης

5.1 Το φαινόμενο «Phishing»

Το phishing χαρακτηρίζεται ως μία ιδιάζουσα μορφή ηλεκτρονικής απάτης, η οποία μάλιστα έχει επεκταθεί σε τέτοιο βαθμό, ώστε να αποτελεί μία από τις συνηθέστερες εκφάνσεις της σήμερα, ενώ έχει απασχολήσει και εξακολουθεί να απασχολεί καθημερινά τις Αρχές σε Παγκόσμιο Επίπεδο. Αναφορικά με την προέλευση του όρου «phishing» έχουν διατυπωθεί διάφορες απόψεις. Σύμφωνα με την επικρατέστερη από αυτές, αποτελεί ένα συνδυασμό των λέξεων «fishing» (=ψάρεμα) και «phreaking» (=η τεχνική της παράνομης διείσδυσης σε τηλεπικοινωνιακά δίκτυα).

Κατά το φαινόμενο αυτό, ο δράστης, αποκρύπτοντας τα στοιχεία της ταυτότητάς του και υποδυόμενος κάποιον άλλον (συνήθως τραπεζικό οργανισμό, γνωστή επιχείρηση, ακόμα και κάποιο οικείο πρόσωπο του θύματος), προβαίνει στην αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails) ή κινητής τηλεφωνίας (SMS[89]), σε ανυποψίαστους χρήστες, με σκοπό την απόκτηση πρόσβασης σε εμπιστευτικές γι' αυτούς πληροφορίες. Οι πληροφορίες αυτές συνήθως σχετίζονται με κωδικούς πρόσβασης σε ηλεκτρονικούς τραπεζικούς λογαριασμούς του θύματος, διαπιστευτήρια (όνομα χρήστη και κωδικούς πρόσβασης) διαφόρων λογαριασμών ή κωδικούς PIN (Personal Identification Number – Προσωπικούς Αριθμούς Αναγνώρισης).

Το χαρακτηριστικότερο παράδειγμα μίας μορφής phishing απάτης είναι όταν κάποιος δέχεται ένα μήνυμα ηλεκτρονικού ταχυδρομείου, στο οποίο ο αποστολέας εμφανίζεται ως κάποιο τραπεζικό ίδρυμα. Παράλληλα η δομή του e-mail είναι τέτοια, που ενσωματώνει γραφικά και σχήματα, τα οποία μιμούνται το λογότυπο της τράπεζας προκειμένου να γίνονται περισσότερο πιστευτά από το χρήστη. Το περιεχόμενο του e-mail, συνήθως προειδοποιεί τους παραλήπτες ότι υπάρχει κάποιο πρόβλημα με τον τραπεζικό τους λογαριασμό ή ότι κάποιος αναρμόδιος έχει αποκτήσει πρόσβαση σε αυτόν και τους συνιστούν να πραγματοποιήσουν άμεσα είσοδο για να αποκαταστήσουν το πρόβλημα. Μάλιστα, στο τέλος του μηνύματος παρέχεται και ένας υπερσύνδεσμος (link), τον οποίο μόλις πατήσει το θύμα, μεταφέρεται σε ένα εικονικό περιβάλλον που προσομοιάζει σε μεγάλο βαθμό αυτό της τράπεζας.

[89] Short Message Service

Στην περίπτωση ενός phishing e-mail, η ηλεκτρονική απάτη συνήθως υλοποιείται με δύο τρόπους. Αρχικά, ο χρήστης πατώντας στον υπερσύνδεσμο που ο αποστολέας του παρέχει, άθελά του μπορεί να εγκαταστήσει κάποιο πρόγραμμα (συνήθως ιό ή δούρειο ίππο), το οποίο με τη σειρά του λειτουργώντας στο παρασκήνιο, θα συλλέγει πληροφορίες από τη δραστηριότητα του χρήστη ή και από τις υπόλοιπες συσκευές που είναι συνδεδεμένες στο δίκτυό του, τις οποίες και εν συνεχεία θα προωθεί στον κακόβουλο δράστη. Μέσω του προγράμματος αυτού επίσης παρέχεται η δυνατότητα στον τελευταίο να αποκτήσει ευκολότερα πρόσβαση στα αρχεία του χρήστη από τα οποία μπορεί είτε να υποκλέψει πληροφορίες, είτε να πραγματοποιήσει μια ransomware επίθεση[90].

Ακόμη, μόλις ο χρήστης επιλέξει τον υπερσύνδεσμο που ο αποστολέας έχει τοποθετήσει στο ηλεκτρονικό μήνυμα και μεταφερθεί στον υποτιθέμενο ιστότοπο της τράπεζας, του ζητείται να εισάγει τα ατομικά του διαπιστευτήρια, τα οποία φυσικά και δεν του παρέχουν πρόσβαση στο λογαριασμό του, αλλά αντιθέτως μεταφέρονται στο δράστη. Στο χρήστη μπορεί στη συνέχεια να εμφανιστεί κάποιο μήνυμα αδυναμίας πρόσβασης ή να τον ανακατευθύνουν σε κάποια άλλη ιστοσελίδα.

Οι phishers δρουν συνήθως μεμονωμένα και ανεξάρτητα, χωρίς όμως ωστόσο να αποκλείεται και η κοινή δράση αυτών μέσα από τη δημιουργία μικρών ομάδων. Σε αντίθεση με τις περισσότερες μορφές ηλεκτρονικών επιθέσεων, οι οποίες αποσκοπούν στην καταστροφή, νόθευση ή υποκλοπή εγγράφων και δεδομένων από τους ηλεκτρονικούς υπολογιστές ή κινητά τηλέφωνα των θυμάτων, η τεχνική του phishing επιδιώκει με έναν έμμεσο τρόπο τον προσπορισμό περιουσιακού οφέλους του δράστη εις βάρος του θύματος.

Αρκετές φορές, οι επιτιθέμενοι εκμεταλλεύονται ορισμένες συγκυρίες προκειμένου να προσθέσουν ένα τόνο πειστικότητας στα e-mails με τα οποία προσπαθούν να εξαπατήσουν τους χρήστες. Αυτές μπορεί να αφορούν στην χρονική περίοδο που στέλνονται τα e-mails (π.χ. εορτές, περίοδος οικονομικής αστάθειας – κρίσεων, κλιματικών αλλαγών ή και παγκοσμίων εντάσεων), καθώς επίσης και την απειρία σχετικά με τον κυβερνοχώρο που χαρακτηρίζει ένα μεγάλο μέρος των χρηστών του διαδικτύου.

[90] https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

Το φαινόμενο του phishing σήμερα έχει πάρει τέτοια έκταση, που σύμφωνα με στατιστική έρευνα της AAG[91] (εταιρεία παροχής τηλεπικοινωνιακών υπηρεσιών), περίπου 3,4 δισεκατομμύρια ανεπιθύμητα (spam) e-mails αποστέλλονται καθημερινά σε παγκόσμιο επίπεδο, ενώ στην ίδια κατηγορία άνηκε και το 48% του συνόλου των e-mails που στάλθηκαν το 2022. Παρά τις σημαντικές προσπάθειες οργανισμών όπως η Google, η οποία καταφέρνει να περιορίσει το 99,9% των spam e-mails που διακινούνται, κάθε phishing επίθεση προκαλεί κατά μέσο όρο 136 $ ζημιά σε κάθε θύμα[92].

5.1.1 Ποινική Αξιολόγηση του Phishing

Η τεχνική του phishing, της παράστασης δηλαδή ψευδών γεγονότων ως αληθινών με σκοπό την απόκτηση περιουσιακού οφέλους εις βάρος του θύματος, θα μπορούσε να υπαχθεί στην πρώτη περίπτωση της τέλεσης απάτης μέσω υπολογιστή του 386 ΠΚ (εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών). Ο δράστης παρουσιάζει στο θύμα ένα ψευδές γεγονός (π.χ. ότι ο λογαριασμός του έχει υποστεί διαδικτυακή προσβολή ή ότι ακολουθώντας έναν εσφαλμένο υπερσύνδεσμο θα μπορέσει να δωρίσει χρήματα υπέρ των πληγέντων από φυσικές καταστροφές) με σκοπό (άμεσος δόλος α' βαθμού) το τελευταίο να σχηματίσει αναληθή εικόνα και να προβεί σε περιουσιακή διάθεση (βλάπτει ξένη περιουσία).

Προκειμένου να μπορέσει το phishing να αξιολογηθεί ποινικά ως απάτη, απαραίτητο στοιχείο της αντικειμενικής υπόστασης είναι η παραπλάνηση που το θύμα πρέπει να έχει υποστεί ως συνέπεια των ψεύτικων γεγονότων που ο δράστης του έχει παρουσιάσει. Επομένως, δεν μπορεί να χαρακτηριστεί ως απάτη μέσω υπολογιστή η περίπτωση κατά την οποία κάποιος στέλνει ένα phishing e-mail, το οποίο όμως δεν επιτυγχάνει τον επιδιωκόμενο σκοπό του, δηλ. δεν τον πείθει για το περιεχόμενό του ή διαγράφεται από τον παραλήπτη, χωρίς αυτός να προβεί σε κάποια περαιτέρω ενέργεια.

Το τελευταίο στοιχείο της εγκληματικής συμπεριφοράς που πρέπει να εξετασθεί είναι η βλάβη της περιουσίας. Στο 386 ΠΚ γίνεται αναφορά για βλάβη ξένης περιουσίας «πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή». Στην περίπτωση του phishing, δεν υπάρχει αυτή η αμεσότητα από πλευράς του θύματος, αλλά παρεμβάλλεται μία ακόμη

[91] https://aag-it.com/the-latest-phishing-statistics/

[92] Σύμφωνα με μελέτη της AAG η οποία αφορά το έτος 2021

ενέργεια, αυτή του διαμοιρασμού των προσωπικών διαπιστευτηρίων με το δράστη. Ο τελευταίος στη συνέχεια με δική του θετική ενέργεια είναι αυτός που προβαίνει στην περιουσιακή μεταβίβαση, η οποία τελικά επέρχεται με έμμεσο τρόπο.

Πρέπει ακόμη να διευκρινισθεί ότι δεν αρκεί το θύμα να υπόκειται περιουσιακή ζημία, αλλά πρέπει αυτή να επέρχεται ως αποτέλεσμα της προηγούμενης παραπλανητικής συμπεριφοράς του δράστη. Έτσι, ένας χρήστης του διαδικτύου ο οποίος άθελά του αποκαλύπτει τα προσωπικά του στοιχεία σε κάποιο τρίτο, ο οποίος και του υποκλέπτει ορισμένο χρηματικό ποσό, δεν μπορεί να χαρακτηρισθεί ως απάτη.

Διχογνωμία επικρατεί σχετικά με το αν και κατά πόσο η αντικατάσταση της άμεσης περιουσιακής διάθεσης (από την πλευρά του θύματος που προβλέπει το 386 ΠΚ) με την έμμεση (η οποία ολοκληρώνεται από την πλευρά του δράστη στην περίπτωση του phishing), μεταβάλλει την α.υ. του εγκλήματος κατά τέτοιο βαθμό, ώστε να το καθιστά ιδιώνυμο έγκλημα (sui generis), το οποίο δε θα μπορεί να ποινικοποιείται με τη συγκεκριμένη διάταξη[93].

