ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΘΕΜΑ: Η απάτη με υπολογιστή (386^{A} ΠΚ)

Διπλωματική Εργασία

της

Σκλαβούνου Μαγδαληνής-Χριστίνας

Επιβλέπων καθηγητής:

κ. Δαλακούρας Θεοχάρης

Θεσσαλονίκη, Νοέμβριος 2023

Η απάτη με υπολογιστή (386^{A} ΠΚ)

Σκλαβούνου Μαγδαληνή – Χριστίνα

Πτυχίο Νομικής, Δημοκρίτειο Πανεπιστήμιο Θράκης, 2021

Διπλωματική Εργασία
υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων
του ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
κ. ΔΑΛΑΚΟΥΡΑΣ ΘΕΟΧΑΡΗΣ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 13/11/2023

ΔΑΛΑΚΟΥΡΑΣ	ΔΑΝΙΗΛ	ΣΑΒΒΙΔΗΣ
ΘΕΟΧΑΡΗΣ	ΓΕΩΡΓΙΟΣ	ΝΙΚΟΛΑΟΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία, εκπονείται στα πλαίσια του μαθήματος «Ηλεκτρονικό Έγκλημα» και του Διϊδρυματικού προγράμματος μεταπτυχιακών σπουδών **«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»**, των πανεπιστημίων της Μακεδονίας και του Δημοκρίτειου Πανεπιστημίου Θράκης.

Η ραγδαία ανάπτυξη των νέων τεχνολογιών, με την οποία ερχόμαστε καθημερινά αντιμέτωποι, πέρα από τα οφέλη που μας έχει προσφέρει, συνεπάγεται ταυτόχρονα και την ανάπτυξη της ηλεκτρονικής εγκληματικότητας, η οποία τα τελευταία χρόνια αποτελεί έναν από τους τομείς που απασχολούν όλο και περισσότερο την Νομική Επιστήμη και πιο συγκεκριμένα το Ποινικό Δίκαιο.

Μία από τις σημαντικότερες εκφάνσεις της είναι και το ζήτημα του Άρθρου 386Α ΠΚ, δηλαδή η **«Απάτη με υπολογιστή»**, το οποίο άρθρο εισήχθη για πρώτη φορά στον Ελληνικό Ποινικό Κώδικα με τον Ν. 1805/1988. Σκοπός της παρούσας εργασίας είναι η ανάλυση της ποινικής αυτής διάταξης, με αναλυτική παρουσίαση του διωκόμενου εγκλήματος, των περιγραφόμενων περιπτώσεων τέλεσης αλλά και της ποινικής τους αντιμετώπισης.

Ειδικότερα, στο πρώτο μέρος της παρούσας εργασίας θα πραγματοποιηθεί προσπάθεια απόδοσης του ορισμού της πολυσυζητημένης έννοιας του ηλεκτρονικού εγκλήματος, περιγραφή των βασικών χαρακτηριστικών του, καθώς και αναφορά στην διάκριση των ηλεκτρονικών εγκλημάτων.

Στο δεύτερο μέρος γίνεται αναφορά στο Διεθνές και Ενωσιακό νομικό πλαίσιο που καλύπτει τόσο το αδίκημα της απάτης με υπολογιστή (386^{A} ΠΚ), όσο και τα ηλεκτρονικά εγκλήματα εν γένει και πιο συγκεκριμένα θα πραγματοποιηθεί αναφορά στην Οδηγία 2013/40/ΕΕ, στην Οδηγία 2019/713/ΕΕ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμών πλην των μετρητών και στη Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα.

Στη συνέχεια, το τρίτο μέρος της παρούσας εργασίας εστιάζει στο εθνικό νομικό πλαίσιο για την αντιμετώπιση της απάτης με υπολογιστή (386^{A} ΠΚ), με εκτενή αναδρομή στην ιστορική εξέλιξη του άρθρου 386^{A} ΠΚ, με ειδικότερες αναφορές στο προστατευόμενο έννομο αγαθό της διάταξης, στην αντικειμενική και υποκειμενική του υπόσταση, στους τρόπους τέλεσης του αδικήματος, σε ζητήματα απόπειρας, συμμετοχής, συρροής, καθώς επίσης και στις προνομιούχες και διακεκριμένες παραλλαγές του αδικήματος.

Στο τέταρτο μέρος επιχειρείται μία σύγκριση του ιδιώνυμου εγκλήματος του Άρθρου 386Α ΠΚ με την περίπτωση της Απάτης «μέσω» υπολογιστή, η οποία υπάγεται στο Άρθρο 386 ΠΚ.

Στο πέμπτο και τελευταίο κεφάλαιο παρουσιάζονται εκτενώς σύγχρονες μορφές απάτης που τελούνται είτε με, είτε «μέσω» υπολογιστή, οι οποίες στοιχειοθετούν είτε το αδίκημα της κοινής απάτης (386 ΠΚ), είτε το αδίκημα της απάτης με υπολογιστή (386^{A} ΠΚ), όπως τα φαινόμενα «skimming», «phishing» και «pharming».

Τέλος, τονίζεται η σημασία της διάταξης της απάτης με υπολογιστή και η ανάγκη εγρήγορσης απέναντι στην ηλεκτρονική εγκληματικότητα.

Λέξεις – κλειδιά: Απάτη με υπολογιστή, Διαδίκτυο, Ηλεκτρονική Εγκληματικότητα, Πρόγραμμα υπολογιστή, Κυβερνοχώρος, Κυβερνοέγκλημα, «skimming», «phishing» και «pharming».

Συμβολισμοί (αν υπάρχουν)

ΠΚ: ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ

ΚΠΔ: ΚΩΔΙΚΑΣ ΠΟΙΝΙΚΗΣ ΔΙΚΟΝΟΜΙΑΣ

πχ: Παραδείγματος Χάριν

σελ.: σελίδα

Βλ.: Βλέπετε

Ν.: Νόμος

Ποιν. Χρον.: Ποινικά Χρονικά

Ποιν. Δικ.: Ποινική Δικαιοσύνη

ΑΠ: Άρειος Πάγος

Η/Υ: Ηλεκτρονικός Υπολογιστής

ΕΕ: Ευρωπαϊκή Ένωση

ΕΙΣΑΓΩΓΗ

Κοινό τόπο αποτελεί πλέον η διαπίστωση ότι η ολοένα αυξανόμενη χρήση του διαδικτύου και των τεχνολογιών πληροφορικής και επικοινωνιών διασυνδέεται ευθέως με την τέλεση παλιών και νεότερων μορφών ποινικών αδικημάτων. Το κυβερνοέγκλημα παράγει ευθέως απρόβλεπτες απειλές για την κοινωνική ευταξία, στο βαθμό που στρέφεται τόσο κατά φυσικών και νομικών προσώπων που στηρίζονται στις νέες τεχνολογίες, όσο συνακόλουθα και κατά κρατικών οντοτήτων και κυβερνητικών πολιτικών. Ενόψει τούτου ακριβώς του στοιχείου της παγκοσμιότητας των δεδομένων, το κυβερνοέγκλημα εμφανίζεται ως διαφορετική από άποψη υφής και έκτασης απειλή για την ασφάλεια της κοινωνίας της πληροφορίας, αλλά και για μια σειρά εννόμων αγαθών και ελευθεριών των πολιτών παγκοσμίως[1].

Τα περισσότερα κράτη εντόπισαν ήδη από τον προηγούμενο αιώνα την ανάγκη νομοθετικής ρύθμισης των περιπτώσεων εγκλημάτων μέσω συστημάτων τεχνολογίας, σε μία προσπάθεια να προλάβουν τις εξελίξεις. Βέβαια, στην πορεία έγινε εμφανές ότι αυτό δεν είναι αρκετό, καθώς η συνεχής εξέλιξη της τεχνολογίας συνεπάγεται και τη συνεχή εξέλιξη των εγκληματικών πράξεων μέσω αυτής. Επομένως, κατέστη αναγκαία η συχνή προσαρμογή των νομοθετημάτων στα νέα δεδομένα, με σκοπό την καλύτερη αντιμετώπιση των ελλειμματικών ενεργειών, αλλά και η νομοθετική προσπάθεια για ενιαία διακρατική δράση[2], καθώς το ηλεκτρονικό έγκλημα ενδέχεται να είναι διασυνοριακό και παγκόσμιο[3].

Ακριβώς σε αυτά τα πλαίσια, δηλαδή της ανάγκης για ενιαία διακρατική δράση και κοινή νομοθετική αντιμετώπιση, η Ευρωπαϊκή Ένωση προέβη σε μία σημαντική κίνηση, υπογράφοντας το 2001 τη Σύμβαση της Βουδαπέστης για το «Έγκλημα στον Κυβερνοχώρο»[4]. Αν και αυτή δεν αποτέλεσε την πρώτη προσπάθεια της Ευρώπης για ρυθμίσεις σχετικά με την ηλεκτρονική εγκληματικότητα[5], εντούτοις ήταν αυτή με την μεγαλύτερη βαρύτητα, καθώς αποτελεί πλέον τη βάση για τις ρυθμίσεις και τις έκτοτε νομοθετικές πρωτοβουλίες σε επίπεδο ευρωπαϊκών κρατών

---

[1] Βλ. Δαλακούρας Θ., Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη (Έκδοση: 2η) 2023, σελ. 1.

[2] Η Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο (2001), αναφέρει, μεταξύ άλλων, στο Προοίμιό της, την ανάγκη για κοινή αντεγκληματική πολιτική για το κυβερνοέγκλημα, λόγω των θεμελιωδών αλλαγών στα δίκτυα υπολογιστών. Βλ. https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0

[3] Ο «Παγκόσμιος» χαρακτήρας του διαδικτύου συνεπάγεται την ανάγκη για ενιαία νομοθετική και κατασταλτική δράση των εθνικών τάξεων. Βλ. Φαραντούρης, Ν. Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, ΠοινΔικ, 2/2003, σελ. 191-196, ιδίως σελ. 196.

[4] Βλ. Δαλακούρας Θ., Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη (Έκδοση: 2η) 2023, σελ. 2.

[5] Μία πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος σε επίπεδο Ευρώπης έγινε σε Συνέδριο του Συμβουλίου της Ευρώπης το 1976 για το Οικονομικό Έγκλημα, ενώ έπειτα ακολούθησε η έκδοση τριών συστάσεων σχετικών με την ηλεκτρονική εγκληματικότητα. Βλ. Δαλακούρας, Θ. Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2023, σελ. 2.

Όπως αναφέρθηκε και παραπάνω, οι μεγάλες τεχνολογικές εξελίξεις και η ευρεία χρήση του διαδικτύου προκάλεσαν την εμφάνιση νέων «ευφυών» μορφών οικονομικού εγκλήματος. Η παρούσα διπλωματική εργασία εξετάζει υπό το πρίσμα των νέων μορφών εγκληματικότητας την εφαρμογή της διάταξης που ρυθμίζει την «ηλεκτρονική» απάτη, καθώς και τη διάκριση της από την «κοινή» απάτη. Η υπαγωγή της σύγχρονης εγκληματικότητας στον κατάλληλο νομικό κανόνα αλλά και γενικότερα νομική αντιμετώπιση του ηλεκτρονικού εγκλήματος δεν απαιτεί μόνο επαρκή γνώση του ποινικού δικαίου αλλά και κατανόηση του τρόπου λειτουργίας της νέας τεχνολογίας.[6]

Άλλωστε είναι γεγονός πως σε «Λερναία Ύδρα», της οποίας η εξόντωση είναι αδύνατη, παραπέμπουν οι **διαδικτυακές και τηλεφωνικές απάτες** που εκτιμάται ότι προκαλούν κάθε χρόνο απώλειες πολλών εκατοντάδων εκατομμυρίων ευρώ τα τελευταία χρόνια.

Οι επιτήδειοι –ελληνικά και διεθνή κυκλώματα– εφευρίσκουν συνεχώς νέους τρόπους εξαπάτησης, αλλά πάντοτε χρησιμοποιούν τη μέθοδο της κοινωνικής μηχανικής για να χειραγωγήσουν ανυποψίαστους πολίτες και να αποσπάσουν πολύτιμες πληροφορίες, όπως **τραπεζικούς κωδικούς**.

Η **Ελληνική Ένωση Τραπεζών (ΕΕΤ)** υπολόγισε πρόσφατα σε περίπου 500.000 ευρώ ανά ημέρα, ή 175 εκατ. ευρώ τον χρόνο, τη λεία χάκερ τραπεζικών λογαριασμών, έστω κι αν πολλά από τα περιστατικά αυτά αποτρέπονται μέσω τεχνολογικών συστημάτων πρόβλεψης της απάτης. Ωστόσο, οι απώλειες εκτιμάται ότι είναι πολύ μεγαλύτερες. Κι αυτό επειδή τα θύματα σε πολλές περιπτώσεις διστάζουν να γνωστοποιήσουν στις Αρχές τα περιστατικά, ενώ ενίοτε δαπανούν σημαντικά ποσά αναθέτοντας σε αμφιβόλου αποτελεσματικότητος ειδικούς (π.χ. ανεξάρτητοι ερευνητές) τον εντοπισμό των δραστών[7].

Συνεπώς είναι γεγονός, ότι στη σημερινή εποχή ο τομέας του ηλεκτρονικού εγκλήματος εμφανίζει τεράστια έξαρση, κάτι που διαπιστώνεται και στη συνεχή διόγκωση της σχετικής με αυτόν νομολογίας. Η αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο ενέχει δυσκολίες λόγω του χαρακτήρα[8] του, με τις Εθνικές, αλλά και Διεθνής αρχές παγκοσμίως να προσπαθούν να προσαρμοστούν στην νέα πραγματικότητα.

---

[6] Βλ. Διαδικτυακός τόπος: https://ziamparas.gr/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1/%CE%B1%CF%80%CE%AC%CF%84%CE%B7-%CE%BC%CE%B5-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE/

[7] Βλ. Διαδικτυακός τόπος: https://www.kathimerini.gr/society/561995401/ilektronikes-apates-oi-deka-pio-sychnes-pagides-odigos-amynas/, άρθρο του Δημήτρη Δελεβέγκου, 11.08.2022

[8] Η ευκολία, η ανωνυμία, η ταχύτητα, ο διασυνοριακός χαρακτήρας, η απροθυμία καταγγελιών και η διακρατική συνεργασία των διωκτικών αρχών είναι τα βασικά χαρακτηριστικά του κυβερνοεγκλήματος. Βλ. Δαλακούρας, Θ. Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2023, σελ. 5-6

ΚΕΦΑΛΑΙΟ Α΄
ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

1. Ορισμός ηλεκτρονικού εγκλήματος

Με το διαδίκτυο και τις τεχνολογίες της πληροφορίας και των επικοινωνιών να εισχωρούν ολοένα και περισσότερο στην καθημερινότητα, πολλαπλασιάζονται, όχι μόνο οι ευκαιρίες και οι δυνατότητες για τους πολίτες και τις επιχειρήσεις, αλλά και οι κίνδυνοι εμφάνισης εγκληματικών δραστηριοτήτων.

Σύμφωνα με τη Δίωξη Ηλεκτρονικού Εγκλήματος, ως ηλεκτρονικό έγκλημα *«θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία»*[9].

Οι όροι που χρησιμοποιούνται διεθνώς για την απόδοση της έννοιας του ηλεκτρονικού εγκλήματος συμπυκνώνονται αφενός στους γενικότερους όρους *e-crime* και *computer-crime* και αφετέρου στους ειδικότερους όρους *cybercrime* και *internet related crime* με του οποίους συνδέεται άρρηκτα το στοιχείο του διαδικτύου. Ως αντίστοιχοι όροι χρησιμοποιούνται στην ελληνική γλώσσα ο γενικότερος όρος *ηλεκτρονικό έγκλημα* και οι ειδικότεροι *δικτυακό έγκλημα* και *κυβερνοέγκλημα* ή *έγκλημα του κυβερνοχώρου*, οι οποίοι ενσωματώνουν το στοιχείο της δικτύωσης. Κατ' εφαρμογή των όρων αυτών μπορούν να καταχωρισθούν ως μορφές του ηλεκτρονικού εγκλήματος αφενός τα εγκλήματα που διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών (computer crimes) και αφετέρου τα εγκλήματα που διαπράττονται ειδικά μέσω διαδικτύου και αναφέρονται ως κυβερνοεγκλήματα (cyber crimes), συνιστώντας μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος[10].

