ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

«ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΠΑΤΕΣ – ΜΟΡΦΕΣ ΕΚΔΗΛΩΣΗΣ ΤΗΣ ΕΓΚΛΗΜΑΤΙΚΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΥΠΟ ΤΟ ΠΡΙΣΜΑ ΤΩΝ ΑΡΘΡΩΝ 386 & 386^{Α} ΠΚ»

Διπλωματική Εργασία

Του

Μιχαήλ Ι. Καραδήμου

Θεσσαλονίκη, Μάρτιος 2024

«ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΠΑΤΕΣ – ΜΟΡΦΕΣ ΕΚΔΗΛΩΣΗΣ ΤΗΣ ΕΓΚΛΗΜΑΤΙΚΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΥΠΟ ΤΟ ΠΡΙΣΜΑ ΤΩΝ ΑΡΘΡΩΝ 386 & 386^{Α} ΠΚ»

Μιχαήλ Ι. Καραδήμος

Απόφοιτος Νομικής Σχολής του Δημοκρίτειου Πανεπιστημίου Θράκης, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Θεοχάρης Ι. Δαλακούρας

Μιχαήλ Ι. Καραδήμος

Περίληψη

Στην εποχή της πληροφορίας και της ραγδαίως αναπτυσσόμενης τεχνολογίας, όλοι οι τομείς της ζωής των ανθρώπων υφίστανται κρίσιμες μεταβολές. Μια εξ αυτών εντοπίζεται στο πλαίσιο της οικονομικής ζωής, η οποία αναπότρεπτα έχει καθοριστεί από τις νεότερες εξελίξεις, με βασική συνέπεια την σταδιακή μετάβαση από την «συμβατική» οικονομία, στην «ψηφιακή». Πλην όμως, πέρα από τις προφανείς θετικές συνέπειες αυτής, που ανάγονται ασφαλώς και μεταξύ άλλων, στην επιτάχυνση και τη διευκόλυνση της καθημερινότητας των μετεχόντων στις οικονομικής φύσης συναλλαγές, αναδεικνύεται ένα ευρύτατο φάσμα, νεοπαγών και κυρίως αγνώστων μέχρι πρότινος κινδύνων, τόσο για το κοινό όσο και για τις νομοθετικές και διωκτικές αρχές, με την παράλληλη διεύρυνση του πρόσφορου, για εγκληματικές και δη απατηλές, συμπεριφορές, πεδίου δράσης. Επί τη βάσει αυτής της διαπίστωσης, δια της παρούσας εργασίας επιχειρείται η συστηματική και ερμηνευτική προσέγγιση, με συγκεκριμένες αναφορές στην περιπτωσιολογία των μορφών εκδήλωσης της εγκληματικής συμπεριφοράς, εν συνόλω της απάτη στη σύγχρονη ψηφιακή εποχή, ως κατά περίπτωση τυποποιείται, στις διατάξεις περί απάτης μέσω υπολογιστή του άρθρ. 386 ΠΚ, άλλως σε εκείνες, περί απάτης με υπολογιστή του άρθρ. 386^{Α} ΠΚ.

Λέξεις Κλειδιά: ποινικό δίκαιο, δίκαιο πληροφορικής, ηλεκτρονικό έγκλημα, ηλεκτρονικό – οικονομικό έγκλημα, κυβερνοέγκλημα, κυβερνοχώρος, κυβερνοασφάλεια, εγκληματολογικά χαρακτηριστικά απατηλές προσβολές, απατηλά μέσα, κοινωνική μηχανική, επέμβαση, δεδομένα συστήματος

Abstract

In the age of information and rapidly developing technology, all areas of people's lives are undergoing critical changes. One of them is to be found in the context of economic life, which has inevitably been determined by recent developments, with the main consequence being the gradual transition from the 'conventional' economy to the 'digital' one. However, apart from the obvious positive consequences of this, which are certainly due, among other things, to the acceleration and facilitation of the everyday life of those involved in financial transactions, a wide range of new and, above all, previously unknown risks emerge, both for the public and for the legislative and law enforcement authorities, with the parallel expansion of the scope for criminal and especially fraudulent behaviour. On the basis of this finding, the present study attempts a systematic and interpretative approach, with specific references to the case study of the forms of manifestation of criminal behaviour, in general fraud in the modern digital era, as it is sometimes standardized in the provisions on computer fraud of Article 386 PC, or else in those on computer fraud of Article 386A PC.

Keywords: criminal law, computer law, e-crime/ cyber-crime, e - economic crime, cyberspace, cybersecurity, forensic characteristics, fraudulent attacks, fraudulent means, social engineering, interference, system data

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ 9

2. ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΈΝΝΟΙΑ ΚΑΙ ΔΙΑΚΡΙΣΕΙΣ 10

3. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΚΑΙ ΤΩΝ ΔΡΑΣΤΩΝ ΤΟΥ 17

3.1. Τα χαρακτηριστικα του ηλεκτρονικου εγκληματος 17

3.2. Τα χαρακτηριστικα του δραστη ηλεκτρονικου εγκληματος 20

4. ΕΥΡΩΠΑΪΚΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ ΚΑΤΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ 23

5. Η ΑΠΑΤΗ ΜΕΣΩ ΥΠΟΛΟΓΙΣΤΗ (386 ΠΚ) 28

5.1. Το προστατευομενο εννομο αγαθο 28

5.2. Αντικειμενικη υποσταση 29

5.3. Υποκειμενικη υποσταση 35

5.4. Ποινικη κυρωση της απατης μεσω υπολογιστη - Έμπρακτη μετανοια ... 36

5.5. Ζητηματα αποπειρας, συμμετοχης και συρροων στην απατη μεσω υπολογιστη 38

6. Η ΑΠΑΤΗ ΜΕ ΥΠΟΛΟΓΙΣΤΗ (386^{Α} ΠΚ) 42

6.1. Η νομοθετικη εξελιξη της διαταξης του αρθρου 386^{Α} ΠΚ και το προστατευομενο εννομο αγαθο 42

6.2. Αντικειμενικη υποσταση 45

6.2.1. Μη ορθή διαμόρφωση προγράμματος υπολογιστή 46

6.2.2. Χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος .. 48

6.2.3. Χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης ταυτότητας 49

6.2.4. Χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας 50

6.2.5. Χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων 51

6.2.6. Κατασκευή, διάθεση ή κατοχή προγράμματος ή συστήματος υπολογιστή που προορίζεται για τη διάπραξη του εγκλήματος του άρθρ. 386^{A} παρ. 1 ΠΚ *53*

6.3. Η βλαβη 54

6.4. Υποκειμενικη υποσταση 55

6.5. Ποινικη κυρωση της απατης με υπολογιστη 55

6.6. Συγκριση της απατης μεσω υπολογιστη (386 ΠΚ) και της απατης με υπολογιστη (386^{A} ΠΚ) 56

7. ΟΙ ΣΥΓΧΡΟΝΕΣ ΜΕΘΟΔΟΙ ΚΑΙ ΜΕΣΑ ΕΞΑΠΑΤΗΣΗΣ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ 58

7.1. Ηλεκτρονικες και διαδικτυακες απατες με χρηση κοινωνικης μηχανικης χειραγωγησης – «Ο ασταθμητος ανθρωπινος παραγοντας» 58

7.2. Συνηθεις τεχνικες εξαπατησης με χρηση κοινωνικης μηχανικης 61

7.3. Η ηλεκτρονικη τραπεζικη απατη (μεσω internet banking) και τα φαινομενα «phishing» και «pharming» ως μορφες ηλεκτρονικης απατης 65

7.4. Οι «ρομαντικες απατες» 71

7.5. Η τελεση ηλεκτρονικης απατης με εργαλειο τα κρυπτονομισματα 75

8. ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΑΡΑΤΗΡΗΣΕΙΣ 78

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΡΟΓΡΑΦΙΑ 81

1. Εισαγωγή

Είναι γεγονός ότι ο 20ός αιώνας σήμανε παγκοσμίως την έναρξη μιας νέας εποχής αλματώδους τεχνολογικής ανάπτυξης και προόδου, με θεαματικά αποτελέσματα σε όλους τους τομείς και τις εκφάνσεις της κοινωνικής και οικονομικής ζωής του ανθρώπου. Τούτη η ραγδαία εξέλιξη της τεχνολογίας οδήγησε προοδευτικά στη σύγχρονη ψηφιακή επανάσταση, στην οποία πρωταγωνιστικό ρόλο κατέχει η διαρκώς αυξανόμενη χρήση των ηλεκτρονικών υπολογιστών, καθώς και η ανακάλυψη και ευρεία διάδοση του Διαδικτύου. Αμφότερα τα τεχνολογικά επιτεύγματα αυτά σύντομα κατέκλεισαν τον κόσμο, μπήκαν σε κάθε σπίτι και επιχείρηση, διαμορφώνοντας νέες συνθήκες καθημερινής ζωής, εργασίας, διασκέδασης, επικοινωνίας, αλλά και νέα πεδία ανάπτυξης κοινωνικών συμπεριφορών.

Σήμερα πλέον μπορεί να γίνει λόγος για «ψηφιοποίηση» των συναλλαγών, των κρατικών δομών και υπηρεσιών, της επιχειρηματικής διάρθρωσης και άλλων, ακόμα και απλών, δραστηριοτήτων του ατόμου. Σε αυτό το πλαίσιο, είναι προφανές ότι μια τέτοια σειρά ριζικών αλλαγών της κοινωνικής πραγματικότητας γρήγορα δημιούργησε την επιτακτική ανάγκη για εκσυγχρονισμό και αναδιάρθρωση των δικαιικών συστημάτων σε πολλαπλά επίπεδα και επιμέρους κλάδους τους. Οι ηλεκτρονικοί υπολογιστές και η λειτουργία τους, αλλά και ο νέος, άγνωστος και πολύπτυχος κόσμος του Διαδικτύου άνοιξαν την «κερκόπορτα» των νομοθετικών μεταρρυθμίσεων οι οποίες ανοικοδόμησαν έναν ολόκληρο καινούριο νομικό κλάδο βασισμένο στην ιχνηλάτηση, συστηματοποίηση και ρύθμιση του συνόλου των νέων παρεχόμενων δυνατοτήτων και των σχέσεων που δημιουργούνταν επί αυτών και έχρηζαν νομοθετικής παρεμβάσεως.

Ωστόσο, παράλληλα με τη θετική εξελικτική πορεία των τεχνολογικών μέσων και της επίδρασής τους, οι ηλεκτρονικοί υπολογιστές και το Διαδίκτυο κατασκεύασαν ένα νέο πεδίο για την ανάπτυξη αρνητικής δράσεως – παραβατικότητας, τόσο με τη δημιουργία καινούριων, άγνωστων έως τότε, αδικημάτων, όσο και με την εξεύρεση καινούριων μεθόδων τέλεσης των ήδη υπαρχόντων. Βάσει του δεδομένου αυτού, ο

ποινικός νομοθέτης εξωθήθηκε στην επανεκτίμηση των άξιων ποινικής προστασίας αγαθών, αναγνωρίζοντας νέα έννομα αγαθά, αλλά και στην πρόβλεψη νέων εγκληματικών τύπων, οι οποίοι αντιστοιχούν είτε σε εν όλω καινούρια αδικήματα, είτε σε εμπλουτισμό των ήδη προβλεφθέντων διατάξεων, ο οποίος συνεπάγεται την επαύξηση της παρεχόμενης προστασίας.

Με την παρούσα εργασία θα επιχειρηθεί η ανάδειξη των μορφών που λαμβάνει η απάτη στη σύγχρονη ψηφιακή εποχή, υπό το πρίσμα των διατάξεων περί απάτης μέσω υπολογιστή του άρθρ. 386 ΠΚ και περί απάτης με υπολογιστή του άρθρ. 386^{Α} ΠΚ.

Ειδικότερα, στο δεύτερο κεφάλαιο της παρούσας θα αναπτυχθεί η έννοια και οι διακρίσεις του ηλεκτρονικού εγκλήματος, καθώς και η κατηγοριοποίησή του για λόγους συστηματοποίησης. Εν συνεχεία, στο τρίτο κεφάλαιο θα αναλυθούν τα χαρακτηρολογικά στοιχεία ηλεκτρονικού εγκλήματος, αλλά και του εγκληματολογικό προφίλ των δραστών του, ενώ στο τέταρτο κεφάλαιο θα παρατεθούν βασικές νομοθετικές πρωτοβουλίες που έχουν ληφθεί σε ευρωπαϊκό επίπεδο για την πρόληψη και καταπολέμηση της ηλεκτρονικής απάτης. Ακολούθως, στο πέμπτο και έκτο κεφάλαιο θα αναλυθούν οι ενδιαφέρουσες για την παρούσα διατάξεις των άρθρων 386 ΠΚ περί απάτης και ειδικά μέσω υπολογιστή και 386^{Α} ΠΚ περί απάτης με υπολογιστή, ενώ το έβδομο κεφάλαιο θα αφιερωθεί στην περιπτωσιολογική αναφορά των μορφών που λαμβάνει σήμερα η σύγχρονη ηλεκτρονική απάτη και τα διάφορα δογματικά ζητήματα τα οποία εγείρονται.

2. Ηλεκτρονικό έγκλημα: Έννοια και διακρίσεις

Για λόγους συστηματοποίησης, χρήσιμο είναι να επιχειρήσουμε να ορίσουμε το Ηλεκτρονικό Έγκλημα ως κατηγορία εγκληματικότητας, να προσδιορίσουμε τα χαρακτηριστικά τα οποία τη συνθέτουν, καθώς και να το διακρίνουμε από συγγενείς έννοιες.

Με την ταχύτατη εξέλιξη των τεχνολογιών και των μέσων τους, αυξήθηκαν ταυτόχρονα και οι ευκαιρίες για την εκμετάλλευσή τους προς εξυπηρέτηση

εγκληματικών σκοπών. Είναι γεγονός ότι τις τελευταίες δεκαετίες έχει σημειωθεί αλματώδης πρόοδος όσον αφορά την εμφάνιση και διάδοση νέων τεχνολογιών: εξάπλωση Διαδικτύου, πρόσβαση μέσω περισσότερων συσκευών π.χ. ηλεκτρονικών υπολογιστών, laptop, smartphones, tablets, smart watches, κ.ά., νέα μέσα πληρωμών, όπως πιστωτικές / χρεωστικές / προπληρωμένες κάρτες, ψηφιακά πορτοφόλια, ψηφιακή μεταφορά χρημάτων, κ.λπ.. Το σύνολο των νέων αυτών τεχνολογιών και η διαρκής ανάπτυξή τους, τόσο ως προς το εύρος των δυνατοτήτων τους όσο και ως προς την ποικιλία και την προσβασιμότητα σε αυτές αφενός έχουν παράσχει και νέα μέσα, ήτοι νέους τρόπους, για την τέλεση «συμβατικών» εγκλημάτων (π.χ. της «κοινής» απάτης του άρ. 386 ΠΚ), αφετέρου δε έχουν δημιουργήσει νέα εγκλήματα με αυτοτελείς νομοτυπικές μορφές (π.χ. της απάτης με ηλεκτρονικό υπολογιστή του άρ. 386^{Α} ΠΚ). Ως εκ τούτου, λόγω της πληθώρας των ηλεκτρονικών εγκλημάτων, έχουν αναπτυχθεί και αντίστοιχα πολυάριθμοι ορισμοί για το ηλεκτρονικό έγκλημα[1].

Αρχικά, αυτό που οφείλουμε να παρατηρήσουμε είναι ότι έχουν χρησιμοποιηθεί κατά διαστήματα διαφορετικοί όροι προκειμένου να περιγράψουν τις νέες αυτές εγκληματικές συμπεριφορές. Ως δικαιολογητική βάση του φαινομένου αυτού, ήτοι της ύπαρξης περισσότερων όρων για την περιγραφή της ίδιας κατηγορίας εγκλημάτων, είναι κυρίως η έλλειψη πρόβλεψης κάποιου κοινώς αναγνωρισμένου ορισμού, ο οποίος θα μπορούσε να έχει δοθεί είτε από νομοθετικά κείμενα της ελληνικής είτε της διεθνούς ή ευρωπαϊκής έννομης τάξης.

Εν πρώτοις, είχε γίνει λόγος για τριμερή διάκριση ανάμεσα σε έγκλημα ηλεκτρονικού υπολογιστή (computer crime), έγκλημα που σχετίζεται με ηλεκτρονικό υπολογιστή (computer related crime) και έγκλημα μέσω υπολογιστή (crime by computer)[2]. Εν συνεχεία, και με την ευρεία εξάπλωση του Διαδικτύου, εμφανίστηκε ο όρος έγκλημα του δικτύου, ενώ συναντά κανείς και ονομασίες όπως κυβερνοέγκλημα, ψηφιακό έγκλημα ή έγκλημα της υψηλής τεχνολογίας[3]. Σημαντική δε προσπάθεια για

[1] Βλ. Clough J., Principles of cybercrime, Cambridge University Press, 2010, σελ. 9.

[2] Βλ. Βουλή των Κοινοτήτων (House of Commons) Καναδά, "Report of the sub-committee on Computer crime", Final Report, Ιούνιος 1983, σελ. 12.

[3] Βλ. Sheridan M., The future of net crime now: part 1 – threats and challenges, 2004, σελ. vi.

τον ορισμό του ηλεκτρονικού εγκλήματος έγινε το 1994 από τους Forester και Morrison, οι οποίοι χρησιμοποίησαν τον όρο «computer crime» και το προσδιόρισαν ως «εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης αυτής»[4].

Κατά μία άποψη της θεωρίας[5], κανένας από τους ανωτέρω αναφερόμενους όρους δεν καταφέρνει να καλύψει πλήρως όλο το εύρος των περιπτώσεων που περιλαμβάνει το ηλεκτρονικό έγκλημα, διότι, αναπόδραστα κάποιο στοιχείο μένει εκτός του ορισμού. Για παράδειγμα, όσες ορολογίες εστιάζουν στο στοιχείο του υπολογιστή, φαίνεται να παραγνωρίζουν τον παράγοντα του Διαδικτύου. Αντίθετα, άλλες όπως το κυβερνοέγκλημα ή το εικονικό έγκλημα φαίνεται να σχετίζονται αποκλειστικά με το Διαδίκτυο. Από την άλλη, είναι σαφές ότι ο όρος «ηλεκτρονικό» έγκλημα, αλλά και «υψηλής τεχνολογίας» ή «εικονικό» έγκλημα είναι ιδιαίτερα ευρείς και στην πραγματικότητα λειτουργούν ως επί το πλείστον ως όροι – ομπρέλα, κυρίως με σκοπό να αναδείξουν την τεχνολογία ως μείζον χαρακτηριστικό των εν λόγω εγκλημάτων.

Κατά μια άλλη άποψη[6], τα ηλεκτρονικά εγκλήματα διακρίνονται σε δύο κατηγορίες και ειδικότερα α) σε εκείνα που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ, η εισβολή σε ηλεκτρονικά αρχεία, ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών β) σε εκείνα που υποστηρίζονται από Η/Υ και στα οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα μαύρου χρήματος που γίνονται ηλεκτρονικά.

Σύμφωνα με μία τρίτη άποψη[7], τα ηλεκτρονικά εγκλήματα κατανέμονται σε τέσσερις κατηγορίες. Η πρώτη περιλαμβάνει κοινά εγκλήματα τα οποία τελούνται με

[4] Βλ. Forester T. / Morrison P., Computer Ethics: Cautionary tales and ethical dilemmas in computing, second edition, The MIT Press, Cambridge, Massachusetts, London, England, 1994.

[5] Βλ. Clough J., Principles of cybercrime, 2010, Cambridge University Press, ό.π.

[6] Βλ. Barrett N., Digital Crime: Policing the Cybernation, Kogan Page Ltd, 1997.

[7] Βλ. Pipkin D., Halting the Hacker: a practical guide to computer security, Prentice Hall Professional Technical Reference, 2002.

χρήση Η/Υ, λ.χ. απάτη, κλοπή στοιχείων ιδιοκτητών πιστωτικών καρτών και κλοπή ηλεκτρονικής ταυτότητας. Στη δεύτερη κατηγορία υπάγονται τα ειδικά εγκλήματα των Η/Υ, ήτοι την επίθεση της άρνησης παροχής υπηρεσιών, την άρνηση πρόσβασης σε πληροφορίες και τη διασπορά καταστρεπτικών ιών, στην τρίτη κατηγορία ανήκουν τα αδικήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία και καταστροφή πληροφοριών που έχουν κλαπεί και τέλος, η τέταρτη κατηγορία περιλαμβάνει τα εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου.

Στο ελληνικό Ποινικό Δίκαιο και Εγκληματολογία συναντά κανείς του όρους ηλεκτρονικό έγκλημα, διαδικτυακό έγκλημα, έγκλημα του κυβερνοχώρου, έννοιες οι οποίες, ωστόσο, εμφανίζουν ορισμένες διαφοροποιήσεις[8]. Ειδικά ως προς το διαδικτυακό έγκλημα ή έγκλημα του κυβερνοχώρου, θα πρέπει να αναφερθεί ότι η ειδοποιός διαφορά τους σε σχέση με τον όρο του ηλεκτρονικού εγκλήματος είναι ότι τελούνται αναγκαίως μέσω του Διαδικτύου (π.χ. κυβερνοεπιθέσεις με τη χρήση κακόβουλων προγραμμάτων ransomware). Στο ανωτέρω πλαίσιο, και βάσει του ορισμού που έχει δώσει η ελληνική υπηρεσία Δίωξης 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». Αξίζει να σημειωθεί ότι ο όρος «ηλεκτρονικό έγκλημα» είναι αυτός που επικράτησε έναντι των υπολοίπων στην ελληνική έννομη τάξη, κάτι το οποίο μάλλον θα πρέπει να αποδοθεί στο ότι αυτήν την ορολογία επέλεξε ο Έλληνας ποινικός νομοθέτης στον ν. 1805/1988[9].

Αντίθετα, όταν χρησιμοποιείται ο όρος Ηλεκτρονικό Έγκλημα, υποδηλώνεται, ως ήδη αναφέρθηκε, η τέλεσή του με τη χρήση ηλεκτρονικού υπολογιστή, δηλαδή όταν ο υπολογιστής είναι το μέσο για την τέλεση της αξιόποινης πράξης, χωρίς όμως να είναι αναγκαία η σύνδεσή του στο Διαδίκτυο. Όταν το έγκλημα τελείται στον χώρο του Διαδικτύου, οπότε ο ηλεκτρονικός υπολογιστής ή άλλη ηλεκτρονική συσκευή (π.χ.

[8] Βλ. Δαλακούρας Θ, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2019, σελ. 3.

[9] Βλ. Νόμος 1805/1988, Εκσυγχρονισμός τον θεσμού τον ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων, ΦΕΚ 199/Α/31-8-1988.

κινητό τηλέφωνο) είναι ο υλικός φορέας διαμέσου του οποίου πραγματοποιείται απλώς η σύνδεση, τότε γίνεται λόγος για έγκλημα του κυβερνοχώρου ή διαδικτυακό έγκλημα[10].

Βάσει, επομένως, των παραπάνω, προκύπτει με σαφήνεια ότι το κυβερνοέγκλημα είναι υποκατηγορία του ηλεκτρονικού, καθώς απαιτεί αφενός μεν την ύπαρξη υπολογιστή, αφετέρου την ύπαρξη σύνδεσης στο Διαδίκτυο. Επιχειρώντας να διακρίνουμε περισσότερες υποκατηγορίες του ηλεκτρονικού εγκλήματος, το οποίο αποτελεί την έννοια γένους, λαμβάνοντας υπόψη και τις ανωτέρω αναφερόμενες αναλύσεις, θα μπορούσαμε να εντοπίσουμε τις κάτωθι[11]:

α) Εγκλήματα που τελούνται τόσο εντός όσο και εκτός Διαδικτύου, δηλαδή εγκλήματα στα οποία η τέλεση διά Διαδικτύου αποτελεί απλώς έναν επιπλέον τρόπο διάπραξης (π.χ. συκοφαντική δυσφήμιση), οπότε γίνεται λόγος για «internet related crime»[12].

β) Εγκλήματα που τελούνται αποκλειστικά σε περιβάλλον ηλεκτρονικών υπολογιστών χωρίς την χρήση Διαδικτύου (computer crimes), δηλαδή εγκλήματα των οποίων το αντικείμενο προσβολής ή ο υλικός φορέας της πράξης είναι ο ηλεκτρονικός υπολογιστής. Στον ελληνικό ΠΚ τέτοια εγκλήματα συνιστούν αυτά των άρθρων 370Β και 370Γ ΠΚ[13].

---

[10] Βλ. σχετικά και την από 22-05-2007 ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Επιτροπή των Περιφερειών «Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο», Βρυξέλλες, COM(2007) 267, σελ. 2, όπου τα εγκλήματα κυβερνοχώρου ορίστηκαν *ως «αξιόποινες πράξεις που διαπράττονται με χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή εναντίον αυτών των δικτύων και συστημάτων».*

[11] Ι. Αγγελής, Διαδίκτυο (Internet) και ποινικό δίκαιο, ΠοινΧρ 2000, 675 επ., Μ. Καιάφα – Γκμπάντι, Ποινικό Δίκαιο και Καταχρήσεις της Πληροφορικής, Αρμ. 2007, 1062

[12] Βλ. Δαλακούρας Θ, Ηλεκτρονικό Έγκλημα, ό.π., σελ. 4.

[13] Βλ. Δαλακούρας Θ, Ηλεκτρονικό Έγκλημα, ό.π., σελ. 4.

γ) Εγκλήματα των οποίων το περιβάλλον του Διαδικτύου αποτελεί μέρος της αντικειμενικής τους υπόστασης, δηλαδή εγκλήματα τα οποία δίχως την πρόσβαση στο Διαδίκτυο δεν θα ήταν αξιόποινες συμπεριφορές, με χαρακτηριστικότερο παράδειγμα την παραγωγή ή διάδοση υλικού παιδικής πορνογραφίας κατά το άρθρο 348^{A} ΠΚ[14].

Οι παραπάνω υπό β) και γ) κατηγορίες εγκλημάτων αποτελούν νέο είδος εγκληματικότητας, που αναπτύχθηκε με την εμφάνιση των νέων τεχνολογιών υπολογιστών και Διαδικτύου, καθώς δεν είναι εφικτή η τέλεσή τους χωρίς τα δύο αυτά στοιχεία, δηλαδή δεν μπορούν να διαπραχθούν εκτός του περιβάλλοντος του Διαδικτύου ή του ηλεκτρονικού υπολογιστή[15].

Περαιτέρω, οφείλουμε να λάβουμε υπόψη και τον τρόπο συστηματοποίησης των ηλεκτρονικών εγκλημάτων που υιοθετήθηκε με τη Σύμβαση της Βουδαπέστης «για το έγκλημα στον Κυβερνοχώρο» του 2001[16]. Συγκεκριμένα, η Σύμβαση αναγνωρίζει τέσσερεις και όχι τρεις κατηγορίες αδικημάτων:

α) Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών (Τίτλος 1 της Σύμβασης, στον οποίο περιλαμβάνονται: παράνομη πρόσβαση, υποκλοπή, παρεμβολές σε δεδομένα, παρεμβολές σε συστήματα και κακή χρήση συσκευών)

---

[14] Βλ. Αγγελής Ι., «Διαδίκτυο (Internet) και ποινικό δίκαιο / Έγκλημα στον Κυβερνοχώρο (Cybercrime – Internet crime)», ΠοινΧρ Ν/2000, σελ. 676 επ., Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ΠοινΔικ 2001, σελ. 1218 επ. και Θ. Δαλακούρας, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, σε Δαλακούρα (επιμ.), Ηλεκτρονικό Έγκλημα, 2019, ο.π.

[15] Βλ. Βλαχόπουλος Κ., Ηλεκτρονικό Έγκλημα: Μορφές, Πρόληψη, Αντιμετώπιση, εκδ. Νομική Βιβλιοθήκη, 2007, σελ. 11.

[16] Βλ. το πλήρες κείμενο της Σύμβασης διαθέσιμο στα ελληνικά στην ιστοσελίδα https://www.lawspot.gr/sites/default/files/annex_files/other/sumvasi_voudapestis_gr.pdf (τελευταία επίσκεψη 10-11-2023).

β) Εγκλήματα σχετικά με υπολογιστές (Τίτλος 2 της Σύμβασης, στον οποίο περιλαμβάνονται: πλαστογραφία σχετική με υπολογιστές, απάτη σχετική με υπολογιστές).

γ) Εγκλήματα σχετικά με το περιεχόμενο – περιλαμβάνει αδικήματα όπως πορνογραφία, λόγος μίσους, κ.τ.λ. (Τίτλος 3 της Σύμβασης, στον οποίο περιλαμβάνεται η παιδική πορνογραφία).

δ) Εγκλήματα σχετικά με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας, προσωπικών δεδομένων και συγγενικών αδικημάτων (Τίτλος 4 της Σύμβασης).