Κατά μία άποψη, το phishing δεν θα πρέπει να αντιμετωπίζεται σαν μία μορφή απάτης μέσω υπολογιστή για τους κάτωθι λόγους:

- Η αποκάλυψη των διαπιστευτηρίων ενός ατόμου σε κακόβουλο τρίτο, δεν συνεπάγεται υποχρεωτικά και ότι ο τελευταίος θα τα αξιοποιήσει προκειμένου να αποκτήσει περιουσιακό όφελος εις βάρος του ανυποψίαστου ατόμου. Συνεπώς, ένας χρήστης που πείθεται για το αναληθές περιεχόμενο ενός μηνύματος και επισκέπτεται μία ψεύτικη τραπεζική ιστοσελίδα διαμοιράζοντας τα προσωπικά του διαπιστευτήρια στον κακόβουλο χρήστη, χωρίς ωστόσο ο τελευταίος να προβαίνει σε κάποια περαιτέρω ενέργεια περιουσιακής μετάθεσης, δεν πληροί την α.υ.ε της απάτης του 386 ΠΚ και επομένως δεν στοιχειοθετείται το υπόψη έγκλημα.
- Το phishing θα μπορούσε να αντιμετωπισθεί ως μία σύνθετη ενέργεια, η οποία περιλαμβάνει περισσότερες από μία πράξεις. Αρχικά έχουμε την παραπλάνηση του θύματος η οποία οδηγεί σε αποκάλυψη των προσωπικών του στοιχείων στο δράστη. Στη συνέχεια, η ενέργεια στην οποία θα προβεί ο κακόβουλος τρίτος (η υπεξαίρεση δηλαδή του χρηματικού ποσού με δική του θετική ενέργεια) αποτελεί μία ξεχωριστή, αυτοτελής αξιόποινη πράξη, η οποία όμως δεν πρέπει να συγχέεται με την απάτη,

[93] Βλ. Βασιλάκη Ε., Τα φαινόμενα phishing και pharming και η ποινική τους αξιολόγηση, ΠοινΧρ ΝΖ/2007

καθόσον αν συνέβαινε κάτι τέτοιο, θα υπήρχε ο κίνδυνος της επικίνδυνης διεύρυνσης του αξιόποινού της.

- Η «κλασική» απάτη του 386 ΠΚ, συνιστά ένα έγκλημα βλάβης, δηλαδή η πλήρωση της α.υ.ε. συνεπάγεται τη βλάβη της περιουσίας του θύματος (εννόμου αγαθού). Αν αντιθέτως θεωρηθεί ως απάτη η παραπλάνηση του αποδέκτη ενός phishing e-mail και ποινικοποιηθεί με το σχετικό άρθρο, τότε η απάτη μετατρέπεται από έγκλημα βλάβης, σε έγκλημα διακινδύνευσης. Δηλαδή η α.υ.ε θα πληρούται απλά και μόνο με την πρόκληση της επικίνδυνης κατάστασης και όχι με την επέλευση της προσβολής του εννόμου αγαθού.

Κατά άλλη άποψη που υποστηρίζει το αντίθετο, το ότι δηλαδή η περίπτωση του phishing συνιστά μια μορφή απάτης προτείνονται τα κάτωθι επιχειρήματα:

- Ένα θύμα το οποίο εν αγνοία του προβαίνει στο διαμοιρασμό των προσωπικών του διαπιστευτηρίων σε κάποιον κακόβουλο τρίτο, διατρέχει διαρκώς τον κίνδυνο να υποστεί περιουσιακή ζημία, καθώς οποιαδήποτε στιγμή ο δράστης μπορεί να προβεί σε υπεξαίρεση ενός χρηματικού ποσού.
- Οι περιπτώσεις κατά τις οποίες ο δράστης δε προβαίνει σε χρηματική λεηλάτηση του χρηματικού λογαριασμού του θύματος είναι στην πράξη ελάχιστες, ίσως και μηδαμινές και για το λόγο αυτό πρέπει να θεωρείται ότι η βλάβη του εννόμου αγαθού της ιδιωτικής περιουσίας σχεδόν βέβαια έπεται της υποκλοπής των προσωπικών στοιχείων.
- Παρόλο που απαιτείται η σύμπραξη περισσοτέρων του ενός ατόμων για την αποπεράτωση της περιουσιακής διάθεσης, η τελευταία αποτελεί μία μορφή «πολύπρακτης περιουσιακής διάθεσης»[94] η οποία όμως δεν «στερεί» από την συμπεριφορά το χαρακτήρα της απάτης.

Αποτελεί γεγονός ότι στην πράξη η υποκλοπή των διαπιστευτηρίων ενός χρήστη, σχεδόν στο σύνολο των περιπτώσεων θα οδηγήσει σε ουσιαστική αποπεράτωση του εγκλήματος με την προσβολή ξένης περιουσίας. Ακόμα και στην περίπτωση κατά την οποία η αποπεράτωση αυτή δεν επέλθει άμεσα, δηλαδή ο δράστης δεν αποκτήσει αμέσως πρόσβαση στον τραπεζικό λογαριασμό του θύματος για να πραγματοποιήσει την μεταφορά του χρηματικού ποσού, αυτό μπορεί να υλοποιηθεί οποιαδήποτε στιγμή και για όσο χρονικό διάστημα ο χρήστης δεν προβαίνει στην αλλαγή των προσωπικών του

[94] Βλ. Βασιλάκη Ε., Τα φαινόμενα phishing και pharming και η ποινική τους αξιολόγηση, ΠοινΧρ ΝΖ/2007και Marbeth-Kubicki, Computer- und Internetstrafrecht

στοιχείων. Επιπλέον, επειδή οι hackers-crackers συνήθως δεν δρουν ανεξάρτητα αλλά ομαδικά, ακόμη και στην περίπτωση κατά την οποία ένας εξ' αυτών δεν αφαιρέσει το χρηματικό ποσό από το θύμα, αυτό πιθανότατα να υλοποιηθεί από κάποιον άλλο συνεργάτη του. Επιπροσθέτως και σε αντίθεση με τη συνήθη περίπτωση της απάτης του «φυσικού» κόσμου, στην περίπτωση του phishing και εφόσον ο κακόβουλος τρίτος διατηρεί στην κατοχή του τα διαπιστευτήρια του θύματος, μπορεί να προβαίνει στην κατ' επανάληψη βλάβη της περιουσίας του, μέχρι η εγκληματική του συμπεριφορά να γίνει τελικά γνωστή από το χρήστη.

Ένα ακόμη στοιχείο το οποίο πρέπει να ερμηνευθεί στενά, είναι το υποκείμενο της του εγκλήματος. Το 386 ΠΚ ορίζει «με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος». Στην περίπτωση του phishing, η αποκάλυψη των προσωπικών στοιχείων γίνεται προς συγκεκριμένο άτομο ή ομάδα ατόμων που ενεργούν όμως με κοινό σκοπό. Πρέπει να διαφοροποιηθεί από την περίπτωση εκείνη κατά την οποία ο πλανημένος εκ παραδρομής αποκαλύπτει τα προσωπικά του διαπιστευτήρια στο διαδίκτυο και στα οποία αποκτά πρόσβαση ένα σύνολο ατόμων. Αντίστοιχα, πρέπει να υπάρχει και διάκριση και στην περίπτωση κατά την οποία ο κακόβουλος χρήστης πείθει το θύμα να του αποκαλύψει τα προσωπικά του στοιχεία και εν συνεχεία προβαίνει στο διαμοιρασμό τους σε τρίτους. Αν δεχτούμε ότι το χρονικό περιθώριο εντός του οποίου «πρέπει να δράσει» ο phisher είναι στενό (καθώς ο χρήστης ανά πάσα στιγμή μπορεί να προβεί σε τροποποίηση των στοιχείων εισόδου στον τραπεζικό του λογαριασμό), τότε είναι «δεσμευμένος» να ενεργήσει μέσα σε σύντομο χρονικό διάστημα, γεγονός που προσδίδει ίσως ένα στοιχείο αμεσότητας στην περιουσιακή διάθεση.

Κατά μία άλλη άποψη, το phishing θα έπρεπε να αντιμετωπίζεται όχι ως μία μορφή απάτης, αλλά αντιθέτως ως μια μορφή κατάρτισης πλαστού εγγράφου και να ποινικοποιηθεί σύμφωνα με το 216 ΠΚ[95], το οποίο ορίζει ότι :

«1. Όποιος καταρτίζει πλαστό ή νοθεύει έγγραφο με σκοπό να παραπλανήσει με τη χρήση του άλλον σχετικά με γεγονός που μπορεί να έχει έννομες συνέπειες τιμωρείται με φυλάκιση και χρηματική ποινή.

2. Με την ίδια ποινή τιμωρείται όποιος για τον παραπάνω σκοπό εν γνώσει χρησιμοποιεί πλαστό ή νοθευμένο έγγραφο.

[95] Τζαννετής Αρ., Το πλαστό έγγραφο, ΠοινΧρ, 2021, εκδ. Σάκκουλα, σελ. 228-229

3. Αν ο υπαίτιος των πράξεων των παρ. 1 και 2 σκόπευε να προσπορίσει στον εαυτό του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται:

α) εάν το συνολικό όφελος ή η συνολική ζημία είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή,

β) εάν το συνολικό όφελος ή η συνολική ζημία υπερβαίνει τις εκατόν είκοσι χιλιάδες (120.000) ευρώ, με κάθειρξη έως δέκα (10) έτη και χρηματική ποινή.

4. Αν οι πράξεις των παρ. 1 και 2 στρέφονται άμεσα κατά του νομικού προσώπου του ελληνικού Δημοσίου, των νομικών προσώπων Δημοσίου Δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και το συνολικό περιουσιακό όφελος ή η συνολική ζημία υπερβαίνει συνολικά τις εκατόν είκοσι χιλιάδες (120.000) ευρώ, επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Οι πράξεις αυτές παραγράφονται μετά είκοσι (20) έτη.»

Αντιπαραβάλλοντας τη διάταξη του άρθρου 216 ΠΚ με την περίπτωση του ηλεκτρονικού ψαρέματος, διαπιστώνουμε τα εξής. Αρχικά το e-mail θα μπορούσε να θεωρηθεί ως μία μορφή ηλεκτρονικού εγγράφου[96], καθώς αποστελλόμενο από τον ηλεκτρονικό υπολογιστή ενός χρήστη, αυτό αποθηκεύεται στο διακομιστή ηλεκτρονικής αλληλογραφίας (mail server), αποκτώντας με τον τρόπο αυτό το στοιχείο της διαιωνιστικής λειτουργίας, καθώς καθίσταται πλέον προσβάσιμο οποιαδήποτε στιγμή από τον παραλήπτη. Παράλληλα, η παραπλάνηση που επέρχεται στην περίπτωση του phishing αφορά σε ένα από τα βασικότερα στοιχεία του εγγράφου, τον αποστολέα του, ο οποίος «υποδύεται» συνήθως ορισμένο νομικό πρόσωπο, χρησιμοποιώντας μάλιστα και ορισμένα χαρακτηριστικά στοιχεία του, όπως την επωνυμία ή το λογότυπό του. Όσον αφορά την ταυτότητα των παραληπτών, το γεγονός ότι αρκετοί από τους αποδέκτες των e-mails δεν επηρεάζονται άμεσα από την πρακτική αυτή (π.χ. επειδή το ηλεκτρονικό μήνυμα στέλνεται απευθείας στα «ανεπιθύμητα» πριν αυτό αναγνωστεί ή επειδή ο συγκεκριμένος χρήστης μπορεί να μη διαθέτει λογαριασμό στο συγκεκριμένο χρηματοπιστωτικό ίδρυμα, δεν αρκεί τον παραπλανητικό σκοπό του αποστολέα. Τέλος, η περιουσιακή μεταβίβαση στην οποία αυτό αποβλέπει (αρχικά μέσω της

[96] Κατά το Αστικό Δίκαιο «Ως ηλεκτρονικό έγγραφο θεωρείται το σύνολο των εγγραφών δεδομένων στον μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή, οι οποίες, αφού γίνουν αντικείμενο επεξεργασίας από την κεντρική μονάδα επεξεργασίας, αποτυπώνονται με βάση τις εντολές του προγράμματος κατά τρόπο αναγνώσιμο από τον άνθρωπο είτε στην οθόνη του μηχανήματος είτε στον προσαρτημένο εκτυπωτή του.»