Άλλωστε η ευκολία τέλεσης των εν λόγω εγκλημάτων είναι απόρροια τόσο του μέσου τέλεσής τους (ηλεκτρονικός υπολογιστής, έξυπνα κινητά τηλέφωνα) που έχει πλέον καταστεί κοινό και διαδεδομένο στην πλειοψηφία των σύγχρονων κοινωνών[11].

---

[9] Βλ. Διαδικτυακό Τόπο: https://e-nomika.gr/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1/

[10] Βλ. Δαλακούρας, Θ. Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2023, σελ. 3

[11] Βλ. Δαλακούρας, Θ. Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2023, σελ. 5

Η ύπαρξη μίας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως για παράδειγμα ενός ηλεκτρονικού υπολογιστή, ενός tablet, ενός notepad ή ενός smartphone (τα οποία smartphones και ταυτίζονται λειτουργικά με τους ηλεκτρονικούς υπολογιστές, όπως συμφωνήθηκε από την Επιτροπή του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα σε συνεδρίαση της, τον Μάρτιο του 2006, δεδομένου ότι τα κινητά τελευταίας τεχνολογίας διαθέτουν πολλαπλές λειτουργίες παραγωγής, εισαγωγής και μεταφοράς δεδομένων, όπως π.χ. η πρόσβαση στο Internet, η αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας, η μεταφορά φωτογραφιών και το «κατέβασμα» εγγράφων)[12], αποτελεί αναπόσπαστο τμήμα του ηλεκτρονικού εγκλήματος και βασική προϋπόθεση για τον χαρακτηρισμό ενός αδικήματος, ως ηλεκτρονικού εγκλήματος. Η συσκευή ηλεκτρονικής επεξεργασίας δεδομένων, ενδέχεται να αποτελεί είτε το στόχο κάποιας επίθεσης, είτε το μέσο διάπραξης κάποιας επίθεσης, είτε τέλος ένα βοηθητικό μέσο για την διάπραξη μίας επίθεσης[13].

1.1. Διακρίσεις ηλεκτρονικών εγκλημάτων και βασικά χαρακτηριστικά

Ο βασικός διαχωρισμός των ηλεκτρονικών εγκλημάτων γίνεται ανάμεσα σε αυτά, που τελούνται με τη χρήση Ηλεκτρονικών Υπολογιστών (Computer Crime), στα οποία συγκαταλέγεται και η απάτη με υπολογιστή (386Α ΠΚ) και σε όσα τελούνται μέσω του Διαδικτύου, τα λεγόμενα Κυβερνοεγκλήματα (Cyber Crime), τα οποία και αποτελούν υποκατηγορία των εγκλημάτων, που τελούνται με τη χρήση Ηλεκτρονικών Υπολογιστών[14].

Αδιαμφησβήτητα τα κυβερνοεγκλήματα διέπονται από ιδιαίτερα χαρακτηριστικά, τα οποία και οδήγησαν στην αναζήτηση και καθιέρωση ειδικών ποινικών ρυθμίσεων για την καταστολή τους. Τα χαρακτηριστικά αυτά μπορούν να συνοψιστούν ως εξής: Α) η ευκολία και Β) η ανωνυμία του αυτουργού στην διάπραξη του εγκλήματος δεδομένου του ευρέως διαδομένου μέσου τέλεσής τους, δηλαδή των συσκευών επεξεργασίας δεδομένων (π.χ. ηλεκτρονικοί υπολογιστές, smartphones κλπ), Γ) η ταχύτητα, σε σχέση με τον χρόνο τέλεσης τους, η οποία μάλιστα καθιστά δυσχερή και την έγκαιρη διαπίστωση τέλεσης του αδικήματος από το θύμα, Δ) ο διασυνοριακός χαρακτήρας, σε σχέση με τον τόπο τέλεσής τους, καθώς δεν είναι απαραίτητη η φυσική παρουσία του αυτουργού για την τέλεση του αδικήματος, γεγονός το οποίο οδηγεί με την σειρά του και σε αναγκαστική Ε) διακρατική συνεργασία των διωκτικών αρχών και τέλος βασικό χαρακτηριστικό σχετικά με την με την απόδειξη τέλεσής του αποτελεί αποτελεί ΣΤ) η απροθυμία καταγγελιών[15].

---

[12] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2019, σελ.5
[13] Βλ. Ι Αγγελή, «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», ΠοινΔικ 2001,1218
[14] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2019, σελ.5
[15] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.5

Το ηλεκτρονικό έγκλημα οφείλει να κατανοηθεί υπό το φως μια τριπλής προσέγγισης, ήτοι α) ως **μία νέα μορφή εγκλήματος**, που διαπράττεται με τη χρήση των ηλεκτρονικών υπολογιστών, β) ως **μία παραλλαγή των ήδη υπαρχόντων εγκλημάτων**, τα οποία διαπράττονται με υπολογιστές (χαρακτηριστικό παράδειγμα αποτελεί το αδίκημα της απάτης με ηλεκτρονικό υπολογιστή) καθώς και γ) ως **μία εγκληματική πράξη που εκδηλώνεται με τη συμμετοχή καθ' οιονδήποτε τρόπο ενός ηλεκτρονικού υπολογιστή**[16].

Ακόμη ένας διαχωρισμός του κυβερνοεγκλήματος, αφορά στον ρόλο που διαδραματίζει η διασυνδεδεμένη σε σύστημα πληροφοριών, συσκευή επεξεργασίας δεδομένων στην διάπραξη των αδικημάτων αυτών. Ως εκ τούτου αυτά μπορούν να κατηγοριοποιηθούν ως εξής:

Α) Στα γνήσια πληροφοριακά εγκλήματα, όπως αυτά που τελούνται, μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών (λ.χ. απάτη, πλαστογραφία).

Β) Στα εγκλήματα με ψηφιακό περιεχόμενο, όπως αυτά που σχετίζονται με την διακίνηση παρανόμου περιεχομένου, μέσω συστημάτων πληροφοριών (λ.χ. παιδική πορνογραφία).

Γ) Στα εγκλήματα κατά πληροφοριακών συστημάτων, όπως αυτά, που διαπράττονται κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων, συνιστώντας υποκατηγορία των κυβερνοεγκλημάτων[17].

Τέλος η βασική κατηγοριοποίηση των κυβερνοεγκλημάτων έχει να κάνει με το περιβάλλον, στο οποίο τελούνται αυτά. Δεδομένης της θέσης, ότι το ηλεκτρονικό έγκλημα διαχωρίζεται από το κοινό έγκλημα, λόγω του περιβάλλοντος διάπραξης αυτού, υφίσταται η παρακάτω κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων:

Α) Σε εγκλήματα, που διαπράττονται τόσο ***σε «κοινό», όσο και σε διαδικτυακό περιβάλλον***, όπως π.χ. η συκοφαντική δυσφήμιση ή η αντιγραφή ενός μουσικού έργου ή μίας κινηματογραφικής ταινίας ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Σε περίπτωση διάπραξης κάποιου από τα εγκλήματα αυτά σε «περιβάλλον διαδικτύου», τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με τη βοήθεια του κυβερνοχώρου (internet related crime).

Β) Σε εγκλήματα που διαπράττονται ***αποκλειστικά σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς τη χρήση του διαδικτύου***. Σε αυτήν την κατηγορία εντάσσονται τα εγκλήματα που προβλέπονται από το άρθρο 370Γ παρ. 1 του Π.Κ.

---

[16] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.5

[17] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.5-6

Γ) Σε εγκλήματα που διαπράττονται ***στον κυβερνοχώρο*** και χαρακτηρίζονται ως κυβερνοεγκλήματα (cyber crimes), όπως π.χ. η μεταβίβαση κρυπτογραφικών κειμένων χωρίς σχετική άδεια ή η διάδοση πορνογραφικού υλικού δια του κυβερνοχώρου (αρ.348^{A} ΠΚ)[18].

ΚΕΦΑΛΑΙΟ Β΄

ΤΟ ΔΙΕΘΝΕΣ ΚΑΙ ΕΝΩΣΙΑΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΗΣ ΑΠΑΤΗΣ ΜΕ ΥΠΟΛΟΓΙΣΤΗ

2. Η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα

Μία εκ των πιο ρηξικέλευθων προσπαθειών για τη νομική προσέγγιση του ηλεκτρονικού εγκλήματος στον Ευρωπαϊκό χώρο και της αντιμετώπισης της εγκληματικότητας στο Διαδίκτυο (Internet), πραγματοποιήθηκε από το Συμβούλιο της Ευρώπης, **το 1976**, όπου έκαναν και την παρθενική τους εμφάνιση οι θεμελιώδεις έννοιες του **«ηλεκτρονικού εγκλήματος»** και του **«κυβερνοεγκλήματος»**. Η σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα, η οποία υπογράφηκε στις 23/11/2001 από τα περισσότερα μέλη του Συμβουλίου της Ευρώπης αλλά και από πολλές τρίτες χώρες μεταξύ των οποίων οι ΗΠΑ, η Αυστραλία και η Ιαπωνία, έχει δε κυρωθεί μέχρι και σήμερα από συνολικά 56 χώρες, τέθηκε σε ισχύ στις 01/07/2004, ενώ από τη χώρα μας υπογράφηκε και κυρώθηκε με διαφορά περίπου 15 ετών, καθώς η κύρωσή της πραγματοποιήθηκε με τον **Ν. 4411/2016**, παράλληλα με τη μεταφορά στην ελληνική έννομη τάξη και της Οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών.

Σκοπό της Σύμβασης, αποτελεί: α) η εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των Κρατών-μελών στον τομέα της εγκληματικότητας στον Κυβερνοχώρο, β) η θέσπιση εσωτερικών δικονομικών διατάξεων για την έρευνα, τη δίωξη και την εκδίκαση των εγκλημάτων του Κυβερνοχώρου και γ) η θέσπιση κανόνων αναφορικά με τη διεθνή συνεργασία[19]. Το κείμενο της σύμβασης περιλαμβάνει τόσο διατάξεις ουσιαστικού όσο και δικονομικού ποινικού δικαίου, καθώς και διατάξεις που αποβλέπουν στην ενίσχυση της συνεργασίας μεταξύ των συμβαλλόμενων κρατών για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας[20]. Αναφορικά με τις ουσιαστικού δικαίου διατάξεις, εντός της σύμβασης προτείνεται η ποινικοποίηση τόσο των γνήσιων πληροφορικών εγκλημάτων, ήτοι των συμπεριφορών που στρέφονται κατά των πληροφορικών

---

[18] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.4

[19] Αγγελή Ι., «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο», ΠοινΔικ 12/2001, σελ. 1218.

[20] Βλ.https://www.coe.int/en/web/conventions/full-list/- conventions/treaty/185/signatures (τελευταία πρόσβαση 31/8/2018)

συστημάτων και των δεδομένων τους (άρ.2-6), όσο και των μη γνήσιων πληροφορικών εγκλημάτων, που προσβάλλουν άλλα έννομα αγαθά, τελούνται όμως μέσω Η/Υ[21]. Στην δε κατηγορία των μη γνήσιων πληροφορικών εγκλημάτων, συμπεριλαμβάνεται και το αδίκημα της απάτης σχετικά με υπολογιστές (άρθρο 8 Σύμβασης).

Η Σύμβαση αποτελείται από τέσσερα κεφάλαια, που θίγουν τα κάτωθι ζητήματα: Στο πρώτο κεφάλαιο (άρθρο 1), προσδιορίζεται η έννοια των πιο βασικών όρων, οι οποίοι αναφέρονται εντός της Σύμβασης, ήτοι του συστήματος του ηλεκτρονικού υπολογιστή, των δεδομένων υπολογιστή, του φορέα παροχής υπηρεσιών και των διακινούμενων δεδομένων. Στο δεύτερο κεφάλαιο (άρθρα 2-22), περιλαμβάνονται τόσο οι διατάξεις του ουσιαστικού ποινικού δικαίου, στις οποίες γίνεται αναφορά στις συμπεριφορές που ποινικοποιούνται στον κυβερνοχώρο, όσο και οι διατάξεις ποινικού δικονομικού δικαίου, οι οποίες καλύπτουν ένα ευρύ φάσμα αδικημάτων τα οποία τελούνται μέσω συστήματος ηλεκτρονικού υπολογιστή και όχι μόνον τα αδικήματα που αναφέρονται στο πρώτο κεφάλαιο της Σύμβασης. Στο τρίτο κεφάλαιο της Σύμβασης (άρθρα 23-35), περιλαμβάνονται, οι διατάξεις σχετικά με τις γενικές αρχές για τη διεθνή συνεργασία (άρθρο 23), τις γενικές αρχές σχετικά με την έκδοση (άρθρο 23), στις γενικές αρχές αμοιβαίας συνδρομής (άρθρα 25-26), τις διαδικασίες που ισχύουν επί αιτημάτων αμοιβαίας συνδρομής σε ενδεχόμενο απουσίας εφαρμοστέων διεθνών συμβάσεων (άρθρα 27-28), τις ειδικές διατάξεις που αφορούν την αμοιβαία συνδρομή που σχετίζεται με προσωρινά μέτρα (άρθρα 29-30), τις διατάξεις που αφορούν τα ερευνητικά μέτρα (άρθρα 31-34), στη σύσταση ενός δικτύου με εικοσιτετράωρη λειτουργία (άρθρο 35). Στο τελευταίο κεφάλαιο περιλαμβάνονται οι τελικές διατάξεις, ήτοι οι σταθερές διατάξεις που διατυπώνονται στις Συμβάσεις του Συμβουλίου της Ευρώπης. Μεταξύ των αδικημάτων που αναφέρονται στη Σύμβαση περιλαμβάνεται και η απάτη σχετική με υπολογιστές (άρθρο 8), η οποία ανήκει στα εγκλήματα σχετικά με το περιεχόμενο (content-related offences), το οποίο μπορεί να διακριθεί σε παράνομο ή βλαβερό[22].

Σύμφωνα με το άρθρο 8 της Σύμβασης: *«Κάθε συμβαλλόμενο μέρος θα λάβει τα νομοθετικά και άλλα μέτρα, που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η από πρόθεση και άνευ δικαιώματος η πρόκληση απώλειας περιουσίας σε κάποιον άλλον με : α) οποιαδήποτε εισαγωγή, τροποποίηση, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικού υπολογιστή, β) οποιαδήποτε επέμβαση στη λειτουργία ενός υπολογιστή ή συστήματος υπολογιστών, με σκοπό να επιφέρει οικονομικό όφελος στον εαυτό του ή σε άλλον».*

---

[21] Βλ. Καϊάφα-Γκμπάντι, Μ., Ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρον 2011, σελ. 489 επ.

[22] Βλ. Ποιν. Χρον. Ι Αγγελή, σελ. 675 επ.

Κατά το επεξηγηματικό υπόμνημα, που συνοδεύει τη Σύμβαση, η ρύθμιση του άρθρου 8 τίθεται με σκοπό να συμπεριλάβει οποιαδήποτε, χωρίς δικαίωμα επέμβαση σε σύστημα Η/Υ, συνοδευόμενη από σκοπό πρόκλησης παράνομου περιουσιακού οφέλους, έτσι ώστε να καταλαμβάνονται και οι περιπτώσεις ηλεκτρονικού χρήματος και κυρίως της απάτης με πιστωτικές κάρτες[23].

Η αιτιολογική έκθεση της Σύμβασης, φροντίζει να ερμηνεύσει, ότι το εδάφιο β΄ του άρθρου 8 της Σύμβασης, κατά το οποίο θα πρέπει να ποινικοποιηθεί, οποιαδήποτε επέμβαση στη λειτουργία ενός υπολογιστή ή συστήματος υπολογιστών, με σκοπό να επιφέρει οικονομικό όφελος στον εαυτό του ή σε άλλον, αφορά κάθε επέμβαση στα μηχανικά μέρη του υπολογιστή, η παρεμπόδιση εκτυπώσεων και άλλες ενέργειες που επηρεάζουν την εγγραφή και ροή των δεδομένων[24].

