ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΑΠΑΤΗ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Διπλωματική Εργασία

του

Κωνσταντίνου Κουτσάκη

Θεσσαλονίκη, Φεβρουάριος 2023

Η ΑΠΑΤΗ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Κωνσταντίνος Κουτσάκης

Πτυχίο Νομικής Σχολής Α.Π.Θ.

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Θεοχάρης Δαλακούρας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/03/2023

....

Κωνσταντίνος Κουτσάκης

Περίληψη

Η διεύρυνση των ηλεκτρονικών συναλλαγών κατά τα τελευταία χρόνια έχει δημιουργήσει ένα νέο, ευρύ και δυναμικό πεδίο εγκληματικότητας. Η ποινική αντιμετώπιση αυτής της νέας εγκληματικής ύλης αποτελεί πρόκληση τόσο για τον θεωρητικό όσο και για τον εφαρμοστή του δικαίου. Ήδη, ο νομοθέτης, με τον ν. 1805/1988, και διαγιγνώσκοντας ότι στις συναλλαγές θα υπεισέλθουν νέες μορφές εγκληματικών συμπεριφορών -με ηλεκτρονικά μέσα-, προσέθεσε το άρθρο 386Α υπό τον τίτλο «Απάτη με υπολογιστή». Η νέα αυτή διάταξη ομοίαζε με αυτή του 386 αλλά είχε μια σημαντική διαφορά. Ενώ στην διάταξη που τυποποιείται η απλή απάτη (386 ΠΚ), η περιουσιακή βλάβη είναι το αποτέλεσμα της πρόκλησης πλάνης σε φυσικό πρόσωπο «πείθοντας κάποιον», στην αντίστοιχη του 386Α η απάτη εμφανίζεται ως αποτέλεσμα της επέμβασης στα δεδομένα του υπολογιστή.

Το άρθρο 386Α του ΠΚ, κατέστη έτσι η κεντρική διάταξη για την αντιμετώπιση των οικονομικών εγκλημάτων που τελούνται με ηλεκτρονικά μέσα, όχι όμως δίχως προβλήματα, όπως επεξηγείται και στο πρώτο κεφάλαιο της εργασίας. Στο δεύτερο κεφάλαιο, γίνεται ιστορική αναδρομή με αναφορά στις απόψεις που έχουν υποστηριχθεί περί της υπαγωγής της πράξης ανάληψης χρημάτων από ΑΤΜ χωρίς δικαίωμα, ενώ στο τρίτο κεφάλαιο εκτίθεται ο τρόπος με τον οποίο επιλύεται το πρόβλημα, μετά τον ν. 4411/2016. Στο τέταρτο κεφάλαιο γίνεται αναλυτική παρουσίαση της σημερινής μορφής του άρθρου 386Α ΠΚ. Ακολούθως, το πέμπτο κεφάλαιο περιλαμβάνει τις νέες ρυθμίσεις που εισήχθησαν με τον ν. 4947/2022, σε συμμόρφωση με την Οδηγία (ΕΕ) 2019/713 για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών. Τέλος, στο έκτο κεφάλαιο επιχειρείται στοχευμένη αναφορά σε νέες μορφές απάτης στο πεδίο των ηλεκτρονικών συναλλαγών.

Λέξεις Κλειδιά: ηλεκτρονικό έγκλημα, ηλεκτρονικές συναλλαγές, απάτη με υπολογιστή

Abstract

The expansion of electronic transactions in recent years has created a new, broad, and dynamic field of crime. This type of crime presents a significant challenge for both legal theorists and practitioners. To address offences related to the rapidly developing field of computers, Law 1805/1988 introduced new provisions concerning computer crimes. Article 386A, titled "Computer fraud" was similar to Article 386 but had one significant difference. While in the simple fraud (Article 386), the property damage is the result of misleading a natural person "by convincing someone", in the counterpart of 386A, the fraud appears as a result of the intervention in the computer data.

Thus, Article 386A of the Penal Code became the central provision for combating financial crimes committed by electronic means, but not without challenges, as explained in the first chapter. In the second chapter, a historical review is conducted regarding the legal rule applied to the act of withdrawing money from an ATM without a right. The third chapter presents the solution to this problem, after the amendments made by Law 4411/2016. The fourth chapter contains a detailed presentation of the current form of Article 386A of the Penal Code, and the fifth chapter includes the provisions introduced by Law 4947/2022, in compliance with Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment. Finally, the sixth chapter makes targeted references to new forms of fraud in the field of electronic transactions.

Keywords: cyber-crime, electronic transactions, computer fraud

Πρόλογος – Ευχαριστίες

Η επιλογή του θέματος της παρούσας έρευνας αφορμάται σε προσωπικές αναζητήσεις του γράφοντος σχετικά με επίκαιρα ζητήματα προσβολών κατά της περιουσίας που τελούνται μέσω του διαδικτύου. Η ποινική αντιμετώπιση της ηλεκτρονικής οικονομικής εγκληματικότητας, αποτελεί μια διαρκή πρόκληση για τον εφαρμοστή του δικαίου. Ακριβώς, όμως, σε αυτή την πρόκληση έγκειται και η γοητεία του συγκεκριμένου αντικειμένου. Η αλληλεπίδραση της τεχνολογίας με τη νομική, προσδίδει στο αντικείμενό μας, τη δυναμική που κάθε σύγχρονος επιστήμονας θα ήθελε να διαπνέει την επιστήμη του.

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου για την εμπιστοσύνη και τη στήριξή του στην ανάθεση της συγκεκριμένης θεματικής. Ευχαριστώ επίσης την οικογένειά μου για τη βοήθεια που μου προσέφερε σε όλα τα επίπεδα.

Περιεχόμενα

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΠ	Άρειος Πάγος
Αρμ	Αρμενόπουλος
ΑρχΝ	Αρχείο Νομολογίας
Βλ.	Βλέπε
εδ.	εδάφιο
ΕΔΔΑ	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ν.	νόμος
ό.π.	όπου παραπάνω
παρ.	παράγραφος
ΠΚ	Ποινικός Κώδικας
ΠΛογ	Ποινικός Λόγος
ΠοινΧρ	Ποινικά Χρονικά
ΠΣ	Πληροφοριακό Σύστημα
σελ.	σελίδα
Υπερ	Υπεράσπιση

1 Εισαγωγή

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Σύμφωνα με την Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος του Νοεμβρίου 2022[1], το α' εξάμηνο του 2022 οι ενεργές κάρτες πληρωμών σε κυκλοφορία ανήλθαν σε 20,4 εκατ., διατηρώντας τον αυξητικό ρυθμό έκδοσής τους. Αντίστοιχα, ο αριθμός των συναλλαγών με κάρτες ανήλθε σε 904 εκατ., παρουσιάζοντας σημαντική αύξηση 19,42% συγκριτικά με το αντίστοιχο περσινό εξάμηνο[2]. Όπως ήταν αναμενόμενο, η αύξηση των ηλεκτρονικών συναλλαγών, οδήγησε και σε τόνωση των νέων μορφών εγκληματικότητας. Ειδικότερα, κατά το πρώτο εξάμηνο του 2022 ο αριθμός των περιστατικών απάτης που καταγράφηκε ανά δίαυλο συναλλαγής ανήλθε σε 1.476 στις συναλλαγές με ATM, σε 17 χιλ. στις πληρωμές μέσω POS και σε 117 χιλ. στις εξ' αποστάσεως συναλλαγές.

Όσο λοιπόν, διευρύνονται οι ηλεκτρονικές συναλλαγές[3] τόσο εντείνεται και το ενδιαφέρον για τη μελέτη των ποινικών συνεπειών που προκύπτουν από τις αθέμιτες συμπεριφορές στις συναλλαγές αυτές. Ήδη ο νομοθέτης, με τον ν. 1805/1988[4], και διαγιγνώσκοντας ότι στις συναλλαγές θα υπεισέλθουν νέες μορφές εγκληματικών συμπεριφορών[5] -με ηλεκτρονικά μέσα- πρόσθεσε το άρθρο 386Α υπό τον τίτλο «Απάτη με υπολογιστή». Η νέα αυτή διάταξη ομοίαζε με αυτή του 386 αλλά είχε μια σημαντική διαφορά. Ενώ στην διάταξη που τυποποιείται η απλή απάτη (386 ΠΚ), η περιουσιακή βλάβη είναι το αποτέλεσμα της πρόκλησης πλάνης σε φυσικό πρόσωπο «πείθοντας κάποιον», στην αντίστοιχη του 386Α η απάτη εμφανίζεται ως αποτέλεσμα της επέμβασης στα δεδομένα του υπολογιστή[6].

---

[1] Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος, Νοέμβριος 2022, σελ. 95.

[2] Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος, Δεκέμβριος 2021, σελ. 72. Ο αριθμός των συναλλαγών με κάρτες το α' εξάμηνο 2021, ανήλθε σε 757 εκατ., ήδη αυξημένο κατά 22% συγκριτικά με το β' εξάμηνο του 2020 (βλ. και Έκθεση Ιανουαρίου 2021, σελ. 54).

[3] Α. Συκιώτου, Το διαδίκτυο ως σύγχρονο όχημα θυματοποίησης, 2009, σελ. 60,61.

[4] Η διάταξη του 386Α προστέθηκε με το άρθρο 5 του ν. 1805/1988 στο τότε 24ο κεφάλαιο του ΠΚ.

[5] R. Doswell – G.L. Simons, Πληροφορική και εγκληματικότητα, 1990, σελ. 46-50. Α. Αργυρόπουλος, Ηλεκτρονική εγκληματικότητα, 2001, σελ. 18.

[6] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 153.

Το άρθρο 386Α του ΠΚ κατέστη έτσι η κεντρική διάταξη για την αντιμετώπιση των οικονομικών[7] εγκλημάτων που τελούνται με ηλεκτρονικά μέσα, όχι όμως δίχως προβλήματα. Ειδικότερα, παρόλη την πρόθεση του νομοθέτη να κάνει ευχερέστερη, με την εισαγωγή του άρθρου 386Α, την ποινική αντιμετώπιση των εγκλημάτων που σχετίζονται με ηλεκτρονικές συναλλαγές με ΑΤΜ, τόσο η θεωρία όσο και η νομολογία το υποδέχθηκαν με έκδηλη αμηχανία[8]. Το κύριο πρόβλημα δημιουργήθηκε επειδή ο Έλληνας νομοθέτης επέλεξε την γενική διατύπωση «με οποιονδήποτε άλλο τρόπο» επηρεασμό των στοιχείων υπολογιστή, αντί να περιλάβει ρητά την περίπτωση της «χωρίς δικαίωμα χρησιμοποίησης (ορθών) στοιχείων» όπως ακριβώς προβλέπει η αντίστοιχη Γερμανική διάταξη, για να καλύψει τις περιπτώσεις αθέμιτης χρήσης καρτών ανάληψης χρημάτων[9].

Λύση στο πρόβλημα επιχειρήθηκε να δοθεί με την εισαγωγή του ν. 4411/2016, ο οποίος αποτελεί κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης). Η τελευταία υποχρέωνε τον Έλληνα νομοθέτη να ποινικοποιήσει, μεταξύ άλλων, και την άνευ δικαιώματος παρέμβαση σε ηλεκτρονικό υπολογιστή[10]. Πράγματι, με τη νέα διάταξη του 386Α, περιλήφθηκε πλέον[11] ρητά στις περιπτώσεις απάτης με υπολογιστή και η χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα[12].

Μπορεί λοιπόν, να παρήλθαν τρείς και πλέον δεκαετίες από την εισαγωγή του άρθρου 386Α στον Ποινικό μας Κώδικα, όμως η προβληματική περί της υπαγωγής στο άρθρο αυτό, διάφορων μορφών ηλεκτρονικής εγκληματικότητας δεν έπαυσε να απασχολεί την επιστήμη και την νομολογία. Κύριο παράδειγμα, αποτελεί η αθέμιτη χρήση κάρτας αυτόματης συναλλαγής σε ΑΤΜ, όπου για κανένα ίσως άλλο θέμα στο Ποινικό Δίκαιο δεν έχουν διατυπωθεί τόσο πολλές και διαφορετικές λύσεις. Μεταξύ άλλων, έχουν

[7] Α. Ζάννη, Το διαδικτυακό έγκλημα, 2005, σελ. 100, 101.

[8] Θ. Σάμιος, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, 2010, σελ. 4.

[9] Δ. Κιούπης, Ποινικό δίκαιο και Internet, 1999 σελ. 114-115.

[10] Άρθρο 8 του ν. 4411/2016: Απάτη σχετική με υπολογιστές «Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας δια της β. παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο».

[11] Θ. Δαλακούρας, Ηλεκτρονικό Έγκλημα, 2023, σελ. 18.

[12] Αιτιολογική έκθεση του σχεδίου νόμου για την Κύρωση της Σύβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, σελ. 6.

υποστηριχθεί οι απόψεις -για την υπαγωγή της πράξης σε διαφορετικά εγκλήματα-, ότι ο επιλήψιμος χρήστης κάρτας αυτόματης συναλλαγής τελεί κλοπή, ή υπεξαίρεση, ή απάτη, ή απάτη με υπολογιστή.

1.2 Σκοπός – Στόχοι

Η παρούσα μελέτη έχει ως αντικείμενο την ποινική αξιολόγηση πράξεων που αναφύονται στο πεδίο εγκληματικότητας των ηλεκτρονικών συναλλαγών. Ξεκινώντας από την πράξη της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ και τα προβλήματα υπαγωγής που δημιουργήθηκαν, μέχρι τις νέες εγκληματικές μορφές που παρουσιάζονται καθημερινά στις ηλεκτρονικές συναλλαγές, εντοπίζεται μια διαρκής προσπάθεια της νομικής επιστήμης να ακολουθήσει τους φρενήρεις ρυθμούς της τεχνολογίας. Η υπαγωγή των σχετικών εγκλημάτων στη νομοτυπική μορφή της διάταξης του άρθρου 386Α του Ποινικού μας Κώδικα δεν είναι πάντοτε ευχερής, διότι και ο εφαρμοστής του δικαίου δεν έχει συχνά την τεχνολογική κατάρτιση για να αντιληφθεί κάποια λεπτά ζητήματα. Έτσι, ο ερευνητής καλείται να φωτίσει κομμάτια που απασχολούν την επιστήμη διαχρονικά ενώ τα ζητήματα αλλάζουν μορφές παράλληλα με την εξέλιξη της τεχνολογίας. Κεντρικές έννοιες για το πρόβλημα εφαρμογής του άρθρου 386Α αποτελούσαν μέχρι πρότινος τα ΑΤΜ και οι κάρτες αυτόματης συναλλαγής. Σήμερα στο ίδιο πεδίο βρίσκονται οι έννοιες του κρυπτοχρήματος και των ψηφιακών πορτοφολιών. Στο μέλλον θα μας απασχολήσουν νέα στοιχεία. Στην έρευνά μας θα επικεντρωθούμε στην ουσία της προβληματικής της απάτης στις ηλεκτρονικές συναλλαγές, ξεκινώντας από τη χωρίς δικαίωμα ανάληψη μετρητών από ΑΤΜ που υπήρξε το γνήσιο πρόβλημα, μέχρι και το τελευταίο κεφάλαιο, όπου αναλύονται οι νέες εγκληματικές μορφές.

1.3 Βασική Ορολογία

Ως Αυτόματα Ταμειολογικά Μηχανήματα (ΑΤΜ), ορίζονται οι ηλεκτρονικές συσκευές που επιτρέπουν στους πελάτες των χρηματοπιστωτικών ιδρυμάτων να διεξάγουν χρηματοοικονομικές συναλλαγές, όπως αναλήψεις και καταθέσεις μετρητών, λήψη πληροφοριών σχετικά με το διαθέσιμο υπόλοιπο του λογαριασμού τους, ενεργοποιήσεις νέων καρτών, ανά πάσα στιγμή και χωρίς την ανάγκη άμεσης αλληλεπίδρασης με το τραπεζικό προσωπικό.

Ως κάρτες αυτόματης συναλλαγής, νοούνται οι πλαστικές -συνήθως- κάρτες πληρωμών, τις οποίες εκδίδουν τα χρηματοπιστωτικά ιδρύματα υπέρ ενός δικαιούχου με σκοπό, κατ' αρχήν, την εισαγωγή τους στα ΑΤΜ για την πραγματοποίηση των ενεργειών

που αναφέρθηκαν αμέσως παραπάνω. Οι περισσότερες από αυτές διαθέτουν τεχνολογία Chip & PIN προσφέροντας μεγαλύτερη ασφάλεια. Έτσι, με μόνη την κατοχή της κάρτας, η οποία περιλαμβάνει στο chip της τα δεδομένα σχετικά με τον κάτοχό της, και την πληκτρολόγησή του PIN, επαληθεύονται τα στοιχεία του κατόχου και πραγματοποιείται η συναλλαγή.

Ως ανέπαφη ανάληψη σε ΑΤΜ με κάρτα ή χωρίς τη φυσική παρουσία κάρτας - μέσω του κινητού τηλεφώνου και τη χρήση της υπηρεσίας ψηφιακού πορτοφολιού- νοείται η απλή προσέγγιση της κάρτας ή του κινητού τηλεφώνου στο ειδικό σημείο του ΑΤΜ. Η απλή προσέγγιση της κάρτας ή του κινητού τηλεφώνου στο ΑΤΜ λειτουργεί ως οιονεί εισαγωγή της κάρτας σε αυτό, αφού έτσι μεταβιβάζονται ασύρματα στο ΑΤΜ τα ίδια δεδομένα που θα μεταβιβάζονταν και με την φυσική εισαγωγή της κάρτας.

1.4 Διάρθρωση της μελέτης

Στο δεύτερο κεφάλαιο της έρευνας γίνεται ιστορική αναδρομή του θεσμού με αναφορά στις απόψεις που έχουν υποστηριχθεί περί της υπαγωγής της πράξης της ανάληψης χρημάτων από ΑΤΜ με χρήση ξένης κάρτας αυτόματων συναλλαγών, ενώ στο τρίτο κεφάλαιο εκτίθεται ο τρόπος με τον οποίο επιλύεται το πρόβλημα, μετά την νομοθετική μεταβολή που επήλθε με τον ν. 4411/2016. Στο τέταρτο κεφάλαιο γίνεται αναλυτική παρουσίαση της σημερινής μορφής του άρθρου 386Α ΠΚ, το οποίο αποτελεί την κορωνίδα της ποινικής αντιμετώπισης του εγκλήματος στις ηλεκτρονικές συναλλαγές. Ακολούθως, το πέμπτο κεφάλαιο περιλαμβάνει τις νέες ρυθμίσεις που εισήχθησαν με τον ν. 4947/2022, σε συμμόρφωση με την Οδηγία (ΕΕ) 2019/713 για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών. Τέλος, στο έκτο κεφάλαιο επιχειρείται στοχευμένη αναφορά σε νέες μορφές εγκληματικότητας στο πεδίο των ηλεκτρονικών συναλλαγών και στην ποινική αξιολόγησή τους.

2 Ιστορική αναδρομή – Το καθεστώς πριν από την εισαγωγή του άρθρου 386Α ΠΚ

2.1 Πρόλογος

Κατά το διάστημα πριν από την ψήφιση του ν. 1805/1988, η νομολογία και η επιστήμη κλήθηκαν να αντιμετωπίσουν τις πρώτες μορφές ηλεκτρονικής εγκληματικότητας με το ήδη υπάρχον νομικό οπλοστάσιο. Ειδικότερα, η πρώτη μορφή ηλεκτρονικού εγκλήματος στις συναλλαγές, η οποία και έλαβε μεγάλες διαστάσεις στην ποινική επιστήμη -λόγω της μη εύκολης υπαγωγής της σε κάποια υπάρχουσα αντικειμενική υπόσταση-, υπήρξε η πράξη της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ. Έτσι, για την ορθότερη και πληρέστερη ανάπτυξη της θεματικής περί απάτης στις ηλεκτρονικές συναλλαγές, θα πρέπει να εκκινήσουμε την έρευνα από την αρχική της διάσταση, με τις διάφορες λύσεις που υποστηρίζονταν πριν από την εισαγωγή του άρθρου 386Α ΠΚ.

2.2 Η λύση της απάτης

Η στοιχειοθέτηση της αντικειμενικής υπόστασης της απάτης (386 ΠΚ) προϋποθέτει πράξεις εξαπάτησης, οι οποίες επιδρώντας σε κάποιον του δημιουργούν πλάνη. Και βέβαια, έγινε εξ' αρχής κατανοητό, ότι η πρόκληση πλάνης στα ΑΤΜ είναι αδύνατη, καθώς αυτά δεν έχουν συνείδηση, ούτε σχηματίζουν παραστάσεις γεγονότων. Το άρθρο 386 ΠΚ αποκλείει ούτως ή άλλως την εφαρμογή του στις περιπτώσεις αυτές, αφού ορίζει ρητά ότι «όποιος … βλάπτει ξένη περιουσία πείθοντας κάποιον». Φυσικά ο «κάποιος» είναι άνθρωπος και όχι μηχάνημα[13]. Έτσι η εφαρμογή του άρθρου 386 ΠΚ πρέπει να αποκλειστεί ήδη από αυτό το σημείο, αφού δεν υφίσταται καν πράξη προκλητική πλάνης. Πάντως, εσφαλμένα, σε δύο περιπτώσεις η ελληνική νομολογία έκρινε την ανάληψη μετρητών με ξένη κάρτα από ΑΤΜ ως απάτη. Η πρώτη περίπτωση αποτελούσε απόφαση πρωτοβάθμιου δικαστηρίου -που πάντως προσβλήθηκε με έφεση και στη

[13] Βλ. Αιτ. Έκθεση του Γερμ. Δεύτερου Νόμου για την Οικονομική Εγκληματικότητα (2. WiKG), σελ. 19. «der Tatbestand des Betruges menschliche Entscheidungsprozesse voraussetzt, die bei dem Einsatz des Computers fehlen» που σημαίνει ότι η α.υ. της απάτης απαιτεί ανθρώπινες διαδικασίες λήψης αποφάσεων που απουσιάζουν κατά τη χρήση υπολογιστών.

συνέχεια το Εφετείο έκρινε ότι η πράξη αποτελεί κλοπή και όχι απάτη[14]. Η δεύτερη περίπτωση αφορούσε την αξιολόγηση περιστατικού ανάληψης από ΑΤΜ με κάρτα αυτόματης συναλλαγής ως απάτης από το Συμβούλιο Πλημμελειοδικών Καστοριάς[15].

2.3 Η λύση της κλοπής

2.3.1 Γενικά

Η απόρριψη της λύσης της απάτης αποτελεί κοινό τόπο για τη θεωρία και τη νομολογία. Όμως δεν συμβαίνει το ίδιο και για τη λύση της κλοπής. Στη Γερμανία ήδη πριν την ψήφιση του άρθρου περί απάτης με υπολογιστή[16] είχε ξεσπάσει έντονη διαμάχη σχετικά με το θέμα της κατάφασης κλοπής ή υπεξαίρεσης ή κρίσης της πράξης μη αξιόποινης, για τον τρίτο που χρησιμοποιεί αθέμιτα την κάρτα αυτόματης συναλλαγής. Αντίστοιχες τάσεις διαμορφώθηκαν και στην Ελλάδα, ακόμη και μετά την τυποποίηση του 386Α με τον ν. 1805/1988[17].

2.3.2 Η έλλειψη συγκατάθεσης της τράπεζας για μεταβίβαση της κυριότητας των χρημάτων στοιχειοθετεί κλοπή

Οι οπαδοί της λύσης της κλοπής υποστήριξαν ότι η περίπτωση ανάληψης χρημάτων μη δικαιούχου από ΑΤΜ αποτελεί κλοπή, διότι ελλείπει η συγκατάθεση της τράπεζας στην μεταβίβαση της κυριότητας των χρημάτων. Σύμφωνα με την άποψη αυτή, η τράπεζα συγκατατίθεται μόνον υπό όρους στη μεταβίβαση της κυριότητας των χρημάτων που παραδίδει μέσω του ΑΤΜ. Εν προκειμένω οι όροι αυτοί δεν πληρούνται, αφού ο μη δικαιούχος χρήστης δεν μπορεί να θεωρηθεί ότι συμμορφώνεται με τους όρους. Συνεπώς, αφού η τράπεζα δεν συγκατατίθεται στη μεταβίβαση της κυριότητας των χρημάτων, τότε αυτός που τα λαμβάνει τελεί κλοπή.

---

[14] ΠοινΧρ ΜΒ (1992), σελ. 197 (παρατηρήσεις Ηλ. Αναγνωστόπουλου επί της εφετειακής απόφασης 1904/1991 του Τριμελούς Εφετείου Αθηνών).

[15] Βούλευμα Συμβουλίου Πλημμελειοδικών Καστοριάς 196/1999 (ο δράστης απηλλάγη λόγω εντελούς ικανοποίησης του θύματος).

[16] ΠοινΔικ 2/2003, Γ. Νούσκαλης, σελ. 182.

[17] Θ. Σάμιος, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, 2010 σελ. 151.

2.3.3 Η ουσιαστική νομιμοποίηση ως θεμέλιος λίθος της λύσης της κλοπής

Η άποψη αυτή έχει ως θεμέλιο την ουσιαστική νομιμοποίηση του χρήστη του ΑΤΜ. Δηλαδή, δεν αρκείται στην τυπική νομιμοποίηση του χρήστη που θα αποτελούνταν από μόνη την κατοχή της κάρτας και τη γνώση του PIN. Και αν θεωρούσαμε την τυπική νομιμοποίηση ικανή τότε δεν θα στοιχειοθετούνταν κανένα αδίκημα, αφού τα χρήματα θα μεταβιβάζονταν με τη συγκατάθεση της τράπεζας στον τυπικώς νομιμοποιούμενο χρήστη. Αντίθετα, σύμφωνα με το ουσιαστικό κριτήριο νομιμοποίησης στο οποίο στηρίζεται η θεωρία περί κλοπής θα πρέπει κάποιος να αποτελεί τον ουσιαστικό δικαιούχο και μόνο τότε η τράπεζα του παρέχει την συγκατάθεσή της για την μεταβίβαση της κυριότητας των χρημάτων.

2.3.4 Η αποδοχή της θεωρίας της κλοπής από νομολογία και θεωρία

Η λύση της κλοπής εμφανίστηκε ως κρατούσα στη νομολογία μας[18]. Μεγαλύτερο ενδιαφέρον αποκτά αυτή η τάση της νομολογίας, αν αναλογιστούμε ότι όλες οι σχετικές αποφάσεις αφορούσαν πράξεις που τελέστηκαν μετά την εισαγωγή του 386Α ΠΚ. Ακόμα και μετά την εισαγωγή του 386Α ΠΚ, πάντως, τη λύση της κλοπής ασπάστηκε και σημαντικό μέρος της θεωρίας. Ο αείμνηστος Στέφανος Παύλου[19], εκλαμβάνοντας τα χρήματα που βρίσκονται στο ΑΤΜ ως εξατομικευμένα κινητά πράγματα, τασσόταν υπέρ της θεωρίας της κλοπής, θεωρώντας ότι η τράπεζα παρέχει συγκατάθεση υπό όρους -και οι όροι αυτοί παραβιάζονται αν ο λαμβάνων τα χρήματα δεν είναι ο ουσιαστικά νομιμοποιούμενος. Η Συμεωνίδου – Καστανίδου κατέληγε στη λύση της κλοπής ακόμα και για την παράνομη διείσδυση και μεταφορά νομισματικών μονάδων σε άλλο λογαριασμό[20].

2.3.5 Κριτική για τη λύση της κλοπής

Η κύρια επιχειρηματολογία ενάντια στη λύση της κλοπής εστιάζει στο ότι η τράπεζα έχει παραιτηθεί εκ των προτέρων από το δικαίωμά της να γνωρίζει αν συναλλάσσεται με τον πραγματικό δικαιούχο της κάρτας αυτόματης ανάληψης. Ενώ εδώ και πολλά χρόνια υπάρχουν τρόποι βιομετρικής επαλήθευσης του χρήστη, οι τράπεζες

[18] ΕφΑθ. 1904/1991, 9474/2002, 5224/2007, ΑΠ 2530/2008 & 355/2009.

[19] Σ. Παύλου, Εγκλήματα κατά της ιδιοκτησίας, 2006, σελ. 38.

[20] Ε. Συμεωνίδου-Καστανίδου, Υπεράσπιση 8 (1998), σελ. 937επ. (με αρχή ότι ο καταθέτης παραμένει κύριος και κάτοχος των νομισματικών μονάδων που εγγράφονται στον λογαριασμό του).

έχουν επιλέξει την τυπική νομιμοποίηση των χρηστών. Γνωρίζουν ότι ενδεχομένως να υπάρχουν καταχρήσεις -και πράγματι υπάρχουν[21]-, όμως χάριν ευκολίας των συναλλαγών επιλέγονται οι ελαστικές ταυτοποιήσεις. Καθόσον, όμως, το μηχάνημα δεν είναι προγραμματισμένο να απορρίπτει τις συναλλαγές του μη πραγματικού δικαιούχου, αλλά να τις αποδέχεται, δεν μπορεί να έχει καμία σημασία η υποθετική βούληση της τράπεζας. Δηλαδή, η μη πλήρωση των όρων συγκατάθεσης, θα έπρεπε να βρίσκει πρακτικό αντίκρισμα με κάποια αντίδραση του ΑΤΜ. Εφόσον δεν έχει υλοποιηθεί κάτι τέτοιο -αν και υπάρχει τεχνικά η δυνατότητα- οποιαδήποτε βούληση της τράπεζας που δεν εξωτερικεύεται, παραμένει άνευ σημασίας. Έτσι η τράπεζα δεν μπορεί να επικαλείται ότι η συναλλαγή έγινε χωρίς την συγκατάθεσή της, όταν η ίδια παραλείπει να ενσωματώσει σε πρακτικό επίπεδο τους όρους της, στην αυτοματοποιημένη διαδικασία[22]. Συνεπώς, η έλλειψη ουσιαστικής νομιμοποίησης αδυνατεί να θεμελιώσει την λύση της κλοπής και το κατασκεύασμα της αόρατης βούλησης της τράπεζας είναι τουλάχιστον εύθραυστο.

Με βάση τα σημερινά δεδομένα και ιδίως μετά τον ν. 4411/2016, η θεωρία της κλοπής δεν έχει πλέον λόγο ύπαρξης. Η θεωρία αυτή υποστηριζόταν ελλείψει της ειδικότερης υπαλλαγής τέλεσης απάτης με υπολογιστή περί χρήσης ορθών στοιχείων χωρίς δικαίωμα[23], όπως αυτή ήδη ίσχυε στον γερμΠΚ. Όπως θα δούμε σε επόμενο κεφάλαιο, μια νέα τροποποίηση, του άρθρου 386Α (ν. 4411/2016) αποδείχθηκε καίρια, ώστε θεωρία και νομολογία να απομακρυνθούν από τη λύση της κλοπής. Σχετικά με την υπαγωγή της πράξης της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ, οι πολυετείς αναζητήσεις επί του ζητήματος, θα είχαν λάβει διαφορετική τροπή, εάν ο Έλληνας νομοθέτης είχε ενσωματώσει την σχετική υπαλλαγή, όπως ακριβώς έπραξε ο Γερμανός[24], ήδη, δεκαετίες πριν.

[21] Βλ. Εισαγωγή.

[22] Θ. Σάμιος, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, 2010, σελ. 185επ.

[23] Οι πράξεις αθέμιτων αναλήψεων μετρητών από ΑΤΜ με ξένη κάρτα, είναι συχνές, διότι δεν χρειάζονται ειδικές γνώσεις βλ. R. Doswell – G.L. Simons, Πληροφορική και εγκληματικότητα, 1990, σελ. 48.

[24] Της χωρίς δικαίωμα εισαγωγής δεδομένων §263a StGB: Computerbetrug.

2.4 Η λύση της υπεξαίρεσης

2.4.1 Γενικά

Σύμφωνα με τη λύση της υπεξαίρεσης επί αναλήψεως χρημάτων χωρίς δικαίωμα σε ΑΤΜ, δεν μπορούμε να κάνουμε λόγο για αφαίρεση των χρημάτων από τον δράστη, αλλά για εκούσια παράδοσή τους εκ μέρους της τράπεζας. Το κύριο επιχείρημα της άποψης αυτής -και παράλληλα μομφή προς τη λύση της κλοπής- είναι ότι η εκούσια παράδοση του πράγματος αποκλείει την αφαίρεση. Ακόμα και αν η τράπεζα πλανάται ως προς την ουσιαστική νομιμοποίηση του προσώπου που τελεί την δίχως δικαίωμα ανάληψη χρημάτων, αυτό δεν στοιχειοθετεί αφαίρεση άρα ούτε και κλοπή.

2.4.2 Οι κρίσιμες έννοιες της κατοχής και της κυριότητας

Το γεγονός ότι η τράπεζα παραδίδει την κατοχή των χρημάτων δεν σημαίνει ότι μεταθέτει και την κυριότητα. Οι υποστηρικτές της λύσης της υπεξαίρεσης τονίζουν τη διαφορά μεταξύ της -υλικής πράξης- παράδοσης κατοχής και της -δικαιοπραξίας- μετάθεσης κυριότητας. Ως προς την υλική πράξη δεν υπάρχει ζήτημα αναζήτησης της αληθούς βούλησης της τράπεζας. Αντίθετα, η δικαιοπρακτική βούληση της τράπεζας κατευθύνεται στη μεταβίβαση κυριότητας μόνο στον ουσιαστικά νομιμοποιούμενο δικαιούχο της κάρτας. Αυτός που πραγματοποιεί ανάληψη μετρητών χωρίς να είναι πραγματικός δικαιούχος δεν μπορεί να αποδεχθεί την πρόταση της τράπεζας, αφού εκείνη δεν απευθύνεται σε αυτόν. Συνεπώς, εφόσον δεν μπορεί να καταστεί κύριος των χρημάτων που του αποδίδει το ΑΤΜ και τα έχει ιδιοποιηθεί, τελεί υπεξαίρεση.

2.4.3 Η αποδοχή της λύσης της υπεξαίρεσης από νομολογία και θεωρία

Η νομολογία έχει αποδεχθεί τη λύση της υπεξαίρεσης εντελώς μεμονωμένα σε υπόθεση[25] όπου το θύμα παρέδωσε εκουσίως την κάρτα του στον δράστη και ο δράστης ανέλαβε ποσό από ΑΤΜ και το οικειοποιήθηκε. Η θεωρία της υπεξαίρεσης αποτέλεσε μια λύση εφεδρική[26], ως απάντηση στις ενστάσεις που προβάλλονταν έναντι των άλλων λύσεων και ως ανάχωμα για να μην μένει ατιμώρητος ο δράστης. Από την άλλη πλευρά,

[25] Βούλευμα 2897/1994 του Συμβουλίου του Διαρκούς Στρατοδικείου Αθηνών.

[26] Θ. Σάμιος, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, 2010, σελ. 227.

στη θεωρία, η λύση της υπεξαίρεσης υποστηρίχθηκε παλαιότερα από τον Μανωλεδάκη[27]. Επίσης, ο Ζησιάδης δεχόταν τούτη τη λύση ως ορθή[28].

2.4.4 Κριτική για τη λύση της υπεξαίρεσης

Η λύση της υπεξαίρεσης πάσχει από την ίδια αδυναμία που ενυπάρχει στη θεμελίωση της λύσης της κλοπής και ισχύουν όσα αναφέρθηκαν παραπάνω υπό το 2.3.5. Εδώ θα πρέπει απλά να συμπληρωθεί ότι η λύση της υπεξαίρεσης περιπλέκει ακόμα περισσότερο τα πράγματα και δεν αποτελεί μια ενιαία λύση όπως η λύση της κλοπής. Με τη λύση της κλοπής, ελλείψει ουσιαστικής νομιμοποίησης, θεωρείται ότι δεν μεταβιβάζεται ούτε η κατοχή, ούτε η κυριότητα. Αντίθετα στη λύση της υπεξαίρεσης, η μεταβίβαση της κυριότητας εξαρτάται από όρο -έτσι αποκλείεται η συγκατάθεση της τράπεζας για μεταβίβαση στον μη δικαιούχο-, αλλά αντίθετα δεν εξαρτάται από όρο η κατοχή τους. Έτσι υλοποιείται το παράδοξο μήνυμα «λάβε τα χρήματα αλλά μην τα ιδιοποιηθείς»[29].