γνωστοποίησης στο δράστη των προσωπικών διαπιστευτηρίων του λογαριασμού του χρήστη και εν συνεχεία μέσω της υπεξαίρεσης του χρηματικού ποσού), αποτελεί γεγονός που συνεπάγεται έννομες συνέπειες.

Τόσο στην περίπτωση που το phishing αντιμετωπιστεί ως απάτη του 386 ΠΚ, όσο και ως μορφή πλαστογραφίας του 216 ΠΚ, το πλαίσιο των ποινών που έχει θέσει ο νομοθέτης είναι παρεμφερές, ενώ και στις δύο περιπτώσεις οι προβλεπόμενοι από το νόμο χρόνοι παραγραφής ανέρχονται στα 5, 15 και 20 έτη ανάλογα με τη βαρύτητα με την οποία θα χαρακτηριστεί το έγκλημα.

5.1.2 Τρόποι προστασίας από το Phishing

Κάθε χρήστης του διαδικτύου οφείλει να διατηρεί τις επιφυλάξεις του σχετικά με καθετί που συναντά κατά την περιήγησή του στον κυβερνοχώρο. Βασική ενέργεια σε περίπτωση λήψης ενός ύποπτου μηνύματος ή e-mail, αποτελεί η διατήρηση της ψυχραιμίας από πλευράς του χρήστη, ενώ υπάρχουν ορισμένα χαρακτηριστικά τα οποία συχνά υποδηλώνουν ότι πρόκειται για μία περίπτωση phishing απάτης.

- Έλεγχος της ηλεκτρονικής διεύθυνσης (e-mail) του αποστολέα

Στις περισσότερες περιπτώσεις ενός phishing μηνύματος ηλεκτρονικού ταχυδρομείου, ο δράστης υποδύεται κάποιον οργανισμό ή τράπεζα χρησιμοποιώντας ακόμα και τα λογότυπά τους προκειμένου να επιτύχει τη μεγαλύτερη δυνατή αληθοφάνεια και να αποφύγει να γίνει αντιληπτός από τον παραλήπτη. Ωστόσο, ελέγχοντας τη διεύθυνση του e-mail του αποστολέα, ο χρήστης μπορεί να διαπιστώσει αν η συγκεκριμένη αποτελεί την επίσημη ηλεκτρονική διεύθυνση της εταιρείας και αντίστοιχα να καταλάβει αν πρόκειται για περίπτωση ή όχι απάτης. Συνήθως οι κακόβουλοι χρήστες επιλέγουν ηλεκτρονικές διευθύνσεις οι οποίες να είναι παραπλήσιες με τις αντίστοιχες «γνήσιες» των οργανισμών (π.χ. national-bank@domain.com αντί για nationalbank@domain.com).

- Έλεγχος περιεχομένου του μηνύματος

Δεν είναι λίγες οι φορές εκείνες στις οποίες το περιεχόμενο του μηνύματος από μόνο του μπορεί να υποδηλώνει ότι πρόκειται για απάτη. Αυτό μπορεί να προκύπτει τόσο από την προσφώνηση (αν δεν είναι η συνήθης που χρησιμοποιείται από το συγκεκριμένο οργανισμό), από τα ορθογραφικά λάθη που ενδεχομένως να υπάρχουν στο κείμενο, από τη διάταξη και τη δομή του μηνύματος κ.λπ. Είναι προφανές ότι ένα e-mail από επίσημο

φορέα συνήθως δε θα έχει ατημέλητη διάταξη, ενώ το ύφος του κειμένου είναι επίσημο και τυπικό. Επίσης, τυχόν ύποπτα συνημμένα του μηνύματος θα πρέπει να αντιμετωπίζονται με επιφύλαξη και θα πρέπει να αποφεύγεται να ανοίγονται.

- Χρησιμοποίηση λογισμικού προστασίας (Antivirus)

Αποτελεί ίσως την συνηθέστερη μορφή προστασίας. Ήδη πολλές εταιρείες όπως η Google εφαρμόζουν τεχνικές ελέγχου του περιεχομένου των ηλεκτρονικών μηνυμάτων που διακινούνται[97]. Η προστασία στα e-mails που παρέχεται μέσω ορισμένων φίλτρων, μπορεί να αφορά στο περιεχόμενο των συνημμένων αρχείων, των υπερσυνδέσμων, αλλά και στον έλεγχο της αυθεντικότητας των χρηστών. Σε περίπτωση που παρατηρηθεί ύποπτη δραστηριότητα, τότε το e-mail μαζί με το περιεχόμενο αυτόματα μεταφέρεται στο φάκελο των ανεπιθύμητων και ο χρήστης προειδοποιείται αναλόγως. Παράλληλα, το ίδιο αποτέλεσμα μπορεί να επιτευχθεί και με την χρήση antivirus προγραμμάτων[98], τα οποία μεταξύ άλλων, εγγυόνται προστασία και από τις περιπτώσεις phishing επιθέσεων.

- Εγκατάσταση των πιο πρόσφατων ενημερώσεων λογισμικού

Κάθε λογισμικό και πρόγραμμα έχει ορισμένες ευπάθειες. Οι hackers και crackers δρουν προσπαθώντας να εκμεταλλευτούν τα κενά ασφαλείας που υπάρχουν σε έναν υπολογιστή ή δίκτυο, προκειμένου να επιτύχουν τις κακόβουλες προθέσεις τους[99]. Οι ενημερώσεις του λογισμικού εκτός από την προσθήκη νέων χαρακτηριστικών και δυνατοτήτων που παρέχουν στους χρήστες, διορθώνουν τυχόν σφάλματα ή κενά ασφαλείας που μπορεί να υπήρχαν στις προηγούμενες εκδόσεις.

- Ενεργοποίηση δυνατότητας αυθεντικοποίησης πολλαπλών παραγόντων (Multi-Factor Authentication)

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων είναι μία πρόσθετη λειτουργία ασφαλείας η οποία απαιτεί περισσότερα από ένα διαπιστευτήρια προκειμένου να καταφέρει κανείς να εισέλθει στο προσωπικό του λογαριασμό. Τα πρόσθετα διαπιστευτήρια ζητούνται από το χρήστη αφού αυτός εισάγει το όνομα χρήστη και τον κωδικό του και μπορεί να είναι μία ερώτηση την οποία ο αυτός έχει προηγουμένως ορίσει, ένας κωδικός PIN ο οποίος θα αποσταλεί στο κινητό τηλέφωνό του, ένα e-mail το οποίο θα λάβει στο λογαριασμό του και θα τον καλεί να επιβεβαιώσει αν προσπαθεί να εισέλθει στον τραπεζικό του λογαριασμό κ.λπ. Έτσι λοιπόν, ακόμη και στην περίπτωση του phishing κατά την οποία

[97] Βλ. https://safety.google/gmail/ και https://support.google.com/a/answer/9157861?hl=en

[98] Βλ. https://us.norton.com/blog/online-scams/what-is-phishing

[99] Βλ. https://ie.norton.com/blog/how-to/the-importance-of-general-software-updates-and-patches

ένας χρήστης θα αποκαλύψει στον κακόβουλο τρίτο τα προσωπικά του διαπιστευτήρια, όταν ο τελευταίος επιχειρήσει να εισέλθει στον τραπεζικό λογαριασμό του θύματος για να προβεί στην περιουσιακή μετάθεση, δε θα μπορέσει να την ολοκληρώσει αν δεν περάσει επιτυχώς και τον τελευταίο έλεγχο ασφαλείας[100]. Η «τακτική» αυτή σήμερα υιοθετείται και ενσωματώνεται ως υποχρεωτική από ολοένα και περισσότερες εταιρείες.

- Αγνόηση ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου

Οι phishers στα μηνύματα και e-mails που στέλνουν χρησιμοποιούν μεθόδους προκειμένου να πανικοβάλλουν τους αποδέκτες. Μηνύματα με θέμα ή περιεχόμενο που αφορά την αναστολή του λογαριασμού του χρήστη, ύποπτη δραστηριότητα που παρατηρήθηκε, οικονομικές συναλλαγές στις οποίες δεν έχει προβεί ο χρήστης, ηλεκτρονικές παραγγελίες αγαθών τις οποίες δεν έχει πραγματοποιήσει κ.α., αποτελούν τις συχνότερες τακτικές εξαπάτησης που χρησιμοποιούν οι phishers. Οι χρήστες στην περίπτωση που παραλάβουν ένα τέτοιο e-mail, οφείλουν να μην το ανοίγουν και να το διαγράφουν αμέσως.

Το αποτελεσματικότερο μέτρο για την αντιμετώπιση της ηλεκτρονικής απάτης υπό την μορφή του phishing είναι η ενημέρωση των χρηστών για το υπόψη φαινόμενο και τους κινδύνους που αυτή εγκυμονεί. Τόσο σε ατομικό, όσο και σε συλλογικό επίπεδο (π.χ. μεταξύ των εργαζομένων σε μία επιχείρηση, σε ένα ίδρυμα, σε έναν οργανισμό κ.λπ.) η ενημέρωση δε θα πρέπει να παραλείπεται, καθώς μπορεί να συμβάλλει στην αποφυγή ανεπιθύμητων καταστάσεων. Για το σκοπό αυτό και με γνώμονα την προστασία των συμφερόντων των πολιτών, οι τράπεζες ενημερώνουν ότι δεν θα ζητήσουν με οποιοδήποτε τρόπο από τους πελάτες τους να προβούν στην αποκάλυψη των προσωπικών τους αριθμών ασφαλείας.

5.2 Το φαινόμενο «Pharming»

Το φαινόμενο pharming αποτελεί μία μορφή απάτης με υπολογιστή, η οποία αν και παρουσιάζει αρκετές ομοιότητες με το phishing, θα μπορούσε να χαρακτηριστεί ως μια πιο επικίνδυνη εκδοχή του. Συνίσταται στον επηρεασμό ενός υπολογιστικού συστήματος (συνήθως με την εγκατάσταση ενός προγράμματος) κατά τρόπο τέτοιο, ώστε ορισμένες υπηρεσίες όπως ο DNS [Domain Name System - που είναι υπεύθυνος

[100] Βλ. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

για την αντιστοίχιση των διευθύνσεων που πληκτρολογεί ο χρήστης (domain names) σε αριθμητικές τιμές (διευθύνσεις IP)], να μην λειτουργούν σωστά[101].