Το γεγονός της ποινικοποίησης του εν λόγω αδικήματος με τη Σύμβαση για το Κυβερνοέγκλημα, καταδεικνύει το ελλιπές νομικό πλαίσιο από πολλές ευρωπαϊκές χώρες για την προστασία από αυτού του είδους επιθέσεις και παρεμβολές, ενώ αποπειράται να θέσει ένα νομικό πλαίσιο, με κοινά θεμελιώδη στοιχεία, για τα συμβαλλόμενα κράτη, δεδομένου του διασυνοριακού χαρακτήρα του κυβερνοεγκλήματος.

Στην ελληνική έννομη τάξη, ο **Ν. 4411/2016**, ο οποίος κύρωσε τη Σύμβαση, επέφερε και την πρώτη τροποποίηση του άρθρου της απάτης με υπολογιστή (386^{Α} ΠΚ), συμπεριλαμβάνοντας στις περιπτώσεις απάτης με υπολογιστή και τη χρήση (ορθών) δεδομένων που δίνεται χωρίς δικαίωμα, όπως λ.χ. στην περίπτωση του δράστη που έχει αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου[25].

Μάλιστα σύμφωνα με την τροποποίηση του άρθρου 386Α του ΠΚ με τον Ν. 4619/2019 φαίνεται αυτό να συμμορφώνεται απόλυτα με τις διατάξεις της Σύμβασης για το Κυβερνοέγκλημα, εισάγοντας στους τρόπους τέλεσης του αδικήματος: α) την χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή και β) την χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης ταυτότητας, όπως ακριβώς αυτές αναφέρονται στο άρθρο 8 της Σύμβασης.

---

[23] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.18
[24] Βλ. Αιτιολογική Έκθεση της Σύμβασης για το Κυβερνοέγκλημα, παρ. 87
[25] Βλ. Θεοχάρης Δαλακούρας, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.18

Επιπλέον η νεοεισαχθείσα παράγραφος 2 του άρθρου 386Α ΠΚ, κατά την οποία: *«Όποιος κατασκευάζει, διαθέτει ή κατέχει πρόγραμμα ή πληροφοριακό σύστημα υπολογιστή που προορίζεται για τη διάπραξη του εγκλήματος της παραγράφου 1 τιμωρείται με φυλάκιση έως δύο έτη και χρηματική ποινή. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή σύστημα υπολογιστή πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παραγράφου 1.»*, φαίνεται να συμβαδίζει με το άρθρο 6 της Σύμβασης, σύμφωνα με το οποίο ποινικοποιείται η κακή χρήση συσκευών.

Ειδικότερα, σύμφωνα με το άρθρο 6 παρ. 1 της Σύμβασης, τα συμβαλλόμενα μέρη καλούνται να ενσωματώσουν στην ποινική έννομη τάξη τους, την τιμωρία των άνευ δικαιώματος και με πρόθεση τελούμενων πράξεων παραγωγής, πώλησης, προμήθειας για χρήση, εισαγωγή, διανομή ή άλλως διάθεσης είτε μίας συσκευής, συμπεριλαμβανομένου και ενός προγράμματος υπολογιστή σχεδιασμένης ή προσαρμοσμένης πρωτίστως με σκοπό τη διάπραξη κάποιου από τα εγκλήματα τα οποία αναφέρονται στα άρθρα 2 έως 5 της Σύμβασης, είτε ενός συνθηματικού ή κωδικού πρόσβασης ή άλλου παρεμφερούς δεδομένου, με τη χρήση του οποίου είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός συστήματος υπολογιστή, πρωτίστως με σκοπό τη διάπραξη κάποιου από τα εγκλήματα τα οποία αναφέρονται στα άρθρα 2 εως 5 της Σύμβασης. Ουσιαστικά με το συγκεκριμένο άρθρο η Σύμβαση ποινικοποιεί τις προπαρασκευαστικές πράξεις απόκτησης πρόσβασης σε υπολογιστικό σύστημα, παράνομης υποκλοπής δεδομένων, επέμβασης στα δεδομένα και στο σύστημα.

Κοινό τόπο σε αμφότερες διατάξεις αποτελεί η πρόθεση, ο σκοπός τέλεσης αξιόποινης πράξης, προκειμένου να αποφευχθεί σύγχυση ή και αφορισμός νέων τεχνολογιών. Άλλωστε η ίδια η παράγραφος 2 του άρθρου 6 της Σύμβασης διασαφηνίζει, ότι οι πράξεις του άρθρου 1 αυτής δεν τιμωρούνται εάν δεν στοχεύουν στη διάπραξη εγκλήματος, αλλά λ.χ. στην πραγματοποίηση επιτρεπτών δοκιμών ή στην προστασίας ενός συστήματος ενός υπολογιστή. Ως εκ τούτου καθίσταται σαφές ότι τόσο οι αναφερόμενες στην παράγραφο 1 του άρθρου 6 της Σύμβασης πράξεις, όσο και οι πράξεις της παραγράφου 2 του άρθρου 386^{A} ΠΚ, παραμένουν ατιμώρητες όταν ελλείπει ο σκοπός τέλεσης αδικήματος, ήτοι ο δόλος, ο οποίος τις καθιστά προπαρασκευαστικές πράξεις ενός αδικήματος και ο οποίος θα αποτελέσει τη λεπτή διαχωριστική γραμμή ανάμεσα στην αυτοτελή τιμωρία ή μη των ως άνω πράξεων.

2.1. Η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών

Οι στόχοι της παρούσας οδηγίας είναι η προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων, και η βελτίωση της συνεργασίας

μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, καθώς και των αρμόδιων ειδικευμένων οργανισμών της Ένωσης και φορέων της Ένωσης, όπως η Eurojust, η Europol και το Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος, καθώς και ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια δικτύων και Πληροφοριών (ENISA)[26].

Η άνω οδηγία φαίνεται να λαμβάνει υπόψη τα σύγχρονα τεχνολογικά δεδομένα και περιέχει σαφείς κυρωτικούς κανόνες κατά των δραστών επιθέσεων κατά συστημάτων πληροφοριών, ιδίως όσον χρησιμοποιούν δίκτυα προγραμμάτων ρομπότ (botnet) ή προβαίνουν σε επιθέσεις μεγάλης κλίμακας κατά συστημάτων πληροφοριών. Και πιο πέρα, ποινικοποιεί την παραγωγή, χρήση και διάθεση των εργαλείων που χρησιμοποιούνται για τη διάπραξη αδικημάτων που αναφέρονται στην οδηγία και τα οποία είναι απολύτως απαραίτητα για το σκοπό αυτό. Για το λόγο δε αυτό, δεν είναι άστοχη η ποινικοποίησή τους, όπως έχει υποστηριχθεί στη θεωρία. Τέλος, η οδηγία αποδίδει σημασία στα δίκτυα συνεργασίας μεταξύ των κρατών μελών, όπως και στη συνεργασία μεταξύ των δημόσιων αρχών και του ιδιωτικού τομέα και της κοινωνίας των πολιτών[27].

Προκάτοχό της Οδηγίας, αποτελούσε η απόφαση – πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της 24ης Φεβρουαρίου 2005 σχετικά με τις επιθέσεις κατά των συστημάτων πληροφοριών, η οποία είχε ως στόχο την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο και την προώθηση της ασφάλειας πληροφοριών σε ό,τι αφορούσε τη νέα μορφή διεθνικής εγκληματικότητας που συνιστούν οι επιθέσεις κατά συστημάτων πληροφοριών. Η Οδηγία, η οποία κατήργησε την απόφαση – πλαίσιο 2005/222/ΔΕΥ, δομήθηκε με βάση την Σύμβαση για το Κυβερνοέγκλημα και ποινικοποίησε μεταξύ άλλων τη χρήση εργαλείων, με τα οποία διαπράττονται τα αδικήματα για πρώτη φορά, δεδομένου ότι η απόφαση-πλαίσιο δεν περιείχε καμία τέτοιου είδους διάταξη. Ειδικότερα σύμφωνα με το άρθρο 7 αυτής: *«Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλουθων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις: α) πρόγραμμα υπολογιστή, που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6, β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών».*

---

[26] Βλ. Οδηγία 2013/40/ΕΕ, Εισ. Σκέψη 1

[27] Βλ. ΣΥΝΗΓΟΡΟΣ, Δίκαιο & Νέες Τεχνολογίες, Επιθέσεις κατά συστημάτων πληροφοριών, Η νέα οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου, Ιωάννης Δ. Ιγγλεζάκης,σελ. 72

Το ως άνω άρθρο βρίσκεται σε απόλυτη σύμπνοια με το άρθρο 6 της Σύμβασης για το Κυβερνοέγκλημα, καθώς και με την παράγραφο 2 του άρθρου 386Α ΠΚ. Ειδοποιό διαφορά, μεταξύ του άρθρου 7 της Οδηγίας και του άρθρου 386Α ΠΚ, αποτελεί η παράλειψη του νομοθέτη να ποινικοποιήσει την πράξη της κατοχής στο 7 της Οδηγίας σε αντίθεση με την παράγραφο 2 του άρθρου 386Α ΠΚ, η οποία ρητά αναφέρει την κατοχή ως τιμωρητέα πράξη. Ακόμη ένα κρίσιμο σημείο, που χρήζει ερμηνείας, αποτελεί η φράση «ήσσονος σημασίας», η οποία προφανώς έχει προστεθεί από το νομοθέτη σε μία προσπάθεια του, να μην γίνει κατάχρηση της διάταξης.

2.2. Η Οδηγία 2019/713/ΕΕ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμών πλην των μετρητών

Η Ενσωμάτωση της Οδηγίας (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου (L 123) πραγματοποιήθηκε στην ελληνική νομοθεσία με τον **Ν. 4947/2022**[28].

Χαρακτηριστική είναι η σκέψη υπ' αρ. 15 του προοιμίου της Οδηγίας (ΕΕ) 2019/713, όπου αναφέρει: *«Η παρούσα οδηγία αναφέρεται σε κλασικές μορφές συμπεριφοράς, όπως απάτη, πλαστογραφία, κλοπή και παράνομη ιδιοποίηση που είχαν διαμορφωθεί από το εθνικό δίκαιο πριν την ψηφιακή εποχή. Επομένως, η επέκταση του πεδίου εφαρμογής της παρούσας οδηγίας στα άυλα μέσα πληρωμής συνεπάγεται τον καθορισμό αντίστοιχων αξιόποινων πράξεων στο ψηφιακό περιβάλλον, προκειμένου να συμπληρωθεί και να ενισχυθεί η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου».*[29]

Είναι γεγονός πως στην σύγχρονη εποχή υπερτερεί η φύση του χρήματος ως άυλης περιουσιακής αξίας, αποσυνδεδεμένης από τον υλικό φορέα της, ο οποίος όλο και σπανιότερα κάνει πλέον την εμφάνισή του στην καθημερινή συναλλακτική πρακτική. Το ίδιο ισχύει και για τα λοιπά περιουσιακά αγαθά, των οποίων η ενσωμάτωση σε υλικούς φορείς συνεχώς υποχωρεί, ενώ κάνουν την εμφάνισή τους νέα περιουσιακά αγαθά a priori άυλα και ψηφιακά (π.χ. NFTs, κρυπτονομίσματα). Τα «εικονικά νομίσματα» αναγνωρίζονται πλέον στην ευρωπαϊκή έννομη τάξη ως άξια ποινικής προστασίας ψηφιακά μέσα συναλλαγής και άυλα μέσα πληρωμής, όπως προκύπτει από τον συνδυασμό των ορισμών των περ. α΄, γ΄ και δ΄ του άρθρου 2 της Οδηγίας (ΕΕ) 2019/713.[30]

---

[28] Βλ. Διαδικτυακός Τόπος: https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-4947-2022

[29] Βλ. Οδηγία (ΕΕ) 2019/713, Εισ. Σκέψη 15

[30] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ., «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.156

Μετά την μεταρρύθμιση του Ποινικού Κώδικα με το Ν. 4411/2016 το έγκλημα της απάτης με υπολογιστή (αρ. 386^{A} ΠΚ) τυποποιεί όλες τις αξιόποινες πράξεις «αφαίρεσης» και «ιδιοποίησης» ψηφιακού χρήματος, με την επιφύλαξη όσων καλύπτονται από τη διάταξη περί απιστίας (αρ. 390 ΠΚ). Οι μεταβολές που επήλθαν στη διάταξη περί απάτης με υπολογιστή διά και από της εισαγωγής του νέου Ποινικού Κώδικα και ιδίως μετά την ενσωμάτωση της Οδηγίας (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 «για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου», επιβεβαιώνουν σε γενικές γραμμές το ως άνω συμπέρασμα και παρά τις όποιες ατέλειές τους κινούνται προς την ορθή κατεύθυνση.[31]

Τέλος το άρθρο 6 της Οδηγίας (ΕΕ) 2019/713 προσδιορίζει την «Απάτη συνδεόμενη με τα συστήματα πληροφοριών», καθώς αναφέρει τα εξής: *«…η άμεση ή έμμεση διενέργεια μεταφοράς χρημάτων, νομισματικής αξίας ή εικονικών νομισμάτων και, κατά συνέπεια, η πρόκληση παράνομης απώλειας περιουσίας άλλου προσώπου, με σκοπό την αποκόμιση παράνομου οφέλους για τον δράστη ή για τρίτους,…,όταν τελείται εκ προθέσεως: α) χωρίς δικαίωμα, με την παρεμπόδιση της λειτουργίας συστήματος πληροφοριών ή την παρεμβολή σε αυτήν, β) χωρίς δικαίωμα, με την εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ηλεκτρονικών δεδομένων.»*[32]

2.3. Η Οδηγία NIS2 (2022/2555/ΕΕ) σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση

Στη συνεχή νομοθετική επαγρύπνηση σχετικά με τα φαινόμενα του διαδικτύου, εντάσσεται η πρόσφατη προσπάθεια της Ευρωπαϊκής Ένωσης με την επικαιροποίηση της Οδηγίας NIS 2016.[33] Με την οδηγία NIS2, που τέθηκε σε ισχύ το 2023, εκσυγχρονίζεται το υφιστάμενο νομικό πλαίσιο ώστε να συμβαδίζει με την αυξημένη ψηφιοποίηση και ένα εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο. Με την επέκταση του πεδίου εφαρμογής των κανόνων κυβερνοασφάλειας σε νέους τομείς και οντότητες, βελτιώνει περαιτέρω την ανθεκτικότητα και τις ικανότητες αντιμετώπισης συμβάντων των δημόσιων και ιδιωτικών οντοτήτων, των αρμόδιων αρχών και της Ευρωπαϊκής Ένωσης στο σύνολό της.[34]

Η παραπάνω Οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση προβλέπει νομικά μέτρα για την ενίσχυση του συνολικού επιπέδου κυβερνοασφάλειας στην Ε.Ε., διασφαλίζοντας:

1. Ετοιμότητα των κρατών μελών, απαιτώντας να είναι κατάλληλα εξοπλισμένα. Για παράδειγμα, με ομάδα αντιμετώπισης συμβάντων ασφάλειας υπολογιστών (CSIRT) και αρμόδια εθνική αρχή συστημάτων δικτύου και

πληροφοριών (NIS). Οι αρμόδιες αρχές θα πρέπει να διασφαλίζουν ότι τα εποπτικά τους καθήκοντα σε σχέση με βασικές και σημαντικές οντότητες ασκούνται από καταρτισμένους επαγγελματίες, οι οποίοι θα πρέπει να διαθέτουν τις απαραίτητες δεξιότητες για την εκτέλεση των εν λόγω καθηκόντων, ιδίως όσον αφορά τη διενέργεια επιτόπιων επιθεωρήσεων και την εποπτεία εκτός των εγκαταστάσεων, συμπεριλαμβανομένου του εντοπισμού αδυναμιών στις βάσεις δεδομένων, το υλικό, τα τείχη προστασίας, την κρυπτογράφηση και τα δίκτυα. Οι εν λόγω επιθεωρήσεις και εποπτεία θα πρέπει να διενεργούνται με αντικειμενικό τρόπο.[35]

2. Συνεργασία μεταξύ όλων των κρατών μελών, με τη σύσταση ομάδας συνεργασίας για τη στήριξη και τη διευκόλυνση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών. Πιο συγκεκριμένα σύμφωνα με την Εισ. Σκέψη 66 της Οδηγίας NIS2: *«Η Ομάδα Συνεργασίας θα πρέπει να στηρίζει και να διευκολύνει τη στρατηγική συνεργασία και την ανταλλαγή πληροφοριών, καθώς και να ενισχύει την εμπιστοσύνη μεταξύ των κρατών μελών. Η Ομάδα Συνεργασίας θα πρέπει να καταρτίζει ανά διετία πρόγραμμα εργασίας. Το πρόγραμμα εργασίας θα πρέπει να περιλαμβάνει τις ενέργειες που θα αναλάβει η Ομάδα Συνεργασίας για την υλοποίηση των στόχων και των καθηκόντων της. Το χρονοδιάγραμμα για την κατάρτιση του πρώτου προγράμματος εργασιών βάσει της παρούσας οδηγίας θα πρέπει να ευθυγραμμιστεί με το χρονοδιάγραμμα του τελευταίου προγράμματος εργασίας που θεσπίστηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148, προκειμένου να αποφευχθούν πιθανές διαταραχές στις εργασίες της ομάδας συνεργασίας.»*
3. Τέλος, μια νοοτροπία ασφάλειας σε όλους τους τομείς που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία μας και βασίζονται σε μεγάλο βαθμό στις ΤΠΕ, όπως η ενέργεια, οι μεταφορές, το νερό, οι τράπεζες, οι υποδομές των χρηματοπιστωτικών αγορών, η υγειονομική περίθαλψη και οι ψηφιακές υποδομές.