Τέλος, ειδική αναφορά αξίζει να γίνει στη διάκριση των ηλεκτρονικών εγκλημάτων στην οποία προβαίνει η Καϊάφα[17], με κριτήριο τη χρήση των συστημάτων πληροφοριών ως μέσων τέλεσης ως κάτωθι:

α) Αξιόποινες πράξεις που αποτελούν *aliud* σε σχέση με τα βασικά τυποποιούμενα στον ΠΚ εγκλήματα, δηλαδή πράξεις οι οποίες δεν παραλλάσσονται ως προς κάποιο στοιχείο από το βασικό (οπότε θα γινόταν λόγος για διακεκριμένη ή προνομιούχα παραλλαγή), αλλά διαφοροποιούνται τόσο από το βασικό, ώστε πλέον πρόκειται για άλλη πράξη (*ιδιώνυμο έγκλημα*[18]). Εάν, λοιπόν, καταργηθεί η διάταξη που τυποποιεί αυτές τις πράξεις, τότε οι εν λόγω συμπεριφορές καθίστανται μη αξιόποινες και δεν τιμωρούνται με τη διάταξη του βασικού. Χαρακτηριστική περίπτωση αποτελεί η ενδιαφέρουσα και για την παρούσα διάταξη του άρθρου 386^{A} ΠΚ περί απάτης με υπολογιστή.

β) Εγκλήματα για την τέλεση των οποίων χρησιμοποιείται σύστημα πληροφοριών, ωστόσο η προσβολή πηγάζει από τα δεδομένα του συστήματος (content-related crimes). Παραδείγματα τέτοιων εγκλημάτων είναι, όπως αναφέρεται και παραπάνω βάσει της κατηγοριοποίησης της Σύμβασης της Βουδαπέστης, τα εγκλήματα

[17] Βλ. Καϊάφα - Γκμπάντι Μ., «Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής», Αρμ 2007, σελ. 1061 επ.

[18] Βλ. Μανωλεδάκης Ι., Ποινικό Δίκαιο: άρθρα 1 – 50 ΠΚ, εκδ. Α.Ν. Σάκκουλα, 2005, σελ. 387-389.

των άρθρων 348^{A} και 348Γ ΠΚ περί παιδικής πορνογραφίας, όπως και τα εγκλήματα των άρθρων 1, 2 και 3 ν. 927/1979 περί εκδήλωσης ρατσιστικού λόγου.

γ) Εγκλήματα τα οποία τελούνται με τη χρήση συστήματος πληροφοριών, όμως το αποτέλεσμα της πράξης στρέφεται κατά δεδομένων. Τα δεδομένα αυτά συνιστούν τα ίδια έννομο αγαθό ή συνδέονται οργανικά με κάποιο έννομο αγαθό, όπως συμβαίνει στην περίπτωση εγκλημάτων κατά της πνευματικής ιδιοκτησίας.

3. Χαρακτηριστικά του ηλεκτρονικού εγκλήματος και των δραστών του

3.1. Τα χαρακτηριστικά του ηλεκτρονικού εγκλήματος

Το Ηλεκτρονικό έγκλημα φέρει ορισμένα ιδιαίτερα χαρακτηριστικά τα οποία το καθιστούν ιδιαίτερα δημοφιλές είδος εγκληματικότητας, ιδίως με τη διάδοση του Διαδικτύου.

Το βασικότερο και προφανέστερο όλων είναι, βεβαίως, η *ταχύτητα*. Ο δράστης του εκάστοτε ηλεκτρονικού εγκλήματος μπορεί να το τελέσει άμεσα, εντός ελάχιστων λεπτών, και μάλιστα από την άνεση του υπολογιστή του (*φορητότητα*), ευρισκόμενος οπουδήποτε σε σχέση με την τοποθεσία όπου βρίσκεται το θύμα. Το Διαδίκτυο μηδενίζει τις αποστάσεις, καθιστώντας δυνατή την πραγματοποίηση π.χ. επιθέσεων σε υπολογιστικά συστήματα επιχειρήσεων σε οποιοδήποτε σημείο του κόσμου [19] (*παγκοσμιότητα δικτύου*).

Επιπρόσθετο στοιχείο – κλειδί της δημοτικότητας των ηλεκτρονικών εγκλημάτων και είναι η *ανωνυμία* που παρέχουν στον δράστη τους. Ο τελευταίος βρίσκεται πίσω από την οθόνη του υπολογιστή του, μπορεί να χρησιμοποιήσει ανώνυμους περιηγητές για την πλοήγησή του στο Διαδίκτυο, ειδικά κατασκευασμένα προγράμματα που εγγυώνται την

[19] Βλ. Βλαχόπουλος Κ., Ηλεκτρονικό Έγκλημα / Μορφές – Πρόληψη – Αντιμετώπιση, ό.π., σελ. 11 επ..

ανωνυμία του χρήστη τους και τη μη ανιχνευσιμότητα των κινήσεών του εντός του δικτύου, ή μπορεί ακόμα και να χρησιμοποιήσει ψευδώνυμα για να καλύψει την ταυτότητά του[20]. Όλες αυτές οι μέθοδοι κατατείνουν σε έναν σκοπό, την παρεμπόδισης σύνδεσης του συγκεκριμένου προσώπου με το έγκλημα και το αποτέλεσμά του, το οποίο πολλές φορές γίνεται αντιληπτό από το θύμα αρκετά αργότερα από τον πραγματικό χρόνο επέλευσής του.

Ακόμα, θα πρέπει να γίνει λόγος για τη *διαθεσιμότητα των μέσων*. Οι ηλεκτρονικοί υπολογιστές είναι πλέον ένα καθημερινό εργαλείο στα χέρια εκατομμυρίων ανθρώπων, ενώ και η πρόσβαση στο Διαδίκτυο αποτελεί σήμερα μια πολύ απλή διαδικασία. Τα παραπάνω στοιχεία συντείνουν στην πιθανή μετουσίωση των μέσων αυτών σε πρόσθετα «όπλα», ευχερώς προσβάσιμα, στη «φαρέτρα» των (κυβερνο)-εγκληματιών, οι οποίοι δεν απαιτείται να έχουν εξειδικευμένες γνώσεις πληροφορικής για να τελέσουν αρκετά αδικήματα αυτού του είδους (π.χ. εξύβριση μέσω διαδικτύου). Ταυτόχρονα, διευκολύνεται τυχόν επικοινωνία πολλών δραστών που λειτουργούν συντονισμένα, σε πραγματικά χρόνο, χωρίς μετακίνηση, εύκολα και ανέξοδα, μέσω ομάδων συζητήσεων (newsgroups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις[21].

Τέλος, έχει βαρύνουσα σημασία να υπογραμμιστεί ότι ένα άλλο, σοβαρό «πλεονέκτημα» των ηλεκτρονικών εγκλημάτων είναι ότι έχει βρει μάλλον απροετοίμαστα τα νομοπαραγωγικά όργανα, με αποτέλεσμα, έχοντας ως σημείο αναφοράς το ελληνικό ποινικό σύστημα, η ισχύουσα νομοθεσία να αποδεικνύεται σε αρκετά σημεία μάλλον ανεπαρκής, τόσο σε επίπεδο ουσιαστικού όσο και δικονομικού δικαίου. Σε αυτό φυσικά συμβάλλουν οι ιδιαιτερότητες στην ταυτότητα των αδικημάτων αυτών, οι οποίες δημιουργούν και δογματικά ζητήματα, όπως ο διαχρονικός προβληματισμός γύρω από τον προσδιορισμό του τόπου τέλεσης των ηλεκτρονικών εγκλημάτων. Έχει λεχθεί κατά καιρούς, ότι η εν λόγω μορφή, είναι έγκλημα

[20] Βλ. και το από 20-10-2010 σχετικό ερώτημα προς το Ευρωπαϊκό Κοινοβούλιο διαθέσιμο στα ελληνικά στην ιστοσελίδα https://www.europarl.europa.eu/doceo/document/E-7-2010-8610_EL.html (τελευταία επίσκεψη 16-11-2023).

[21] Βλ. Κιούπης Δ., Ποινικό Δίκαιο και Internet, εκδ. Αντ. Ν. Σάκκουλα, 1999, σελ. 27 επ.

αποστάσεως, «χωρίς πατρίδα», αφού οι προπαρασκευαστικές πράξεις, η εξωτερίκευση της συμπεριφοράς, ο εντοπισμός της τοποθεσίας του δράστη και τα αποτελέσματα του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους, με αποτέλεσμα να υπάγονται συνήθως, με βάση την αρχή της εδαφικότητας ταυτοχρόνως σε πολλές δικαιοδοσίες[22]. Ο διασυνοριακός χαρακτήρας του κυβερνοεγκλήματος απαιτεί κατά κανόνα διεθνή δράση αλλά και στενή, συνεχή και αποτελεσματική διακρατική συνεργασία των διωκτικών αρχών[23].

Δυσχέρειες υπάρχουν και στον προσδιορισμό του χρόνου τέλεσης, καθώς το θύμα συχνά καθυστερεί να αντιληφθεί ότι έλαβε χώρα κάποια επίθεση εις βάρος του[24]. Εκτός όμως από τα θέματα αυτά, δυσκολίες εντοπίζονται και στο κομμάτι της απόδειξης, καθώς τα αρμόδια όργανα των διωκτικών αρχών θα πρέπει να διαθέτουν ειδικές γνώσεις και να εκπαιδεύονται συνεχώς, ώστε να συμπορεύονται με τις διαρκείς τεχνολογικές

[22] Βλ. Κιούπης Δ σε Δαλακούρας Θ (επιμ.), Ηλεκτρονικό Έγκλημα, ό.π., σελ 42 επ. και Κιούπης Δ., Ο τόπος τέλεσης του διαδικτυακού εγκλήματος και η απροσδόκητη διεύρυνσης της έννοιας της ημεδαπής (άρθρο 5 παρ. 3 ΠΚ), ΠοινΧρ 2014, σελ. 561 επ.

[23] Βλ. Δημόπουλος Χ., Εγκληματολογική, Αστυνομική & Δικανική Ανακριτική, εκδ. Νομική βιβλιοθήκη, 2021, σελ. 308. Παπαθανασίου, Α. / Γέρμανος, Γ. Εξέλιξη και ανάπτυξη νέων μορφών ψηφιακής εγκληματικότητας στον κυβερνοχώρο σε εποχές Κρίσης,, διαθέσιμο στον ιστότοπο http://crime-in-crisis.com/%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7-%CE%BA%CE%B1%CE%B9-%CE%B1%CE%BD%CE%AC%CF%80%CF%84%CF%85%CE%BE%CE%B7-%CE%BD%CE%AD%CF%89%CE%BD-%CE%BC%CE%BF%CF%81%CF%86%CF%8E%CE%BD-%CF%88%CE%B7%CF%86%CE%B9/ (τελευταία επίσκεψη 09-11-2023).

[24] Βλ. Βλαχόπουλος Κ., Ηλεκτρονικό Έγκλημα / Μορφές – Πρόληψη – Αντιμετώπιση, ό.π..

εξελίξεις, ενώ σε αρκετές περιπτώσεις είναι αναγκαία η συνεργασία των διωκτικών αρχών περισσότερων κρατών, γεγονός που επιβραδύνει τις ερευνητικές διαδικασίες[25].

Επιπλέον, η καταγραφή της ηλεκτρονικής εγκληματικότητας είναι βέβαιο ότι δεν αποδίδει τις πραγματικές τιμές της, από την στιγμή που συγκριτικά μικρός αριθμός των εγκλημάτων αυτών καταγγέλλονται και ακόμα μικρότερος οδηγείται ενώπιον της ποινικής δικαιοσύνης. Εν τούτοις, βάσει των διαθέσιμων στοιχείων, η συντριπτική πλειοψηφία των αξιόποινων συμπεριφορών που αναφέρονται και διώκονται από τις αρχές, καταλαμβάνεται από εγκλήματα όπως, α) η πορνογραφία ανηλίκων, β) οι απάτες μέσω διαδικτύου (π.χ. με πιστωτικές κάρτες), γ) οι κακόβουλες εισβολές σε δίκτυο (hacking), δ) η διαδικτυακή πειρατεία, ε) η διακίνηση πειρατείας λογισμικού, στ) η διακίνηση ναρκωτικών ουσιών και όπλων, ζ) η σωματεμπορία, η) η υφαρπαγή προσωπικών δεδομένων, θ) ο εκφοβισμός μέσω διαδικτύου cyberbulling - η κυβερνοτρομοκρατία, και ι) το ι) το κακόβουλο λογισμικό[26].

3.2. Τα χαρακτηριστικά του δράστη ηλεκτρονικού εγκλήματος

Προκειμένου να εξετάσουμε τα επιμέρους χαρακτηριστικά των δραστών του ηλεκτρονικού εγκλήματος, ιδιαιτέρως κρίσιμη παρουσιάζεται εν προκειμένω, η επιρροή των «εγκληματικών ευκαιριών»[27]. Σύμφωνα με την πάγια επιστημονική αντίληψη, η τέλεση μιας αξιόποινης πράξης, είναι η συνιστώσα τριών παραμέτρων: α) του κινήτρου, β) των διαθέσιμων μέσων και γ) της εξεύρεσης των κατάλληλων συνθηκών, δηλαδή της ευκαιρίας που στην πράξη δύναται να λάβει την μορφή *ελκυστικού στόχου, κενού*

[25] Βλ. Δημόπουλος Χ., Εγκληματολογική, Αστυνομική & Δικανική Ανακριτική, ό.π., σελ. 308, Παπαθανασίου, Α. / Γέρμανος, Γ., «Εξέλιξη και ανάπτυξη νέων μορφών ψηφιακής εγκληματικότητας στον κυβερνοχώρο σε εποχές Κρίσης», ό.π.

[26] Βλ. Βλαχόπουλος Κ., Ηλεκτρονικό Έγκλημα / Μορφές – Πρόληψη – Αντιμετώπιση, ό.π., σελ. 55.

[27] Κουράκης Ν., Το οικονομικό έγκλημα στην Ελλάδα σήμερα, ΠοινΔικ, 6/2000, σελ. 644 - 654

ασφαλείας, εγγύτητας, αξίας, ευκολίας απόκτησης, μεταφερσιμότητας[28]. Μεταξύ άλλων, θεωρείται ότι ένας από τους κυριότερους λόγους που ωθούν κάποιον στην τέλεσης ενός εγκλήματος με τα χαρακτηριστικά του ηλεκτρονικού, είναι η αποκόμιση οικονομικού οφέλους, εις βάρος της περιουσίας του θύματος ή τρίτου, ακόμη και αν αυτός δεν είναι καθορισμένος εξ αρχής. Επομένως, αναφερόμαστε σε εγκληματίες του λευκού κολλάρου[29], οι οποίοι εκμεταλλεύονται για την πραγμάτωση των εγκληματικών τους ενεργειών, την πρόσβαση τους σε υπολογιστικά, συνήθως εταιρικά – εμπορικά ή κυβερνητικά συστήματα, την οποία διατηρούν, ενόψει της θέσεως εργασίας τους, της ιδιότητός του και των ανατιθέμενων σε αυτούς καθηκόντων[30].

Εντούτοις, μόνο η συνδρομή του κινήτρου για την τέλεση ενός ηλεκτρονικού εγκλήματος δεν αρκεί για να πεις κανείς με βεβαιότητα ότι το άτομο θα διαπράξει την αξιόποινη πράξη, με δεδομένο ότι ιδιαίτερα κρίσιμος είναι και ο ρόλος της πραγματικής δυνατότητας, μιας αντικειμενικά ελκυστικής στο μάτι του δράστη - που φέρει ούτως ή άλλως το κίνητρο - περίστασης. Εξάλλου, η ευρηματικότητα των δραστών του ηλεκτρονικού εγκλήματος και η ίδια η ανάπτυξη της τεχνολογίας και του Διαδικτύου, με την πλειάδα των υφιστάμενων δυνατοτήτων, γεννά με βεβαιότητα τέτοιες ευκαιρίες, σε σημείο να μην είναι καν εφικτή σε πραγματικό χρόνο η συνολική χαρτογράφηση του φαινομένου και των μορφών που δύναται να λάβει.

---

[28] Βλ. Πιτσελά Α., Η εγκληματολογική προσέγγιση του οικονομικού εγκλήματος, Εκδ. Σάκκουλα Αθήνα-Θεσσαλονίκη, 2010, σελ. 74 και Συλικός Γ., Τα Οικονομικά Εγκλήματα στην σύγχρονη πραγματικότητα, Τα Οικονομικά Εγκλήματα στην σύγχρονη πραγματικότητα, ΤΝΠ QUALEX ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ, 1-2/2021, σελ. 110 – 118

[29] *«White-collar crime»* είναι το έγκλημα με οικονομικά κίνητρα, που δεν είναι βίαιο και διαπράττεται από άτομα σε επιχειρήσεις, τις ίδιες τις επιχειρήσεις και κυβερνητικούς παράγοντες. Για πρώτη φορά, κατονομάστηκαν με αυτόν τον όρο από τον κοινωνιολόγο Έντουιν Σάδερλαντ το 1939, ενώ του δόθηκε παράλληλα ο ορισμός, ως *«ένα εγκλήματος που διαπράττεται από ένα άτομο ευυπόληπτο και υψηλού κοινωνικού κύρους κατά τη διάρκεια της απασχόλησής του»*, βλ. Sutherland E. H., White Collar Crime – The Uncut Version, New Haven & London, Yale University Press, 1983.

[30] Βλ. Hamerton C, "White-Collar Cybercrime: Evaluating the Redefinition of a Criminological Artifact", Journal of Law and Criminal Justice December 2020, Vol. 8, No. 2, pp. 67-79.

Αναφορικά με την «αντικειμενικά ελκυστική» περίσταση, οφείλουμε να επισημάνουμε ότι ο παράγοντας αυτός, συνδυάζεται με την εκάστοτε υποκειμενική, εν πολλοίς ενδιάθετη ψυχολογική αλλά και αντιληπτική κατάσταση και προετοιμασία του δράστη, όταν του παρουσιάζεται η συγκεκριμένη, κακώς εννοούμενη, ευκαιρία να παρανομήσει εις βάρος της περιουσίας τρίτων, χρησιμοποιώντας ηλεκτρονικά μέσα. Σύμφωνα με τους Grabosky και Walkley[31], το ήδη υπάρχον για πολλούς κίνητρο έχει επιταθεί ένεκα της διεύρυνσης του πεδίου δράσης και των δυνατοτήτων, ειδικά σε προχωρημένους χρήστες του Διαδικτύου και των εφαρμογών της πληροφορικής. Περαιτέρω, ο ολοένα αυξανόμενος ανταγωνισμός για το κέρδος, έχει οδηγήσει ακόμη και στην «κανονικοποίηση» και στην εκλογίκευση των αθέμιτων και σε πολλές περιπτώσεις παράνομων επιχειρηματικών πρακτικών των δραστών ηλεκτρονικών εγκλημάτων, με σκοπό κυρίως να δικαιολογηθούν, έστω σε κάποιο βαθμό.

Πλην όμως, αξίζει να αναφερθεί για την πληρέστερη αποτύπωση των θεωριών περί καταλληλόλητας μιας ευκαιρίας και του ήδη προϋπάρχοντος κινήτρου, η άποψη του Cook[32], προκειμένου να αντιληφθούμε την αλληλεπίδραση των δύο αυτών παραμέτρων. Ειδικότερα, λαμβάνοντας υπόψη τη συνήθη τάση των δραστών να επιδιώκουν τον μέγιστο δυνατό κέρδος με το μικρότερο δυνατό ρίσκο, προκύπτει ότι είναι εξίσου κρίσιμο κριτήριο η επιρροή της αντίληψης της διακινδύνευσης, της πιθανότητας σύλληψης και επιβολής, βαριάς ή μη, ποινής καθώς επίσης και της εγγύτητας και της ευαλωτότητας ενός στόχου, που δεν φέρει τις απαιτούμενες αποτρεπτικές ασφαλιστικές δικλείδες. Πλην όμως, για να συμβεί αυτό, η εν λόγω αντίληψη οφείλει να διέρχεται μιας ορθολογικής προσέγγισης, την οποία άλλωστε επιδεικνύουν, στην συντριπτική του πλειονότητα, οι συνήθως, πλήρως οργανωμένοι δράστες του οικονομικού εγκλήματος.

[31] Βλ. Grabosky P. / Walkley S., “Computer Crime and White-Collar Crime”, Springer, 2007, σελ. 364-375.

[32] Βλ. Cook P. “The Demand and Supply of Criminal Opportunities”. Crime and Justice vol. 7, University of Chicago Press, 1986, σελ. 1-27.

4. Ευρωπαϊκό θεσμικό πλαίσιο κατά του ηλεκτρονικού εγκλήματος

Σε επίπεδο Ευρωπαϊκής Ένωσης, η ιδέα για τη δημιουργία ενιαίου θεσμικού πλαισίου αντιμετώπισης της ηλεκτρονικής εγκληματικότητας (και, αναπόδραστα, της κυβερνοεγκληματικότητας ως ειδικότερη εκδήλωσή της) και με ποινικού δικαίου διατάξεις ξεκίνησε να υλοποιείται μόνο περί τα τέλη της δεκαετίας του 1990.

Ειδικότερα, την 13.09.1989 εκδόθηκε από το Συμβούλιο της Ευρώπης η σύσταση R (89) 9 για το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή, η οποία αποτέλεσε μια σύντομη προτροπή προς τα κράτη *«…να λαμβάνουν υπόψη την έκθεση για το έγκλημα που σχετίζεται με υπολογιστές που εκπονήθηκε από την Ευρωπαϊκή Επιτροπή για τα Προβλήματα του Εγκλήματος κατά την επανεξέταση ή την έγκριση νέας νομοθεσίας»* και *«…να υποβάλουν έκθεση στον Γενικό Γραμματέα του Συμβουλίου της Ευρώπης κατά τη διάρκεια του 1993 σχετικά με τις εξελίξεις στη νομοθεσία τους, τη δικαστική πρακτική και τις εμπειρίες από τη διεθνή νομική συνεργασία όσον αφορά το έγκλημα που σχετίζεται με υπολογιστές»*. Σχετικώς εκδόθηκε και η από 11.09.1995 σύσταση με αριθμό R (95) σχετικά με τ ζητήματα εφαρμογής ανακριτικών πράξεων επί συστημάτων πληροφορικής και ιδίως της κατάσχεσης και έρευνας ηλεκτρονικών υπολογιστών και των περιεχόμενων σε αυτούς δεδομένων.

Νομοθέτημα – σταθμός για την αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί η υπ' αριθ. 185 Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα, η οποία υπεγράφη την 23η Νοεμβρίου 2001 στη Βουδαπέστη, τέθηκε σε εφαρμογή το 2004 και η οποία ήδη αναφέρθηκε ανωτέρω στην παρούσα[33].

Η Σύμβαση χωρίζεται σε τρία βασικά κεφάλαια[34]:

[33] Βλ. Βαγενά Ε. Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεργκλήματος, ΔίΜΕΕ 2017, σελ. 28 επ.

[34] Υπάρχει και τέταρτο κεφάλαιο, το οποίο αφορά τελικές διατάξεις και ρήτρες.

α) Το πρώτο κεφάλαιο περιέχει ορισμούς για τα συστήματα υπολογιστών, τα δεδομένα υπολογιστών, τους παρόχους υπηρεσιών και τα δεδομένα κίνησης.

β) Το δεύτερο κεφάλαιο ασχολείται με τα μέτρα που πρέπει να ληφθούν σε εθνικό επίπεδο και χωρίζεται σε δύο τμήματα: η πρώτη ενότητα αφορά το ουσιαστικό δίκαιο και ασχολείται με την τυποποίηση ηλεκτρονικών εγκλημάτων και ειδικότερα την παράνομη πρόσβαση, παράνομη υποκλοπή, παρεμβολή στα δεδομένα, παρεμβολή στο σύστημα, κατάχρηση συσκευών, πλαστογραφία που σχετίζεται με τον υπολογιστή, απάτη που σχετίζεται με υπολογιστή, αδικήματα που σχετίζονται με την παιδική πορνογραφία και αδικήματα που σχετίζονται με τα πνευματικά δικαιώματα.

Ιδίως όσον αφορά την απάτη που σχετίζεται με υπολογιστή, η Σύμβαση προβλέπει υποχρέωση των συμβαλλόμενων κρατών να ορίσουν ως ποινικό αδίκημα « η εκ προθέσεως και χωρίς δικαίωμα, πρόκληση απώλειας περιουσίας σε άλλο πρόσωπο με: α) οποιαδήποτε εισαγωγή, μεταβολή, διαγραφή ή απόκρυψη δεδομένων υπολογιστή, β) οποιαδήποτε παρέμβαση στη λειτουργία συστήματος υπολογιστή, με δόλια ή ανέντιμη πρόθεση να αποκομίσει, χωρίς δικαίωμα, οικονομικό όφελος για τον εαυτό του ή για άλλο πρόσωπο».

Η δεύτερη ενότητα του δεύτερου κεφαλαίου ασχολείται με διαδικαστικά θέματα και θέματα επιβολής του νόμου, συμπεριλαμβανομένης της διατήρησης των αποθηκευμένων δεδομένων, διατήρηση και μερική αποκάλυψη δεδομένων κίνησης, εντολή παραγωγής, έρευνα και κατάσχεση δεδομένων υπολογιστή, συλλογή δεδομένων κίνησης σε πραγματικό χρόνο και υποκλοπή δεδομένων περιεχομένου, ενώ το τρίτο κεφάλαιο περιέχει διατάξεις σχετικά με την αμοιβαία δικαστική συνδρομή και τους κανόνες έκδοσης.

Η Σύμβαση της Βουδαπέστης περιλαμβάνει επίσης δύο Πρόσθετα Πρωτόκολλα. Το πρώτο υπεγράφη την 28.01.2003 σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών, ενώ το δεύτερο αφορά την ενισχυμένη συνεργασία και την αποκάλυψη ηλεκτρονικών αποδεικτικών στοιχείων και έχει ανοίξει προς υπογραφή από τα μέρη από την 12η Μαΐου 2022. Μέχρι σήμερα έχει υπογραφεί από 43 συμβαλλόμενα μέρη, μέλη της Ε.Ε. και μη, ωστόσο έχει κυρωθεί μόνο από την Ιαπωνία και τη Σερβία. Όσον αφορά

την Ελλάδα, καθυστέρησε ιδιαίτερα να κυρώσει με τυπικό νόμο τη Σύμβαση της Βουδαπέστης εκδίδοντας τον ν. 4411/2016, ενώ είχε υπογράψει τη Σύμβαση ήδη από 28-01-2003.

Φυσικά, εκτός από την ανωτέρω Σύμβαση υπάρχουν πλείστα νομοθετικά κείμενα τα οποία απαρτίζουν και συμπληρώνουν το θεσμικό πλαίσιο περί αντιμετώπισης του ηλεκτρονικού εγκλήματος. Ενδεικτικά αναφερόμαστε στα εξής:

- Η απόφαση-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου (28.05.2001) «για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών», η οποία έχει αντικατασταθεί από την Οδηγία 2019/713. Η τελευταία αυτή Οδηγία έχει ενσωματωθεί στην ελληνική έννομη τάξη με τον ν. 4947/2022. Αξίζει να αναφερθεί ότι η ενσωμάτωση της Οδηγίας αυτής έγινε με τροποποιήσεις επί των ισχυουσών διατάξεων του ΠΚ και όχι δια της θέσπισης ενός ειδικού ποινικού νόμου για λόγους συστηματικής ενότητας των σχετικών κανόνων δικαίου, καθόσον η Οδηγία προβλέπει αδικήματα σχετικά με τα μέσα πληρωμής πλην των μετρητών, που αφορούν σε έννομα αγαθά, τα οποία ήδη προστατεύονται στον ΠΚ[35].
- Η Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (07.03.2002) «σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους». η εν λόγω Οδηγία έχει τροποποιηθεί δυνάμει της Οδηγίας 2009/140/ΕΚ και έχει ενσωματωθεί στην ελληνική έννομη τάξη με τον ν. 4070/2012. Με τον ίδιο νόμο ενσωματώθηκαν και οι Οδηγίες 2002/20/ΕΚ «σχετικά με την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών», 2002/21/ΕΚ «για το κανονιστικό πλαίσιο για τα δίκτυα και τις υπηρεσίες ηλεκτρονικών επικοινωνιών» και

[35] Βλ. Κεφάλαια 9 και 23 του ΠΚ. Ειδικά ως προς τις ενδιαφέρουσες για την παρούσα διατάξεις, με τον ν. 4947/2022 τροποποιήθηκαν οι παρ. 1 και 2 άρθρου 386Α ΠΚ περί απάτης με υπολογιστή, για την ενσωμάτωση των άρθρων 3, 6 και παρ. 4 και 5 άρθρου 9 της Οδηγίας.

2002/22/ΕΚ «με την καθολική υπηρεσία και τα δικαιώματα των χρηστών αναφορικά με δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών»[36].