2.5 Η αδυναμία των λύσεων που υποστηρίχθηκαν να επιλύσουν το πρόβλημα

Τελικά η φύση της πράξης της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ δεν είναι έγκλημα κατά της ιδιοκτησίας. Η κάρτα αυτόματης ανάληψης και ο PIN είναι απλά μέσα της τυπικής νομιμοποίησης του χρήστη. Εφόσον ο τελευταίος επιτύχει την τυπική του νομιμοποίηση δεν τελεί βεβαιότατα κοινή απάτη (386 ΠΚ), εφόσον όπως είδαμε παραπάνω το άρθρο αυτό δεν έχει εφαρμογή σε ηλεκτρονικά συστήματα. Δεν τελεί όμως ούτε κλοπή ούτε υπεξαίρεση, αφού η τράπεζα συγκατατίθεται δια του ΑΤΜ στη μεταβίβαση της κατοχής και της κυριότητας σε οποιονδήποτε χρήστη εμφανίζεται ως τυπικά νομιμοποιούμενος.

2.6 Η επέμβαση του Έλληνα νομοθέτη και η εισαγωγή του 386Α ΠΚ

Διαγιγνώσκοντας, ο Έλληνας νομοθέτης, την ανάγκη κάλυψης εγκληματικής ύλης, η οποία δεν θα μπορούσε να υπαχθεί στις παραδοσιακές αντικειμενικές υποστάσεις,

[27] Ι. Μανωλεδάκης, Εγκλήματα κατά της ιδιοκτησίας, 2002, σελ. 34.

[28] Β. Ζησιάδης, Η οικονομική εγκληματικότητα, 2002, σελ. 111 «Νομίζουμε, ότι στην περίπτωση αυτή, ορθότερη είναι η άποψη ότι πρόκειται για κλοπή ή για υπεξαίρεση».

[29] Θ. Σάμιος, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, 2010, σελ. 208.

επενέβη με την εισαγωγή νέων διατάξεων που είχαν ως σκοπό να συμβαδίσουν με τις τεχνολογικές εξελίξεις. Το έργο της νομοθέτησης ήταν δύσκολο, καθότι οι νέες αντικειμενικές υποστάσεις θα έπρεπε να είναι μεν ευρείες –ώστε να καλύπτουν ύλη που θα προκύψει από τις μέλλουσες τεχνολογικές εξελίξεις-, αλλά και στενές -ώστε να μην υπάρχει ζήτημα αντισυνταγματικότητας[30]. Σύμφωνα με την Εισηγητική Έκθεση του σχεδίου νόμου της 9ης Μαΐου 1988, η θέσπιση νέων ποινικών διατάξεων ήταν αναγκαία «γιατί η αξιόποινη δραστηριότητα, η οποία μπορεί να αναπτυχθεί στον τομέα της πληροφορικής, δεν καλύπτεται πλήρως από την υπάρχουσα ποινική νομοθεσία[31]». Έτσι, με το άρθρο 5 του ν. 1805/1988 εισήχθη το άρθρο 386Α με τον τίτλο «απάτη με υπολογιστή». Το νέο αυτό ειδικό έγκλημα απάτης θα διέπραττε όποιος επηρεάζει μια διαδικασία επεξεργασίας δεδομένων υπολογιστή «με μη κατάλληλη διαμόρφωση ή αθέμιτη παρέμβαση ή με τη χρησιμοποίηση εσφαλμένων ή ελλιπών στοιχείων»[32].

2.7 Η πρώτη προσπάθεια αντιμετώπισης της απάτης στις ηλεκτρονικές συναλλαγές μέσω του 386Α ΠΚ

2.7.1 Η αντιμετώπιση του προβλήματος υπαγωγής για τη χωρίς δικαίωμα ανάληψη μετρητών από ΑΤΜ στην ελληνική έννομη τάξη

Παρόλο που το άρθρο 386Α ΠΚ, κατά το χρόνο της θέσπισής του, είχε να αντιμετωπίσει κατά κύριο λόγο την χωρίς δικαίωμα χρήση κωδικών καρτών αυτόματης συναλλαγής[33], στην Εισηγητική Έκθεση του ελληνικού νόμου δεν γίνεται καμία ειδική αναφορά στα ΑΤΜ. Ίσως βέβαια, ο Έλληνας νομοθέτης, να μην ήταν αρκετά εξοικειωμένος με την εγκληματική ύλη των αυτόματων μηχανών ανάληψης, δεδομένου

[30] Σύμφωνα με το άρθρο 7 παρ. 1 του Συντάγματος, ο νόμος πρέπει να ορίζει τα στοιχεία της πράξης. Αυτή η απαίτηση για την μη αοριστία της πράξης δεν επαναλαμβάνεται στο άρθρο 7 της ΕΣΔΑ, αν και το ΕΔΔΑ έχει αποδεχτεί με νομολογία του, ότι ο νόμος πρέπει να περιγράφει με επάρκεια την πράξη.

[31] Η Εισηγητική Έκθεση, συνεχίζοντας αναφέρει ότι «αυτή η νέα μορφή τεχνολογίας μπορεί να ανοίξει δρόμους σε νέες, άγνωστες και με εφαρμογές αντίστοιχης τεχνολογίας μεθόδους εγκληματικής δράσης, οι οποίες δεν προβλέπονται από τον Ποινικό Κώδικα και τους ισχύοντες ειδικούς ποινικούς νόμους».

[32] Βλ. Κ. Βλαχόπουλο, Ηλεκτρονικό έγκλημα, 2007, υποσημείωση 129, σελ. 144 «προκαλεί εντύπωση το πόσο νωρίς προστέθηκαν στο υπάρχον νομοθετικό πλαίσιο».

[33] ΑρχΝ ΝΕ' (2004), Νικολαΐδης, 465 επ.

ότι πριν την εισαγωγή του άρθρου 386Α ΠΚ, ουδέποτε είχε κριθεί στην ελληνική νομολογία περίπτωση ανάληψης από ΑΤΜ με ξένη κάρτα[34].

2.7.2 Η αντιμετώπιση του προβλήματος στη Γερμανική έννομη τάξη

Από την άλλη πλευρά, στην εισηγητική έκθεση του γερμανικού νόμου αναφέρεται χαρακτηριστικά ότι ο λόγος της εισαγωγής της διάταξης § 263a του γερμΠΚ, θα πρέπει να αναζητηθεί στην προσπάθεια να αντιμετωπιστούν οι καταχρήσεις σε ΑΤΜ δια της αθέμιτης χρησιμοποίησης δεδομένων. Ο Γερμανός νομοθέτης, μάλιστα, δεν αρκέστηκε σε εξαγγελία του λόγου εισαγωγής, αλλά προέβλεψε ρητά στον νόμο την περίπτωση της «χωρίς δικαίωμα χρησιμοποίησης (ορθών) στοιχείων», επιλύοντας μια για πάντα το πρόβλημα εφαρμογής, σε σχέση με την αθέμιτη χρήση καρτών αυτόματης συναλλαγής.

3 Το πρόβλημα εφαρμογής του άρθρου 386Α ΠΚ και η αναζήτηση λύσης μέσα από την αντικειμενική του υπόσταση

Φαίνεται ότι ο Έλληνας νομοθέτης, δεν επιδίωξε πραγματικά να διαλευκάνει αν με τη νέα διάταξη του 386Α, καλύπτεται η πράξη της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ. Αντίθετα από το γερμανικό της πρότυπο, η ελληνική διάταξη περιέλαβε την περίπτωση «με οποιονδήποτε άλλο τρόπο» επηρεασμού των στοιχείων[35] υπολογιστή, δημιουργώντας πλήθος προβλημάτων. Έτσι η λύση της απάτης με υπολογιστή δεν έγινε ποτέ αποδεκτή από την πλειοψηφία της νομολογίας και της επιστήμης για την αντιμετώπιση της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ. Υπ' αυτή την έννοια, δικαιολογημένα ο Ναμίας[36], έκανε λόγο για «προχειρότητα» της διάταξης, «αν όχι … ατυχή επιλογή του Έλληνα νομοθέτη».

---

[34] Η μόνη σχετική υπόθεση που είχε απασχολήσει την ελληνική νομολογία, ήταν η ανάληψη από τον ίδιο τον δικαιούχο, καθ' υπέρβαση του πιστωτικού ορίου. Η πράξη αυτή κρίθηκε ως κλοπή από Διαρκ.Στρατ.Θεσσ 401/1986, ΠοινΧρ ΛΣΤ' (1986), σελ. 776.

[35] Στη σημερινή μορφή της διάταξης 386Α ΠΚ, τα «στοιχεία υπολογιστή» έχουν αντικατασταθεί από τον όρο «δεδομένα υπολογιστή», αφού αυτή η ορολογία ακολουθείται από τη Σύμβαση του Συμβουλίου της Ευρώπης (της 21ης Νοεμβρίου 2001) «για το έγκλημα στον κυβερνοχώρο» και την Οδηγία 2013/40/ΕΕ (12ης Αυγούστου 2013) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

[36] Ο. Ναμίας, ΠοινΧρ ΝΓ' (2003), σελ. 493.

3.1 Τα «δεδομένα υπολογιστή»

Σύμφωνα με το άρθρο 1 στοιχείο β' της Σύμβασης της Βουδαπέστης[37], ως δεδομένο υπολογιστή νοείται κάθε «αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη για να υποστεί επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή». Συνεπώς, δεδομένα υπολογιστή αποτελούν τα δεδομένα που περιέχει το chip και η μαγνητική λωρίδα της κάρτας αυτόματης συναλλαγής και τα δεδομένα που περιέχει η κάρτα ή το κινητό τηλέφωνο, τα οποία μεταδίδονται εντός κοντινού πεδίου για την επίτευξη της ανέπαφης συναλλαγής. Τα παραπάνω δεδομένα αφορούν πληροφορίες σχετικά με τον χρήστη, το διαθέσιμο υπόλοιπο του λογαριασμού του, τους πόντους επιβράβευσης που τυχόν διαθέτει, τον αριθμό PIN, καθώς και τις επιτρεπόμενες εναπομείνασες προσπάθειες εισαγωγής του. Αντίθετα, δεν είναι δεδομένο υπολογιστή ο ίδιος ο υλικός φορέας της κάρτας, δηλαδή το πλαστικό υλικό της.

3.2 Ο «επηρεασμός»

Ο δράστης του αδικήματος του άρθρου 386Α ΠΚ βλάπτει ξένη περιουσία «επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή» με κάποιον από τους αναφερόμενους τρόπους. Έτσι, αντικείμενο του επηρεασμού είναι το αποτέλεσμα της διαδικασίας επεξεργασίας δεδομένων και όχι τα «στοιχεία του υπολογιστή» όπως οριζόταν στο προ του ν. 4411/2016 καθεστώς. Και επί του παλαιού καθεστώτος γινόταν δεκτό ότι ο επηρεασμός των στοιχείων του υπολογιστή μπορεί να περιλαμβάνει τόσο τα εισαγόμενα «input», όσο και τα εξαγόμενα στοιχεία «output», δηλαδή το αποτέλεσμα της επεξεργασίας των δεδομένων[38]. Βέβαια, η αντίστοιχη γερμανική διάταξη έκανε πάντα λόγο για επηρεασμό του αποτελέσματος της επεξεργασίας δεδομένων (Ergebnis eines Datenverarbeitungsvorgangs) και στο αποτέλεσμα αυτό

[37] Βλ. και τεχνικό κανόνα DIN-Norm 44300 (αριθμός 19), όπου ως στοιχεία υπολογιστή νοούνται «όλες οι πληροφορίες που εκφράζονται μέσω σημείων ή συνεχών λειτουργιών, επί τη βάση γνωστών ή εικαζόμενων συμφωνιών, προκειμένου να καταστούν αντικείμενο επεξεργασίας». Στον κανόνα αυτό κατέφευγε η γερμανική επιστήμη για τον προσδιορισμό των στοιχείων στην αντίστοιχη διάταξη 263a του ΓερμΠΚ. Βλ. ΠλημμΑθ 638/2008 (ΠοινΧρ. Ξ/2010, σελ. 775).

[38] Δ. Κιούπης, Ποινικό δίκαιο και internet, 1999 σελ. 116, 117 υποσημείωση 165.

στρεφόμασταν και εμείς για να εντοπίσουμε το αληθινό νόημα του επηρεασμού[39], ακόμα και πριν τον ν. 4411/2016.

3.2.1 Η κανονιστική προσέγγιση του επηρεασμού

Ο Μυλωνόπουλος[40] υποστήριξε ότι «ο επηρεασμός … είναι νομικά αξιόλογος μόνον όταν δημιουργείται μία κατάσταση ανάλογη προς την απάτη του άρθρου 386 ΠΚ, δηλαδή όταν το αποτέλεσμα της επεξεργασίας αποκλίνει, λόγω της συμπεριφοράς του δράστη, από εκείνο που θα επιτυγχανόταν με κανονική και σύννομη εκτέλεση[41] του προγράμματος και η απόκλιση αυτή μπορεί να καταλογιστεί στον δράστη[42]». Έτσι, κατά την άποψη αυτή, ο επηρεασμός δεν συνίσταται μόνο σε τεχνική παρέκκλιση αλλά κρίνεται και με βάση την σύννομη[43] ή μη εκτέλεση του προγράμματος. Ως σύννομη εκτέλεση, δε, νοείται εκείνη που δεν αποκλίνει από τον νόμιμο και προσδοκώμενο τρόπο εκτέλεσης ενός προγράμματος.

3.2.2 Η τεχνική προσέγγιση του επηρεασμού

Σε αντίθεση με την κανονιστική προσέγγιση, η τεχνική προσέγγιση του επηρεασμού των στοιχείων, εντοπίζει τον επηρεασμό στην απλή παραβίαση των κανόνων λειτουργίας του προγράμματος του υπολογιστή. Ο Ναμίας θεωρεί ότι ο επηρεασμός συντρέχει όταν το αποτέλεσμα της επεξεργασίας αποκλίνει από εκείνο που θα επιτυγχανόταν με κανονική εκτέλεση του προγράμματος -όχι κατ' ανάγκη και σύννομη[44].

Η «κανονικότητα» της εκτέλεσης του προγράμματος λοιπόν, ανάγεται σε κριτήριο για να διαγνωσθεί αν προκλήθηκε ή όχι ο επηρεασμός. Έτσι, είναι αναγκαία η τεχνική διερεύνηση, «κατά πόσο το παραγόμενο αποτέλεσμα ανταποκρίνεται στον τρόπο προγραμματισμού του υπολογιστή, ήτοι στο σύνολο αποθηκευμένων στο σύστημα

---

[39] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 57, Δ. Κιούπης, ό.π., Γ. Μπουρμάς, ΠοινΧρ ΝΑ' (2001), σελ. 470,Ι. Καρακώστας, Δίκαιο και Internet, 2009, σελ. 247.

[40] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 57.

[41] Χ. Μυλωνόπουλος, Ποινικό Δίκαιο - Ειδικό Μέρος, 2016, σελ. 552.

[42] Έτσι και σε Συμβ.Ναυτ.Πειραιώς 418/1996.

[43] Βλ. Συμβ.Πλημ.Κιλκίς 54/2012 ΠοινΔνη 2014, σελ. 238 «Σε αυτή την περίπτωση ο δράστης επηρεάζει τα στοιχεία του υπολογιστή όταν το αποτέλεσμα της επεξεργασίας των δεδομένων, λόγω της συμπεριφοράς του αποκλίνει από εκείνο που θα επιτυγχανόταν με κανονική και σύννομη εκτέλεση του προγράμματος».

[44] Ο. Ναμίας, Σύγχρονες μορφές (ηλεκτρονικής) απάτης στις τραπεζικές συναλλαγές, Τιμητικός Τόμος Ανδρουλάκη, 2003, σελ. 467 επ. και ΠοινΧρ. ΝΓ' (2003), σελ. 491.

στοιχείων, δεδομένων και εντολών και τον τρόπο συσχετισμού τους, όπως αυτός έχει εκ των προτέρων καθοριστεί στο συγκεκριμένο πρόγραμμα»[45]. Ο Μπουρμάς[46] θεωρεί ότι «ο επηρεασμός θα συνίσταται στο αποτέλεσμα της επεξεργασίας των δεδομένων του Η/Υ, το οποίο θα πρέπει να αποκλίνει από εκείνο το αποτέλεσμα, που αναμένεται από την κανονική και άνευ παρεμβάσεως εκτέλεση του προγράμματος».

3.2.3 Η προηγούμενη θέση της θεωρίας σχετικά με τη (μη) κατάφαση του στοιχείου του επηρεασμού στην περίπτωση της ανάληψης μετρητών από ΑΤΜ με ξένη κάρτα

Σύμφωνα με τον Παπαδαμάκη[47], «η χρησιμοποίηση ορθών δεδομένων χωρίς δικαίωμα (π.χ. η χρήση κλεμμένης πιστωτικής κάρτας) δεν συνιστά επηρεασμό του προγράμματος ή των δεδομένων υπολογιστή, αλλά εκμετάλλευση της (ανεπηρέαστης ως προς το πρόγραμμα ή τα δεδομένα) λειτουργίας του υπολογιστή». Απαιτώντας μια αναλογία με την παραπλάνηση της κοινής απάτης κρίνει ότι αυτό που προκαλεί την περιουσιακή βλάβη δεν είναι εδώ ο επηρεασμός του μηχανήματος[48]. Αντίθετα, είναι ο ίδιος ο δράστης που με δική του πράξη τελεί την περιουσιακή βλάβη, εκμεταλλευόμενος απλά, το ΑΤΜ. Τονίζεται έτσι, η διαφορά του επηρεασμού -που συνεπάγεται ένα παγιωμένο μετασχηματισμό του προγράμματος- και της απλής εκμετάλλευσης του ΑΤΜ. Καταλήγει ότι η απλή εκμετάλλευση του ΑΤΜ[49] «δεν θα πρέπει να ταυτίζεται με τον επηρεασμό, διότι μια τέτοια θεώρηση ίσως θα οδηγούσε σε απαγορευμένη διασταλτική συμπλήρωση του γράμματος διάταξης (άρθρο 1 ΠΚ, 7 παρ. 1 Συντάγματος)».

Αντίστοιχα, η Καϊάφα – Γκμπάντι[50] ορίζοντας αρνητικά τον επηρεασμό, υποστηρίζει ότι αυτός δεν συντρέχει, «όταν τα στοιχεία του υπολογιστή είναι και λειτουργούν κανονικά στη συγκεκριμένη περίπτωση, όπως ακριβώς συμβαίνει και στις περιπτώσεις της νόμιμης χρήσης τους». Με αυτό το σκεπτικό θεωρεί ότι δεν συντρέχει το

[45] Ό.π.

[46] Γ. Μπουρμάς, ΠοινΧρ ΝΑ' (2001), σελ. 470.

[47] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 159-161.

[48] Το μηχάνημα συνεχίζει να λειτουργεί όπως εξαρχής προγραμματίστηκε.

[49] Δηλαδή η εισαγωγή στο ΑΤΜ ορθών δεδομένων (γνήσιας κάρτας) από την πλευρά του δράστη για την πρόκληση της περιουσιακής βλάβης.

[50] Μ. Καϊάφα – Γκμπάντι, Αρμενόπουλος 61 (2007), σελ. 1080.

στοιχείο του επηρεασμού στην περίπτωση ανάληψης μετρητών από ΑΤΜ με ξένη κάρτα, αφού η χρήση του ΑΤΜ με γνήσια κάρτα αποτελεί κανονική χρήση του συστήματος.

3.2.4 Η θέση της νομολογίας σχετικά με το στοιχείο του επηρεασμού

Η πρόσφατη νομολογία του Αρείου Πάγου δέχεται παγίως ότι συντρέχει το στοιχείο του επηρεασμού στην περίπτωση της ανάληψης μετρητών από ΑΤΜ με ξένη (γνήσια) κάρτα. Για παράδειγμα στην απόφαση ΑΠ 562/2020 αναφέρεται ότι «έβλαψαν ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή, με τη χρήση ψευδών στοιχείων» «εισήγαγαν κάρτα αυτόματων αναλήψεων … σε μηχανήματα ΑΤΜ … και πληκτρολογώντας τον αριθμό PIN, του οποίου είχαν λάβει γνώση προηγουμένως, επηρέασαν τα στοιχεία του υπολογιστή που διαθέτουν τα μηχανήματα αυτά, προβαίνοντας σε αναλήψεις μετρητών[51]». Αντίστοιχα, η ΑΠ 1726/2019 επισημαίνει ότι «εισήγαγαν την κάρτα ανάληψης χρημάτων την οποία είχαν αφαιρέσει παρανόμως από την κατοχή της εγκαλούσας … πληκτρολογώντας και τον αριθμό PIN τον οποίο έλαβαν γνώση παρανόμως … και με τον τρόπο αυτό επηρέασαν τα στοιχεία του υπολογιστή που διαθέτει το μηχάνημα αυτό, παραπλανώντας τους υπαλλήλους της … για το ότι είναι νόμιμοι κάτοχοι της ανωτέρω κάρτας». Η τελευταία, με την αναφορά της σε παραπλάνηση των υπαλλήλων δείχνει, βέβαια, να συγχέει την απάτη με υπολογιστή με την κοινή απάτη[52]. Όπως εύστοχα τονίζεται στην ΑΠ 813/2015, «το έγκλημα της απάτης με υπολογιστή του αρ. 386Α ΠΚ 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

[51] «εμφανίζοντας στο ηλεκτρονικό πρόγραμμα αυτοματοποιημένης διαδικασίας εκταμίευσης μετρητών, που είχε σχεδιαστεί να υπακούει σε εντολές του εμφανιζόμενου ως νομίμου κατόχου της ως άνω κάρτας, ότι αυτοί (κατηγορούμενοι) ήταν οι νόμιμοι κάτοχοι των εν λόγω καρτών και δικαιούνταν σε ανάληψη των σχετικών ποσών από τον ανωτέρω τραπεζικό λογαριασμό». Διαφορετική η περίπτωση που έκρινε η ΑΠ 1087/2019 στην οποία οι κατηγορούμενοι δημιούργησαν αυτοσχέδιους μηχανισμούς παγίδευσης με τους οποίους υπέκλεπταν τα στοιχεία των γνήσιων καρτών και στη συνέχεια δημιουργούσαν νέες πλαστές κάρτες -κλώνους.

[52] Αναφέρεται, προφανώς, για να παρουσιάσει την δομική ομοιότητα της συμπεριφοράς της απάτης με υπολογιστή προς την κοινή απάτη, «αφού η συμπεριφορά αυτή θα συνιστούσε πράξη εξαπάτησης με συμπερασματικά συναγόμενη δήλωση αν είχε τελεστεί ενώπιον υπαλλήλου της τράπεζας», βλ. Χ. Μυλωνόπουλο, Ποινικό Δίκαιο – Ειδικό Μέρος, 2016, σελ. 553.

εγκρίνει ή να χορηγεί[53] κλπ., αλλά αποκλειστικά και μόνο με τον επηρεασμό των στοιχείων του υπολογιστή»[54]. Η ίδια απόφαση επαναλαμβάνει και την κρίση του ΤριμΕφΑθ ότι, «εισάγοντας την κάρτα και πληκτρολογώντας τον PIN επηρέασε με τον τρόπο αυτό τα στοιχεία του υπολογιστή των μηχανημάτων ΑΤΜ, διότι η εκ μέρους της χρήση της πιστωτικής κάρτας παρείχε στον υπολογιστή την συμπερασματικά συναγόμενη δήλωση ότι η χρήση γινόταν κάθε φορά από τον νόμιμο κάτοχο της πιστωτικής κάρτας, ενώ αυτό δεν συνέβαινε». Τέλος, η ΠλημμΑθ. 3668/2006, αν και δεν αφορά περίπτωση ανάληψης από ΑΤΜ, τονίζει ότι ο επηρεασμός των στοιχείων Η/Υ πρέπει να προκαλεί άμεση μείωση ξένης περιουσίας[55].

3.2.5 Συμπεράσματα σχετικά με το στοιχείο του επηρεασμού

Συμπερασματικά, ως επηρεασμός θα πρέπει να νοείται κάθε επέμβαση στο σύστημα, η οποία καθιστά παρεκκλίνοντα τα αποτελέσματα της διαδικασίας επεξεργασίας, σε σύγκριση με τα αποτελέσματα που θα επέρχονταν, σύμφωνα με την κανονική λειτουργία του προγράμματος και τείνει στη δημιουργία περιουσιακής βλάβης. Συνεπώς, αν θεωρήσουμε ότι στην περίπτωση μας το αποτέλεσμα της διαδικασίας επεξεργασίας του προγράμματος του ΑΤΜ, είναι να παραδίδονται τα χρήματα στον νόμιμο κάτοχο της κάρτας, τότε εκείνος που εισάγει την κάρτα και τον αριθμό PIN χωρίς να είναι νόμιμος κάτοχος, επηρεάζει το αποτέλεσμα της διαδικασίας βλάπτοντας τον πραγματικό δικαιούχο[56]. Και τούτο, διότι χωρίς την πράξη του τα αποτελέσματα δεν θα επέρχονταν καθόλου ή θα επέρχονταν διαφορετικά. Με τούτη την ερμηνεία αποφεύγεται και η ταύτιση του επηρεασμού με την απλή εκμετάλλευση του συστήματος. Γιατί δεν

---

[53] Με την ίδια διατύπωση και η Πλημμ.Αθ. 1213/2007 (ΠοινΧρ ΝΗ/2008, σελ. 634) απορρίπτει την απάτη με υπολογιστή «όταν η περιουσιακή βλάβη επέρχεται με την παραπλάνηση ενός φυσικού προσώπου που είναι αρμόδιο να λαμβάνει αποφάσεις ή να διενεργεί έλεγχο ή να εγκρίνει ή να χορηγεί κλπ.».

[54] Το ΤριμΕφΑθ που δίκαζε σε δεύτερο βαθμό την υπόθεση αυτή, έκανε και πάλι λόγο για παραπλάνηση των υπαλλήλων: «εισάγοντας και … πληκτρολογώντας τον αριθμό PIN … με τον τρόπο αυτό επηρέασε τα στοιχεία του υπολογιστή παραπλανώντας τους υπαλλήλους Τράπεζας … για το ότι είναι νόμιμος κάτοχος της ανωτέρω πιστωτικής και δικαιούχος του συνδεδεμένου με αυτές τραπεζικού λογαριασμού».

[55] Σύμφωνα με την Πλημμ.Αθ. 3668/2006 (ΠοινΧρ ΝΖ/2007, σελ. 271) «η περιουσιακή ζημία είναι άμεση όταν δεν απαιτείται παρεμβολή ανθρώπινης συμπεριφοράς μεταξύ της επεξεργασίας των στοιχείων και της μείωσης της περιουσίας, όπως για παράδειγμα όταν ο υπολογιστής εμφανίζει αυξημένο ποσό στον λογαριασμό του δράστη». Επίσης σε: Χ. Μυλωνόπουλο, Ειδικό Ποινικό, 2016, σελ. 556.

[56] Και δη, με την χωρίς δικαίωμα εισαγωγή ορθών στοιχείων.

μπορεί να δικαιολογείται η κατάφαση του στοιχείου του επηρεασμού όταν η χρήση γίνεται σύμφωνα με την ενδεδειγμένη λειτουργικότητα του μηχανήματος, χωρίς να προκαλείται βλάβη. Και όταν οι δικαστικές αποφάσεις κάνουν λόγο για «αποτέλεσμα διαφορετικό από εκείνο που θα προέκυπτε»[57], αν και αποφεύγουν να ορίσουν «εκείνο που θα προέκυπτε», τελικά «εκείνο», είναι το αποτέλεσμα της διαδικασίας επεξεργασίας δεδομένων το οποίο προκύπτει από την κανονική και σύννομη λειτουργία του.

3.3 Ο τρόπος πρόκλησης του επηρεασμού: Σε ποια υπαλλαγή τέλεσης υπάγεται η χωρίς δικαίωμα χρήση γνήσιας ξένης κάρτας;

Το προηγούμενο καθεστώς προέβλεπε τέσσερις περιπτώσεις επηρεασμού: «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». Με την τροποποίηση του 386Α ΠΚ (παρ. 11 του άρθρου 2 του ν. 4411/3-8-16), ορίζονται πλέον πέντε περιπτώσεις επηρεασμού: 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 δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, ή ε) με τη χωρίς δικαίωμα[58] αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας.

3.3.1 «α) Μη ορθή διαμόρφωση του προγράμματος»

Η πράξη της ανάληψης χρημάτων από ΑΤΜ με ξένη γνήσια κάρτα δεν αφορά την περίπτωση της μη ορθής διαμόρφωσης του προγράμματος. Αυτό συμβαίνει διότι, ο δράστης εισάγοντας την κάρτα και τον αριθμό PIN, δεν αλλοιώνει, ούτε προσθέτει, ούτε αποκρύπτει, ούτε παρακάμπτει βήματα της διαδικασίας, ούτε μεταβάλλει κατ' οποιονδήποτε τρόπο το τρέχον πρόγραμμα ούτε δημιουργεί νέο[59].

[57] ΑΠ 1152/1999 «προκαλεί αποτέλεσμα διαφορετικό από εκείνο που θα προέκυπτε και έτσι βλάπτει ξένη περιουσία προς όφελος αυτού ή τρίτου».

[58] Άλλωστε με το άρθρο 8 παρ. 2β του ν. 4411/2016 (κύρωση της Σύμβασης της Βουδαπέστης), ο Έλληνας νομοθέτης υποχρεώθηκε να ποινικοποιήσει την άνευ δικαιώματος παρέμβαση σε ηλεκτρονικό υπολογιστή.

[59] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 59.

3.3.2 «β) Χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα»

Για παρέμβαση στη λειτουργία πληροφοριακού συστήματος δεν μπορεί να γίνει λόγος στην περίπτωση της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ. Ο επιλήψιμος κάτοχος της κάρτας δεν παρεμβαίνει ούτε από την οθόνη αφής ή το πληκτρολόγιο του ΑΤΜ επηρεάζοντας τη διαδικασία επεξεργασίας, ούτε στα στοιχεία του hardware του τελευταίου[60].

3.3.3 «γ) Χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης ταυτότητας»

Η τρίτη υπαλλαγή του εγκλήματος αναφέρεται στον επηρεασμό δια της χρησιμοποίησης μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας. Στην περίπτωση που μας απασχολεί τα δεδομένα που εισάγει ο χρήστης της κάρτας και ορθά είναι και πλήρη. Είναι αφενός ορθά, διότι ανταποκρίνονται στην πραγματικότητα (τόσο τα δεδομένα που περιέχονται στην κάρτα όσο και ο PIN είναι πραγματικά), αφετέρου πλήρη, διότι δεν έχει παραλειφθεί κανένα δεδομένο[61] που να εκφράζει την πραγματικότητα. Ιδίως, δε, στην περίπτωσή μας δεν χρησιμοποιείται κανένα τέχνασμα για να εισαχθεί στο ΑΤΜ μη ορθό δεδομένο αναγνώρισης ταυτότητας. Τούτη η περίπτωση εφαρμόζεται στην περίπτωση χρήσης πλαστής κάρτας. Τότε τα δεδομένα που ενσωματώνει η κάρτα είναι μη ορθά, αφού δεν ανταποκρίνονται στην πραγματικότητα.

Στο πλαίσιο του καθεστώτος, προ της τροποποίησης της διάταξης 386Α με τον ν. 4411/2016, γινόταν προσπάθεια θεμελίωσης της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ με ξένη κάρτα, σε αυτή -γ΄- υπαλλαγή. Το κύριο επιχείρημα αποτελούσε, ότι τα στοιχεία που εισάγονται είναι ορθά και πλήρη μόνο όταν εισάγονται από τον νομιμοποιούμενο χρήστη. Όταν αντίθετα, τα στοιχεία εισάγονται από μη νομιμοποιούμενο πρόσωπο, τότε αυτά δεν θεωρούνται ορθά και πλήρη -με την έννοια ότι τμήμα της επιζητούμενης πραγματικότητας των δεδομένων αποτελεί και η νομιμοποίηση του χρήστη του ΑΤΜ. Συνεπώς, αυτή η άποψη δεν έχει καμιά αξία[62] αν η ορθότητα και η πληρότητα

---

[60] Χ. Μυλωνόπουλος, Ποινικό Δίκαιο – Ειδικό μέρος, 2016, σελ. 550.

[61] Στ. Παύλου, Γ. Μπέκας, Ποινικό ΙΙΙ Εγκλήματα κατά της Ιδιοκτησίας, Περιουσίας & Ζωής, 2020, σελ. 307, 308.

[62] Μ. Καϊάφα-Γκμπάντι, Αρμενόπουλος 61(2007), σελ. 1081-1082: «η αντιμετώπιση των πιο πάνω συμπεριφορών με παραδοσιακά εγκλήματα κατά της ιδιοκτησίας ή περιουσίας, σε όποιο μέτρο μπορούν να τις καλύψουν, είναι η μόνη εναπομένουσα λύση, όσο ο Έλληνας νομοθέτης δεν περιλαμβάνει ρητά, όπως

των δεδομένων αντιμετωπιστεί αντικειμενικά: Τα στοιχεία είναι ορθά και πλήρη ανεξάρτητα από το ποιος τα εισάγει. Αντίθετα είναι υποστηρίξιμη, αν η ορθότητα εκτιμηθεί με βάση το υποκείμενο[63] που χρησιμοποιεί τα δεδομένα και όχι την αντικειμενική ακρίβειά τους. Ειδικότερα, αν εστιάσουμε στην έλλειψη της πληρότητας, με την έννοια ότι ένα τμήμα της πραγματικότητας, -δηλαδή η νομιμοποίηση του χρήστη-, απουσιάζει. Πάντως, η προτίμηση του του υποκειμενικού κριτηρίου της ορθότητας είναι αυθαίρετη και έτσι, η όλη θεμελίωση τουλάχιστον εύθραυστη. Άλλωστε η απουσία βιομετρικής ταυτοποίησης των χρηστών στα ΑΤΜ[64], μας οδηγεί στο αντίθετο συμπέρασμα -ότι δηλαδή δεν είναι επιζητούμενη η υποκειμενική ορθότητα[65].

3.3.4 «δ) Χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας»

Η περίπτωση της χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ με γνήσια κάρτα, εμπίπτει στην υπαλλαγή του επηρεασμού, με την χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη δεδομένων υπολογιστή. Ο δράστης, βέβαια, που προβαίνει στην ανάληψη μετρητών, δεν επηρεάζει το ΑΤΜ αλλοιώνοντας, διαγράφοντας, μεταδίδοντας ή εξαλείφοντας τα δεδομένα. Όμως, αυτό που με βεβαιότητα κάνει, είναι να εισάγει χωρίς δικαίωμα δεδομένα υπολογιστή. Εισάγοντας, δηλαδή, την κάρτα αυτόματης ανάληψης και τον αριθμό PIN της, χωρίς δικαίωμα, πληροί την αντικειμενική υπόσταση

τούτο συμβαίνει αντίθετα σε άλλες έννομες τάξεις, και τη χωρίς δικαίωμα χρησιμοποίηση στοιχείων στην απάτη με υπολογιστή».

[63] Θ. Σάμιος σε Ποινικές Επιστήμες - θεωρία και πράξη: Προσφορά τιμής στην Άννα Μπενάκη Ψαρούδα, Τόμος Β, 2008, σελ. 534.

[64] Παρόλο που η τεχνολογία υπάρχει εδώ και χρόνια και ανευρίσκεται στο σύνολο των σύγχρονων smartphones, λίγες τράπεζες παγκοσμίως εφοδιάζουν τα ΑΤΜ τους με συστήματα βιομετρικής αναγνώρισης.

Εξαίρεση αποτελεί, η τράπεζα Bradesco στη Βραζιλία, η οποία έχει εγκαταστήσει στα ΑΤΜ της σύστημα αναγνώρισης της παλάμης του χεριού από το 2006. Βλ. Ε. Μπακιρλή, Σύγχρονη Τεχνολογία και Αντεγκληματική Πολιτική, 2019, σελ. 39.