Σύμφωνα με το άρθρο 2 παρ.1 της Οδηγίας NIS2: *«Η παρούσα οδηγία εφαρμόζεται σε δημόσιες ή ιδιωτικές οντότητες των τύπων που αναφέρονται στο παράρτημα Ι ή ΙΙ οι οποίες χαρακτηρίζονται ως μεσαίες επιχειρήσεις δυνάμει του άρθρου 2 του παραρτήματος της σύστασης 2003/361/ΕΚ ή υπερβαίνουν τα ανώτατα όρια για τις μεσαίες επιχειρήσεις που αναφέρονται στο εν λόγω άρθρο και οι οποίες παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της Ένωσης.» Μερικές επιχειρήσεις που* προσδιορίζονται από τα κράτη μέλη ως φορείς εκμετάλλευσης βασικών υπηρεσιών, είναι οι επιχειρήσεις που δραστηριοποιούνται στον τομέα της ενέργειας, των μεταφορών, της δημόσιας διοίκησης και του διαστήματος, ταχυδρομικές υπηρεσίες, επιχειρήσεις παραγωγής ιατροτεχνολογικών προϊόντων, εταιρείες που παρέχουν χρηματοοικονομικές υπηρεσίες - όπως τράπεζες, φορείς παροχής υπηρεσιών πληρωμής, εταιρείες επενδύσεων και οι πάροχοι ψηφιακών υπηρεσιών, όπως οι μηχανές αναζήτησης, οι υπηρεσίες υπολογιστικού νέφους κ.α. Όλοι οι παραπάνω θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας και να ενημερώνουν τις αρμόδιες εθνικές αρχές για σοβαρά περιστατικά κυβερνοεπίθεσης που ενδεχομένως θα προκύψουν κατά την λειτουργία τους.

Τέλος, η οδηγία δεν θα εφαρμόζεται σε οντότητες που ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της δημόσιας ασφάλειας, της άμυνας, ή της επιβολής του νόμου, συμπεριλαμβανομένων και των δραστηριοτήτων που σχετίζονται με την πρόληψη, τη διερεύνηση, τον εντοπισμό και τη δίωξη ποινικών αδικημάτων, από ορισμένες υποχρεώσεις που ορίζονται στην παρούσα οδηγία όσον αφορά τις εν λόγω δραστηριότητες.[36]

ΚΕΦΑΛΑΙΟ Γ΄

Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ

3. Το άρθρο 386Α Π.Κ

Με το άρθρο 5 του Ν. 1805/1988 εισήλθε στην Ελληνική Ποινική Έννομη Τάξη το άρθρο 386Α ΠΚ με τον τίτλο «ΑΠΑΤΗ ΜΕ ΗΛΕΚΤΡΟΝΙΚΟ ΥΠΟΛΟΓΙΣΤΗ». Το παραπάνω άρθρο αποτελούσε μια παραλλαγή του αδικήματος της απάτης (386 ΠΚ) και η εισαγωγή του φανέρωσε το πόσο αναγκαία ήταν η αναθεώρηση του τότε Ποινικού Κώδικα, ώστε να συμβαδίζει με τις σύγχρονες μορφές εγκληματικότητας που είχαν κάνει την εμφάνισή τους.[37]

Μάλιστα η διατύπωση της διάταξης της απάτης με ηλεκτρονικό υπολογιστή βασίστηκε στο αντίστοιχο άρθρο 263a του Γερμανικού Κώδικα με ορισμένες διαφοροποιήσεις.[38]

---

[31] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ., «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.157

[32] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ., «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.15

[33] Κυβερνοασφάλεια: οι νέοι κανόνες της ΕΕ για την καταπολέμηση του ηλεκτρονικού εγκλήματος | Νομικά Νέα | Lawspot

[34] https://digital-strategy.ec.europa.eu/el/policies/nis2-directive

[35] Οδηγία NIS2, Εισαγ. Σκέψη 125 σελ. 26

[36] Οδηγία NIS2

[37] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 194

[38] Βλ. Γ. Νούσκαλης, Ποιν Δικ 2/2003 (Έτος 6ο), σελ. 178, «Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση»

3.1. Η νομοτυπική μορφή του άρθρου 386Α Π.Κ.

Το κείμενο του άρθρου 386Α Π.Κ για την αντιμετώπισης της απάτης με υπολογιστή, μετά τις αλλεπάλληλες νομοθετικές μεταβολές που επέφεραν οι Ν.4411/2016, Ν.4619/2019, Ν.4855/2021 και το αρ. 16 του Ν.4947/2022 έχει σήμερα ως εξής:

«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 ζημία 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 είκοσι (20) έτη.»

3.2. Ιστορική εξέλιξη

Σύμφωνα με το αρ. 5 του **Ν.1805/1988** μετά το άρθρο 386 του Ποινικού Κώδικα προστέθηκε νέο άρθρο που έλαβε τον αριθμό 386Α και είχε διαμορφωθεί ως εξής: «Άρθρο 386 Α Απάτη με υπολογιστή: *Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα».*[39]

Αξίζει να αναφερθεί σε αυτό το σημείο, ότι στην αρχική του μορφή το άρθρο 386Α ΠΚ ανέφερε ως τρόπους τέλεσης του, τους εξής: *α) την μη ορθή διαμόρφωση του προγράμματος, β) την επέμβαση κατά την εφαρμογή του γ) τη χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων δ) οποιονδήποτε άλλο τρόπο.* Με το δ΄ χωρίο από τους τρόπους τέλεσης ο νομοθέτης θέλησε να εντάξει στο χώρο του αξιοποίνου της κατ' άρθρο 386Α ΠΚ, απάτης και τρόπους επηρεασμού του υπολογιστή, που ενώ δεν καλύπτονται από τους υπόλοιπους τρόπους τέλεσης (λ.χ. οι επιρροές από Hardware), είναι όμως ισάξιοι από πλευράς βαρύτητας με αυτές και μπορούν να προκύψουν από την αλματώδη ανάπτυξη της πληροφορικής. Σε κάθε περίπτωση θα επρόκειτο για τρόπο επηρεασμού του υπολογιστή και όχι για απλή εκμετάλλευση των δυνατοτήτων του υπολογιστή.[40]

Η επόμενη μορφή του παραπάνω άρθρου, η οποία επήλθε μέσω του άρθρου 2 του **Ν. 4411/2016**, με το οποίο προστέθηκαν τότε οι συμπεριφορές της «χωρίς δικαίωμα χρήσης δεδομένων» και της «χωρίς δικαίωμα παρέμβασης σε πληροφοριακό σύστημα», αφαιρώντας ή πιο σωστά εξειδίκευσε την γενική ρήτρα τέλεσης του αδικήματος της περ. δ΄ («*με οποιονδήποτε άλλο τρόπο»*), καθώς και η παλαιά υπαλλαγή της «επέμβασης κατά την εφαρμογή του προγράμματος» διευρύνθηκε και υποκαταστάθηκε από την χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα συνολικά (υλισμικό [hardware] και λογισμικό-πρόγραμμα [software]).[41]

---

[39] https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/n-1805-1988.html
[40] Βλ. Αδάμ Χ. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, Εκδόσεις Σάκκουλα 2016, σελ. 168
[41] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ., «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.161-162

Με το **Ν. 4619/2019** του Ποινικού Κώδικα επήλθαν αρκετές αλλαγές στο άρθρο της απάτης με υπολογιστή. Ειδικότερα, το άρθρο 386Α ΠΚ, απαριθμεί περιοριστικά πλέον τους τρόπους τέλεσης του αδικήματος και προσθέτει τον πέμπτο τρόπο τέλεσης του αδικήματος, κατά τον οποίο τελεί απάτη με υπολογιστή όποιος βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή, *με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας.* Επιπλέον, η νέα τροποποίηση του άρθρου, ποινικοποιεί στην παράγραφο 2 τις προπαρασκευαστικές πράξεις του αδικήματος και τέλος προσθέτει την παράγραφο 3 του άρθρου τις προϋποθέσεις χαρακτηρισμού της πράξης ως κακουργήματος, σε περίπτωση που αυτή στρέφεται εναντίον του Ελληνικού Δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης.

Στη συνέχεια με το άρθρο 93 του **Ν. 4855/2021** τροποποιήθηκε η περ. ε΄ του πρώτου εδαφίου της παρ. 1 του άρθρου 386Α ΠΚ ως προς το πλαίσιο ποινής, με την προσθήκη της περίπτωσης ιδιαίτερα μεγάλης προξενηθείσας ζημίας και του αντίστοιχου πλαισίου ποινής και το άρθρο 386Α διαμορφώνεται ως εξής:

«1. Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή: α) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή, β) με τη χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή, γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, ή ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων τιμωρείται με φυλάκιση, και 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 σύστημα υπολογιστή 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 σύστημα υπολογιστή πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παρ. 1.

Αν η απάτη με υπολογιστή στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 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 είκοσι (20) έτη.».[42]

---

[42] ΝΟΜΟΣ

Τέλος με το άρθρο 16 του **Ν. 4947/2022** επήλθε η τελευταία τροποποίηση του άρθρου 386Α ΠΚ και πιο συγκεκριμένα τροποποιήθηκε η παρ. 1 και 2 του άρθρου 386Α ΠΚ (άρθρα 3, 6 και παρ. 4 και 5 άρθρου 9 της Οδηγίας (ΕΕ) 2019/713). Στο άρθρο 386Α ΠΚ επήλθαν οι εξής αλλαγές: α) στην περ. β` της παρ. 1 και στην παρ. 2 η αναφορά σε πρόγραμμα ή σύστημα υπολογιστή και στη λειτουργία αυτού αντικαθίσταται από την αναφορά στο πληροφοριακό σύστημα, β) στην παρ. 1: βα) στις περ. γ` και δ` η αναφορά σε δεδομένα υπολογιστή εξειδικεύεται ως αναφορά σε ψηφιακά δεδομένα, ββ) στην περ. δ` προστίθεται η αναφορά στη μετάδοση ψηφιακών δεδομένων, βγ) στην περ. ε` προστίθεται η αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση νομισματικής αξίας και το άρθρο 386Α ΠΚ έχει λάβει τη νομοτυπική μορφή του όπως διατυπώνεται παραπάνω.

3.3. Το προστατευόμενο έννομο αγαθό

Το προστατευόμενο έννομο αγαθό της απάτης με υπολογιστή αποτελεί η περιουσία ως σύνολο. Στην έννοια της περιουσίας υπάγεται τόσο το λογιστικό χρήμα, όσο και οι απαιτήσεις και τα δικαιώματα που προέρχονται από την επεξεργασία στοιχείων ενός υπολογιστή.[43]

Ωστόσο έχει υποστηριχτεί ότι μπορεί επικουρικά ή δευτερευόντως να θεωρηθούν ως προστατευόμενα έννομα αγαθά η εμπιστοσύνη στην ασφάλεια και αξιοπιστία της μεταφορά κεφαλαίων, μέσω της επεξεργασίας δεδομένων[44] ή τα συστήματα συναλλαγών χωρίς μετρητά χρήματα.[45]

Βέβαια το γεγονός ότι ο ίδιος ο νομοθέτης τοποθέτησε το άρθρο της απάτης με υπολογιστή στο 23ο κεφάλαιο του ποινικού κώδικα που αφορά τα εγκλήματα κατά περιουσιακών αγαθών και πιο συγκεκριμένα στην υποκατηγορία των εγκλημάτων κατά της περιουσίας, σε συνδυασμό με την γραμματική ερμηνεία του άρθρου, σύμφωνα με την οποία: *«Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία»*, καθώς και το γεγονός ότι το άρθρο της απάτης με υπολογιστή δομήθηκε με βάση το άρθρο της κοινής απάτης, συγκλίνουν στο συμπέρασμα ότι προστατευόμενο έννομο αγαθό της απάτης με υπολογιστή αποτελεί η περιουσία, ως σύνολο.

3.4. Η αντικειμενική υπόσταση του άρθρου 386Α Π.Κ.

Η απάτη με υπολογιστή στη βασική της μορφή είναι πλημμέλημα, δεδομένου ότι τιμωρείται με φυλάκιση. Μάλιστα αποτελεί ένα ιδιώνυμο έγκλημα, καθώς αν και έχει σχέση με την πράξη της κλασσικής απάτης, δεν μπορεί να θεωρηθεί παραλλαγή της.[46]

---

[43] Βλ. Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 208

[44] Βλ. Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και ποινικό δίκαιο, σελ. 57

[45] Βλ. Γ. Νούσκαλης, ΠοινΔικ 2/2003 (Έτος 6ο), σελ. 180

[46] Βλ. Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 195

Επιπλέον το έγκλημα της απάτης με υπολογιστή (386Α ΠΚ), αποτελεί ένα γνήσιο πολύτροπο ή υπαλλακτικώς μικτό έγκλημα, το οποίο μπορεί να τελεστεί με πλείονες εξειδικευμένους τρόπους. Πιο συγκεκριμένα το αδίκημα της απάτης με υπολογιστή τελείται όταν βλάπτεται ξένη περιουσία με τον επηρεασμό του αποτελέσματος μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή (κατ' αντιστοιχία της πλάνης της κοινής απάτης) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή ή με τη χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή ή με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας ή με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης ταυτότητας ή με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων.[47]

Τέλος η απάτη με υπολογιστή είναι κοινό έγκλημα, διότι δράστης μπορεί να είναι οποιοσδήποτε, χωρίς να απαιτείται η συνδρομή κάποιας συγκεκριμένης ιδιότητας στο πρόσωπό του.[48]

3.5. Τρόποι τέλεσης

Το αδίκημα του άρθρου 386Α ΠΚ, όπως αναφέρθηκε και παραπάνω αποτελεί ένα υπαλλακτικώς μικτό αδίκημα που μπορεί να τελεστεί με πέντε διαφορετικούς τρόπους, οι οποίοι απαριθμούνται περιοριστικά και είναι οι εξής:

1) Η μη ορθή διαμόρφωση προγράμματος υπολογιστή

Αρχικά αξίζει να σημειωθεί πως ως πρόγραμμα ορίζεται ένα σύνολο δεδομένων, με τα οποία παρέχονται εντολές στον υπολογιστή. Η μη ορθή διαμόρφωση προγράμματος υπολογιστή, αποτελεί τον πρώτο τρόπο τέλεσης του αδικήματος της απάτης με υπολογιστή. Αυτή μπορεί να πραγματωθεί με εκπόνηση ενός νέου, ολικά ή μερικά προγράμματος, ή με την αλλοίωση του ήδη υπάρχοντος ή με την απόκρυψη δεδομένων. Η αλλοίωση μπορεί αν γίνει με την προσθήκη ή εξάλειψη εντολών και γενικά με τη μεταβολή του, ώστε να παρακάμπτονται έλεγχοι ή επεξεργασία στοιχείων.[49]

Η μη ορθότητα της διαμόρφωσης ενός προγράμματος, ενδέχεται να υφίσταται, όταν το πρόγραμμα αυτό αποτελεί πρόσφορο μέσο, περιέχει εγγενώς τον κίνδυνο, για την επέλευση παράνομης περιουσιακής βλάβης και ως εκ τούτου η λειτουργία του προγράμματος αποκλίνει από την κοινωνικά αποδεκτή αποστολή του για την οποία προορίζεται.[50]

---

[47] Βλ. Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 195
[48] Βλ. Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 196
[49] Βλ. Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 196
[50] Βλ. Ειρ. Βασιλάκη, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, ΑΝΤ. Ν. ΣΑΚΚΟΥΛΑΣ, σελ. 599

Το έγκλημα τελείται με τον συγκεκριμένο τρόπο όταν ο δράστης διαμορφώνει το πρόγραμμα, δηλαδή είτε το κατασκευάζει από την αρχή ή επεμβαίνει και αναδιαμορφώνει το πρόγραμμα στη συνέχεια, ώστε αυτό να μην δίνει στον υπολογιστή τις κατάλληλες εντολές και επομένως να μην συνάγονται τα ορθά συμπεράσματα, παρόλο που του δίνονται ορθά εξωτερικά δεδομένα.