- Η Οδηγία 2002/58/ΕΚ (12.07.2002) «σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής»[37], ενσωματούμενη στην Ελλάδα με τον ν. 3471/2006.
- Η Οδηγία 2009/110/ΕΚ (16.09.2009) «για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος, την τροποποίηση των οδηγιών 2005/60/ΕΚ και 2006/48/ΕΚ και την κατάργηση της οδηγίας 2000/46/ΕΚ», η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον ν. 4021/2011, όπως ισχύει κατόπιν τροποποίησής του από τον ν. 4537/2018.
- Η Οδηγία 2013/40/ΕΕ «για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου», ενσωματώθηκε στην ελληνική έννομη τάξη με το ν. 4411/2016, μαζί με τη Σύμβαση της Βουδαπέστης.
- Η Οδηγία 2016/680/ΕΕ (27.04.2016) «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου». Η Ελλάδα έχει ενσωματώσει την Οδηγία αυτή με τον ν. 4624/2019.
- Ο Κανονισμός 679/2016/ΕΕ (27.04.2016) «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Με τον ν. 4624/2019 προβλέφθηκε το σύνολο των ρυθμίσεων που εισήχθησαν με τον Κανονισμό στην ελληνική έννομη τάξη. Σημειώνεται ότι το ισχύον νομοθετικό πλαίσιο για την προστασία

[36] Η εν λόγω Οδηγία τροποποιήθηκε δυνάμει της Οδηγίας 2009/136/ΕΚ.

[37] Η εν λόγω Οδηγία τροποποιήθηκε δυνάμει της Οδηγίας 2009/136/ΕΚ.

των προσωπικών δεδομένων αντικατέστησε την Οδηγία 95/46/ΕΚ, η οποία είχε ενσωματωθεί με τον ν. 2472/1997.

- Η Οδηγία 2016/1148/ΕΕ (06.07.2016) «σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση», η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον ν. 4577/2018. Σήμερα η εν λόγω Οδηγία έχει αντικατασταθεί από την Οδηγία 2022/2555/ΕΕ, η οποία θα πρέπει να ενσωματωθεί από τις εθνικές έννομες τάξεις των κρατών – μελών έως την 17η Οκτωβρίου 2024[38].
- Ο Κανονισμός 2019/881/ΕΕ (17.04.2019) «σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια)».

Από τα παραπάνω προκύπτει η πρόθεση της Ένωσης να οργανώσει ένα αποτελεσματικό πλαίσιο, όχι μόνο για την καταστολή της ηλεκτρονικής εγκληματικότητας, αλλά κυρίως για την πρόληψή της, δίνοντας έμφαση στη λήψη μέτρων κυβερνοασφάλειας. Όσον αφορά τις ποινικές διατάξεις, η Ε.Ε. έχει τη δυνατότητα να συνεχίσει να νομοθετεί μέσω Οδηγιών, οι οποίες δεν έχουν άμεση εφαρμογή αλλά απαιτείται η ενσωμάτωσή τους. Ωστόσο, σε άλλα πεδία παρατηρείται όλο και συχνότερα το φαινόμενο να νομοθετεί μέσω Κανονισμών, με άμεση ισχύ για τα κράτη μέλη, καθώς το κλειδί για την επίτευξη της στοχοθεσίας της Ένωσης είναι η πλήρης εναρμόνιση των επιμέρους εθνικών εννόμων τάξεων[39].

---

[38] Βλ. Ι. Ιγγλεζάκη, Δίκαιο Πληροφορικής, Δ΄ Έκδοση, 2021, Νομική Βιβλιοθήκη, σελ. 403 επ. (653) και https://www.europol.europa.eu/ec3.

[39] Βλ. σχετικά και τη νέα προσωρινή συμφωνία για τη θέσπιση νομοθεσίας σχετικά με τις απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία, η οποία θα έχει τη μορφή Κανονισμού, Επίσημη ιστοσελίδα του Συμβουλίου της ΕΕ, "Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products", 30-11-2023, διαθέσιμο στον ιστότοπο https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-

5. Η απάτη μέσω υπολογιστή (386 ΠΚ)

5.1. Το προστατευόμενο έννομο αγαθό

Το έγκλημα της απάτης τυποποιείται στο άρθρο 386 του ΠΚ [40], το οποίο εντάσσεται στο 23ο Κεφάλαιο για τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας. Ως έγκλημα κατά της περιουσίας θεωρείται και η «κοινή» απάτη του 386 ΠΚ, η οποία μπορεί να διαπραχθεί και *μέσω* υπολογιστή, ήτοι ο υπολογιστής εδώ αποτελεί έναν από τους πλείονες τρόπους για την παραπλάνηση του ατόμου.

Η περιουσία ως έννομο αγαθό περιλαμβάνει όλα τα αγαθά ενός προσώπου που έχουν οικονομική αξία και μπορούν να αποτιμηθούν σε χρήμα, εφόσον δεν αποδοκιμάζονται από την έννομη τάξη, σύμφωνα με τη κρατούσα στους θεωρητικούς νομική-οικονομική θεωρία[41], ενώ η νομολογία τείνει να υιοθετεί την αμιγή οικονομική

---

products/#:~:text=Main%20objectives%20of%20the%20new,legislation%20in%20EU%20member%20states. (τελευταία επίσκεψη 01-12-2023).

[40] Όπως αυτό τροποποιήθηκε με τον ν. 4619/2019: *«1. Όποιος με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή. 2. Αν η απάτη στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημιά που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά είκοσι (20) έτη»*.

[41] Βλ. Μυλωνόπουλος Χ., Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, εκδ. Π.Ν. Σάκκουλας Δίκαιο και Οικονομία, 2006, σελ. 439, Παπαδαμάκης Α. Τα περιουσιακά εγκλήματα, άρθρα 385 – 405 ΠΚ. Εκδόσεις Σάκκουλα, δ΄ έκδοση 2022, σελ. 78 επ., Παύλου Σ., Μπέκας Ι., Αποστολίδου Α., Ποινικό Δίκαιο – Ειδικό Μέρος, τ. Α΄: Τα εγκλήματα κατά των

θεωρία, βάσει της οποίας δεν ενδιαφέρει η προέλευση των αποτιμητών σε χρήμα αγαθών, δηλαδή δεν ενδιαφέρει εάν επιδοκιμάζονται ή αποδοκιμάζονται από το δίκαιο για να κριθούν προστατευτέα[42].

Ιδίως όταν πρόκειται για απάτη μέσω υπολογιστή, συνήθως η βλαπτόμενη περιουσία συνίσταται σε χρηματικά ποσά τραπεζικών λογαριασμών, τα οποία μεταφέρονται μέσω των παρεχόμενων και ευρέως γνωστών υπηρεσιών e-banking, κατόπιν εξαπάτησης του δικαιούχου του λογαριασμού και χρήστη των ηλεκτρονικών τραπεζικών υπηρεσιών[43].

5.2. Αντικειμενική υπόσταση

Σύμφωνα με τη βασική μορφή του εγκλήματος, απάτη τελεί *«όποιος με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος»*.

περιουσιακών αγαθών (άρθρα 372 επ., 385 επ. ΠΚ), της ζωής (άρθρα 299 επ. ΠΚ) και της σωματικής ακεραιότητας (άρθρα 308 επ. ΠΚ), Εκδόσεις Π.Ν. Σάκκουλα, 2020, σελ. 362

[42] Βλ. ενδ. ΑΠ 404/2019, ΤΝΠ ΝΟΜΟΣ

[43] Βλ. Φιλόπουλος Π., Ποινική Προστασία Απορρήτου, εκδ. Α.Ν. Σάκκουλας, 2015, σελ. 42 επ., όπου γίνεται λόγος για τις περιπτώσεις απάτης με ειδικότερη ονομασία «phising» και «pharming». Σε αυτές τις πράξεις, ο δράστης αποστέλλει απατηλά email και προωθεί πλαστές ιστοσελίδες ως επίσημες – έγκυρες, προκειμένου να παραπλανηθεί ο αποδέκτης του email / επισκέπτης της ιστοσελίδας και να καταχωρίσει κάποιον κωδικό αριθμό, π.χ. web banking, αριθμό τραπεζικού λογαριασμού, χρεωστικής ή πιστωτικής κάρτας ή ακόμα και του κινητού τηλεφώνου, ο οποίος πολλές φορές είναι συνδεδεμένος με τις υπηρεσίες internet banking του χρήστη.

Από τα παραπάνω προκύπτει καταρχάς ότι το έγκλημα της απάτης είναι κοινό («όποιος»), ήτοι δράστης μπορεί να είναι οποιοσδήποτε χωρίς να φέρει συγκεκριμένη ιδιότητα. Επιπλέον, είναι υπαλλακτικώς μικτό έγκλημα[44], καθώς οι περισσότεροι τρόποι τέλεσης (εξαπάτησης) μπορούν να εναλλαχθούν ή να λάβουν χώρα διαδοχικά επί της ίδιας μονάδας εννόμου αγαθού / υλικό αντικείμενο της αξιόποινης πράξης, χωρίς να θεωρείται ότι ο δράστης τελεί περισσότερα εγκλήματα[45].

Επιπλέον, είναι έγκλημα βλάβης, η οποία θα πρέπει να επέλθει σε ξένη περιουσία, με την έννοια που δόθηκε ανωτέρω. Ενώ η αξιόποινη συμπεριφορά είναι ίδια σε όλες τις περιπτώσεις απάτης, δηλαδή η βλάβη είναι το αποτέλεσμα της περιουσιακής διάθεσης στην οποία προέβη το θύμα κατόπιν της παραπλάνησης ή εξαπάτησής του από τον δράστη, στην απάτη μέσω υπολογιστή ο υπολογιστής αποτελεί το μέσο για την επίτευξη της παραπλάνησης ή της εξαπάτησης. Περαιτέρω, ο υπολογιστής μπορεί να βρίσκεται εκτός σύνδεσης ή μπορεί να συνδέεται στο Διαδίκτυο, οπότε θα γίνεται λόγος για κυβερνοέγκλημα.

Ως βλάβη, τώρα, της περιουσίας του θύματος νοείται η μείωσή της, δηλαδή η επί έλαττον διαφορά μεταξύ της χρηματικής αξίας την οποία είχε πριν την περιουσιακή διάθεση που προκλήθηκε με την απατηλή συμπεριφορά και εκείνης που απέμεινε μετά από αυτήν[46]. Από την παραπάνω ερμηνεία της έννοιας της βλάβης προκύπτει ότι κρίσιμη

---

[44] Βλ. ενδ. την πάγια νομολογία του Ανώτατου Ακυρωτικού ΟλΑΠ 1/2020, ΤΝΠ ΝΟΜΟΣ, ΟλΑΠ 3/2019, ΑΠ 196/2015, ΑΠ 1634/2008, ΑΠ 587/2006, ΤΝΠ ΝΟΜΟΣ (πρβλ. Μπέκα Ι. Ποινικό Δίκαιο – Ειδικό Μέρος, τ. Α΄: Τα εγκλήματα κατά των περιουσιακών αγαθών (άρθρα 372 επ., 385 επ. ΠΚ), της ζωής (άρθρα 299 επ. ΠΚ) και της σωματικής ακεραιότητας (άρθρα 308 επ. ΠΚ), Εκδόσεις Π.Ν. Σάκκουλα, 2020, σελ. 362, αναφορικά με την έννοια του «γνήσιου πολύτροπου εγκλήματος», σελ. 364, υποσημ. 54).

[45] Υπό την προϋπόθεση φυσικά ότι δεν μεσολαβεί ειρήνευση του αγαθού, και πάλι υπό την επιφύλαξη εφαρμογής του άρ. 98 ΠΚ περί κατ' εξακολούθηση τέλεση

[46] Βλ. Καμπέρου Ε. σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), εκδ. Νομικής Βιβλιοθήκη, 2020, σελ. 3078, Μπέκας Ι. ο.π. σελ. 365, υποσημ.45

είναι η λογιστική διαφορά[47] ανάμεσα στο πριν και το μετά την περιουσιακή διάθεση. Έτσι, προϋποτίθεται μικρότερης αξίας αντιπαροχή σε σχέση με την παροχή στην οποία προέβη ή αντιπαροχή η οποία στον συγκεκριμένο πρόσωπο (εξαπατώμενο) είναι άχρηστη, σύμφωνα με τις ειδικότερες περιστάσεις που συντρέχουν και τον αφορούν. Αξίζει, μάλιστα, να αναφερθεί ότι στην έννοια της περιουσίας εντάσσονται και οι προσδοκίες κέρδους, εφόσον κατά τη συνήθη πορεία των πραγμάτων καθίσταται βάσιμη, πιθανή και αναμενόμενη η αύξηση της περιουσίας του παραπλανηθέντος / εξαπατηθέντος[48]. Σε κάθε περίπτωση ως περιουσιακή βλάβη νοούνται και τα δικαστικά έξοδα και εν γένει ο ένδικος αγώνας στον οποίο πρέπει να προχωρήσει το θύμα προκειμένου να ικανοποιήσει την απαίτησή του, οπότε θεωρείται βλάβη και η απειλή ή διακινδύνευση της περιουσίας, εφόσον επιφέρει μείωση της ενεστώσας αξίας της[49].

Επιπροσθέτως, χρήσιμο είναι να διευκρινιστεί ότι για την τέλεση της απάτης δεν είναι υποχρεωτικό το πρόσωπο που προβαίνει σε περιουσιακή διάθεση κατόπιν εξαπάτησης / παραπλάνησης να είναι και αυτό του οποίου η περιουσία βλάφθηκε από τη διάθεση αυτή. Τούτο έχει την έννοια ότι αποδέκτης της απατηλής / παραπλανητικής συμπεριφοράς μπορεί να προβαίνει σε περιουσιακή διάθεση η οποία δεν αφορά τη δική του περιουσία, αλλά αυτήν κάποιου τρίτου προσώπου, εφόσον έχει την σχετική εκ του νόμου δυνατότητα να διαθέτει την ξένη περιουσία[50] (τριγωνική απάτη). Πλην όμως, η πράξη εξαπάτησης πρέπει υποχρεωτικά να απευθύνεται και να ενεργεί στο νοητικό – στη

[47] Βλ. Καμπέρου Ε. σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π., Φράγκος Κ., Online κατ' άρθρο ερμηνεία του Ποινικού Κώδικα, εκδ. Α.Ν. Σάκκουλα, 2020, διαθέσιμο σε: https://www.sakkoulas-online.gr/ .

[48] Βλ. νομολογιακά παραδείγματα ΑΠ 5/2001, ΠοινΧρ 2001, σελ. 591 επ., ΣυμβΑΠ 771/1975, ΠοινΧρ 1976, σελ. 155 και Παπαδαμάκης Α., Πρόσφατες νομολογιακές διακυμάσεις και ερμηνευτικές εκτροπές στα εγκλήματα της απάτης και της απιστίας, Ποινική Δικαιοσύνη, Τεύχος 4-5, Νομική Βιβλιοθήκη, 2012

[49] Βλ. ενδ. ΑΠ 2060/2019, ΑΠ 790/2019, ΑΠ 1089/2015 ΤΝΠ ΝΟΜΟΣ.

[50] Βλ. ενδ. ΑΠ 506/1994, ΠοινΧρ 1994, σελ. 627 επ,

συνείδηση συγκεκριμένου, διάφορου του δράστη, φυσικού προσώπου και όχι εν γένει και αορίστως προς το ευρύ κοινό. [51]

Η πλάνη του προσώπου που προβαίνει στην περιουσιακή διάθεση προέρχεται είτε από την (εν γνώσει) παράσταση ψευδών γεγονότων ως αληθινών (τέλεση με ενέργεια του δράστη), είτε από την αθέμιτη απόκρυψη (τέλεση με ενέργεια του δράστη) ή παρασιώπηση (τέλεση με παράλειψη) αληθινών γεγονότων. Ως προς την παράσταση ψευδών γεγονότων ως αληθινών, ως τέτοια θεωρείται η ανακοίνωση του δράστη σε κάποιον μιας σκέψης ή η βεβαίωση ή ο ισχυρισμός σχετικά με ένα γεγονός, το οποίο όμως αφίσταται της πραγματικότητας[52]. Σύμφωνα δε με την πάγια νομολογία του Αρείου Πάγου, παράσταση ψευδούς γεγονότος συνιστά *«οποιαδήποτε ανακοίνωση, δήλωση, διαβεβαίωση ή ισχυρισμός αυτού, που εμπεριέχει ανακριβή παρουσίαση ή απεικόνιση της πραγματικότητας»*[53].

Στην έννοια της παράστασης εμπίπτει και τόσο η ρητή όσο και αυτή που γίνεται με έργα ή ενδεικτικές πράξεις ή που συνάγεται από τη συνολική συμπεριφορά του δράστη[54], ενώ, εάν ο αποδέκτης γνωρίζει ήδη την αλήθεια ή γνωρίζει την αναλήθεια των γεγονότων που αφορά η παράσταση εκ μέρους δράστη, τότε δεν θεωρείται ότι υπάρχει παραπλάνηση σε βάρος του και ως εκ τούτου δεν διαπράττεται απάτη.

Επιπλέον, ως γεγονότα, κατά την έννοια του 386 ΠΚ νοούνται τα πραγματικά περιστατικά, ήτοι τα συμβεβηκότα του εξωτερικού κόσμου, που απεικονίζουν την πραγματικότητα, τα οποία ανάγονται στο παρελθόν ή στο παρόν και όχι εκείνα που πρόκειται να συμβούν στο μέλλον, όπως είναι οι απλές υποσχέσεις ή οι συμβατικές

[51] Βλ. Μπέκα, ο.π, σελ. 376, Παπαδαμάκης Α. ο.π., σελ. 154

[52] Βλ. Καμπέρου Ε. σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π., σελ. 3069. Μπέκα Ι., ο.π., σελ. 371 και ενδεικτικά νομολογιακά παραδείγματα ΑΠ 404/2019 και ΑΠ 623/2019, αμφότερες δημοσιευμένες στην ΤΝΠ ΝΟΜΟΣ

[53] Βλ. ενδ. 72/1019, ΤΝΠ ΝΟΜΟΣ.

[54] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, εκδ. Σάκκουλα, 2022, σελ. 78 επ., *ίδιος* Παρατηρήσεις στην ΑΠ 52/1999, Υπεράσπιση, σελ. 929

υποχρεώσεις, ή ακόμα οι υποκειμενικές κρίσεις, εκτιμήσεις και προβλέψεις, οι οποίες δεν συνοδεύονται από κάποιο επιπλέον στοιχείο το οποίο να συνηγορεί στο ότι θα συμβούν με αυξημένη πιθανότητα η οποία να αγγίζει τη βεβαιότητα[55]. Έτσι, εάν οι υποσχέσεις συνοδεύονται από άλλες παραστάσεις ψευδών γεγονότων, κατά τρόπο που να δημιουργείται η εντύπωση μελλοντικής εκπλήρωσής τους με βάση την εμφανιζόμενη ψευδή κατάσταση, τότε οι υποσχέσεις αυτές αποτελούν απατηλή συμπεριφορά[56].

Σχετικά με την απόκρυψη, η αληθής έννοια της οποίας συχνά συγχέεται με αυτές της παράστασης και της παρασιώπησης[57], ως τέτοια νοείται η με ενέργεια παρεμπόδιση του θύματος να πληροφορηθεί την πραγματικότητα / αλήθεια, την οποία ο δράστης συσκοτίζει. Η δε απόκρυψη θα πρέπει να είναι αθέμιτη, δηλαδή ο δράστης να μη δικαιολογείται εκ του νόμου να προβεί στην απόκρυψη, διαφορετικά η πράξη του δεν είναι άδικη[58].

Επιπροσθέτως, ως προς την παρασιώπηση αληθινών γεγονότων, ήτοι την παράλειψη ανακοίνωσης αυτών, ζήτημα έχει τεθεί εάν αποτελεί έγκλημα γνήσιας ή μη γνήσιας παράλειψης, οπότε και απαιτείται επιπλέον και η συνδρομή των προϋποθέσεων που αναφέρονται στο άρθρο 15 ΠΚ. Το ερώτημα τέθηκε δεδομένου ότι η χρησιμοποιούμενη από τον νόμο λέξη «παρασιώπηση» περιλαμβάνει στην ουσία της την παράλειψη ανακοίνωσης, ωστόσο σύμφωνα με την πάγια άποψη της νομολογίας, θα πρέπει να συντρέχουν πράγματι οι όροι του άρθρου 15 ΠΚ, δηλαδή ο δράστης να έχει την ιδιαίτερη νομική υποχρέωση άρσης της προϋπάρχουσας πλάνης, ή αποτροπή της

[55] Βλ. Μπέκα, ο.π, σελ. 367 επ. και ενδεικτικά νομολογιακά παραδείγματα ΑΠ 1063/2009, ΠοινΧρ, σελ. 300 (όπου κρίθηκε ότι δεν συνιστά γεγονός, η υπόσχεση εκτέλεσης οικοδομικής εργασίας εντός του συμβατικώς συμφωνηθέντος χρόνου) και ΠλημΘεσσ 991/2007, ΠοινΧρ, σελ. 166 (δεν συνιστά γεγονός, η υπόσχεση επιστροφής οφειλόμενου ποσού)

[56] Βλ. ενδ. ΑΠ 1/2019, ΤΝΠ ΝΟΜΟΣ, Παπαδαμάκης Α. ο.π., όπου και περαιτέρω παραπομπές στην παγίως προσανατολισμένη στην αποδοχή της εξωτερικής διάστασης του γεγονότος αντίληψη της ελληνικής νομολογίας και θεωρίας

[57] Βλ, Μπέκα, ο.π., σελ. 372

[58] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, εκδ. Σάκκουλα, 2022, σελ. 90

δημιουργίας ή της εδραίωσης πλάνης από τον νόμο, σύμβαση ή προηγούμενη ενέργειά του[59]. Τέτοια υποχρέωση ανακοίνωσης, σύμφωνα με την νομολογία[60] αν και γίνεται δεκτό πως δεν υφίσταται στις συμβάσεις γενικό καθήκον διαφώτισης[61], υποβαθρώνεται στις διατάξεις των άρθρων 197, 288 και 300 ΑΚ, ήτοι επί των συναλλακτικών ηθών και τη επιβαλλόμενη από τις περιστάσεις, καλόπιστη συμπεριφορά, ενώ ο Μπέκας συμπληρώνει ότι δύναται επίσης να ερείδεται πηγάζει ευθέως από κανόνα δικαίου ή σύστημα τέτοιων.[62] Επομένως, καθίσταται σαφές ότι και εδώ η διάταξη αξιώνει η παρασιώπηση να είναι «αθέμιτη» [63], διότι ο δράστης έχει την υποχρέωση να αποκαλύψει στο θύμα το αληθές γεγονός ή να το αποτρέψει από το να θεμελιώσει μία εσφαλμένη αντίληψη της πραγματικότητας, υποχρέωση που μπορεί να είναι συμβατική ή νόμιμη. Στις περιπτώσεις της παρασιώπησης εμπίπτει και το καθήκον αληθείας το οποίο θεμελιώνουν οι γενικές αρχές των συναλλακτικών ηθών και της καλής πίστης, οι οποίες

[59] Βλ. ΟλΑΠ 1/2020, ΟλΑΠ 3/2019, ΤΝΠ ΝΟΜΟΣ.

[60] Ενδεικτικά ΑΠ 101/2018, ΑΠ 293/2006)

[61] Βλ. Μπαλής, Γενικαί Αρχαί, 1950, σελ. 186

[62] Βλ, Μπέκα, ο.π., σελ. 373-374, υποσημ. 108 και 109, με αναφορές στις διατάξεις των άρθρων του ΑΚ (υποχρεώσεις εντολοδόχου προς εντολέα, διαχειριστή εταιρείας προς εταίρους, πωλητή προς αγοράστη κλπ)

[63] Σύμφωνα με την άποψη που θεωρεί ότι η εν λόγω περίπτωση συνιστά έγκλημα γνήσιας παράλειψης και ως εκ τούτου δεν απαιτείται η συνδρομή των όρων του άρθρου 15 ΠΚ, η παρασιώπηση θα πρέπει να είναι αθέμιτη, υπό την έννοια ότι ο δράστης δεν δικαιούται σύμφωνα με τον νόμο να προβεί σε παρασιώπηση των πραγματικών γεγονότων. Κατά την άποψη αυτή ο όρος «αθέμιτη» παρασιώπηση είναι στενότερος, διότι δεν περιλαμβάνει την προηγούμενη ενέργεια του δράστη (σε αντίθεση με το άρθρο 15 ΠΚ), επομένως θα κρίνεται κατά περίπτωση εάν η εκάστοτε προγενέστερη της παρασιώπησης συμπεριφορά του δράστη θα μπορούσε πράγματι να θεμελιώσει τον αθέμιτο χαρακτήρα της παρασιώπησης, ενώ στην περίπτωση που δεχθούμε την εφαρμογή του άρθρου 15 ΠΚ (μη γνήσιας παράλειψης έγκλημα), τότε a priori η προηγούμενη συμπεριφορά του δράστη θα θεμελιώνει την ιδιαίτερη υποχρέωσή του να άρει την πλάνη του θύματος, βλ. Καμπέρου Ε. σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π., σελ. 3070.

επιβάλλουν σε ορισμένες περιστάσεις το «καθήκον διαφώτισης», ιδίως όταν συντρέχει κίνδυνος να υποστεί το άλλο πρόσωπο ιδιαίτερα μεγάλη οικονομική ζημία[64].

Τέλος, η περιουσιακή βλάβη, που, όπως προεκτέθηκε, υπάρχει σε περίπτωση μείωσης ή χειροτέρευσης της περιουσίας του παθόντος, πρέπει, ως στοιχείο της αντικειμενικής υπόστασης του εγκλήματος της απάτης, να είναι άμεσο, αναγκαίο και αποκλειστικό αποτέλεσμα της περιουσιακής διάθεσης, ήτοι της πράξης, παράλειψης ή ανοχής, στην οποία προέβη εκείνος που πλανήθηκε από την απατηλή συμπεριφορά του δράστη[65]. Πρέπει να υπάρχει, δηλαδή, αλυσιδωτός αιτιώδης σύνδεσμος μεταξύ αφενός της απατηλής συμπεριφοράς και της πλάνης που προκλήθηκε από αυτή, καθώς και μεταξύ της πλάνης αυτής και της περιουσιακής βλάβης, η οποία πρέπει να είναι το άμεσο, αναγκαίο και αποκλειστικό αποτέλεσμα της πλάνης και της από αυτή πράξης, παράλειψης ή ανοχής του πλανηθέντος[66].

5.3. Υποκειμενική υπόσταση

Από τον συνδυασμό των διατάξεων 26 ΠΚ και 18 ΠΚ προκύπτει ότι, δεδομένου του πλημμελληματικού χαρακτήρα της απάτης στη βασική της μορφή, τιμωρείται μόνο όταν τελείται από δόλο και μάλιστα οποιουδήποτε βαθμού (άρα και ενδεχόμενου), ενώ η εξ αμελείας τέλεση αποκλείεται δεδομένης της έλλειψης τυποποίησης του αδικήματος από αμέλειας στον νόμο. Ο δράστης, επομένως, θα πρέπει να γνωρίζει έστω ως ενδεχόμενο ότι η απατηλή συμπεριφορά του μπορεί να οδηγήσει σε πλάνη του θύματος και περαιτέρω σε περιουσιακή διάθεση και εξ αυτής βλάβη του και να το αποδέχεται. Ειδικά, όμως, ως προς την πράξη της παράστασης ψευδούς γεγονότων ως αληθινών η

[64] Βλ. Καμπέρου Ε. σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π..

[65] Βλ. ΑΠ 1/2019, ΤΝΠ ΝΟΜΟΣ.

[66] Βλ. Ζήσης Α. Ποινικός Κώδικας, εκδόσεις Σάκκουλα 2022, σελ 722 επ. Πληροφορία από sakkoulas-online, Μπέκας, ο.π. σελ. σελ. 381 επ.

διάταξη αξιώνει ο δράστης να την τελεί «εν γνώσει» του, συνεπώς θα πρέπει να συντρέχει τουλάχιστον άμεσος δόλος β' βαθμού, δηλαδή ο δράστης να γνωρίζει με βεβαιότητα ότι παραθέτει στο θύμα ψευδή γεγονότα ως αληθινά και να το αποδέχεται[67].

Επιπλέον η διάταξη προβλέπει ότι ο δράστης θα πρέπει να έχει «σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος», χωρίς να απαιτείται για να θεωρείται το έγκλημα τελεσθέν να αποκομίσει πράγματι το όφελος αυτό. Ο περαιτέρω σκοπός τούτος, ο οποίος αντιστοιχεί σε άμεσο δόλο α' βαθμο, καθιστά το έγκλημα υπερχειλούς υποκειμενικής υπόστασης, διότι υπερβαίνει τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος και αφορά ένα στοιχείο (το παράνομο περιουσιακό όφελος) η συνδρομή του οποίου δεν απαιτείται για να καταφαθεί η πράξη[68].