Το παραπάνω έχει ως συνέπεια όταν ο χρήστης κατά την περιήγησή του στο διαδίκτυο πληκτρολογεί μία διεύθυνση, ο DNS να τον παραπέμπει σε κάποια διαφορετική, πλαστή ιστοσελίδα η οποία ελέγχεται από τον κακόβουλο δράστη. Οι πλαστές αυτές ιστοσελίδες είναι σε τέτοιο βαθμό αληθοφανείς, ώστε η διάκρισή τους από τις αυθεντικές να καθίσταται μία ιδιαίτερα δύσκολη υπόθεση. Στην περίπτωση που το θύμα επισκεφτεί ένα διαδικτυακό ιστότοπο τράπεζας για να πραγματοποιήσει τις συναλλαγές του, τα χρήματά του πιθανότατα θα καταλήξουν σε λογαριασμό των pharmers[102]. Το φαινόμενο αυτό ονομάζεται και Domain Name Server (DNS) Hijacking[103] ή DNS Spoofing. Αυτό συνήθως μπορεί να συμβεί με τέσσερεις τρόπους:

- Σε κάθε υπολογιστή υπάρχουν ρυθμίσεις που καθορίζουν το ποιος θα είναι ο DNS που θα χρησιμοποιηθεί κατά την περιήγηση στο διαδίκτυο. Πολλές φορές οι δράστες χρησιμοποιώντας κακόβουλο λογισμικό (ιοί ή δούρειοι ίπποι) προσβάλλουν ένα υπολογιστικό σύστημα, κατορθώνοντας να αλλάξουν τις αποθηκευμένες ρυθμίσεις DNS και χωρίς η ενέργεια αυτή να γίνει αντιληπτή από το χρήστη. Η μέθοδος αυτή ονομάζεται Local DNS Hijack.
- Οι δρομολογητές (routers) που χρησιμοποιούνται για την διασύνδεση ενός τοπικού δικτύου με το διαδίκτυο, πολλές φορές έχουν αποθηκευμένους δικούς τους DNS και ανακατευθύνουν απευθείας τους χρήστες στις επιθυμητές ιστοσελίδες. Μια διαδικτυακή επίθεση σε κάποιο δρομολογητή, μπορεί να έχει ως συνέπεια την διαφοροποίηση των αποθηκευμένων σε αυτόν ρυθμίσεων DNS, με αποτέλεσμα ο τελευταίος να παραπέμπει τους χρήστες σε πλαστές ιστοσελίδες που ελέγχονται από κακόβουλους τρίτους. Η τεχνική αυτή ονομάζεται Router DNS Hijack.
- Οι Man-in-the-middle DNS επιθέσεις[104] αποτελούν μία από τις πιο επικίνδυνες εκφάνσεις του pharming. Στην περίπτωση αυτή, ένας εισβολέας παραβάλλεται μεταξύ της επικοινωνίας δύο χρηστών προκειμένου να υποκλέψει ή να αλλοιώσει τα στοιχεία που διαβιβάζονται. Όταν η επικοινωνία πραγματοποιείται μεταξύ

[101] https://csrc.nist.gov/glossary/term/pharming

[102] Βλ. Βασιλάκη Ε., Τα φαινόμενα phishing και pharming και η ποινική τους αξιολόγηση, ΠοινΧρ NZ/2007

[103] https://www.imperva.com/learn/application-security/dns-hijacking-redirection/

[104] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

του χρήστη και ενός DNS, τότε οι πληροφορίες σχετικά με την αντιστοίχιση των διευθύνσεων IP πιθανώς να μην είναι οι σωστές και να ανακατευθύνουν το χρήστη σε κακόβουλο ιστότοπο.

- Τέλος στην περίπτωση του Rogue DNS Server[105], οι hackers-crackers ρυθμίζουν έναν διακομιστή DNS στον οποίο εισάγουν εγγραφές, οι οποίες παραπέμπουν σε διευθύνσεις IP με κακόβουλο περιεχόμενο. Ο διακομιστής αυτός μπορεί είτε να έχει δημιουργηθεί εξ' αρχής από κακόβουλους τρίτους για το σκοπό αυτό, είτε να είναι ένας νόμιμος διακομιστής ο οποίος έχει παραβιαστεί και του οποίου οι εγγραφές έχουν τροποποιηθεί. Με τον τρόπο αυτό, τα αιτήματα των χρηστών παραπέμπονται στον εσφαλμένο διακομιστή και οι ίδιοι ανακατευθύνονται σε ιστοσελίδες πλαστού περιεχομένου.

Το 2019 σημειώθηκε στη Βενεζουέλα μία από τις χαρακτηριστικότερες επιθέσεις pharming[106]. Το διάστημα εκείνο και ενώ η χώρα βρισκόταν σε άμεση ανάγκη για ανθρωπιστική βοήθεια, ο πρόεδρος της χώρας, Juan Guaidó, προχώρησε σε δημόσια έκκληση ζητώντας από τον λαό να ενισχύσει το νέο κίνημα εθελοντών που είχε σχηματιστεί (Voluntarios por Venezuela) και συνεργαζόταν με διεθνείς οργανισμούς για τη σωτηρία της χώρας. Οι νέοι εθελοντές που υπέβαλλαν ηλεκτρονικά την εγγραφή τους στο υπόψη κίνημα, έπρεπε να καταθέσουν ορισμένα προσωπικά τους στοιχεία, όπως ταυτότητα, αριθμό τηλεφώνου, διεύθυνση κ.λπ.

Αρκετά σύντομα (μόλις 5 ημέρες αργότερα) εμφανίστηκε μία νέα, πλαστή ιστοσελίδα η οποία είχε αρκετές ομοιότητες με την γνήσια στη διάταξη και στη δομή, ενώ και το όνομά της (domain name) παρέπεμπε στην αυθεντική. Επιπλέον, σε εθνικό επίπεδο, τόσο η γνήσια όσο και η πλαστή ιστοσελίδα ανακατεύθυναν τους επισκέπτες τους στην ίδια διεύθυνση IP, η οποία ανήκε στον κάτοχο της πλαστής ιστοσελίδας. Με τον τρόπο αυτό, πρακτικά όποιος χρήστης επισκεπτόταν είτε τον πλαστό είτε τον αυθεντικό ιστοχώρο, τα προσωπικά του στοιχεία κατέληγαν στον ψεύτικο[107].

[105] https://www.securesenses.net/2022/08/rogue-dns-server.html

[106] https://www.kaspersky.com/resource-center/definitions/pharming

[107] https://securelist.com/dns-manipulation-in-venezuela/89592/

5.2.1 Ποινική Αξιολόγηση του Pharming

Εκ πρώτης όψεως, το pharming μοιάζει να συγγενεύει με το phishing ως μια μορφή εξαπάτησης των χρηστών με σκοπό την οικονομική εκμετάλλευσή τους. Ωστόσο θα πρέπει να διερευνήσουμε καλύτερα τον τρόπο τον οποίο χρησιμοποιούν οι κακόβουλοι χρήστες για να επιτύχουν τους σκοπούς τους, προκειμένου να μπορέσουμε να αποφανθούμε για το ποια ποινική διάταξη αρμόζει περισσότερο στην περίπτωσή του.

Το phishing όπως αναφέρθηκε, είναι μια τεχνική στην οποία παρέχεται στο χρήστη ένας «έτοιμος» από τον απατεώνα υπερσύνδεσμος και με διάφορες τεχνικές προσπαθεί να τον πείσει (συνήθως υποκινούμενος από το αίσθημα του φόβου) να τον επισκεφτεί. Στη συνέχεια, το θύμα εν αγνοία του προβαίνει την αποκάλυψη των διαπιστευτηρίων του, χωρίς να γνωρίζει την πραγματική ταυτότητα του δράστη, ο οποίος τελικά προβαίνει σε χρηματική λεηλάτηση του τραπεζικού του λογαριασμού.

Απεναντίας, η τεχνική που εφαρμόζεται από τους hackers κατά το φαινόμενο του pharming είναι διαφορετική. Στην περίπτωση αυτή δεν παρέχεται στο θύμα μία έτοιμη, απατηλή επιλογή, αλλά αντιθέτως, πραγματοποιείται από τον ίδιο το δράστη μία παρέμβαση στο πληροφοριακό σύστημα του θύματος. Η παρέμβαση αυτή αφορά στην αλλοίωση ή τροποποίηση ορισμένων ρυθμίσεων, οι οποίες με βεβαιότητα πλέον θα ανακατευθύνουν το χρήστη στην επιθυμητή πλαστή ιστοσελίδα. Θα μπορούσαμε λοιπόν να πούμε ότι ο δράστης στην περίπτωση του pharming προβαίνει ο ίδιος σε θετική ενέργεια προκειμένου να «αναγκάσει» το θύμα να έρθει σε επαφή με την πλαστή πραγματικότητα που έχει δημιουργήσει και δεν επαφίεται στην επιλογή του χρήστη.

Η ενέργεια αυτή της παράνομης παρέμβασης σε πληροφοριακό σύστημα μας παραπέμπει στο 370Δ, σύμφωνα με το οποίο:

«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 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».

Και στις 4 περιπτώσεις παρέμβασης σε διακομιστή DNS που αναφέρθηκαν προηγουμένως (Local DNS Hijack, Router DNS Hijack, Man-in-the-middle DNS επίθεση και Rogue DNS Server) πραγματοποιούνται παρεμβάσεις από τον κακόβουλο χρήστη, οι οποίες εστιάζουν σε διαφορετικό σημείο του πληροφοριακού συστήματος ή δικτύου του θύματος κάθε φορά, καθώς και σε πληροφορίες οι οποίες μεταδίδονται από και προς αυτό.

Οι παρεμβάσεις αυτές πραγματοποιούνται «χωρίς δικαίωμα», δηλαδή εκλείπει η συναίνεση του νόμιμου κατόχου[108], η οποία υπό άλλες συνθήκες δε θα οδηγούσε στην πλήρωση της α.υ. του εγκλήματος. Επίσης, ο δράστης παρεμβαίνοντας στο πληροφοριακό σύστημα τρίτου, παραβιάζει ή παρακάμπτει τις απαγορεύσεις και τα μέτρα ασφαλείας που υπάρχουν στον υπολογιστή και στο δίκτυο. Τα τελευταία περιλαμβάνουν μέτρα όπως το τείχος προστασίας (firewall), διάφορα προγράμματα antivirus[109], πρωτόκολλα που εξασφαλίζουν την ασφαλή και κρυπτογραφημένη επικοινωνία μεταξύ των ανταποκριτών του δικτύου[110] κ.λπ. Τα περισσότερα από αυτά μάλιστα, αποτελούν τεχνικά μέτρα τα οποία πλέον υιοθετούνται από όλα τα σύγχρονα πληροφοριακά συστήματα, χωρίς να απαιτείται ειδική ρύθμιση από το χρήστη.

Τέλος, δεδομένου ότι η πράξη αυτή του κακοπροαίρετου χρήστη εμφορείται από τον απαιτούμενο δόλο (άμεσος δόλος α' βαθμού), ο οποίος είναι προαπαιτούμενος, θα μπορούσαμε να καταλήξουμε ότι στην περίπτωση του pharming πληρούται η α.υ. του εγκλήματος της παράνομης πρόσβασης σε πληροφοριακό σύστημα της §2 του 370Δ ΠΚ.