[65] Ούτε και όποιος συναλλάσσεται με το ΑΤΜ προβαίνει σε οποιαδήποτε δήλωση ότι νομιμοποιείται ουσιαστικά. Αυτό που δηλώνει είναι ότι γνωρίζει τον PIN κάτι που είναι απολύτως αληθές. Η εισαγωγή του PIN είναι δήλωση τυπικής νομιμοποιήσεως και όχι ουσιαστικής. Έτσι δεν διαπράττει έγκλημα και όποιος εξουσιοδοτείται να προβεί σε ανάληψη για να εξυπηρετήσει τον πραγματικό δικαιούχο. Βλ. Θ. Σάμιο, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, σελ. 299-300 “τα γνήσια κέρματα που τοποθετούνται στον αυτόματο πωλητή δεν χάνουν την γνησιότητά τους επειδή είναι κλεμμένα».

της συγκεκριμένης υπαλλαγής του εγκλήματος του άρθρου 386Α του ΠΚ. Έτσι, η «χωρίς δικαίωμα χρησιμοποίηση (ορθών) δεδομένων», όπως προβλεπόταν εδώ και δεκαετίες, στην αντίστοιχη Γερμανική διάταξη, ήρθε -έστω και εσχάτως- για να καλύψει τις περιπτώσεις αθέμιτης χρήσης καρτών ανάληψης χρημάτων και στην χώρα μας[66].

Η προσθήκη της περίπτωσης δ' της «χωρίς δικαίωμα εισαγωγής δεδομένων», επήλθε με τον ν. 4411/2016, ο οποίος αποτελεί κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης). Η τελευταία υποχρέωνε τον Έλληνα νομοθέτη να ποινικοποιήσει, μεταξύ άλλων, και την άνευ δικαιώματος παρέμβαση σε ηλεκτρονικό υπολογιστή[67]. Σύμφωνα, δε, με το άρθρο 2 περ. δ' της Οδηγίας 2013/40/ΕΕ[68], ως «χωρίς δικαίωμα» νοείται «η συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου». Το στοιχείο «χωρίς δικαίωμα» στο άρθρο 386Α ΠΚ, συνιστά ειδικό στοιχείο του αδίκου που οριστικοποιεί τον άδικο χαρακτήρα της σχετικής συμπεριφοράς[69].

Άλλωστε, και σύμφωνα με την αιτιολογική έκθεση του σχεδίου νόμου για την Κύρωση της Σύβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, η νέα διάταξη του 386Α, περιέλαβε πλέον ρητά στις περιπτώσεις απάτης με υπολογιστή και τη χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα, για να καλύψει περιπτώσεις, όπως αυτή που μας απασχολεί εδώ[70].

---

[66] Δ. Κιούπης, Ποινικό δίκαιο και Internet, 1999 σελ. 114-115.

[67] Άρθρο 8 του ν. 4411/2016: Απάτη σχετική με υπολογιστές «Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας δια της β. παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο».

[68] Άρθρο 2 περ. δ' της Οδηγίας 2013/40/ΕΕ της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών.

[69] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 162.

[70] Αιτιολογική έκθεση του σχεδίου νόμου για την Κύρωση της Σύβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο, σελ. 6.

3.3.5 «ε) Χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας»

Η περίπτωση αυτή αφορά την αξιοποίηση των ηλεκτρονικών εφαρμογών μεταφοράς χρημάτων (e-banking), χωρίς δικαίωμα[71]. Αφορά, δηλαδή, περιπτώσεις δραστών που έχουν αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου[72] και αξιοποιούν τις εφαρμογές για να προβούν σε αθέμιτες μετακινήσεις χρηματικών ποσών[73]. Έτσι, η λύση της κλοπής, στην οποία αναφερθήκαμε παραπάνω[74], δεν μπορεί πια να υποστηρίζεται για την περίπτωση της μεταφοράς νομισματικών μονάδων σε άλλο λογαριασμό[75].

3.3.6 Η ρήτρα «με οποιονδήποτε άλλο τρόπο» ως περίπτωση επηρεασμού πριν από την τροποποίηση του άρθρου 386Α ΠΚ με τον ν. 4411/2016

Για λόγους πληρότητας, θα πρέπει να αναφερθεί ότι πριν από την τροποποίηση της διάταξης του 386Α με τον ν. 4411/2016, τυποποιούνταν ως υπαλλαγή τέλεσης της απάτης με υπολογιστή, η «με οποιονδήποτε άλλο τρόπο» πρόκληση επηρεασμού των στοιχείων υπολογιστή. Τούτη η γενική ρήτρα «με οποιονδήποτε άλλο τρόπο», κατακρίθηκε από την πλειοψηφία της επιστήμης[76], διότι δεν μπορούσε να θεωρηθεί σύμφωνη με την επιταγή του άρθρου 7 παρ. 1 του Συντάγματος ο νόμος «να ορίζει τα στοιχεία της πράξης». Σε κάθε περίπτωση, όμως, η υπαλλαγή αυτή δεν αφορούσε -μάλλον- τη χωρίς δικαίωμα ανάληψης χρημάτων από ΑΤΜ με γνήσια κάρτα, αν και ο Μυλωνόπουλος είχε υποστηρίξει το αντίθετο[77]. Συμφωνία υπήρχε μόνο για την περίπτωση του πιστού αντιγράφου γνήσιας κάρτας, την οποία ενέτασσε η θεωρία σε αυτή την υπαλλαγή τέλεσης. Και τούτο συνέβαινε διότι τόσο η δημιουργία πλαστής κάρτας όσο και οι πολλαπλοί

[71] Η ΑΠ 1700/2010 αντιμετώπισε περίπτωση χρησιμοποίησης username και κωδικών πρόσβασης (που είχαν υποκλαπεί προηγουμένως) για τη μεταφορά χρημάτων μέσω e-banking.

[72] Δ. Κιούπης, Ποινικό Δίκαιο και Internet, 1999, σελ. 119.

[73] Για το ζήτημα βλ. Ι. Μοροζίνη σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, 2023, σελ. 131επ.

[74] Βλ. παραπάνω 2.3.4.

[75] Ε. Συμεωνίδου-Καστανίδου, Υπεράσπιση 8 (1998), σελ. 937επ.

[76] Ο. Ναμίας, ΠοινΧρ ΝΓ' (2003), σελ. 492 «ρήτρα γενική και αόριστη και ως εκ τούτου προβληματική», Ν. Κουράκης, Το έγκλημα της απάτης, 2001, σελ. 207επ. «συνταγματικά αμφίβολη αοριστία».

[77] Χ. Μυλωνόπουλος Ειδικό Ποινικό, 2016, σελ. 552: «η ευρεία διατύπωση … επιτρέπει την υπαγωγή σ' αυτήν και περιπτώσεων επηρεασμού ακόμη και μη τη μη σύννομη χρήση ορθών στοιχείων».

κλώνοι της εντάσσονταν στην ειδικότερη υπαλλαγή της «χρησιμοποίησης μη ορθών στοιχείων»[78].

4 Η σημερινή μορφή της απάτης με υπολογιστή (386Α ΠΚ)

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.

[78] Θ. Σάμιος, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, 2010, σελ. 358,359.

4.1 Το προστατευόμενο έννομο αγαθό

Τόσο η διατύπωση της διάταξης, όσο και η συστηματική της κατάταξη στο 23ο κεφάλαιο των εγκλημάτων κατά περιουσιακών αγαθών, δεν αφήνουν περιθώριο αμφισβήτησης ότι το προστατευόμενο έννομο αγαθό της διάταξης 386Α ΠΚ είναι η αποτιμητή σε χρήμα περιουσία, ως σύνολο οικονομικών στοιχείων του παθόντος[79]. Έχουν, βέβαια, υποστηριχθεί επικουρικά και άλλες απόψεις σχετικά με το προστατευόμενο αγαθό, χωρίς ιδιαίτερη απήχηση στη δική μας έννομη τάξη. Για παράδειγμα έχει υποστηριχθεί ότι προστατεύονται τα συστήματα συναλλαγών χωρίς μετρητά ή η ασφάλεια των περιουσιακών συναλλαγών μέσω υπολογιστή[80].

4.2 Αντικειμενική υπόσταση

4.2.1 Υποκείμενο τέλεσης

Δράστης του εγκλήματος μπορεί να είναι οποιοδήποτε πρόσωπο όπως προδίδει το γράμμα του νόμου «όποιος». Πρόκειται επομένως για έγκλημα κοινό.

4.2.2 Αντικείμενο προσβολής

Αντικείμενο προσβολής του εγκλήματος της απάτης με υπολογιστή είναι η συγκεκριμένη περιουσία, ως σύνολο οικονομικών στοιχείων αποτιμητών σε χρήμα[81]. Παλαιότερα, γινόταν δεκτό ότι η διατύπωση της διάταξης έχει «θυματολογικό χαρακτήρα»[82]. Αυτό σήμαινε, ότι η περιουσιακή βλάβη εμφανιζόταν αποσυνδεδεμένη από το πρόσωπο του θύματος, έτσι ώστε να νοείται βλάβη και χωρίς την εξειδίκευση των προσώπων των οποίων μειώθηκε η περιουσία τους. Υπό τη σημερινή μορφή του άρθρου 386Α κάτι τέτοιο δεν μπορεί να γίνει δεκτό, αφού πλέον δεν υπάρχει η πρόβλεψη ότι «περιουσιακή βλάβη υπάρχει ακόμα και αν τα πρόσωπα είναι άδηλα»[83].

---

[79] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 57.

[80] Βλ. Νούσκαλη σε ΠοινΔικ 2/2003, σελ. 178,180.

[81] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 155.

[82] Ειρ. Βασιλάκη, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σελ. 219.

[83] Το άρθρο 386Α παρ. 1 μέχρι και το ν. 4411/2016, ανέφερε στα δύο τελευταία του εδάφια: «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».

Η αποσύνδεση, βέβαια, από τα πρόσωπα των θυμάτων δεν ήταν τυχαία επιλογή του νομοθέτη, αφού συνήθως η απάτη με υπολογιστή προσβάλλει την περιουσία περισσότερων φυσικών ή νομικών προσώπων και όχι ένα πρόσωπο ατομικά. Για παράδειγμα η άντληση 0,1 ευρώ από κάθε χρήστη ηλεκτρονικής τραπεζικής, μπορεί να αποτελεί μικρή βλάβη για κάθε επιμέρους υποκείμενο που προσβλήθηκε, αλλά η συνολική ζημία που προκαλείται από την πράξη είναι μεγάλη και το έγκλημα θα είναι ένα[84]. Έτσι, ο Παπαδαμάκης κρίνει[85] ότι οι περισσότερες περιουσίες των χρηστών αποτελούν έτσι μια επιφάνεια προσβολής, εκτίθενται στην προσβολή του δράστη ως μία περιουσία και έτσι συνδέονται με την τέλεση μιας απάτης με υπολογιστή[86].

4.2.3 Αξιόποινη συμπεριφορά

Στο άρθρο 386Α ΠΚ περιγράφονται περισσότερες από μία μορφές εγκληματικής δράσης. Στην πρώτη παράγραφο περιγράφεται το βασικό έγκλημα και οι τρόποι τέλεσής του, οπότε πρόκειται για πολύτροπο ή υπαλλακτικώς μικτό έγκλημα[87]. Στην παρ. 2 ποινικοποιούνται αυτοτελώς ως ιδιώνυμο έγκλημα οι προπαρασκευαστικές πράξεις που προορίζονται για τη διάπραξη του εγκλήματος της παρ. 1. Τέλος, στο β' εδάφιο της παρ. 1 και στην παρ. 3 μορφοποιούνται δύο διακεκριμένες παραλλαγές, όταν η απάτη με υπολογιστή προξένησε ζημία μεγαλύτερη από 120.000 ευρώ ή και στρέφεται κατά του δημοσίου.

4.2.4 Το βασικό έγκλημα της 386Α παρ. 1 – Επηρεασμός του αποτελέσματος μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή

4.2.4.1 Τα δεδομένα υπολογιστή

Σύμφωνα με το άρθρο 1 στοιχείο β' της Σύμβασης της Βουδαπέστης[88], ως δεδομένο υπολογιστή νοείται κάθε «αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή

[84] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 68.

[85] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 156.

[86] Πάντως, υπό το ισχύον καθεστώς, αν τα πρόσωπα παραμείνουν άδηλα δεν θα μπορεί να διωχθεί η πράξη της βασικής μορφής του 386Α. Ι. Μοροζίνης σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, 2023, σελ. 171.

[87] Κ. Φράγκος, Ποινικός Κώδικας, 2020, σελ. 1903.

[88] Βλ. και τεχνικό κανόνα DIN-Norm 44300 (αριθμός 19), όπου ως στοιχεία υπολογιστή νοούνται «όλες οι πληροφορίες που εκφράζονται μέσω σημείων ή συνεχών λειτουργιών, επί τη βάση γνωστών ή εικαζόμενων συμφωνιών, προκειμένου να καταστούν αντικείμενο επεξεργασίας». Στον κανόνα αυτό κατέφευγε η

κατάλληλη για να υποστεί επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή». Αυτός ο ευρύς ορισμός περιλαμβάνει όλα τα επεξεργάσιμα από τον υπολογιστή στοιχεία (σκληρός δίσκος, usb, κάρτα μνήμης, μνήμη flash, πιστωτική κάρτα), καθώς κάθε εκτελέσιμο πρόγραμμα που επιφέρει κάποια λειτουργικότητα στο σύστημα (π.χ. exe, apk)[89].

4.2.4.2 Ο επηρεασμός

Ως επηρεασμός[90] νοείται κάθε επέμβαση στο σύστημα, η οποία καθιστά παρεκκλίνοντα τα αποτελέσματα της διαδικασίας επεξεργασίας, σε σύγκριση με τα αποτελέσματα που θα επέρχονταν, σύμφωνα με τη λειτουργικότητα του προγράμματος, στην οποία είχε αποβλέψει ο δημιουργός του. Η παρέκκλιση αυτή θα πρέπει να μπορεί να καταλογιστεί αντικειμενικά στο δράστη, ενώ ο επηρεασμός αντιστοιχεί στην επενέργεια των απατηλών δηλώσεων στο νοητικό του αποδέκτη τους (κοινή απάτη – 386 ΠΚ)[91].

Αν μεταξύ του επηρεασμού και της περιουσιακής βλάβης υπάρχει ενδιάμεσο πρόσωπο με ελεγκτική αρμοδιότητα, τότε στοιχειοθετείται η κοινή απάτη του άρθρου 386 ΠΚ. Αυτό συμβαίνει διότι σε αυτή την περίπτωση η αιτία της περιουσιακής βλάβης δεν είναι ο επηρεασμός των αποτελεσμάτων της διαδικασίας επεξεργασίας αλλά το πρόσωπο που πλανάται. Το τελευταίο προβαίνει τελικά σε περιουσιακή διάθεση μέσω της ανοχής εισαγωγής ή περαιτέρω επεξεργασίας των στοιχείων[92]. Αν, όμως, το πρόσωπο δεν έχει θέση ελεγκτή και απλά παραλαμβάνει τα δεδομένα χωρίς να μπορεί να τα εξετάσει, τότε δεν αποκλείεται η τέλεση απάτης με υπολογιστή[93]. Κατά τα λοιπά, ισχύουν για το στοιχείο του επηρεασμού, όσα εκτενώς αναφέρθηκαν στο 3.2.

4.2.4.3 Το αποτέλεσμα της διαδικασίας επεξεργασίας

γερμανική επιστήμη για τον προσδιορισμό των στοιχείων στην αντίστοιχη διάταξη 263a του ΓερμΠΚ. Βλ. ΠλημμΑθ 638/2008 (ΠοινΧρ. Ξ/2010, σελ. 775).

[89] Το άνοιγμα αρχείων με τέτοιες καταλήξεις, επιτρέπουν στον υπολογιστή να εκτελεί μία ή περισσότερες λειτουργίες, που είναι προγραμματισμένες στα αρχεία αυτά.

[90] Βλ. αναλυτικά παραπάνω 4.2.

[91] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 58.

[92] Α. Παπαδαμάκης, Περιουσιακά Εγκλήματα, 2020, σελ. 157.

[93] Ό.π., σελ. 65.

Αντικείμενο του επηρεασμού είναι το αποτέλεσμα της διαδικασίας επεξεργασίας δεδομένων. Αν και στο προ του ν. 4411/2016 καθεστώς το αντικείμενο επηρεασμού αποτελούσαν τα «στοιχεία του υπολογιστή», ακόμα και τότε γινόταν δεκτό ότι ο επηρεασμός των στοιχείων του υπολογιστή μπορεί να γίνει τόσο στα εισαγόμενα «Eingabephase», όσο και τα εξαγόμενα στοιχεία[94], δηλαδή στο αποτέλεσμα της επεξεργασίας των δεδομένων[95]. Η αντίστοιχη γερμανική διάταξη διατυπώθηκε εξ' αρχής με αναφορά σε επηρεασμό του αποτελέσματος της επεξεργασίας δεδομένων[96]. Για να την τέλεση του αδικήματος, θα πρέπει -μόνο-[97] το αποτέλεσμα της διαδικασίας επεξεργασίας να προκαλεί άμεσα οικονομική ζημία[98].

4.2.5 Οι τρόποι τέλεσης

Το βασικό έγκλημα της πρώτης παραγράφου του άρθρου 386Α ΠΚ[99], περιλαμβάνει πέντε τρόπους με τους οποίους μπορεί να επέλθει ο επηρεασμός του αποτελέσματος μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή. Παρακάτω αναλύονται ξεχωριστά οι τρόποι τέλεσης της παρ. 1.

4.2.5.1 α) Με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή

Ο πρώτος τρόπος τέλεσης περιγράφεται ως επηρεασμός του αποτελέσματος μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή «με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή». Το «πρόγραμμα» αποτελεί υποσύνολο που περιλαμβάνεται στον ευρύτερο όρο «δεδομένα υπολογιστών» , σύμφωνα και με τον ορισμό της Σύμβασης

[94] Στη Γερμανική 2. WiKG, σελ 18,20 «Outputmanipulationen».

[95] Δ. Κιούπης, Ποινικό δίκαιο και internet, 1999 σελ. 116,117 υποσημείωση 165.

[96] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 57, Δ. Κιούπης Ό.π., Γ. Μπουρμάς, ΠοινΧρ ΝΑ' (2001), σελ. 470, Ι. Καρακώστας, Δίκαιο και Internet, 2009, σελ. 247.

[97] Ό.π. (2. WiKG) η οικονομική ζημία πρέπει να εξαρτάται μόνο από το αποτέλεσμα εργασίας του υπολογιστή «halt vom Arbeitsergebnis des Computers abhängt».

[98] Αιτ. Έκθ. του Δεύτερου Νόμου για την Οικονομική Εγκληματικότητα (2. WiKG), σελ. 19 «daß er den Anwendungsbereich des Tatbestandes auf die Fälle beschränkt, in denen das Ergebnis eines Datenverarbeitungsvorganges unmittelbar einen Vermögensschaden herbeiführt». Περιορίζει το εύρος του αδικήματος σε περιπτώσεις κατά τις οποίες το αποτέλεσμα της διαδικασίας επεξεργασίας προκαλεί άμεσα οικονομική ζημία.

[99] Για την πρακτική εφαρμογή του 386Α ΠΚ βλ. Αιτ. Έκθεση 2. WiKG, σελ. 21, όπου αναφέρει τις εξουσιοδοτήσεις άμεσης χρέωσης, τις μεταφορές σε ταμιευτήρια και τις τραπεζικές συναλλαγές.

της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο[100]. Συνεπώς, το πρόγραμμα δεν είναι παρά ένα ειδικότερο στοιχείο των δεδομένων. Κατ' επέκταση δε, η «μη ορθή διαμόρφωση προγράμματος υπολογιστή», αποτελεί μια ειδικότερη περίπτωση του τρίτου τρόπου τέλεσης περί «χρησιμοποίησης μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή»[101].

Ο όρος διαμόρφωση, σημαίνει το να δίνει κάποιος σε κάτι μορφή, σχήμα[102]. Συνεπώς, η πράξη της διαμόρφωσης μπορεί να περιλαμβάνει τη δημιουργία ολικά η μερικά νέου προγράμματος[103]. Είμαστε, άλλωστε, εξοικειωμένοι με τον όρο «format», ο οποίος μεταφράζεται κατ' ακριβολογία ως διαμόρφωση. Τον όρο αυτό χρησιμοποιούμε και στην καθομιλουμένη, για να περιγράφουμε τη διαγραφή όλων ή μέρους[104] των στοιχείων από μια μονάδα σκληρού δίσκου και την εκ νέου εγκατάσταση του λειτουργικού συστήματος.

Το να δίνει κανείς σχήμα, όμως, επεκτείνεται σε κάθε επέμβαση που μπορεί να προκαλέσει κάποιος στο πρόγραμμα, τόσο εν τη γενέσει του, όσο και στη συνέχεια. Έτσι εκτός από την εν όλω ή εν μέρει δημιουργία νέου προγράμματος, μπορεί να αφορά και σε εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη δεδομένων του προγράμματος[105].

Εισαγωγή, αποτελεί η προσθήκη νέων δεδομένων στο πρόγραμμα, ενώ αλλοίωση είναι η μετατροπή των ήδη υπαρχόντων. Διαγραφή σημαίνει την απλή αφαίρεση στοιχείων από τον φορέα των δεδομένων ενώ εξάλειψη την ολοσχερή απομάκρυνση τους[106]. Τέλος, μετάδοση αποτελεί η μεταφορά τους.

---

[100] Άρθρο 1 στ. β' της Σύμβασης της Βουδαπέστης «δεδομένα υπολογιστών σημαίνει αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη για να υποστεί επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή».

[101] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 58.

[102] Ο ορισμός αυτός δίνεται σε λεξικά της νέας ελληνικής γλώσσας.

[103] Για πρόγραμμα μη ορθά διαμορφωμένο από την αρχή κάνει λόγο η Αιτ.. Έκθεση του 2. WiKG «Wird das Programm von vornherein unrichtig gestaltet».

[104] Στις ρυθμίσεις του λειτουργικού συστήματος των Windows περιλαμβάνεται η επιλογή για «Δημιουργία και διαμόρφωση διαμερισμάτων σκληρού δίσκου», που σημαίνει τη μερική διαμόρφωση - τμήματος του σκληρού δίσκου. Στην αγγλική έκδοση περιγράφεται ως «Create and format a hard disk partition».

[105] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 59.

[106] Ό.π.

Αρκετά συνήθης είναι η πρακτική της τροποποίησης του προγράμματος με στόχο την παράκαμψη ή την αφύσικη λειτουργία του ελέγχου αναγνώρισης της ταυτότητας. Και αυτή η πρακτική θα αποτελεί «μη ορθή διαμόρφωση του προγράμματος». Επίσης μη ορθή διαμόρφωση αποτελεί η εισαγωγή δεδομένων σε διαφορετικό πλαίσιο ή η αποσιώπησή τους[107].

Το «μη ορθό» της διαμόρφωσης μπορεί να κριθεί τόσο υποκειμενικά όσο και αντικειμενικά. Κατά την υποκειμενική θεώρηση, μη ορθή είναι η διαμόρφωση του προγράμματος, όταν η λειτουργικότητά του δεν ανταποκρίνεται στη βούληση του νόμιμου κατόχου του. Βέβαια, η βούληση του νόμιμου κατόχου δεν είναι πάντοτε ευχερώς εξακριβώσιμη, αλλά ούτε και η ακεραιότητα που επιδιώκει ο νόμιμος κάτοχος δεν είναι πάντα άξια ποινικής προστασίας[108]. Μπορεί ακόμα, ένα πρόγραμμα να εξυπηρετεί εξ' αρχής εγκληματικούς σκοπούς και τότε κατά υποκειμενική θεώρηση θα είναι ορθό, αφού καμία απόκλιση δε θα υπάρχει από τη στόχευση του νόμιμου κατόχου του[109].

Ούτε και η λεγόμενη αντικειμενική άποψη δε φαίνεται όμως αρκετά πειστική. Σύμφωνα με αυτή, το πρόγραμμα είναι ορθό όταν εκπληρώνει την αποστολή του. Και πάλι η εκπλήρωση της αποστολής θα κρινόταν από το δημιουργό του και έτσι θα καταλήγαμε στο άτοπο να προστατεύεται το πρόγραμμα που εκπληρώνει εγκληματική αποστολή. Συνεπώς και οι δύο λύσεις που κρίνουν τη (μη) ορθότητα σε σχέση με το στόχο του προγράμματος – κατόχου είναι επισφαλείς.

Ορθότερο θα ήταν να κρίνουμε το «μη ορθό» της διαμόρφωσης με βάση το αν η δημιουργία ή τροποποίηση του προγράμματος είχε στόχο να δημιουργήσει μια κατάσταση ανάλογη με την πλάνη του φυσικού προσώπου και να θίξει περιουσιακά αγαθά. Έτσι, μη ορθή διαμόρφωση θα υπάρχει, όταν α) το πρόγραμμα δεν επιτελεί πια τη νόμιμη

---

[107] Αιτ. Έκθεση 2. WiKG, σελ. 20. Αποσιώπηση είναι η παρακράτηση και συγκάλυψη δεδομένων ώστε να μην εισαχθούν στην κανονική διαδικασία επεξεργασίας, βλ. ό.π.

[108] Ο νομοθέτης, δεν επιδιώκει την ποινικοποίηση της τυπικής (μη) ορθότητας. Αυτό που τον ενδιαφέρει είναι αν η μη ορθότητα, ισοδυναμεί με κατάσταση ανάλογη με την πλάνη φυσικού προσώπου. Έτσι, μια απλή επενέργεια στο πρόγραμμα που α) διατηρεί τη νόμιμή του λειτουργικότητα, παρέχοντας τα ίδια ορθά αποτελέσματα και β) μεταβάλλει απλά τον τρόπο, χωρίς να θίγει περιουσιακά αγαθά, δεν μπορεί να χαρακτηρίζεται ως «μη ορθή». Αποτελεί μόνο μια διαμόρφωση «χωρίς δικαίωμα».

[109] Π.χ. διαμόρφωση του προγράμματος εξ' αρχής από τον κάτοχό του ώστε να προκαλεί περιουσιακή βλάβη σε τρίτους. Τούτο, δεν αποτελεί μη ορθή διαμόρφωση, αφού δεν παρεκκλίνει από τη βούληση του κατόχου του.

λειτουργικότητα του και β) κατέστη πρόσφορο να προκαλέσει περιουσιακή βλάβη τρίτου[110].

4.2.5.2 β) Με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα

Σύμφωνα με το άρθρο 386Α παρ. 1 περίπτωση β) του ΠΚ, το έγκλημα της απάτης με υπολογιστή τελείται «επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή, με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα».

Πριν από την τελευταία τροποποίηση του άρθρου 386Α με το άρθρο 16 του ν. 4947/2022, ο συγκεκριμένος τρόπος τέλεσης περιγραφόταν ως «χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή». Με την τελευταία τροποποίηση, οι όροι του «προγράμματος» και «συστήματος υπολογιστή» έχουν αντικατασταθεί από τον ορθότερο και ευρύτερο όρο «πληροφοριακό σύστημα»[111].

Ο ορισμός του πληροφοριακού συστήματος δίνεται στο άρθρο 13 περ. στ' του ΠΚ σύμφωνα το οποίο «Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών». Ο ορισμός αυτός, εισήχθη για πρώτη φορά στον ΠΚ με τον ν. 4411/2016 και αποτελεί μεταφορά, στο εθνικό δίκαιο, της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

Η τροποποίηση του άρθρου 386Α, ώστε να γίνεται αναφορά τώρα σε πληροφοριακό σύστημα και όχι σε πρόγραμμα ή σύστημα υπολογιστή, κρίθηκε επιβεβλημένη, διότι η Οδηγία (ΕΕ) 2019/713[112] ακολουθεί αυτό τον ορισμό. Συγκεκριμένα, το άρθρο 2 στοιχείο ε' της Οδηγίας (ΕΕ) 2019/713 αναφέρει ότι για τους

---

[110] Ό.π. σελ. 62.

[111] Άρθρο 16 του ν. 4947/2022: «Στο άρθρο 386Α ΠΚ επέρχονται οι εξής αλλαγές: α) στην περ. β' της παρ. 1 και στην παρ. 2 η αναφορά σε πρόγραμμα ή σύστημα υπολογιστή και στη λειτουργία αυτού αντικαθίσταται από την αναφορά στο πληροφοριακό σύστημα». Βλ. και Αιτ. Έκθεση σελ. 43.

[112] Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 17ης Απριλίου 2019 για την καταπολέμηση της απάτης και της πλαστογραφίας πλην των μετρητών και την αντικατάσταση της απόφασης πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου.

σκοπούς της, ισχύει ο ορισμός «σύστημα πληροφοριών» κατά την έννοια του άρθρου 2 στοιχείο α' της Οδηγίας 2013/40/ΕΕ.

Σύμφωνα, δε, με το άρθρο 2 περ. δ' της Οδηγίας 2013/40/ΕΕ[113], ως «χωρίς δικαίωμα» νοείται «η συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου». Το στοιχείο «χωρίς δικαίωμα» στο άρθρο 386Α ΠΚ, συνιστά ειδικό στοιχείο του αδίκου που οριστικοποιεί τον άδικο χαρακτήρα της σχετικής συμπεριφοράς[114].

Παρέμβαση στο πληροφοριακό σύστημα είναι κάθε επηρεασμός της διαδικασίας επεξεργασίας δεδομένων που εκτελείται σε αυτό. Δηλαδή η παρέμβαση μπορεί να γίνει σε μία ή περισσότερες συσκευές οι οποίες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία δεδομένων. Νοείται δε, και παρέμβαση στα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από τη συσκευή ή την ομάδα συσκευών, αφού η παρέμβαση αυτή μπορεί να μεταβάλλει το σκοπό, τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών. Συνεπώς, η παρέμβαση μπορεί να αφορά τόσο στο hardware της συσκευής, εφόσον με αυτή επηρεάζεται η επεξεργασία δεδομένων, όσο και τα ψηφιακά δεδομένα, αν η παρέμβαση σε αυτά μεταβάλλει τη λειτουργία του πληροφοριακού συστήματος.

4.2.5.3 γ) Με τη χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας

Η τρίτη υπαλλαγή, αναφέρεται στον επηρεασμό του αποτελέσματος μιας διαδικασίας επεξεργασίας, μέσω της χρησιμοποίησης μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας. Μη ορθά ψηφιακά δεδομένα θεωρούνται αυτά που δεν ανταποκρίνονται στην πραγματικότητα, ενώ ελλιπή κρίνονται τα δεδομένα όταν έχει παραλειφθεί κάποιο στοιχείο[115] που εκφράζει την πραγματικότητα.

---

[113] Άρθρο 2 στ. δ' της Οδηγίας 2013/40/ΕΕ της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών.

[114] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 162.

[115] Στ. Παύλου, Γ. Μπέκας, Ποινικό ΙΙΙ Εγκλήματα κατά της Ιδιοκτησίας, Περιουσίας & Ζωής, 2020, σελ. 307, 308.

Είναι φανερό στο σημείο αυτό, ότι συγκεκριμένος ο τρόπος τέλεσης παρουσιάζει έντονα κοινά στοιχεία με την απάτη του άρθρου 386 ΠΚ. Τα «μη ορθά» ψηφιακά δεδομένα αντιστοιχούν στην παράσταση ψευδών γεγονότων, ενώ τα «ελλιπή» στην απόκρυψη ή παρασιώπηση της κοινής απάτης. Τα δεδομένα αντιστοιχούν στα γεγονότα της απάτης του 386 ΠΚ, οπότε θα πρέπει να αναφέρονται στο παρόν ή το παρελθόν.

Χρησιμοποίηση, σημαίνει την εισαγωγή των μη ορθών ή ελλιπών ψηφιακών δεδομένων στον υπολογιστή. Αν η χρησιμοποίηση δεν έχει αρχίσει, δε νοείται καν απόπειρα[116]. Οποιαδήποτε εισαγωγή μη ορθών δεδομένων στον υπολογιστή αποτελεί «χρησιμοποίηση» και έτσι καθίσταται δυνατή η περίπτωση χρησιμοποίησης παρένθετων προσώπων που τα εισάγουν. Κατά μία άποψη σε αυτή την περίπτωση θα τιμωρηθεί ως έμμεσος αυτουργός αυτός που χρησιμοποιεί τα παρένθετα πρόσωπα ως όργανά του[117]. Κατ' άλλη άποψη ο καλόπιστος χειραγωγούμενος πράττει άδικα παρά την έλλειψη δόλου, οπότε είναι δυνατή η τιμώρηση του κακόπιστου υποκινητή ως ηθικού αυτουργού[118].

Η χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων αναγνώρισης ταυτότητας, αφορά την με τεχνάσματα εισαγωγή στοιχείων που δεν ανταποκρίνονται ολικά ή μερικά στην πραγματικότητα. Με αυτά τα τεχνάσματα επιτυγχάνεται μια κατάσταση αντίστοιχη της πλάνης της κοινής απάτης, ώστε το σύστημα να επιτρέψει την είσοδο σε μη δικαιούμενο πρόσωπο. Αυτός ο τρόπος τέλεσης αφορά την περίπτωση χρήσης πλαστών διαπιστευτηρίων, όπως για παράδειγμα η χρήση πλαστής κάρτας[119] που ενσωματώνει δεδομένα που δεν ανταποκρίνονται στην πραγματικότητα.

Κατά την υποκειμενική θεώρηση, τα στοιχεία που εισάγονται είναι ορθά και πλήρη μόνο όταν εισάγονται από τον νομιμοποιούμενο[120] χρήστη. Όταν αντίθετα, τα στοιχεία

---

[116] Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 64.

[117] Ό.π. σελ. 65 αυτά τα πρόσωπα δεν μπορούν να τιμωρηθούν, εκτός των άλλων, αφού δεν έχουν σκοπό κτήσης παράνομου περιουσιακού οφέλους. ΕφΑθ. 1081/08, ΠοινΧρ. Ξ, σελ. 762, ΠλημμΑθ. 638/08, ΠοινΧρ Ξ, σελ. 775.

[118] Στ. Παύλου, Γ. Μπέκας, Ποινικό ΙΙΙ Εγκλήματα κατά της Ιδιοκτησίας, Περιουσίας & Ζωής, 2020, σελ. 310.

[119] Βλ. ΑΠ 1087/2019 όπου αναφέρεται ότι «έκαναν χρήση μη ορθών στοιχείων, δηλαδή των πλαστών καρτών – κλώνων». Βλ. Γ. Δανιήλ σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, 2023, σελ. 94 επ. «η αντιγραφή των δεδομένων γνήσιας κάρτας αυτόματης συναλλαγής σε λευκή κάρτα με την μέθοδο του skimming στοιχειοθετεί το έγκλημα της κατάρτισης πλαστού εγγράφου».

[120] Θ. Σάμιος σε Ποινικές Επιστήμες - θεωρία και πράξη: Προσφορά τιμής στην Άννα Μπενάκη Ψαρούδα, Τόμος Β, 2008, σελ. 534.

εισάγονται από μη νομιμοποιούμενο πρόσωπο, τότε αυτά δεν θεωρούνται ορθά και πλήρη. Κατά την αντικειμενική θεώρηση τα στοιχεία είναι ορθά και πλήρη ανεξάρτητα από το ποιος τα εισάγει. Η τελευταία αυτή άποψη εμφανίζεται περισσότερο εναρμονισμένη με την ταχύτητα των συναλλαγών, αφού δεν είναι πρακτικό να αναζητείται πάντοτε ο νομιμοποιούμενος χρήστης[121].

4.2.5.4 δ) Με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης της ταυτότητας

Ο τέταρτος τρόπος τέλεσης, περιγράφει τον επηρεασμό με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης ταυτότητας. Με την ενσωμάτωση της Οδηγίας (ΕΕ) 2019/713 με τον ν. 4947/2022, η αναφορά σε δεδομένα υπολογιστή που γινόταν προηγουμένως εδώ, εξειδικεύτηκε στην αναφορά σε ψηφιακά δεδομένα.

Σύμφωνα με το άρθρο 13 στοιχείο ζ' του ΠΚ, «ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία». Ο ορισμός αυτός εισήχθη για πρώτη φορά με τον ν. 4411/2016, ο οποίος ενσωμάτωσε την Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών[122].