Εν συνεχεία, περιουσιακό όφελος συνιστά η αύξηση της περιουσίας του ίδιου του δράστη ή άλλου, καθώς και η ευνοϊκότερη διαμόρφωση της περιουσιακής κατάστασης οποιουδήποτε από αυτούς[69]. Το περιουσιακό αυτό όφελος είναι παράνομο, όταν ο δράστης ή το άλλο πρόσωπο δεν έχει νόμιμη αξίωση κατά του παθόντος, ενώ θα πρέπει να υπάρχει αντιστοιχία ανάμεσα στην περιουσιακή βλάβη του παθόντος και τον προσπορισμό του οφέλους υπέρ του δράστη, υπό την έννοια ότι ακριβώς η περιουσιακή βλάβη του θύματος συνιστά το όφελος στο οποίο προσβλέπει ο δράστης.

5.4. Ποινική κύρωση της απάτης μέσω υπολογιστή - Έμπρακτη μετάνοια

Η βασική μορφή της απάτης, άρα και αυτής που τελείται μέσω υπολογιστή, είναι πλημμελληματικού χαρακτήρα για την οποία απειλείται ποινή φυλάκισης, ήτοι από 10

[67] Βλ. Φράγκος Κ., Online κατ' άρθρο ερμηνεία του Ποινικού Κώδικα, ό.π..

[68] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, ό.π., σελ. 144.

[69] Βλ. ΑΠ 1/2019, ΤΝΠ ΝΟΜΟΣ.

ημέρες έως 5 έτη βάσει του άρθρου 53 ΠΚ, σωρευτικά με χρηματική ποινή έως 360 ημερήσιες μονάδες ύψους από 1,00 έως 100,00 Ευρώ έκαστη, σύμφωνα με το άρθρο 57 παρ. 1, 2γ και 3 ΠΚ[70].

Στο τελευταίο εδάφιο της παρ. 1 του άρθρου 386 ΠΚ εντοπίζεται η πρώτη διακεκριμένη παραλλαγή του εγκλήματος της απάτης (και μέσω υπολογιστή) κακουργηματικού χαρακτήρα, όταν η ζημία και το αντίστοιχο επιδιωκόμενο περιουσιακό όφελος υπερβαίνει τις 120.000 Ευρώ. Η προβλεπόμενη ποινή είναι πρόσκαιρη κάθειρξη έως 10 έτη και χρηματική ποινή, η οποία παραμένει ίδια με την απειλούμενη στη βασική μορφή, δηλαδή δεν προβλέπεται κάποιο υψηλότερο ελάχιστο όριο.

Η δεύτερη παράγραφος του άρθρου 386 ΠΚ θεσπίστηκε με τον ν. 4619/2019 λόγω κατάργησης του ν. 1608/1950 «περί καταχραστών του Δημοσίου» με το άρθρο 462 ΠΚ. Επομένως, προβλέφθηκε ειδική διακεκριμένη παραλλαγή για τις περιπτώσεις που η πράξη στρέφεται και πλήττει την περιουσία του Δημοσίου με προξενηθείσα ζημία άνω των 120.000 Ευρώ, για την οποία απειλείται πρόσκαιρη κάθειρξη τουλάχιστον 10 ετών (ήτοι 10 έως 15 έτη) και χρηματική ποινή έως 1.000 ημερήσιες μονάδες (ύψους από 1,00 έως 100.00 Ευρώ έκαστη). Εκτός από τη βαρύτερη χρηματική ποινή που απειλείται, η εν λόγω μορφή απάτης είναι η βαρύτερη όλων και λόγω αυξημένου χρόνου για την παραγραφή της (20 έτη).

Τέλος, στο άρθρο 387 ΠΚ τυποποιείται η προνομιούχα μορφή της απάτης «μικρής αξίας». Το εν λόγω άρθρο παραπέμπει προς εφαρμογή του άρθρου 377 ΠΚ περί κλοπής «ευτελούς αξίας», βάσει του οποίου επιβάλλεται μόνο χρηματική ποινή ή παροχή κοινωφελούς εργασίας, όταν η προκληθείς με την πράξη της απάτης ζημία ήταν μικρής αξίας, η οποία καθορίζεται ad hoc κατόπιν αξιολόγησης της εκάστοτε εξατομικευμένης περίπτωσης.

Περαιτέρω, σύμφωνα με τα διαλαμβανόμενα στις παρ. 2 και 3 του άρθρου 405 ΠΚ, η έμπρακτη μετάνοια προβλέπεται ως λόγος εξάλειψης του αξιοποίνου[71], η οποία,

[70] Σημειώνεται ότι δυνάμει του άρθρου 405 ΠΚ η πλημμεληματική μορφή της απάτης είναι πλέον κατ' 'έγκληση διωκόμενο, εκτός αν στρέφεται κατά των οικονομικών συμφερόντων της ΕΕ, σύμφωνα με τον ειδικό ποινικό νόμο ν. 4689/2020.

κατά την οικεία νομοθετική ρήτρα, εφαρμόζεται εφόσον ο δράστη προβεί σε αποκατάσταση της περιουσιακής ζημίας και ικανοποίηση του παθόντος. Πρόκειται, κατά τον Παπαδαμάκη, για μια περίπτωση γνήσιας έμπρακτης μετάνοιας (παρ. 2) και δύο περιπτώσεις ποινικής-αποζημιωτικής διευθέτησης (παρ. 3)[72].

5.5. Ζητήματα απόπειρας, συμμετοχής και συρροών στην απάτη μέσω υπολογιστή

Σύμφωνα με το άρθρο 42 παρ. 1 ΠΚ, για να γίνει λόγος για απόπειρα τέλεσης απάτης, ο δράστης θα πρέπει να ξεκινήσει να πραγματώνει έστω και ένα μέρος της αντικειμενικής υπόστασης του εγκλήματος (αρχή εκτέλεσης), δηλαδή να ξεκινήσει να πραγματοποιεί την παράσταση ψευδών γεγονότων ως αληθών / την αθέμιτη απόκρυψη / παρασιώπηση των αληθινών, καλύπτοντας την πράξη αυτή με τον αναγκαίο δόλο για την παραπλάνηση, περιουσιακή διάθεση του θύματος και πρόκληση βλάβης στην περιουσία του και με σκοπό τον προσπορισμού του αντίστοιχου περιουσιακού οφέλους[73].

Ειδικά όσον αφορά την απάτη μεσώ υπολογιστή, θα πρέπει να διευκρινιστεί ότι, δεδομένου ο υπολογιστής αποτελεί το μέσο για την τέλεση της αξιόποινης πράξης, η

[71] *«(...) 2. Το αξιόποινο των εγκλημάτων που προβλέπονται στο άρθρο 386, στις παρ. 1 και 3 του άρθρου 386Α και στα άρθρα 386Β, 387, 389, 390, 394, 397 και 404 εξαλείφεται αν ο υπαίτιος, με δική του θέληση και πριν από την πρώτη εξέτασή του ως υπόπτου ή κατηγορουμένου ικανοποιήσει εντελώς τον ζημιωθέντα χωρίς παράνομη βλάβη τρίτου. Η μερική μόνο ικανοποίηση εξαλείφει το αξιόποινο κατά το αντίστοιχο μόνο μέρος.3. Εάν ο υπαίτιος των εγκλημάτων που αναφέρονται στην προηγούμενη παράγραφο μέχρι την αμετάκλητη παραπομπή του στο ακροατήριο ικανοποιήσει εντελώς τον ζημιωθέντα, καταβάλλοντας αποδεδειγμένα το κεφάλαιο και τους τόκους υπερημερίας, από την ημέρα τέλεσης του εγκλήματος, απαλλάσσεται από κάθε ποινή. Η διάταξη του προηγούμενου εδαφίου εφαρμόζεται και για τα πλημμελήματα που προβλέπονται στα ίδια άρθρα μέχρι το τέλος της αποδεικτικής διαδικασίας στο πρωτοβάθμιο δικαστήριο.»*

[72] Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 4η έκδ., 2022, σ. 144

[73] Βλ. ενδ. ΑΠ 1466/2017, ΤΝΠ ΝΟΜΟΣ.

αγορά ή άλλη προετοιμασία του ηλεκτρονικού υπολογιστή (π.χ. ρύθμιση, εγκατάσταση προγραμμάτων, δημιουργία λογαριασμών, κ.ά.) δεν μπορούν να θεωρηθούν αρχή εκτέλεσης του εγκλήματος, λόγω απουσίας του στοιχείου της επικοινωνίας η οποία απαιτείται τόσο για την παράσταση ψευδών γεγονότων, όσο και για την παρασιώπηση και απόκρυψη των αληθινών. Ομοίως, τυχόν αποστολή αιτημάτων φιλίας ή μηνύματος στα μέσα κοινωνικής δικτύωσης δεν αποτελούν επικοινωνία, όπως αυτή ορίστηκε παραπάνω, ως αντιθέτως η απευθείας αποστολή μηνύματος ή email συνιστούν επικοινωνία, για την οποία δεν απαραίτητη η συμμετοχή του αποδέκτη αυτού – θύματος. Ως εκ τούτου, δεν καταφάσκεται απόπειρα απάτης στην περίπτωση που το θύμα τελικώς δεν παραπλανάται, ώστε να προχωρήσει σε επιζήμια για την περιουσία του (ή τρίτου) διάθεση (π.χ. δεν ακολουθεί τον σύνδεσμο που παρατίθεται στο παραπλανητικό email). Αντιθέτως, πράξεις όπως οι ως άνω αναφερόμενες περί αγοράς εξοπλισμού ηλεκτρονικού υπολογιστή, προετοιμασία της σύνδεσης στο Διαδίκτυο, κ.λπ., τέτοιου είδους πράξεις αποτελούν μόνο προπαρασκευαστικές ενέργειες, οι οποίες, ελλείψει ρητής τυποποίησής τους ως αυτοτελώς αξιόποινες, στερούνται ποινικού ενδιαφέροντος[74].

Όσον αφορά τις μορφές συμμετοχής στο έγκλημα της απάτης, και μέσω υπολογιστή, όλες μπορούν να υπάρξουν. Έτσι, κατ' άρθρο 45 ΠΚ η απάτη μπορεί να τελεστεί κατά συναυτουργία, όταν δύο ή πλείονες δράστες προβαίνουν σε παράσταση ψευδών γεγονότων ως αληθινών (π.χ. μέσω ηλεκτρονικών μηνυμάτων σε group chat όπου συμμετέχει το θύμα[75]), εφόσον η πράξη όλων τελεί σε άμεση χρονική συνάφεια με τη δημιουργία της πλάνης στο θύμα και εφόσον συντρέχει στο πρόσωπο όλων ο υπερχειλής σκοπός προσπορισμού παράνομου περιουσιακού οφέλους. Διαφορετικά, ελλείψει του χρονικού κριτηρίου, θα πρέπει να δεχθούμε ότι πρόκειται για απλή συνέργεια[76] κατ' άρθρ. 47 ΠΚ.

[74] Βλ. ΑΠ 1698/2003, ΤΝΠ ΝΟΜΟΣ.

[75] Βλ. και ΑΠ 367/2017, ΤΝΠ ΝΟΜΟΣ.

[76] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, ό.π., σελ. 152.

Περαιτέρω, άμεση συνέργεια κατ' άρθρο 47 ΠΚ είναι η συνδρομή που παρέχεται στο δράστη της αξιόποινης πράξης κατά τη διάρκειά της και στην εκτέλεσή της, με την παροχή του αντικειμένου της προσβολής στη διάθεση του φυσικού αυτουργού, μάλιστα δε κατά τέτοιο τρόπο, ώστε χωρίς αυτή τη συνδρομή δεν θα ήταν δυνατή με βεβαιότητα η διάπραξη του εγκλήματος υπό τις περιστάσεις που τελέστηκε[77]. Έτσι, στην περίπτωση της απάτης μέσω ηλεκτρονικού υπολογιστή, ως άμεσος συνεργός θα μπορούσε να θεωρηθεί το πρόσωπο που συμμετέχει ως παίκτης σε απατηλό παίγνιο ηλεκτρονικού καζίνο το οποίο έχει οργανωθεί και διεξάγεται από τους δράστες της απάτης, και με σκοπό προσπορισμού στο πρόσωπο των διοργανωτών παράνομου περιουσιακού οφέλους από τη ζημία που θα υποστεί το θύμα ως (ομοίως) παίκτης στο ίδιο παίγνιο.

Αντιθέτως, οποιαδήποτε άλλη συνδρομή και ιδίως η συνδρομή που παρέχεται στο δράστη της αξιόποινης πράξης πριν από την τέλεσή της, είναι απλή συνέργεια. Για την ύπαρξη απλής συνέργειας, υποκειμενικά απαιτείται δόλος του συνεργού, ο οποίος συνίσταται στη γνώση της τέλεσης από τον αυτουργό ορισμένης αξιόποινης πράξης και στη βούληση ή αποδοχή να συμβάλει με τη συνδρομή του στην πραγμάτωσή της, διευκολύνοντας τον αυτουργό. Η συνδρομή του απλού συνεργού μπορεί να είναι είτε υλική είτε ψυχική. Η ψυχική συνδρομή μπορεί να παρασχεθεί με την ενεργό παρουσία του απλού συνεργού στον τόπο της πράξης, με την ενίσχυση της απόφασης του αυτουργού για την τέλεση της πράξης, καθώς και με την ενθάρρυνση αυτού με οποιονδήποτε τρόπο[78].

Αναφορικά με τον τρόπο συρροής του εγκλήματος της απάτης μέσω υπολογιστή με άλλες αξιόποινες πράξεις, συχνή είναι η περίπτωση της συρροής με το έγκλημα της πλαστογραφίας (άρθρ. 216 ΠΚ αλλά και μετά χρήσεως, 216 παρ. 2 ΠΚ), είτε όταν η απάτη είναι τετελεσμένη, είτε στο στάδιο της απόπειρας.

Καταρχάς, η πλαστογραφία μετά χρήσεως (αρ. 216 παρ. 2 ΠΚ) συμπροστατεύει πέρα από το έννομο αγαθό του υπομνήματος και την διακινδύνευση της περιουσίας. Η

[77] Βλ. ενδ. ΑΠ 449/2022, ΤΝΠ ΝΟΜΟΣ.

[78] Βλ. ΑΠ 552/2020, ΑΠ 1806/2019, ΤΝΠ ΝΟΜΟΣ.

Νομολογία παγίως[79] δέχεται αληθινή συρροή μεταξύ τους, με το επιχείρημα ότι κάθε μία από τις πράξεις είναι αυτοτελής, στοιχειοθετείται από ιδιαίτερα περιστατικά και δεν αποτελεί η μία συστατικό της άλλης ή επιβαρυντική περίσταση, ούτε αναγκαίο μέσο διαπράξεως αυτής. Ωστόσο, όταν τα πραγματικά περιστατικά που συνιστούν την χρήση του πλαστού, ταυτίζονται με αυτά της απάτης, θα πρέπει να εξεταστεί η περίπτωση της φαινομενικής συρροής υπέρ της απάτης που προστατεύει και την βλάβη της περιουσίας[80]. Η λύση, όμως, της φαινομενικής συρροής υπέρ της απάτης παραβλέπει ένα σοβαρό σκόπελο, αυτό της ανάγκης αξιολόγησης του προσβαλλομένου εννόμου αγαθού του υπομνήματος, γι' αυτό και ορθότερη κρίνεται, κατά την άποψη του γράφοντος, η αληθινή συρροή. Από την άλλη, όταν η απάτη βρίσκεται σε στάδιο απόπειρας, γίνεται δεκτό ότι μόνο για διακινδύνευση περιουσίας μπορεί να γίνει λόγος. Δεδομένου, λοιπόν, ότι η πλαστογραφία συνίσταται απλώς στην πλαστοποιητική ενέργεια και δεν συμπεριλαμβάνει χρήση του πλαστού, τα έννομα αγαθά είναι διαφορετικά, γι' αυτό και γίνεται λόγος για αληθινή συρροή[81].

Επίσης συχνή περίπτωση στην πράξη αποτελεί η συρροή της απάτης με την υπεξαίρεση (375 ΠΚ). Εάν στρέφονται κατά διαφορετικού υλικού αντικειμένου, τότε είναι σαφές ότι η συρροή είναι αληθινή, καθώς οι δύο αξιόποινες πράξεις αποτελούνται από διαφορετικά στοιχεία[82] και προστατεύουν διαφορετικά έννομα αγαθά (περιουσία / ιδιοκτησία). Όταν οι δύο πράξεις στρέφονται κατά του ίδιου υλικού αντικειμένου, η συρροή μπορεί να είναι φαινομενική, εάν ο δράστης υπεξαίρεσε το κινητό πράγμα και εν συνεχεία τελεί την πράξη της απάτης για να συγκαλύψει την υπεξαίρεση, επομένως η ζημία συνίσταται στην οριστική ματαίωση της ανάκτησης του πράγματος από το θύμα, με αποτέλεσμα να εγκολπώνεται κατά τρόπο μόνιμο στην περιουσία του δράστη, είτε όταν ο δράστης αποκτά το πράγμα με πράξη απάτης, οπότε η υπεξαίρεση αποτελεί την

[79] Βλ. ενδ.ΑΠ 949/2008, 1017/2011, 303/2013, 506/2017, στην επίσημη ιστοσελίδα του Αρείου Πάγου.

[80] Βλ. Μυλωνόπουλος Χ., Ποινικό Δίκαιο Ειδικό μέρος, ό.π., σελ. 504.

[81] Βλ. ΑΠ 406/1996, Υπερ 1996, 975 με παρατηρήσεις Λ. Μαργαρίτη.

[82] Βλ. Καμπέρου Ε. σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π.., σελ. 1782.

ουσιαστική αποπεράτωση του εγκλήματος (ήτοι του υπερχειλούς σκοπού προσπορισμού παράνομου περιουσιακού οφέλους)[83].

6. Η απάτη με υπολογιστή (386^{A} ΠΚ)

6.1. Η νομοθετική εξέλιξη της διάταξης του άρθρου 386^{A} ΠΚ και το προστατευόμενο έννομο αγαθό

Το άρθρο 386^{A} περί απάτης με υπολογιστή προστέθηκε το πρώτον στον ΠΚ με τον τροποποιητικό ν. 1805/1988 «Εκσυγχρονισμός τον θεσμού τον ποινικού μητρώου, τροποποίηση ποινικών διατάξεων και ρύθμιση άλλων σχετικών θεμάτων»[84], σύμφωνα με το οποίο *«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»*.

[83] Το έγκλημα της απάτης μπορεί να συρρέει και με άλλες αξιόποινες πράξεις, π.χ. το έγκλημα της ακάλυπτης επιταγής κατ' άρθρο 79 ν. 5960/1933, της ευρωαπάτης (ν. 4689/2020, της φοροδιαφυγής (άρθρο 66 ν. 4987/2022), της λαθρεμπορίας (άρ. 155ν. 2960/2001 όπως ισχύει μετά τον ν. 5042/2023), της καταδολίευσης δανειστών άρ. 397 ΠΚ.

[84] Πρβλ. σχετ. Μυλωνόπουλος Χρ. Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, Συμβολή στην ερμηνεία των άρθρων 13γ, 370Β, 370Γ και 386^{A} ΠΚ (άρθρο 25 ν. 1805/1988), 1991, σελ. 54 και Βασιλάκης Ε. Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών – Η αντιμετώπιση του προβλήματος με την εισαγωγή του ν. 1805/1988, 1993, σελ. 185

Ο βασικότερος λόγος για τον οποίο αποφασίστηκε η τυποποίηση νέου εγκλήματος ήταν διότι δεν γινόταν δεκτό ότι η νομοτυπική μορφή της απάτης του άρθρ. 386 ΠΚ μπορούσε να καλύψει την πρόκληση περιουσιακής βλάβης όταν αυτή τελείται με την επέμβαση του προσώπου σε ένα πληροφορικό σύστημα, ελλείψει της αναγκαίας επικοινωνίας που απαιτείται ανάμεσα στον δράστη και το θύμα για την παράσταση ψευδών γεγονότων ή παρασιώπηση / απόκρυψη αληθινών[85]. Ήταν δε σαφές ότι η πολιτεία έπρεπε να μεριμνήσει για την ποινικοποίηση της ανωτέρω συμπεριφοράς, καθώς την περίοδο έκδοσης του ν. 1805/1988 ήταν ιδιαίτερα δημοφιλής η παράνομη χρήση κωδικών από κάρτες σε μηχανήματα αυτόματης ανάληψης χρημάτων (ΑΤΜ), ενώ αργότερα η διάταξη υπέστη τροποποίηση, ώστε να καλύπτει και άλλες μορφές απάτης που έκαναν την εμφάνισή του μετά την ανακάλυψη και διάδοση του Διαδικτύου[86].

Η ως άνω αναφερόμενη τροποποίηση έλαβε χώρα, όπως ήδη αναφέρθηκε, με τον ν. 4411/2016, με τον οποίο επήλθαν αλλαγές και στο άρθρο 13 ΠΚ, όπου προστέθηκαν ορισμοί για τις έννοιες των ψηφιακών δεδομένων και του πληροφοριακού συστήματος (στοιχεία ζ' και στ'). Έτσι, η νέα νομοτυπική μορφή του εγκλήματος προέβλεπε «*Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα*»[87].

[85] Βλ. Ιγγλεζάκης Ι., Δίκαιο Πληροφορικής, εκδ. Α.Ν. Σάκκουλα, 2018, σελ. 332.

[86] Βλ. Νούσκαλης Γ., «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», ΠοινΔικ 2/2003, σελ. 178 επ.

[87] Η αξιόποινη συμπεριφορά της χωρίς δικαίωμα χρήσης δεδομένων καλύπτει και την περίπτωση που ο δράστης εισάγει ορθά (και όχι ψευδή) δεδομένα προκειμένου να βλάψει ξένη περιουσία και να προσπορίσει στον εαυτό του αντίστοιχο παράνομο περιουσιακό όφελος π.χ. όταν κατέχει

Με τον ν. 4619/2019 (νέος ΠΚ) η διάταξη του άρθρ. 386^{Α} ΠΚ τροποποιήθηκε εκ νέου και σήμερα, μετά τον διορθωτικό ν. 4855/2021 και τον τροποποιητικό ν. 4947/2022 έχει 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».

χωρίς δικαίωμα το όνομα χρήστη και τον κωδικό πρόσβασης web banking του θύματος, βλ. σχετ. Αιτιολογική Έκθεση ν. 4411/2016.

Σχετικά με το προστατευόμενο έννομο αγαθό του άρθρ. 386^{A} ΠΚ, ορθότερο είναι να δεχθούμε ότι είναι το ίδιο με τη διάταξη του άρθρ. 386 ΠΚ όπως αναλύθηκε ανωτέρω, δηλαδή η περιουσία του παθόντος, δεδομένου ότι αμφότερες οι διατάξεις ανήκουν στο 23^{ο} κεφάλαιο του ΠΚ περί εγκλημάτων κατά της περιουσίας[88]. Επιπλέον, έχει γίνει λόγος και για προστασία της ασφάλειας των περιουσιακών συναλλαγών μέσω υπολογιστή, λαμβάνοντας κανείς υπόψη την ευρεία διάδοση αυτών των συναλλαγών οι οποίες έχουν εγκαθιδρύσει τη νέα ψηφιακή πραγματικότητα[89].

6.2. Αντικειμενική υπόσταση

Πρωτίστως θα πρέπει να σημειωθεί ότι η απάτη με υπολογιστή είναι ιδιώνυμο έγκλημα εν συγκρίσει με αυτό της απάτης του άρθρου 386 ΠΚ, εφόσον προσβάλλει καταρχήν την περιουσία με αντίστοιχο προς την απάτη τρόπο, αλλά χωρίς να περιλαμβάνει όλα τα στοιχεία της βασικής απάτης, αποτελώντας παραλλαγή της[90]. Ως έγκλημα δομήθηκε κατ' αντιστοιχία προς την απάτη του άρθρου 386 ΠΚ, με την οποία τελεί σε σχέση αλληλοαποκλεισμού και από την οποία διαφέρει κατά το ότι τελείται όταν η περιουσιακή βλάβη επέρχεται όχι με την παραπλάνηση ενός φυσικού προσώπου που είναι αρμόδιο να λαμβάνει αποφάσεις ή να διενεργεί έλεγχο ή να εγκρίνει ή να χορηγεί κλπ αλλά αποκλειστικά και μόνο με τον επηρεασμό των στοιχείων του υπολογιστή, δηλαδή με την επέμβαση του δράστη κατά τον προγραμματισμό του

[88] Βλ. Μπουρμάς Γ., σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π.., σελ. 3141.

[89] Βλ. Νούσκαλης Γ., «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», ό.π., Ι. Ιγγλεζάκης, ο.π., σελ. 405, Παπαδαμάκης, ο.π., σελ. 151

[90] Βλ. Μπουρμάς Γ., σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π..

συστήματος και την επεξεργασία των δεδομένων σε οποιαδήποτε φάση της λειτουργίας του υπολογιστή[91].

Επιπλέον, πρόκειται για ένα υπαλλακτικώς μικτό έγκλημα, καθώς οι περισσότεροι τρόποι τέλεσης μπορούν να εναλλαχθούν επί της ίδιας μονάδας εννόμου αγαθού. Είναι επίσης, όπως και η κοινή απάτη του άρθρου 386 ΠΚ, έγκλημα κοινό («όποιος»), δεδομένου ότι δράστης μπορεί να είναι οποιοσδήποτε χωρίς να φέρει συγκεκριμένη ιδιότητα. Βασικό στοιχείο και στο έγκλημα της απάτης με υπολογιστή είναι η αντιστοιχία περιουσιακής βλάβης και προσπορισμού παράνομου περιουσιακού οφέλους υπέρ του δράστη ή τρίτου.

Όπως διεξοδικότερα θα αναπτυχθεί ακολούθως, η αντικειμενική υπόσταση του αδικήματος συγκροτείται, σε αδρές γραμμές από την συμπεριφορά του δράστη, η οποία πραγματώνεται ουσιαστικά με κάποιον από τους περιοριστικά αναφερόμενους στη διάταξη, τρόπους τέλεσης και το άμεσο αποτέλεσμα, τον επηρεασμό, διαμέσου της συμπεριφοράς αυτής, του επηρεασμού των στοιχείων του η/υ.

6.2.1. Μη ορθή διαμόρφωση προγράμματος υπολογιστή

Ως πρώτος τρόπος τέλεσης τυποποιείται η *μη ορθή διαμόρφωση προγράμματος υπολογιστή*, όπου ως πρόγραμμα υπολογιστή θεωρείται «ένα σύνολο δεδομένων με τα οποία παρέχονται εντολές στον υπολογιστή, στην εκάστοτε γλώσσα την οποία αντιλαμβάνεται, ώστε να επεξεργάζεται άλλα εξωτερικά δεδομένα που εισάγονται κάθε φορά σε αυτόν και να εξάγει συμπεράσματα από αυτά»[92]. Επομένως, ο υπολογιστής «διαβάζει» εκάστη εντολή διατρέχοντας τα δεδομένα που εισήχθησαν, την εκτελεί, και κάνει το ίδιο με όλες τις εντολές που δόθηκαν σε αυτόν.

[91] Βλ. ΑΠ 734/2021, επίσημη ιστοσελίδα του Αρείου Πάγου.

[92] Βλ. Μπουρμάς Γ., σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π. και Μπέκας, ο.π., σελ 414

Εξάλλου, ένα σύστημα δεδομένων *διαμορφώνεται ορθά* και συνακολούθως *λειτουργεί ορθά*, όταν δεν αποκλίνει από τον κοινωνικό του προορισμό καθώς επίσης και όταν εξ αυτού επιτρέπεται η συναγωγή ορθών συμπερασμάτων. Εξ αντιδιαστολής, και κατά την έννοια της διάταξης αυτής, ένα πρόγραμμα που εκ της αρχικής του διαμόρφωσης, εξυπηρετεί την περιουσιακή μετάθεση, όπως για παράδειγμα το σύστημα παροχής υπηρεσιών πληρωμών μιας τραπεζικής εταιρείας[93], δύναται να είναι δεκτικό *μη ορθής διαμόρφωση* και ασφαλώς να επιφέρει εξ αυτής, το αξιούμενο από την αντικειμενική υπόσταση του αδικήματος, αποτέλεσμα. Συνάγεται λοιπόν, για την τέλεση του εγκλήματος του άρθρ. 386^{A} ΠΚ με τον τρόπο αυτόν, ο δράστης μπορεί είτε να «τρέξει» ένα εν όλω ή εν μέρει νέο πρόγραμμα (αποθηκεύοντάς το σε κάποιο μέρος του υπολογιστή ή σε εξωτερικό μέσο αποθήκευσης π.χ. μονάδα usb), είτε αλλοιώνοντας ήδη εγκατεστημένο στον υπολογιστή πρόγραμμα (π.χ. με αλλαγή ή παράλειψη εντολών στην προϋπάρχουσα αλληλουχία), είτε αποκρύπτοντας δεδομένα προς ανάγνωση και επεξεργασία [94]. Ως εκ τούτου, γίνεται λόγος για «χειραγώγηση» του προγράμματος, η οποία συνεπάγεται τη μη ορθή επεξεργασία των δεδομένων[95], ενώ μη ορθή διαμόρφωση θα πρέπει να δεχθούμε ότι συντρέχει όταν τα αποτελέσματα στα οποία καταλήγει η επεξεργασία είναι πρόσφορα να προκαλέσουν περιουσιακή βλάβη ή έρχονται σε αντίθεση με μια νόμιμη κατάσταση[96]. Το πότε είναι ορθή η διαμόρφωση εξαρτάται από τη βούληση του χειριστή ή ιδιοκτήτη του ηλεκτρονικού υπολογιστή, εκτός από περιπτώσεις όπου ο νόμος καθορίζει την ορθότητα, π.χ. στον υπολογισμό μισθών και συντάξεων[97].