Όπως και στην περίπτωση του phishing, κατά μία άλλη άποψη, το pharming θα πρέπει να αντιμετωπίζεται ως μία μορφή πλαστογραφίας[111]. Προκειμένου όμως να ευσταθεί ο ισχυρισμός αυτός, πρέπει να εξετασθεί κατά πόσο η δημιουργία μίας πλαστής ιστοσελίδας μπορεί να θεωρηθεί ως κατάρτιση ενός πλαστού εγγράφου. Πράγματι, η ύπαρξη μίας βάσης δεδομένων στην οποία να αποθηκεύονται όλες οι πληροφορίες που αφορούν τόσο τη δομή της ιστοσελίδας, όσο και τους χρήστες που την επισκέπτονται αποτελεί απαραίτητο στοιχείο της ορθής λειτουργίας μίας ιστοσελίδας. Με άλλα λόγια απαιτείται η ύπαρξη ενός συνόλου ηλεκτρονικών αρχείων, αποθηκευμένα σε υπολογιστή

[108] Βλ. Κιούπης Δ., Ποινικό δίκαιο και internet, 1999

[109]https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/texnika_metra

[110] Όπως https, sftp, ssh κ.λπ.

[111] Τζαννετής Αρ., Το πλαστό έγγραφο, ΠοινΧρ, 2021, εκδ. Σάκκουλα, σελ. 229-232

τρίτου ή σε κάποιον διακομιστή, τα οποία θα περιέχουν τις «πλαστές» πληροφορίες για το περιεχόμενό της. Προκειμένου τα ηλεκτρονικά αρχεία μίας βάσης δεδομένων και κατ' επέκταση η ίδια η ιστοσελίδα να θεωρηθούν ότι ανήκουν στην κατηγορία των ηλεκτρονικών εγγράφων κατά τον ορισμό του Αστικού Δικαίου, πρέπει το περιεχόμενό της να είναι ικανό να οδηγήσει στη συντέλεση γεγονότος με έννομη συνέπεια (π.χ. περιουσιακή μεταβίβαση). Έτσι, ένας ιστοχώρος που ενημερώνει τους χρήστες σχετικά με κάτι αναληθές, χωρίς όμως από αυτό να προκύπτουν έννομες συνέπειες δεν πρέπει να θεωρηθεί ότι εμπίπτει στην κατηγορία των ηλεκτρονικών εγγράφων.

Όπως αναφέρθηκε παραπάνω, η παρέμβαση στο DNS μπορεί να γίνει με διαφόρους τρόπους. Η επιλογή της δικαιολογητικής βάσης της πλαστογραφίας για ποινικοποίηση του φαινομένου του pharming, δεν έγκειται στο γεγονός της χρήσης ενός ή περισσοτέρων DNS που έχουν υποστεί τροποποιήσεις με αποτέλεσμα να μην πραγματοποιείται η ανακατεύθυνση στη σωστή ιστοσελίδα. Αντιθέτως, η δημιουργία μίας ιστοσελίδας η οποία προσομοιάζει σε μεγάλο βαθμό τη γνήσια, μιμούμενος ο κακόβουλος τρίτος με τον τρόπο αυτό το πραγματικό νομικό πρόσωπο, και από την οποία μπορούν να προκύψουν έννομες συνέπειες, είναι η πράξη που πληροί την α.υ.ε του 216 ΠΚ.

5.2.2 Τρόποι προστασίας από το Pharming

Οι περισσότερες τεχνικές αποτροπής των phishing επιθέσεων που αναφέρθηκαν προηγουμένως μπορούν να συμβάλλουν αποτελεσματικά και στην καταπολέμηση του φαινομένου του pharming.[112] Υπάρχουν ωστόσο και ορισμένα πρόσθετα μέτρα που μπορεί να εφαρμόσει κανείς για να ελαττώσει σημαντικά τις πιθανότητες να υποστεί μία pharming επίθεση[113].

- Επιλογή ενός αξιόπιστου τηλεπικοινωνιακού παρόχου

Ένας πάροχος εκτός από τη δυνατότητα πρόσβασης στο διαδίκτυο που προσφέρει στους χρήστες του, εφαρμόζει ορισμένα μέτρα προστασίας και αποκλεισμού υπόπτων ιστοσελίδων. Πολλοί πάροχοι επίσης προμηθεύουν στους πελάτες τους δρομολογητές, οι

[112] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

[113] Βλ. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf καθώς και https://www.kaspersky.com/resource-center/definitions/pharming

οποίοι έχουν τους δικούς τους ενσωματωμένους DNS και οι οποίοι ανακατευθύνουν τους περιηγητές στους επιθυμητούς ιστοχώρους. Συνεπώς, η επιλογή ενός τηλεπικοινωνιακού παρόχου που εφαρμόζει υψηλές προδιαγραφές ασφαλείας, αποτελεί ένα καίριο ζήτημα.

- Έλεγχος των διευθύνσεων που πληκτρολογούνται

Αποτελεί συχνή πρακτική για τους κακόβουλους δημιουργούς μίας πλαστής ιστοσελίδας η επιλογή ενός ονόματος domain που παραπέμπει στην αυθεντική. Ένας απρόσεκτος χρήστης που θα πληκτρολογήσει εκ παραδρομής λανθασμένο όνομα, μπορεί άθελά του να οδηγηθεί σε μία πλαστή ιστοσελίδα, με ανεπιθύμητες γι' αυτόν συνέπειες.

- Χρήση αξιόπιστων DNS που εφαρμόζουν τις πιο πρόσφατες ενημερώσεις ασφαλείας

Όπως και κάθε υπολογιστικό σύστημα, έτσι και ένας διακομιστής DNS πρέπει να διαθέτει τις πιο πρόσφατες ενημερώσεις κώδικα ασφαλείας (security patches). Ένα κενό ασφαλείας, το οποίο εντοπίζεται σε μία έκδοση λογισμικού και δεν αποκαθίσταται με την επόμενη ενημέρωση λογισμικού, συνήθως αποτελεί στόχο που επιδιώκουν να εκμεταλλευτούν οι χάκερς για την προσβολή ενός δικτύου.

- Αποφυγή ιστοσελίδων στις οποίες η πρόσβαση δεν γίνεται μέσω ασφαλούς σύνδεσης

Όπως αναφέρθηκε προηγουμένως, το πρωτόκολλο επικοινωνίας που χρησιμοποιείται ως επί το πλείστον για τη διαβίβαση μιας ιστοσελίδας μέσω διαδικτύου είναι το https (Hyper Text Transfer Protocol Secure), το οποίο παρέχει κρυπτογράφηση των δεδομένων που μεταφέρονται. Οι περισσότεροι περιηγητές ιστού (browsers) προειδοποιούν τους χρήστες όταν πρόκειται να εισέλθουν σε ένα ιστοχώρο στον οποίο η σύνδεση δεν είναι ασφαλής (κρυπτογραφημένη). Παράλληλα, κάθε χρήστης μπορεί να επαληθεύει τα πιστοποιητικά ασφαλείας της κάθε ιστοσελίδας που επισκέπτεται, προκειμένου να ελέγξει την αυθεντικότητα και νομιμότητά της.

- Ενεργοποίηση επεκτάσεων ασφαλείας

Τέλος, αρκετοί browsers σήμερα παρέχουν τη δυνατότητα ενεργοποίησης ορισμένων προσθηκών[114] (plug-ins), οι οποίες ελέγχουν κάθε φορά τη διεύθυνση IP την οποία έχει επισκεφτεί ο χρήστης. Στη συνέχεια, αντιστοιχίζουν την τρέχουσα διεύθυνση με αυτήν που έχουν ήδη αποθηκευμένη σε δική τους βάση δεδομένων για τη συγκεκριμένη

[114] Προγράμματα τα οποία λειτουργούν παράλληλα με τον περιηγητή ιστού και παρέχουν στους χρήστες ορισμένες πρόσθετες δυνατότητες

ιστοσελίδα. Εάν δεν υπάρχει αντιστοίχιση, τότε στο χρήστη εμφανίζεται ένα προειδοποιητικό μήνυμα για είσοδο σε ύποπτο ιστοχώρο.

5.3 Η Χωρίς Δικαίωμα Ανάληψη Χρημάτων από ΑΤΜ

Η περίπτωση της άνευ δικαιώματος ανάληψης χρημάτων από μία αυτόματη ταμειολογιστική μηχανή (ΑΤΜ), αποτελεί ένα από τα παλαιότερα αλλά συνάμα και χαρακτηριστικότερα παραδείγματα της ηλεκτρονικής απάτης σήμερα, η οποία με την πάροδο του χρόνου και την εμφάνιση καινοτόμων τεχνολογιών καθίσταται ιδιαιτέρως πολυδιάστατη.

Οι σύγχρονες ηλεκτρονικές συναλλαγές, πραγματοποιούνται με την ηλεκτρονική, λογιστική εγγραφή νομισματικών μονάδων από το λογαριασμό ενός φυσικού ή νομικού προσώπου σε ενός άλλου[115]. Ο τελευταίος με τον τρόπο αυτό και όντας δικαιούχος του ηλεκτρονικού λογαριασμού, αποκτά απαίτηση έναντι της τράπεζας για την απόδοση του συγκεκριμένου αυτού ποσού. Προκειμένου να μπορέσει κανείς να έχει πρόσβαση στον τραπεζικό του λογαριασμό, απαραίτητη προϋπόθεση ήταν η χρησιμοποίηση μίας κάρτας αυτόματης συναλλαγής[116].

Οι κάρτες αυτόματης συναλλαγής εκδίδονται από κάποιο χρηματοπιστωτικό ίδρυμα (συνήθως τράπεζα) υπέρ ενός φυσικού ή νομικού προσώπου, προκειμένου αυτό να είναι σε θέση να διαχειρίζεται το χρηματικό ποσό που διαθέτει στον τραπεζικό του λογαριασμό. Το γεγονός ότι κάθε κάρτα περιέχει έναν μυστικό αριθμό αναγνώρισης (PIN – Personal Identification Number), καθώς και διάφορες πληροφορίες σχετικά με το δικαιούχο του λογαριασμού, τις καθιστά απόλυτα προσωποπαγής.

Το 1996 και με σκοπό να αποφευχθούν τα αυξανόμενα περιστατικά περιουσιακών απωλειών που σημειώνονταν ως συνέπεια της δημιουργίας και χρησιμοποίησης πλαστών χρεωστικών και πιστωτικών καρτών κατ' απομίμηση των γνήσιων, δημιουργήθηκε μία μέθοδος πληρωμής η οποία ονομάστηκε EMV, παίρνοντας το όνομά της από τα αρχικά των 3 μεγάλων εταιρειών που συνέπραξαν για τη δημιουργία της (Europay, Mastercard και Visa). Οι κάρτες που ενσωμάτωναν την

[115] Βλ. Ναμίας Ο., Σύγχρονες μορφές (ηλεκτρονικής) απάτης στις τραπεζικές συναλλαγές, σελ.487, ΠοινΧρ ΝΓ/2003

[116] Αναφέρονται και ως «έξυπνες κάρτες»

τεχνολογία αυτή[117], κρυπτογραφούσαν τα αποθηκευμένα δεδομένα σε τσιπ ολοκληρωμένων κυκλωμάτων[118], λειτουργώντας με τον τρόπο αυτό σαν ένας μικρός υπολογιστής, γεγονός που τις καθιστούσε εξαιρετικά δύσκολο να αντιγραφούν. Μεταξύ των πληροφοριών (δεδομένων) που αποθηκεύονται σε μία κάρτα chip είναι ο αριθμός της κάρτας, ο λογαριασμός με τον οποίον αυτή είναι συνδεδεμένη, το PIN και ο αριθμός των ανεπιτυχών προσπαθειών εισαγωγής του, το ημερήσιο όριο ανάληψης του λογαριασμού κ.λπ.