Η ίδια οδηγία[123] ορίζει και την «χωρίς δικαίωμα» ως «συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου».

---

[121] Έτσι δεν διαπράττει έγκλημα και όποιος εξουσιοδοτείται να προβεί σε ανάληψη για να εξυπηρετήσει τον πραγματικό δικαιούχο. Βλ. Θ. Σάμιο, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, σελ. 299-300 «τα γνήσια κέρματα που τοποθετούνται στον αυτόματο πωλητή δεν χάνουν τη γνησιότητά τους επειδή είναι κλεμμένα».

[122] Άρθρο 1 στ. β' της Σύμβασης της Βουδαπέστης «δεδομένα υπολογιστών σημαίνει αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη για να υποστεί επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή».

[123] Άρθρο 2 στ. δ' της Οδηγίας 2013/40/ΕΕ της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών.

Συνεπώς, απάτη με υπολογιστή της δ' περίπτωσης της παρ. 1 του 386Α ΠΚ τελεί όποιος χωρίς εξουσιοδότηση πρόσβασης από το νόμιμο δικαιούχο (ή με παρεμβολή ή υποκλοπή), εισάγει, αλλοιώνει, διαγράφει, μεταδίδει ή εξαλείφει ορθές πληροφορίες επεξεργάσιμες από το πληροφοριακό σύστημα.

Ιδίως, την υπαλλαγή αυτή τελεί, όποιος εισάγει, αλλοιώνει, διαγράφει κλπ. ψηφιακά δεδομένα αναγνώρισης της ταυτότητας. Συνηθέστατη περίπτωση αυτού του είδους απάτης με υπολογιστή στις συναλλαγές, αποτελεί η χωρίς δικαίωμα ανάληψη χρημάτων από ΑΤΜ. Ο χρήστης, δηλαδή, που εισάγει χωρίς δικαίωμα την κάρτα στο ΑΤΜ και τον αριθμό PIN της, τελεί τη συγκεκριμένη υπαλλαγή του εγκλήματος του άρθρου 386Α του ΠΚ.

4.2.5.5 ε) Χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας

Ως λογισμικό προορισμένο για τη μετακίνηση χρημάτων πρέπει να θεωρηθεί κάθε εφαρμογή λογισμικού, επιγραμμική ή μη (online ή offline), η οποία έχει τη λειτουργικότητα να εξυπηρετεί τη μετακίνηση χρημάτων ή νομισματικής αξίας. Η περίπτωση αυτή αφορά ιδίως την αξιοποίηση των ηλεκτρονικών εφαρμογών μεταφοράς χρημάτων (e-banking), χωρίς δικαίωμα[124]. Αφορά, δηλαδή, περιπτώσεις δραστών που έχουν αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου[125] και αξιοποιούν τις εφαρμογές για να προβούν σε αθέμιτες μετακινήσεις χρηματικών ποσών[126].

Και πάλι ο όρος «χωρίς δικαίωμα», θα έχει την έννοια κάθε συμπεριφοράς, η οποία δεν είναι εξουσιοδοτημένη από το νόμιμο δικαιούχο του συστήματος ή δεν επιτρέπεται δυνάμει του εθνικού δικαίου. Η έννοια της αξιοποίησης δε, είναι τόσο ευρεία, που περιλαμβάνει κάθε χωρίς δικαίωμα επενέργεια στο λογισμικό μετακίνησης χρημάτων. Πάντως ο όρος «αξιοποίηση», αν και χρήσιμος για την ευρύτητά του, έχει μια θετική χροιά που δεν ταιριάζει στην περιγραφή εγκλήματος.

Με τον ν. 4947/2022 που ενσωμάτωσε την Οδηγία (ΕΕ) 2019/713 για την καταπολέμηση της απάτης και της πλαστογραφίας πλην των μετρητών, το 386Α παρ. 1 ε

[124] Η ΑΠ 1700/2010 αντιμετώπισε περίπτωση χρησιμοποίησης username και κωδικών πρόσβασης (που είχαν υποκλαπεί προηγουμένως) για τη μεταφορά χρημάτων μέσω e-banking.

[125] Δ. Κιούπης, Ποινικό Δίκαιο και Internet, 1999, σελ. 119.

[126] Για το ζήτημα βλ..Ι. Μοροζίνη σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, 2019, σελ. 145.

διευρύνθηκε εννοιολογικά, περιλαμβάνοντας και την αξιοποίηση λογισμικού για τη μετακίνηση νομισματικής αξίας. Στην προηγούμενη μορφή της διάταξης γινόταν αναφορά μόνο στην αξιοποίηση λογισμικού για μετακίνηση χρημάτων. Η τροποποίηση αυτή είναι στοχευμένη και συμβαδίζει με την προσθήκη του στοιχείου η΄ στο άρθρο 13 του ΠΚ. Το τελευταίο ορίζει ότι μέσο πληρωμής πλην των μετρητών είναι κάθε προστατευόμενος μηχανισμός, ο οποίος επιτρέπει στο χρήστη του να μεταφέρει χρήματα ή νομισματική αξία, μεταξύ άλλων, μέσω ψηφιακών μέσων συναλλαγής[127].

Συνεπώς, το έγκλημα της ε' υπαλλαγής της παρ. 1 του άρθρου 386Α, τελεί όποιος επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή, αξιοποιεί χωρίς δικαίωμα ηλεκτρονικές εφαρμογές τραπεζικής, εφαρμογές μετακίνησης κρυπτοχρήματος, ψηφιακά πορτοφόλια και κάθε συναφές μέσο με το οποίο διακινείται νομισματική αξία.

4.2.6 Η βλάβη ξένης περιουσίας

Ο επηρεασμός του αποτελέσματος επεξεργασίας δεδομένων με κάποιον από τους παραπάνω τρόπους τέλεσης, δεν αρκεί για τη στοιχειοθέτηση του εγκλήματος της απάτης με υπολογιστή. Θα πρέπει, ακόμα, ο επηρεασμός να προκαλεί άμεσα μείωση ξένης περιουσίας[128]. Δηλαδή, δεν αρκεί απλά αιτιώδης σύνδεσμος μεταξύ του επηρεασμού και της περιουσιακής μείωσης, αλλά απαιτείται αμεσότητα στην πρόκληση της τελευταίας[129]. Η περιουσιακή ζημία είναι άμεση, όταν δεν παρεμβάλλεται κάποια ανθρώπινη συμπεριφορά μεταξύ της επεξεργασίας και της περιουσιακής μείωσης. Αντίθετα, δεν στοιχειοθετείται το 386Α ΠΚ, όταν το αποτέλεσμα επεξεργασίας διευκολύνει απλά τον δράστη να πετύχει περιουσιακό όφελος, το οποίο δεν προέρχεται από τον υπολογιστή, αλλά από τον άνθρωπο που εγκρίνει το αποτέλεσμα επεξεργασίας του υπολογιστή.

---

[127] Άρθρο 13 στοιχείο η' ΠΚ «μέσο πληρωμής πλην των μετρητών είναι 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».

[128] Αιτ. Έκθ. του Δεύτερου Νόμου για την Οικονομική Εγκληματικότητα (2. WiKG), σελ. 19 «unmittelbar einen Vermögensschaden herbeiführt». Περιορίζει το εύρος του αδικήματος σε περιπτώσεις κατά τις οποίες το αποτέλεσμα της διαδικασίας επεξεργασίας προκαλεί άμεσα οικονομική ζημία.

[129] Χ. Μυλωνόπουλος, Ποινικό δίκαιο – Ειδικό μέρος, 2016, σελ. 556.

Υπό το καθεστώς προ της εισαγωγής του νέου Ποινικού Κώδικα (ν. 4619/2019), υπήρχε πρόβλεψη στα δύο τελευταία εδάφια[130] ότι «Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα» και ότι «Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα». Έτσι, δεχόμασταν ότι τα πρόσωπα των οποίων η περιουσία βλάφθηκε, δεν είναι απαραίτητο να είναι ατομικά προσδιορισμένα.

Γινόταν έτσι λόγος για «θυματολογικό χαρακτήρα»[131] της διάταξης, αφού η περιουσιακή βλάβη εμφανιζόταν αποσυνδεδεμένη από τα θύματα. Η αποσύνδεση από τους παθόντες, δεν ήταν φυσικά τυχαία επιλογή του νομοθέτη. Πράγματι, η απάτη με υπολογιστή προσβάλλει συνήθως την περιουσία περισσότερων και όχι μόνο ένα πρόσωπο, ενώ το σύνολο των προσώπων που βλάπτονται μπορεί να μην είναι γνωστά. Η πρόβλεψη αυτή, είχε αξία για την αιτιολόγηση της δικαστικής απόφασης, η οποία δεν θεωρούνταν αναιτιολόγητη ακόμα και αν δεν ανέφερε τους παθόντες[132].

Ο νέος ΠΚ (ν. 4619/2019)[133], δεν περιλαμβάνει αυτά τα δύο εδάφια και άρα πλέον η επελθούσα ζημία δεν διαφοροποιείται καθόλου από την κοινή απάτη. Συνεπώς, μόνο με τους όρους του 98 ΠΚ, θα μπορούν να αθροιστούν οι επιμέρους περιουσιακές ζημίες. Επίσης, θα πρέπει να υπάρχει σχέση υλικής αντιστοιχίας ανάμεσα στην προκληθείσα βλάβη και στο σκοπούμενο όφελος. Τέλος, θα πρέπει να γίνει δεκτό ότι απόφαση που δεν προσδιορίζει τον παθόντα και τη ζημία του, πάσχει λόγω έλλειψης αιτιολογίας[134].

4.2.7 Το ιδιώνυμο έγκλημα της 386Α παρ. 2 - Οι προπαρασκευαστικές πράξεις

4.2.7.1 Κατασκευή, διάθεση ή κατοχή προγράμματος ή πληροφοριακού συστήματος

[130] Βλ. τη μορφή του 386Α παρ. 1 εδ. β' και γ' κατά τον ν. 4411/2016.

[131] Ειρ. Βασιλάκη, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σελ. 219.

[132] Βλ. υπ. 79, 80. Θα ήταν πρακτικά αδύνατο να προσδιορίζεται στην απόφαση κάθε ένας από το ευρύ πλήθος που έχει βλαφθεί. Οι περισσότερες περιουσίες των χρηστών αποτελούν μια επιφάνεια προσβολής, εκτίθενται στην προσβολή του δράστη ως μία περιουσία και έτσι συνδέονται με την τέλεση μιας απάτης με υπολογιστή.

[133] Τα ίδια ισχύουν και σύμφωνα με την τελευταία τροποποίηση του ΠΚ με το ν. 4947/2022.

[134] Ι. Μπέκας, σε Στεφ. Παύλου/Ι. Μπέκα/Αν. Αποστολίδου, Ποινικό Δίκαιο – Ειδικό μέρος, 2021.

Η δεύτερη παράγραφος του άρθρου 386Α αποτελεί ένα ιδιώνυμο έγκλημα, καθώς ποινικοποιεί αυτοτελώς, τις πράξεις που προορίζονται για τη διάπραξη του εγκλήματος της παρ. 1. Πρόκειται για έγκλημα αφηρημένης διακινδύνευσης[135].

Κατασκευή αποτελεί τη δημιουργία προγράμματος ή πληροφοριακού συστήματος, με προορισμό να χρησιμοποιηθεί για να βλάψει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας υπολογιστή, με κάποιον από τους τρόπους που αναλύθηκαν αμέσως παραπάνω. Είναι προφανές ότι ο κατασκευαστής ενός εν δυνάμει επικίνδυνου προϊόντος που ανά πάσα στιγμή μπορεί να χρησιμοποιηθεί και να βλάψει την περιουσία τρίτων, δεν μπορεί να μένει ατιμώρητος.

Το ίδιο ισχύει και για όποιον δεν είναι κατασκευαστής του εν δυνάμει βλαπτικού προγράμματος ή ΠΣ, αλλά το διαθέτει. Διάθεση σημαίνει την προσφορά του προγράμματος/ΠΣ στο κοινό. Εκείνος που διαθέτει τέτοιο πρόγραμμα ή ΠΣ, είναι το ίδιο άξιος τιμωρίας με τον κατασκευαστή, διότι χωρίς την παρέμβασή του, το προϊόν αυτό μπορεί να μην κατέληγε ποτέ στον διατεθειμένο να το χρησιμοποιήσει, δράστη.

Αλλά και ο κάτοχος του προγράμματος ή ΠΣ, το οποίο προορίζεται για τη διάπραξη του 386Α παρ. 1., τελεί το έγκλημα της παρ. 2. Διότι δεν είναι εύλογο να αναμένουμε από τον δράστη να περατώσει το έγκλημα της παρ. 1[136], αν και γνωρίζουμε ότι εκείνος κατέχει ήδη μια εστία κινδύνου[137], την οποία μπορεί να ενεργοποιήσει οποτεδήποτε[138].

4.2.7.2 Ο προσωπικός λόγος απαλλαγής από την ποινή

Στο εδάφιο β' της δεύτερης παραγράφου του άρθρου 386Α ΠΚ θεσπίζεται υποχρεωτικός λόγος απαλλαγής από την ποινή. Αφορά τον δράστη ο οποίος καταστρέφει με δική του θέληση, το πρόγραμμα ή το πληροφοριακό σύστημα που είχε κατασκευάσει, διέθετε ή κατείχε, πριν το χρησιμοποιήσει για τη διάπραξη της απάτης με υπολογιστή της

[135] Γ. Μπουρμάς σε Α. Χαραλαμπάκη, Ο νέος ποινικός κώδικας – ερμηνεία κατ' άρθρο του ν. 4619/2019, 2020, σελ. 3146.

[136] Η περάτωση μπορεί να επέρχεται με ένα «κλικ».

[137] Δηλαδή το πρόγραμμα ή το πληροφοριακό σύστημα, το οποίο είναι σε θέση να βλάψει ανά πάσα στιγμή την περιουσία τρίτων.

[138] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 163. Τονίζει ότι «θα πρέπει να αναγνωριστεί ένα είδος διακριτής χωροχρονικής εγγύτητας» μεταξύ της προπαρασκευής και της διάπραξης του εγκλήματος. Διαφορετικά, θα κινδύνευαν με πρόχειρες ποινικοποιήσεις οι ασχολούμενοι με προγράμματα και ΠΣ.

παρ. 1. Με την εισαγωγή αυτής της ειδικής μορφής έμπρακτης μετάνοιας[139], η οποία οδηγεί σε υποχρεωτική εξάλειψη του αξιοποίνου, επιδιώκεται η ενθάρρυνση των προσώπων που βρίσκονται «ένα κλικ» μακριά από το έγκλημα, να απαλλαχθούν εντελώς από την ποινή. Καταστρέφοντας το προγράμματα ή ΠΣ, δεν υπάρχει πλέον κάποια εστία κινδύνου για το έννομο αγαθό της περιουσίας, οπότε δεν δικαιολογείται η τιμώρηση του κατασκευαστή, αυτού που διαθέτει ή του κατόχου. Ακριβώς επειδή, με την πράξη της καταστροφής, δηλώνει με τον πιο ευθύ τρόπο ότι θέλει να αποσυρθεί από την εγκληματική δράση.

4.3 Υποκειμενική υπόσταση

Η απάτη με υπολογιστή σε κάθε μορφή της τελείται μόνο με δόλο, δηλαδή με πρόθεση. Ο δράστης, θα πρέπει να γνωρίζει και να αποδέχεται την πραγμάτωση των στοιχείων της αντικειμενικής υπόστασης και την αιτιακή σχέση τους. Δηλαδή, θα πρέπει να γνωρίζει τον τρόπο πρόκλησης και το αποτέλεσμα του επηρεασμού, οπότε για τα στοιχεία αυτά αρκεί και ο ενδεχόμενος δόλος. Άρα ο δράστης που δεν είναι βέβαιος για την αναλήθεια των στοιχείων αλλά αποδέχεται το ενδεχόμενο να είναι αναληθή, τελεί[140] το έγκλημα[141].

Η υποκειμενική υπόσταση του άρθρου 386Α ΠΚ, όμως, περιλαμβάνει επίσης και τον σκοπό παράνομου περιουσιακού οφέλους. Ο δράστης, δηλαδή, θα πρέπει να γνωρίζει και να επιδιώκει τον προσπορισμό περιουσιακού οφέλους στον εαυτό του ή σε άλλον. Πρόκειται για υπερχειλή υποκειμενική υπόσταση που συνδέεται με τον άμεσο δόλο α' βαθμού, δηλαδή με γνώση και επιδίωξη (έγκλημα σκοπού). Χωρίς τη συνδρομή αυτού του σκοπού η πράξη δεν είναι καν αρχικά άδικη, οπότε ο σκοπός αποτελεί υποκειμενικό στοιχείο του αδίκου. Για το περιουσιακό όφελος απαιτείται επιδίωξη (άμεσος δόλος α' βαθμού), ενώ για το στοιχείο του παρανόμου και τα πραγματικά περιστατικά που το απαρτίζουν, αρκεί ενδεχόμενος δόλος[142].

---

[139] Ό.π.

[140] Στ. Παύλου, Γ. Μπέκας, Ποινικό ΙΙΙ Εγκλήματα κατά της Ιδιοκτησίας, Περιουσίας & Ζωής, 2020, σελ. 310.

[141] Γ. Μπουρμάς σε Α. Χαραλαμπάκη, Ο νέος ποινικός κώδικας – ερμηνεία κατ' άρθρο του ν. 4619/2019, 2020, σελ. 3145.

[142] Χ. Μυλωνόπουλος, Ποινικό δίκαιο – Ειδικό μέρος, 2016, σελ. 557.

Συνεπώς, ο δράστης που δεν επιδιώκει τον πορισμό περιουσιακού οφέλους δεν μπορεί να τιμωρηθεί, ακόμα και αν τελεί με δόλο (β΄ ή ενδεχόμενο) τα υπόλοιπα στοιχεία της αντικειμενικής υπόστασης (π.χ. γνωρίζει ως πιθανή την αναλήθεια[143] ή την πρόκληση περιουσιακής ζημίας και την αποδέχεται). Ελλείποντος του σκοπού περιουσιακού οφέλους, δεν μπορεί να τιμωρηθεί ούτε για απατηλή πρόκληση βλάβης (389 ΠΚ), αφού εκείνη προϋποθέτει άνθρωπο που πείθεται. Μια αναλογία ώστε να καλύπτονται και περιπτώσεις επηρεασμού υπολογιστή, θα αποτελούσε απαγορευμένη αναλογία προς θεμελίωση του αξιοποίνου[144].

Υπάρχει περίπτωση ο φυσικός αυτουργός να μην έχει δόλο ως προς τον επηρεασμό των στοιχείων, αλλά κάποιος να τον χρησιμοποιεί ως όργανό του για να τελέσει το έγκλημα. Τότε κατά μία άποψη συντρέχει περίπτωση έμμεσης αυτουργίας, οπότε αυτός που τον χρησιμοποιεί και διατηρεί την βουλητική και υλική κυριαρχία, θα τιμωρηθεί ως έμμεσος αυτουργός[145]. Σύμφωνα με άλλη άποψη, μπορεί να θεμελιωθεί κανονικά ηθική αυτουργία, αφού η πράξη είναι άδικη αλλά όχι καταλογιστή[146].

4.4 Απόπειρα

Σύμφωνα με το άρθρο 42 του ΠΚ «Όποιος έχοντας αποφασίσει να εκτελέσει κακούργημα ή πλημμέλημα επιχειρεί πράξη που περιέχει τουλάχιστον αρχή εκτέλεσης, τιμωρείται, αν το κακούργημα ή πλημμέλημα δεν ολοκληρώθηκε, με ποινή ελαττωμένη (άρθρο 83)». Η απόπειρα στην απάτη με υπολογιστή είναι και νοητή και δυνατή[147]. Αν παρά τον επηρεασμό, ο δράστης δεν καταφέρνει να βλάψει την ξένη περιουσία, τότε τελεί το 386Α σε απόπειρα.

4.4.1 Αρχή εκτέλεσης

Αρχή εκτέλεσης του εγκλήματος της ΠΚ 386Α, υπάρχει όταν ο επηρεασμός έχει αρχίσει. Αντίθετα, η απλή εκκίνηση ενός προγράμματος που περιέχει μη ορθά ή ελλιπή

[143] Ό.π. Π.χ. τελεί το έγκλημα αυτός που δηλώνει σε μηχανογραφικό δελτίο ότι είναι έγγαμος, ενώ γνωρίζει ως ενδεχόμενο ότι έχει εκδοθεί το διαζύγιό του, για να συνεχίσει να εισπράττει σχετικό επίδομα.

[144] Ό.π.

[145] Χ. Μυλωνόπουλος, Ηλεκτρονικοί υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 65. ΕφΑθ. 1081/08, ΠοινΧρ. Ξ, σελ. 762, ΠλημμΑθ. 638/08, ΠοινΧρ Ξ, σελ. 775.

[146] Στ. Παύλου, Γ. Μπέκας, Ποινικό ΙΙΙ Εγκλήματα κατά της Ιδιοκτησίας, Περιουσίας & Ζωής, 2020, σελ. 310.

[147] Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, 2020, σελ. 162.

δεδομένα, το οποίο δεν έχει επηρεάσει ακόμα τη λειτουργία του υπολογιστή, αποτελεί μη τιμωρητή προπαρασκευαστική πράξη[148]. Συνεπώς, χωρίς τον πραγματικό επηρεασμό από τα ψευδή ή ανακριβή δεδομένα, το έγκλημα δεν υφίσταται ούτε με τη μορφή της απόπειρας[149].

4.4.2 Προπαρασκευαστικές πράξεις

Όπως είδαμε παραπάνω, η δεύτερη παράγραφος του 386Α ΠΚ έχει αναγάγει τις προπαρασκευαστικές πράξεις της κατασκευής, διανομής ή κατοχής προγραμμάτων ή ΠΣ, τα οποία προορίζονται για τη διάπραξη της παρ. 1. Για την εκτενέστερη ανάλυση βλ. 4.2.7. Σε αυτό το σημείο θα πρέπει απλά να τονίσουμε την ανάγκη για διάκριση, μεταξύ της προπαρασκευής, της απόπειρας και της διάπραξης του εγκλήματος. Αυτή, έχει ιδιαίτερη σημασία για την περίπτωση που ο κατασκευαστής του προγράμματος το εκκινήσει χωρίς να επηρεάσει τη λειτουργία του υπολογιστή. Σε αυτή την περίπτωση θα τιμωρηθεί μόνο σύμφωνα με την παρ.2 του 386Α ΠΚ. Αν αντίθετα, επηρεάσει το αποτέλεσμα, χωρίς να βλάψει ξένη περιουσία τελεί το 386Α ΠΚ παρ. 1 σε απόπειρα. Αν, πάλι, το επηρεάσει καταφέρνοντας να βλάψει ξένη περιουσία τελεί ολοκληρωμένο το 386Α ΠΚ.

4.5 Συμμετοχή

Κάθε μορφή συμμετοχής είναι δυνατή στο έγκλημα του 386Α ΠΚ. Είναι δηλαδή δυνατή τόσο η ηθική αυτουργία, η άμεση και απλή συνέργεια, όσο και η συναυτουργία.

4.5.1 Ηθική αυτουργία

Η ΑΠ 734/2021, έκρινε ότι δεν πάσχει η αιτιολογία της απόφασης που θεμελιώνει ηθική αυτουργία σε απάτη με υπολογιστή, ακόμα και αν γίνεται απλή μόνο αναφορά στον τρόπο πρόκλησης. Συγκεκριμένα αποφάνθηκε, ότι αρκεί η αναφορά του τρόπου πρόκλησης της απόφασης για τέλεση του 386Α «με πειθώ και φορτικότητα», χωρίς να χρειάζεται περαιτέρω εξειδίκευση των στοιχείων αυτών[150].

---

[148] Χ. Μυλωνόπουλος, Ηλεκτρονικοί υπολογιστές και Ποινικό Δίκαιο, 1991, σελ. 64.

[149] Γ. Μπουρμάς σε Α. Χαραλαμπάκη, Ο νέος ποινικός κώδικας – ερμηνεία κατ' άρθρο του ν. 4619/2019, 2020, σελ. 3145.

[150] Βλ. ΑΠ 734/2021 «με πειθώ, φορτικότητα και υπόσχεση οικονομικών ωφελημάτων τους κατέπεισε και εμφάνιζαν στο αυτοματοποιημένο μηχανογραφικό σύστημα της παθούσας ότι είχαν πραγματοποιήσει δήθεν συναλλαγή μαζί του … Τούτο επετύγχαναν με τρόπο που τους υπέδειξε, δηλαδή με το να διατρέχουν εκάστη

4.5.2 Άμεση συνέργεια

Είναι δυνατή η παροχή άμεσης συνδρομής στον δράστη της απάτης με υπολογιστή κατά την τέλεση και στην εκτέλεσή της. Συνεπώς είναι νοητή η άμεση συνέργεια στο έγκλημα του 386Α του ΠΚ και το δικαστήριο μπορεί να επιβάλει στον υπαίτιο, ο οποίος συμβάλλει καθοριστικά στο έγκλημα θέτοντας το αντικείμενο προσβολής στη διάθεση του φυσικού αυτουργού, την ποινή του αυτουργού (άρθρο 47 εδ. β' του νέου ΠΚ). Πάντως, για την ύπαρξη άμεσης συνέργειας, θα πρέπει να στοιχειοθετείται η αντικειμενική υπόσταση του εγκλήματος της απάτης με υπολογιστή (κύρια πράξη), χωρίς να εξετάζεται αν ο αυτουργός είναι ικανός προς καταλογισμό[151].

4.5.3 Απλή συνέργεια

Με την ΑΠ 367/2017, αναιρέθηκε η απόφαση 5911/2015 του Τριμελούς Εφετείου Αθηνών, καθώς η εφετειακή απόφαση έκρινε ένοχο τον αναιρεσείοντα ως απλό συνεργό, ενώ τα εκτιθέμενα πραγματικά περιστατικά περιέγραφαν τη δράση φυσικού αυτουργού του 386Α ΠΚ[152]. Συγκεκριμένα περιέγραφαν ως απλή συνέργεια τη δράση σερβιτόρου, ο οποίος υπέκλεψε τα στοιχεία κάρτας, την οποία του παρέδωσε ο νόμιμος κάτοχος της για να πληρώσει το γεύμα του. Πράγματι, αν ο σερβιτόρος παρέδιδε τα στοιχεία της κάρτας σε άλλους θα ήταν συνεργός. Στην κρινόμενη, όμως, περίπτωση, ήταν ο ίδιος αυτός που στη συνέχεια επηρεάζοντας τα στοιχεία ηλεκτρονικού υπολογιστή, χρησιμοποίησε τα στοιχεία αυτά χωρίς δικαίωμα για να αγοράσει χρόνο ομιλίας. Συνεπώς, έπρεπε να κριθεί ως φυσικός αυτουργός απάτης με υπολογιστή.

πιστωτική κάρτα όχι καθ' όλο το μήκος της ειδικής υποδοχής της συσκευής αλλά από τμήμα αυτής, προκειμένου να αναγνωρίζονται ηλεκτρονικά όχι άπαντα τα στοιχεία εγκυρότητας εκάστης πιστωτικής».

[151] ΑΠ 1071/2021.

[152] ΑΠ 367/2017 «αφού ο ίδιος έλαβε στην κατοχή του την πιστωτική κάρτα....κατάφερε να υποκλέψει τα πλήρη στοιχεία της πιστωτικής κάρτας και του κατόχου της, στην συνέχεια επηρεάζοντας τα στοιχεία ηλεκτρονικού υπολογιστή, χρησιμοποίησε τα στοιχεία αυτά στο διαδίκτυο και συγκεκριμένα μέσω ηλεκτρονικού υπολογιστή συνδέθηκε με την ιστοσελίδα της εταιρείας κινητής τηλεφωνίας, εισήλθε στο πρόγραμμα αγοράς χρόνου και χωρίς κανένα δικαίωμα πληκτρολόγησε τα στοιχεία της πιστωτικής που είχε υποκλέψει...με αντίστοιχο παράνομο περιουσιακό όφελος του κατηγορουμένου και των αγνώστων συναυτουργών του...». Ωστόσο, κατά τρόπο αντιφατικό, επισημαίνεται, ότι ο αναιρεσείων ενήργησε έτσι «ως απλός συνεργός αγνώστων ατόμων» είναι επομένως φανερή η αντίφαση και ασάφεια που δημιουργείται ως προς τον τρόπο τέλεσης της απάτης με υπολογιστή (απλή συνέργεια ή φυσική αυτουργία)».

4.5.4 Συναυτουργία

Η ΑΠ 131/2013 αντιμετώπισε περίπτωση συναυτουργίας στο έγκλημα του 386Α ΠΚ. Αφορούσε κατηγορουμένους, οι οποίοι με κοινό δόλο, δηλαδή με συναπόφασή τους, για να αποκομίσουν από κοινού οφέλη, παγίδευαν τα ΑΤΜ με αυτοσχέδιο μηχανισμό αντιγραφής καρτών αυτόματης ανάληψης. Με το μηχανισμό αυτό κατέγραφαν τους κωδικούς των καρτών, τους οποίους οι νόμιμοι κάτοχοί τους πληκτρολογούσαν στο ΑΤΜ. Στη συνέχεια ενεργώντας από κοινού, κατάρτιζαν πλαστές κάρτες ανάληψης χρημάτων, τις τοποθετούσαν σε ΑΤΜ, και χρησιμοποιώντας τον κωδικό, που επίσης είχαν αντιγράψει, προέβαιναν σε αναλήψεις χρημάτων, σε χρέωση των λογαριασμών των νόμιμων κατόχων των καρτών.

4.6 Διακεκριμένες μορφές της απάτης με υπολογιστή

Με την εισαγωγή του νέου Ποινικού Κώδικα (ν. 4619/2019), προβλέφθηκαν εντός του 386Α δύο διακεκριμένες μορφές απάτης με υπολογιστή. Αυτές εντοπίζονται στο β' εδάφιο της πρώτης παραγράφου, καθώς και στην τρίτη παράγραφο του άρθρου 386Α.

4.6.1 Η 386Α παρ. 1 εδ. β'

Σύμφωνα με το β' εδάφιο της παρ. 1 του 386Α «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». Η πρόβλεψη αυτή ακολουθεί το ενιαίο ποσοτικό κριτήριο (αξία του αντικειμένου ή ζημία άνω των 120.000€), το οποίο ακολουθεί ο νέος ΠΚ για τη διαμόρφωση των κακουργηματικών μορφών των βασικών εγκλημάτων. Αυτό το κριτήριο παρά την ανελαστικότητά του, παρέχει την αναγκαία ασφάλεια δικαίου[153].

4.6.2 Η 386Α παρ. 3

Στην τρίτη παράγραφο του εγκλήματος της απάτης με υπολογιστή αναφέρεται ότι «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

[153] Αιτιολογική έκθεση του ν. 4619/2019, σελ. 72. «Οι κακουργηματικές μορφές των βασικών εγκλημάτων στηρίζονται σε ενιαίο ποσοτικό κριτήριο (αξία του αντικειμένου ή ζημία άνω των 120.000€). Το εν λόγω κριτήριο παρέχει ασφάλεια δικαίου η οποία αντισταθμίζει τα επισημασθέντα κατά καιρούς μειονεκτήματά του».

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».

Πρόκειται για την κακουργηματική μορφή της απάτης με υπολογιστή που διαφοροποιείται από την αμέσως παραπάνω (386Α παρ. 1 εδ' β), κατά το ότι απαιτείται η απάτη να στρέφεται αμέσως κατά του νομικού προσώπου του Ελληνικού Δημοσίου ή ΝΠΔΔ ή ΟΤΑ. Η μεγαλύτερη απειλούμενη ποινή, καθώς και η επιμήκυνση του χρόνου παραγραφής (είκοσι έτη αντί δεκαπέντε)[154], εξασφαλίζει τη μείζονα προστασία της δημόσιας περιουσίας από τις απάτες με υπολογιστή.

4.7 Παραγραφή

Το βασικό έγκλημα της απάτης με υπολογιστή (386 παρ. 1 εδάφιο α') παραγράφεται μετά 5 έτη από την τέλεση της πράξης, αφού πρόκειται για πλημμέλημα (ΠΚ 111, 112). Περαιτέρω, η προθεσμία της παραγραφής του πλημμελήματος αναστέλλεται όσο διαρκεί η κύρια διαδικασία, όχι όμως πέραν των τριών ετών (ΠΚ 113)[155]. Το έγκλημα της 386Α παρ. 1 εδ. β', ως κακούργημα παραγράφεται μετά από 15 έτη, ενώ της παρ. 3 μετά από 20 έτη, αφού τούτο ορίζεται ρητά. Η προθεσμία της παραγραφής, αναστέλλεται για τις κακουργηματικές μορφές, το πολύ πέντε έτη.

4.8 Ποινική κύρωση

4.8.1 Για τη βασική μορφή της 386Α παρ. 1, εδ. α'

Ο δράστης του βασικού εγκλήματος της απάτης με υπολογιστή τιμωρείται με φυλάκιση. Αν δε, η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, τιμωρείται με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Σύμφωνα με το άρθρο 83 περ. ε' εδ. τελ. του ΠΚ «Αν ο νόμος προβλέπει σωρευτικά ποινή φυλάκισης και χρηματική ποινή, μπορεί να επιβληθεί και μόνο η τελευταία». Συνεπώς, για την περίπτωση απάτης με υπολογιστή που προκάλεσε ιδιαίτερα μεγάλη ζημία, εάν υπάρχει περίπτωση απόπειρας

[154] Με τις προβλέψεις αυτές του νέου ΠΚ, κατέστη περιττός ο απαρχαιωμένος και προβληματικός ν. 1608/50 και καταργήθηκε.

[155] Η ΑΠ 367/2017, κρίνοντας έναν αναιρετικό λόγο παραδεκτό και βάσιμο, έπαυσε οριστικά την ποινική δίωξη διότι παρήλθε χρονικό διάστημα μεγαλύτερο της οκταετίας, έως το χρόνο συζητήσεως και διασκέψεως.

(ΠΚ 42 παρ. 1), συνέργειας (ΠΚ 47) ή ελαφρυντικών περιστάσεων (ΠΚ 84), μπορεί να επιβληθεί μόνο χρηματική ποινή.

4.8.2 Για τη διακεκριμένη μορφή της 386Α παρ. 1, εδ. β'

Στο β' εδάφιο της πρώτης παραγράφου του 386Α ΠΚ, προβλέπεται η κακουργηματική μορφή απάτης με υπολογιστή, με απειλούμενη ποινή κάθειρξης 5 έως 10 έτη και χρηματική ποινή. Η ποινή αυτή διαμορφώνεται σε 1 έως 6 έτη και χρηματική ποινή, αν συντρέχουν ελαφρυντικές περιστάσεις. Αν στο πρόσωπο του υπαιτίου συντρέχουν περισσότεροι λόγοι μείωσης της ποινής τότε το πλαίσιο ποινής θα είναι 6 μήνες έως 6 έτη (85 παρ. 1 ΠΚ).

4.8.3 Για το ιδιώνυμο έγκλημα της 386Α παρ. 2

Σύμφωνα με τη δεύτερη παράγραφο του 386Α ΠΚ, τιμωρείται με φυλάκιση έως 2 έτη και χρηματική ποινή, ο κατασκευαστής, αυτός που διαθέτει ή ο κάτοχος προγράμματος ή ΠΣ, το οποίο προορίζεται για τη διάπραξη του εγκλήματος της παρ. 1. Στην ίδια παράγραφο, προβλέπεται και υποχρεωτικός προσωπικός λόγος απαλλαγής από την ποινή. Αφορά τον δράστη που καταστρέφει με δική του θέληση το πρόγραμμα ή ΠΣ, πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παρ. 1.

4.8.4 Για την ιδιαίτερα διακεκριμένη μορφή της 386Α παρ. 3

Στην τρίτη παράγραφο της διάταξης 386Α, προβλέπεται ως ιδιαίτερα διακεκριμένη παραλλαγή, η κακουργηματική απάτη με υπολογιστή κατά του Ελληνικού δημοσίου, ΝΠΔΔ ή ΟΤΑ. Η απειλούμενη ποινή για την τελευταία είναι κάθειρξη τουλάχιστον 10 ετών και χρηματική ποινή έως 1.000 ημερήσιες μονάδες.