---

[93] Βλ. Παπαδαμάκης Α., ο.π., σελ. 156, όπου με περαιτέρω παραπομπές (ενδ. Νομολογία: ΑΠ 367/2017 ΠοινΧρ 2018.752) γίνεται λόγος για την κρίσιμη παράμετρο της *προσφορότητας του προγράμματος* να εκπληρώσει τον σκοπό της μη ορθής διαμόρφωσης του

[94] Βλ. Μπουρμάς Γ., σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π..

[95] Βλ. Φράγκος Κ., Online κατ' άρθρο ερμηνεία του Ποινικού Κώδικα, ό.π..

[96] Βλ. Βασιλάκη Ε., Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, εκδ. Αντ. Ν. Σάκκουλας, 1993, σελ. 203.

[97] Βλ. ΑΠ 1152/1999, ΠοινΔικ 1999, σελ. 1297 επ., πρβλ. σχετ. Μπέκα Ι. ο.π., σελ. 414

6.2.2. Χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος

Ως χωρίς δικαίωμα παρέμβαση θεωρείται αυτή που γίνεται χωρίς ο παρεμβαίνων να έχει λάβει σχετική προς τούτο άδεια ή εξουσιοδότηση του ιδιοκτήτη ή κατόχου του προγράμματος όπου παρεμβαίνει ή του ηλεκτρονικού υπολογιστή στον οποίο είναι εγκατεστημένο το πρόγραμμα. Η διαφορά με τον πρώτο τρόπο τέλεσης συνίσταται στο γεγονός ότι στην υπό εξέταση περίπτωση η μη ορθή επεξεργασία είναι παροδική, καθώς ο δράστης επεμβαίνει, επηρεάζοντας την διαδικασία επεξεργασίας δεδομένων[98], και αποτρέπει την συναγωγή ορθών συμπερασματικών, καθότι τα δεδομένα που εισάγονται μπορεί να είναι ορθά, όμως η προηγηθείσα παρέμβαση δεν στηρίζεται σε προηγούμενη συγκατάθεση του πραγματικού δικαιούχου / κατόχου[99].

Περίπτωση τέλεσης του εγκλήματος με αυτήν τη μορφή αποτελεί όταν ο δράστης παρεμβαίνει είτε με άλλο πρόγραμμα εισβολέα είτε με άλλον κατάλληλο τεχνικά τρόπο (λ.χ. μέσω των μηχανικών μερών του η/υ[100]) και χρησιμοποιεί χωρίς σχετική άδεια το όνομα χρήστη και τον κωδικό πρόσβασης κάποιου προσώπου ώστε να εισέλθει στον τραπεζικό του λογαριασμό και να μεταφέρει χρήματα σε δικό του λογαριασμό. Τα δεδομένα είναι μεν τα σωστά, ωστόσο το πρόσωπο που τα εισάγει δεν ταυτίζεται με αυτό που αφορούν τα δεδομένα, ούτε έχει λάβει σχετική εξουσιοδότηση από τον πραγματικό δικαιούχο για να πραγματοποιήσει τις διενεργηθείσες συναλλαγές.

---

[98] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, ό.π., σελ. 156

[99] Βλ. Μπουρμάς Γ., σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π., Μπέκας Ι. ο.π. σελ. 414

[100] Βλ. Μπέκας, ο.π., σελ. 415, υποσημ. 383

6.2.3. Χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης ταυτότητας

Ως ήδη αναφέρθηκε, ο ν. 4411/2016 εισήγαγε στο άρθρο 13 στοιχείο ζ' ΠΚ την έννοια του πληροφοριακού συστήματος, το οποίο ορίζεται ως *«η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία»*. Ως εσφαλμένα ή ελαττωματικά δεδομένα θεωρούνται αυτά που δεν αποτυπώνουν την αλήθεια, ενώ ως ελλιπή αυτά που αποτυπώνουν μόνο μέρος αυτής[101], σύμφωνα με το συμφέρον του δράστη που τα εισάγει[102]. Στο μέτρο, λοιπόν, που αυτή η μορφή τέλεσης αναφέρεται σε δεδομένα υπολογιστή, τα οποία με τη σειρά τους αναφέρονται σε παρουσίαση γεγονότων, είναι εμφανής η παραπομπή στην απάτη του άρθρ. 386 ΠΚ όπου γίνεται παράσταση ψευδών γεγονότων ως αληθινών.

Αξίζει να αναφερθεί ότι η απάτη του 386^{A} ΠΚ καταφάσκεται μόνο εάν το αποτέλεσμα των μη ορθών ή ελλιπών δεδομένων αποδίδεται αποκλειστικά μέσα από τη διεργασία των δεδομένων από τον υπολογιστή, χωρίς παρέμβαση στην επεξεργασία από κάποιο πρόσωπο. Στην τελευταία αυτή περίπτωση, εάν δηλαδή παρεμβάλλεται παρέμβαση από πρόσωπο πριν προβεί στην περιουσιακή διάθεση, το οποίο παραπλανάται από τα μη ορθά ή ελλιπή δεδομένα, πρόκειται για απάτη του άρθρ. 386 ΠΚ[103].

Ειδική αναφορά γίνεται στον συγκεκριμένο τρόπο τέλεσης (αναφερόμενος ενδεικτικά – «ιδίως» – και όχι περιοριστικά) για τα δεδομένα αναγνώρισης ταυτότητας. Λαμβάνοντας υπόψη τον ορισμό για τα ψηφιακά δεδομένα, όπως παρατέθηκαν ανωτέρω,

---

[101] ΕφΘεσσ 1177/2008, Ποιν Χρ, σελ. 765 επ., ΑΠ 1059/1955, ΠοινΧρ, 1996, σελ. 97 επ. και ΤριμΕφΚακΑθ 4689/2018, ΠοινΔικ 2020, σελ. 731 (ορ. υποσημ. 120)

[102] Βλ. Μπουρμάς Γ., σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π..

[103] Βλ. Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, ό.π., σελ. 188.

και την έννοια των δεδομένων προσωπικού χαρακτήρα, στα οποία εντάσσονται τα στοιχεία ταυτοποίησης ενός προσώπου, όπως αναφέρεται στον ΓΚΠΔ[104], ως τέτοια νοούνται τα επεξεργάσιμα από υπολογιστή ή άλλο πρόγραμμα δεδομένα τα οποία περιλαμβάνουν και εμφανίζουν πληροφορίες με τις οποίες πραγματοποιείται η ταυτοποίηση κάποιου προσώπου.[105]

6.2.4. Χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας

Η την εν λόγω μορφή τέλεσης αποτελεί αντιστοιχία της περίπτωσης α' του άρθρου 8 της Σύμβασης της Βουδαπέστης, την οποία ενσωμάτωσε ο ν. 4411/2016, όπως ήδη έχει αναφερθεί.

Ο δράστης εν προκειμένω εισάγει στον υπολογιστή (εξωτερικά) εσφαλμένα δεδομένα, τα οποία ο υπολογιστής επεξεργάζεται με τη σωστή μέθοδο, ωστόσο το αποτέλεσμα που παράγεται είναι εσφαλμένο, λόγω των δεδομένων. Για παράδειγμα, κάνοντας χρήση των αναγνωριστικών κωδικών πρόσβασης στο e-banking λογαριασμό κάποιου, το σύστημα, αφότου επεξεργαστεί τα δεδομένα με την διαδικασία, σύμφωνα με την οποία αρχικώς και του προορισμού του διαμορφώθηκε από τον κατασκευαστεί του, θα παράσχει πρόσβαση στον εκάστοτε χρήστη, πλην όμως δίχως κατ' ανάγκη στην πραγματικότητα, το πρόσωπο εκείνου που προέβη στην εισαγωγή των ορθών δεδομένων,

---

[104] Βλ. άρθρ. 4 παρ. 1 ΓΚΠΔ ««δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου».

[105] Βλ. Μπέκας, ο.π., σελ. 415, ενδ. ΑΠ 243/2009, ΠοινΧρ, σελ. 25

να ταυτίζεται με τον κάτοχο του λογαριασμού[106]. Επίσης, ο δράστης μπορεί να αλλοιώνει τα δεδομένα που ήδη υπάρχουν στον υπολογιστή, δηλαδή να τα τροποποιεί χρησιμοποιώντας προς τούτο κάποιο πρόγραμμα κακόβουλου λογισμικού (ransomware[107])[108].

Ως προς τη διαγραφή και την εξάλειψη δεδομένων, η ειδοποιός διαφορά τους έγκειται στο ότι η μεν διαγραφή μπορεί να γίνει χωρίς τη χρήση κακόβουλου προγράμματος, εφόσον συνήθως η συγκεκριμένη δυνατότητα υπάρχει και στον υπολογιστή στον οποίο παρεμβαίνει ο δράστης, ενώ η εξάλειψη γίνεται με τη χρήση τέτοιου λογισμικού, το οποίο αφαιρεί τα δεδομένα από τον ηλεκτρονικό υπολογιστή όπου έχουν αποθηκευτεί.

6.2.5. Χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων

Ο πέμπτος και τελευταίος τρόπος τέλεσης θεωρήθηκε από τον νομοθέτη του ν. 4619/2019 ως απολύτως αναγκαία προσθήκη, προκειμένου να καλυφθούν οι περιπτώσεις όπου οι δράστες ηλεκτρονικής απάτης στοχεύουν στο ηλεκτρονικό – ψηφιακό χρήμα, το

---

[106] Βλ. Μπέκας ο.π., σελ. 415

[107] *Το ransomware είναι ένας τύπος κακόβουλου λογισμικού ή λογισμικού κακόβουλης λειτουργίαςπου απειλεί το θύμα καταστρέφοντας ή εμποδίζοντας την πρόσβαση σε κρίσιμα δεδομένα ή συστήματα έως ότου καταβληθούν λύτρα. Ιστορικά, τα περισσότερα ransomware στόχευαν ιδιώτες, αλλά πιο πρόσφατα, το ανθρώπινα ελεγχόμενο ransomware, το οποίο στοχεύει οργανισμούς, έχει γίνει η μεγαλύτερη και πιο δύσκολη απειλή ως προς την πρόληψη και την κατάργησή της. Με το ransomware με ανθρώπινο έλεγχο, μια ομάδα εισβολέων χρησιμοποιεί τη συλλογική της ευφυΐα για να αποκτήσει πρόσβαση στο εταιρικό δίκτυο ενός οργανισμού. Ορισμένες επιθέσεις αυτού του είδους είναι τόσο εξελιγμένες που οι εισβολείς χρησιμοποιούν εσωτερικά οικονομικά έγγραφα που έχουν αποκαλύψει προκειμένου να ορίσουν την τιμή των λύτρων* (πηγή: https://www.microsoft.com/el-gr/security/business/security-101/what-is-ransomware).

[108] Βλ. Φιλόπουλος Π., Ποινική Προστασία Απορρήτου, ό.π., σελ.182.

οποίο αποτελεί και τον κύριο τρόπο διεξαγωγής των συναλλαγών της σύγχρονης συναλλακτικής εποχής. Συναφώς, με τον τόπο αυτό επιδιώκεται η κάλυψη των περιπτώσεων απάτης μέσω web-banking καθώς και χρήσης κλεμμένης κάρτας αυτόματης συναλλαγής σε ΑΤΜ, η οποία κατά το παρελθόν είχε προκαλέσει έντονη θεωρητική συζήτηση, ως προς την αληθή ποινική της αξιολόγηση[109]. Συγκεκριμένα δε, η άνευ δικαιώματος αξιοποίηση του λογισμικού, αιτιωδώς οδηγεί στον επηρεασμό του ηλεκτρονικού υπολογιστή[110] και στην εξαγωγή εσφαλμένων συμπερασμάτων από την «επηρεασμένη» διαδικασία επεξεργασίας. Δια αυτής (της επεξεργασίας) επιδιώκεται η παράνομη προσπέλαση των ασφαλιστικών δικλείδων τραπεζικού λογαριασμού, ακολούθως η περιουσιακή μετάθεση των κατατεθειμένων σε αυτό, χρημάτων και η συνεπεία αυτής, περιουσιακή ζημία του δικαιούχου του λογαριασμού. Πλην όμως, όπως και στην περίπτωση του άνω αναφερόμενου, υπό στοιχεία 6.2.1., πρώτου προβλεπόμενου τρόπου τέλεσης, η τελική διαπίστωση της τέλεσης απάτης με η/υ και όχι απάτης του άρθρου 386 ΠΚ, εξαρτάται από το εάν ο επηρεασμό του η/υ για τον οποίο γίνεται λόγος αρκεί για την επέλευση του ζημιογόνου αποτελέσματος ή εάν μεσολαβεί φυσικό πρόσωπο που πλανήθηκε από την προηγηθείσα επεξεργασία και τα εσφαλμένα

[109] Βλ. Μπουρμάς Γ., Περαιτέρω προβληματισμοί για την ποινική αξιολόγηση της άνευ δικαιώματος ανάληψης μετρητών από ΑΤΜ και των ηλεκτρονικών τραπεζικών συναλλαγών (web-banking), ΠοινΔικ 2014, σελ. 1111 και Μυλωνόπουλος Χρ, Ποινικό δίκαιο, Ειδικό Μέρος [Εγκλήματα κατά Περιουσιακών Αγαθών, Εγκλήματα κατά της Ιδιοκτησίας (άρθρ. 372-381 ΠΚ), Εγκλήματα κατά της Περιουσίας (άρθρ. 385-405 ΠΚ), Εγκλήματα σχετικά με τα Υπομνήματα (άρθρ. 216-222 ΠΚ)], Νομική Βιβλιοθήκη, εκδ. 2021, σελ. 489 επ.

[110] Σύμφωνα με την νομολογία (ΕφΘεσσ 1177/2008, ΠοινΧρ, σελ. 765), ως επηρεασμός νοείται η σε οποιοδήποτε στάδιο της επεξεργασίας επέμβαση, είτε κατά την εισαγωγή των δεδομένων στον η/υ, είτε κατά τη ροή το προγράμματος, είτε κατά την εκροή, στα μηχανικά μέρη του η/υ, που οδηγεί στην αλλοίωση των δεδομένων και σε αποκλίνον, σε σχέση με το αναμενόμενη από ορθή επεξεργασία, αποτέλεσμα, σε κάθε δε περίπτωση σε μη σύννομη εκτέλεση του προγράμματος

συμπεράσματα, προβαίνοντας το ίδιο σε περιουσιακή διάθεση. Τότε ασφαλώς θα ομιλούμε και πάλι για βασική απάτη[111].

Για τον λόγο αυτόν με τον ν. 4947/2022 προστέθηκε στο άρθρο 13 ΠΚ η περίπτωση η', με την οποία εισάγεται η έννοια του μέσου πληρωμής πλην των μετρητών, και ως τέτοιο θεωρείται ο *«άυλος ή υλικός προστατευμένος μηχανισμός, αντικείμενο ή αρχείο ή συνδυασμός τους, εκτός από το νόμιμο νόμισμα, ο οποίος επιτρέπει, μόνος του ή σε συνδυασμό με διαδικασία ή σειρά διαδικασιών, στον κάτοχο ή στον χρήστη του να μεταφέρει χρήματα ή νομισματική αξία, μεταξύ άλλων, μέσω ψηφιακών μέσων συναλλαγής. Ως «προστατευμένος μηχανισμός, αντικείμενο ή αρχείο» νοείται μηχανισμός, αντικείμενο ή αρχείο που προστατεύεται από την απομίμηση ή δόλια χρήση, για παράδειγμα μέσω σχεδιασμού, κωδικοποίησης ή υπογραφής»*.

6.2.6. Κατασκευή, διάθεση ή κατοχή προγράμματος ή συστήματος υπολογιστή που προορίζεται για τη διάπραξη του εγκλήματος του άρθρ. 386^{A} παρ. 1 ΠΚ

Στη δεύτερη παράγραφο του άρθρου 386^{A} ΠΚ εισήχθη νεοπαγής τυποποίηση ιδιώνυμου εγκλήματος[112], για την κατασκευή, διάθεση ή κατοχή προγράμματος ή συστήματος υπολογιστή προοριζόμενου να χρησιμοποιηθεί για την τέλεση απάτης με υπολογιστή, υπό οποιαδήποτε μορφή από τις ως άνω αναφερθείσες. Με αυτήν τη νομοθετική επιλογή κατέστη σαφές ότι δεν επαρκούσε η διάταξη 292Γ ΠΚ σχετικά με την κατοχή ή διάθεση λογισμικών ή συσκευών που προορίζονται για την τέλεση εγκλημάτων σε βάρος της λειτουργίας πληροφοριακών συστημάτων γενικά.

Με τη δεύτερη παράγραφο έχουμε πλέον διεύρυνση του αξιοποίνου, με την αναγωγή προπαρασκευαστικών πράξεων σε αυτοτελή εγκλήματα, κάτι το οποίο δεν

[111] Μυλωνόπουλος, Τα εγκλήματα της ιδιοκτησίας και της περιουσίας, εκδ. Σάκκουλα, σελ. 1063 και ενδ. ΑΠ 367/2017 ΤΝΠ ΝΟΜΟΣ

[112] Βλ. Μπέκας, ο.π., σελ. 419

υφίσταται ως πρόβλεψη στην περίπτωση της απάτης μέσω υπολογιστή του άρ. 386 ΠΚ, όπως ήδη έχει αναφερθεί. Στην προκείμενη περίπτωση η ποινικοποίηση των προπαρασκευαστικών πράξεων μπορεί να θεωρηθεί δικαιολογημένη, δεδομένου ότι το πρόγραμμα ή ο υπολογιστής *προορίζεται κατά λειτουργικό σκοπό* (π.χ. λόγω κακόβουλου λογισμικού ή άλλων προγραμμάτων εγκατεστημένων σε αυτόν) να εξυπηρετεί την τέλεση ηλεκτρονικής απάτης.

6.3. Η βλάβη

Όπως ήδη αναφέρθηκε ανωτέρω, αποτέλεσμα της συμπεριφοράς του δράστη, η οποία αντιστοιχεί σε έναν από τους ως άνω αναφερόμενους τρόπους τέλεσης, είναι, όχι η παραπλάνηση κάποιου προσώπου, αλλά ο παράνομος επηρεασμός του αποτελέσματος που παράγει και εμφανίζει ο υπολογιστής, δηλαδή θα πρέπει να υπάρχει αιτιώδης σύνδεσμος ανάμεσα στα δύο αυτά μεγέθη. Εν συνεχεία, θα πρέπει να λάβει χώρα η περιουσιακή διάθεση, η οποία γίνεται αποκλειστικά μέσω υπολογιστή, ως άμεσο και αιτιώδες αποτέλεσμα των ανωτέρω δύο, ήτοι της συμπεριφοράς του δράστη και το εσφαλμένο αποτέλεσμα που παρουσιάζει ο υπολογιστής. Τέλος, θα πρέπει να επέλθει η βλάβη στην περιουσία του θύματος, η οποία να είναι επίσης άμεσο και αιτιώδες αποτέλεσμα όλων των προηγούμενων επενεργειών, ήτοι της περιουσιακής διάθεσης και του επηρεασμού των στοιχείων του υπολογιστή από τη συμπεριφορά του δράστη[113].

Εάν, λοιπόν, το επεξεργαστικό αποτέλεσμα δεν οδηγεί άμεσα και αιτιακά στην περιουσιακή διάθεση αλλά μόνο τη διευκολύνει, ώστε ο δράστης εν συνεχεία να προχωρήσει σε άλλες ενέργειες (π.χ. απάτης του 386 ΠΚ[114]), τότε δεν τελείται το έγκλημα του 386^{A} ΠΚ[115].

[113] Βλ. Μπουρμάς Γ., σε Χαραλαμπάκη Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), ό.π., σελ. 1344.

[114] Πρβλ. άνωθεν, ανάλυση της αντικειμενικής υπόστασης αναφορικά με τους υπό στοιχεία 6.2.1. και 6.2.4. τρόπους τέλεσης και στις περιπτώσεις που μεσολαβεί εξαπάτηση φυσικού προσώπου, καθοριστική για την συντέλεση της περιουσιακής διάθεσης και συνακόλουθης βλάβης

6.4. Υποκειμενική υπόσταση

Για το έγκλημα της απάτης με υπολογιστή απαιτείται συνδρομή δόλου οποιουδήποτε βαθμού, όπως και στην απάτη του άρ. 386 ΠΚ, δηλαδή γνώση όλων των στοιχείων την αντικειμενικής υπόστασης και της αιτιακής του σχέσης[116], ο οποίος δε δόλος να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης. Αξίζει να προσεχθεί ότι εν προκειμένω δεν απαιτείται ο δράστης να γνωρίζει την αναλήθεια των στοιχείων που εισάγει ή εκμεταλλεύεται εν γένει, επομένως τιμωρείται και εάν αποδειχθεί ότι γνώριζε ως ενδεχόμενη την περίπτωση να είναι αναληθή και την αποδέχθηκε[117].

Επιπλέον, και η απάτη με υπολογιστή είναι έγκλημα υπερχειλούς υποκειμενικής υπόστασης, καθώς ο δράστης θα πρέπει να έχει σκοπό τον προσπορισμό παράνομου περιουσιακού οφέλους για τον εαυτό του ή τρίτο[118].

6.5. Ποινική κύρωση της απάτης με υπολογιστή

---

[115] Βλ. σχετικώς, Παπαδαμάκη, Τα περιουσιακά εγκλήματα, σελ. 155, σύμφωνα με τον οποίο, προκειμένου να θεωρηθεί η πράξη επηρεασμού δεδομένων υπολογιστή ως απάτη του 386^{A} ΠΚ, απαιτείται ως *οριστικό αποτέλεσμα και να μεταφράζεται σε απώλεια-μετακίνηση περιουσιακών στοιχείων*.

[116] Παπαδαμάκη, Τα περιουσιακά εγκλήματα, σελ. 160

[117] Βλ. Μπέκας, ο.π. σελ. 413, αναφορικά με την ταύτιση της απαιτούμενης υποκειμενικής επικάλυψης μεταξύ του βασικού εγκλήματος της απάτης και του ιδιώνυμου της απάτης με υπολογιστή, πλην όμως, αφορώσα διαφορετικά αντικειμενικά στοιχεία (εν προκειμένω στην απάτη με η/υ, για τις συμπεριφορές που επιδρούν σε αυτό)

[118] Βλ. ενδ. ΑΠ 1087/2019, ΤΝΠ ΝΟΜΟΣ, Παπαδαμάκης Α. Τα περιουσιακά εγκλήματα, σελ. 160

Η απάτη με υπολογιστή τιμωρείται, όπως και η βασική απάτη, σωρευτικά με ποινή φυλάκισης (10 ημέρες έως 5 έτη) και χρηματική ποινή (έως 360 ημερήσιες μονάδες ύψους από 1,00 έως 100,00 Ευρώ εκάστη).

Ομοίως, όσον αφορά τις διακεκριμένες παραλλαγές της πράξης ισχύουν όσα αναφέρθηκαν και παραπάνω στην παρούσα σχετικά με υτές της κοινής απάτης του άρ. 386 ΠΚ, ήτοι: 1) εάν η ζημία υπερβαίνει τις 120.000 Ευρώ, απειλείται πρόσκαιρη κάθειρξη έως 10 έτη και χρηματική ποινή (παρ.1 εδ. τελευταίο) και 2) εάν παθών είναι το Δημόσιο και η ζημία υπερβαίνει τις 120.000 Ευρώ, απειλείται πρόσκαιρη κάθειρξη τουλάχιστον 10 ετών και χρηματική ποινή έως 1.000 ημερήσιες μονάδες (παρ. 3).

Ωστόσο, στην περίπτωση των προνομιούχων παραλλαγών, εντοπίζονται δύο αντί για μία μορφές, ήτοι η περίπτωση του 377 ΠΚ, η οποία ισχύει και για την απάτη του άρ. 386 ΠΚ και αυτή της παραγράφου 2 η οποία αφορά, όπως ήδη αναλύθηκε παραπάνω, τις προπαρασκευαστικές πράξεις, για τις οποίες προβλέπεται φυλάκιση έως 2 έτη και χρηματική ποινή. Η συγκεκριμένη πράξη μπορεί να παραμείνει ατιμώρητη και ο δράστης να απαλλαγεί, εάν καταστρέψει με ίδια θέληση (και όχι π.χ. επειδή έγινε αντιληπτός και επίκειται σε βάρος του άσκηση δίωξης) το πρόγραμμα ή το σύστημα υπολογιστή, πριν προχωρήσει σε χρήση του για την τέλεση της απάτης του 386^{A} ΠΚ.

6.6. Σύγκριση της απάτης μέσω υπολογιστή (386 ΠΚ) και της απάτης με υπολογιστή (386^{A} ΠΚ)

Όπως αναδείχθηκε με ενάργεια από την ανάλυση των δύο διατάξεων, η απάτη μέσω υπολογιστή και η απάτη με υπολογιστή εμφανίζουν σημαντικές ομοιότητες, αλλά διαφορές, σε σημείο να έπρεπε να αποτελούν, σύμφωνα με τον νομοθέτη, διαφορετικό έγκλημα, ιδιώνυμο, βάσει των ως άνω αναπτυχθέντων. Εξάλλου, αυτός είναι ο δικαιολογητικός λόγος που, όπως τονίστηκε, η απάτη με υπολογιστή δεν θεωρείται παραλλαγή του βασικό αδικήματος αλλά ιδιώνυμο έγκλημα, εφόσον προσβάλλει μεν την

περιουσία κατά τρόπο ανάλογο με την απάτη του 386 ΠΚ, πλην όμως δίχως να εμπεριέχει όλα τα στοιχεία αυτής[119].