Ο τρόπος λειτουργίας μίας κάρτας τσιπ είναι ο ακόλουθος. Η κάρτα του κάθε χρήστη έχει ένα μοναδικό μυστικό αριθμό αναγνώρισης (PIN). Ο κωδικός αυτός κρυπτογραφείται έτσι ώστε να μην είναι αναγνώσιμος και παράγεται ένα μοναδικό αποτέλεσμα, το οποίο και αποθηκεύεται σε ένα τμήμα της μνήμης του τσιπ. Όταν ο χρήστης επιθυμεί να εισέλθει στον τραπεζικό του λογαριασμό μέσω ενός ATM, του ζητείται να εισάγει τον αριθμό αναγνώρισης. Ο κωδικός που θα εισάγει ο χρήστης υπόκειται στον ίδιο αλγόριθμο κρυπτογράφησης με το αρχικό PIN. Τέλος, το εισαγόμενο PIN συγκρίνεται με το αποθηκευμένο και μόνο στην περίπτωση που αυτά ταυτίζονται, μπορεί ο χρήστης να αποκτήσει πρόσβαση στον τραπεζικό του λογαριασμό. Οι διαδικασίες της κρυπτογράφησης και της σύγκρισης των δύο PIN, πραγματοποιούνται εξ' ολοκλήρου εντός του τσιπ της κάρτας, με αποτέλεσμα να μην αποθηκεύονται τυχόν δεδομένα στην μνήμη άλλων υπολογιστικών συστημάτων[119]. Με την ταύτιση των δύο PIN, το άτομο μπορεί μέσω του ATM που είναι συνδεδεμένο διαδικτυακά με το κεντρικό υπολογιστικό σύστημα της τράπεζας, να προβεί σε μεταφορά νομισματικών μονάδων προς άλλους λογαριασμούς, με τις ενέργειές του αυτές να καταγράφονται σε μητρώα της τράπεζας.

Η ραγδαία εξέλιξη της τεχνολογίας όπως είναι αναμενόμενο, δεν θα μπορούσε να αφήσει ανεπηρέαστο και τον χρηματοοικονομικό τομέα. Το internet banking, το οποίο επέτρεπε στους πελάτες να έχουν πρόσβαση στους τραπεζικούς τους λογαριασμούς από τον ηλεκτρονικό τους υπολογιστή, είχε γνωρίσει τεράστια απήχηση ήδη από τις αρχές της δεκαετίας του 2000[120], ενώ η εμφάνιση των smartphones έχει οδηγήσει στην μετεξέλιξη του internet banking σε mobile banking. Παράλληλα, η εισαγωγή της

[117] Είναι επίσης γνωστές και ως κάρτες chip

[118] https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-does-a-chip-card-work

[119] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-157.pdf

[120] https://en.wikipedia.org/wiki/Online_banking

τεχνολογίας RFID (Radio Frequency Identification) στις κάρτες αυτόματης συναλλαγής, έχει επιτρέψει την ανέπαφη ταυτοποίηση με τη χρήση ραδιοκυμάτων, παραλείποντας αρκετές φορές την ταυτοποίηση μέσω του κωδικού PIN.

5.3.1 Ποινική Αξιολόγηση της Χωρίς Δικαίωμα Ανάληψης Χρημάτων από ΑΤΜ

Η χρήση μυστικών κωδικών αναγνώρισης στις τραπεζικές υπηρεσίες είτε αυτές παρέχονται μέσω διαδικτύου (web banking) είτε μέσω ΑΤΜ, εφαρμόζονται με σκοπό να περιορίζουν κάθε άλλο πέρα από το νόμιμο δικαιούχο τους να τις εκμεταλλευτεί. Διχογνωμία επικρατούσε για αρκετά χρόνια σχετικά με το αν το φαινόμενο της παράνομης εισόδου σε έναν τραπεζικό λογαριασμό από μη νομιμοποιούμενα γι' αυτό πρόσωπα, πληρούσε την α.υ. της απάτης με υπολογιστή, καθώς και σε ποια υποκατηγορία της ηλεκτρονικής απάτης αυτό εμπίπτει. Στο Γερμανικό Ποινικό Δίκαιο, η πράξη αυτή κατά κρατούσα άποψη υπάγεται στην περίπτωση της «μη εξουσιοδοτημένης χρήσης δεδομένων» του άρθρου 263α περί απάτης με υπολογιστή.

Στο Ελληνικό Ποινικό Δίκαιο μέχρι πριν λίγα χρόνια και εξαιτίας της έλλειψης αντίστοιχης διάταξης, το φαινόμενο αυτό αξιολογούταν με διαφορετικούς τρόπους σε θεωρία και νομολογία[121]. Κατά μία άποψη, η ανάληψη χρημάτων από ΑΤΜ χωρίς δικαίωμα έπρεπε να υπαχθεί στην περίπτωση της χρησιμοποίησης "μη ορθών" ή "ελλιπών" στοιχείων του 386Α ΠΚ, καθώς μεταξύ των στοιχείων που εμπεριέχονται εντός του μαγνητικού τσιπ της κάρτας συγκαταλέγεται και η ταυτότητα του χρήστη της, η οποία είναι μοναδική και αποκλείει οποιονδήποτε άλλο μη δικαιούχο από τη χρήση της. Κατά άλλες απόψεις, το φαινόμενο αυτό υπάγονταν στις ποινικές υποστάσεις της κλοπής, υπεξαίρεσης, αφού αποκτώντας κανείς πρόσβαση στην κάρτα και το PIN τρίτου (αφαιρώντας δηλαδή ξένο κινητό πράγμα από την κατοχή άλλου ή/και προβαίνοντας σε ηλεκτρική και κάθε άλλης μορφής ενέργεια) στοιχειοθετείται το έγκλημα της κλοπής του 372 ΠΚ.

Την ασάφεια αυτή του Ποινικού μας Δικαίου, ήρθε να επιλύσει η τελευταία τροποποίηση του 386Α ΠΚ, με την οποία προστέθηκε μία επιπλέον περίπτωση τέλεσης

[121] Βλ. Σάμιος Θ., Η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων ως τρόπος τελέσεως της απάτης με υπολογιστή (άρθρο 386Α' ΠΚ)

απάτης με υπολογιστή «με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας». Στην περίπτωση της παράνομης ανάληψης χρημάτων από ΑΤΜ, ο δράστης εκμεταλλεύεται μία αυτοματοποιημένη λειτουργία του μηχανήματος (το οποίο με το λογισμικό που διαθέτει και την πρόσβαση στο διαδίκτυο που έχει μπορεί να προσομοιαστεί με ηλεκτρονικό υπολογιστή), χωρίς να αλλοιώνει ή να παρεμβαίνει με οποιονδήποτε τρόπο στη λειτουργία του. Ο όρος «χωρίς δικαίωμα» αναφέρεται σε οποιοδήποτε άτομο δεν είναι ο νόμιμος δικαιούχος του λογαριασμού βάσει της παρεπόμενης με την τράπεζα σύμβασης ή οποιοδήποτε τρίτος δεν του έχει παρασχεθεί υπεξουσιοδότηση[122] από τον κάτοχο. Επίσης, η έλλειψη αναφοράς περί καρτών αυτόματης συναλλαγής, συνεπάγεται ότι η έκταση του άρθρου δεν περιορίζεται αποκλειστικά στην περίπτωση της παράνομης ανάληψης χρημάτων από ένα ΑΤΜ, αλλά επεκτείνεται και καλύπτει και την περίπτωση της χωρίς δικαίωμα μεταφοράς χρημάτων από τον τραπεζικό λογαριασμό του δικαιούχου σε αυτόν του δράστη ή τρίτου.

5.4 Το φαινόμενο «Skimming»

Ένα φαινόμενο το οποίο έχει παρατηρηθεί εδώ και κάποια χρόνια, είναι οι παγιδεύσεις των αυτόματων ταμειολογιστικών μηχανημάτων (ΑΤΜ), μία μέθοδος γνωστή και ως «skimming». Η μέθοδος του skimming είναι ένας τρόπος παρέμβασης στην ομαλή λειτουργία μίας τερματικής συσκευής πώλησης ή ανάληψης χρημάτων, με τον οποίο ο δράστης καταφέρνει να αποσπάσει μεγάλα χρηματικά ποσά από τους τραπεζικούς λογαριασμούς των θυμάτων. Πως λειτουργεί όμως η μέθοδος αυτή;

Αρχικά, ο παραβάτης εγκαθιστά συσκευές σε τερματικές συσκευές όπως ΑΤΜ, POS (point-of-sale) κ.λπ. Ο ρόλος των συσκευών αυτών, είναι η καταγραφή των διαπιστευτηρίων που στη συνέχεια θα εισάγει ο χρήστης προκειμένου να αποκτήσει πρόσβαση στον τραπεζικό του λογαριασμό. Παράλληλα, καταγράφονται και τα στοιχεία της κάρτας, τα οποία χρησιμοποιούνται για τη δημιουργία πλαστών καρτών (κλώνων),

[122] Γίνεται αναφορά για υπεξουσιοδότηση καθώς ορθότερο είναι ως εξουσιοδοτημένος να θεωρείται ο κύριος της κάρτας ή του ηλεκτρονικού λογαριασμού από την τράπεζα, ο οποίος και στη συνέχεια υπεξουσιοδοτεί κάποιον τρίτο - Βλ. Σάμιος Θ., Η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων ως τρόπος τελέσεως της απάτης με υπολογιστή (άρθρο 386Α' ΠΚ), σελ. 539

με τις οποίες στη συνέχεια πραγματοποιούνται οι υπεξαιρέσεις. Τα στοιχεία που υποκλέπτονται από τις συσκευές αυτές, μπορούν να αποσταλούν στους δράστες είτε ασύρματα, είτε όταν αυτοί τις πάρουν στην κατοχή τους.

Οι συσκευές που χρησιμοποιούνται για την παγίδευση ενός ΑΤΜ μπορεί να είναι[123]:

- μικροσκοπικές κάμερες οι οποίες τοποθετούνται σε κάποιο μη εμφανές σημείο του ΑΤΜ και είναι δύσκολα ορατές με γυμνό μάτι.
- πλαστικές επικαλύψεις που τοποθετούνται πάνω από το πληκτρολόγιο του ΑΤΜ και καταγράφει τη σειρά των αριθμών που πληκτρολογεί το άτομο.
- πλαστικές επικαλύψεις που τοποθετούνται πάνω από τη θυρίδα υποδοχής της κάρτας στο ΑΤΜ και κατά την εισαγωγή της αντιγράφει τα δεδομένα που είναι αποθηκευμένα στη μαγνητική λωρίδα της (τσιπ).

Το φαινόμενο του skimming έχει λάβει τέτοιες διαστάσεις σε παγκόσμια κλίμακα, που σύμφωνα με έρευνα του FBI[124], οι ετήσιες απώλειες των ιδιωτών και των τραπεζών ανέρχονται σε σχεδόν 1 δισεκατομμύριο δολάρια, με το ποσό αυτό να εξακολουθεί να αυξάνεται δραματικά. Παράλληλα, το 2022 σημειώθηκε αύξηση των περιστατικών skimming που άγγιξε το 368% σε σχέση με την περασμένη χρονιά[125].