4.8.5 Εξάλειψη του αξιοποίνου και απαλλαγή από την ποινή

Το αξιόποινο της απάτης με υπολογιστή 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. Με τη μερική ικανοποίηση εξαλείφεται μερικά μόνο το αξιόποινο (405 παρ. 2 ΠΚ). Υπάρχει επίσης, πρόβλεψη για απαλλαγή από την ποινή, αν ο υπαίτιος μέχρι την αμετάκλητη παραπομπή του στο ακροατήριο, ικανοποιήσει εντελώς τον ζημιωθέντα. Για την απαλλαγή από την ποινή της

πλημμελληματικής απάτης με υπολογιστή, η εντελής ικανοποίηση θα πρέπει να γίνει μέχρι το τέλος της αποδεικτικής διαδικασίας στο πρωτοβάθμιο δικαστήριο[156].

4.8.5.1 Η εξάλειψη του αξιοποίνου και η απαλλαγή δεν αφορούν την 386Α παρ. 2

Για την περίπτωση των προπαρασκευαστικών πράξεων απάτης με υπολογιστή της 386Α παρ. 2, δεν προβλέπεται εξάλειψη του αξιοποίνου και απαλλαγή από την ποινή, αφού φυσικά, σε αυτή την περίπτωση δεν υπάρχει καν ζημιωθείς (405 παρ. 2,3). Βέβαια, για εκείνον που αποσύρεται από τα εγκληματικά του κίνητρα, καταστρέφοντας το εν δυνάμει βλαπτικό πρόγραμμα υπολογιστή ή ΠΣ πριν το χρησιμοποιήσει, προβλέπεται προσωπικός λόγος απαλλαγής από την ποινή[157].

4.9 Προβλήματα συρροής

4.9.1 Συρροή με τα εγκλήματα των άρθρων 386 ΠΚ (απάτη) και 372 ΠΚ (κλοπή)

Η κοινή απάτη του άρθρου 386 ΠΚ και η απάτη με υπολογιστή, τελούν σε σχέση αμοιβαίου αποκλεισμού[158]. Αυτό συμβαίνει διότι η κοινή απάτη προϋποθέτει πρόσωπο που πλανάται, ενώ η απάτη με υπολογιστή επηρεασμό του αποτελέσματος επεξεργασίας δεδομένων υπολογιστή. Έτσι, όταν έχει εφαρμογή το ένα έγκλημα, κατά λογική αναγκαιότητα δεν μπορεί να εφαρμοστεί το άλλο.

Ο ίδιος αλληλοαποκλεισμός, ισχύει και στη σχέση μεταξύ απάτης με υπολογιστή και κλοπής, αφού δεν είναι δυνατόν το περιουσιακό όφελος δια του επηρεασμού υπολογιστή να συμπίπτει με την αφαίρεση εξατομικευμένων κινητών πραγμάτων από την κατοχή άλλου.

4.9.2 Συρροή με το έγκλημα του άρθρου 216 ΠΚ (πλαστογραφία)

Είναι πιθανό, η απάτη με υπολογιστή να συρρέει με την πλαστογραφία με χρήση του πλαστού. Αυτό θα συμβαίνει κατά κύριο λόγο όταν υπάρχει αλλοίωση μέσου, το οποίο χρησιμοποιείται από τον υπολογιστή ή περιφερειακή μνήμη υπολογιστή. Για να προστατεύεται, βέβαια, αυτό το μέσο ως έγγραφο, θα πρέπει να προορίζεται να αποδείξει γεγονότα που έχουν έννομη σημασία. Κατά την κρατούσα άποψη στη νομολογία, η

[156] Μ. Μαργαρίτης – Α. Μαργαρίτη, Ποινικός Κώδικας Ερμηνεία – Εφαρμογή, 2020, σελ. 1252 «Είναι αυτοτελής ισχυρισμός, ο περί ικανοποίησης του παθόντος».

[157] Βλ. παραπάνω 4.2.7.2.

[158] Χ. Μυλωνόπουλος, Ποινικό Δίκαιο – Ειδικό Μέρος, 2016, σελ. 558.

κακουργηματική απάτη με υπολογιστή συρρέει αληθινά με την κακουργηματική πλαστογραφία με χρήση[159]. Αντίθετα η απόπειρα κακουργηματικής απάτης με υπολογιστή συρρέει φαινομενικά με την κακουργηματική πλαστογραφία με χρήση και απορροφάται από την τελευταία. Επίσης φαινομενική συρροή έχουμε και στην περίπτωση τετελεσμένης απάτης με υπολογιστή, η οποία απορροφάται από την κακουργηματική πλαστογραφία μετά χρήσεως ή χρήση πλαστού της 216 παρ. 3β[160].

4.9.3 Συρροή με το έγκλημα της εγκληματικής οργάνωσης (187 ΠΚ)

Αληθινή και πραγματική είναι η συρροή μεταξύ της απάτης με υπολογιστή και της συμμετοχής σε εγκληματική οργάνωση. Αυτό συμβαίνει διότι με τις δύο διατάξεις προστατεύονται διαφορετικά έννομα αγαθά, δηλαδή η περιουσία με την πρώτη και η δημόσια τάξη με την δεύτερη. Πραγματική είναι δε η συρροή, διότι τα δύο εγκλήματα τελούνται με διαφορετικές πράξεις.

4.10 Ειδικές ρυθμίσεις

4.10.1 Νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες (ν. 4557/2018)

Το άρθρο 386Α ΠΚ, συγκαταλέγεται στα «βασικά αδικήματα» του ν. 4557/2018[161] για την «Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας». Πρόκειται για ενσωμάτωση της Οδηγίας (ΕΕ) 2018/1673 σχετικά με την καταπολέμηση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες μέσω του ποινικού δικαίου. Στόχος της Οδηγίας είναι, οι δράστες της νομιμοποίησης εσόδων από παράνομες δραστηριότητες να υπόκεινται σε αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις σε όλα τα κράτη μέλη[162].

[159] Γ. Δανιήλ σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, 2023, σελ. 99.

[160] 216 παρ. 3: «Αν ο υπαίτιος των πράξεων των παρ. 1 και 2 σκόπευε να προσπορίσει στον εαυτό του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται: β) εάν το συνολικό όφελος ή η συνολική ζημία υπερβαίνει τις εκατόν είκοσι χιλιάδες (120.000) ευρώ, με κάθειρξη έως δέκα (10) έτη και χρηματική ποινή».

[161] Άρθρο 4 στοιχείο ζ' του ν. 4557/2018, όπως αυτός τροποποιήθηκε με το ν. 4816/2021.

[162] Αιτιολογική σκέψη 22 της Οδηγίας (ΕΕ) 2018/1673.

Ως «εγκληματική δραστηριότητα», νοείται η διάπραξη των βασικών αδικημάτων του άρθρου 4 του ν. 4557/2018[163]. Συνεπώς, για τη στοιχειοθέτηση της νομιμοποίησης εσόδων από εγκληματική δραστηριότητα, προϋποτίθεται η τέλεση του βασικού εγκλήματος -στην περίπτωσή μας του 386Α ΠΚ- και επιπλέον πράξεις που κατατείνουν στο ξέπλυμα. Τέτοιες πράξεις είναι η μετατροπή ή μεταβίβαση της περιουσίας που προέρχεται από εγκληματική δραστηριότητα. Είναι επίσης η απόκρυψη ή συγκάλυψη της αλήθειας όσον αφορά την προέλευσή της ή η απόκτηση, κατοχή ή χρήση τέτοιας περιουσίας εν γνώσει ότι προέρχεται από εγκληματική δραστηριότητα. Ακόμα, συνιστά ξέπλυμα, η χρησιμοποίηση του χρηματοπιστωτικού τομέα, με την τοποθέτηση ή διακίνηση σε αυτόν εσόδων από εγκληματική δραστηριότητα με σκοπό να προσδοθεί νομιμοφάνεια στα σχετικά έσοδα[164].

4.10.2 Καταπολέμηση της απάτης και άλλων παράνομων δραστηριοτήτων εις βάρος των οικονομικών συμφερόντων της Ε.Ε. (ν. 4689/2020)

Με το νόμο 4689/2020 ενσωματώθηκε η Οδηγία (ΕΕ) 2017/1371 «Σχετικά με την καταπολέμηση, μέσω του ποινικού δικαίου, της απάτης εις βάρος των συμφερόντων της Ένωσης». Σύμφωνα με το άρθρο 21 παρ. 1 του ν. 4689/2020, στόχος είναι η ενίσχυση της

[163] Άρθρο 3 στοιχείο 23 του ν. 4557/2018.

[164] Το άρθρο 2 του ν. 4557/2018, όπως αυτό τροποποιήθηκε με το ν. 4816/2021 ορίζει ότι: «Νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες (ξέπλυμα χρήματος) συνιστούν οι εξής πράξεις:

α) η μετατροπή ή η μεταβίβαση περιουσίας εν γνώσει του γεγονότος ότι προέρχεται από εγκληματική δραστηριότητα, ή από πράξη συμμετοχής σε τέτοια δραστηριότητα, με σκοπό την απόκρυψη ή τη συγκάλυψη της παράνομης προέλευσής της, ή την παροχή συνδρομής σε οποιονδήποτε ενέχεται στη δραστηριότητα αυτή για να αποφύγει τις έννομες συνέπειες των πράξεών του,

β) η απόκρυψη ή συγκάλυψη της αλήθειας, όσον αφορά τη φύση, την προέλευση, τη διάθεση, τη διακίνηση ή τη χρήση περιουσίας ή τον τόπο όπου αυτή βρίσκεται ή την κυριότητα επ' αυτής, ή τα σχετικά με αυτή δικαιώματα, εν γνώσει του γεγονότος ότι η περιουσία αυτή προέρχεται από εγκληματική δραστηριότητα ή από πράξη συμμετοχής σε τέτοια δραστηριότητα,

γ) η απόκτηση, κατοχή ή χρήση περιουσίας, εν γνώσει, κατά τον χρόνο κτήσης, ή κατά τον χρόνο περιέλευσης της κατοχής ή της χρήσης, του γεγονότος ότι η περιουσία προέρχεται από εγκληματική δραστηριότητα ή από πράξη συμμετοχής σε τέτοια δραστηριότητα,

δ) η χρησιμοποίηση του χρηματοπιστωτικού τομέα με την τοποθέτηση σε αυτόν ή τη διακίνηση μέσω αυτού εσόδων που προέρχονται από εγκληματικές δραστηριότητες, με σκοπό να προσδοθεί νομιμοφάνεια στα εν λόγω έσοδα».

προστασίας κατά των ποινικών αδικημάτων που θίγουν τα οικονομικά συμφέροντα της Ευρωπαϊκής Ένωσης.

Συνοπτικά, με τον ν. 4689/2020 εισάγονται επικουρικές διατάξεις[165], με στόχο να τιμωρούνται οι προσβολές ενωσιακών συμφερόντων, για τις οποίες ο δράστης δεν θα μπορούσε να τιμωρηθεί -ή θα τιμωρούνταν ελαφρύτερα- με βάση το άρθρο 386Α[166]. Έτσι, εάν μια προσβολή των οικονομικών συμφερόντων της Ε.Ε., στοιχειοθετεί παράλληλα το έγκλημα του 386Α και προβλέπεται από το τελευταίο μεγαλύτερη ποινή, τότε οι διατάξεις του ν. 4689/2020 θα απωθούνται σύμφωνα με τη σχετική ρήτρα επικουρικότητας[167]. Εάν αντίθετα ο δράστης δεν μπορεί να τιμωρηθεί με βάση το 386Α ΠΚ ή τιμωρείται ελαφρύτερα με βάση αυτό, τότε θα εφαρμόζονται οι διατάξεις του ν. 4689/2020[168].

4.11 Τόπος τέλεσης

Ως τόπος τέλεσης της απάτης με υπολογιστή, θεωρείται τόσο ο τόπος όπου ο υπαίτιος διέπραξε την αξιόποινη ενέργεια, όσο και ο τόπος όπου επήλθε το αποτέλεσμα[169]. Δηλαδή, τόπος τέλεσης είναι ο τόπος όπου έλαβε χώρα ο επηρεασμός του αποτελέσματος της διαδικασίας επεξεργασίας δεδομένων υπολογιστή με κάποιον από τους πέντε τρόπους, καθώς και ο τόπος όπου επήλθε στον παθόντα η βλάβη – μείωση περιουσίας. Πιο

[165] Βλ. άρθρο 24 του ν. 4689/2020 «1. Όποιος χρησιμοποιεί ή υποβάλλει ψευδείς, ανακριβείς ή ελλιπείς δηλώσεις ή έγγραφα ή αποσιωπά πληροφορίες κατά παράβαση ειδικής νομικής υποχρέωσης ανακοίνωσής τους και, με τον τρόπο αυτό, λαμβάνει ή παρακρατεί παρανόμως επιχορηγήσεις ή όμοιας φύσης οικονομικές παροχές που δεν συνδέονται άμεσα με ισάξιες αντιπαροχές και προέρχονται από τον προϋπολογισμό της Ευρωπαϊκής Ένωσης ή τους προϋπολογισμούς των κάθε είδους οργάνων και οργανισμών της, ανεξαρτήτως του εκάστοτε φορέα διαχείρισης, τιμωρείται με φυλάκιση, εκτός αν η πράξη τιμωρείται βαρύτερα με βάση τα άρθρα 386, 386Α ή 386Β του Π.Κ.. Με την ίδια ποινή και την ίδια επιφύλαξη τιμωρείται και όποιος εν γνώσει χρησιμοποιεί νόμιμα ληφθείσες παροχές υπό την παραπάνω έννοια, οι οποίες υπάγονται με βάση τον νόμο ή τη σύμβαση χορήγησής τους σε συγκεκριμένους περιορισμούς, κατά παράβαση αυτών των περιορισμών». Βλ. και παρ. 2,3 του ίδιου.

[166] Δυνάμει του άρθρου 3 παρ. 2 στοιχ. α', β΄, γ΄ και 4 παρ. 3 της Οδηγίας (ΕΕ) 1371/2017, έπρεπε να ποινικοποιηθούν συμπεριφορές που προσβάλλουν τα οικονομικά συμφέροντα της Ε.Ε., αλλά δεν καλύπτονται από το υφιστάμενο ποινικό οπλοστάσιο των άρθρων 375, 386, 386Α, 386Β και 390 ΠΚ.

[167] Βλ. άρθρο 24 παρ. 1,2,3 του ν. 4689/2020 «εκτός αν η πράξη τιμωρείται βαρύτερα με βάση τα άρθρα 386 ή 386Α Π.Κ.».

[168] Π. Παναγιωτόπουλος σε Επίκαιρα ζητήματα οικονομικού ποινικού δικαίου, διεύθυνση σειράς Μ. Καϊάφα – Γκμπάντι, 2021, σελ. 61 επ.

[169] Για τον τόπο τέλεσης του διαδικτυακού εγκλήματος βλ. Θ. Κριθαρά, Ποινικό δίκαιο και διαδίκτυο, 2009.

συγκεκριμένα, ο τόπος όπου έγινε λήψη των μη ορθών δεδομένων από τον παθόντα, αποτελεί τον τόπο όπου επήλθε το αποτέλεσμα, καθώς τα μη ορθά δεδομένα με τη λήψη τους, εγγράφηκαν στον σκληρό δίσκο του θύματος (μεταβολή στον εξωτερικό κόσμο)[170].

4.12 Διεθνής δικαιοδοσία

Οι ηλεκτρονικές συναλλαγές μπορούν να λάβουν χώρα οπουδήποτε στον κόσμο, άρα και οπουδήποτε μπορεί επέλθει ο επηρεασμός του αποτελέσματος διαδικασίας επεξεργασίας δεδομένων υπολογιστή[171]. Με τον νέο ΠΚ καταργήθηκε η διάταξη του άρθρου 5 παρ. 3 ΠΚ που είχε εισαχθεί με το άρθρο 2 του ν. 4267/2014. Η τελευταία είχε επεκτείνει αδικαιολόγητα την αρχή της εδαφικότητας, προβλέποντας ότι «όταν η πράξη τελείται μέσω διαδικτύου, τόπος τέλεσης θεωρείται και η ελληνική επικράτεια, εφόσον στο έδαφός της παρέχεται πρόσβαση στα συγκεκριμένα μέσα ανεξάρτητα από τον τόπο εγκατάστασής τους»[172]. Με το τρέχον καθεστώς, αν η απάτη με υπολογιστή στρέφεται κατά ημεδαπού θα διώκεται σύμφωνα με τους όρους των άρθρων 6 και 7 του ΠΚ, ενώ σε κάθε περίπτωση, οι ελληνικοί ποινικοί νόμοι θα εφαρμόζονται σε ημεδαπούς ή αλλοδαπούς, ανεξάρτητα του τόπου τέλεσης, αν πρόκειται για έγκλημα σχετικό με τα μέσα πληρωμής πλην των μετρητών[173].

4.13 Δικονομικά ζητήματα

4.13.1 Η ποινική δίωξη

Για την ποινική δίωξη της ΠΚ 386Α παρ. 1, απαιτείται έγκληση (405 παρ. 1). Αντίθετα, η δίωξη είναι αυτεπάγγελτη στο ιδιώνυμο έγκλημα της 386Α παρ. 2 καθώς και στην παρ. 3. Η αυτεπάγγελτη δίωξη στις περιπτώσεις προπαρασκευαστικών πράξεων απάτης με υπολογιστή (386Α παρ. 2), προβλέφθηκε για πρώτη φορά στην τελευταία τροποποίηση του ΠΚ με τον ν. 4947/2022. Πρόκειται για καίρια νομοθετική επέμβαση, καθώς η πράξη της 386Α παρ. 2, θα παρέμενε de facto ακαταδίωκτη, εφόσον για τις

[170] Για την καθ΄ ύλην αρμοδιότητα του Τριμελούς πλημμελειοδικείου βλ. Θ. Δαλακούρα, Ο Νέος Κώδικας Ποινικής Δικονομίας, 2020, σελ. 103-107.

[171] Δ. Κιούπης, Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, 2023, σελ. 47.

[172] Αιτιολογική Έκθεση του ν. 4619/2019, σελ. 4.

[173] Με τον ν. 4947/2022 προστέθηκε στο στοιχείο η' του άρθρου 8 η αναφορά εκτός από το νόμισμα και στα «μέσα πληρωμής πλην των μετρητών».

προπαρασκευαστικές πράξεις δεν υπάρχουν άμεσα παθόντες και δικαιούχοι σε υποβολή έγκλησης. Δηλαδή αν απαιτούνταν έγκληση, κανείς δεν θα μπορούσε να είναι εγκαλών, αφού το αξιόποινο του 386Α παρ. 2 περιορίζεται στον χρόνο πριν την προσβολή του εννόμου αγαθού[174].

4.13.2 Παράσταση για υποστήριξη της κατηγορίας

Ήδη από τον ν. 4620/2019, σύμφωνα με το άρθρο 63 του ΚΠΔ, οι ζημιωθέντες μπορούν να παραστούν στο δικαστήριο μόνο για την υποστήριξη της κατηγορίας. Έχει κριθεί ότι στην περίπτωση ανάληψης μετρητών από ΑΤΜ με πλαστή κάρτα, νομιμοποιείται σε παράσταση προς υποστήριξη της κατηγορίας η τράπεζα που αναγκάστηκε να αποζημιώσει τους νόμιμους δικαιούχους (ΑΠ 131/2013).

4.13.3 Άρση του απορρήτου

Σύμφωνα το άρθρο 6 παρ. 1α' του ν. 5002/2022, επιτρέπεται η άρση του απορρήτου για τη διακρίβωση κακουργηματικών μορφών απάτης με υπολογιστή (386Α παρ. 1 εδ. β' και παρ. 3). Η απάτη με υπολογιστή συγκαταλέγεται, όμως, και στα λίγα πλημμελήματα για τα οποία μπορεί να αρθεί το απόρρητο (6 παρ. 2α' του ν. 5002/2022). Για την άρση του απορρήτου των επικοινωνιών στις περιπτώσεις αυτές, το συμβούλιο εκδίδει εντός 48 ωρών, ειδικά αιτιολογημένο βούλευμα μετά από πρόταση του εισαγγελέα. Σε εξαιρετικά επείγουσες περιπτώσεις την άρση μπορεί να διατάξει ο εισαγγελέας ή ο ανακριτής[175].

4.13.4 Ευρωπαϊκή εντολή υποβολής και ευρωπαϊκή εντολή διατήρησης στοιχείων

Σε ένα περιβάλλον διασυνοριακής ηλεκτρονικής εγκληματικότητας, η συνεργασία των κρατών για την έρευνα και τη δίωξη των εγκλημάτων αποτελεί αδιαπραγμάτευτο όρο. Πολύ σημαντικότερη είναι η συνεργασία, για ποινικά αδικήματα τα οποία τελούνται με

[174] Για το ίδιο λόγο -ότι δεν υπάρχει ζημιωθείς-, αποκλείεται και η εξάλειψη του αξιοποίνου λόγω εντελούς ικανοποίησης καθώς και η απαλλαγή από την ποινή, βλ. 5.8.5.1.

[175] Η παρ. 3 του άρθρου 6 του ν. 5002/2022 ορίζει ότι: «Στην περίπτωση αυτή, ο εισαγγελέας ή ο ανακριτής υποχρεούται να εισαγάγει το ζήτημα, μέσα σε προθεσμία τριών (3) ημερών, στο αρμόδιο δικαστικό συμβούλιο, το οποίο ελέγχει παράλληλα τη συνδρομή των εξαιρετικά επειγουσών περιστάσεων. Διαφορετικά, η ισχύς της σχετικής διάταξης αίρεται αυτοδικαίως. Αν εντός ευλόγου χρόνου, που δεν μπορεί να υπερβαίνει τις πέντε (5) ημέρες συνολικά, δεν εκδοθεί βούλευμα, τα ευρήματα δεν είναι αξιοποιήσιμα».

υπολογιστή. Οι πληροφορίες για τα αδικήματα αυτά βρίσκονται κατά κανόνα διαθέσιμες μόνο σε ηλεκτρονική μορφή, ενώ και η μορφή αυτή, είναι συνυφασμένη με την παροδικότητα[176].

Με βάση τα παραπάνω δεδομένα, η Επιτροπή, εισήγαγε πρόταση για την υιοθέτηση Κανονισμού «σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις». Σύμφωνα με την τελευταία, θεσπίζονται κανόνες με τους οποίους, μία αρμόδια δικαστική αρχή μπορεί να διατάξει έναν πάροχο υπηρεσιών που παρέχει υπηρεσίες στην Ένωση, να υποβάλει ή να διατηρήσει ηλεκτρονικές πληροφορίες που μπορούν να χρησιμεύσουν ως αποδεικτικά στοιχεία[177].

Ο Κανονισμός αυτός αναμένεται να συνδράμει καταλυτικά στη διερεύνηση και τη δίωξη της απάτης με υπολογιστή, καθότι οι πληροφορίες σχετικά με το συγκεκριμένο αδίκημα βρίσκονται κατ' αρχήν σε ηλεκτρονική μορφή και συνήθως εκτός συνόρων. Πάντως, σε κάθε περίπτωση, θα πρέπει να επιδιωχθεί η ισορροπία μεταξύ της ποινικής αξίωσης της πολιτείας για διακρίβωση του εγκλήματος και της προστασίας των υποκειμένων των δεδομένων[178].

---

[176] Αιτιολογική Σκέψη 32 της Πρότασης Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις.

[177] Ό.π. Αιτ. σκέψη 15.

[178] Η πρόταση του Κανονισμού φαίνεται να δίδει την δέουσα σημασία σε ζητήματα προστασίας των πληροφοριών. Βλ. σκέψη 11γ «Μόνο εξουσιοδοτημένα πρόσωπα θα πρέπει να έχουν πρόσβαση σε πληροφορίες που περιέχουν δεδομένα προσωπικού χαρακτήρα», σκέψη 43β «δεν θα πρέπει χρησιμοποιούνται για σκοπούς άλλους από εκείνους για τους οποίους συλλέχθηκαν σύμφωνα με τον παρόντα κανονισμό», σκέψη 43γ «Οι ηλεκτρονικές πληροφορίες που έχουν συλλεχθεί κατά παράβαση οποιασδήποτε από τις προϋποθέσεις που απαριθμούνται στον παρόντα κανονισμό θα πρέπει να διαγράφονται χωρίς αδικαιολόγητη καθυστέρηση», σκέψη 43δ «Οι ηλεκτρονικές πληροφορίες που έχουν συλλεγεί κατά παράβαση του παρόντος κανονισμού δεν θα πρέπει να γίνονται δεκτές ενώπιον δικαστηρίου».

5 Οι νέες ρυθμίσεις για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών

5.1 Γενικά

Με τον ν. 4947/2022, ενσωματώθηκε στην ελληνική έννομη τάξη η Οδηγία (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 «για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης - πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου (L 123)». Η Οδηγία (ΕΕ) 2019/713 επιδιώκει την εναρμόνιση της νομοθεσίας των κρατών μελών στα αδικήματα, που αφορούν στα μέσα πληρωμής πλην των μετρητών. Πράγματι, τα αδικήματα της απάτης και της πλαστογραφίας, συνιστούν απειλή για την ασφάλεια των συναλλαγών, αντιπροσωπεύουν πηγή εισοδήματος για το οργανωμένο έγκλημα και ευνοούν την ανάπτυξη άλλων εγκληματικών δραστηριοτήτων, όπως της τρομοκρατίας και της διακίνησης ναρκωτικών. Επίσης, αποτελούν εμπόδιο στην ψηφιακή ενιαία αγορά, διότι κλονίζουν την εμπιστοσύνη των καταναλωτών και προκαλούν άμεσες οικονομικές ζημιές[179].

5.2 Ο τρόπος ενσωμάτωσης της Οδηγίας (ΕΕ) 2019/713

Επιλέχθηκε η ενσωμάτωση της Οδηγίας με τροποποίηση του Ποινικού Κώδικα, αντί της θέσπισης ενός ειδικού ποινικού νόμου που θα περιλάμβανε τις σχετικές ρυθμίσεις. Αυτός ο τρόπος ενσωμάτωσης δεν επελέγη τυχαία, αλλά προτιμήθηκε για λόγους συστηματικής ενότητας. Η Οδηγία προβλέπει πράγματι αδικήματα σχετικά με τα μέσα πληρωμής πλην των μετρητών, τα οποία συνδέονται με έννομα αγαθά, τα οποία ήδη προστατεύονται στον ΠΚ και συγκεκριμένα στο ένατο και εικοστό τρίτο κεφάλαιό του. Έτσι, με την ενσωμάτωσή της στον ΠΚ, αποφεύχθηκε η παράλληλη ισχύς περισσότερων νόμων γενικότερου και ειδικότερου περιεχομένου με το ίδιο κατ' ουσίαν αντικείμενο[180].

[179] Αιτιολογικές σκέψεις 1 και 2 της Οδηγίας (ΕΕ) 2019/713.

[180] Αιτιολογική έκθεση για το Σχέδιο νόμου του Υπουργείου Δικαιοσύνης με τίτλο «Ενσωμάτωση της Οδηγίας (ΕΕ) 2019/713 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 για την καταπολέμηση της απάτης και της πλαστογραφίας μέσων πληρωμής πλην των μετρητών και την αντικατάσταση της απόφασης-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου», σελ. 2.

5.3 Ορισμοί

5.3.1 Το μέσο πληρωμής πλην των μετρητών

Στο άρθρο 13 του ΠΚ, το οποίο αφορά στην έννοια των όρων του κώδικα, προστέθηκε η περίπτωση η΄, ώστε να μεταφερθούν αυτούσιοι οι ορισμοί που προβλέπονται στην Οδηγία (ΕΕ) 2019/713[181]. Συγκεκριμένα, δίνονται οι ορισμοί για το «μέσο πληρωμής πλην των μετρητών» και για τον «προστατευόμενο μηχανισμό, αντικείμενο ή αρχείο». Οι έννοιες αυτές είναι απαραίτητες τόσο για την ερμηνεία των νέων διατάξεων που εισάγονται στον ΠΚ, όσο και για εκείνες που τροποποιούνται με τις νέες ρυθμίσεις του ν. 4947/2022[182].

Συγκεκριμένα το άρθρο 13 περ. η' του ΠΚ αναφέρει ότι «Μέσο πληρωμής πλην των μετρητών είναι 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[183]. 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».

Συνεπώς, μέσο πληρωμής πλην των μετρητών είναι ο άυλος ή υλικός μηχανισμός, αντικείμενο ή αρχείο[184], ο οποίος χρησιμεύει στη μεταφορά χρημάτων ή νομισματικής αξίας[185] και προστατεύεται από την απομίμηση ή δόλια χρήση.

---

[181] Άρθρο 2 στοιχεία α και β της Οδηγίας (ΕΕ) 2019/713.

[182] Η προσθήκη των όρων αυτών στο γενικό μέρος του ΠΚ και όχι σε επιμέρους κεφάλαια του ειδικού μέρους, κρίθηκε ορθότερη, αφού πολλές διατάξεις διαφορετικών κεφαλαίων αφορούν στα μέσα πληρωμής πλην των μετρητών. Βλ. αιτ. έκθεση ν. 4947/2022, σελ. 8.

[183] Σύμφωνα με την Οδηγία (ΕΕ) 2019/713 άρθρο 2 γ'.

[184] Ή συνδυασμός τους.

[185] Το άρθρο 2 σημείο 2 της Οδηγίας 2009/110/ΕΚ αναφέρει ότι «ως ηλεκτρονικό χρήμα, νοείται οιαδήποτε αποθηκευμένη σε ηλεκτρονικό, μεταξύ άλλων και μαγνητικό υπόθεμα νομισματική αξία αντιπροσωπευόμενη από απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για τον σκοπό της πραγματοποίησης πράξεων πληρωμών όπως ορίζονται στο άρθρο 4 σημείο 5) της οδηγίας 2007/64/ΕΚ και η οποία γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη».

5.3.2 Οι λοιποί ορισμοί της Οδηγίας (ΕΕ) 2019/713

Στο άρθρο 2 της Οδηγίας (ΕΕ) 2019/713, δίδονται επιπλέον, οι ορισμοί για το ψηφιακό μέσο συναλλαγής, το εικονικό νόμισμα, το σύστημα πληροφοριών, τα ηλεκτρονικά δεδομένα και το νομικό πρόσωπο.

Ως ψηφιακό μέσο συναλλαγής[186], νοείται κάθε μορφή ηλεκτρονικού χρήματος ή εικονικό νόμισμα. Για το συγκεκριμένο όρο, κρίθηκε ότι δεν απαιτείται ειδική ρύθμιση, που να καθορίζει την έννοιά του. Αυτή η επιλογή δικαιολογείται από το ότι αμφότερες οι έννοιες του «ηλεκτρονικού χρήματος» και του «εικονικού νομίσματος», οι οποίες συγκροτούν το ψηφιακό μέσο συναλλαγής, προβλέπονται ήδη, η μεν πρώτη στο άρθρο 10 του ν. 4021/2011[187], η δε δεύτερη στο άρθρο 3 του ν. 4557/2018.

Εικονικό νόμισμα[188], αποτελεί, δε, «η ψηφιακή αναπαράσταση αξίας η οποία δεν εκδίδεται από κεντρική τράπεζα ή δημόσια αρχή ούτε έχει την εγγύησή τους, δεν συνδέεται κατ' ανάγκη με νομίμως κυκλοφορούν νόμισμα και δεν διαθέτει το νομικό καθεστώς νομίσματος ή χρήματος, όμως γίνεται αποδεκτή από φυσικά ή νομικά πρόσωπα ως μέσο συναλλαγής, και η οποία μπορεί να μεταφέρεται, να αποθηκεύεται και να διακινείται ηλεκτρονικά». Ο ορισμός αυτός για το εικονικό νόμισμα, έχει ήδη περιληφθεί στο άρθρο 3 αριθ. 24 του ν. 4557/2018.

Περαιτέρω, οι ορισμοί του «συστήματος πληροφοριών» και των «ηλεκτρονικών δεδομένων»[189], αντιστοιχούν στους ορισμούς του «πληροφοριακού συστήματος» και των «ψηφιακών δεδομένων», οι οποίοι προβλέπονται ήδη στις περ. στ΄ και ζ΄ του άρθρου 13 του ΠΚ, μετά τη μεταφορά στο εθνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013.

---

[186] Άρθρο 2 σημείο γ’ της Οδηγίας (ΕΕ) 2019/713.

[187] Σύμφωνα με το άρθρο 10 παρ. 1 του ν. 4021/2011 ως ηλεκτρονικό χρήμα νοείται «οποιαδήποτε νομισματική αξία αποθηκευμένη σε ηλεκτρονικό, συμπεριλαμβανομένου μαγνητικού, υπόθεμα, που εμφανίζεται ως απαίτηση έναντι του εκδότη ηλεκτρονικού χρήματος, η οποία έχει εκδοθεί κατόπιν παραλαβής χρηματικού ποσού για το σκοπό της πραγματοποίησης πράξεων πληρωμών όπως ορίζονται στο άρθρο 4 παρ. 5 του ν. 3862/2010 (Α' 113) και γίνεται δεκτή από άλλα φυσικά ή νομικά πρόσωπα πέραν του εκδότη». Ο ορισμός αυτός υιοθετήθηκε από το άρθρο 2 σημείο 2 της Οδηγίας 2009/110/ΕΚ -στην ίδια παραπέμπει το 2 γ’ της Οδηγίας (ΕΕ) 2019/713.

[188] Άρθρο 2 σημείο δ’ της Οδηγίας (ΕΕ) 2019/713.

[189] Ο.π. σημεία ε’ και στ’.

Τέλος, ως «νομικό πρόσωπο»[190] ορίζεται η οντότητα που διαθέτει νομική προσωπικότητα σύμφωνα με το ισχύον δίκαιο, εξαιρουμένων των κρατών ή των δημόσιων φορέων κατά την άσκηση κρατικής εξουσίας και των δημόσιων διεθνών οργανισμών.

5.4 Οι αλλαγές στο 9ο Κεφάλαιο του ΠΚ (εγκλήματα σχετικά με το νόμισμα, άλλα μέσα πληρωμής και ένσημα)

5.4.1 Η παραχάραξη νομίσματος και άλλων υλικών μέσων πληρωμής (ΠΚ 207 παρ. 2)

Ήδη με τον νέο ΠΚ (ν. 4619/2019), θεσπίστηκε ως ειδικότερη αυτοτελής πράξη η «πλαστοποίηση των άλλων μέσων πληρωμής»[191]. Με το ν. 4947/2022 τροποποιήθηκε[192] η δεύτερη παράγραφος του άρθρου 207 ΠΚ, ώστε να συμβαδίζει με την Οδηγία (ΕΕ) 2019/713.

Στην τρέχουσα μορφή της, η παρ. 2 του άρθρου 207 ΠΚ έχει ως εξής: «Με την ίδια ποινή[193] τιμωρείται και όποιος, με τον ίδιο σκοπό, παραποιεί ή νοθεύει κάθε άλλο υλικό μέσο πληρωμής, εκτός από το νόμισμα, όπως πιστωτικές κάρτες, χρεωστικές κάρτες και λοιπές κάρτες που εκδίδονται από χρηματοπιστωτικά ιδρύματα, ταξιδιωτικές επιταγές, λοιπές επιταγές και συναλλαγματικές».

Συνεπώς, με κάθειρξη έως 10 έτη και χρηματική ποινή τιμωρείται όποιος παραποιεί ή νοθεύει κάθε άλλο υλικό μέσο πληρωμής, εκτός από το νόμισμα, με σκοπό να το θέσει (ενν. το υλικό μέσο πληρωμής) σε κυκλοφορία σαν γνήσιο.

---

[190] Ό.π. σημείο ζ'.

[191] Στην αιτιολογική έκθεση του νέου ΠΚ (ν. 4619/2019), σελ. 45, αναφέρεται ότι «θεσπίστηκε ως ειδικότερη αυτοτελής πράξη η πλαστοποίηση των άλλων μέσων πληρωμής, στην εννοιολογική περιγραφή των οποίων ακολουθούνται οι προβλέψεις της Απόφασης - Πλαισίου 2001/413/ΔΕΥ».