Βασική διαφορά είναι ο τρόπος της εξαπάτησης του θύματος, καθώς αφενός μεν στην απάτη μέσω υπολογιστή εξακολουθεί να υπάρχει το στοιχείο της επικοινωνίας του δράστη με το θύμα, το οποίο παραπλανάται και προβαίνει στην επιζήμια για την περιουσία του ίδιου ή τρίτου διάθεση[120]. Αντιθέτως, στην απάτη με υπολογιστή δεν υπάρχει επικοινωνία του δράστη με το θύμα, αλλά όλη η συμπεριφορά εκδηλώνεται εντός του περιβάλλοντος του ηλεκτρονικού υπολογιστή και των δεδομένων που είναι ήδη αποθηκευμένα σε αυτόν ή εισάγονται από τον δράστη, δηλαδή αυτό που υφίσταται την «παραπλάνηση» είναι το ίδιο το σύστημα του υπολογιστή, το οποίο καταλήγει σε εσφαλμένα αποτελέσματα κατόπιν επεξεργασίας, εξαιτίας της παρεμβατικής συμπεριφοράς του δράστη[121]. Ακριβώς αυτά τα αποτελέσματα θα πρέπει να αποτελούν την αιτία για την περιουσιακή διάθεση του θύματος, ομοίως πραγματοποιούμενη με υπολογιστή, η οποία με τη σειρά της θα οδηγήσει στη βλάβη της περιουσίας του

[119] Βλ. Μπέκα, ό.π., σελ. 412

[120] Βλ. Ιγγλεζάκης Ι. ο.π., σελ. 405 (658)

[121] Ενδ. ΤριμΕφΚακΑθ 4689/2018, ΠοινΔικ 2020, σελ. 731: *«Το έγκλημα της απάτης με υπολογιστή του άρθρου 386Α τελείται όταν η περιουσιακή βλάβη επέρχεται όχι με την παραπλάνηση ενός φυσικού προσώπου που είναι αρμόδιο να λαμβάνει αποφάσεις ή να διενεργεί έλεγχο ή να εγκρίνει ή να χορηγεί κ.λπ., αλλά αποκλειστικά και μόνο με τον επηρεασμό των στοιχείων του υπολογιστή, δηλαδή με την επέμβαση του δράστη κατά τον προγραμματισμό του συστήματος και την επεξεργασία των δεδομένων, σε οποιαδήποτε φάση της λειτουργίας του υπολογιστή. Έτσι, δεν στοιχειοθετείται κοινή απάτη του άρθρου 386 ΠΚ στην περίπτωση που ο δράστης επεμβαίνει ευθέως στην εξέλιξη του προγράμματος ή και στα μηχανικά μέρη του υπολογιστή και με μη ορθή διαμόρφωση του προγράμματος ή με τη χρησιμοποίηση κατά τον προγραμματισμό του συστήματος μη ορθών ή ελλιπών στοιχείων, προκαλεί αποτέλεσμα διαφορετικό από εκείνο που θα προέκυπτε από τη διαδικασία της επεξεργασίας των στοιχείων και έτσι βλάπτει ξένη περιουσία προς όφελος αυτού ή τρίτου (ΑΠ 367/2017 ΝΟΜΟΣ, ΑΠ 813/2015 ΠοινΧρ 2017, 179).»*

διαθέτοντος ή τρίτου και η αξία της οποίας αποτελεί τον υπερχειλή σκοπό για προσπορισμού παράνομου περιουσιακού οφέλους εκ μέρους του δράστη.[122]

Συνεπώς, προκύπτει ότι η απάτη μέσω υπολογιστή μπορεί να έχει τη μορφή spamming email, το οποίο συνιστά μορφή επικοινωνίας ανάμεσα στον δράστη και το θύμα, όπου το θύμα παραπλανάται από το περιεχόμενο του email (π.χ. ότι κέρδισε κάποιο χρηματικό ποσό, ή πρέπει να επιβεβαιώσει τους κωδικούς του, ή ότι έχει κάποια ειδοποίηση από την τράπεζά του ή άλλη υπηρεσία όπου διατηρεί λογαριασμό) και πατάει τον σύνδεσμο ο οποίος συνοδεύει το email, με αποτέλεσμα να προβαίνει εντός του απατηλού περιβάλλοντος όπου θα οδηγηθεί από τον σύνδεσμο σε περιουσιακή διάθεση. Από την άλλη, πρόκειται για απάτη με υπολογιστή όταν ο δράστης χρησιμοποιεί χωρίς δικαίωμα τραπεζική κάρτα σε ATM για να κάνει αναλήψεις ή μεταφορές, ή σε τερματικό αυτόματων συναλλαγών (POS), επειδή παρεμβαίνει στο ηλεκτρονικό σύστημα ενός υπολογιστή ή στα δεδομένα του.

7. Οι σύγχρονες μέθοδοι και μέσα εξαπάτησης στις ηλεκτρονικές απάτες

7.1. Ηλεκτρονικές και διαδικτυακές απάτες με χρήση κοινωνικής μηχανικής χειραγώγησης – «Ο αστάθμητος ανθρώπινος παράγοντας»

Κατά την επισκόπηση των πρακτικών μορφών εκδήλωσης της εγκληματικής συμπεριφοράς που περιλαμβάνει ως σύνολο τα αδικήματα της απάτης μέσω υπολογιστή και της απάτης με υπολογιστή, η κοινωνική μηχανική, ένας νεωτεριστικός όρος που προκύπτει κατόπιν ακριβούς μετάφρασης από τον αντίστοιχο χρησιμοποιούμενο στην

[122] Βλ. Παπαδαμάκης Α. ο.π., σελ 154 επ.

αγγλική (social engineering), αναδεικνύεται ως μια εκ των πλέον κρίσιμων απειλών της σύγχρονης ψηφιακής εποχής.

Πιο αναλυτικά, η εν λόγω μέθοδος χειραγώγησης, αν και εξετάζεται στην παρούσα εξ αφορμής του συχνότατου εντοπισμού της σε περιστατικά απάτης, έχει απασχολήσει σε επίπεδο επιστημονικής διερεύνησης, το μάρκετινγκ, την ψυχολογία, την κοινωνιολογία και την πολιτική επιστήμη. Εν γένει, έχει διαπιστωθεί ότι χάρη στην κοινωνική μηχανική, δηλαδή στη δόλια εκμετάλλευση των ευάλωτων στοιχείων της ανθρώπινης υπόστασης και των επιμέρους προσωπικοτήτων του κοινωνικού συνόλου ή κάποιου συγκεκριμένου μέρους αυτού, επιδιώκεται η επιμελώς κεκαλυμμένη εξαπάτηση και ιδίως η συντονισμένη και προμελετημένη καθοδήγησή, σε αποφάσεις, ενέργειες και παραλείψεις, συνήθως προς όφελος και καθ' υπόδειξη εκείνου που επιχειρεί την χειραγώγηση. Σύμφωνα με τον Κέβιν Μίτνικ, έναν από τους πρώτους γνωστούς στο ευρύ κοινό, χάκερς, *«Είναι πολύ ευκολότερο να ξεγελάσεις κάποιον στο να σου δώσει έναν κωδικό πρόσβασης για ένα σύστημα παρά να προσπαθήσεις να σπάσεις τον κωδικό»*[123]. Η συγκεκριμένη φράση αποδίδει με τον πλέον γλαφυρό τρόπο τη σημασία του ανθρωπίνου παράγοντα και της αξιοποίησης των αδυναμιών του εκάστοτε θύματος στην περίπτωση της εξαπάτησης με σκοπό την απόσπαση παράνομου περιουσιακού οφέλους[124] . Η ουσία και η επιτυχία της κοινωνικής μηχανικής βασίζεται στις ανθρώπινες αδυναμίες των χειριστών των συστημάτων αυτών, στην παραπλάνηση και εξαπάτησή τους, προκειμένου να αποσπάσουν την πληροφορία και κατ' επέκταση την πρόσβαση. Με άλλα λόγια, μέσω ενός τεχνάσματος ή κάποιας πράξης εξαπάτησης, ένα πρόσωπο οδηγείται στο να κάνει κάτι, που, υπό διαφορετικές συνθήκες, αν δηλαδή εξέλιπε η ως άνω χειραγώγηση, δεν θα έπραττε.

Σε ό,τι αφορά ειδικώς στις απάτες μέσω ή με υπολογιστή, όπου γίνεται χρήση κοινωνικής μηχανικής χειραγώγησης, παρατηρείται ότι αυτή αναπτύσσεται προκειμένου

[123] Βλ. Mitnick K, Η τέχνη της απάτης, ο ανθρώπινος παράγοντας στην ασφάλεια, εκδ. Ωκεανίδα, 2003.

[124] Βλ. Βασιλειάδης Α., «Οι 7 ευπάθειες του ανθρώπου που εκμεταλλεύεται η κοινωνική μηχανική», 05-11-2018, διαθέσιμο στον ιστότοπο: https://cerebrux.net (τελευταία επίσκεψη 01-12-2023).

να αποσπαστούν εμπιστευτικές πληροφορίες οι οποίες είναι απαραίτητες για την πρόσβαση σε υπολογιστικά συστήματα. Στην πράξη λοιπόν, καθίσταται σαφές πως η συγκεκριμένη τεχνική εξαπάτησης δεν περιλαμβάνει ενέργειες παράκαμψης των δικλείδων ασφαλείας ενός συστήματος και μη εξουσιοδοτημένη πρόσβαση σε αυτό, όπως θα ανέμενε κανείς να συμβαίνει όταν γίνεται λόγος για «σπάσιμο» των σύμμετρων κωδικών ασφαλείας. Η παραπάνω μέθοδος, που είναι ευρέως διαδεδομένη ως «χάκινγκ - hacking», έβρισκε κατά γενική ομολογία εφαρμογή κυρίως στην πρώτη περίοδο της τεχνολογικής άνθισης, προς τα τέλη του περασμένου αιώνα και τις αρχές του τρέχοντος, κυρίως διότι, τα τότε υφιστάμενα πληροφοριακά συστήματα παρουσίαζαν σημαντικά κενά ασφαλείας, με συνέπεια να καθίστανται εύκολοι στόχοι.

Τα βήματα προόδου στην κυβερνοασφάλεια επιδιώκουν την ελαχιστοποίηση του πεδίου δράσης επίδοξων και επιδέξιων χάκερς, οι οποίοι έχουν σταδιακά στραφεί σε εναλλακτικές μεθόδους, μια εκ των οποίων είναι και το υπό εξέταση, εργαλείο εξαπάτησης της χειραγώγησης μέσω κοινωνικής μηχανικής. Σε πλήρη αντίθεση με όσα ισχύουν και αναφέρονται παραπάνω για την αθέμιτη, μη εξουσιοδοτημένη παράνομη διείσδυση, κατόπιν παράκαμψης των ψηφιακών μέσων προστασίας, διαπιστώνεται ότι χάρη στην κοινωνική μηχανική, επιτυγχάνεται η ψυχολογική εξάρτηση και υποκίνηση του θύματος να παραχωρήσει τρόπον τινά μια ιδιάζουσα άδεια προς τον θύτη, με θετική του ενέργεια ή δια της παράλειψης του να αντισταθεί σε εξωτερική επέμβαση - όπως θεωρητικά θα αναμενόταν εκ των περιστάσεων να πράξει.

Συναφώς, επισημαίνεται πως η δόλια εκμετάλλευση των ευάλωτων στοιχείων, στην πρώτη περίπτωση ενός συστήματος ασφαλείας και στην δεύτερη, ενός φυσικού, προσώπου, συνιστά το βασικό σημείο τομής και παραλληλισμού των δύο αυτών παράνομων συμπεριφορών. Έχει διαπιστωθεί πως οι βασικές αδυναμίες των ανθρώπων, που αφορούν την ψυχική τους κατάσταση, είναι ενδεικτικά η συμπόνια, η απληστία, ο φόβος και η περιέργεια για το άγνωστο, το δέος ενώπιον κάποιας φαινομενικά ανώτερης αρχής ή του αξιώματος, η μη επίδειξη της δέουσας προσοχής και η ανετοιμότητα ως προς την ορθολογική διαχείριση μιας πιεστικής κατάστασης.

7.2. Συνήθεις τεχνικές εξαπάτησης με χρήση κοινωνικής μηχανικής

Όπως αναδείχθηκε παραπάνω, η αποτελεσματικότητα ή μη της επιδιωχθείσας μέσω των τεχνικών της κοινωνικής μηχανικής χειραγώγησης εξαρτάται απολύτως από τον βαθμό εμπιστοσύνης που επιτυγχάνεται μεταξύ θύματος και θύτη, καθώς και την προθυμία του πρώτου, να αποκαλύψει ευαίσθητες πληροφορίες, μοναδικούς κωδικούς, προσωπικά στοιχεία και διαπιστευτήρια σύνδεσης, ή σε κάθε περίπτωση, να καθοδηγηθεί τεχνηέντως σε πράξεις ή παραλείψεις, δυνητικά βλαπτικές για την περιουσία του [125]. Το υπό εξέταση φαινόμενο, όπως προκύπτει από πρόσφατες μελέτες, βρίσκεται σε πλήρη ακμή και σε συνεχή εξέλιξη των μορφών που, κατά την συνήθη πρακτική, έχει παρατηρηθεί να εκλαμβάνει[126]. Αξίζει να σημειωθεί ότι τα σύγχρονα συστήματα, ακόμη και όσα χρησιμοποιούμε στην καθημερινότητα μας, όπως ένας κοινός browser (φυλλομετρητής – πρόγραμμα περιήγησης) ή ο πάροχος του ηλεκτρονικού μας ταχυδρομείου, ειδοποιούν τον χρήστη καθώς διαθέτουν σχετικά αποτελεσματικούς μηχανισμούς ανίχνευσης κακόβουλων μηνυμάτων ή λογισμικού, όπως για παράδειγμα η γνωστή αυτόματη καταχώρισης ύποπτων μηνυμάτων, στον «κάδο» των ανεπιθύμητων (spams), εντούτοις, όπως αποδεικνύεται από την προφανή επικράτηση των σχετικών εγκληματικών πρακτικών, ο τελικός κριτής και ο πλέον κρίσιμος παράγοντας, ήταν και παραμένει ο άνθρωπος[127].

---

[125] Βλ. Lohani S., "Social Engineering: Hacking into Humans", International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 2019, διαθέσιμο στον ιστότοπο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391 (τελευταία επίσκεψη 01-12-2023).

[126] Βλ. Chaganti R. / Bhushan B. / Nayyar A. / Mourade A., "Recent trends in social engineering scams and case study of gift card scam", Cornell University, 31-10-2021, διαθέσιμο στον ιστότοπο https://arxiv.org/pdf/2110.06487.pdf (τελευταία επίσκεψη 01-12-2023).

[127] Βλ. McKay J, "*DeFi-ing Cyber Attacks*: A statistical analysis of cybersecurity attacks in decentralized finance", 27-04-2022, διαθέσιμο στον ιστότοπο https://tellingstorieswithdata.com/inputs/pdfs/final_paper-2022-jack_mckay.pdf (τελευταία επίσκεψη 01-12-2023).

Εν προκειμένω, με βάση τα υφιστάμενα στοιχεία[128], το phishing, ή αλλιώς ηλεκτρονικό ψάρεμα, παρουσιάζεται ως ο πλέον διαδομένος τρόπος εφαρμογής της κοινωνικής μηχανικής επί σκοπώ χειραγώγησης και εξαπάτησης του θύματος, παρά το γεγονός ότι στις μέρες τόσο τα πληροφοριακά συστήματα όσο και τα άτομα που τα χρησιμοποιούν καθημερινά, είναι εξαιρετικά ενημερωμένα και θεωρητικά τουλάχιστον, υποψιασμένα. Η τεχνική αυτή, βασίζεται συνήθως στην αποστολή μηνυμάτων spam ή στην δημιουργία ενός ιστοτόπου με παραπλανητικές πληροφορίες. Στην περίπτωση δε, που η ιστοσελίδα για την οποία γίνεται λόγος συνιστά απομίμηση μιας γνήσιας ιστοσελίδας, για παράδειγμα κάποιας εταιρείας ή ενός οργανισμού, έχει επικρατήσει ο όρος pharming. Η μαζικότητα με την οποία λειτουργεί το φαινόμενο, καταδεικνύει πως αφορά γενικά περιπτώσεις, δίχως κάποια διάκριση ή συγκεκριμένη στόχευση ως προς την ανεύρεση ευάλωτου στόχου.

Με ανάλογο τρόπο λειτουργεί και η τεχνική του δολώματος, κατά την αγγλική λέξη «baiting», όπου και πάλι μέσω κακόβουλων και παραπλανητικών μηνυμάτων, ή ακόμη και με συμβατικό τρόπο και την ταχυδρομική αποστολή ενός μολυσμένου με υιό, δίσκου usb, ο δράστης της απατηλής συμπεριφοράς υπόσχεται στο θύμα, κάποιο χρηματικό έπαθλο σε διαγωνισμό, δωρεάν πρόσβαση (gift card) σε κάποια συνδρομητική πλατφόρμα ψηφιακού περιεχομένου (Netflix, Spotify, Amazon), ως αντάλλαγμα για μια σειρά από εμπιστευτικές προσωπικές πληροφορίες, οι οποίες είτε παρέχονται απευθείας από το ίδιο το θύμα, σε κάποια ιστοσελίδα όπου ανακατευθύνθηκε μέσω του παραπλανητικού μηνύματος, είτε χάρη στην εγκατάσταση κακόβουλου λογισμικού.

Περαιτέρω, ειδικότερη μορφή ψαρέματος, τυγχάνει το λεγόμενο spear phishing, όπου ακριβώς επιχειρείται, και πάλι μέσω της αποστολής μηνυμάτων, η πραγματοποίηση στοχευμένων - και όχι μαζικών, όπως στην πρώτη περίπτωση - επιθέσεων είτε εις βάρος

[128] Βλ. επίσημα στοιχεία: Federal Bureau of Investigation, Internet Crime Report, 2021, διαθέσιμο στον ιστότοπο https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (τελευταία επίσκεψη 01-12-2023), Τσίγκανου Ι., «Η στατιστική αποτύπωση του εγκληματικού φαινομένου στη σύγχρονη Ελλάδα», 11/2016, διαθέσιμο στον ιστότοπο https://theartofcrime.gr/η-στατιστική-αποτύπωση-του-εγκληματι/ (τελευταία επίσκεψη 01-12-2023).

φυσικών προσώπων, είτε εις βάρος οργανισμών και επιχειρήσεων[129]. Η διαφορά της συγκεκριμένης τεχνικής, η οποία φανερώνει και την πλήρη αξιοποίηση του εργαλείου της κοινωνικής μηχανικής, έγκειται στο γεγονός ότι, προ της αποστολής του μηνύματος, προηγείται έρευνα του υποψήφιου θύματος και κυρίως των λεπτομερειών για την οικογένεια, την εργασία του, τις συνήθειες του και εν γένει για των στοιχείων της προσωπικότητάς του που το καθιστούν ευάλωτο[130]. Η συγκεκριμένη μορφή πρόκλησης πλάνης με σκοπό την εξαπάτηση και την περιουσιακή βλάβη, συνήθως εκδηλώνεται με υποσχέσεις για καταβολή ενός τεράστιου χρηματικού ποσού, σε αντάλλαγμα με κάποιες κρίσιμες πληροφορίες. Οι κρισιμότεροι παράγοντες της ανθρώπινης υπόστασης που διευκολύνουν τέτοιες πρακτικές, είναι, ενόψει όσων επισημάνθηκαν παραπάνω, είναι η απληστία και η απροσεξία του υποψήφιου θύματος.

Η ίδια ως άνω περιγραφόμενη λογική προσέγγιση των στοχευμένων επιθέσεων, εφαρμόζεται και στην τεχνική χειραγώγησης που φέρει την ονομασία water holing[131]. Η ονομασία που έχει δοθεί, συνιστά μεταφορά μιας πραγματικής κατάστασης, κατά την οποία τα αρπακτικά πουλιά «παραμονεύουν» σε σημεία όπου πηγάζει ή εκβάλει το νερό, προκειμένου να επιτεθούν στα θηράματά τους. Τα βασικά στοιχεία που εντοπίζουμε στην συγκεκριμένη τεχνική είναι η σε βάθος μελέτη των ιδιαίτερων χαρακτηριστικών της προσωπικότητας του υποψήφιου στόχου, αξιοποιώντας συνήθως μεθόδους ανίχνευσης της καθημερινής ψηφιακής του δραστηριότητας και ιδίως της συχνότητας με την οποία επισκέπτεται συγκεκριμένους ιστοτόπους. Με αυτό τον τρόπο, η πράξη εξαπάτησης, η οποία συνήθως επιδιώκεται μέσω κακόβουλου λογισμικού εγκατεστημένου στις

[129] Βλ. Butavicius M. / Parsons K. / Pattinson M. / McCormac A., "Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails", Australasian Conference on Information Systems, Cornell University, 2015.

[130] Βλ. Chetioui K. / Bah B. / Alami A. / Bahnasse A., "Overview of social engineering attacks on social networks", Procedia Computer Science vol. 198, 2022, σελ. 656-661.

[131] Βλ. Ismail, K. A./ Singh, M. M. / Mustaffa, N. / Keikhosrokiani, P. / Zulkefli, Z., "Security strategies for hindering watering hole cybercrime attack", Procedia Computer Science, vol. 124, 2017, σελ. 656–663.

ιστοσελίδες ενδιαφέροντος, στηρίζεται στην προηγηθείσα έρευνα και στην κατά μια έννοια σκιαγράφηση του προφίλ του θύματος και των τυχόν ευάλωτων σημείων του.

Από όλες τις περιπτώσεις που αναφέρθηκαν συνάγεται πως η πράξη εξαπάτησης και η συνεπεία αυτής πρόκληση πλάνη στην απάτη μέσω υπολογιστή επέρχεται χάρη στις τεχνικές της κοινωνικής μηχανικής, της στόχευσης στην απληστία και την περιέργεια του παραλήπτη και κυρίως χάρη στις δελεαστικές υποσχέσεις που φέρονται ότι του παρέχονται. Μια εξίσου συνήθης πρακτική – τέχνασμα των δραστών είναι η πρόκληση στο θύμα συναισθημάτων αναστάτωσης, ανησυχίας, άγχους και φόβου, που και πάλι επιδιώκεται μέσω γραπτών μηνυμάτων (email, sms, social media messenger apps). Η ειδοποιός διαφορά σε σχέση με τις παραπάνω αναφερόμενες μεθόδους χειραγώγησης εντοπίζεται στο περιεχόμενο των μηνυμάτων αυτών, όπου αυτή τη φορά, δεν πρόκειται για μια δήθεν παροχή αλλά για κάποιον φερόμενο κίνδυνο που αντιμετωπίζει το θύμα.

Όπως παρατηρούμε από παρόμοιες επιθέσεις που λαμβάνουν χώρα, το απατηλό μήνυμα αναφέρει ότι δήθεν έχει ανασταλεί προσωρινά η ισχύς κάποιας τραπεζικής κάρτας ή ότι έχουν διενεργηθεί «ύποπτες» τραπεζικές συναλλαγές από τον λογαριασμό e-banking του θύματος, ζητώντας από τον αποδέκτη του μηνύματος να ακολουθήσει κάποιους συνδέσμους ή βήματα επαλήθευσης και ταυτοποίησης, όπου συνήθως είτε απαιτείται η παροχή κρίσιμων πληροφοριών και ιδίως των μοναδικών κωδικών είτε εγκαθίσταται κακόβουλο λογισμικό (ransomware) στην συσκευή του χρήστη, μάλιστα εντός πιεστικού για τον παραλήπτη, χρονικού πλαισίου, με στόχο ασφαλώς να μειωθεί ο διαθέσιμος χρόνος αντίδρασης και ενδελεχούς εξέτασης της γνησιότητας του μηνύματος. Στην ουσία λοιπόν, πρόκειται για μια τραγική ειρωνεία, καθότι η πράξη εξαπάτησης εκδηλώνεται με την ψευδή παράσταση ενός δήθεν επικείμενου κινδύνου, ο οποίος όχι μόνο δεν υφίσταται στην πραγματικότητα αλλά έτι περαιτέρω «καραδοκεί» και εξυπηρετείται από το ίδιο το παραπλανητικά προειδοποιητικό μήνυμα.

Περαιτέρω, προκειμένου να προκληθεί, με την μέγιστη δυνατή αποτελεσματικότητα, η επιδιωκόμενη κατάσταση πλάνης στο θύμα, με σκοπό ακολούθως εκείνο να προβεί ή σε κάθε περίπτωση να επιτρέψει την περιουσιακή διάθεση, ιδιαιτέρως κρίσιμη παράμετρος είναι οι τεχνικές λεπτομέρειες, τα εξωτερικά χαρακτηριστικά του μηνύματος και ο βαθμός αξιοπιστίας που φέρονται αυτά να του

προσδίδουν. Επιπλέον, έχει παρατηρηθεί ότι η πράξη εξαπάτησης, όπως κι αν αρχικώς εκδηλώνεται κατά την αρχική προσέγγιση του θύματος επιχειρείται να υποστηριχθεί ως προς το κύρος της με κάποιο τηλεφώνημα ή φωνητικό μήνυμα προερχόμενο από πρόσωπο, είτε υπαρκτό είτε μηχανικά κατασκευασμένο με την μέθοδο των deepfakes[132], που δηλώνει μια ψεύτικη ταυτότητα, εκπροσώπου εταιρείας, κρατικού οργανισμού ή υπαλλήλου τεχνικής υποστήριξης, αποβλέποντας να εξασφαλίσει την εμπιστοσύνη του θύματος, το οποίο σαφώς επηρεάζεται εν γένει από προηγούμενα σχετικά του βιώματα[133].

Οι επιθέσεις ηλεκτρονικού ψαρέματος, οι οποίες αξιοποιούν τεχνικές κοινωνικής μηχανικής για την χειραγώγηση των εκάστοτε θυμάτων τους, δεν περιορίζονται σε όσα αναφέρθηκαν ανωτέρω στο παρόν εκπόνημα. Από την ίδια την φύση του ηλεκτρονικού οικονομικού εγκλήματος και κυρίως την ιδιότητά να εκδηλώνεται συνήθως με παράνομες μεθόδους, κατά κύριο λόγο, άγνωστες και μη αντιληπτές στον απλό χρήστη, αναδεικνύεται ότι η πληροφόρηση που διατηρούμε, αν και συνεχώς εμπλουτίζεται, χαρακτηρίζεται ως ανεπαρκής και συνήθως, μη ενημερωμένη ως προς τις τελευταίες εξελίξεις. Μόνο εκ του γεγονότος ότι παρατηρείται προοδευτική προσαρμογή των τεχνικών phishing, τόσο στην αυξανόμενη επαγρύπνηση των χρηστών όσο και στις δικλείδες ασφαλείας των σύγχρονων πληροφοριακών συστημάτων, συμπεραίνουμε πως ο κίνδυνος είναι άμεσος και ουδόλως αμελητέος ως προς την σοβαρότητά του.

7.3. Η ηλεκτρονική τραπεζική απάτη (μέσω internet banking) και τα φαινόμενα «phishing» και «pharming» ως μορφές ηλεκτρονικής απάτης

[132] Βλ. Frankovits G., Mirsky Y., "The Threat of Real Time Deepfakes", Cornell University, 04-06-2023, διαθέσιμο στον ιστότοπο https://arxiv.org/pdf/2306.02487.pdf (τελευταία επίσκεψη 01-12-2023).

[133] Βλ. Mouton, F. / Leenen, L. / Venter, H. S., "Social engineering attack examples, templates and scenarios" Computers & Security, vl. 59, 2016, σελ. 186–209.

Όπως έχει ήδη γίνει λόγος στο πλαίσιο της παρούσας εργασίας, η μετατόπιση του ενδιαφέροντος της συναλλακτικής καθημερινότητας από την παραδοσιακή, της εκ του σύνεγγυς διενέργειας, σταδιακά προς την εξ αποστάσεως μορφή της, με χρήση των εργαλείων της τεχνολογίας και της πληροφορικής, έχει αναδειχθεί ως η πλέον σημαίνουσα παράμετρος της σύγχρονης οικονομίας[134]. Το εμπόριο, τόσο εντός όσο και εκτός συνόρων, κατόπιν και των αναπόδραστων συνεπειών της παρατεταμένης περιόδου της παγκόσμιας πανδημίας ανέπτυξε μηχανισμούς «άμυνας και επιβίωσης», κυρίως αξιοποιώντας την ηλεκτρονική τραπεζική. Κατά τον ίδιο τρόπο, ο καθένας από εμάς, ανεξαρτήτως ηλικίας και επιπέδου τεχνολογικής κατάρτισης, οδηγήθηκε - μέχρι ενός σημείου βιαίως - στην προσαρμογή του στα νέα δεδομένα και κυρίως στην εξοικείωσή του με τραπεζικές συναλλαγές, μέσω ιστοσελίδων τραπεζικών ιδρυμάτων, γνωστότερων με την ονομασία internet, web ή online banking ή των αντίστοιχων εφαρμογών (applications ή εν συντομία apps) για «έξυπνα τηλέφωνα»[135].

Ακολούθως, σύμφωνα με στοιχεία της Τράπεζας της Ελλάδος, τα οποία έχουν αναδημοσιευτεί στον ηλεκτρονικό τύπο[136], το 2021, δηλαδή κατά το χρονικό σημείο έξαρσης της πανδημίας και του κατ' οίκον περιορισμού, τα περιστατικά, τα οποία εν συνόλω χάριν συντομίας, χαρακτηρίζονται ως ηλεκτρονικές απάτες και εκδηλώθηκαν με χρήση εφαρμογών και ιστοσελίδων για μεταφορών ψηφιακών μονάδων αξίας (χρημάτων) από λογαριασμό σε λογαριασμό, σημείωσαν ραγδαία αύξηση, κατά ποσοστό

[134] Βλ. Μπώλος Α., «Ηλεκτρονική τραπεζική απάτη - Κατανομή κινδύνου και βάρος απόδειξης», ΧρονΙΔ, 2023, σελ. 90 επ.

[135] Βλ. Στεργίου Λ., «Το ebanking ήρθε για να μείνει», 20-02-2021, διαθέσιμο στον ιστότοπο https://www.capital.gr/oikonomia/3527107/to-ebanking-irthe-gia-na-meinei/ (τελευταία επίσκεψη 01-12-2023), του ίδιου, «Οι πελάτες του ebanking ξεπέρασαν τα τραπεζικά καταστήματα», 09-02-2021, διαθέσιμο στον ιστότοπο https://www.capital.gr/epixeiriseis/3524226/oi-pelates-tou-ebanking-xeperasan-ta-trapezika-katastimata/ (τελευταία επίσκεψη 01-12-2023).

[136] Βλ. Τζώρτζη Ε., «Ηλεκτρονικές απάτες: Πώς και πότε θα δίνουν αποζημίωση οι τράπεζες», Καθημερινή, 26-01-2023, διαθέσιμο στον ιστότοπο https://www.kathimerini.gr/economy/562247020/ilektronikes-apates-pos-kai-pote-tha-dinoyn-apozimiosi-oi-trapezes/ (τελευταία επίσκεψη 01-12-2023).