Έτσι, μη ορθή διαμόρφωση προγράμματος είναι η χειραγώγηση του προγράμματος, η οποία μπορεί να επιχειρηθεί εξαρχής ή μεταγενέστερα, με αποτέλεσμα τη μη ορθή επεξεργασία των δεδομένων που εισάγονται στον υπολογιστή. Η ορθότητα της διαμόρφωσης του προγράμματος καθορίζεται από την βούληση του δικαιούχου, δηλαδή του ιδιοκτήτη του υπολογιστή. Ωστόσο, είναι δυνατόν ο τρόπος διαμόρφωσης του προγράμματος να προβλέπεται απευθείας από τον νόμο, όπως συμβαίνει για παράδειγμα με τα προγράμματα για τον υπολογισμό μισθών ή συντάξεων.[51]

2) Χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή

Εδώ ουσιαστικά, πρόκειται για παρεμβάσεις παροδικού χαρακτήρα στο πληροφοριακό σύστημα, σε αντίθεση με τις παρεμβάσεις του προηγούμενου τρόπου τέλεσης της μη ορθής διαμόρφωσης, οι οποίες έχουν μόνιμο χαρακτήρα είτε από τη χρονική στιγμή που κατασκευάζεται το πρόγραμμα, είτε επιγενόμενα. Αντίθετα σε αυτόν τον τρόπο τέλεσης η επέμβαση στο πρόγραμμα ή στο σύστημα του υπολογιστή αφορά σε συγκεκριμένη εισαγωγή ορθών εξωτερικών δεδομένων και τελείται παράλληλα με αυτήν.[52] Επομένως ο δράστης, χωρίς να έχει το δικαίωμα ή να του έχει δοθεί η άδεια, προβαίνει σε επηρεασμό του πληροφοριακού συστήματος[53] με σκοπό να αποκτήσει περιουσιακό όφελος. Τέτοια περίπτωση θα μπορούσε να αποτελεί για παράδειγμα η χρήση ενός τρίτου προγράμματος υπολογιστή, το οποίο χρησιμοποιείται ως πρόγραμμα – «εισβολέας», το οποίο εμποδίζει τη σωστή του λειτουργία, κάνοντάς το ουσιαστικά «υποχείριο» για τον δράστη, όπως ακριβώς συμβαίνει με την περίπτωση του «hacking».[54]

---

[51] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 196-197

[52] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ.

[53] Ο ορισμός του πληροφοριακού συστήματος υπάρχει στον Ποινικό Κώδικα. Συγκεκριμένα, στο Άρθρο 13 περ. στ', το πληροφοριακό σύστημα ορίζεται ως: «συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών».

[54] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 206

3) Η χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας

Ο τρίτος τρόπος τέλεσης του αδικήματος της απάτης με υπολογιστή εμφανίζει ομοιότητες περισσότερο από όλους τους υπόλοιπους, με την κοινή απάτη. Πιο συγκεκριμένα, ο παραπάνω τρόπος τέλεσης φαίνεται να αντιστοιχεί στην αθέμιτη απόκρυψη ή παρασιώπηση γεγονότων της κοινής απάτης (386 ΠΚ), καθώς και στην παράσταση ψευδών γεγονότων. Σε αυτήν την περίπτωση δεν υπάρχει παρέμβαση του δράστη στον υπολογιστή και στο πρόγραμμα αυτού, το οποίο εκτελείται κανονικά με βάση τα προβλεπόμενα. Όμως, τα στοιχεία που εισάγονται σε αυτόν είναι μη ορθά[55] ή ελλιπή, κάτι που συνεπάγεται ότι το αποτέλεσμα που εξάγεται είναι μέσα στα πλαίσια της επιθυμίας του δράστη. Μη ορθά είναι τα δεδομένα του υπολογιστή που δεν ανταποκρίνονται στην πραγματικότητα, ενώ ελλιπή είναι εκείνα που εκφράζουν ανακριβώς την πραγματικότητα στην οποία αναφέρονται και η οποία έχει αποφασιστική σημασία για την επεξεργασία των δεδομένων. Κρίσιμο για τη στοιχειοθέτηση της απάτης με υπολογιστή είναι τα δεδομένα να αφορούν γεγονότα και όχι προγνώσεις ή αξιολογικές κρίσεις.[56]

Τέλος, στην περίπτωση γ' του Άρθρου 386Α ΠΚ φαίνεται να εντάσσεται και το αρκετά διαδεδομένο τα τελευταία χρόνια, φαινόμενο του "Skimming"[57], κατά το οποίο ο δράστης έχει «παγιδεύσει» το μηχάνημα ΑΤΜ, με αποτέλεσμα, όταν το θύμα εισάγει την κάρτα του, ο δράστης να αποκτά τα στοιχεία και να δημιουργεί μία κάρτα «κλώνο», την οποία έπειτα θα χρησιμοποιήσει για να εισέλθει στον λογαριασμό του ανυποψίαστου θύματος και να αφαιρέσει χρήματα.

4) Η χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητα

Στη συγκεκριμένη περίπτωση, αναφερόμαστε σε παράνομη χρήση πραγματικών δεδομένων, τα οποία εισάγονται, αλλοιώνονται ή διαγράφονται στον υπολογιστή.[58]

---

[55] Στη χρησιμοποίηση μη ορθών στοιχείων αναφέρεται η Απόφαση του Τριμελούς Εφετείου Κακουργημάτων Αθηνών (ΤρΕφΚακΑθηνών 4689/2018), με τον δράστη να συμπεριλαμβάνει στον κατάλογο επιδομάτων μη δικαιούχους. Αναλυτικά βλ. Απάτη με υπολογιστή, ΤρΕφΚακΑθ 4689/2018, ΠοινΔικ, 7/2020, σελ. 731-733.

[56] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 198

[57] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 204

[58] «Κανονική αλλά χωρίς δικαίωμα εκτέλεση προγράμματος». Βλ. Μυλωνόπουλος, Χ. Ποινικό Δίκαιο, Ειδικό μέρος, 4η Έκδοση, Νομική Βιβλιοθήκη, 2021, σελ. 487.

Τα δεδομένα είναι ορθά - αληθινά, όμως ο δράστης δεν έχει δικαίωμα να τα χρησιμοποιήσει. Για παράδειγμα, η πράξη τελείται όταν κάποιος χρησιμοποιεί το όνομα χρήστη τρίτου προσώπου και τον κωδικό πρόσβασής του, προκειμένου να εισέλθει στον τραπεζικό του λογαριασμό και να προβεί σε ανάληψη των χρημάτων του. Άλλη περίπτωση που εντάσσεται στην συγκεκριμένη κατηγορία απάτης με υπολογιστή είναι η χωρίς άδεια πρόσβαση στον υπολογιστή μιας εταιρίας και η μεταφορά χρηματικών ποσών σε κοινό λογαριασμό των συνεταίρων, από όπου στη συνέχεια ο κάθε ένας αντλεί με χρεωστική κάρτα μετρητά χρήματα για δικό του λογαριασμό.[59]

5) Η χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων

Ο πέμπτος τρόπος τέλεσης του αδικήματος της απάτης με υπολογιστή, αποτελεί μία νεοεισαχθείσα διάταξη του νέου Ποινικού Κώδικα, η οποία κατέστησε πλέον σαφές ότι η μεταφορά χρημάτων μέσω «web banking» από μη δικαιούμενο πρόσωπο συνιστά απάτη με υπολογιστή.[60] Πρόκειται λοιπόν, για μία ακόμη περίπτωση κατά την οποία το λογισμικό (πρόγραμμα) ενός υπολογιστή λειτουργεί ως μέσο διακίνησης και διασφάλισης περιουσιακών στοιχείων[61] με τους επιτήδειους να προσπαθούν να εισέλθουν με παράνομο τρόπο στο λογαριασμό του θύματος και να πάρουν τα χρήματά του. Τέλος, γίνεται αποδεκτό ότι η συγκεκριμένη διάταξη αφορά και τα λεγόμενα «κρυπτονομίσματα», τα οποία πλέον έχουν ευρεία εφαρμογή[62], απασχολώντας και τη δικαιοσύνη.[63]

3.6. Η ανάγκη ύπαρξης υλικής αντιστοιχίας οφέλους και βλάβης

Για την πραγμάτωση της αντικειμενικής υπόστασης της απάτης με υπολογιστή απαιτείται η σχέση υλικής αντιστοιχίας ανάμεσα στην περιουσιακή βλάβη του θύματος και στο παράνομο περιουσιακό όφελος του δράστη. Η σχέση υλικής αντιστοιχίας αποτελεί άγραφο στοιχείο της αντικειμενικής υπόστασης του εγκλήματος, δεδομένου ότι η απάτη με υπολογιστή αποτελεί έγκλημα περιουσιακής μετάθεσης.

---

[59] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 199

[60] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 199

[61] Η σημασία των εξ' αποστάσεως τραπεζικών συναλλαγών είχε ήδη εντοπιστεί από τις αρχές της δεκαετίας του 2000, αποτελώντας σημαντική έκφανση της προστασίας της ρύθμισης του Άρθρου 386 Α ΠΚ. Βλ. Νούσκαλης, Γ., Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ). Το παρελθόν και το μέλλον του Άρθρου 386 Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαική Ένωση, ΠοινΔικ, 2/2003, σελ. 178-190, ιδίως σε. 178-179.

[62] Βλ.Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ., «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη, 2023, σελ.167.

[63] Ενδιαφέρον παρουσιάζει το Βούλευμα του Συμβουλίου Πλημμελειοδικών Θεσσαλονίκης (828/2022), το οποίο αναφέρεται στα κρυπτονομίσματα/bticoins. Βλ. Απάτη με υπολογιστή, ΣυμβΠλημΘεσ 828/2022, ΠοινΔικ, 8-9/2022, σελ. 1228-1233.

Ο επηρεασμός των στοιχείων του υπολογιστή πρέπει να προκαλεί άμεσα μείωση ξένης περιουσίας. Η περιουσιακή ζημία είναι άμεση όταν δεν απαιτείται παρεμβολή ανθρώπινης συμπεριφοράς μεταξύ της επεξεργασίας των στοιχείων και της μείωσης της περιουσίας, όπως για παράδειγμα όταν ο υπολογιστής εμφανίζει αυξημένο ποσό στον λογαριασμό του δράστη.[64]

3.7. Η υποκειμενική υπόσταση του άρθρου 386^{A} Π.Κ.

Το αδίκημα της απάτης με υπολογιστή τελείται μόνο με δόλο. Ο δόλος του δράστη της απάτης με υπολογιστή είναι όμοιος με τον δόλο του δράστη της κοινής απάτης. Το υπό εξέταση αδίκημα είναι έγκλημα σκοπού, υπερχειλούς υποκειμενικής υπόστασης, διότι ο δράστης απαιτείται να έχει σκοπό παράνομου περιουσιακού οφέλους για τον εαυτό του ή για τρίτο. Για να στοιχειοθετεί το αδίκημα της απάτης με υπολογιστή αρκεί η ύπαρξη ενδεχόμενου δόλου.[65] Ωστόσο, ως προς τον σκοπό του πορισμού παράνομου περιουσιακού οφέλους στον εαυτό του δράστη ή σε τρίτον, απαιτείται δόλος πρώτου (α΄) βαθμού. Συνεπώς η τυχόν πραγμάτωση των στοιχείων της αντικειμενικής υπόστασης του αδικήματος με την επέμβαση σε ένα υπολογιστή, με κάποιον από τους τρόπους τέλεσης του άρθρου 386^{A} ΠΚ, χωρίς όμως να υφίσταται ταυτόχρονα και σκοπός προσπόρισης παράνομου περιουσιακού οφέλους, δεν αρκεί για την τέλεση του αδικήματος του άρθρου 386^{A} ΠΚ.[66]

3.8. Ποινικές κυρώσεις

Όσον αφορά την απειλούμενη ποινή που προβλέπεται για τις παπεριπτώσεις της παραγράφου 1 του Άρθρου 386 Α ΠΚ, αυτή αρχικά ορίζει ότι τιμωρούνται με φυλάκιση, όπου σύμφωνα με το άρθρο 53 ΠΚ η διάρκεια της φυλάκισης δεν υπερβαίνει τα πέντε έτη ούτε είναι κατώτερη των δέκα ημερών. Στα τελευταία του εδάφια του Άρθρου 386Α ΠΚ επιβάλλονται αναφέρονται υψηλότερες ποινές, οπότε μιλάμε για διακεκριμένες περιπτώσεις του εγκλήματος της Απάτης με υπολογιστή. Έτσι, αν η ζημία που προκλήθηκε από το έγκλημα είναι «ιδιαίτερα μεγάλη», προβλέπεται φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή, ενώ αν υπερβαίνει τις 120.000 ευρώ, προβλέπεται κάθειρξη έως δέκα έτη[67] και χρηματική ποινή.

---

[64] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 200

[65] Βλ. Χρίστος Μυλωνόπουλος, Ειδικό Μέρος, Ποινικό Δίκαιο, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, Π.Ν.ΣΑΚΟΥΛΑΣ, ΑΘΗΝΑ 2006, σελ. 525

[66] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 200

[67] Βλ. Άρθρο 52 παρ. 2 ΠΚ

Επίσης, είναι αδιάφορο αν η προηγουμένως αναφερθείσα ζημία αφορά ένα ή περισσότερα άτομα, αλλά σημασία έχει το συνολικό ποσό αυτής.[68] Διακεκριμένη περίπτωση τέλεσης του εγκλήματος είναι και αυτήν που περιγράφεται στην παράγραφο 3, όταν στρέφεται κατά του ελληνικού Δημοσίου, των ΝΠΔΔ και των ΟΤΑ, με ζημία μεγαλύτερη των 120.000 ευρώ, όπου επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες.