[192] Ο νέος ποινικός κώδικας (ν. 4619/2019) όριζε στην παρ. 2 του άρθρου 207 ότι «με την ίδια ποινή τιμωρείται και όποιος, με τον ίδιο σκοπό, παραποιεί ή νοθεύει κάθε άλλο ενσώματο μέσο, εκτός από το νόμισμα, που λόγω της ιδιαίτερης φύσης του, μόνο του ή σε συνδυασμό με άλλο μέσο πληρωμής, επιτρέπει στον κάτοχο ή στο χρήστη του να μεταφέρει χρήματα ή νομισματική αξία και προστατεύεται από την απομίμηση ή τη δόλια χρήση μέσω σχεδιασμού, κωδικού ή υπογραφής ή άλλου πρόσφορου τρόπου».

[193] Σύμφωνα με την παρ. 1 του 207 ΠΚ «Όποιος παραποιεί ή νοθεύει νόμισμα οποιουδήποτε κράτους ή εκδοτικής αρχής, είτε κατά είτε πριν από το χρόνο νόμιμης κυκλοφορίας του είτε κατά το διάστημα κατά το οποίο γίνεται δεκτό προς ανταλλαγή από τους αρμόδιους φορείς, με σκοπό να το θέσει σε κυκλοφορία σαν γνήσιο, ή κατέχει πλαστό νόμισμα με τον ίδιο σκοπό, τιμωρείται με κάθειρξη έως δέκα (10) έτη και χρηματική ποινή».

Με τη ρύθμιση αυτή του 207 παρ. 2 ΠΚ, η ελληνική νομοθεσία εναρμονίζεται με το άρθρο 4 της Οδηγίας (ΕΕ) 2019/713. Η τελευταία υποχρέωνε τα κράτη μέλη, να διασφαλίσουν ότι θα τιμωρείται ως ποινικό αδίκημα η δόλια πλαστογράφηση ή παραποίηση των υλικών μέσων πληρωμής πλην μετρητών (περ. β΄ άρθρου 4 Οδηγίας) καθώς και την κατοχή και προμήθεια τέτοιων πλαστογραφημένων ή παραποιημένων υλικών μέσων πληρωμής (περ. γ΄ και δ΄ άρθρου 4 Οδηγίας).

Ως προς την κατοχή και προμήθεια πλαστογραφημένων ή παραποιημένων μέσων πληρωμής, εισήχθη νέα παράγραφος 2Α στο άρθρο 207 ΠΚ. Σύμφωνα με την τελευταία «Με ποινή φυλάκισης και χρηματική ποινή τιμωρείται όποιος, με τον ίδιο σκοπό, προμηθεύεται ή κατέχει το παραποιημένο ή νοθευμένο υλικό μέσο της παρ. 2». Συνεπώς, η παρ. 2Α τιμωρεί με ποινή φυλάκισης και χρηματική ποινή όποιον προμηθεύεται ή κατέχει παραποιημένο ή νοθευμένο υλικό μέσο πληρωμής, με σκοπό να το θέσει σε κυκλοφορία ως γνήσιο[194].

Έτσι, όποιος παραποιεί ή νοθεύει πιστωτικές κάρτες, με σκοπό να τις θέσει σε κυκλοφορία ως γνήσιες, θα τιμωρείται σύμφωνα με την παρ. 2 του 207 ΠΚ, με κάθειρξη έως 10 έτη και χρηματική ποινή, πέραν της πιθανής ποινικής ευθύνης του για απάτη με υπολογιστή -αν πχ αν προβεί σε ανάληψη από ΑΤΜ[195]. Ως μικρότερης απαξίας έγκλημα, αντίθετα, αντιμετωπίζεται η κατοχή ή προμήθεια πλαστών καρτών η οποία θα τιμωρείται σύμφωνα με την παρ. 2Α του 207 ΠΚ.

5.4.2 Η παραποίηση και νόθευση άυλων μέσων πληρωμής (ΠΚ 209)

Με τον ν. 4947/2022 προστέθηκε στον ΠΚ το άρθρο 209 με τίτλο «Παραποίηση και νόθευση άυλων μέσων πληρωμής». Η συγκεκριμένη διάταξη, αφορά στη δόλια πλαστογράφηση ή παραποίηση των άυλων μέσων πληρωμής, καθώς και στην προμήθεια, κατοχή και διάθεση πλαστογραφημένων ή παραποιημένων άυλων μέσων πληρωμής πλην των μετρητών (περ. β΄, γ΄ και δ΄ άρθρου 5 Οδηγίας). Η ρύθμιση αυτή εισήχθη, διότι υπήρχε νομοθετικό κενό ως προς την αντιμετώπιση της συγκεκριμένης εγκληματικής συμπεριφοράς.

5.4.2.1 209 παρ. 1 ΠΚ

[194] Άρθρο 4 περ. γ' και δ' της Οδηγίας (ΕΕ) 2019/713.

[195] Βλ. παραπάνω 4.3.3 και 5.2.5.3.

Η πρώτη παράγραφος του άρθρου 209 παρ. 1 ορίζει ότι «Όποιος παραποιεί ή νοθεύει άυλο μέσο πληρωμής με σκοπό να το θέσει σε κυκλοφορία ως γνήσιο, τιμωρείται με κάθειρξη έως δέκα (10) έτη και χρηματική ποινή». Συνεπώς, θα μπορεί τώρα να τιμωρηθεί, όποιος πλαστογραφεί ή παραποιεί έναν άυλο μηχανισμό, ο οποίος χρησιμεύει στη μεταφορά χρημάτων ή νομισματικής αξίας και προστατεύεται από την απομίμηση ή τη δόλια χρήση. Συνεπώς, όποιος εκδίδει κρυπτοχρήμα με παράνομη διαμόρφωση του προστατευόμενου ψηφιακού μηχανισμού (blockchain) έτσι παραποιεί το προστατευόμενο σύστημα και θα αντιμετωπίζει απειλούμενη ποινή κάθειρξης έως 10 έτη και χρηματική ποινή[196].

Επιπλέον, το άρθρο 209 παρ. 1 ΠΚ προστέθηκε στις αξιόποινες πράξεις του άρθρου 254 ΚΠΔ, για τις οποίες επιτρέπεται η διενέργεια ειδικών ανακριτικών πράξεων. Για τη διενέργεια των συγκεκριμένων ανακριτικών πράξεων, ενόψει της ιδιαιτερότητάς τους, θα πρέπει να τηρούνται οι αυξημένες διατυπώσεις που προβλέπονται στον νέο ΚΠΔ[197].

5.4.2.2 209 παρ. 2 ΠΚ

Την ίδια ποινή -κάθειρξης έως 10 έτη και χρηματική ποινή-, αντιμετωπίζει και όποιος προμηθεύει, κατέχει ή διαθέτει πλαστογραφημένο ή παραποιημένο άυλο μέσο πληρωμής. Έτσι, η προμήθεια, κατοχή ή διάθεση πλαστογραφημένων ή παραποιημένων άυλων μέσων πληρωμής, κρίνεται ίσης βαρύτητας με την πράξη πλαστογράφησης ή παραποίησης, κατά τον ίδιο τρόπο που η κατάρτιση ή νόθευση εγγράφου, τιμωρείται το ίδιο με τη χρήση πλαστού (216 παρ.2).

5.4.2.3 209 παρ. 3 ΠΚ

Αντίθετα, σε ιδιαίτερα ελαφρές περιπτώσεις μικρής αξίας άυλων μέσων πληρωμής, οι πράξεις της πλαστογράφησης ή παραποίησης τιμωρούνται με φυλάκιση έως τρία (3) έτη και οι πράξεις της προμήθειας, κατοχής ή διάθεσης τιμωρούνται με ποινή φυλάκισης έως ένα (1) έτος. Έτσι, στην περίπτωση μικρής αξίας άυλου μέσου πληρωμής, η απλή προμήθεια, κατοχή ή διάθεση, υποβαθμίζεται σε σχέση με την πράξη πλαστογράφησης ή παραποίησης.

---

[196] Α. Χαραλαμπάκης συν. Γ. Μπουρμάς, Οι αλλαγές του νέου ποινικού κώδικα, 2022, σελ. 142.

[197] Αιτιολογική έκθεση του νέου ΚΠΔ, σελ. 76 επ.

5.4.3 Η παράνομη απόκτηση άυλων μέσων πληρωμής (ΠΚ 210)

Ο νόμος 4947/2022 πρόσθεσε νέα διάταξη στον ΠΚ με τίτλο «Παράνομη απόκτηση άυλων μέσων πληρωμής». Σύμφωνα με την τελευταία, ποινικοποιείται η παράνομη απόκτηση άυλων μέσων πληρωμής, ιδίως με τους τρόπους της παράνομης πρόσβασης σε συστήματα πληροφοριών, της παράνομης παρεμβολής σε σύστημα, της παράνομης παρεμβολής σε δεδομένα και της παράνομης υποκλοπής. Το έγκλημα αυτό τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών και χρηματική ποινή.

Η ένταξη του αδικήματος αυτού στο 9ο κεφάλαιο του ΠΚ, σε αντίθεση με το αντίστοιχο του, το οποίο αφορά στα υλικά μέσα πληρωμής και εντάχθηκε στο 23ο κεφάλαιο (άρθρο 394 ΠΚ), έγινε έτσι ώστε να διατηρηθεί η ταυτότητα του νομικού λόγου του τελευταίου (394 ΠΚ), ως αφορώντος ενσώματα αντικείμενα[198].

Για το συγκεκριμένο έγκλημα δημιουργούνται ζητήματα οριοθέτησής του με την απάτη με υπολογιστή του άρθρου 386Α ΠΚ. Η εμπειρία των ηλεκτρονικών συναλλαγών αποδεικνύει ότι κάθε παράνομη απόκτηση άυλου μέσου πληρωμής συνοδεύεται προηγουμένως από απάτη με υπολογιστή. Έτσι, το άρθρο 210 ΠΚ τιμωρεί την πραγμάτωση του σκοπού του δράστη της απάτης με υπολογιστή και η συνταγματικότητα του κρίνεται αμφισβητούμενη[199].

5.4.4 Αποδοχή και διάθεση παρανόμως αποκτηθέντων άυλων μέσων πληρωμής (ΠΚ 210Α)

Το άρθρο 210Α τιμωρεί την αποδοχή και διάθεση παρανόμως αποκτηθέντων άυλων μέσων πληρωμής. Πρόκειται για ενσωμάτωση των περ. γ’ και δ’ άρθρου 5 της Οδηγίας (ΕΕ) 2019/713. Η απειλούμενη ποινή για το έγκλημα αυτό είναι φυλάκιση έως τρία έτη και χρηματική ποινή. Το άρθρο αυτό τελεί κατ’ αντιστοιχία με το άρθρο 394 για την αποδοχή και διάθεση προϊόντων του εγκλήματος, το οποίο έχει και την ίδια απειλούμενη ποινή.

[198] Αιτιολογική έκθεση του ν. 4947/2022, σελ. 9.

[199] Α. Χαραλαμπάκης συν. Γ. Μπουρμάς, Οι αλλαγές του νέου ποινικού κώδικα, 2022, σελ. 136 όπου γίνεται λόγος για διπλή αξιολόγηση της ίδιας δράσης.

5.4.5 Διακεκριμένες περιπτώσεις στο πλαίσιο εγκληματικής οργάνωσης (ΠΚ 210Β)

Με τον ν. 4947/2022 προστέθηκε το άρθρο 210Β ΠΚ, το οποίο προβλέπει στην πρώτη του παράγραφο ότι «η τέλεση των κακουργημάτων των παρ. 1 και 2 του άρθρου 207, του πρώτου εδαφίου της παρ. 1 του άρθρου 208 και της παρ. 1 του άρθρου 209 στο πλαίσιο εγκληματικής οργάνωσης συνιστά επιβαρυντική περίσταση». Πιο συγκεκριμένα, για την εφαρμογή της επιβαρυντικής περίστασης, θα πρέπει η τέλεση των αναφερόμενων κακουργημάτων να εξυπηρετεί τους στόχους της εγκληματικής οργάνωσης[200].

Αυτό το άρθρο προστέθηκε σε συμμόρφωση με το 9 παρ. 6 της Οδηγίας (ΕΕ) 2019/713[201]. Το τελευταίο απαιτεί ποινή στερητική της ελευθερίας με ανώτατο όριο τουλάχιστον πέντε (5) έτη, όταν οι πράξεις των μεταφερθέντων στο εσωτερικό δίκαιο αδικημάτων των άρθρων 3 έως 6 της Οδηγίας τελούνται στο πλαίσιο εγκληματικής οργάνωσης.

5.4.6 Οι προπαρασκευαστικές πράξεις παραχάραξης και πλαστογράφησης (ΠΚ 211)

Το άρθρο 211 τροποποιήθηκε, ώστε να περιληφθούν στο πεδίο εφαρμογής του και οι προπαρασκευαστικές πράξεις για την τέλεση των αδικημάτων 3 έως 6 της Οδηγίας. Το άρθρο 211 ΠΚ ορίζει ότι «Όποιος, προετοιμάζοντας τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 207, 208, 208Α, 208Β, της παρ. 1 του άρθρου 209 και του άρθρου 210, κατασκευάζει, κατέχει ή διαθέτει εργαλείο, αντικείμενο, μηχανισμό ή ψηφιακά δεδομένα ή άλλα μέσα πρωτίστως σχεδιασμένα ή ειδικά προσαρμοσμένα για τον σκοπό αυτόν, καθώς και ολογραφήματα ή λοιπά συστατικά στοιχεία του νομίσματος ή μέσων πληρωμής πλην των μετρητών, τα οποία χρησιμεύουν για την προστασία από την παραχάραξη του νομίσματος ή την παραποίηση και τη νόθευση των μέσων πληρωμής πλην των μετρητών, τιμωρείται με φυλάκιση έως δύο (2) έτη και χρηματική ποινή».

Δεδομένης της μεγάλης προετοιμασίας και της τεχνικής εξειδίκευσης που απαιτείται για να διαπραχθεί ένα έγκλημα σχετικό με τα άυλα μέσα πληρωμής, ο νομοθέτης έκρινε αναγκαία την ποινικοποίηση των πράξεων που πραγματοποιούνται για

[200] Α. Χαραλαμπάκης συν. Γ. Μπουρμάς, Οι αλλαγές του νέου ποινικού κώδικα, 2022, σελ. 155.

[201] Επίσης στο προοίμιο της Οδηγίας (ΕΕ) 2019/713, σκέψη 19, αναφέρεται ότι «Είναι σκόπιμο να προβλέπονται πιο αυστηρές ποινές όταν το έγκλημα διαπράττεται στο πλαίσιο εγκληματικής οργάνωσης, όπως ορίζεται στην απόφαση-πλαίσιο 2008/841/ΔΕΥ του Συμβουλίου».

προπαρασκευή των εγκλημάτων 207 έως 210 ΠΚ. Για την στοιχειοθέτηση του εγκλήματος της ΠΚ 211 δεν αρκεί ο δράστης να κατασκευάζει, κατέχει ή διαθέτει τα αναφερόμενα αντικείμενα, αλλά απαιτείται επιπλέον να προβεί σε πράξη προετοιμασίας τέλεσης για κάποιο από τα εγκλήματα που αναφέρονται[202]. Η πρόβλεψη για την τιμώρηση των προπαρασκευαστικών πράξεων εντοπίζεται και στο το άρθρο 7 της Οδηγίας (ΕΕ) 2019/713. Το τελευταίο ορίζει ότι τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να ποινικοποιηθεί «η διαδικασία παραγωγής, προμήθειας για ιδία χρήση ή για λογαριασμό άλλου, συμπεριλαμβανομένης της εισαγωγής, εξαγωγής, πώλησης, μεταφοράς ή διανομής, ή η διάθεση μηχανισμού ή μέσου, ηλεκτρονικών δεδομένων ή άλλων μέσων πρωτίστως σχεδιασμένων ή ειδικά προσαρμοσμένων για τους σκοπούς της τέλεσης οποιουδήποτε από τα αδικήματα που αναφέρονται στο άρθρο 4 στοιχεία α) και β), στο άρθρο 5 στοιχεία α) και β) ή στο άρθρο 6».

5.4.7 Η εξάλειψη του αξιοποίνου λόγω έμπρακτης μετάνοιας (ΠΚ 212)

Επήλθε μεταβολή στο άρθρο 212 ΠΚ, ώστε να περιλάβει και το άρθρο 209 (παραποίηση και νόθευση άυλων μέσων πληρωμής) στα αδικήματα για τα οποία εξαλείφεται το αξιόποινο σε περίπτωση έμπρακτης μετάνοιας. Έτσι η παρ. 1 του 212 ΠΚ έχει ως εξής «Το αξιόποινο των πράξεων των άρθρων 207, 208, 208Α, 208Β και 209 εξαλείφεται αν ο υπαίτιος με τη θέλησή του και πριν από κάθε κυκλοφορία ακυρώσει ή καταστρέψει τα πλαστά ή καθ' υπέρβαση κατασκευασθέντα πριν εξεταστεί με οποιονδήποτε τρόπο για την πράξη του από τις αρμόδιες αρχές».

Έτσι, προβλέπεται υποχρεωτική εξάλειψη του αξιοποίνου για εκείνον που π.χ. κατασκεύασε πλαστές πιστωτικές κάρτες και τις κατέστρεψε αλλά και για εκείνον που ακυρώσει την επέμβαση-παραποίηση στον άυλο μηχανισμό, ο οποίος χρησιμεύει στη μεταφορά χρημάτων ή νομισματικής αξίας.

[202] Α. Χαραλαμπάκης συν. Γ. Μπουρμάς, Οι αλλαγές του νέου ποινικού κώδικα, 2022, σελ. 156.

5.5 Οι αλλαγές στο 23ο κεφάλαιο του ΠΚ (εγκλήματα κατά περιουσιακών αγαθών)

5.5.1 Η κλοπή και υπεξαίρεση ευτελούς αξίας δεν έχει εφαρμογή στα υλικά μέσα πληρωμής πλην των μετρητών (377 εδ. γ' ΠΚ)

Το πρώτο εδάφιο του άρθρου 377 ΠΚ ορίζει ότι αν η κλοπή ή υπεξαίρεση έχουν αντικείμενο πράγμα μικρής αξίας, τότε επιβάλλεται χρηματική ποινή ή παροχή κοινωφελούς εργασίας. Με τον ν. 4947/2022, προστέθηκε τρίτο εδάφιο στο 377 ΠΚ, σύμφωνα με το οποίο «Το πρώτο εδάφιο δεν εφαρμόζεται σε περίπτωση κλοπής ή υπεξαίρεσης που έχει ως αντικείμενο υλικό μέσο πληρωμής πλην των μετρητών».

Με την προσθήκη αυτή, ο ΠΚ εναρμονίζεται με τις προβλέψεις τις Οδηγίας (ΕΕ) 2019/713. Ειδικότερα, σύμφωνα με το άρθρο 9 παρ. 2 της Οδηγίας[203], τα κράτη μέλη οφείλουν να διασφαλίσουν ότι η κλοπή ή άλλη παράνομη ιδιοποίηση υλικού μέσου πληρωμής πλην των μετρητών[204], τιμωρείται με ποινή φυλάκισης, το ανώτατο όριο της οποίας ανέρχεται τουλάχιστον σε δύο έτη.

Έτσι, δε νοείται η προνομιούχα μορφή «ευτελούς αξίας», όταν πρόκειται για κλοπή ή υπεξαίρεση αντικειμένου που αποτελεί υλικό μέσο πληρωμής πλην των μετρητών. Άρα ο κλέπτης ή υπεξαιρέτης μιας χρεωστικής κάρτας, θα τιμωρείται κανονικά για κλοπή (372 ΠΚ) ή υπεξαίρεση (375 ΠΚ), παρόλο που η κάρτα ως υλικό αντικείμενο είναι κάτι ευτελές.

5.5.2 Η διακεκριμένη περίπτωση της τέλεσης κλοπής ή υπεξαίρεσης υλικών μέσων πληρωμής στο πλαίσιο εγκληματικής οργάνωσης (379Α ΠΚ)

Στον ποινικό κώδικα προστέθηκε με το ν. 4947/2022 το άρθρο 379Α με τίτλο «Διακεκριμένες περιπτώσεις στο πλαίσιο εγκληματικής οργάνωσης». Σύμφωνα με τη νέα διάταξη, τα πλημμελήματα της κλοπής και της υπεξαίρεσης που αφορούν σε υλικά μέσα πληρωμής πλην των μετρητών, καθώς και της φθοράς ψηφιακών δεδομένων, όταν

[203] Το άρθρο 9 παρ. 2 της Οδηγίας (ΕΕ) 2019/713 ορίζει ότι «Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν ότι τα αδικήματα που αναφέρονται στο άρθρο 3, στο άρθρο 4 στοιχεία α) και β) και στο άρθρο 5 στοιχεία α) και β) τιμωρούνται με ποινή φυλάκισης, το ανώτατο όριο της οποίας ανέρχεται τουλάχιστον σε δύο έτη».

[204] Το άρθρο 4 στοιχείο α' της Οδηγίας (ΕΕ) 2019/713 ορίζει ότι «Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν ότι, όταν τελούνται εκ προθέσεως, οι ακόλουθες πράξεις τιμωρούνται ως ποινικά αδικήματα: α) η κλοπή ή άλλη παράνομη ιδιοποίηση υλικού μέσου πληρωμής πλην των μετρητών».

τελούνται στο πλαίσιο εγκληματικής οργάνωσης, τιμωρούνται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή.

Το νέο άρθρο ακολουθεί τους ορισμούς του 9 παρ. 6 της Οδηγίας (ΕΕ) 2019/713, το οποίο προβλέπει ποινή φυλάκισης, το ανώτατο όριο της οποίας ανέρχεται τουλάχιστον σε πέντε έτη, εφόσον τα αδικήματα τελούνται στο πλαίσιο εγκληματικής οργάνωσης κατά την έννοια της απόφασης-πλαίσιο 2008/841/ΔΕΥ.

Η εισαγωγή αυτής της διακεκριμένης περίπτωσης, εξηγείται από την ιδιαίτερη απαξία που αποδίδεται στις κλοπές και τις υπεξαιρέσεις υλικών μέσων πληρωμής, όταν αυτές τελούνται στο πλαίσιο εγκληματικής οργάνωσης. Έτσι, τα μέλη της εγκληματικής οργάνωσης η οποία είχε στόχο τη διάπραξη κλοπών ή υπεξαιρέσεων καρτών, θα τιμωρηθούν με την αυξημένη ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή[205].

5.5.3 Η απάτη με υπολογιστή (386Α ΠΚ)

Παραπάνω, έγινε εκτενής ανάπτυξη σχετικά με το έγκλημα της απάτης με υπολογιστή. Στο σημείο αυτό, θα πρέπει απλά να συνοψίσουμε τις αλλαγές που επήλθαν στο άρθρο 386Α ΠΚ με τον ν. 4947/2022. Συγκεκριμένα στις περ. β', γ', δ' της παρ. 1, οι όροι «λειτουργία προγράμματος» και «δεδομένα υπολογιστή», αντικαταστάθηκαν από τους ευρύτερους «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα», ενώ στην περ. ε' έγινε εννοιολογική διεύρυνση με τη συμπερίληψη της «νομισματικής αξίας», ως στοιχείου της αντικειμενικής υπόστασης. Τέλος, τροποποιήθηκε η παρ. 2 του 386Α ΠΚ, και αντί για τον όρο «σύστημα υπολογιστή», πλέον γίνεται λόγος για «πληροφοριακό σύστημα», καθώς θεωρήθηκε ορθότερη η χρήση του συγκεκριμένου όρου[206].

5.5.4 Η αποδοχή και διάθεση κλεμμένων ή παρανόμως ιδιοποιημένων υλικών μέσων πληρωμής (394 παρ. 4 ΠΚ)

Στο άρθρο 394 προστέθηκε τέταρτη παράγραφος σύμφωνα με την οποία «Όποιος κατέχει κλεμμένο ή παρανόμως ιδιοποιημένο υλικό μέσο πληρωμής πλην των μετρητών, καθώς και όποιος προμηθεύεται ή με οποιονδήποτε άλλον τρόπο ιδιοποιείται κλεμμένο υλικό μέσο πληρωμής πλην των μετρητών, τιμωρείται με φυλάκιση έως τρία (3) έτη και

[205] Με την ίδια ποινή απειλείται ο δράστης της ΠΚ 372 παρ. 1, σε περίπτωση που το αντικείμενο της κλοπής, είναι ιδιαίτερα μεγάλης αξίας.

[206] Αιτιολογική έκθεση του ν. 4947/2022, σελ. 11.

χρηματική ποινή». Με τον τρόπο αυτό τιμωρείται η κατοχή, προμήθεια, ή με οποιονδήποτε άλλο τρόπο ιδιοποίηση κλεμμένου υλικού μέσου πληρωμής πλην των μετρητών[207]. Έτσι, με αυτό το άρθρο θα τιμωρείται όποιος, για παράδειγμα, προμηθεύεται κλεμμένες πιστωτικές κάρτες.

5.5.5 Η διακεκριμένη περίπτωση τέλεσης πλημμελημάτων όταν τελούνται στο πλαίσιο εγκληματικής οργάνωσης (394Α ΠΚ)

5.5.5.1 Η πλημμελληματική απάτη με υπολογιστή που αφορά σε μέσα πληρωμής πλην των μετρητών

Με τον ν. 4947/2022 θεσπίστηκε το νέο άρθρο 394Α ΠΚ, με τίτλο «Διακεκριμένη περίπτωση στο πλαίσιο εγκληματικής οργάνωσης». Σύμφωνα με το τελευταίο, τυποποιείται ως διακεκριμένη περίπτωση η τέλεση των πλημμελημάτων (περ. α' έως ε' της παρ. 1) της απάτης με υπολογιστή που αφορά μέσα πληρωμής πλην των μετρητών, όταν τελείται στο πλαίσιο εγκληματικής οργάνωσης.

Συνεπώς, όποιος επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή που αφορά μέσα πληρωμής πλην των μετρητών, με κάποιον από τους πέντε τρόπους[208] και οι πράξεις αυτές τελούνται στο πλαίσιο εγκληματικής οργάνωσης, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή.

5.5.5.2 Η αποδοχή και διάθεση προϊόντων του εγκλήματος που αφορά σε μέσα πληρωμής πλην των μετρητών

Με την ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή τιμωρείται και όποιος κατέχει κλεμμένο ή παρανόμως ιδιοποιημένο υλικό μέσο πληρωμής πλην των μετρητών, καθώς και όποιος προμηθεύεται ή με οποιονδήποτε άλλον τρόπο ιδιοποιείται

[207] Το άρθρο 4 δ' της Οδηγίας (ΕΕ) 2019/713 ορίζει ότι πρέπει να τιμωρείται ως ποινικό αδίκημα «η προμήθεια για ιδία χρήση ή για λογαριασμό άλλου, συμπεριλαμβανομένης της αποδοχής, ιδιοποίησης, αγοράς, μεταβίβασης, εισαγωγής, εξαγωγής, πώλησης, μεταφοράς ή διανομής κλεμμένου, πλαστού ή παραποιημένου υλικού μέσου πληρωμής πλην των μετρητών για δόλια χρήση».

[208] 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.

κλεμμένο υλικό μέσο πληρωμής πλην των μετρητών, όταν αυτές οι πράξεις τελούνται στο πλαίσιο εγκληματικής οργάνωσης. Π.χ. εγκληματική οργάνωση που προμηθεύεται κλεμμένες πιστωτικές ή χρεωστικές κάρτες.

5.6 Αξιολόγηση των νέων ρυθμίσεων

Οι νέες ρυθμίσεις κινούνται προς τη σωστή κατεύθυνση, διασφαλίζοντας πληρέστερα τις ηλεκτρονικές συναλλαγές. Οι εξελίξεις στο πεδίο των ηλεκτρονικών άυλων περιουσιακών στοιχείων (κρυπτοχρήμα, NFT's), κατέστησαν αναγκαία όσο ποτέ και την ποινική προστασία των άυλων μηχανισμών που χρησιμεύουν για τη διακίνησή τους. Καθώς το μεγαλύτερο μέρος της αξίας αντικατοπτρίζεται πλέον σε ηλεκτρονική μορφή, είναι λογικά αναμενόμενο η προστασία του νομίσματος να έχει διέλθει σε μια νέα εποχή, με τις νέες διατάξεις να προστατεύουν πλέον ηλεκτρονικές νομισματικές αξίες. Κατά τον ίδιο τρόπο που μπορεί κάποιος να θέσει σε κυκλοφορία ένα πλαστό χαρτονόμισμα, μπορεί πλέον να θέσει σε κυκλοφορία ένα πλαστό κρυπτονόμισμα και να θίγει κατά παρόμοιο τρόπο τις συναλλαγές. Είναι επομένως εύστοχη η όμοια ποινική αντιμετώπιση του παραδοσιακού με το νέο αντικείμενο του εγκλήματος. Το νόμισμα «ως επίσημο μέτρο αξίας και μέσο συναλλαγής, το οποίο εξειδικεύεται στην ανταλλασσόμενη σε συγκεκριμένη περίπτωση αξία και εξατομικεύεται σε χαρτονομίσματα ή κέρματα», κατά την παραδοσιακή θεώρηση του Μανωλεδάκη[209], μπορεί να έχει μεταβάλλει τον χαρακτήρα του αλλά η ουσία της ποινικής προστασίας του παραμένει ίδια. Κατά τον τρόπο που το παραδοσιακό νόμισμα εμφανίζεται ως ιδιαίτερα προστατευμένο έγγραφο, αφού η κατασκευή του όσον αφορά τα υλικά και τις μεθόδους γίνεται έτσι ώστε τα σημεία ασφαλείας να εγγυώνται την γνησιότητά του[210], έτσι και οι νέες ηλεκτρονικές μορφές εγγυόνται – ίσως κατά πολύ ασφαλέστερο τρόπο, μέσω της αλυσίδας τμημάτων- τη δική τους γνησιότητα, δυσχεραίνοντας την πλαστοποίηση και καθιστώντας εύκολο τον έλεγχο γνησιότητας[211].

[209] Ι. Μανωλεδάκης, Η διαλεκτική των εννόμων αγαθών, 1973, σελ. 78. Στ. Παύλου, Τα εγκλήματα περί το νόμισμα, 1988, σελ. 42.

[210] Στ. Παύλου, Τα εγκλήματα περί το νόμισμα, 1988, σελ. 64 επ.

[211] Η αλυσίδα τμημάτων (blockchain) αποτελεί μια κατανεμημένη βάση δεδομένων, της οποίας τα τμήματα (blocks), συνδέονται κατά τέτοιο τρόπο, ώστε οποιαδήποτε τροποποίηση, να μεταβάλει τον αριθμό hash του συγκεκριμένου block, δυσχεραίνοντας έτσι οποιαδήποτε απόπειρα πλαστοποίησης της αλυσίδας. Ό.π.

Πάντως, πιο περίπλοκη παραμένει η σχέση του έννομου αγαθού του με αυτό της περιουσίας[212]. Και σε αυτό το σημείο εντοπίζεται και η βασική μας ένσταση για τις νέες ρυθμίσεις, εστιάζοντας στη νέα διάταξη του 210 ΠΚ, που φαίνεται να μην μπορεί να συμβιβάσει τα δύο έννομα αγαθά. Με τη συγκεκριμένη διάταξη, επιχειρήθηκε ποινικοποίηση της παράνομη απόκτηση άυλων μέσων πληρωμής, ιδίως με τους τρόπους της παράνομης πρόσβασης σε συστήματα πληροφοριών, της παράνομης παρεμβολής σε σύστημα, της παράνομης παρεμβολής σε δεδομένα και της παράνομης υποκλοπής.

Για το συγκεκριμένο έγκλημα, φαίνεται να δημιουργούνται ζητήματα οριοθέτησής του με την απάτη με υπολογιστή του άρθρου 386Α ΠΚ, καθώς από την πρακτική των ηλεκτρονικών συναλλαγών, αποδεικνύεται ότι κάθε παράνομη απόκτηση άυλου μέσου πληρωμής συνοδεύεται προηγουμένως από απάτη με υπολογιστή. Το άρθρο 210 ΠΚ καταλήγει, λοιπόν, να τιμωρεί μη σκόπιμα την πραγμάτωση του σκοπού του δράστη της απάτης με υπολογιστή, εγείροντας ζητήματα αντισυνταγματικότητας. Ο υπερτονισμός, έτσι, της λειτουργίας του άυλου μέσου πληρωμής ως φορέα αξίας, πέρα από την προστασία του ως μέσου συναλλαγής[213] φαίνεται να δημιουργεί προβλήματα.

[212] Ό.π. σελ. 70.

[213] «Γι' αυτό και θα πρέπει να αποκρουσθεί η ιστορικά παρωχημένη άλλωστε άποψη, ότι το νόμισμα προστατεύεται, διότι μέσω της πλαστοποιήσεώς του μπορεί ή καλύτερα επιδιώκει κανείς, να φθάσει σε προσβολή της περιουσίας, διότι έτσι θα αυτονομούσαμε και θα υπερτονίζαμε τη λειτουργία του νομίσματος ως φορέα αξίας από την λειτουργία του ως μέσου συναλλαγής» Ό.π. σελ. 73.

6 Η απάτη στις ηλεκτρονικές συναλλαγές και νέες μορφές απάτης στο πεδίο της ηλεκτρονικής εγκληματικότητας

6.1 Η απάτη στις ηλεκτρονικές συναλλαγές με τη χρήση πιστωτικής ή χρεωστικής κάρτας

Το α' εξάμηνο του 2022, ο αριθμός των περιστατικών απάτης που καταγράφηκε στις πληρωμές μέσω POS, ανήλθε σε 17.000[214]. Κατά το αντίστοιχο εξάμηνο του 2021, ο αριθμός διαμορφωνόταν σε 11.600[215]. Αυτή η μορφή απάτης στις συναλλαγές τελείται κατά βάση με τη χωρίς δικαίωμα εισαγωγή της κάρτας και του PIN της στο τερματικό μηχάνημα, η οποία θα συνεπάγεται περιουσιακή ζημία για τον πραγματικό δικαιούχο και κατ' επέκταση απάτη με υπολογιστή (386Α ΠΚ)[216].

Βέβαια, η ραγδαία αύξηση της απάτης με POS, δικαιολογείται και από την υιοθέτηση των ανέπαφων πληρωμών από την πλειοψηφία των συναλλασσομένων με πλαστικό χρήμα. Ως ανέπαφη πληρωμή με τη χρήση χρεωστικών ή πιστωτικών καρτών, νοείται η απλή προσέγγιση στο τερματικό μηχάνημα, χωρίς την ανάγκη εισαγωγής της κάρτας και του αριθμού PIN της. Κατ' αυτό τον τρόπο η καθημερινότητα των χρηστών γίνεται ευκολότερη, καθώς μπορούν να εκτελέσουν πληρωμές παρακάμπτοντας την εισαγωγή της κάρτας και του PIN της, πλην όμως γίνεται ευκολότερη η απάτη στις συναλλαγές αυτές.

Αυτό συμβαίνει όταν, τρίτοι μη νομιμοποιούμενοι χρήστες, αποσπούν πιστωτικές ή χρωστικές κάρτες και προβαίνουν σε πληρωμές με POS. Χωρίς δηλαδή να είναι δικαιούχοι, προσεγγίζουν τις κάρτες στα τερματικά POS και έτσι δηλώνουν ψευδώς ότι νομιμοποιούνται στην εκτέλεση της εκάστοτε συναλλαγής. Έτσι, έστω και ανέπαφα, εισάγονται δεδομένα χωρίς δικαίωμα στο POS και άρα τελείται απάτη με υπολογιστή (386Α ΠΚ).

---

[214] Έκθεση χρηματοπιστωτικής σταθερότητας της Τράπεζας της Ελλάδος, Νοέμβριος 2022, σελ. 97. Σύμφωνα με την έκθεση Μαΐου 2022, σελ. 114 «Οι οικονομικές ζημίες που καταγράφηκαν στις συναλλαγές απάτης με κάρτες πληρωμών ανήλθαν σε 13,4 εκατ. ευρώ το 2021, αυξημένες κατά 4% συγκριτικά με το 2020 και κατά 23% σε σχέση με το 2019».

[215] Έκθεση χρηματοπιστωτικής σταθερότητας της Τράπεζας της Ελλάδος, Δεκέμβριος 2021, σελ. 74.