609% και κατά 320%, ως προς το συνολικό οικονομικό τους αποτύπωμα, το οποίο ασφαλώς μεταφράζεται σε ζημία, σε σχέση με τα στοιχεία που είχαν καταγραφεί την προηγούμενη περίοδο[137].

Στα πλαίσια αυτά, αξίζει να αναφέρουμε πως η ορολογία phishing, που συνηθίζεται να χρησιμοποιείται ευρέως προκειμένου να περιγραφούν οι σύγχρονες μορφές απατηλής πρόκλησης περιουσιακής βλάβης, ιδίως στις τραπεζικές συναλλαγές, έχει προκύψει, κατά παράφραση - εν είδη λογοπαιγνίου - της αγγλικής λέξης fishing, η οποία σημαίνει ψάρεμα[138]. Λαμβάνοντας δε, υπόψη όλα όσα αναφέρθηκαν παραπάνω σε σχέση με τις παραμέτρους της ανθρώπινης ψυχολογίας που χειραγωγούν και εκμεταλλεύονται για εγκληματικό όφελος, καθίσταται σαφές ότι η λεκτική αυτή αναλογία και αναφορά σε αυτή τη συμβατική δραστηριότητα υποδηλώνει ακριβώς ότι οι εγκληματίες του κυβερνοχώρου, δρουν κατ' τρόπο παρόμοιο με τους αλιείς[139].

Ειδικότερα, η κρίσιμη για την περιουσιακή βλάβη πράξη εξαπάτησης των υποψήφιων θυμάτων είναι εξαιρετικά περίπλοκο να καθοριστεί με ακρίβεια, παρά μόνο περιπτωσιολογικά, καθότι από την πράξη έχει προκύψει ότι παρουσιάζει μια ευρύτατη ποικιλία εξωτερικών χαρακτηριστικών και γνωρισμάτων, εξαιτίας της ευρηματικότητας των εγκληματικών πρακτικών και των τεχνικών χειραγώγησης. Ενδεικτικά, όπως αναφέρεται από τον Ευ. Μαργαρίτη[140], οι δυο πιο συνηθισμένες περιπτώσεις παράνομων

---

[137] Συγκεκριμένα, σύμφωνα με το άρθρο (βλ. υποσημείωση αμέσως παραπάνω) καταγράφηκαν *«8.365 περιστατικά απάτης συνολικής αξίας 26,3 εκατ. ευρώ, σε σχέση με τα 1.179 περιστατικά, συνολικής αξίας 6,2 εκατ. ευρώ το 2020».*

[138] Βλ. Κιούπης Δ., Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, εκδ. Νομική Βιβλιοθήκη, 2010, σελ. 201.

[139] Βλ. Βασιλάκη Ε., «Τα φαινόμενα Phishing, Pharming και η ποινική τους αξιολόγηση», ΠοινΧρ ΝΖ/2007, σελ. 860 επ., Μεταξάκης Ε., Η ποινική αντιμετώπιση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (επ' αφορμή της ΠραξΑρχειοθΕισΠρΑθ της 2.3.2013), ΠοινΔικ, Τεύχος 8-9/2015, Αύγουστος-Σεπτέμβριος, Νομοθεσία, Νομολογία, Θεωρία & Πράξη του Ποινικού Δικαίου, σελ. 681 επ.

[140] Βλ. Μαργαρίτης Ε., «Casum sentit dominus? - Οι νέες ρυθμίσεις για την ευθύνη των Τραπεζών σε περίπτωση Phishing», ΤΝΠ QUALEX, ΣΥΝήΓΟΡΟΣ, 155/2023, σελ. 32 - 36

πρακτικών phishing εκδηλώνονται είτε με μήνυμα που καλεί τον χρήστη δήθεν να επιβεβαιώσει τα στοιχεία του, καταχωρίζοντας τους κωδικούς του σε κάποια πλαστή σελίδα στην οποία έχει κατευθυνθεί μέσω ενός συνημμένου στο μήνυμα υπερσυνδέσμου (hyperlink)[141] είτε με μήνυμα που τον ειδοποιεί να προβεί σε τροποποίηση των κωδικών του, επειδή δήθεν εντοπίστηκε και απετράπη κάποια επιχειρούμενου παραβίαση.

Περαιτέρω, όπως άλλωστε συμβαίνει και στην περίπτωση της κοινής απάτης, με συμβατικά μέσα εξαπάτησης, καθοριστικό ρόλο για την τεχνική αλίευσης προσωπικών δεδομένων στο διαδίκτυο, διαδραματίζει, η πλάνη του προσώπου, το οποίο εν τέλει είναι ο φορέας του εννόμου αγαθού ή ελέγχει εν πάση περιπτώσει την κρίσιμη περιουσιακή μετάθεση. Σκοπός του δράστη είναι να παρουσιάσει στο θύμα μια ψευδή απεικόνιση της πραγματικότητας, προκειμένου το τελευταίο, ενεργώντας κατά την πεπλανημένη αντίληψή του αυτοβούλως και πάντοτε υπό την προσχεδιασμένη καθοδήγησή του πρώτου, να προβεί στην αποκάλυψη εμπιστευτικών πληροφοριών, χάρη στις οποίες διενεργούν μη εξουσιοδοτημένες και άρα παράνομες, ηλεκτρονικές συναλλαγές (σύμμετροι κωδικοί πρόσβασης σε σύστημα internet - banking, αριθμοί πιστωτικών καρτών, PIN) ή αποβλέπουν εν γένει στην υφαρπαγή του ψηφιακού αποτυπώματος της ταυτότητας ενός ατόμου (identity theft), αξιοποιώντας αναγνωριστικά στοιχεία, όπως οι κωδικοί taxisnet[142].

Ένα μεγάλο ποσοστό περιστατικών ηλεκτρονικής τραπεζικής απάτης με την τεχνική της αθέμιτης αλίευσης δεδομένων (phishing) συνυπάρχει με μια άλλη, συναφή μέθοδο εξαπάτησης που καλείται pharming, η οποία αποδίδεται στα ελληνικά ως η δόλια

[141] Πρβλ. στην συνέχεια το σημείο που επεξηγεί την τεχνική εξαπάτησης «pharming».

[142] Βλ. Τσιπτσέ Σ., «Ηλεκτρονικό ψάρεμα ή αλλιώς phishing ή αλλιώς… διαδικτυακή απάτη», 16-02-2023, διαθέσιμο στον ιστότοπο https://finupnews.gr/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CF%88%CE%AC%CF%81%CE%B5%CE%BC%CE%B1-%CE%AE-%CE%B1%CE%BB%CE%BB%CE%B9%CF%8E%CF%82-phishing-%CE%AE-%CE%B1%CE%BB%CE%BB%CE%B9%CF%8E%CF%82/ (τελευταία επίσκεψη 01-12-2023).

εκτροπή ιστοτόπων [143] . Στην πράξη, η υφαρπαγή των κωδικών ή εν γένει των εμπιστευτικών πληροφοριών, εν προκειμένω, πρακτικά επιτυγχάνεται χάρη στην καλόπιστη παραχώρησή τους από τον ίδιο τον φορέα τους. Η μεθοδολογία των δραστών απαιτεί σαφώς ιδιαίτερα προηγμένες γνώσεις τεχνολογίας, καθότι σε πρώτο στάδιο καταρτίζουν ιστοσελίδες που σε μεγάλο βαθμό ομοιάζουν με τους αντίστοιχους ιστοτόπους συστημάτων ηλεκτρονικής τραπεζικής συναλλαγής. Συγκεκριμένα, με παράνομη διείσδυση στο λογισμικό της συσκευής του θύματος, συνήθως με hacking ήτοι με τη χρήση κακόβουλου λογισμικού, ο δράστης παρεμβαίνει στο σύστημα του υπολογιστή του θύματος και τροποποιεί εν αγνοία του κρίσιμες ρυθμίσεις, προκειμένου όταν το θύμα πληκτρολογεί στην γραμμή αναζήτησης του φυλλομετρητή (broswer) την διεύθυνση της αυθεντικής ιστοσελίδας (domain name), να ανακατευθύνεται στην πλαστή, όπου ακριβώς αναμένεται να παραπλανηθεί από το περιεχόμενο, να παράσχει τους κωδικούς του και να προχωρήσει στην επιζήμια περιουσιακή διάθεση[144].

Η παρέμβαση του δράστη στο σύστημα του υπολογιστή του θύματος, ώστε αυτό να ανακατευθύνεται στις κακόβουλες ιστοσελίδες που επιθυμεί ο δράστης, γίνεται με παρέμβαση τον τοπικό διακομιστή DNS. Λόγω, λοιπόν, του ότι η παρέμβαση πραγματοποιείται με μόλυνση της μνήμης DNS, καθώς προγραμματίζεται να ανακατευθύνεται στις απατηλές ιστοσελίδες, ο δράστης τιμωρείται για την πράξη του άρθρ. 370Β ΠΚ περί παράνομης πρόσβασης σε σύστημα πληροφοριών.

Με αμφότερους τους τρόπους, δηλαδή με πρακτική «phishing» και «pharming» ο δράστης επιδιώκει να παραπλανήσει το θύμα για να προβεί σε περιουσιακή διάθεση και να προσπορίσει ο δράστης εν συνεχεία το παράνομο περιουσιακό όφελος από τη ζημία που θα υποστεί το θύμα. Ωστόσο, προκύπτει ότι η περιουσιακή διάθεση δεν είναι το άμεσο απότοκο της παραπλανητικής συμπεριφοράς του δράστη, διότι είναι σύνηθες ο τελευταίος να αποκτά τα στοιχεία που χρειάζεται (π.χ. κωδικούς internet banking), τα οποία ο ίδιος χρησιμοποιεί σε κάποια πλατφόρμα (π.χ. τράπεζας) και κάνει την περιουσιακή διάθεση προς τον εαυτό του ή τρίτο. Για τον λόγο αυτόν υπάρχει

[143] Βλ. Βασιλάκη Ε., «Τα φαινόμενα Phishing, Pharming και η ποινική τους αξιολόγηση», ό.π.

[144] Βλ. Αρκούλη Κ., Προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, Νομική Βιβλιοθήκη, 2010, σελ. 11-12.

διχογνωμία κατά πόσο περιπτώσεις που συνίστανται στα ανωτέρω πραγματικά περιστατικά μπορούν να θεωρηθούν απάτη του άρθρ. 386 ΠΚ.

Σύμφωνα με τη γερμανική θεωρία, έχουν αναπτυχθεί δύο διαφορετικές γνώμες[145], η πρώτη εκ των οποίων απορρίπτει τον χαρακτηρισμό της πράξης ως απάτης κατά την έννοια του άρθρ. 386 ΠΚ, διότι αφενός μεν ο δράστης δεν είναι βέβαιο ότι θα χρησιμοποιήσει τα υποκλαπέντα στοιχεία του θύματος, αφετέρου η υποκλοπή των στοιχείων αυτών, εφόσον μόνη δεν μπορεί να οδηγήσει στην περιουσιακή διάθεση, αποτελεί ανεπίτρεπτη διεύρυνση του αξιοποίνου, αναγάγοντας σε αυτοτελές έγκλημα προπαρασκευαστική πράξη.

Κατά την αντίθετη γνώμη, η μέθοδος «phishing» εντάσσεται στη νομοτυπική μορφή της απάτης, δεδομένου ότι με την απόκτηση από τον δράστη των στοιχείων του θύματος, έχει ξεκινήσει σε βάρος του εννόμου αγαθού της περιουσίας του θύματος μία αυτοδύναμη πορεία προς τη βλάβη, η οποία μπορεί να επέλθει ανά πάσα στιγμή σύμφωνα με την εγκληματική διάθεση του δράστη. Το ότι απαιτούνται περισσότερες πράξεις για να επέλθει το εγκληματικό αποτέλεσμα δεν σημαίνει ότι διαρρηγνύεται ο αιτιώδης σύνδεσμος που απαιτείται ανάμεσα στη συμπεριφορά και τη διάθεση και εν συνεχεία βλάβη, δεδομένου ότι το έγκλημα μπορεί απλώς να χαρακτηριστεί πολύπρακτο, όπως συμβαίνει και με άλλες εγκληματικές συμπεριφορές.

Κατά την άποψη του γράφοντος ορθότερη κρίνεται η δεύτερη άποψη, ότι οι μέθοδοι «phishing» και «pharming» είναι μορφές απάτης μέσω ή με υπολογιστή (ανάλογα με τα πραγματικά περιστατικά), διότι στην πραγματικότητα ο δράστης έχει αποφασίσει να χρησιμοποιήσει τα στοιχεία που υπέκλεψε κατά τους παραπάνω τρόπους, γι' αυτό άλλωστε προέβη και στο σύνολο των ενεργειών που οδήγησαν στην υποκλοπή τους. Η παράνομη παρέμβαση στο σύστημα του υπολογιστή, η κατασκευή απατηλής ιστοσελίδας ή η αποστολή του email με τον απατηλό σύνδεσμο αποτελούν μέρος της

[145] Βλ. Βασιλάκη Ε., «Τα φαινόμενα Phishing, Pharming και η ποινική τους αξιολόγηση», ό.π.

συνολικής σχεδιασμένης εγκληματικής δράσης από την οποία ο δράστης προσδοκά το παράνομο περιουσιακό όφελος[146].

Αξίζει να τεθεί στην παρούσα ο προβληματισμός σχετικά με το αν υπάρχει αρχή εκτέλεσης, και άρα απόπειρα απάτης μέσω υπολογιστή, στην περίπτωση που ο δράστης αποστείλει email με απατηλό σύνδεσμο στο πλαίσιο τέλεσης απάτης με τη μορφή «phishing», ωστόσο το email αυτό αρχειοθετείται αυτόματα από τον υπολογιστή του θύματος στην κατηγορία «spam» και το θύμα δεν λαμβάνει τελικά ποτέ γνώση του περιεχομένου του. Εδώ τίθεται ζήτημα ερμηνείας του εύρους του όρου «επικοινωνία» η οποία απαιτείται για να λάβει χώρα η παράσταση των ψευδών γεγονότων ως αληθών. Εάν δεχθούμε ότι για να υπάρξει επικοινωνία θα πρέπει το μήνυμα που αποστέλλει ο πομπός να φτάσει και να γίνει αντιληπτό από τον δέκτη, τότε δεν συντρέχει αυτό το στοιχείο στην προκείμενη περίπτωση και άρα δεν υπάρχει καν απόπειρα απάτης, εάν όμως δεχθούμε ότι αρκεί να αποσταλεί το μήνυμα από τον πομπό διότι θα μπορούσε να λάβει γνώση αυτού οποτεδήποτε ο δέκτης (καθώς πρόκειται για γραπτό μήνυμα το οποίο ενέχει έναν βαθμό μονιμότητας αποτύπωσής του στον φορέα, σε αντίθεση με την προφορική παράσταση ψευδών γεγονότων), τότε υπάρχει έστω αρχή εκτέλεσης της παραπλάνησης και άρα στοιχειοθετείται, εφόσον συντρέχει και η απαραίτητη υποκειμενική υπόσταση, απόπειρα του εγκλήματος.

7.4. Οι «ρομαντικές απάτες»

Όπως είναι ευρέως γνωστό, η ταχύτατη τεχνολογική πρόοδος έχει συνδεθεί άρρηκτα με την εξάπλωση της δημοφιλίας των μέσων κοινωνικής δικτύωσης όπως είναι το Facebook, το Instagram, το Twitter, το TikTok και άλλα[147]. Ανάμεσα στις πλείστες δυνατότητες που παρέχουν στους χρήστες τους συμπεριλαμβάνεται και η επιλογή

[146] Βλ. και Βασιλάκη Ε., «Τα φαινόμενα Phishing, Pharming και η ποινική τους αξιολόγηση», ό.π.

[147] Βλ. Finkel E. J. / Eastwick P. W./ Karney B. R. / Reis H. T. / Sprecher S., "Online dating. Psychological Science in the Public Interest", 2012, vol. 13(1), σελ. 3–66.

δωρεάν πρόσβασης σε ψηφιακά «δωμάτια» συνομιλίας, κυρίως με σύνδεση στο διαδίκτυο (chatrooms), όπου πέραν της απλής επικοινωνίας, συνεννόησης και ανταλλαγής απόψεων, δίδεται η ευκαιρία προσέγγισης συντρόφων, δηλαδή ακριβώς για αναζήτηση και δημιουργία ρομαντικής σχέσης με άτομα από διαφορετικά μέρη του κόσμου.

Οι διαδικτυακές γνωριμίες τυγχάνουν σήμερα, χωρίς την παραμικρή προκατάληψη, κοινωνικά αποδεκτές και αποτελούν ίσως κανόνα, ιδιαιτέρως για τις νεότερες γενιές, οι οποίες είναι σαφώς πιο εξοικειωμένες. Η ανάγκη των σύγχρονων ανθρώπων για «εύκολη» ρομαντική προσέγγιση, χωρίς να απαιτείται καν η ελάχιστη εκ του σύνεγγυς προσωπική αλληλεπίδραση, αναδεικνύεται έτι περαιτέρω από την γέννησης της ιδέας για την δημιουργία και την θέση σε μαζική ψηφιακή κυκλοφορία, της κατά κάποιον τρόπο, μετεξέλιξης των παραπάνω κοινωνικών δικτύων, εξειδικευμένων σε υπηρεσίες διαδικτυακής αλληλεπίδρασης με αποκλειστικό σκοπό των χρηστών, την εξεύρεση συντρόφου, οι οποίες είναι οι γνωστές εφαρμογές γνωριμιών. Οι ειδικοί της ψυχικής υγείας έχουν πολλάκις κρούσει τον κώδωνα του κινδύνου, αφενός για την αλλοτρίωση και τον σταδιακό εκφυλισμό της ανθρώπινης επαφής και των διαπροσωπικών σχέσεων, αφετέρου δε, ιδιαιτέρως πρόσφατα, έχουν εκφραστεί ανησυχίες, όχι μόνο για την αποτελεσματικότητα και την ασφάλεια τους αλλά έτι περαιτέρω και για τις επιπτώσεις στην αυτοπεποίθηση και την ψυχική τους κατάσταση [148]. Ως εκ τούτου, τα θύματα της συγκεκριμένης μορφής εκδήλωσης της απατηλής συμπεριφοράς, εξαιτίας ακριβώς του γεγονότος ότι, όπως θα αναδειχθεί στην συνέχεια, πείθονται κινούμενα κυρίως από τον απατηλό συναισθηματικό δεσμό, όχι μόνο υποφέρουν από αρνητικά συναισθήματα όπως κατάθλιψη, αμηχανία, θυμό και φόβο[149], που ασφαλώς επηρεάζουν και τις μετέπειτα διαπροσωπικές τους σχέσεις, αλλά μπορούν να καταλήξουν θύματα απάτης με σημαντική περιουσιακή ζημίας εις βάρος τους.

---

[148]Βλ. αρθρογραφία της συντακτικής ομάδας της ιστοσελίδας *the school of life*, με τίτλο «*WHY DATING APPS WON'T HELP YOU FIND LOVE»* https://www.theschooloflife.com/article/why-dating-apps-wont-help-you-find-love/ (τελευταία επίσκεψη 01-12-2023).

[149] Βλ. Buchanan T. / Whitty M. T., "The online dating romance scam: Causes and consequences of victimhood", Psychology, Crime & Law, 2014, 20 (3), σελ. 261–283.

Η αμιγώς ψηφιακή αλληλεπίδραση έχει αναπότρεπτα διευρύνει το πλαίσιο για εγκλήματα στον κυβερνοχώρο, όπως είναι για παράδειγμα, η «ρομαντική απάτη»[150]. Σε πρώτο επίπεδο και με γνώμονα την κατανόηση του ζητήματος, είναι ιδιαιτέρως χρήσιμο να εξετάσουμε τον τρόπο εκδήλωσης της εγκληματικής συμπεριφοράς που περιλαμβάνει τον εντοπισμό και την προσέγγιση των θυμάτων, καθώς επίσης και μια σειρά προπαρασκευαστικών ενεργειών των δραστών. Ειδικότερα, όπως έχει παρατηρηθεί ως μοτίβο στις περιπτώσεις αυτές, το πλέον κρίσιμο στοιχείο των δραστών τέτοιου είδους απάτης είναι πρωτίστως η απόκρυψη των αληθινών προσωπικών τους στοιχείων, αξιοποιώντας στο έπακρο την δυνατότητα ανωνυμίας που τους εξασφαλίζει η περιήγηση στο διαδίκτυο και οι διάφορες εφαρμογές γνωριμιών. Κατά, την συνήθη πρακτική των εγκληματιών αυτών, συνήθως επιλέγουν να παρουσιάζουν στα υποψήφια θύματα τους μια επινοημένη ή κλεμμένη από άλλους ανυποψίαστους χρήστες, κυρίως των μέσων κοινωνικής δικτύωσης, «γοητευτική» ταυτότητα και κατά κύριο λόγο αποβλέπουν στην προσέγγιση ευάλωτων και μοναχικών ανθρώπων που αναζητούν την συντροφικότητα[151], με τους οποίους επιθυμούν δήθεν να δημιουργήσουν σχέση.

Οι δράστες της ρομαντικής απάτης επιδιώκουν να δημιουργήσουν κλίμα εμπιστοσύνης και ασφάλειας στα δυνητικά θύματά τους, μέσω μιας ρομαντικής προσέγγισης και υπόσχεσης κάθε τύπου δέσμευσης ή σχέσης[152]. Αυτό συνήθως το πετυχαίνουν, εφόσον προηγουμένως έχουν φροντίσει, με ιδιαίτερη επιμέλεια ούτως ώστε, τα προφίλ τους, αφενός να δείχνουν απολύτως πιστευτά - σαν να επρόκειτο για πραγματικά– αφετέρου δε, να καθρεπτίζουν μια πολυδάπανη και πολυτελή ζωή ενός

[150] Κατά μετάφραση του αγγλικού όρου romance scams ή άλλως απάτες catfishing.

[151] Βλ. Buchanan T. / Whitty M. T., "The online dating romance scam: Causes and consequences of victimhood", ό.π..

[152] Βλ. Lazarus S. / Whittaker J. M. / McGuire M. R. /Platt L., "What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021)" Journal of Economic Criminology, 2, 2023.

ατόμου αξιόπιστου και κυρίως «υπεράνω πάσης υποψίας»[153]. Ο απλουστευμένος τρόπος λειτουργίας των εφαρμογών αυτών στηρίζεται κατά μείζονα λόγο στην δύναμη της εικόνας, και ειδικότερα στην εντύπωση που μπορεί να προκαλέσει στον χρήστη μια «προσεγμένη» φωτογραφική απεικόνιση με ενδείξεις πλούτου, ακριβών αυτοκινήτων, ρούχων, ταξιδιών κλπ.. Ακόμη, δεν αποκλείεται το ενδεχόμενο και κατ' ιδίαν συναντήσεων – ρομαντικών ραντεβού, για να στηριχθεί ακόμη περισσότερο το ψευδές αφήγημα της δήθεν σχέσης. Όταν ο δράστης επιτύχει στο πρώτο αυτό στάδιο του επιδιωκόμενου, κατ' επίφαση συναισθηματικού δεσμού, ακολούθως αναμένει την κατάλληλη ευκαιρία ή ακόμη, επινοεί μια αφορμή, ένα περιστατικό ή εν γένει ένα λόγο να ζητήσει από το θύμα χρήματα, πάντοτε με την μορφή δανείου και ως προσωρινή διευκόλυνση.

Επιπλέον, ενδέχεται να παρουσιάσει μια πιεστική κατάσταση, συνήθως αφορώσα επείγον ζήτημα υγείας ή προσωρινής οικονομικής αδυναμίας, προκειμένου να παραπλανήσει το θύμα εκμεταλλευόμενος τον συναισθηματικό του δεσμό με τον ίδιο, είτε να παρέχει πρόσβαση στους λογαριασμούς του, είτε ακόμη και να δημιουργήσει κοινό τραπεζικό λογαριασμό. Μάλιστα, συχνά παρατηρείται ότι τέτοιοι τραπεζικοί λογαριασμοί χρησιμοποιούνται από τον δράστη της ρομαντικής απάτης για νομιμοποίηση εσόδων από άλλες εγκληματικές δραστηριότητες. Βέβαια, σε μια τέτοια περίπτωση το θύμα της ρομαντικής απάτης δεν μπορεί να θεωρηθεί συμμέτοχος ή συνεργός του δράστη, καθώς εκλείπει η συνδρομή στο πρόσωπό του του αναγκαίου δόλου.

Επί τη βάσει όλων των παραπάνω, συμπεραίνουμε ότι η δόλια εκμετάλλευση για προσπορισμό παράνομου περιουσιακού οφέλους, ενός επίπλαστου ερωτικού δεσμού και της συναισθητικής εξάρτησης που αυτός συνεπάγεται, συνιστά περίπτωση κοινωνικής μηχανικής χειραγώγησης του θύματος. Ως προς την ποινική απαξία της εν λόγω συμπεριφοράς, με ασφάλεια μπορεί κανείς να ισχυριστεί ότι πρόκειται για κοινή απάτη μέσω υπολογιστή και όχι για απάτη με υπολογιστή, δεδομένου ότι μέσω υπολογιστή

[153] Βλ. Kopp C. / Layton R. / Sillitoe J. / Gondal I., "The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles", International Journal of Cyber Criminology Vol 9 Issue 2 July – December 2015, σελ. 205 - 217.

γίνεται η προσέγγιση του θύματος, με την πραγματοποίηση επικοινωνίας και την παράσταση ψευδών γεγονότων ως αληθών. Άλλωστε, σε κάθε περίπτωση, ο πλανηθείς είναι φυσικό πρόσωπο, το οποίο ενόψει των συνεπειών της πλάνης που προκλήθηκε εξαιτίας της πίστης του ότι διατηρεί, μια ανύπαρκτη στην πραγματικότητα, συναισθητική σχέση, οδηγήθηκε αιτιωδώς στο να προβεί σε περιουσιακή διάθεση εις βάρος της περιουσίας του και προς όφελος του δράστη.

Σε ό,τι αφορά ειδικότερα τα διάφορα στάδια διαδικτυακής ερωτικής αναζήτησης, γνωριμίας και συναναστροφής μεταξύ θύτη και θύματος, με σαφή συναισθηματική χειραγώγηση του δεύτερου από τον πρώτο, προκύπτει ότι η πλάνη πηγάζει μεν από την ολικά ψευδή πεποίθηση περί ύπαρξης ενός ειλικρινούς συναισθηματικού δεσμού, ωστόσο η προσβολή της περιουσίας, ήτοι η περιουσιακή διάθεση, εδράζεται κυρίως στην πλάνη που δημιουργήθηκε ενόψει μιας συγκεκριμένη, επίσης ψευδούς και σκηνοθετημένης αφορμής περί οικονομικής αδυναμίας του δράστη. Επομένως οι προηγούμενες ενέργειες του εκάστοτε δράστη, που κατατείνουν ασφαλώς στο να κερδίσουν εν γένει την εμπιστοσύνη του θύματος και να κάμψουν, κάποια ενδεχόμενη καχυποψία του, συνιστούν προπαρασκευαστικές πράξεις, ενώ η πράξη εξαπάτησης και η συνεπεία αυτής πλάνη του θύματος που οδηγεί αιτιωδώς στην προσβολή της περιουσίας του, συνιστούν με την σειρά τους, την αξιόποινη απατηλή συμπεριφορά.

7.5. Η τέλεση ηλεκτρονικής απάτης με εργαλείο τα κρυπτονομίσματα

Ζήτημα διχογνωμίας αποτελεί στην επιστήμη εάν είναι δυνατό να χρησιμοποιηθούν τα κρυπτονομίσματα ως μέσο για τη διάπραξη απάτης και συγκεκριμένα της απάτης – πυραμίδας (ponzi scheme).

Αρχικά, θα πρέπει να διευκρινιστεί εν συντομία τι ακριβώς είναι τα κρυπτονομίσματα, τα οποία θα μπορούσαν να οριστούν ως *«ψηφιακά νομισματικά συστήματα και συστήματα πληρωμών που υπάρχουν στο Διαδίκτυο μέσω*

αποκεντρωμένων, κατανεμημένων δικτύων που χρησιμοποιούν μια κοινή τεχνολογία δεδομένων που είναι γνωστή ως blockchain σε συνδυασμό με ασφαλή κρυπτογράφηση»[154].

Συναφώς, η Ε.Ε. στο πλαίσιο του Κανονισμού MiCA «για τις αγορές κρυπτοστοιχείων και την τροποποίηση της οδηγίας (ΕΕ) 2019/1937» ο οποίος θα εφαρμοστεί εντός του 2024, αναφέρεται στα κρυπτονομίσματα ως «κρυπτοστοιχεία» και τα ορίζει ως *«ψηφιακή αναπαράσταση αξίας ή δικαιωμάτων που μπορούν να μεταβιβαστούν και να αποθηκευτούν ηλεκτρονικά, με χρήση τεχνολογίας κατανεμημένου καθολικού ή παρόμοιας τεχνολογίας»*. Ιδιαίτερα γνωστά κρυπτονομίσματα αποτελούν το Bitcoin και το Ethereum.