[123] https://www.bankrate.com/banking/what-is-atm-skimming/

[124] Βλ. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/skimming

[125] https://www.fico.com/blogs/us-card-skimming-grew-nearly-5x-2022-new-fico-data-shows

Πηγή: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/skimming

5.4.1 Ποινική Αξιολόγηση του Skimming

Με την μέθοδο του skimming, της παγίδευσης δηλαδή ενός ATM ή μιας τερματικής συσκευής πληρωμής (Point Of Sale) με μέσα, ο δράστης αποσκοπεί στην απόκτηση των ατομικών διαπιστευτηρίων του χρήστη, καθώς και των στοιχείων της προσωπικής του κάρτας αυτόματης συναλλαγής. Τις πληροφορίες αυτές, τις χρησιμοποιεί στη συνέχεια προκειμένου να κατασκευάσει καινούργιες κάρτες-κλώνους στις οποίες και αντιγράφει τα δεδομένα αυτά. Τέλος, αξιοποιώντας την κάρτα-κλώνο, προβαίνει στην υπεξαίρεση χρηματικών ποσών από τον τραπεζικό λογαριασμό του

θύματος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος.

Η απόκτηση των προσωπικών διαπιστευτηρίων του χρήστη, μέσα στα οποία πρέπει να συγκαταλέγονται και τα στοιχεία που βρίσκονται εντός της μαγνητικής λωρίδας της κάρτας του[126], τα οποία είναι μοναδικά και αποτελούν μαζί με την υπόλοιπη κάρτα μέρος της συμβάσης του ιδιώτη με το τραπεζικό ίδρυμα, εκ πρώτης όψεως μπορεί να εμφανίζει αρκετές ομοιότητες με την τεχνική του phishing. Υπάρχει όμως μία βασική διαφορά η οποία εντοπίζεται στην πράξη ουσιαστικής αποπεράτωσης του εγκλήματος.

Στην περίπτωση του skimming, μόλις ο εγκληματίας αποκτήσει τα δεδομένα της κάρτας του θύματος, προβαίνει στη συνέχεια στη δημιουργία όμοιων καρτών, τις οποίες αξιοποιεί εν τέλει προκειμένου να αποκτήσει πρόσβαση και έλεγχο επί του λογαριασμού του χρήστη. Το γεγονός της χρήσης πλαστής κάρτας με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτοντας την περιουσία τρίτου με τον επηρεασμό της διαδικασίας επεξεργασίας δεδομένων υπολογιστή, κατά κρατούσα άποψη[127], πληροί την α.υ. του εγκλήματος της απάτης με υπολογιστή (386Α ΠΚ). Συγκεκριμένα με την εγκληματική αυτή του συμπεριφορά, ο δράστης χρησιμοποιεί[128] μη ορθά ψηφιακά δεδομένα και συγκεκριμένα δεδομένα αναγνώρισης ταυτότητας (πλαστές κάρτες αυτόματης συναλλαγής), προκειμένου να επηρεάσει την ορθή λειτουργία ενός υπολογιστικού συστήματος (εν προκειμένω του ΑΤΜ). Αντιθέτως, στην περίπτωση του phishing, δεν μπορεί να γίνει αναφορά περί μη ορθότητας ή έλλειψης των στοιχείων, καθώς σε ανάλογη περίπτωση δε θα του επιτρεπόταν η πρόσβαση στο λογαριασμό.

Αρχικά, το ΑΤΜ από τη στιγμή που έχει αυτόνομο επεξεργαστή με τον οποίο εκτελεί τις εντολές που του εισάγονται θα πρέπει να αντιμετωπίζεται ως υπολογιστής. Όταν μία κάρτα αυτόματης συναλλαγής εισαχθεί εντός ενός ΑΤΜ και «ξεκλειδωθεί» εισάγοντας το ορθό κωδικό πρόσβασης (PIN), τότε πραγματοποιείται αντιστοίχιση του διασυνδεδεμένου σε αυτή λογαριασμού του χρήστη με αυτόν που βρίσκεται αποθηκευμένος στις βάσεις δεδομένων του τραπεζικού ιδρύματος. Ο όρος του

[126] Βλ. Σάμιος Θ., Η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων ως τρόπος τελέσεως της απάτης με υπολογιστή (άρθρο 386Α' ΠΚ), σελ. 524

[127] Βλ. ΑΠ 1087/2019 καθώς και ΑΠ 908/2020

[128] Ως χρησιμοποίηση θεωρείται η εισαγωγή των στοιχείων σε ένα υπολογιστικό σύστημα, προκειμένου αυτά να καταστούν αντικείμενο επεξεργασίας - Βλ. Σάμιος Θ., Η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων ως τρόπος τελέσεως της απάτης με υπολογιστή (άρθρο 386Α' ΠΚ), σελ. 525

«επηρεασμού του αποτελέσματος διαδικασίας επεξεργασίας δεδομένων» αναφέρεται στο γεγονός ότι το παραγόμενο αποτέλεσμα (της εισόδου στον τραπεζικό λογαριασμό του νόμιμου δικαιούχου και παροχής της δυνατότητας πραγματοποίησης αναλήψεων από αυτόν) δεν θα έπρεπε να είχε πραγματοποιηθεί με τη στιγμή που δεν είχε εισαχθεί σε αυτό η γνήσια κάρτα του δικαιούχου, αλλά μία πλαστή απομίμηση.

Όπως και στην περίπτωση του phishing, βασικό στοιχείο της α.υ.ε είναι ο σκοπός του δράστη να προσπορίσει σε αυτόν παράνομο περιουσιακό όφελος, εις βάρος κάποιου φυσικού ή νομικού προσώπου, καθώς και η αιτιώδης συνάφεια μεταξύ των δυο αυτών περιουσιακών μεταβιβάσεων.

5.4.2 Τρόποι προστασίας από το Skimming

Μεταξύ των ενεργειών που μπορεί να εφαρμόσει ο κάθε χρήστης για να αποφύγει να πέσει θύμα αυτού του είδους της ηλεκτρονικής απάτης είναι:

- Απόκρυψη του PIN κατά την πληκτρολόγηση

Αποτελεί το πιο απλό αλλά ταυτόχρονα ουσιώδες μέτρο που πρέπει να εφαρμόζει ο καθένας. Ακόμα και στην περίπτωση όπου υπάρχει πλησίον του ATM εγκατεστημένη από το δράστη μία κάμερα για την υποκλοπή των στοιχείων που αυτός εισάγει, ο χρήστης θα είναι προστατευμένος εάν το PIN που εισάγει δεν είναι ορατό.

- Προτίμηση των ανέπαφων συναλλαγών

Καθώς οι συσκευές παγίδευσης δύνανται εκτός από ATM να τοποθετηθούν και σε τερματικές μηχανές πληρωμής (POS), η επιλογή πληρωμής με τη χρήση καρτών ανέπαφα χωρίς την απαίτηση για εισαγωγή του PIN, αποτελεί ένα απλό βήμα για τον περιορισμό του φαινομένου αυτού.

- Έλεγχος του ATM για οτιδήποτε ύποπτο, σπασμένο, χαλαρό ή γρατσουνισμένο μπορεί να βρίσκεται επί αυτού[129]

Οι «skimmers» επιδιώκουν οι συσκευές παγίδευσης που θα χρησιμοποιήσουν να μην είναι εύκολα ορατές και αντιληπτές από το μέσο χρήστη. Επίσης θα πρέπει να φαίνονται σαν να αποτελούν φυσικό τμήμα του ATM ενώ το χρώμα τους πρέπει είναι

[129] https://www.entrepreneur.com/business-news/what-is-card-skimming-heres-how-to-prevent-the-rising/450457

εναρμονισμένο με το σύνολο, προκειμένου να μην προκαλέσουν τυχόν υποψίες στους χρήστες.

- Χρησιμοποίηση ΑΤΜ που βρίσκονται σε κεντρικά σημεία ή εντός τραπεζικών καταστημάτων

Όπως είναι εύκολα αντιληπτό, ένα ΑΤΜ το οποίο βρίσκεται σε κεντρικό σημείο, φυλάσσεται σε διαρκή βάση ή βρίσκεται εντός του καταστήματος, δύσκολα θα αποτελέσει στόχο για παγίδευση από έναν εγκληματία.

- Ενεργοποίηση δυνατότητας λήψης ειδοποιήσεων για τις κινήσεις που πραγματοποιούνται στο λογαριασμό

Όταν ο χρήστης ειδοποιείται ηλεκτρονικά μέσω του κινητού του τηλεφώνου για κάθε κίνηση που συμβαίνει στον τραπεζικό του λογαριασμό, είναι σε θέση να ελέγχει καλύτερα και να διαπιστώσει αμέσως τυχόν ανεπιθύμητες συναλλαγές που πραγματοποιούνται χωρίς την έγκρισή του.

- Άμεση ενημέρωση της τράπεζας σε περίπτωση κράτησης της κάρτας από το ΑΤΜ[130]

Όταν με την ολοκλήρωση ή ακύρωση μίας συναλλαγής, δεν επιστραφεί η κάρτα στο χρήστη, τότε αυτός οφείλει να ενημερώσει άμεσα το τραπεζικό ίδρυμα, προκειμένου να προβεί στην ακύρωση και στην επανέκδοση αυτής. Με τον τρόπο αυτό, ακόμα και αν έχει κατορθώσει ο δράστης να αποκτήσει αντίγραφο των ψηφιακών δεδομένων της κάρτας, δε θα μπορεί να την αξιοποιήσει για δημιουργία πλαστών αντιγράφων αυτής.

- Χρήση καρτών που διαθέτουν τεχνολογία chip

Οι κάρτες που έχουν ενσωματωμένη την τεχνολογία τσιπ, έχουν κρυπτογραφημένες τις πληροφορίες που είναι αποθηκευμένες σε αυτές. Αυτό βέβαια δεν λειτουργεί ως πανάκεια, αλλά παρέχει επιπλέον προστασία στους χρήστες, καθώς οι συσκευές παγίδευσης που μπορούν να υποκλέψουν στοιχεία από αυτού του είδους τις κάρτες είναι σημαντικά λιγότερες συγκριτικά με εκείνες που στοχεύουν στις κάρτες μαγνητικών λωρίδων (magnetic stripe).

[130] https://www.bankrate.com/banking/what-is-atm-skimming/#avoid

6 Επίλογος - Συμπεράσματα

Η τεχνολογία μέσω των ηλεκτρονικών υπολογιστών μας έχει καλωσορίσει σε ένα νέο, και άνευ περιορισμών όσον αφορά τις επιλογές, κόσμο. Δυνατότητες οι οποίες μέχρι πριν λίγα χρόνια φάνταζαν προϊόν της επιστημονικής φαντασίας, έχουν καταστεί πλέον εφικτές με το πάτημα ενός πλήκτρου, εκμηδενίζοντας τις αποστάσεις και σαφέστατα παρέχοντας ασυναγώνιστη ευκολία και άνεση στους χρήστες.