Ωστόσο, σύμφωνα με το Άρθρο 405 ΠΚ, όπως αυτό ισχύει μετά τον Ν.4855/2021, απαιτείται έγκληση για την κίνηση ποινικής δίωξης στην περίπτωση της απάτης με υπολογιστή του άρθρου 386^{A} παρ. 1 και παρ. 2 ΠΚ. Αντίθετα για την παρ. 3 του άρθρου 386^{A} ΠΚ, δηλαδή στην περίπτωση που η απάτη με υπολογιστή στρέφεται κατά του ελληνικού δημοσίου, των ΝΠΔΔ και των ΟΤΑ και η ζημία που προκλήθηκε συνολικά είναι μεγαλύτερη των 120.000 ευρώ δεν απαιτείται έγκληση, αλλά η δίωξη κινείται αυτεπάγγελτα.[69]

3.9 Παραλλαγές του αδικήματος

3.9.1. Προνομιούχες παραλλαγές

Οι προπαρασκευαστικές πράξεις τέλεσης της απάτης με υπολογιστή τυποποιούνται στο άρθρο 386^{A} παρ. 2 ΠΚ και αποτελούν αυτοτελές έγκλημα. Στη συγκεκριμένη διάταξη προβλέπεται ότι όποιος κατασκευάζει, διαθέτει ή κατέχει πρόγραμμα ή σύστημα υπολογιστή που προορίζεται για τη διάπραξη του εγκλήματος της πρώτης παραγράφου του ίδιου άρθρου, τιμωρείται με φυλάκιση έως δύο έτη και χρηματική ποινή.

Απαραίτητη προϋπόθεση για την κατάφαση του συγκεκριμένου αδικήματος είναι η διαπίστωση ότι το υπό εξέταση πρόγραμμα ή σύστημα υπολογιστή προορίζεται για την τέλεση απάτης με υπολογιστή του άρθρου 386^{A} παρ. 1 ΠΚ.

Οι προβλεπόμενες στο άρθρο 386^{A} παρ. 2 ΠΚ πράξεις μένουν ατιμώρητες όταν δεν προορίζονται για τέλεση απάτης με υπολογιστή. Μάλιστα, από κάθε ποινή απαλλάσσεται, όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή σύστημα υπολογιστή, πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος που προβλέπεται στην πρώτη παράγραφο.[70]

---

[68] Βλ. Ζέκος, Ι. Διαδίκτυο, Η/Υ & Τηλεπικοινωνίες στο ελληνικό δίκαιο, Εκδόσεις Σάκκουλα, 2017, σελ. 353.

[69] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 200-201

[70] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 201

3.9.2 Διακεκριμένες παραλλαγές

Στο άρθρο 386^{A} ΠΚ, τυποποιούνται πέρα από την απάτη με υπολογιστή στη βασική της μορφή, δύο διακεκριμένες παραλλαγές του εγκλήματος. Έτσι, η απλά διακεκριμένη μορφή του εγκλήματος θεμελιώνεται όταν η ζημία που προκλήθηκε από το έγκλημα είναι «ιδιαίτερα μεγάλη», επιβάλλοντας φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή, ενώ αν υπερβαίνει τις 120.000 ευρώ, προβλέπεται κάθειρξη από πέντε έως δέκα έτη και χρηματική ποινή.[71]

Στην τρίτη παράγραφο του άρθρου 386^{A} ΠΚ προβλέπεται ως ιδιαίτερα διακεκριμένη παραλλαγή η απάτης με υπολογιστή όταν στρέφεται κατά του ελληνικού Δημοσίου, των ΝΠΔΔ και των ΟΤΑ, με ζημία μεγαλύτερη των 120.000 ευρώ, όπου σε αυτήν την περίπτωση επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες.

Η απλή διακεκριμένη μορφή, όπως ήδη αναφέρθηκε και παραπάνω, εξακολουθεί να διώκεται κατ' έγκληση[72], ενώ η ιδιαίτερα διακεκριμένη μορφή της απάτης με υπολογιστή που στρέφεται κατά του ελληνικού Δημοσίου, των ΝΠΔΔ και των ΟΤΑ, όταν η ζημία ξεπερνάει συνολικά το ύψος των 120.000 ευρώ, διώκεται αυτεπάγγελτα.

3.10. Αξιόποινες προπαρασκευαστικές πράξεις (αρ. 386^{A} παρ. ΠΚ) και έμπρακτη μετάνοια

Στο άρθρο 386^{A} παρ. 2 ΠΚ του νέου Ποινικού κώδικα ποινικοποιείται ως ενέχουσα τυπικό κίνδυνο τέλεσης της πράξης της πρώτης παραγράφου της παραπάνω διάταξης, η κατασκευή ή η προμήθεια των instrumentorum sceleris. Ωστόσο, η διατύπωση της διάταξης είναι αρκετά διευρυμένη προκαλώντας σύγχυση εκ πρώτης όψεως σχετικά με το τι υπάγεται σε αυτήν. Επομένως, με τελολογική συσταλτική ερμηνεία της παραπάνω διάταξης καθίστανται τιμωρητέες οι πράξεις κατασκευής, κατοχής, διάθεσης προγραμμάτων ή πληροφοριακών συστημάτων που είναι αντικειμενικώς a priori ειδικά προορισμένα (εκ κατασκευής) για τέλεση πράξεων του άρθρου 386^{A} ΠΚ.[73] Η δεύτερη παράγραφος του άρθρου της απάτης με υπολογιστή επαπειλεί τον δράστη τέλεσης με ποινή φυλάκισης έως και δύο ετών, σε αντίθεση με το βασικό αδίκημα, το οποίο επίσης αποτελεί πλημμέλημα, αλλά χωρίς να πραγματοποιείται αναφορά στο πλαίσιο ποινής του, παραχωρώντας κατ' αυτόν τον τρόπο το δικαίωμα στην ελληνική δικαιοσύνη να αποφανθεί ανάλογα με το βαθμό της προσβολής της πράξης.

---

[71] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 202

[72] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 178

[73] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 179

Τέλος, στο εδάφιο β΄ του άρθρου 386^{A} ΠΚ προβλέπεται ειδική περίπτωση έμπρακτης μετάνοιας. Πιο συγκεκριμένα, το άρθρο 386^{A} ΠΚ παρ. 2 εδ. β΄ ορίζει ότι: *«Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή σύστημα υπολογιστή πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παρ. 1.»* Επομένως, σύμφωνα με το γράμμα του νόμου, ο δράστης που καταστρέφει αυτοβούλως το επικίνδυνο πρόγραμμα ή πληροφοριακό σύστημα οποτεδήποτε[75], χωρίς να το έχει χρησιμοποιήσει για τον προορισμό του, δηλαδή για την διάπραξη των αδικημάτων που προβλέπονται ονομαστικά στο άρθρο 386^{A} παρ. 1 ΠΚ, δεν διώκεται ποινικά.

3.11. Απόπειρα – Συμμετοχή – Συρροή – Έγκληση

Σύμφωνα με το άρθρο 42 παρ. 1 ΠΚ ορίζεται ότι: *«1. Όποιος, έχοντας αποφασίσει να τελέσει έγκλημα, αρχίζει να εκτελεί την περιγραφόμενη στο νόμο αξιόποινη πράξη, τιμωρείται, αν το έγκλημα δεν ολοκληρώθηκε, με μειωμένη ποινή (άρθρο 83).»* Συνεπώς για να στοιχειοθετεί το άρθρο 42 παρ. 1 ΠΚ και να τελεστεί το αδίκημα της απόπειρας ενός εγκλήματος απαιτείται αρχή εκτέλεσης της περιγραφόμενης στο νόμο αξιόποινης πράξης. Δυνάμει της αιτιολογικής έκθεσης του Νέου Ποινικού Κώδικα αναφέρεται ότι: *«…προσδιορίζεται ειδικότερα με μεγαλύτερη σαφήνεια το περιεχόμενο της αρχής εκτέλεσης του εγκλήματος, ώστε να είναι πλέον σαφές ότι το έγκλημα μπορεί να θεωρηθεί ότι βρίσκεται σε απόπειρα μόνο όταν έχει πραγματωθεί ένα τμήμα της αντικειμενικής του υπόστασης.»*[76]

Επομένως στην απάτη με υπολογιστή, απόπειρα με βάση το τυπικό αντικειμενικό κριτήριο νοείται μόνο σε περιπτώσεις που δεν ολοκληρώθηκε η επεξεργασία των δεδομένων π.χ. επειδή έλαβε χώρα διακοπή ρεύματος, διακοπή σύνδεσης στο διαδίκτυο ή βλάβη του Η/Υ μετά την εισαγωγή δεδομένων.[77]

Βάσει του νέου Ποινικού κώδικα οι μορφές συμμετοχής σε εγκλήματα, όπως διατυπώνονται στο άρθρο 47 ΠΚ είναι οι εξής: φυσικός αυτουργός, ήτοι δράστης, έμμεσος αυτουργός, ηθικός αυτουργός, προβοκάτορας, συνεργός και πέραν αυτών υφίσταται και η έννοια της συναυτουργίας. Έχει καταργηθεί η διάκριση μεταξύ άμεσου και απλού συνεργού και προβλέφθηκε, ότι στον συνεργό επιβάλλεται καταρχήν μειωμένη ποινή. Παρέχεται, ωστόσο, στο δικαστήριο η δυνατότητα να επιβάλει πλήρη ποινή αν ο υπαίτιος προσφέρει τη συνδρομή του κατά την τέλεση της πράξης και θέτει με αυτήν το αντικείμενο της προσβολής στη διάθεση του φυσικού αυτουργού.[78]

---

[75] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 179

[76] Βλ. Αιτιολογική Έκθεση Ν. Ποινικού Κώδικα

[77] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 177

[78] Βλ. Αιτιολογική Έκθεση στο σχέδιο του νόμου «Κύρωση του Ποινικού Κώδικα», σελ. 5

Ωστόσο, για να θεμελιωθεί συναυτουργία με το στενό τυπικό αντικειμενικό κριτήριο κατά την εισαγωγή ψηφιακών δεδομένων με πληκτρολόγηση θα έπρεπε οι δράστες που εμφορούνται από κοινό δόλο (συναπόφαση) και σκοπό προσπορισμού περιουσιακού οφέλους να πιέζουν από κοινού τα πλήκτρα ή ο ένας να βαστά το χέρι του άλλου κατά την πληκτρολόγηση. Πάντως ο χειραγωγών καλόπιστο να εισάγει (τα ελλιπή ή ορθά) ψηφιακά δεδομένα στο πληροφοριακό σύστημα ή να παρέμβει στη λειτουργία του κατά τρόπο που προκαλεί ζημιογόνα για τρίτο επεξεργασία τους είναι έμμεσος αυτουργός απάτης με υπολογιστή, αφού ο καλόπιστος δεν έχει σκοπό προσπορισμού παρανόμου περιουσιακού οφέλους στον εαυτό του ή σε τρίτο και επομένως δεν πράττει άδικα.[79]

Ένα ιδιαιτέρως ενδιαφέρον ζήτημα της απάτης με υπολογιστή αποτελεί η συρροή του αδικήματος με άλλα και ο τρόπος αντιμετώπισής τους, είτε ως ένα ενιαίο αδίκημα, είτε η διατήρηση αυτοτέλειας του αδίκου τους, εστιάζοντας κατά συνέπεια στην αληθινή και φαινομένη συρροή.

Αρχικά, μεταξύ των εγκλημάτων της απάτης (386 ΠΚ) και της απάτης με υπολογιστή (386Α ΠΚ), υπάρχει σχέση αμοιβαίου αποκλεισμού και επομένως αποκλείεται και η μεταξύ τους αληθινή συρροή,[80] δεδομένου ότι για την τέλεση της κλασσικής απάτης απαιτείται παραπλάνηση φυσικού προσώπου, ενώ για την στοιχειοθέτηση της απάτης με υπολογιστή η παράνομη περιουσιακή ζημία προκύπτει από την απευθείας παρέμβαση στον υπολογιστή, στο πρόγραμμα ή στα δεδομένα του.[81.] Σύμφωνα με την υπ' αριθμ. 68/2014 απόφαση του Εφετείου Δυτικής Στερεάς Ελλάδος: *«Μεταξύ της απάτης του άρ. 386 ΠΚ και της διάταξης του άρ. 386Α ΠΚ δεν υπάρχει αληθινή συρροή, αλλά σχέση αμοιβαίου αποκλεισμού αν ταυτίζονται τα περιστατικά, αφού η κοινή απάτη τελείται με την παραπλάνηση κάποιου φυσικού προσώπου, ενώ για το παρόν έγκλημα απαιτείται ανεξάρτητα από παραπλάνηση, η αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων του υπολογιστή».*[82]

Δεδομένου, ότι η απάτη αποτελεί το κατ' εξοχήν αδίκημα αυτοβλάβης, αποκλείεται το ενδεχόμενο αληθούς συρροής της και με το αδίκημα της κλοπής (άρθρο 372 ΠΚ), καθώς και με το αδίκημα της υπεξαίρεσης (άρθρο 375 ΠΚ), οι οποίες προυποθέτουν επενέργεια επί ενσώματου υλικού αντικειμένου (πράγματος). Επομένως ομοίως με την κοινή απάτη, τα δύο παραπάνω αδικήματα τελούν σε σχέση αμοιβαίου αποκλεισμού με την απάτη με υπολογιστή.[83]

---

[79] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 177

[80] Βλ. Αδάμ Παπαδαμάκης, Τα περιουσιακά εγκλήματα, Β' Έκδόση, Εκδόσεις Σάκκουλα, 2016, σελ. 171

[81] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 208

[82] Βλ. 68/2014 Εφετ.Δυτ.Στερ.Ελλάδας

[83] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 177-178

Αρκετά ιδιαίτερη, είναι η σχέση μεταξύ των αδικημάτων της πλαστογραφίας μετά χρήσεως και της τετελεσμένης απάτης με υπολογιστή, καθώς η πλαστογραφία (άρθρο 216 ΠΚ) αποτελεί το συνηθέστερο μέσο τέλεσης του αδικήματος της απάτης με υπολογιστή.

Η ελληνική νομολογία έχει δεχτεί, ότι: «τα εγκλήματα της πλαστογραφίας με χρήση κατ' επάγγελμα και της απάτης με υπολογιστή κατ' επάγγελμα συρρέουν αληθινά μεταξύ τους, αφού ουδέν εξ αυτών αποτελεί ουσιαστικό του άλλου, ενώ το έγκλημα της απόπειρας απάτης απλής ή με τις επιβαρυντικές της περιστάσεις ή της απάτης με υπολογιστή σε απόπειρα δεν συρρέει με το έγκλημα της πλαστογραφίας με χρήση όταν αμφότερα απαρτίζονται από τα ίδια ιστορικά δεδομένα (πραγματικά περιστατικά) αλλά στην περίπτωση αυτή ισχύει η αρχή της απορροφήσεως».