Τα κρυπτονομίσματα είναι εξαιρετικά δημοφιλές μέσο αναπαράστασης αξίας, δεδομένου ότι μέχρι σήμερα δεν έχουν τεθεί υπό κρατική εποπτεία και η αυξομείωση της αξίας του στηρίζεται στον κανόνα της αγοράς περί προσφοράς και ζήτησης[155], ενώ παρέχουν σημαντικό βαθμό ανωνυμίας στον κάτοχο – χρήστη τους ως προς τα στοιχεία της ταυτότητάς του, διότι η χρήση μπορεί να γίνει και με ψευδώνυμο. Ωστόσο, στο σύστημα του blockchain αποτυπώνεται κατά τρόπο μόνιμο κάθε συναλλαγή που πραγματοποιείται με κάθε μονάδα (ή μέρος αυτής) κρυπτονομίσματος, με αποτέλεσμα η ανωνυμία να είναι μόνο φαινομενική[156].

Ενόψει των ανωτέρω πλεονεκτημάτων που παρουσιάζουν τα κρυπτονομίσματα, συχνά γίνονται αντικείμενα για την τέλεση διάφορων εγκληματικών πράξεων, όπως την αγορά παράνομων αγαθών ή υπηρεσιών στο dark web, όπου γίνονται δεκτές πληρωμές σε κρυπτονομίσματα π.χ. αγορά ναρκωτικών ουσιών ή όπλων.

---

[154] Βλ. Hayes S., "Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin", Telematics and Informatics, 13-05-2016, σελ. 1308.

[155] Βλ. Bloomenthal A., "What Determines the Price of 1 Bitcoin?", 16-06-2020, διαθέσιμο στα αγγλικά στην ιστοσελίδα https://www.investopedia.com/tech/what-determines-value-1-bitcoin/#citation-1 (τελευταία επίσκεψη 03-12-2023).

[156] Βδοκάκη Μ., Κρυπτονομίσματα στην Ελλάδα και τον κόσμο - Νομολογιακές εξελίξεις και καθημερινές πρακτικές, ΣΥΝ, 151/2022, σελ. 72 – 75 και Παρασκευοπούλου-Κόλλια Μ., Εικονικά νομίσματα – κρυπτονομίσματα , ΠοινΔικ, 11/2022, σελ. 1507-1521

Τώρα, όσον αφορά τη χρήση τους για την τέλεση τριγωνικής απάτης, σημαντικό είναι να αναφερθεί ότι τέτοιου είδους απάτη τελείται όταν ένα αξιόγραφο εμφανίζεται ψευδώς να είναι μεγάλης αξίας, με σκοπό να προσελκύσει καινούρια πρόσωπα τα οποία θα επενδύσουν σε αυτό, θεωρώντας πεπλανημένα ότι πρόκειται για μεγάλη επιχειρηματική – επενδυτική ευκαιρία[157]. Η εν λόγω εντύπωση δημιουργείται επειδή τα χρήματα που έχουν καταβάλει οι νεότεροι επενδυτές δίνονται ως δήθεν κέρδη στους προηγούμενους, ώστε να φαίνεται ότι το αξιόγραφο είναι επικερδές. Έτσι, δημιουργείται ένας κύκλος, βάσει του οποίου τα χρήματα των εξαπατηθέντων επενδυτών δίνονται στους προηγούμενους, επίσης εξαπατηθέντες, επενδυτές, κάτι το οποίο συντηρεί την πλάνη τους, ενώ στην πραγματικότητα πρόκειται για «φούσκα». Όσο ο κύκλος αυτός διευρύνεται, τόσο μεγαλύτερο ποσό συγκεντρώνεται στα χέρια των δραστών, οι οποίοι μπορούν ανά πάσα στιγμή να αποσύρουν το ποσό αυτό και να εξαφανιστούν, προκαλώντας στους επενδυτές αντίστοιχη με την καταβολή που πραγματοποίησαν περιουσιακή ζημία.

Σύμφωνα με μία γνώμη, στο παραπάνω σχήμα δεν είναι δυνατό να αντικατασταθούν τα αξιόγραφα από τα κρυπτονομίσματα, διότι το σύστημά τους είναι εξολοκλήρου και εξ ορισμού αποκεντρωμένο και οι συναλλαγές γίνονται με διαφάνεια. Εφόσον λοιπόν δεν υπάρχει κάποιος διαχειριστής ή διενεργών έλεγχο, δεν είναι εφικτό να τελεστεί απάτη[158]. Σύμφωνα με την ίδια άποψη, τα κρυπτονομίσματα δεν δομούνται σε σχήμα πυραμίδας, καθώς οποιοσδήποτε κάτοχος κρυπτονομίσματος μπορεί να αποκομίσει κέρδος εάν το πουλήσει σε υψηλότερη τιμή, όπως με κάθε άλλο αγαθό της αγοράς, χωρίς να χρειάζεται να πείσει τον αγοραστή για αυτό.

Βέβαια, η εν λόγω άποψη δεν ανταποκρίνεται στην αληθή εγκληματική πρακτική, καθώς ήδη έχουν υπάρξει απάτες ponzi με αντικείμενο κρυπτονομίσματα, ιδίως κατά τα

[157] Βλ. Bartoletti M. / Carta S. / Cimoli T. / Saia R., “Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact”, Future Generation Computer Systems 102, 2020, σελ. 259–277.

[158] Βλ. Granot Er'el, “On the Origin of the Value of Cryptocurrencies”, 2018, διαθέσιμο στον ιστότοπο https://www.intechopen.com/books/blockchain-and-cryptocurrencies/onthe-origin-of-the-value-of-cryptocurrencies (τελευταία επίσκεψη 03-12-2023).

πρώτα έτη εμφάνισής τους, οπότε και δεν υπήρχε ουδεμία θεσμική πρόβλεψη για αυτά. Τα κρυπτονομίσματα προς το παρόν θεωρούνται, και φορολογούνται σε κάποια κράτη, ως επενδυτικό προϊόν, συνεπώς η απάτη μέσω υπολογιστή είναι εφικτή να διαπραχθεί, όταν ο δράστης παριστάνει ψευδώς ότι κάποιο κρυπτονόμισμα αποτελεί σοβαρή επενδυτική ευκαιρία και το θύμα προβαίνει σε περιουσιακή (χρηματική) διάθεση για να αγοράσει ποσότητα από αυτό.

8. Συμπεράσματα – Παρατηρήσεις

Σύμφωνα με το σύνολο όσων διαμείφθηκαν στην παρούσα, προκύπτει ότι η ηλεκτρονική εγκληματικότητα ακολουθεί κατά πόδας την εξάπλωση της τεχνολογίας και των ψηφιακών εργαλείων, τα οποία εδραιώνονται για την πραγματοποίηση συναλλαγών στην καθημερινότητα όλων. Η ηλεκτρονική απάτη μέσω υπολογιστή και με υπολογιστή, όπως οι εγκληματικές αυτές πράξεις αναλύθηκαν παραπάνω, αποτελούν συχνό φαινόμενο προκαλώντας σημαντική περιουσιακή βλάβη στα θύματα και διαταράσσοντας την ασφάλεια των συναλλαγών εν γένει.

Ο ελληνικός Ποινικός Κώδικας έχει κάνει σημαντικές προσπάθειες από το 1988 έως σήμερα για τη θέσπιση διατάξεων που θα προστατεύουν με τον πληρέστερο δυνατό τρόπο το έννομο αγαθό της περιουσίας από εγκληματικές συμπεριφορές απάτης με τη χρήση των νέων τεχνολογιών, ανταποκρινόμενος και στις υποχρεώσεις του από την Ε.Ε..

Η ποικιλομορφία και η ευελιξία του ηλεκτρονικού εγκλήματος, όπως αναδείχθηκε και αποτυπώθηκε στο σύνολο της παρούσας εργασίας, είναι σαφές ότι επιβάλλει επαγρύπνηση σε επίπεδο νομοθετικής παρέμβασης αλλά και τον σταδιακό εκσυγχρονισμό των παραδοσιακών δραστηριοτήτων και μέσων επιβολής του νόμου, με νέα εξελιγμένα και προσαρμοσμένα εργαλεία. Ιδίως δε, κρίνεται σκόπιμο, πέραν της ανάπτυξης κατάλληλων ασφαλιστικών δικλείδων, να δοθεί η δέουσα προσοχή στο πεδίο της δημιουργίας δομών συνεργασίας μεταξύ των διαφόρων ενδιαφερόμενων μερών, μιας συνεκτικής προσέγγισης και ενός στρατηγικού πλαισίου για την κοινοτική πολιτική με

γνώμονα πάντοτε την αποτελεσματική αντιμετώπιση και στο μέτρο του δυνατού, καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Μια πρόταση που κερδίζει ολοένα και περισσότερο έδαφος ανάμεσα στους θεωρητικούς της επιστήμης και προκρίνεται και από τον συντάξαντα την παρούσα μελέτη, είναι η έγκριση ενιαίων νομοθετικών μέτρων κοινού χαρακτήρα σε ευρωπαϊκό επίπεδο καθώς και η συγκρότηση νέων εξειδικευμένων στον έλεγχο του Κυβερνοεγκλήματος, οργανισμών σε επίπεδο Ευρωπαϊκής Ένωσης. Σε κάθε περίπτωση πάντως, διαπιστώνεται, ένεκα και της συνεχούς και σε κάποιες περιπτώσεις ανεξέλεγκτης εξέλιξης του φαινομένου, ότι με σχετική βεβαιότητα προβλέπεται η ανάγκη μελέτης των στατιστικών δεικτών των περιπτώσεων τέλεσης της ηλεκτρονικής απάτης, ιδίως εντός του Διαδικτύου, καθώς και των μορφών που αυτή κάθε φορά εκλαμβάνει.

Βιβλιογραφία – Αρθρογραφία

Ελληνική

Αγγελής Ι., «Διαδίκτυο (Internet) και ποινικό δίκαιο / Έγκλημα στον Κυβερνοχώρο (Cybercrime – Internet crime)», ΠοινΧρ Ν/2000, σελ. 676 επ.

Αγγελής Ι., Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ΠοινΔικ 2001, σελ. 1218 επ.

Αγγελής Ι., Διαδίκτυο (Internet) και ποινικό δίκαιο, ΠοινΧρ 2000, 675 επ.

Αγγελής Ι. Το νομικό πλαίσιο για την ασφάλεια στον Κυβερνοχώρο κατά το ελληνικό ποινικό δίκαιο, ΠοινΔικ. 2001, 1293 επ.

Αποστολίδου Α, Απάτη - Η πλάνη ως αποτέλεσμα πράξης εξαπάτησης και η Περιουσιακή Διάθεση στο Έγκλημα της Απάτης. Εκδόσεις Αντ. Ν. Σάκκουλα, 2000

Βαγενά Ε. Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεργκλήματος, ΔίΜΕΕ 2017

Βασιλάκη Ε., Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, εκδ. Αντ. Ν. Σάκκουλας, 1993.

Βασιλάκη Ε., «Τα φαινόμενα Phishing, Pharming και η ποινική τους αξιολόγηση», ΠοινΧρ ΝΖ/2007, σελ. 860 επ

Βασιλειάδης Α., «Οι 7 ευπάθειες του ανθρώπου που εκμεταλλεύεται η κοινωνική μηχανική», 05-11-2018, https://cerebrux.net (τελευταία επίσκεψη 01-12-2023).

Βδοκάκη Μ., Κρυπτονομίσματα στην Ελλάδα και τον κόσμο - Νομολογιακές εξελίξεις και καθημερινές πρακτικές, ΤΝΠ QUALEX ΣΥΝ, 151/2022, σελ. 72 - 75

Βλαχόπουλος Κ., Ηλεκτρονικό Έγκλημα: Μορφές, Πρόληψη, Αντιμετώπιση, εκδ. Νομική Βιβλιοθήκη, 2007.

Βρούστης Χ, Προβληματισμοί επί της διεύρυνσης της κατ' έγκληση δίωξης των εγκλημάτων κατά περιουσιακών εννόμων αγαθών, ΠοινΧρον 2021, 161

Δαλακούρας Θ. (επιμ.), Ηλεκτρονικό Έγκλημα, εκδ. 1η, Νομική Βιβλιοθήκη, 2019

Δαλακούρας Θ. (επίμ.), Ηλεκτρονικό Έγκλημα, εκδ. 2η, Νομική Βιβλιοθήκη, 2023

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

Δημόπουλος Χ., Εγκληματολογική, Αστυνομική & Δικανική Ανακριτική, εκδ. Νομική Βιβλιοθήκη, 2021.

Επίσημη ιστοσελίδα του Συμβουλίου της ΕΕ, "Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products", 30-11-2023, https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/#:~:text=Main%20objectives%20of%20the%20new,legislation%20in%20EU%20member%20states. (τελευταία επίσκεψη 01-12-2023).

Ζήσης Α. Ποινικός Κώδικας. Εκδ. Σάκκουλα, 2022

Ιγγλεζάκης Ι., Δίκαιο Πληροφορικής, εκδ Δ΄, Α.Ν. Σάκκουλα, 2018.

Ιγγλεζάκης Ι (επιμ.), Δίκαιο Πληροφορικής & Διαδικτύου, (Σύγχρονη Νομοθεσία/Βασική Εμπορική Νομοθεσία) 4η εκδ., Εκδόσεις Σάκκουλα, 2023,

Καϊάφα - Γκμπάντι Μ, «Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής», Αρμ 2007, σελ. 1061 επ.

Κιούπης Δ., Ποινικό Δίκαιο και Internet, εκδ. Αντ. Ν. Σάκκουλα, 1999.

Κιούπης Δ., Ο τόπος τέλεσης του διαδικτυακού εγκλήματος και η απροσδόκητη διεύρυνσης της έννοιας της ημεδαπής (άρθρο 5 παρ. 3 ΠΚ), ΠοινΧρ 2014, σελ. 561 επ.

Κιούπης Δ., Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, εκδ. Νομική Βιβλιοθήκη, 2010, σελ. 201

Κιούπης Δ, Εγκλήματα κατά της ιδιοκτησίας και της περιουσίας. Η διεύρυνση του καταλόγου των κατ' έγκληση διωκομένων εγκλημάτων. Πρακτικές λύσεις και θεωρητικά θεμέλια, διαθέσιμο σε: https://theartofcrime.gr

Κονταξής Αθ., Ποινικός Κώδικας, Τόμος Β΄, Έκδοση Γ΄, Αθήνα, 2000

Κουράκης Ν., Το οικονομικό έγκλημα στην Ελλάδα σήμερα, ΠοινΔικ, 6/2000, σελ. 644 - 654

Κωσταρά Α. Ποινικό δίκαιο (επιλογές ειδικού μέρους), δ΄ έκδοση, 2020, Νομική Βιβλιοθήκη, σελ. 571 επ.

Λάζος Γ., Πληροφορική & έγκλημα, 2001

Μανωλεδάκης Ι., Ποινικό Δίκαιο: άρθρα 1 – 50 ΠΚ, εκδ. Α.Ν. Σάκκουλα, 2005.

Μαργαρίτης Ευ., Casum sentit dominus? - Οι νέες ρυθμίσεις για την ευθύνη των Τραπεζών σε περίπτωση Phishing, ΤΝΠ QUALEX ΣΥΝ, 155/2023, σελ. 32 – 36

Μαργαρίτης Μιχ, Ποινικός Κώδικας, 2η Έκδοση 2009,Δίκαιο & Οικονομία Εκδόσεις Π.Ν. Σάκκουλα

Μαργαρίτης Λ. Περιουσιακά εγκλήματα και τρόπος διώξεώς τους (ΜΕΡΟΣ Α΄), ΤΝΠ QUALEX ΠοινΔικ, 5/2021, σελ. 672 – 681

Μεταξάκης Ε., Η ποινική αντιμετώπιση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (επ' αφορμή της ΠραξΑρχειοθΕισΠρΑθ της 2.3.2013), ΠοινΔικ, Τεύχος 8-9/2015, Αύγουστος-Σεπτέμβριος, Νομοθεσία, Νομολογία, Θεωρία & Πράξη του Ποινικού Δικαίου, σελ. 681 επ.

Μπουρμάς Γ., Περαιτέρω προβληματισμοί για την ποινική αξιολόγηση της άνευ δικαιώματος ανάληψης μετρητών από ΑΤΜ και των ηλεκτρονικών τραπεζικών συναλλαγών (web-banking), ΠοινΔικ 2014, σελ. 1111

Μπώλος Α., «Ηλεκτρονική τραπεζική απάτη - Κατανομή κινδύνου και βάρος απόδειξης», ΧρονΙΔ, 2023, σελ. 90 επ.

Μυλωνόπουλος Χρ., Ποινικό δίκαιο – Ειδικό μέρος, εκδόσεις Σάκκουλα, 2006

Μυλωνόπουλος Χρ. Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, εκδ. Π.Ν. Σάκκουλας Δίκαιο και Οικονομία, 2006.

Μυλωνόπουλος Χρ., Ειδικό μέρος - Εγκλήματα κατά της ιδιοκτησίας (άρθρα 372-384 ΠΚ), εγκλήματα κατά της περιουσίας (άρθρα 385-406Α ΠΚ), εγκλήματα περί τα υπομνήματα (άρθρα 216-223ΠΚ), εκδ. 3η Π.Ν. Σάκκουλας, 2016

Μυλωνόπουλος Χρ, Ποινικό δίκαιο, Ειδικό Μέρος [Εγκλήματα κατά Περιουσιακών Αγαθών, Εγκλήματα κατά της Ιδιοκτησίας (άρθρ. 372-381 ΠΚ), Εγκλήματα κατά της Περιουσίας (άρθρ. 385-405 ΠΚ), Εγκλήματα σχετικά με τα Υπομνήματα (άρθρ. 216-222 ΠΚ)], Νομική Βιβλιοθήκη, εκδ. 2021

Μυλωνόπουλος Χρ. Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, Εκδόσεις Σάκκουλα, 1991.

Νούσκαλης Γ., «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», ΠοινΔικ 2/2003, σελ. 178 επ.

Παπαδαμάκης Α. Τα περιουσιακά εγκλήματα, άρθρα 385 – 405 ΠΚ. Εκδόσεις Σάκκουλα, δ΄ έκδοση 2022,

Παπαδαμάκης Α., Τα περιουσιακά εγκλήματα, εκδ. Α.Ν. Σάκκουλα, 2000

Παπαδαμάκης Α., Πρόσφατες νομολογιακές διακυμάσεις και ερμηνευτικές εκτροπές στα εγκλήματα της απάτης και της απιστίας, Ποινική Δικαιοσύνη, Τεύχος 4-5, Νομική Βιβλιοθήκη, 2012

Παπαθανασίου, Α. / Γέρμανος, Γ. Εξέλιξη και ανάπτυξη νέων μορφών ψηφιακής εγκληματικότητας στον κυβερνοχώρο σε εποχές Κρίσης, 26-01-2016, http://crime-in-crisis.com/%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7-%CE%BA%CE%B1%CE%B9-%CE%B1%CE%BD%CE%AC%CF%80%CF%84%CF%85%CE%BE%CE%B7-%CE%BD%CE%AD%CF%89%CE%BD-%CE%BC%CE%BF%CF%81%CF%86%CF%8E%CE%BD-%CF%88%CE%B7%CF%86%CE%B9/ (τελευταία επίσκεψη 09-11-2023).

Παύλου Σ., Μπέκας Ι., Αποστολίδου Α., Ποινικό Δίκαιο – Ειδικό Μέρος, τ. Α΄: Τα εγκλήματα κατά των περιουσιακών αγαθών (άρθρα 372 επ., 385 επ. ΠΚ), της ζωής (άρθρα 299 επ. ΠΚ) και της σωματικής ακεραιότητας (άρθρα 308 επ. ΠΚ), Εκδόσεις Π.Ν. Σάκκουλα, 2020

Παύλου Σ., Γ. Μπέκας Γ., Ποινικό ΙΙΙ, Εγκλήματα κατά ιδιοκτησία, περιουσίας και ζωής, Δίκαιο & Οικονομία Εκδόσεις Π.Ν. Σάκκουλα, 2011

Περπερής Α, «Ο ρόλος των κινήτρων και των ευκαιριών στη δόμηση του προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος» - διαθέσιμο στην ηλεκτρονική έκδοση του νομικού περιοδικού CrimeinCrisis - Τιμητικός Τόμος Νέστορα Κουράκη (http://crime-in-crisis.com

Πιτσελά Α., Η εγκληματολογική προσέγγιση του οικονομικού εγκλήματος, Εκδ. Σάκκουλα Αθήνα-Θεσσαλονίκη, 2010.

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 το πρίσμα του Ουσιαστικού Ποινικού Δικαίου, ΤΝΠ QUALEX ΠοινΔικ, 10/2022, σελ. 1321 - 1333

Στεργίου Λ., «Οι πελάτες του ebanking ξεπέρασαν τα τραπεζικά καταστήματα», 09-02-2021, https://www.capital.gr/epixeiriseis/3524226/oi-pelates-tou-ebanking-xeperasan-ta-trapezika-katastimata/ (τελευταία επίσκεψη 01-12-2023).

Στεργίου Λ., «Το ebanking ήρθε για να μείνει», 20-02-2021, https://www.capital.gr/oikonomia/3527107/to-ebanking-irthe-gia-na-meinei/ (τελευταία επίσκεψη 01-12-2023).

Συλικός Γ., Τα Οικονομικά Εγκλήματα στην σύγχρονη πραγματικότητα, Τα Οικονομικά Εγκλήματα στην σύγχρονη πραγματικότητα, ΤΝΠ QUALEX ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ, 1-2/2021, σελ. 110 – 118

Γ. Συλίκος, Οι Νέοι Ποινικοί Κώδικες, Πράξη και Λόγος ΠΔ, Τόμος 2019, σελ. 498 και επ.

Τζώρτζη Ε., «Ηλεκτρονικές απάτες: Πώς και πότε θα δίνουν αποζημίωση οι τράπεζες», Καθημερινή, 26-01-2023, διαθέσιμο στον ιστότοπο https://www.kathimerini.gr/economy/562247020/ilektronikes-apates-pos-kai-pote-tha-dinoyn-apozimiosi-oi-trapezes/ (τελευταία επίσκεψη 01-12-2023).

Τσίγκανου Ι., «Η στατιστική αποτύπωση του εγκληματικού φαινομένου στη σύγχρονη Ελλάδα», 11/2016, https://theartofcrime.gr/η-στατιστική-αποτύπωση-του-εγκληματι/ (τελευταία επίσκεψη 01-12-2023).

Τσιπτσέ Σ., «Ηλεκτρονικό ψάρεμα ή αλλιώς phishing ή αλλιώς… διαδικτυακή απάτη», 16-02-2023, https://finupnews.gr/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-

%CF%88%CE%AC%CF%81%CE%B5%CE%BC%CE%B1-%CE%AE-%CE%B1%CE%BB%CE%BB%CE%B9%CF%8E%CF%82-phishing-%CE%AE-%CE%B1%CE%BB%CE%BB%CE%B9%CF%8E%CF%82/ (τελευταία επίσκεψη 01-12-2023).

Φιλόπουλος Π., Ποινική Προστασία Απορρήτου, εκδ. Α.Ν. Σάκκουλας, 2015.

Φράγκος Κ., Online κατ' άρθρο ερμηνεία του Ποινικού Κώδικα, εκδ. Α.Ν. Σάκκουλα, 2020, https://www.sakkoulas-online.gr/

Χαραλαμπάκης Α., Ο Νέος Ποινικός Κώδικας: Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Τόμος Δεύτερος (Άρθρα 235-469), εκδ. Νομικής Βιβλιοθήκη, 2020.

Χαραλαμπάκης Α., Συλλογικό Έργο, Ποινικός Κώδικας - Κατ' Άρθρο Ερμηνεία, Νομική Βιβλιοθήκη, 2014

Ξενόγλωσση

Barrett N., Digital Crime: Policing the Cybernation, Kogan Page Ltd, 1997.

Bartoletti M. / Carta S. / Cimoli T. / Saia R., "Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact", Future Generation Computer Systems 102, 2020, σελ. 259–277. Διαθέσιμο μέσω του ιστοτόπου ResearchGate (file:///C:/ /%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82/Mining_Bytecode_Features_of_Smart_Contracts_to_Det.pdf)

Bloomenthal A., "What Determines the Price of 1 Bitcoin?", 16-06-2020, διαθέσιμο στα αγγλικά στην ιστοσελίδα https://www.investopedia.com/tech/what-determines-value-1-bitcoin/#citation-1 (τελευταία επίσκεψη 03-12-2023).

Butavicius M. / Parsons K. / Pattinson M. / McCormac A., "Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing

Emails", Australasian Conference on Information Systems, Cornell University, 2015. (https://arxiv.org/pdf/1606.00887.pdf) (τελευταία επίσκεψη 20-12-2023).

Chaganti R. / Bhushan B. / Nayyar A. / Mourade A., "Recent trends in social engineering scams and case study of gift card scam", Cornell University, 31-10-2021, διαθέσιμο στον ιστότοπο https://arxiv.org/pdf/2110.06487.pdf (τελευταία επίσκεψη 01-12-2023).

Chetioui K. / Bah B. / Alami A. / Bahnasse A., "Overview of social engineering attacks on social networks", Procedia Computer Science vol. 198, 2022, σελ. 656-661. Διαθέσιμο μέσω του ιστοτόπου ResearchGate (file:///C:/ /%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82/1-s2.0-S1877050921025412-main-Kaoutar.pdf)

Cook P. "The Demand and Supply of Criminal Opportunities". Crime and Justice vol. 7, University of Chicago Press, 1986, σελ. 1-27.

Federal Bureau of Investigation, Internet Crime Report, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (τελευταία επίσκεψη 01-12-2023).

Forester T. / Morrison P., Computer Ethics: Cautionary tales and ethical dilemmas in computing, second edition, The MIT Press, Cambridge, Massachusetts, London, England, 1994.

Frankovits G., Mirsky Y., "The Threat of Real Time Deepfakes", Cornell University, 04-06-2023, διαθέσιμο στον ιστότοπο https://arxiv.org/pdf/2306.02487.pdf (τελευταία επίσκεψη 01-12-2023).

Grabosky P. / Walkley S., "Computer Crime and White-Collar Crime", Springer, 2007, σελ.. 364-375.

Granot Er'el, “On the Origin of the Value of Cryptocurrencies”, 2018, https://www.intechopen.com/books/blockchain-and-cryptocurrencies/onthe-origin-of-the-value-of-cryptocurrencies (τελευταία επίσκεψη 03-12-2023).

Hayes S., “Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin”, Telematics and Informatics, 13-05-2016, σελ. 1308. (https://deliverypdf.ssrn.com/delivery.php?ID=726071067021026018092029119124121028058084022041061078026026029075120028068088090010010097040106104063121089080097009115105099022084007077063118067120097101065067075017040017005106092101081028119112103073101026096109007121010104017106081082026000127105&EXT=pdf&INDEX=TRUE) (τελευταία επίσκεψη 20-12-2023).

Ismail, K. A./ Singh, M. M. / Mustaffa, N. / Keikhosrokiani, P. / Zulkefli, Z., “Security strategies for hindering watering hole cybercrime attack”, Procedia Computer Science, vol. 124, 2017, σελ. 656–663. Διαθέσιμο μέσω του ιστοτόπου ResearchGate (file:///C://%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82/Security_Strategies_for_Hindering_Watering_Hole_Cy.pdf) (τελευταία επίσκεψη 20-12-2023).

Kopp C. / Layton R. / Sillitoe J. / Gondal I., “The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles”, International Journal of Cyber Criminology Vol 9 Issue 2 July – December 2015, σελ. 205 - 217. (https://www.cybercrimejournal.com/pdf/Koppetal2015vol9issue2.pdf) (τελευταία επίσκεψη 05-01-2023).

Lazarus S. / Whittaker J. M. / McGuire M. R. /Platt L., “What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021)” Journal of Economic Criminology, 2, 2023. Διαθέσιμο μέσω του ιστοτόπου ResearchGate (file:///C://%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%C

F%83%CF%84%CE%AE%CF%82/LAZARUS_ET_AL_2023A.pdf) (τελευταία επίσκεψη 20-12-2023).

Lohani S., “Social Engineering: Hacking into Humans”, International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391 (τελευταία επίσκεψη 01-12-2023).

McKay J, “DeFi-ing Cyber Attacks: A statistical analysis of cybersecurity attacks in decentralized finance”, 27-04-2022, διαθέσιμο στον ιστότοπο https://tellingstorieswithdata.com/inputs/pdfs/final_paper-2022-jack_mckay.pdf (τελευταία επίσκεψη 01-12-2023).

Mitnick K, Η τέχνη της απάτης, ο ανθρώπινος παράγοντας στην ασφάλεια, εκδ. Ωκεανίδα, 2003.