[216] Η ΑΠ 734/2021 έκρινε περίπτωση απάτης με υπολογιστή «εφόσον, με τις συσκευές POS που παραπάνω αναφέρονται έγινε με τη μέθοδο της "τοπικής" συναλλαγής και με την πληκτρολόγηση αυθαίρετων κωδικών παράκαμψη του αυτοματοποιημένου συστήματος».

6.2 Η απάτη στις ανέπαφες συναλλαγές με τη χρήση smartphone

Είναι χαρακτηριστικό ότι ένα μεγάλο μέρος των πληρωμών, πραγματοποιούνται με την ανέπαφη προσέγγιση του κινητού τηλεφώνου στο POS, χωρίς την παρουσία κάρτας. Η τεχνολογία που χρησιμοποιούν τα έξυπνα τηλέφωνα για την επίτευξη της συναλλαγής ονομάζεται NFC (Near Field Communication – επικοινωνία κοντινού πεδίου), ενώ πολλές φορές η πληρωμή συνοδεύεται από τη βιομετρική αναγνώριση του χρήστη (αναγνώριση προσώπου ή δακτυλικών αποτυπωμάτων). Τα βιομετρικά, δε, στοιχεία διακρίνονται σε βιολογικά και συμπεριφορικά[217]. Τα πρώτα ονομάζονται και στατικά διότι ο χρήστης εισάγει στο σύστημα ένα σταθερό και αμετάβλητο βιομετρικό δείκτη (π.χ. ίριδα του ματιού), ενώ τα δεύτερα λέγονται και δυναμικά διότι το δείγμα μπορεί να αλλάζει κάθε φορά (π.χ. υπογραφή, βηματισμός, φωνή)[218]. Έτσι, οι ανέπαφες πληρωμές μέσω smartphone γίνονται ακόμα πιο ασφαλείς, σε σύγκριση με τις πλαστικές κάρτες. Και πάλι, βέβαια, δεν μπορεί να αποκλειστεί η τέλεση της απάτης με υπολογιστή (386Α ΠΚ) από τρίτο μη νομιμοποιούμενο χρήστη ο οποίος χρησιμοποιεί ξένο κινητό τηλέφωνο. Τούτο θα προϋποθέτει και την προσπέλαση των τεχνολογικών εμποδίων που τυχόν το κινητό τηλέφωνο περιλαμβάνει π.χ. εισαγωγή κωδικού για την εκτέλεση της συναλλαγής[219].

6.3 Η απάτη στις εξ' αποστάσεως συναλλαγές

Το υψηλότερο ποσοστό απάτης, εντοπίζεται στις εξ' αποστάσεως συναλλαγές, οι οποίες εκτελούνται χωρίς τη φυσική παρουσία κάρτας (card not present – CNP). Ειδικότερα, το α' εξάμηνο του 2022, ο αριθμός περιστατικών απάτης χωρίς τη φυσική παρουσία κάρτας ανήλθε σε 117.000. Τα περιστατικά αυτά είναι πολύ περισσότερα τόσο σε σύγκριση με τις απάτες στα ATM (1.476) όσο και στα POS (17.000)[220]. Ιδιαίτερη, δε σημασία, δεν έχει μόνο ο αριθμός των περιστατικών απάτης, αλλά και η αξία που αυτά

[217] Ε. Μπακιρλή, Σύγχρονη Τεχνολογία και Αντεγκληματική Πολιτική, 2019, σελ. 25.

[218] Τα βιομετρικά στοιχεία διακρίνονται στα βιολογικά τα οποία ονομάζονται και στατικά διότι ο χρήστης εισάγει στο σύστημα ένα σταθερό και αμετάβλητο βιομετρικό δείκτη.

[219] Ι. Μοροζίνης σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, 2023, σελ. 144. Αφού κατά τη βούληση του ιστορικού νομοθέτη οποιαδήποτε μεταφορά χρημάτων γίνεται με υποκλοπή και εισαγωγή ξένων ορθών κωδικών συνιστά απάτη με υπολογιστή.

[220] Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος, Νοέμβριος 2022, σελ. 97, 98.

αντικατοπτρίζουν. Συγκεκριμένα, η αξία των περιστατικών απάτης στις εξ' αποστάσεως συναλλαγές, ήταν 5 εκατομμύρια ευρώ μόνο για το πρώτο εξάμηνο του 2022[221].

Τα συγκεκριμένα περιστατικά απάτης, αφορούν κυρίως διαδικτυακές συναλλαγές με εμπόρους του εξωτερικού, με κάρτες που έχουν εκδοθεί στην Ελλάδα. Τα υψηλότερα ποσοστά απάτης στις διασυνοριακές συναλλαγές μέσω διαδικτύου, οφείλονται κυρίως στην πιο περιορισμένη χρήση του διεθνούς προτύπου συναλλαγών 3D Secure στο εξωτερικό, σε σύγκριση με την Ελλάδα[222]. Το 3D Secure αποτελεί πρότυπο ασφαλείας, το οποίο απαιτεί από τον χρήστη της κάρτας να εισάγει έναν ειδικό κωδικό, προκειμένου να επαληθεύσει ότι είναι νόμιμος κάτοχός της[223].

Με τον ν. 4537/2018, ενσωματώθηκε στο εθνικό μας δίκαιο, η Οδηγία (ΕΕ) 2015/2366 «για τις υπηρεσίες πληρωμών στην εσωτερική αγορά», η οποία μεταξύ άλλων επιδιώκει την ενίσχυση της ασφάλειας στις συναλλαγές[224]. Σύμφωνα με το άρθρο 97 της Οδηγίας (ΕΕ) 2015/2366, «τα κράτη μέλη πρέπει να διασφαλίζουν ότι ένας πάροχος υπηρεσιών πληρωμών εφαρμόζει αυστηρή εξακρίβωση της ταυτότητας του πελάτη»[225]. Ειδικότερα, η παρ. 2 του άρθρου 96 του ν. 4537/2018 ορίζει για τις ηλεκτρονικές πράξεις πληρωμής που διενεργούνται εξ αποστάσεως ότι, «οι πάροχοι υπηρεσιών πληρωμών εφαρμόζουν ισχυρή ταυτοποίηση πελάτη, η οποία περιλαμβάνει στοιχεία που συνδέουν δυναμικά τη συναλλαγή με συγκεκριμένο ποσό και συγκεκριμένο δικαιούχο».

Έτσι, απαιτείται πλέον ισχυρή ταυτοποίηση[226] για τους χρήστες, σύμφωνα με την οποία θα πρέπει να πιστοποιούνται δύο ή περισσότερα στοιχεία, από κάτι που ξέρουν

---

[221] Αντίθετα η αξία των περιστατικών απάτης με ΑΤΜ ήταν 679.000 ευρώ και με POS 490.000 ευρώ.

[222] Ό.π.

[223] Για τη λειτουργία του πρωτοκόλλου 3D Secure βλ. Σ. Συρμακέζη, Το δίκαιο στην ψηφιακή εποχή, 2012, σελ. 116 - 117.

[224] Αιτιολογικές σκέψεις 91 έως 96 της Οδηγίας (ΕΕ) 2015/2366.

[225] Άρθρο 97 παρ. 1 της Οδηγίας (ΕΕ) 2015/2366: «Τα κράτη μέλη διασφαλίζουν ότι ένας πάροχος υπηρεσιών πληρωμών εφαρμόζει αυστηρή εξακρίβωση της ταυτότητας του πελάτη, όταν ο πληρωτής: α)έχει πρόσβαση στον λογαριασμό πληρωμών του διαδικτυακά, β) διενεργεί την έναρξη πράξης πληρωμής ηλεκτρονικά, γ)εκτελεί οιαδήποτε ενέργεια, μέσω εξ αποστάσεως διαύλου, η οποία μπορεί να ενέχει κίνδυνο απάτης στον τομέα των πληρωμών ή άλλων παραβιάσεων».

[226] Ως «ισχυρή ταυτοποίηση», σύμφωνα με το στοιχείο 30 του άρθρου 4 του ν. 4537/2018, νοείται «η ταυτοποίηση με βάση τη χρήση δύο ή περισσότερων στοιχείων που αφορούν γνώση (στοιχείο το οποίο μόνο ο χρήστης υπηρεσίας πληρωμών γνωρίζει), κατοχή (στοιχείο το οποίο μόνο ο χρήστης κατέχει) και κάποιο μοναδικό εγγενές χαρακτηριστικό του (στοιχείο το οποίο ο χρήστης είναι), στοιχεία τα οποία είναι ανεξάρτητα μεταξύ τους, ως προς το ότι η παραβίαση του ενός δεν θέτει σε κίνδυνο την αξιοπιστία των

(PIN, κωδικός κλπ.), κάτι που έχουν (π.χ. υπολογιστής, κινητό) και κάτι που είναι (βιομετρική αναγνώριση προσώπου, αποτυπωμάτων, φωνής κ.α.). Κατ' αυτό τον τρόπο υιοθετήθηκε πλέον το πρωτόκολλο 3D Secure 2, το οποίο υποστηρίζει την αποστολή πλήθους σημαντικών δεδομένων (διεύθυνση, πληροφορίες συσκευής, ιστορικό συναλλαγών), τα οποία αξιολογεί η τράπεζα για να εγκρίνει την συναλλαγή.

Συχνή περίπτωση, αποτελεί η δημιουργία απατηλών ιστοσελίδων ηλεκτρονικού εμπορίου, οι οποίες διαθέτουν προϊόντα σε ιδιαίτερα ανταγωνιστικές τιμές. Οι χρήστες πραγματοποιούν πληρωμή στον έμπορο, όμως τα προϊόντα δεν υπάρχουν και άρα ουδέποτε αποστέλλονται. Η συγκεκριμένη μορφή απάτης αποτελεί κοινή απάτη (386 ΠΚ), αφού οι δράστες πείθουν τα θύματα ότι είναι φερέγγυοι έμποροι και μπορούν να διαθέσουν τα εκάστοτε εμπορεύματα. Αυτά τα γεγονότα που δεν ανταποκρίνονται στην πραγματικότητα, ενώ λαμβάνοντας τα ποσά βλάπτουν την περιουσία των θυμάτων. Τέτοιας μορφής απάτη μπορεί να αποφευχθεί με αναζήτηση πληροφοριών και κριτικών για το συγκεκριμένο κατάστημα. Ακόμα, από τις ύποπτες ιστοσελίδες απουσιάζουν συνήθως βασικά στοιχεία (έδρα, αριθμός Γ.Ε.ΜΗ[227] κλπ).

6.4 Phishing

Το phishing αποτελεί μία σύγχρονη μορφή εγκληματικής δράσης μέσω διαδικτύου, κατά την οποία αποστέλλονται -μαζικά συνήθως- e-mails[228], με στόχο να πειστούν τα πιθανά θύματα να αποκαλύψουν ευαίσθητες πληροφορίες, όπως στοιχεία δεδομένων ταυτότητας, τραπεζικά δεδομένα ή στοιχεία πιστωτικών καρτών. Η πρακτική αυτή στηρίζεται στη λογική των πιθανοτήτων, ότι κάποια έστω από τα χιλιάδες υποψήφια θύματα στα οποία έχει αποσταλεί το σχετικό παραπλανητικό μήνυμα, θα πειστούν να παραδώσουν στους δράστες τα προσωπικά τους στοιχεία[229]. Αν δε, το θύμα πειστεί να

υπολοίπων και η διαδικασία της οποίας είναι σχεδιασμένη κατά τρόπο που να προστατεύεται η εμπιστευτικότητα των δεδομένων ταυτοποίησης».

[227] Ο αριθμός Γ.Ε.ΜΗ πρέπει να αναγράφεται υποχρεωτικά στα ηλεκτρονικά καταστήματα δυνάμει της παρ. 3 του ν. 4919/2022.

[228] Cybercrime and Society, M. Yar, 2013, σελ. 86.

[229] Συνήθως, οι δράστες επιδιώκουν την εκμετάλλευση του θυμικού, ώστε τα παραπλανητικά μηνύματα να δημιουργούν έντονα συναισθήματα στα υποψήφια θύματα. Δεν είναι τυχαίο ότι τα μηνύματα αυτά, εστιάζουν στη δημιουργία χαράς ή φόβου. Κλασική περίπτωση κατά την οποία δημιουργούνται έντονα συναισθήματα, αποτελεί η λεγόμενη «Νιγηριανή απάτη» και οι παραλλαγές της. Σύμφωνα με αυτή, το θύμα επιλέχθηκε από κάποιον αξιωματούχο, που χρειάζεται βοήθειά του, για τη μεταφορά ενός μεγάλου ποσού.

καταβάλλει κατευθείαν ποσά στον δράστη εξαιτίας της παραπλάνησης του, τότε στοιχειοθετείται κοινή απάτη 386 ΠΚ.

Σε μια πιο σύνθετη μορφή, αποστέλλεται μήνυμα ηλεκτρονικού ταχυδρομείου στο οποίο εμφανίζεται ως αποστολέας ένα τραπεζικό ίδρυμα και περιέχει τα αυθεντικά λογότυπά του. Το μήνυμα αναφέρει ότι υπάρχει κάποιο πρόβλημα (π.χ. «κλειδώθηκε η κάρτα σας») και ζητείται από το θύμα να διευθετήσει το ζήτημα «κάνοντας κλικ» σε κάποιον σύνδεσμο.

Ο σύνδεσμος αυτός ανακατευθύνει σε μια ιστοσελίδα που ομοιάζει με το περιβάλλον ηλεκτρονικής τραπεζικής συγκεκριμένης τράπεζας. Ο χρήστης πείθεται ότι η τράπεζα απαιτεί τα προσωπικά στοιχεία του (username, password) και τα εισάγει στο πλαστό περιβάλλον που δημιούργησε ο δράστης. Εάν δε, ο δράστης χρησιμοποιεί τεχνικές ανακατεύθυνσης στην πλαστή ιστοσελίδα με DNS poisoning, τότε το phishing συνδυάζεται και με pharming[230].

Με την εισαγωγή τους, τα στοιχεία περιέρχονται στην κατοχή του δράστη και εκείνος τα εισάγει στην πραγματική πλατφόρμα e-banking για να αποσπάσει χρηματικά

Έτσι, του υπόσχονται μεγάλο μέρος του συγκεκριμένου ποσού, με αντάλλαγμα τα τραπεζικά του στοιχεία ή και την καταβολή ποσών στον αξιωματούχο που χρειάζεται προσωρινά βοήθεια. Ο χρήστης δίδει τα προσωπικά του στοιχεία ή και καταβάλλει χρηματικά ποσά, ενώ ποτέ δεν λαμβάνει το αντάλλαγμα που περιμένει.

Άλλη περίπτωση, η οποία όμως δημιουργεί συναισθήματα φόβου, αποτελεί η αποστολή μηνύματος «από τον Αρχηγό της αστυνομίας», που ενημερώνει τον αποδέκτη ότι είναι ένοχος εγκλημάτων και ότι αν δεν καταβάλει τα χρήματα που απαιτούνται, θα συλληφθεί άμεσα. Τέλος, τον ψυχικό κόσμο του θύματος εκμεταλλεύονται οι «ρομαντικές απάτες», στις οποίες ο δράστης επενδύει στο συναισθηματικό δέσιμο μέσω διαδικτύου, ώστε να απαιτεί από το θύμα χρήματα για τη στήριξή του, για την αγορά δώρων για τον επικείμενο αρραβώνα κλπ.

[230] Για την στοιχειοθέτηση του εγκλήματος της πλαστογραφίας σε αυτή την περίπτωση βλ. Γ. Δανιήλ σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, 2023, σελ. 97. Φ. Σπυρόπουλος, Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών, 2016, σελ. 106 «τα δεδομένα τα οποία πληκτρολογεί και καταχωρεί ο χρήστης στην ψεύτικη σελίδα να γίνονται γνωστά στον hacker -άρα, τελικώς μπορεί να υποστηριχθεί ότι το phishing είναι η ολοκλήρωση του pharming». Ε. Μεταξάκης, Κυβερνοέγκλημα, σελ. 379.

ποσά[231]. Έτσι, τελεί και το έγκλημα της 386Α παρ. 1 ε' του ΠΚ «με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων»[232].

Εξελιγμένη και πιο περίπλοκη μορφή του phishing, αποτελεί το «spear phishing». Το τελευταίο στοχεύει σε συγκεκριμένους οργανισμούς ή άτομα επιδιώκοντας την εξουσιοδοτημένη πρόσβαση σε εμπιστευτικά δεδομένα. Η διαφορά με το phishing, έγκειται στο ότι οι επιθέσεις είναι εξατομικευμένες και ότι γίνεται χρήση εξελιγμένων τακτικών πλαστοπροσωπίας του αποστολέα[233].

6.5 Η νέα ρύθμιση για τον περιορισμό της ευθύνης του πληρωτή για μη εγκεκριμένες πράξεις πληρωμής (phishing)

6.5.1 Η εισαγωγή της νέας ρύθμισης – αιτιολογικές σκέψεις

Οι καταναλωτές υφίστανται τη μεγαλύτερη επιβάρυνση από τα περιστατικά απάτης στις ηλεκτρονικές συναλλαγές. Τούτο δεν καθορίζεται μόνο, λόγω των ποσοστών επιμερισμού της ζημίας (το β' εξάμηνο του 2021 το 54% των ζημιών επιβάρυνε τους κατόχους των καρτών), αλλά κυρίως, λόγω της περιορισμένης οικονομικής ισχύος τους.

Σύμφωνα με το άρθρο 22 του σχεδίου νόμου «για την ενσωμάτωση της Οδηγίας (ΕΕ) 2020/1828», εισάγεται ρύθμιση με την οποία περιορίζεται, υπό προϋποθέσεις, η ευθύνη του καταναλωτή σε περιπτώσεις phishing, στο ποσό των €1.000, ακόμη και σε περιπτώσεις βαριάς αμέλειας. Σκοπός της νέας προσθήκης είναι η προστασία του καταναλωτή για περιπτώσεις «phishing», δηλαδή πρακτικών εξαπάτησης (με πλαστές ιστοσελίδες, ηλεκτρονικά μηνύματα ή ειδοποιήσεις), με τις οποίες οι δράστες πληροφορούνται ή υφαρπάζουν τους μυστικούς κωδικούς («PIN», «TAN») των καταναλωτών για διαδικτυακές συναλλαγές και μεταφορές χρημάτων[234].

---

[231] Ό.π. σελ. 102 αναφέρει ότι πρόκειται για αλίευση στοιχείων που στη συνέχεια θα χρησιμοποιηθούν για τη χωρίς δικαίωμα πρόσβαση σε δεδομένα.

[232] Αν δε, η πραγματική πλατφόρμα απαιτεί κωδικό μιας χρήσης (OTP – one time password), τότε η πλαστή πλατφόρμα μπορεί να περιέχει και πεδίο εισαγωγής για τον κωδικό αυτό, τον οποίο πληροφορείται ο δράστης. Για τη χωρίς δικαίωμα χρήση συστημάτων πληρωμών στο internet βλ. Γ. Νούσκαλη σε ΠοινΔικ 2/2003, σελ. 184.

[233] Αυτό τον ορισμό, δίνει ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια.

[234] Ανάλυση συνεπειών ρύθμισης για την ενσωμάτωση της Οδηγίας (ΕΕ) 2020/1828 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2020 «σχετικά με τις αντιπροσωπευτικές αγωγές για την προστασία των συλλογικών συμφερόντων των καταναλωτών και για την κατάργηση της Οδηγίας

Ταυτόχρονα, γίνεται χρήση της ευχέρειας που παρέχει η Οδηγία (ΕΕ)[235] 2015/2366 σχετικά με τις υπηρεσίες πληρωμών στην εσωτερική αγορά (PSD2), για εισαγωγή νομοθετικού περιορισμού - ορίου ευθύνης του πληρωτή, όταν δεν υφίσταται δόλος/πρόθεση. Ο εν λόγω περιορισμός, ο οποίος δεν εισήχθη με τον ν. 4537/2018, κρίθηκε πλέον αναγκαίος, καθότι το καταναλωτικό κοινό δεν μπορεί να μένει απροστάτευτο ενώ επεκτείνονται τα περιστατικά phishing.

6.5.2 Το άρθρο 74 του ν. 4537/2018

Σύμφωνα με το άρθρο 74 του ν. 4537/2018[236], «Κατά παρέκκλιση από το άρθρο 73, ο πληρωτής ευθύνεται μέχρι του ανώτατου ποσού των πενήντα (50) ευρώ για τις ζημίες από τη διενέργεια μη εγκεκριμένων πράξεων πληρωμής, οι οποίες προκύπτουν είτε από τη χρήση απολεσθέντος ή κλαπέντος μέσου πληρωμών είτε από υπεξαίρεσή του». Συνεπώς, σε περίπτωση απώλειας, κλοπής ή υπεξαίρεσης κάρτας πληρωμών και πραγματοποίησης μη εγκεκριμένων συναλλαγών με αυτές, ο νόμιμος δικαιούχος ευθύνεται μέχρι το ποσό των 50 ευρώ[237].

Σύμφωνα με το ίδιο άρθρο, η ευθύνη του πληρωτή δεν υπάρχει εφόσον: «α) η απώλεια, κλοπή ή υπεξαίρεση του μέσου πληρωμών δεν ήταν δυνατό να εντοπιστεί από τον πληρωτή πριν από τη διενέργεια πράξης πληρωμής, εκτός αν ο πληρωτής είχε ενεργήσει με δόλο ή β) η ζημία είχε προκληθεί από πράξεις ή παραλείψεις υπαλλήλου, αντιπροσώπου ή υποκαταστήματος ενός παρόχου υπηρεσιών πληρωμών ή οντότητας στην οποία ο πάροχος υπηρεσιών πληρωμών είχε αναθέσει τις δραστηριότητές του». Αυτές οι δύο εξαιρέσεις από την ευθύνη του πληρωτή είναι εύλογες και εναρμονίζονται

2009/22/ΕΚ», ενίσχυση της προστασίας των καταναλωτών, ρυθμιστικό πλαίσιο για την παλαίωση οίνων και άλλες επείγουσες διατάξεις για την ενίσχυση της ανάπτυξης, σελ. 10.

[235] Η Οδηγία (ΕΕ) 2015/2366, παρέχει σημαντική προστασία στους καταναλωτές σε περίπτωση απάτης που σχετίζεται με υπηρεσίες πληρωμών, όμως διακρίνεται και από κάποιες αδυναμίες. Για παράδειγμα δεν οριοθετείται σαφώς η «βαριά αμέλεια», αλλά γίνεται απλή αναφορά ότι «νοείται ως κάτι βαρύτερο από την απλή αμέλεια», αφήνοντας την αξιολόγηση της στη βάση του εθνικού δικαίου. Επίσης δεν καλύπτονται οι διαδικασίες ανάκτησης κεφαλαίων. Εντούτοις, σε καμία περίπτωση δεν θα πρέπει να παραγνωρίζεται η αξία της Οδηγίας, ακόμα και με τις παραλείψεις της.

[236] Τα ίδια αναφέρει το άρθρο 74 της Οδηγίας (ΕΕ) 2015/2366.

[237] Σύμφωνα με τη αιτιολογική σκέψη 71 της Οδηγίας (ΕΕ) 2015/2366, το ποσό των 50 ευρώ, λειτουργεί ως κίνητρο στον χρήστη των υπηρεσιών, ώστε να ειδοποιεί έγκαιρα τον πάροχο για τυχόν κλοπή ή απώλεια του μέσου πληρωμών.

με τη γενική αρχή του δικαίου, ότι κανείς δεν υποχρεούται στα αδύνατα. Αν για παράδειγμα η αφαίρεση/υπεξαίρεση του μέσου πληρωμής έγινε με τρόπο που δεν μπορούσε να γίνει αντιληπτός από τον πληρωτή ή αν ακόμα εμπλέκεται προστηθείς της τράπεζας, τότε δεν μπορεί να θεμελιώνεται καμία ευθύνη του.

Το άρθρο συνεχίζει αναφέροντας ότι «Ο πληρωτής ευθύνεται για όλες τις ζημίες που σχετίζονται με κάθε μη εγκεκριμένη πράξη πληρωμής, εφόσον οι ζημίες αυτές οφείλονται είτε σε δόλο είτε στη μη τήρηση μιας ή περισσοτέρων από τις υποχρεώσεις που έχει, σύμφωνα με το άρθρο 69, από πρόθεση ή βαριά αμέλεια[238]. Στις περιπτώσεις αυτές, δεν ισχύει το ανώτατο ποσό που αναφέρεται στο πρώτο εδάφιο της παρούσας παραγράφου». Συνεπώς, ο πληρωτής ευθύνεται απεριόριστα αν δεν χρησιμοποιεί το μέσο πληρωμών σύμφωνα με τους όρους που διέπουν την έκδοση και τη χρήση του (π.χ. αν μόλις παραλάβει την κάρτα, δε λάβει κάθε εύλογο μέτρο για την ασφαλή φύλαξη του PIN της). Ευθύνεται επίσης, εάν δεν ειδοποιεί έγκαιρα τον πάροχο υπηρεσιών πληρωμών ή τον φορέα που ο τελευταίος ορίζει, μόλις αντιληφθεί απώλεια, κλοπή, υπεξαίρεση του μέσου πληρωμών ή μη εγκεκριμένη χρήση του (άρθρο 69).

6.5.3 Η απαλλαγή του καταναλωτή για ζημίες άνω των χιλίων ευρώ

Η κρίσιμη ρύθμιση που προστέθηκε στο εδάφιο δ' της παρ. 1 του άρθρου 74 του ν. 4537/2018 έχει ως εξής: «Αν ο πληρωτής είναι καταναλωτής και εφόσον οι ζημιές οφείλονται σε βαριά αμέλεια, ευθύνεται μέχρι του ανώτατου ποσού των χιλίων (1.000) ευρώ, λαμβάνοντας υπόψη ιδίως τη φύση των εξατομικευμένων διαπιστευτηρίων ασφαλείας και τις ειδικότερες περιστάσεις υπό τις οποίες το μέσο πληρωμής απωλέσθη, εκλάπη ή υπεξαιρέθηκε».

Για την εφαρμογή αυτού του εδαφίου απαιτείται ο πληρωτής να είναι καταναλωτής. Σύμφωνα δε, με το στοιχείο 20 του άρθρου 4 του ν. 4537/2018, ως καταναλωτής νοείται «το φυσικό πρόσωπο που δεν ενεργεί για εμπορικούς,

[238] Αιτ. σκέψη 72 «Για να εκτιμηθεί αν υπάρχει αμέλεια ή βαριά αμέλεια του χρήστη υπηρεσιών πληρωμών, θα πρέπει να λαμβάνονται υπόψη όλες οι περιστάσεις. Τα αποδεικτικά στοιχεία και ο βαθμός της καταγγελλόμενης αμέλειας θα πρέπει να αξιολογούνται βάσει του εθνικού δικαίου. Ωστόσο, ενώ η έννοια της αμέλειας συνεπάγεται παράβαση του καθήκοντος επιμέλειας, με τον όρο βαριά αμέλεια θα πρέπει να νοείται κάτι βαρύτερο από την απλή αμέλεια, που θα αφορά μορφές συμπεριφοράς που παρουσιάζουν σημαντικό βαθμό έλλειψης επιμέλειας, παραδείγματος χάριν η περίπτωση όπου τα διαπιστευτήρια που χρησιμοποιούνται για την έγκριση πράξης πληρωμής φυλάσσονται δίπλα στο μέσο πληρωμής κατά τρόπο ανοικτό και ευχερώς ανιχνεύσιμο από τρίτους».

επιχειρηματικούς ή επαγγελματικούς σκοπούς, όσον αφορά συμβάσεις υπηρεσιών πληρωμών που καλύπτονται από τον παρόντα νόμο». Συνεπώς, αυτή η πρόβλεψη αφορά φυσικά πρόσωπα και δη αυτά να μην ενεργούν για επαγγελματικούς σκοπούς[239].

Μολαταύτα, στο άρθρο 61 του ν. 4537/2018 ορίζεται ότι «όταν ο χρήστης υπηρεσιών πληρωμών δεν είναι καταναλωτής, ο χρήστης υπηρεσιών πληρωμών και ο πάροχος υπηρεσιών πληρωμών μπορεί να συμφωνούν ότι δεν εφαρμόζεται εν όλω ή εν μέρει -μεταξύ άλλων- το άρθρο 74». Συνεπώς οι τράπεζες μπορούν με όρο να αποκλείουν την εφαρμογή του άρθρου 74 σε όσους δεν είναι καταναλωτές.

Βέβαια, δεν θα μπορούν να αποκλείσουν την εφαρμογή του άρθρου 74 στις πολύ μικρές επιχειρήσεις, καθώς, στον παρόντα τουλάχιστον χρόνο, τα άρθρα 61 έως 101, εκτός από το άρθρο 100, εφαρμόζονται στις πολύ μικρές επιχειρήσεις κατά τον ίδιο τρόπο, όπως στους καταναλωτές[240]. Ως μικρή επιχείρηση νοείται[241] «η επιχείρηση η οποία, κατά τη στιγμή της σύναψης της σύμβασης παροχής υπηρεσιών πληρωμών, εμπίπτει στην έννοια του άρθρου 2 παρ. 9 του ν. 2251/1994»[242]. Για να εμπίπτει δε, στην έννοια αυτή, θα πρέπει η επιχείρηση να πληροί σωρευτικά τις εξής προϋποθέσεις: α) η σύμβασή της να περιλαμβάνει όρους που δεν αποτέλεσαν αντικείμενο ατομικής διαπραγμάτευσης μεταξύ των μερών, β) να πληροί τα κριτήρια της «πολύ μικρής επιχείρησης», σύμφωνα με το άρθρο 2 παρ. 2 του ν. 4308/2014[243] και γ) να είναι τελικός αποδέκτες των παρεχόμενων

[239] Σύμφωνα με το άρθρο 1α παρ. 1 του ν. 2251/1994, όπως αυτό ισχύει με το ν. 4967/2022, «καταναλωτής είναι κάθε φυσικό πρόσωπο το οποίο ενεργεί για λόγους οι οποίοι δεν εμπίπτουν στην εμπορική, επιχειρηματική, βιοτεχνική ή ελευθέρια επαγγελματική δραστηριότητα».

[240] Η πρόβλεψη εφαρμογής και για τις μικρές επιχειρήσεις αποτελεί ευχέρεια που δίνει η Οδηγία (ΕΕ) 2015/2366 στην παρ. 3 του άρθρου 61 « Τα κράτη μέλη μπορούν να ορίζουν ότι οι διατάξεις του παρόντος τίτλου εφαρμόζονται στις πολύ μικρές επιχειρήσεις κατά τον ίδιο τρόπο όπως και στους καταναλωτές».

[241] Σύμφωνα με το στοιχείο 36 του άρθρου 4 του ν. 4537/2018.

[242] Το άρθρο 2 παρ. 9 του ν. 2251/1994, εισάγει εξαίρεση που αφορά στον έλεγχο των Γενικών Όρων Συναλλαγών (Γ.Ο.Σ.), όρων δηλαδή που έχουν προδιατυπωθεί μονομερώς από τον προμηθευτή (π.χ. τράπεζα για χρήση σε απεριόριστο αριθμό μελλοντικών συμβάσεων. Κατ' αυτό τον τρόπο καλύπτονται από τις προστατευτικές ρυθμίσεις για τους Γ.Ο.Σ. και όσα πρόσωπα (φυσικά ή νομικά) δεν είναι καταναλωτές και σωρευτικά: α) η σύμβαση περιλαμβάνει όρους που δεν αποτέλεσαν αντικείμενο ατομικής διαπραγμάτευσης μεταξύ των μερών, β) πληρούν τα κριτήρια της «πολύ μικρής επιχείρησης», σύμφωνα με το άρθρο 2 παρ. 2 του ν. 4308/2014 και γ) είναι τελικοί αποδέκτες των παρεχόμενων προϊόντων ή υπηρεσιών.

[243] Ορίζεται ότι «Πολύ μικρές οντότητες είναι οι οντότητες οι οποίες κατά την ημερομηνία του ισολογισμού τους δεν υπερβαίνουν τα όρια δύο τουλάχιστον από τα ακόλουθα τρία κριτήρια: α) Σύνολο ενεργητικού

υπηρεσιών. Συνεπώς, έτσι θα καλύπτονται από την ευνοϊκή τροποποίηση του άρθρου 74 εδ. τελ. και οι πολύ μικρές επιχειρήσεις, για τις οποίες το κόστος απάτης στις ηλεκτρονικές συναλλαγές είναι πολλές φορές δυσβάστακτο.

Προχωρώντας στα υπόλοιπα στοιχεία της νέας ρύθμισης, για τον όρο της βαριάς αμέλειας έγινε λόγος παραπάνω. Δεν υπάρχουν συγκεκριμένα κριτήρια για την οριοθέτησή της, παρά μόνο ότι θα πρέπει να νοείται κάτι βαρύτερο από την απλή αμέλεια. Έτσι θα αφορά μορφές συμπεριφοράς που παρουσιάζουν σημαντικό βαθμό έλλειψης επιμέλειας (πχ ο κωδικός PIN να βρίσκεται δίπλα στο μέσο πληρωμής κατά τρόπο ανοικτό και ευχερώς ανιχνεύσιμο από τρίτους).

Κατ' αυτό τον τρόπο «αν ο πληρωτής είναι καταναλωτής και εφόσον οι ζημιές οφείλονται σε βαριά αμέλεια, ευθύνεται μέχρι του ανώτατου ποσού των χιλίων (1.000) ευρώ». Τούτο σημαίνει ότι ο πληρωτής θα απαλλαγεί για ζημίες πέραν των 1000 ευρώ, οι οποίες προέκυψαν από τη χρήση μέσου πληρωμών το οποίο χάθηκε ή κλάπηκε ή υπεξαιρέθηκε εξαιτίας βαριάς αμέλειας.

Για την εξισορρόπηση των συμφερόντων τραπεζών – πληρωτών προστέθηκε και ο όρος «λαμβάνοντας υπόψη ιδίως τη φύση των εξατομικευμένων διαπιστευτηρίων ασφαλείας και τις ειδικότερες περιστάσεις υπό τις οποίες το μέσο πληρωμής απωλέσθη, εκλάπη ή υπεξαιρέθηκε». Αυτή η πρόβλεψη διατυπώθηκε για να μην επωμίζονται τα τραπεζικά ιδρύματα τις ζημίες πέραν των 1000 ευρώ για πληρωτές που επιδεικνύουν ακραία αμελή συμπεριφορά και ενώ τους διέθεσαν τα απαραίτητα μέτρα ασφαλείας.

6.5.4 Οι πρόσθετοι και πιο εξελιγμένοι μηχανισμοί ελέγχου των συναλλαγών

Επιπροσθέτως και μετά τις αντιδράσεις των τραπεζικών ιδρυμάτων, σχετικά με την απαλλαγή του πληρωτή για ζημίες πέραν των 1000 ευρώ, προστέθηκε ένα επιπλέον εδάφιο. Σύμφωνα με το τελευταίο «Το τέταρτο εδάφιο δεν εφαρμόζεται, αν ο πάροχος αποδείξει ότι διαθέτει και εφαρμόζει πρόσθετους, αποτελεσματικούς και πιο εξελιγμένους μηχανισμούς ελέγχου των συναλλαγών, από αυτούς που εφαρμόζει για την ισχυρή ταυτοποίηση των συναλλαγών, για συναλλαγές που μπορούν να προκαλέσουν ζημία άνω των (1.000) ευρώ, όπως ιδίως μηχανισμούς που αξιοποιούν τεχνολογίες τεχνητής νοημοσύνης ή επιπλέον κωδικό ή βιομετρική ταυτοποίηση ή τηλεφωνική επιβεβαίωση».

(περιουσιακών στοιχείων): 350.000 ευρώ, β) Καθαρό ύψος κύκλου εργασιών: 700.000 ευρώ, γ) Μέσος όρος απασχολουμένων κατά τη διάρκεια της περιόδου: 10 άτομα».