Μάλιστα έχει γίνει δεκτό, ότι «η πράξη της απόπειρας απάτης απλής ή με υπολογιστή με την κοινή ή επιβαρυντική της μορφή απορροφάται από την πράξη της πλαστογραφίας με χρήση με τις επιβαρυντικές της περιστάσεις και ότι αμφότερα τα ανωτέρω εγκλήματα συρρέουν μεταξύ τους αληθινά, όταν απαρτίζονται από διαφορετικά πραγματικά περιστατικά».[84]

Τέλος, όσον αφορά τη συρροή της απάτης με υπολογιστή με την απιστία (άρθρο 390 ΠΚ), αυτές συρρέουν φαινομενικά κατ' ιδέαν λόγω της σχέσης αλληλοτομής που υφίσταται μεταξύ τους. Πιο συγκεκριμένα η απάτη με υπολογιστή ως ψηφιακό furtum καλύπτει προσβολές της περιουσίας τόσο εκ των έξω (κλοπή, απάτη κλπ.), όσο και των έσω (υπεξαίρεση εμπιστευμένων άυλων αγαθών). Η χωρίς δικαίωμα μεταφορά χρημάτων με αξιοποίηση λογισμικού από πρόσωπο που έχει την επιμέλεια ή την διαχείριση ξένης περιουσίας, δηλαδή την ιδιότητα του διαχειριστή εντοπίζεται στο πεδίο αλληλοτομής των δύο άρθρων (π.χ. ο επίτροπος ή δικαστικός συμπαραστάτης που μεταφέρει χρήματα από τον τραπεζικό λογαριασμό του επιτροπευόμενου ή του συμπαραστατούμενου κάνοντας χρήση κωδικών web banking που κατέχει λόγω της ιδιότητάς του προβεί σε παράνομη περιουσιακή ζημία του ανήλικου ή του συμπαραστατούενου πράττοντας «χωρίς δικαίωμα» και κατά «παράβαση των κανόνων επιμελούς διαχείρησης». Επιπλέον μεταξύ των παραπάνω δύο άρθρων υφίσταται και σχέση επικουρικότητας, διότι στις δύο διατάξεις οι απειλούμενες ποινικές κυρώσεις ταυτίζονται πλήρως όσον αφορά το βασικό έγκλημα και τις διακεκριμένες παραλλαγές. Ωστόσο, διαφέρουν μόνο στο ότι δεν προβλέπεται προνομιούχα παραλλαγή απιστίας με ζημία μικρής αξίας. Επομένως όταν η ζημία είναι μικρής αξίας, η απιστία είναι οπωσδήποτε αυστηρότερη διάταξη και απωθεί την απάτη με υπολογιστή. Και στις υπόλοιπες, όμως, περιπτώσεις η απιστία είναι η κύρια διάταξη και απωθεί την απάτη με υπολογιστή ως επικουρική λόγω της εντονότερης προσβολής της περιουσίας από τον εγγυητή της ακεραιότητας της περιουσίας διαχειριστή αυτή.[85]

---

[84] Βλ. ΑΠ 190/2009, ΑΠ 573/2009, ΑΠ 66/2007, 28/2010 Συμβ.Εφετ.Θεσσαλ

[85] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 179-180

Κατά το άρθρο 405 παρ. 1 ΠΚ, όπως έχει ήδη αναφερθεί και παραπάνω στο παρόν πόνημα, απαιτείται έγκληση για τη δίωξη της απάτης με υπολογιστή σε όλες τις περιπτώσεις, πλην των πράξεων που στρέφονται ευθέως κατά του ελληνικού δημοσίου, των ΝΠΔΔ και των ΟΤΑ και επιπλέον (σωρευτικά) η συνολική ζημία που προκλήθηκε υπερβαίνει τις 120.000 ευρώ δεν απαιτείται έγκληση, αλλά η δίωξη κινείται αυτεπάγγελτα. Η απάτη με υπολογιστή με συνολική ζημία κάτω των 120.000 ευρώ διώκεται και σε αυτές τις περιπτώσεις μόνο κατ' έγκληση.[86]

3.12. Ποινική Συνδιαλλαγή και Ποινική Διαπραγμάτευση

Στο άρθ. 301 του ΚΠΔ, προβλέπεται η ποινική συνδιαλλαγή μέχρι την τυπική περάτωση της κύριας ανάκρισης. Η θέσπιση της εν λόγω διαδικασίας επίλυσης ποινικών διαφορών υπακούει στις συστάσεις του Συμβουλίου της Ευρώπης αλλά και στην αναγκαιότητα αποσυμφόρησης της σχετικής ποινικής ύλης. Η εμπειρία από τις έννομες τάξεις εφαρμογής τέτοιων ειδικών διαδικασιών (ΗΠΑ, Μ. Βρετανία, Ιταλία) αποδεικνύει ότι ένα σημαντικό ποσοστό ποινικών υποθέσεων (από 60-86%) επιλύεται με τον τρόπο αυτό ενώ παράλληλα επιτρέπει την ικανοποιητική υλοποίηση της τακτικής διαδικασίας στις υπόλοιπες περιπτώσεις.[87]

Η ποινική συνδιαλλαγή εφαρμόζεται σε περιορισμένο αριθμό αδικημάτων και ειδικότερα στα κακουργήματα: α) που προβλέπονται στα άρθρα 216 παρ. 3 και 4(πλαστογραφία) και 242 παρ. 3, 4 και 5 ΠΚ (ψευδής βεβαίωση υπαλλήλου), β) που χωρίς βία ή απειλή στρέφονται κατά της ιδιοκτησίας και της περιουσίας, ήτοι της διακεκριμένης περίπτωσης κλοπής (άρθ.374 ΠΚ), της υπεξαίρεσης αντικειμένου αξίας άνω των 120.000 ευρώ (άρθ. 375§2,3 του ΠΚ), της απάτης με προκληθείσα ζημία άνω των 120.000 ευρώ (άρθ. 386§1 εδ. β΄ του ΠΚ), της απάτης με υπολογιστή με προκληθείσα ζημία άνω των 120.000 ευρώ (άρθ. 386Α§1 εδ. β', 2 του ΠΚ), της απάτης σχετικά με τις επιχορηγήσεις, με προκληθείσα ζημία άνω των 120.000 ευρώ (άρθ. 386Β§1 εδ. β΄ του ΚΠΔ), της απιστίας με προκληθείσα ζημία άνω των 120.000 ευρώ (άρθ. 390§1 εδ. β΄, 2 του ΠΚ) και γ) που προβλέπονται στους νόμους 1599/1986 (της ψευδούς υπεύθυνης δήλωσης με την οποία ο δράστης επιχείρησε να προσπορίσει στον εαυτό του ή άλλον περιουσιακό όφελος βλάπτοντάς άλλον, εάν το όφελος ή η βλάβη ξεπερνά τις 75.000 ευρώ), 2960/2001 (της κακουργηματικής λαθρεμπορίας, όταν δηλ. οι δασμοί, φόροι και λοιπές επιβαρύνσεις που στερήθηκε το Δημόσιο ή η Ευρωπαϊκή Ένωση υπερβαίνουν το ποσό των εκατόν πενήντα χιλιάδων (150.000) ευρώ), 4557/2018 (της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες) και 4174/2013 (των κακουργηματικών περιπτώσεων φοροδιαφυγής), ανεξάρτητα από την συνδρομή ή μη επιβαρυντικών περιστάσεων.

---

[86] Βλ. Ιωάννης Κ. Μοροζίνης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 178

[87] Βλ. Α. Παπαδαμάκης, Ποινική Δικονομία, ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑ, 7η έκδ., 2017, σελ. 448

Επίσης, μετά κατάργηση του Ν. 1608/50, περιλαμβάνονται και οι περιπτώσεις που στρέφονται κατά του Δημοσίου, οι οποίες προβλέπονται ως επιβαρυντικές περιπτώσεις σε αδικήματα του ΠΚ. Η ως άνω ένταξη διεύρυνε και τον κύκλο των ατόμων, που λαμβάνουν μέρος στην ποινική συνδιαλλαγή, με τον νόμιμο εκπρόσωπο του Δημοσίου, να προστίθεται, σε αυτόν, ως παθόντας.[88]

Ο Ν. 4620/2019, εισήγαγε στον Κώδικα Ποινικής Δικονομίας το 303 ΚΠΔ, το οποίο πραγματώνεται την νεοπαγή διαδικασία της ποινικής διαπραγμάτευσης που αποτελεί τον πιο διαδεδομένο διεθνώς τύπο εναλλακτικής διαχείρισης των ποινικών υποθέσεων. Η ποινική διαπραγμάτευση στο δίκαιό μας, όπως προκύπτει από την παράγραφο 1 του άρθρου 303 ΚΠΔ, αφορά τον κύκλο των αυτεπαγγέλτως διωκόμενων πλημμελημάτων και κακουργημάτων και αυτή είναι μία εκ των βασικότερων διαφορών της με την ποινική συνδιαλλαγή.[89]

Αντικείμενο της ποινικής διαπραγμάτευσης, αποτελεί αποκλειστικά και μόνο η επιβλητέα κύρια ή παρεπόμενη ποινή. Η διαδικασία αυτή, προκειμένου να εφαρμοστεί θέτει ως προαπαιτούμενο την αυτεπάγγελτη δίωξη των αδικημάτων, με αποτέλεσμα να μην χαίρει εφαρμογής επί του αδικήματος της απάτης με υπολογιστή, το οποίο κατά το νέο άρθρο 405 ΚΠΔ διώκεται μόνο κατόπιν υποβολής έγκλησης από τον παθόντα, λαμβανομένου υπόψη του ατομικού χαρακτήρα του προσβαλλόμενου εννόμου αγαθού της περιούσιας.

Συνοψίζοντας, καταλήγουμε ότι ο δρόμος της ποινικής συνδιαλλαγής, είναι προτιμητέος από την πλευρά ενός κατηγορουμένου, ο οποίος πράγματι έχει τελέσει την πράξη για την οποία κατηγορείται, υπό την προϋπόθεση να αποζημιώσει τον παθόντα, δεδομένης της προνομιακής μεταχείρισης, που επιφυλάσσει το εν λόγω άρθρο για τον ίδιο. Ωστόσο, η ένταξη των ανωτέρω εναλλακτικών τρόπων απονομής δικαιοσύνης, στην ελληνική έννομη τάξη, απαιτεί αλλαγή νοοτροπίας, ώστε παράλληλα με την αποσυμφόρηση της δικαστικής ύλης, να επικρατήσει στη συνείδηση του δικαστικού κόσμου η καταλλαγή και συμφιλίωση, ως τρόπος αποκατάστασης της δικαϊκής ειρήνης.[90]

---

[88] https://www.esdi.gr/nex/images/stories/pdf/epimorfosi/2019/zarkaziaspoin_2019.pdf

[89] Βλ. Νικόλαος Δαγκλής Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 323

[90] Βλ. Θεοχάρης Δαλακούρας, Ο νέος Κώδικας Ποινικής Δικονομίας – Μία πρώτη ερμηνευτικής προσέγγιση του Ν. 4620/2019, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, 2019, σελ. 88

ΚΕΦΑΛΑΙΟ Δ΄

4. Η απάτη «με» υπολογιστή και η απάτη «μέσω» υπολογιστή

Το έγκλημα της Απάτης με υπολογιστή (Άρθρο 386Α ΠΚ) παρουσιάζει πολλές ομοιότητες με το έγκλημα της κοινής Απάτης (Άρθρο 386 ΠΚ). Αρχικά, τόσο η απάτη, όσο και η απάτη με υπολογιστή αποτελούν εγκλήματα αυτοβλάβης και αποτελέσματος. Και τα δύο αποτελούν κοινά εγκλήματα, καθώς μπορούν να τελεστούν από οποιονδήποτε, προσβάλλουν το ίδιο έννομο αγαθό, αυτό της περιουσίας και έχουν υπερχειλή υποκειμενική υπόσταση. Μάλιστα, άλλη μια ομοιότητα που παρουσιάζουν είναι ότι και στα δύο αδικήματα απαιτείται να υφίσταται το στοιχείο της αμεσότητας της περιουσιακής διάθεσης και εκείνο της υλικής αντιστοιχίας μεταξύ περιουσιακής βλάβης και παράνομου περιουσιακού οφέλους. Τέλος, για την κίνηση δίωξης και στα δύο αδικήματα σύμφωνα με το άρθρο 405 παρ. 1 ΠΚ απαιτείται καταρχήν υποβολή έγκλησης, ενώ και στα δύο προβλέπονται προνομιούχες και διακεκριμένες παραλλαγές.

Ωστόσο, όπως επίσης έχει ήδη αναφερθεί, τα δύο παραπάνω εγκλήματα τελούν σε σχέση σχέση αμοιβαίου αποκλεισμού μεταξύ τους. Δηλαδή, μπορείς να τελέσεις ή το 386 ή το 386Α. Στο άρθρο 386 ΠΚ η παραπλάνηση ενός φυσικού προσώπου οδηγεί στην περιουσιακή βλάβη, ενώ στο άρθρο 386Α ΠΚ ο επηρεασμός μίας επεξεργασίας δεδομένων οδηγεί αντίστοιχα στην περιουσιακή βλάβη. Υπάρχει λοιπόν μία «αντιστοιχία» ανάμεσα στις δύο διατάξεις, συνδέεται δηλαδή η πλάνη που προκαλείται με την πειθώ στο θύμα (Άρθρο 386 ΠΚ), με τον επηρεασμό του συστήματος υπολογιστή (Άρθρο 386^{Α} ΠΚ). Σε αυτό το σημείο όμως βρίσκεται και η μεγαλύτερη διαφορά μεταξύ των δύο ρυθμίσεων, καθώς στην πρώτη απαιτείται να επέλθει πλάνη σε φυσικό πρόσωπο, ενώ στην απάτη με υπολογιστή απαιτείται ο επηρεασμός του ίδιου του συστήματος του υπολογιστή, για να έχει ο δράστης το επιθυμητό αποτέλεσμα.

Στην περίπτωση, λοιπόν, που ένας υπολογιστής χρησιμοποιείται ως μέσο για την τέλεση του αδικήματος της κλασσικής απάτης, καθώς ο δράστης για να πετύχει τον σκοπό του παραπλανεί μέσου αυτού το θύμα, τότε πραγματώνεται η απάτη «μέσω υπολογιστή», καθώς σε αυτήν την περίπτωση ο υπολογιστής αποτελεί απλώς ένα μέσο για την επίτευξη του σκοπού του δράστη που δεν είναι άλλος από την περιουσιακή βλάβη του θύματος.

Τα εγκλήματα στις περιπτώσεις αυτές τελούνται συνήθως από δράστες που πιθανώς εκμεταλλεύονται την θέση τους σε επιχειρήσεις και την πρόσβασή τους σε ηλεκτρονικούς υπολογιστές, δρώντας σε βάρος των πελατών.[91] Σε αυτές λοιπόν τις περιπτώσεις εφαρμόζεται το άρθρο 386 ΠΚ. Όταν όμως ένας υπολογιστής επηρεάζεται ως σύστημα ώστε να επιτευχθεί περιουσιακή ζημία, τότε πραγματώνεται η απάτη με υπολογιστή και εφαρμόζεται η διάταξη του άρθρου 386^{Α} ΠΚ.

---

[91] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 208

Επομένως, αν και εξετάζοντας τα δύο άρθρα παρατηρούμε ότι εμφανίζουν πολλές ομοιότητες, η ειδοποιός διαφορά τους έγκειται στο ποιος «πλανάται» για να επέλθει η περιουσιακή βλάβη. Έτσι στην κοινή απάτη θύμα της πλάνης που προκαλεί ο δράστης αποτελεί ο ανθρώπινος νους, ενώ στην απάτη με υπολογιστή «πλανάται», ορθώς επηρεάζεται ένα σύστημα υπολογιστή.

ΚΕΦΑΛΑΙΟ Ε'

5. Μορφές απάτης με ή μέσω υπολογιστή στην σύγχρονη εποχή

Στην σημερινή εποχή τόσο το αδίκημα της κοινής απάτης μέσω υπολογιστή (άρθρο 386 ΠΚ), όσο και το αδίκημα της απάτης με υπολογιστή (άρθρο 386^{A} ΠΚ) βρίσκουν εφαρμογή σε πληθώρα περιπτώσεων. Μερικές από τις πιο διαδεδομένες θα τις αναλύσουμε στη συνέχεια.