Η επιδημιολογική πανδημία του COVID-19, παράλληλα μαζί με όλες τις υπόλοιπες επιπτώσεις που επέφερε, ίσως αποτέλεσε το προοίμιο για την ψηφιοποίηση αρκετών διαδικασιών της καθημερινότητάς μας. Παράλληλα όμως, κάθε φορά που μία τεχνολογική καινοτομία μας καλωσορίζει σε ένα νέο κόσμο, αυτός λειτουργεί και ως πρόσφορο έδαφος για την εμφάνιση και ευδοκίμηση νέων μορφών αξιόποινων συμπεριφορών. Αντιστοίχως, όσο συνεχίζουμε να εξερευνούμε τα όρια του απέραντου κόσμου της τεχνολογίας με φρενήρη ρυθμό, οι νέες μορφές παραβατικών συμπεριφορών συνεχίζουν να πολλαπλασιάζονται, απαιτώντας τη διαρκή επαγρύπνηση του νομοθέτη. Συνάμα, ο διασυνοριακός χαρακτήρας τους επιβάλλει τη διακρατική συνεργασία των διωκτικών αρχών για την αποτελεσματική πρόληψη και καταστολή τους, ενώ η νομοθετική τάξη κάθε χώρας οφείλει να προσαρμόζεται και να συμβαδίζει με τις διεθνείς συμβάσεις και εξελίξεις, ούτως ώστε να επιτυγχάνεται και μία ορθότερη σε ποινικό πλαίσιο αντιμετώπισή τους.

Η ηλεκτρονική απάτη αποτελεί μία από τις χαρακτηριστικότερες και συνηθέστερες εκφάνσεις του ηλεκτρονικού εγκλήματος σήμερα. Σύμφωνα με πρόσφατη μελέτη της πολυεθνικής εταιρείας IBM[131], το 83% των εταιρειών σε παγκόσμια κλίμακα έχουν υποστεί ηλεκτρονικές απάτες τουλάχιστον μία φορά από τη στιγμή της ίδρυσής τους. Οι κίνδυνοί στο τεχνολογικό περιβάλλον ελλοχεύουν διαρκώς και πληθαίνουν, ενώ σε πολλές περιπτώσεις δεν υπάρχει κατάλληλο μέτρο που να μπορεί να εγγυηθεί την πλήρη ακεραιότητα. Ο ισχυρισμός του Robert Mueller[132] ότι «υπάρχουν δύο είδη εταιρειών: αυτές που έχουν πέσει θύμα hacking και αυτές που δεν έχουν πέσει θύμα ακόμα», αποτελεί ίσως μία περισσότερο ρεαλιστική, παρά πεσιμιστική αντίληψη.

---

131 Βλ. https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High

132 Πρώην διευθυντή του FBI, δικηγόρου και ειδικού εισαγγελέα

Αυτό που αποτελεί γεγονός καίριας σημασίας και οφείλει κάθε συνειδητός χρήστης του κυβερνοχώρου να κατανοήσει, είναι ότι η πανάκεια, όταν αναφερόμαστε στην ασφάλεια σε τεχνολογικό περιβάλλον, αποτελεί μάλλον μία ουτοπική αντίληψη. Η σωστή ενημέρωση για τους κινδύνους που εγκυμονεί η χρήση του διαδικτύου μπορεί να συμβάλει στην αποφυγή ανεπιθύμητων καταστάσεων, καθώς και να επιβεβαιώσει τον ισχυρισμό ότι η πρόληψη αποτελεί πάντα την καλύτερη θεραπεία.

7 Βιβλιογραφική Επισκόπηση

7.1 Ελληνική Βιβλιογραφία

1) Αγγελής Ι., Διαδίκτυο και Ποινικό Δίκαιο, ΠοινΧρ Ν/2000
2) Βασιλάκη Ε., Τα φαινόμενα phishing και pharming και η ποινική τους αξιολόγηση, ΠοινΧρ ΝΖ/2007
3) Δαλακούρας Θ., Έννοια, διακρίσεις και χαρακτηριστικά των εγκλημάτων στον κυβερνοχώρο, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη
4) Δαλακούρας Θ., Οι ειδικότερες διατάξεις της Σύμβασης για το έγκλημα στον κυβερνοχώρο, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη
5) Δαλακούρας Θ., Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη
6) Ιγγλεζάκης Ι., Έγκλημα πληροφορικής, Κυβερνοέγκλημα και κυβερνοασφάλεια, Δίκαιο Πληροφορικής, 2021, 4η έκδοση, εκδ. Σάκκουλα
7) Κάτος Β., Ψηφιακά Πειστήρια, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη
8) Κάτος Β., Η φύση των ψηφιακών πειστηρίων, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη
9) Κιούπης Δ., Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, 2000
10) Κιούπης Δ., Ποινικό δίκαιο και internet, 1999
11) Κιούπης Δ., Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη
12) Κουράκης Ν., Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001
13) Μπουρμάς Γ., Στοιχεία Απάτης με ΗΥ κατ' άρθρο 386Α ΠΚ και διάκριση από την Κοινή Απάτη του 386 ΠΚ, 2001
14) Μοροζίνης Ι., Η μεταφορά χρημάτων «χωρίς δικαίωμα» ως προσβολή της περιουσίας, Ηλεκτρονικό Έγκλημα, 2019, εκδ. Νομική Βιβλιοθήκη
15) Μυλωνόπουλος Χρ., Ποινικό Δίκαιο – Ειδικό Μέρος, 4η έκδοση, 2021, εκδ. Νομική Βιβλιοθήκη

16) Μυλωνόπουλος Χρ., Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991
17) Ναμίας Ο., Σύγχρονες μορφές (ηλεκτρονικής) απάτης στις τραπεζικές συναλλαγές, ΠοινΧρ ΝΓ/2003
18) Νούσκαλης Γ., Απάτη με ΗΥ – Παρελθόν και Μέλλον του άρθρου 386Α ΠΚ υπό το πρίσμα των εξελίξεων στην ΕΕ, ΠοινΔικ 2/2003
19) Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, Άρθρα 385-406 ΠΚ, Εγκλήματα Περιουσιακής μετάθεσης, 2000, εκδ. Σάκκουλα
20) Σάμιος Θ., Η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων ως τρόπος τελέσεως της απάτης με υπολογιστή (άρθρο 386Α' ΠΚ), 2003
21) Τζαννετής Αρ., Το πλαστό έγγραφο, ΠοινΧρ, 2021, εκδ. Σάκκουλα
22) Φραγκάκης Δ, Ιστορικά Αρχεία στο Διαδίκτυο, Βιβλιοθήκες και Πληροφόρηση, τεύχος 16, 2003
23) Χλούπης Γ., Υπερεθνικό Έγκλημα με τη χρήση Η/Υ, 1999

7.2 Ξενόγλωσση Βιβλιογραφία

1) Internet of Things Applications, Challenges and Related Future Technologies, World Scientific News 67(2) (2017) 126-148
2) Internet of Things Applications, Challenges and Related Future Technologies, World Scientific News 67(2) (2017) 126-148
3) A Detailed Study on Wireless LAN Technologies - Vijay Chandramouli,. Department of Computer Science and Engineering, The University of Texas at Arlington
4) https://www.nccoe.nist.gov/iot
5) https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing
6) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
7) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf
8) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-157.pdf

7.3 Βιβλιογραφία από Ανοιχτές Πηγές – Διαδίκτυο

1) https://www.statista.com/statistics/209096/share-of-internet-users-in-the-total-world-population-since- 2006/
2) https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/
3) http://www2.ic.uff.br/~michael/kr1999/1-introduction/1_02-protocol.htm
4) https://www.informatique-mania.com/el/linternet/quels-types-de-reseaux-informatiques-existent/
5) https://www.fortinet.com/resources/cyberglossary/what-is-dns
6) https://www.computerhope.com/jargon/s/server.htm
7) https://www.britannica.com/technology/P2P
8) https://www.bbvaopenmind.com/en/articles/the-internet-global-evolution-and-challenges/
9) https://www.internetsociety.org/internet/history-internet/brief-history-internet
10) https://www.livescience.com/internet
11) https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission-control-protocol--tcp
12) https://www.javatpoint.com/what-is-world-wide-web
13) http://www.eeei.gr/odhgos/netsc404/whaturl.htm
14) https://www.lab.com.gr/deep-web-%CE%BA%CE%B1%CE%B9-dark-web-%CF%84%CE%BF-%CE%AC%CE%B3%CE%BD%CF%89%CF%83%CF%84%CE%BF-internet/
15) https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different
16) https://www.the-sun.com/lifestyle/tech-old/271948/what-dark-web-how-work/
17) https://www.youtube.com/watch?v=xHeOUd4E9As&ab_channel=SecNewsTV
18) https://hqsoftwarelab.com/blog/the-history-of-iot-a-comprehensive-timeline-of-major-events- infographic/
19) https://edu.gcfglobal.org/en/computer-science/hardware-and-software/1/#
20) https://el.wikipedia.org/wiki/%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CF%82

21) https://stigma.host/programming-languages/
22) http://karakos.gr/apospasma.pdf
23) https://www.statista.com/statistics/700894/global-ransom-payers-rate/
24) https://www.avast.com/c-hacker-types
25) http://cisco.num.edu.mn/CCNA_R&S1/course/module11/11.2.1.1/11.2.1.1.html
26) https://aag-it.com/the-latest-phishing-statistics/
27) https://safety.google/gmail/ και
https://support.google.com/a/answer/9157861?hl=en
28) https://us.norton.com/blog/online-scams/what-is-phishing
29) https://ie.norton.com/blog/how-to/the-importance-of-general-software-updates-and-patches
30) https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
31) https://csrc.nist.gov/glossary/term/pharming
32) https://www.imperva.com/learn/application-security/dns-hijacking-redirection/
33) https://www.securesenses.net/2022/08/rogue-dns-server.html
34) https://www.kaspersky.com/resource-center/definitions/pharming
https://securelist.com/dns-manipulation-in-venezuela/89592/
35) https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/texnika_metra
36) https://www.kaspersky.com/resource-center/definitions/pharming
37) https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-does-a-chip-card-work
38) https://en.wikipedia.org/wiki/Online_banking
39) https://www.bankrate.com/banking/what-is-atm-skimming/
40) https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/skimming
41) https://www.fico.com/blogs/us-card-skimming-grew-nearly-5x-2022-new-fico-data-shows
42) https://www.entrepreneur.com/business-news/what-is-card-skimming-heres-how-to-prevent-the-rising/ 450457
43) https://www.bankrate.com/banking/what-is-atm-skimming/#avoid

44) https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High

7.4 Αποφάσεις

1) ΑΠ 908/2020
2) ΑΠ 1087/2019
3) ΑΠ 96/2017
4) ΑΠ 65/2016
5) ΑΠ 742/2012
6) ΑΠ 1152/1999
7) ΑΠ 751/1998
8) ΤρΕφΚακΑθ 4689/2018

8 Κυρώσεις για λογοκλοπή

Η λογοκλοπή είναι ένα πολύ σοβαρό παράπτωμα. Με απόφαση με το άρθ. 7.2 του Κανονισμού «σε περιπτώσεις λογοκλοπής ή παράλειψης αναφοράς στη μεταπτυχιακή Διπλωματική Εργασία, η ελάχιστη κύρωση, μετά από απόφαση της ΕΔΕ, είναι η υποχρέωση του φοιτητή να επιλέξει άλλον επιβλέποντα καθηγητή με διαφορετικό θέμα Διπλωματικής και να επαναλάβει το τρίτο εξάμηνο με ανάλογες πρόσθετες οικονομικές υποχρεώσεις, ενώ μέγιστη κύρωση μπορεί να είναι η οριστική διαγραφή του από το Πρόγραμμα. Εάν έχει ήδη αποφοιτήσει, ανακαλείται το Μεταπτυχιακό Δίπλωμα Ειδίκευσης και προωθείται το θέμα στο Δικαστικό Γραφείο του Πανεπιστημίου για την έναρξη των ανάλογων νομικών διαδικασιών».