5.1. *«Skimming»*

Η μέθοδος skimming συνίσταται στην αντιγραφή των δεδομένων καρτών και συγκεκριμένα εκείνων των δεδομένων που βρίσκονται καταγεγραμμένα στη μαγνητική λωρίδα, μεταξύ των οποίων είναι και ο αριθμός PIN της κάρτας. Σε αυτήν την περίπτωση ο δράστης κατασκευάζει αυτοσχέδιο μηχανισμό παγίδευσης καρτών αναλήψεων, τον οποίο στη συνέχεια τοποθετεί σε ΑΤΜ και συγκεκριμένα κάτω από τον καρταναγνώστη που υπάρχει στην είσοδο του θαλάμου που στεγάζει το ΑΤΜ. Σε αυτόν τον μηχανισμό τοποθετείται κάμερα, η οποία καταγράφει τους κωδικούς αριθμούς των καρτών, καθώς επίσης και τους αριθμούς πρόσβασης (pin) στους τραπεζικούς λογαριασμούς τους, για την ανάληψη χρημάτων κατά την πληκτρολόγησή τους. Ο δράστης μέσω του παραπάνω μηχανισμού υποκλέπτει τα προσωπικά δεδομένα από την πρωτότυπη κάρτα κατά την ώρα της συναλλαγής από τον νόμιμο κάτοχό της. Στη συνέχεια ο δράστης κατασκευάζει κάρτα – κλώνο της, τοποθετώντας σε αυτήν μέσω του κατάλληλου λογισμικού Η/Υ, τους κωδικούς που έχει υποκλέψει και τα υπόλοιπα στοιχεία της μαγνητικής κάρτας. Έτσι, πλέον με την κάρτα – κλώνο που έχει δημιουργήσει μπορεί να εκταμιεύσει παράνομα ποσά από τον λογαριασμό του νόμιμου δικαιούχο. Στην περίπτωση αυτή τελείται απάτη με υπολογιστή, κατ' εφαρμογή του άρθρου 386^{A} παρ. 1 περ. γ΄ ΠΚ, καθώς ο δράστης χρησιμοποιεί μη ορθά δεδομένα (πλαστές κάρτες).[92]

Το παραπάνω φαινόμενο έχει απασχολήσει τα τελευταία χρόνια και τη δικαιοσύνη, καθώς δεν είναι λίγες οι φορές που επιτήδειοι έχουν προβεί στην παγίδευση μηχανήματος ΑΤΜ για να αποκομίσουν παράνομο περιουσιακό όφελος.[93]

---

[92] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 204

[93] Βλ. ΑΠ 131/2013, ΑΠ 1087/2019, ΑΠ 908/2020 (από την ιστοσελίδα του Άρειου Πάγου)

5.2. «Phishing»

Ωστόσο, πρέπει να αναφερθούν και κάποιες περιπτώσεις εγκλημάτων τα οποία, αν και δεν εντάσσονται στις περιπτώσεις του Άρθρου 386Α ΠΚ, εντούτοις Δημιουργείται συχνά σύγχυσή τους με αυτό. Αρχικά, πρέπει να σημειωθεί το φαινόμενο του «phishing», το οποίο είναι πολύ διαδεδομένο τα τελευταία χρόνια. Επιγραμματικά, το «phishing» είναι η συνηθισμένη πρακτική αποστολής παραπλανητικών e-mails, τα οποία υποτίθεται ότι προέρχονται από επίσημους φορείς (τράπεζες κ.α.) και συνήθως έχουν ως στόχο την απόκτηση των τραπεζικών στοιχείων του θύματος, το οποίο καλείται να πατήσει σε έναν σύνδεσμο (link) και να συμπληρώσει τον αριθμό του τραπεζικού του λογαριασμού, τον προσωπικό αριθμό αναγνώρισης PIN και έναν πρόσθετο αριθμό, ο οποίος καθιστά δυνατή την εκτέλεση συναλλαγών μέσω διαδικτύου (TAN). Αν ο παραλήπτης αποκαλύψει αυτά τα στοιχεία, τότε ο δράστης – phisher διεισδύει στον λογαριασμό του, χρησιμοποιώντας όλες τις απαραίτητες πληροφορίες που του έδωσε ο παραλήπτης του παραπλανητικού e-mail και προβαίνει στην παράνομη περιουσιακή βλάβη του πλέον θύματος, μεταφέροντας χρήματα σε λογαριασμό της επιλογής του. Η συγκεκριμένη πράξη τιμωρείται με την κοινή απάτη του άρθρου 386 ΠΚ και όχι με τη διάταξη του άρθρου 386Α ΠΚ. Η τυχόν, ωστόσο, αποστολή του παραπλανητικού phising e-mail, χωρίς να προκληθεί παραπλάνηση του αποδέκτη του συνιστά απόπειρα απάτης, καθώς ο phisher γνωρίζει το περιεχόμενο του email και έχει σκοπό να αποκομίσει παράνομο περιουσιακό όφελος.[94]

5.3. «Pharming»

Παρόμοια με την μέθοδο του «phishing» είναι και η μέθοδος του «pharming», σύμφωνα με την οποία ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και τον επηρεάζει κατά τέτοιο τρόπο, ώστε ο συγκεκριμένος υπολογιστής να μπορεί να επισκέπτεται μόνο πλαστές ιστοσελίδες, ακόμη κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου. Ούτε σε αυτήν την περίπτωση εφαρμόζεται η διάταξη του άρθρου 386Α ΠΚ, αλλά βρίσκει εφαρμογή η διάταξη του 370Β ΠΚ, όπως ακριβώς συμβαίνει και με το «hacking», δεδομένου ότι στο άρθρο 370Β ΠΚ τυποποιείται ως αξιόποινη πράξη η παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα.[95]

---

[94] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 204-205

[95] Βλ. Νικόλαος Μ. Σαββίδης, Δαλακούρας Θ. «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη 2023, σελ. 205-206

ΕΠΙΛΟΓΟΣ/ΣΥΜΠΕΡΑΣΜΑΤΑ

Η συνεχής εξέλιξη που παρατηρείται στις νέες τεχνολογίες καθιστά επιτακτική την ανάγκη εγρήγορσης τόσο των πολιτών για την προσωπική τους ασφάλεια, όσο και του νομοθέτη για την πάταξη του ηλεκτρονικού εγκλήματος. Στη σημερινή εποχή, όπου η εργασία μας, οι καθημερινές δραστηριότητές μας, η επικοινωνία μας με τους συνανθρώπους μας, καθώς και οι συναλλαγές μας μπορούν να γίνουν «με το πάτημα ενός κουμπιού», αυτό έχει επιφέρει ως αποτέλεσμα την δημιουργία μιας σχέσης εξάρτησης από τις «έξυπνες» συσκευές μας, που έχουν εισχωρήσει καταλυτικά στη ζωή μας (smartphone, smartwatch κλπ.), την οποία και προσδιορίζουν καθοριστικά. Αν και ομολογουμένως το διαδίκτυο και οι νέες τεχνολογίες έχουν διευκολύνει τη ζωή μας, ωστόσο δεν είναι λίγες και οι φορές που την έχουν δυσχεράνει και την εκθέτουν σε άγνωστους κινδύνους.

Είναι γεγονός πως η σύγχρονη κοινωνία αντιμετωπίζει δυσκολίες σχετικά με την αντιμετώπιση των ηλεκτρονικών εγκλημάτων, πόσο μάλλον με την αντιμετώπιση του φαινομένου της απάτης με υπολογιστή, λόγω της ανωνυμίας που χαρακτηρίζει το διαδίκτυο. Η προσπάθεια που έχει γίνει με το πέρασμα των χρόνων από την πλευρά του ποινικού νομοθέτη είναι αισθητή, ωστόσο λόγω της ραγδαίας εξέλιξης των νέων τεχνολογιών απαιτείται συνεχής ενημέρωση των ποινικών διατάξεων και νομοθετική εγρήγορση για την αντιμετώπιση των νέων μορφών εγκληματικότητας που εμφανίζονται.

Όσον αφορά στο άρθρο της απάτης με υπολογιστή (386^{A} ΠΚ), η ύπαρξη μιας ξεχωριστής ποινικής διάταξης από αυτή της κοινής απάτης (386 ΠΚ) υποδηλώνει ακριβώς την μεγάλη σημασία των περιπτώσεων επηρεασμού του αποτελέσματος της διαδικασίας επεξεργασίας δεδομένων υπολογιστή με σκοπό την προσπόριση παράνομου περιουσιακού οφέλους στην σύγχρονη κοινωνία, καθώς τα θύματα τέτοιων ενεργειών καθημερινά πληθαίνουν.

Συγκεκριμένα, καθώς οι οικονομικές συναλλαγές των πολιτών τα τελευταία χρόνια έχουν μεταφερθεί στο διαδίκτυο με την χρήση είτε Η/Υ, είτε κάποιας άλλης ηλεκτρονικής συσκευής (π.χ. winbank μέσω εφαρμογής στα κινητά τηλέφωνα), οι δράστες αναζητούν συνεχώς νέους τρόπους απόκτησης παράνομου οικονομικού οφέλους, εκμεταλλευόμενοι τον επηρεασμό ενός συστήματος υπολογιστή ή την αδυναμία ενός προγράμματος, αναπτύσσοντας την κατάλληλη τεχνογνωσία για την επίτευξη του σκοπού τους.

Είναι γεγονός πως ο εντοπισμός των δραστών τέτοιων ενεργειών συχνά είναι δύσκολος, λόγω των ιδιαίτερων χαρακτηριστικών (κυρίως της ανωνυμίας) των υπολογιστών και του διαδικτύου. Επομένως ιδιαίτερη έμφαση θα πρέπει να δοθεί στον τομέα της πρόληψης, με την ενημέρωση των πολιτών κάθε ηλικίας σχετικά με τους κινδύνους που ελλοχεύουν στο διαδίκτυο. Αυτή θα μπορούσε να επιτευχθεί κυρίως μέσω του σχολίου, όπου από νεαρή ηλικία θα παρέχεται η απαιτούμενη ενημέρωση, αλλά και η τεχνογνωσία για την αποφυγή κινδύνων. Το διαδίκτυο, όπως εξάλλου και κάθε μορφή ανθρώπινης δραστηριότητας, μπορεί να μην καταστεί ποτέ απόλυτα ακίνδυνο, όμως με την κατάλληλη προσπάθεια και ευαισθητοποίηση, υφίσταται η δυνατότητα εγκληματικά

φαινόμενα, όπως αυτό της απάτης μέσω υπολογιστή, να γνωρίσουν δραματική μείωση και να επιτευχθεί με αυτόν τον τρόπο, ένα ασφαλέστερο ψηφιακό περιβάλλον για όλους.

Αξίζει να σημειωθεί σε αυτό το σημείο, ότι πολλά υποσχόμενη για την κυβερνοασφάλεια αποτελεί η Οδηγία NIS2, με την οποία, όπως αναφέρθηκε και παραπάνω, εκσυγχρονίζεται το υφιστάμενο νομικό πλαίσιο, ώστε να συμβαδίζει με την αυξημένη ψηφιοποίηση και το εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο. Τα νομικά μέτρα που προβλέπει να λάβουν τα κράτη – μέλη της Ένωσης είναι αναγκαία, όπως η διακρατική συνεργασία, η ανταλλαγή πληροφοριών και τεχνογνωσίας μεταξύ τους, καθώς και η στελέχωση των αρμόδιων κρατικών οργάνων για την πρόληψη και καταστολή του ηλεκτρονικού εγκλήματος με εξειδικευμένο έμπειρο προσωπικό. Εξίσου αναγκαία, όμως, είναι και η ενσωμάτωσή της στην εθνική νομοθεσία κάθε κράτους – μέλους όσον το δυνατόν συντομότερα!

Συνοψίζοντας, είναι γεγονός πως το ηλεκτρονικό έγκλημα σήμερα παγκοσμίως βρίσκεται σε πλήρη άνθηση. Ωστόσο, με τις σωστές νομοθετικές ρυθμίσεις, με ενημέρωση και εγρήγορση, καθώς και με την κατάλληλη τεχνογνωσία μπορεί να αντιμετωπιστεί, όπως συνέβαινε με κάθε νέο εγκληματικό φαινόμενο που έκανε την εμφάνισή του εδώ και χρόνια.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία

Δαλακούρας Θ., «Ηλεκτρονικό Έγκλημα», Ουσιαστικές και Δικονομικές Όψεις, 2η Έκδοση, Νομική Βιβλιοθήκη, 2023.

Δαλακούρας Θ., Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2019.

Δαλακούρας Θ., Ο νέος Κώδικας Ποινικής Δικονομίας – Μία πρώτη ερμηνευτικής προσέγγιση του Ν. 4620/2019, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, 2019

Παπαδαμάκης, Α. «Τα περιουσιακά εγκλήματα – Άρθρα 385-406Α ΠΚ», Β' Έκδοση, Εκδόσεις Σάκκουλα, 2016.

Παπαδαμάκης, Α. «Ποινική Δικονομία», Β' Έκδοση, Εκδόσεις Σάκκουλα, 7η έκδοση, 2017

Μυλωνόπουλος Χ., «Ειδικό μέρος, Ποινικό δίκαιο, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας» Π.Ν. ΣΑΚΚΟΥΛΑΣ, Αθήνα 2006

Μυλωνόπουλος, Χ. «Ποινικό Δίκαιο, Ειδικό μέρος», 4η Έκδοση, Νομική Βιβλιοθήκη, 2021.

Ζέκος, Ι. «Διαδίκτυο, Η/Υ & Τηλεπικοινωνίες στο ελληνικό δίκαιο», Εκδόσεις Σάκκουλα, 2017.

Βασιλάκη Ειρ., «Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών», ΑΝΤ. ΣΑΚΚΟΥΛΑΣ, 1993

<u>Νομικά Περιοδικά - Αρθρογραφία</u>

Ι Αγγελή, «Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», ΠοινΔικ 2001

Βασιλάκη, Ε. Τα φαινόμενα Phishing, Pharming και η ποινική τους αξιολόγηση, ΠοινΧρον, ΝΖ/2007, σελ. 860-863.

Κουράκης, Ν., Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ, 6/2001, σελ. 2567-2595.

Νούσκαλης, Γ., Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ). Το παρελθόν και το μέλλον του Άρθρου 386 Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαική Ένωση, ΠοινΔικ, 2/2003, σελ. 178-190.

Σαββίδης, Ν. Απάτη και Απάτη με Υπολογιστή στον ΝΠΚ, όπως τροποποιήθηκε με τον Ν. 4855/2021. Συγχρόνως, η προσέγγιση ορισμένων σύγχρονων μορφών ηλεκτρονικού εγκλήματος, υπό του Πρίσμα του Ουσιαστικού Ποινικού Δικαίου, ΠοινΔικ, 10/2022, σελ. 1321-1333.

Φαραντούρης, Ν. Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο – Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, ΠοινΔικ, 2/2003, σελ. 191-196.

Καϊάφα-Γκμπάντι, Μ., Ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρον 2011, σελ. 489 επ.

Αιτιολογική Έκθεση της Σύμβασης για το Κυβερνοέγκλημα

Αιτιολογική Έκθεση του Νέου Ποινικού Κώδικα

Οδηγία 2013/40/ΕΕ, Εισ. Σκέψη 1

Οδηγία (ΕΕ) 2019/713, Εισ. Σκέψη 15

Οδηγία NIS2 (2022/2555/ΕΕ)

Απάτη με υπολογιστή, ΣυμβΠλημΘεσ 828/2022, ΠοινΔικ, 8-9/2022, σελ. 1228-1233.

Απάτη με υπολογιστή, ΤρΕφΚακΑθ 4689/2018, ΠοινΔικ, 7/2020, σελ. 731-733.

ΣΥΝΗΓΟΡΟΣ, Δίκαιο & Νέες Τεχνολογίες, Επιθέσεις κατά συστημάτων πληροφοριών, Η νέα οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου, Ιωάννης Δ. Ιγγλεζάκης.

ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

www.hellenicparliament.gr

https://lawdb.intrasoftnet.com/ (ΝΟΜΟΣ)

https://www.areiospagos.gr/nomologia/apofaseis.asp

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0

https://ziamparas.gr/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1/%CE%B1%CF%80%CE%AC%CF%84%CE%B7-%CE%BC%CE%B5-%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE/

https://www.kathimerini.gr/society/561995401/ilektronikes-apates-oi-deka-pio-sychnes-pagides-odigos-amynas/

https://e-nomika.gr/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1/

https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/n-1805-1988.html

https://www.esdi.gr/nex/images/stories/pdf/epimorfosi/2019/zarkazi-aspoin_2019.pdf

https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-4947-2022

Κυβερνοασφάλεια: οι νέοι κανόνες της ΕΕ για την καταπολέμηση του ηλεκτρονικού εγκλήματος | Νομικά Νέα | Lawspot

https://digital-strategy.ec.europa.eu/el/policies/nis2-directive

https://www.coe.int/en/web/conventions/full-list/- conventions/treaty/185/signatures

ΝΟΜΟΛΟΓΙΑ

ΑΠ 131/2013

ΑΠ 1087/2019

ΑΠ 908/2020

ΑΠ 190/2009

ΑΠ 573/2009

ΑΠ 66/2007

Υπ’ αριθμ. 28/2010 Βούλευμα Συμβ.Εφετ.Θεσσαλ

Υπ’ αριθμ. 828/2022 Βούλευμα ΣυμβΠλημΘεσ

Υπ’ αριθμ. 68/2014 απόφαση του Εφετ.Δυτ.Στερεάς Ελλάδας

Υπ’ αριθ. 4689/2018 απόφαση του Τριμ.Εφετ,Κακ,Αθηνών