Όπως αναλύθηκε παραπάνω, το εδάφιο δ' προβλέπει περιορισμό της ευθύνης του πληρωτή μέχρι το ποσό των 1000 ευρώ, εφόσον οι ζημίες οφείλονται σε βαριά αμέλεια. Αντίθετα, το νέο εδάφιο τελ. προβλέπει τη μη εφαρμογή της πρόβλεψης περί απαλλαγής του πληρωτή, εφόσον ο πάροχος αποδείξει ότι διαθέτει και εφαρμόζει πρόσθετους και πιο εξελιγμένους μηχανισμούς ελέγχου. Έτσι, τα τραπεζικά ιδρύματα απαλλάσσονται από την κάλυψη των ζημιών άνω των 1000 ευρώ, εφόσον αποδεικνύουν ότι διαθέτουν και εφαρμόζουν τέτοιους μηχανισμούς.

Ως «πρόσθετοι και πιο εξελιγμένοι» θα πρέπει να θεωρούνται οι μηχανισμοί που υπερβαίνουν την ταυτοποίηση με βάση δύο ή περισσότερα στοιχεία που αφορούν γνώση, κατοχή και κάποιο μοναδικό εγγενές χαρακτηριστικό[244]. Δεν αρκεί δηλαδή, για την απαλλαγή της τράπεζας, η απαίτηση κωδικού πρόσβασης, η κατοχή κινητού τηλεφώνου και η έγκριση συναλλαγής με ειδοποίηση push, αλλά απαιτείται απόδειξη ότι εφαρμόζεται κάτι επιπλέον αυτών, όπως για παράδειγμα μηχανισμός που αξιοποιεί τεχνολογίες τεχνητής νοημοσύνης.

6.5.5 Αξιολόγηση της ρύθμισης

Με τη συγκεκριμένη πρόβλεψη του τελευταίου εδαφίου επιχειρείται η κινητοποίηση των τραπεζών, ώστε να εισάγουν ακόμα πιο ισχυρούς μηχανισμούς ταυτοποίησης και ελέγχου[245], για συναλλαγές που μπορούν να προκαλέσουν ζημία άνω των 1000 ευρώ. Θετικό στοιχείο είναι και ότι το βάρος απόδειξης σχετικά με την εφαρμογή των εξελιγμένων μηχανισμών βαρύνει τα τραπεζικά ιδρύματα. Από την άλλη πλευρά οι καταναλωτές μπορεί να επωμίζονται εύκολα την ευθύνη για ζημίες πέραν των 1000 ευρώ, ακόμα και αν οι τράπεζες εισάγουν και εφαρμόζουν «εξελιγμένους» μηχανισμούς που

[244] Σύμφωνα με το άρθρο 4 στοιχείο 30 του ν. 4537/2018, ως ισχυρή ταυτοποίηση πελάτη νοείται «η ταυτοποίηση με βάση τη χρήση δύο ή περισσότερων στοιχείων που αφορούν γνώση (στοιχείο το οποίο μόνο ο χρήστης υπηρεσίας πληρωμών γνωρίζει), κατοχή (στοιχείο το οποίο μόνο ο χρήστης κατέχει) και κάποιο μοναδικό εγγενές χαρακτηριστικό του (στοιχείο το οποίο ο χρήστης είναι), στοιχεία τα οποία είναι ανεξάρτητα μεταξύ τους, ως προς το ότι η παραβίαση του ενός δεν θέτει σε κίνδυνο την αξιοπιστία των υπολοίπων και η διαδικασία της οποίας είναι σχεδιασμένη κατά τρόπο που να προστατεύεται η εμπιστευτικότητα των δεδομένων ταυτοποίησης».

[245] Στο ίδιο πνεύμα κινείται η παρ. 2 του άρθρου 74 του ν. 4537/2018, ορίζοντας ότι «Εάν ο πάροχος υπηρεσιών πληρωμών του πληρωτή δεν απαιτεί ισχυρή ταυτοποίηση του πελάτη, ο πληρωτής ευθύνεται για τυχόν οικονομικές συνέπειες, μόνο αν έχει ενεργήσει με δόλο». Συνεπώς, χωρίς ισχυρή ταυτοποίηση, ο πελάτης δε φέρει καμία ευθύνη παρά μόνο αν ενήργησε με δόλο.

λειτουργούν υποτυπωδώς. Χωρίς, δηλαδή, να παρέχουν πραγματική επιπλέον προστασία, να εισαχθούν από τις τράπεζες «τυπικά» για την απαλλαγή από την ευθύνη. Π.χ. εφαρμογή μηχανισμού ο οποίος λειτουργεί με τεχνητή νοημοσύνη και ελέγχει ύποπτες συναλλαγές με ελάχιστη, όμως, πρακτική αξία και αμφίβολη αποτελεσματικότητα για την αποτροπή μη εξουσιοδοτημένων συναλλαγών. Για να αποφευχθεί ένα τέτοιο ενδεχόμενο θα πρέπει η ΤτΕ να καθορίζει το περιεχόμενο και τις ειδικότερες απαιτήσεις και προδιαγραφές των πρόσθετων και πιο εξελιγμένων μηχανισμών[246]. Πάντως, στο τελικό κείμενο του ν. 5019/2023, προστέθηκε ο όρος «αποτελεσματικούς», ώστε οι μηχανισμοί που δεν είναι αρκούντως αποτελεσματικοί, να μην δύνανται να απαλλάσσουν τις τράπεζες.

Σε κάθε περίπτωση, τελική δικλείδα ασφαλείας για την προστασία του καταναλωτή θα πρέπει να αποτελεί ο δικαστικός έλεγχος. Η κρίση, δηλαδή, εάν στη συγκεκριμένη περίπτωση πράγματι τα κρινόμενα μέτρα ήταν επαρκή και πρόσφορα για την αποτροπή του συγκεκριμένου κινδύνου ζημίας, κατά τη συνήθη πορεία των πραγμάτων, τηρουμένων των αρχών της αναλογικότητας και της προστασίας των οικονομικών συμφερόντων του καταναλωτή.

Ως αντιρρήσεις που θα μπορούσαν να διατυπωθούν για τη βασική ρύθμιση του εδ. δ’ είναι η ενδεχόμενη έξαρση πλασματικών απατών (συμπαιγνίες), οι οποίες θα έπληττα τα τραπεζικά ιδρύματα. Επιπλέον αρνητικό στοιχείο αποτελεί η πιθανή επανάπαυση των καταναλωτών σχετικά με τις απάτες, εφόσον ακόμα και εκείνη η συμπεριφορά που θα στοιχειοθετεί βαριά αμέλεια, δε θα μπορούσε να τους κοστίσει περισσότερα από 1000 ευρώ. Τέλος, εφόσον τα σχετικά ποσά θα καλύπτονται από τις τράπεζες, οι πληρωτές ίσως να μην ενδιαφέρονται για τη δίωξη των δραστών, και δεδομένου ότι τα εγκλήματα διώκονται κατ’ έγκληση και οι αξιώσεις είναι αμεταβίβαστες, οι τράπεζες δε θα μπορούσαν να στραφούν κατά των δραστών[247].

Ακόμα και έτσι πάντως, το συμφέρον των πολλών και αδυνάμων είναι τόσο άξιο προστασίας ώστε να δικαιολογεί σαφώς τη νομοθετική παρέμβαση. Παρά τις αμφισβητήσεις, η συγκεκριμένη μπορεί να λειτουργήσει ως μοχλός πίεσης προς τις

[246] Βλ. 94 Παρ. 6 του ν. 4537/2018 όπου αναφέρεται ότι με απόφαση της Τράπεζας της Ελλάδος καθορίζεται το περιεχόμενο και οι ειδικότερες προδιαγραφές και απαιτήσεις της ισχυρής ταυτοποίησης.

[247] Πάντως στην περίπτωση της ανάληψης μετρητών με πλαστή κάρτα, η ΑΠ 131/2013 έκρινε ότι η τράπεζα νομιμοποιείται για παράσταση προς υποστήριξη της κατηγορίας.

τράπεζες για την εισαγωγή νέων εξελιγμένων μεθόδων ταυτοποίησης, οι οποίες θα απέτρεπαν οποιαδήποτε μη εγκεκριμένη πράξη πληρωμής[248].

6.6 Smishing

Το smishing αφορά την αποστολή παραπλανητικών SMS στο κινητό τηλέφωνο του υποψήφιου θύματος. Αποτελεί παραλλαγή του phishing και διαπράττεται με τους ίδιους τρόπους, με μόνη διαφορά το μέσο αποστολής του παραπλανητικού μηνύματος. Αντί δηλαδή να αποστέλλεται μέσω e-mail (phishing), επιλέγεται ως τρόπος αποστολής το SMS. Για την ποινική του αντιμετώπιση ισχύουν τα ίδια με το phishing.

6.7 Sim swapping

Το «sim swapping», αποτελεί τεχνική των δραστών που αναπτύχθηκε κατά τα τελευταία χρόνια για την παραβίαση των επιπλέον ασφαλιστικών δικλείδων που εισήχθησαν στις ηλεκτρονικές συναλλαγές. Ειδικότερα, για την πραγματοποίηση ηλεκτρονικών συναλλαγών, δεν αρκούν πια τα στοιχεία της πιστωτικής κάρτας. Χρειάζεται επιπλέον η επιβεβαίωση της συναλλαγής μέσω κωδικού μιας χρήσης που αποστέλλεται στο κινητό τηλέφωνο του νόμιμου κατόχου της κάρτας.

Οι δράστες με την τεχνική του «sim swapping» επιδιώκουν να αποκτήσουν πρόσβαση στην κάρτα SIM του θύματος με τον λιγότερο σύνθετο τρόπο που θα μπορούσε να επιτευχθεί κάτι τέτοιο. Απευθύνονται, δηλαδή, στους παρόχους κινητής τηλεφωνίας και ισχυρίζονται ότι έχουν χάσει ή καταστρέψει την παλιά τους κάρτα SIM και χρειάζονται μία νέα σε αντικατάστασή της. Έτσι τελούν την κοινή απάτη του άρθρου 386 ΠΚ.

Βέβαια, οι πάροχοι, απαιτούν πλήθος προσωπικών στοιχείων για την παράδοση νέας κάρτας SIM, τα οποία λογικά δεν μπορούν να γνωρίζουν οι δράστες. Έτσι, οι τελευταίοι, συνδυάζουν πολλές φορές και την τεχνική του phishing για να αποκτήσουν τις πληροφορίες που θα κληθούν να παραδώσουν στους παρόχους κινητής τηλεφωνίας.

[248] Για την αποφυγή της κάλυψης των ζημιών άνω των χιλίων ευρώ, οι τράπεζες θα εισάγουν πρόσθετους και πιο εξελιγμένους μηχανισμούς ελέγχου για τις συναλλαγές αυτές.

6.8 Απάτες που σχετίζονται με το κρυπτοχρήμα

6.8.1 Ορισμός του κρυπτοχρήματος

Τα τελευταία έτη, τα «κρυπτονομίσματα» έχουν γίνει ευρύτερα γνωστά στο κοινό, κερδίζοντας συνεχώς έδαφος στις συναλλαγές. Βέβαια, ο όρος «κρυπτονόμισμα» δεν είναι ακριβής. Και τούτο διότι για την ιδιότητα του νομίσματος απαιτείται η κρατικώς καθιερωμένη μονάδα συναλλαγής. Νόμισμα, είναι λοιπόν το χρήμα εν στενή εννοία, με τη σημασία του νόμιμου νομίσματος το οποίο έχει επιβληθεί από το κράτος ως υποχρεωτικό μέσο πληρωμής[249]. Αντίθετα, χρήμα, σύμφωνα με τον πρακτικό ορισμό, αποτελεί οτιδήποτε απολαμβάνει γενικής αποδοχής ως μέσο πληρωμών[250]. Κρυπτοχρήμα, τελικά, ονομάζεται το αποκεντρωμένο μέσο πληρωμής που βασίζεται στην κρυπτογραφία, τόσο για την πραγματοποίηση συναλλαγών όσο και για τη δημιουργία νέων μονάδων του ίδιου[251]. Εφόσον απολαμβάνει γενικής αποδοχής ως μέσο πληρωμών μπορεί να θεωρηθεί χρήμα υπό ευρεία έννοια[252].

6.8.2 Βασικά χαρακτηριστικά

Βασικά χαρακτηριστικά του κρυπτοχρήματος είναι η αποκέντρωση και η αυξημένη ανωνυμία. Χαρακτηρίζεται μεν αποκεντρωμένο, διότι δεν εκδίδεται από τις κεντρικές τράπεζες κρατών, όπως δηλαδή συμβαίνει με το επίσημο νόμισμα. Εμφανίζει δε αυξημένο το στοιχείο της ανωνυμίας, καθότι η εύρεση του κατόχου του είναι ιδιαίτερα δυσχερής. Επίσης είναι άυλο, επειδή συνήθως δεν έχει υλική υπόσταση και ψηφιακό διότι οι μονάδες του αποτελούν ουσιαστικά τα ψηφιακά κλειδιά για την πρόσβαση στον λογαριασμό και την πραγματοποίηση συναλλαγών. Είναι τέλος, μετατρέψιμο σε νόμιμο χρήμα, αλλά χωρίς τον έλεγχο κεντρικού φορέα, υπόκειται σε ραγδαίες αυξομειώσεις.

6.8.2.1 Διαφορές με το λογιστικό - πλαστικό χρήμα

Το κρυπτοχρήμα δεν έχει σχέση με το ηλεκτρονικό -λογιστικό, πλαστικό- χρήμα. Το τελευταίο είναι πάντοτε εκπεφρασμένο σε νομισματικές μονάδες κρατικών

[249] Ε. Μεταξάκης, Bitcoin – Κρυπτοχρήμα και κυβερνοέγκλημα, 2017, σελ. 38.

[250] Ό.π. σελ. 39.

[251] Ό.π. σελ. 32.

[252] Ό.π. σελ. 42.

νομισμάτων[253], κάτι που δεν συμβαίνει στην περίπτωση του κρυπτοχρήματος[254]. Άλλωστε και τα μέσα πρόσβασης στο λογιστικό χρήμα (π.χ. βιβλιάριο[255], χρεωστική κάρτα[256]), διαφοροποιούνται σαφώς από το ίδιο το χρήμα, κάτι που δεν ισχύει στην περίπτωση του κρυπτοχρήματος. Έτσι, η απώλεια ή κλοπή του βιβλιαρίου ή της κάρτας[257] δεν συνεπάγεται την απώλεια του λογιστικού χρήματος. Ο δικαιούχος μπορεί να προβεί σε επανέκδοση του βιβλιαρίου ή της κάρτας[258] του και τότε θα ανακτήσει τον έλεγχο των κεφαλαίων του.

Αντίθετα, στην περίπτωση του κρυπτοχρήματος, τα λογιστικά ποσά που κάποιος κατέχει, ταυτίζονται απολύτως με το ψηφιακό πορτοφόλι του και το ιδιωτικό κλειδί του. Υπάρχει τέτοια στενή σύνδεση ώστε αν απωλέσει το ιδιωτικό του κλειδί, δεν θα μπορέσει ποτέ να ανακτήσει τον έλεγχο του κρυπτοχρήματος που διέθετε.

6.8.2.2 Ειδικότερα για την ανωνυμία

Η ελευθερία -απουσία κεντρικού ελέγχου-, και η ανωνυμία αποτελούν τη βασική ιδεολογία στην οποία εδράζεται το κρυπτοχρήμα. Βέβαια, στην πραγματικότητα, δεν μπορεί να γίνεται λόγος για πλήρη ανωνυμία. Πρόκειται για ψευδωνυμία, αφού η αλυσίδα

---

[253] Βλ. Ι. Μοροζίνη σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, 2023, σελ. 142 επ. «Τα χρήματα δεν είναι σήμερα κατά κύριο λόγο κέρματα και τραπεζογραμμάτια, αλλά ψηφιακά δεδομένα αποθηκευμένα σε πληροφοριακά συστήματα ... συνεπώς χρειάζεται μετατόπιση του κέντρου βάρους από την ιδιοκτησία στην περιουσία».

[254] Ό.π. σελ. 37.

[255] Οι εγγραφές σε αυτό αποτελούν απόδειξη ύπαρξης ενοχικού και όχι εμπράγματου δικαιώματος. Ο δικαιούχος του βιβλιαρίου δεν θεωρείται κάτοχος των νομισματικών μονάδων που εγγράφονται ως υπόλοιπο στο βιβλιάριό του. Χ. Μυλωνόπουλος, Ληστεία κατά του δημοσίου και απάτη με παράλειψη, ΠοινΧρ 1997, σελ. 1113,1114.

[256] Γ. Μπουρμάς, Περαιτέρω προβληματισμοί για την ποινική αξιολόγηση της άνευ δικαιώματος ανάληψης μετρητών από ΑΤΜ και των ηλεκτρονικών τραπεζικών συναλλαγών (web banking) (με αφορμή τις ΑΠ 737/2012 και ΑΠ 742/2012), ΠοινΔικ 2014, σελ. 1117.

[257] Η κλοπή της κάρτας αντιμετωπιζόταν από τη νομολογία ως κλοπή ευτελούς αξίας. Βλ. ΣυμβΠλημΚαστ 196/1999, ΠοινΧρ 1999, σελ. 1058 (πιστωτική κάρτα), παρατ. Θ. Σάμιος. ΑΠ 127/2004, ΠΛογ 2004, σελ. 189 (πιστωτική κάρτα), Θ. Σάμιος, Αποτελεί η κάρτα αυτόματης συναλλαγής «πράγμα ευτελούς αξίας»;, ΠοινΧρ 2000, σελ. 667.

[258] Επειδή η κάρτα διαθέτει στοιχεία εγγράφου, πρέπει να γίνει δεκτή η εφαρμογή της ΠΚ 222 περί υπεξαγωγής εγγράφου -σε περίπτωση αφαίρεσης και στη συνέχεια με σκοπό βλάβης άλλου απόκρυψη, βλάβη ή καταστροφή της κάρτας-. Δεν εφαρμόζεται η ΠΚ 372. Χ. Μυλωνόπουλος, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ. 47.

τμημάτων περιλαμβάνει κάθε συναλλαγή και το εκάστοτε δημόσιο κλειδί χαρτογραφεί τις συναλλαγές είτε μόνο του είτε σε συνδυασμό με άλλα δεδομένα που μπορούν να ζητήσουν οι αρχές από καταστήματα, ανταλλακτήρια κλπ. Συνεπώς, οι διευθύνσεις κρυπτοχρήματος, μπορούν να οδηγήσουν, σε συνδυασμό με άλλα προσωπικά δεδομένα, στην ταυτοποίηση του χρήστη που πραγματοποίησε την συναλλαγή[259]. Ακόμα και με την χρήση διαφόρων εργαλείων ανωνυμοποίησης[260] (π.χ. VPN[261]), δεν μπορεί επιτευχθεί παρά μία επίφαση ανωνυμίας, εφόσον οι αρχές μπορούν να απευθυνθούν στις εταιρείες που τα διαχειρίζονται και να επιτύχουν άρση της ανωνυμίας. Ως πιο ενδεδειγμένη μέθοδος ανωνυμοποίησης, θεωρείται η αγορά διαφόρων μονάδων κρυπτοχρήματος που προσανατολίζονται στην ανωνυμία (π.χ. Zerocash[262], Dash κλπ).

6.8.3 Ο τρόπος εκτέλεσης των συναλλαγών

Για την εκτέλεση συναλλαγών, κάθε κάτοχος κρυπτοχρήματος, διαθέτει μία διεύθυνση, ήτοι ένα δημόσιο κλειδί, το οποίο δημιουργείται από την εφαρμογή πορτοφολιού κρυπτοχρήματος (crypto wallet). Η διεύθυνση αυτή είναι αλφαριθμητική, αποτελούμενη από 26 μέχρι 35 χαρακτήρες. Η ίδια διεύθυνση μπορεί να κοινοποιείται ελεύθερα, χωρίς να διακινδυνεύεται το πορτοφόλι του χρήστη, αφού η τιμή της μπορεί να υπολογιστεί μόνο με βάση με το ιδιωτικό κλειδί χωρίς να είναι δυνατός ο υπολογισμός του

[259] Ό.π., σελ. 120-123. Για τα προσωπικά δεδομένα βλ. αναλυτικά Ε. Αλεξανδροπούλου – Αιγυπτιάδου, Προσωπικά Δεδομένα, 2016, σελ. 43επ.

[260] Διατίθενται στην αγορά κάποιοι ειδικοί ανωνυμοποιητές κρυπτοχρήματος οι οποίοι αναλαμβάνουν να αποκρύψουν την προέλευση του, αναμειγνύοντας μονάδες του. Ωστόσο, η παράδοση μονάδων στους διαχειριστές αυτών των ανωνυμοποιητών εμπεριέχει πολλούς κινδύνους (οικειοποίηση, πτώχευση, παρακολούθηση).

[261] Οι ανωνυμοποιητές VPN επιτυγχάνουν την ανωνυμία μέσω της απόκρυψης του διαδικτυακού πρωτοκόλλου του χρήστη. Το τελευταίο αποτελεί δεδομένο προσωπικού χαρακτήρα, χωρίς ο χαρακτηρισμός αυτός να αναιρείται λόγω της ανάπτυξης μέσων ανωνυμοποίησης. Βλ. Γνώμη 4/2009 της Ομάδας του άρθρου 29 της Οδηγίας 95/46/ΕΚ. Η αιτιολογική σκέψη 26 της Οδηγίας αναφέρει ότι «Για να διαπιστωθεί ότι η ταυτότητα ενός προσώπου μπορεί να εξακριβωθεί, πρέπει να λαμβάνεται υπόψη το σύνολο των μέσων που μπορούν ευλόγως να χρησιμοποιηθούν, είτε από τον υπεύθυνο επεξεργασίας, είτε από τρίτο, για να εξακριβωθεί η ταυτότητα του εν λόγω προσώπου». Η αξιολόγηση αυτών «των μέσων που μπορούν να χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας» είναι δυναμική και μεταβάλλεται όσο εξελίσσεται η τεχνολογία.

[262] Το πρωτόκολλο Zerocash αποκρύπτει την προέλευση, το ποσό και τον προορισμό της συναλλαγής.

ιδιωτικού κλειδιού με βάση το δημόσιο[263]. Για μεγαλύτερη ευχέρεια τόσο οι διευθύνσεις bitcoin όσο και τα ιδιωτικά κλειδιά μπορούν να λάβουν τη μορφή QR Code (Quick Response Code).

Για τη μεταφορά μονάδων κρυπτοχρήματος, οι χρήστες απλά εισάγουν στο ψηφιακό πορτοφόλι τους τη διεύθυνση του παραλήπτη (δημόσιο κλειδί), επιλέγουν το ποσό και το αποστέλλουν.

6.8.3.1 Ειδικότερα ο τρόπος εκτέλεσης των συναλλαγών με τεχνικούς όρους (blockchain)

Σε μια πιο τεχνική ανάλυση, οι συναλλαγές πραγματοποιούνται με την αποστολή του δημόσιου κλειδιού (διεύθυνση) του νέου δανειστή μιας τιμής κατακερματισμού της προηγούμενης συναλλαγής -από την οποία προήλθαν οι προς μεταβίβαση μονάδες- και μία ψηφιακή υπογραφή προερχόμενη από το ιδιωτικό κλειδί του οφειλέτη[264]. Το ποσό θα εμφανίζεται ως διαθέσιμο στην αλυσίδα τμημάτων (blockchain).

Το Blockchain αποτελεί μια τεχνολογία αιχμής για την ασφάλεια των συναλλαγών. Η κεντρική ιδέα στηρίζεται στην αποκέντρωση και στην ασφάλεια που αυτή προσφέρει. Ειδικότερα, αντί να χρησιμοποιείται ένας κεντρικός φορέας που συγκεντρώνει τον έλεγχο, στην τεχνολογία blockchain οι συναλλαγές πιστοποιούνται από πολλαπλούς ομότιμους κόμβους. Διότι είναι πολύ πιο εύκολο να παραβιαστεί ένα κεντρικό σύστημα[265], από το να αναληφθεί η πλειοψηφία της επεξεργαστικής ισχύος από κακόπιστους κόμβους[266]. Πιο τεχνικά, η αλυσίδα τμημάτων (blockchain) αποτελεί έναν κατανεμημένο[267] λογιστικό κατάλογο (distributed ledger), στον οποίο οι συναλλαγές ή τα δεδομένα[268] συνδέονται

---

[263] Ε. Μεταξάκης, Bitcoin – Κρυπτοχρήμα και κυβερνοέγκλημα, 2017, σελ. 53-54.

[264] Ό.π.

[265] Π.χ. Τα έγγραφα που εκδίδονται από το gov.gr φέρουν έναν μοναδικό κωδικό που αποτελείται από 22 χαρακτήρες που προκύπτουν με την κωδικοποίηση base64 (διαφορετικοί χαρακτήρες A-Z, a-z, 0-9), ενός μη ανιχνεύσιμου αριθμού μήκους 128 bits (2^128 διαφορετικοί αριθμοί). Το gov.gr διαθέτει επίσης ειδική σελίδα για τον έλεγχο της εγκυρότητας των εγγράφων. Στην θεωρητική περίπτωση παραβίασης των κεντρικών υποδομών του ΕΔΥΤΕ, οι χρήστες θα μπορούσαν να εκτεθούν, κάτι που δεν θα συνέβαινε εάν υιοθετούνταν η τεχνολογία Blockchain.

[266] Ε. Μεταξάκης, Bitcoin – Κρυπτοχρήμα και κυβερνοέγκλημα, 2017, σελ. 38.

[267] Κατανεμημένη ονομάζεται η βάση δεδομένων, της οποίας τα αποθηκευτικά μέσα δεν συνδέονται όλα με ένα υπολογιστικό σύστημα, αλλά με περισσότερα.

[268] Κάποιες φορές προστίθενται και μεταδεδομένα στην αλυσίδα τμημάτων. Σύμφωνα με το άρθρο 1 παρ. 4 του ΠΔ 25/2014 ως Μεταδεδομένα ορίζονται τα «Σύνολα δομημένης πληροφορίας που περιγράφουν και

μεταξύ τους σε μπλοκ δεδομένων. Αυτή η σύνδεση, καθιστά τα δεδομένα αμετάβλητα από κακόπιστους τρίτους και αδιαμφισβήτητα για όλους τους κατανεμημένους κόμβους (Nodes).

6.8.3.2 Η αξιοπιστία των συναλλαγών

Κάθε φορά που πραγματοποιείται μια συναλλαγή (π.χ. πίστωση ποσού στην δημόσια διεύθυνση του δανειστή), αυτή αποστέλλεται αμέσως στο εκάστοτε δίκτυο[269] και εμφανίζεται ως ανεπιβεβαίωτη συναλλαγή. Κάθε συναλλαγή επιβεβαιώνεται με την ένταξη της στην αλυσίδα τμημάτων[270]. Οι εξορύκτες (miners), έχουν αναλάβει τη διαδικασία επαλήθευσης των νέων συναλλαγών και την προσθήκη τους στην αλυσίδα τμημάτων. Τα νέα τμήματα[271] της αλυσίδας δημιουργούνται με τον αλγόριθμο SHA-256, ο οποίος κρυπτογραφεί μαθηματικά και κατακερματίζει την πληροφορία του μπλοκ, με τρόπο μη αναστρέψιμο (one way encryption). Κάθε μπλοκ συνδέεται με κρυπτογράφηση και υπογράφεται ψηφιακά από κάθε κόμβο με το προηγούμενο του, καθιστώντας έτσι κάθε προσπάθεια αλλαγής των δεδομένων αδύνατη.

6.8.4 Η νομική αντιμετώπιση του κρυπτοχρήματος στα επιμέρους κράτη

Στην ΕΕ υιοθετούνται κανόνες για την ιχνηλασιμότητα, την αποτροπή νομιμοποίησης μαύρου χρήματος και την προστασία των καταναλωτών. Τον Ιούνιο του 2022 επετεύχθη προσωρινή συμφωνία μεταξύ του Κοινοβουλίου και του Συμβουλίου για τη θέσπιση νέων κανόνων για την καλύτερη αξιοποίηση των δυνατοτήτων των

χαρακτηρίζουν ηλεκτρονικά έγγραφα, ηλεκτρονικούς φακέλους και ηλεκτρονικά αρχεία και επιτρέπουν την ταύτιση, διαχείριση, αναζήτηση, ανάκτηση, πρόσβαση και επιβεβαίωση της γνησιότητάς τους από ανθρώπους ή συστήματα».

[269] Π.χ. δίκτυο bitcoin.

[270] Για να μεταβιβασθεί περαιτέρω το κρυπτοχρήμα, πρέπει να εντοπίζεται στην αλυσίδα τμημάτων. Άρα το κρυπτοχρήμα έχει υπόσταση μόνο εντός της αλυσίδας.

[271] Η τιμή κατάτμησης που πρέπει να υπολογίζεται για κάθε νέο τμήμα της αλυσίδας όλο και δυσκολεύει. Όταν πρωτοεμφανίστηκε το Bitcoin αρκούσε για την εξόρυξη ένας απλός οικιακός ηλεκτρονικός υπολογιστής. Στις μέρες μας η εξόρυξη είναι συμφέρουσα μόνο με υψηλών επιδόσεων κάρτες γραφικών (GPU) ή με ειδικούς ηλεκτρονικούς υπολογιστές εξόρυξης. Βλ. Ε. Μεταξάκη, Bitcoin – Κρυπτοχρήμα και κυβερνοέγκλημα, 2017, σελ. 63, 65.

κρυπτοστοιχείων και τον μετριασμό των κινδύνων[272]. Το ΔΕΕ, πάντως, είχε ήδη αποδεχτεί το Bitcoin ως μέσο πληρωμής[273].

Στη Γαλλία, οι πάροχοι υπηρεσιών ανταλλαγής κρυπτοχρήματος ή ψηφιακού πορτοφολιού καθώς και οι σχετικές πλατφόρμες συναλλαγών, οφείλουν να αιτούνται άδεια από την Αρχή, να εφαρμόζουν πρακτικές know your customer και να συμμορφώνονται με τους κανονισμούς κατά του ξεπλύματος μαύρου χρήματος και χρηματοδότησης της τρομοκρατίας[274]. Από την άλλη πλευρά στη Γερμανία το κρυπτοχρήμα δεν εμπίπτει στο νομικό καθεστώς του νομίσματος ή του χρήματος αλλά στη βάση συμφωνίας ή πρακτικής γίνεται δεκτό ως μέσο πληρωμής ή εξυπηρετεί επενδυτικούς σκοπούς. Απαιτείται επίσης άδεια για συναλλαγές σε εμπορική κλίμακα, με ειδική μέριμνα για την προστασία του χρηματοπιστωτικού συστήματος και των καταναλωτών από τους σχετικούς κινδύνους[275]. Στο Λουξεμβούργο το κρυπτοχρήμα αντιμετωπίζεται με ουδετερότητα, καθώς γίνεται μεν μνεία στους κινδύνους που το συνοδεύουν, αλλά η νομοθεσία του προσαρμόζεται συνεχώς στην τεχνολογία του blockchain[276]. Για την έκδοση, την παροχή υπηρεσιών και την λειτουργία ανταλλακτηρίων απαιτείται άδεια[277].

Εκτός ΕΕ: Τον Σεπτέμβριο του 2021 η κεντρική τράπεζα της Κίνας ανακοίνωσε ότι όλες σχετικές με τα κρυπτοστοιχεία επιχειρηματικές δραστηριότητες θεωρούνται παράνομες οικονομικές δραστηριότητες. Αντίθετα στην Ιαπωνία το κρυπτοχρήμα αντιμετωπίζεται απλώς επιφυλακτικά, καθώς εφαρμόζονται πολιτικές πρόληψης της τρομοκρατίας και «know your customer». Η Ελβετία, ήδη από τον Αύγουστο του 2021 εισήγαγε ρυθμιστικό πλαίσιο για την τεχνολογία blockchain, εκτιμώντας ότι η ασφάλεια δικαίου θα αποτελέσει πυλώνα για την καινοτομία και την εξέλιξη. Περαιτέρω, για τη διαφύλαξη της ακεραιότητας και της καλής φήμης του χρηματοοικονομικού της

[272] https://www.consilium.europa.eu/el/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/.

[273] ΔΕΕ C-264/14: https://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=EL.

[274] Βλ. Code monétaire et financier, Articles L54-10-1 επ. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072026/LEGISCTA000038509568/#LEGISCTA000038509568.

[275] https://www.bafin.de/dok/17964164.

[276] https://www.chd.lu/fr/dossier/8055.

[277] https://www.cssf.lu/en/virtual-assets/.

συστήματος, εφαρμόζει πολιτικές αποτροπής του ξεπλύματος μαύρου χρήματος και της τρομοκρατίας[278].

Οι ΗΠΑ, πρωτοπορώντας στη νομοθεσία για το κρυπτοχρήμα, επηρεάζουν συνεχώς τις σχετικές εξελίξεις στο διεθνές δίκαιο. Σύμφωνα με το δίκαιο των ΗΠΑ το κρυπτοχρήμα αποτελεί ψηφιακή απεικόνιση αξίας, άλλης από την αναπαράσταση του δολαρίου ή ξένου νομίσματος[279]. Το κρυπτοχρήμα αντιμετωπίζεται φορολογικά ως περιουσία, ενώ κατά τα λοιπά ισχύουν οι γενικές αρχές περί φορολογίας. Ιδιαίτερα σημαντική κρίνεται η δημοσίευση του πρώτου ολοκληρωμένου πλαισίου «Για την υπεύθυνη ανάπτυξη ψηφιακών στοιχείων». Το πλαίσιο αυτό, ακολουθεί τις προτεραιότητες που καθορίστηκαν στο Εκτελεστικό Διάταγμα του Προέδρου της 9ης Μαρτίου 2022[280], στοχεύοντας στην προστασία καταναλωτών και επενδυτών, στην προώθηση της χρηματοοικονομικής σταθερότητας, στην καταπολέμηση του ξεπλύματος μαύρου χρήματος και της τρομοκρατίας κ.α.

Χρήσιμος αναδεικνύεται και ο ορισμός της FATF[281] για το εικονικό χρήμα, όπως έγινε δεκτός και από ορισμένες πολιτείες των ΗΠΑ. Ειδικότερα, ορίζεται ότι «Εικονικό χρήμα σημαίνει την η ψηφιακή αναπαράσταση αξίας που χρησιμοποιείται ως μέσο ανταλλαγής, ως λογιστική μονάδα ή ως μέσο διαφύλαξης αξιών και δεν αποτελεί νόμιμο χρήμα». Στη διατύπωση που υιοθέτησε η Ουάσιγκτον[282], αναφέρεται επίσης ότι «ο όρος δεν περιλαμβάνει το λογισμικό ή τα πρωτόκολλα που διέπουν τη μεταφορά της ψηφιακής αναπαράστασης αξίας, περιεχόμενο σχετικό με βιντεοπαιχνίδια, κάρτα επιβράβευσης ή κουπόνι δώρου».

[278] https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html.

[279] https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions.

[280] https://crsreports.congress.gov/product/pdf/IN/IN12039.

[281] Financial Task Force, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf, σελ. 4.

[282] H.B. 1179, 66 Leg., Reg. Sess. (Wash. 2019), https://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Bills/1179-S.pdf σελ. 7.

Ιδιαίτερο ενδιαφέρον παρουσιάζει, τέλος, ο ορισμός της FATF για τον πάροχο ψηφιακού πορτοφολιού[283]. Σύμφωνα με αυτόν: «Πάροχος ψηφιακού πορτοφολιού είναι μία οντότητα, η οποία παρέχει πορτοφόλι εικονικού χρήματος (εφαρμογή λογισμικού ή άλλο μέσο για την κατοχή, αποθήκευση και μεταφορά εικονικού χρήματος)».

6.8.5 Η εγκληματική δράση που σχετίζεται με το κρυπτοχρήμα

Η επέκταση του κρυπτοχρήματος στις συναλλαγές, δημιούργησε ένα νέο και ευρύ πεδίο εγκληματικότητας, το οποίο σχετίζεται άμεσα ή έμμεσα με αυτό. Άμεσα, καθότι το ίδιο το κρυπτοχρήμα γίνεται στόχος απάτης[284] και έμμεσα, διότι χρησιμοποιείται ως μέσο πληρωμής[285] ή ξεπλύματος χρήματος από άλλες εγκληματικές δραστηριότητες. Επίσης πολλές φορές το κρυπτοχρήμα αποτελεί όχημα για την πραγματοποίηση άλλων μορφών απάτης (τύπου Ponzi, επενδυτικές απάτες).

6.8.5.1 Ειδικά για τις απάτες που σχετίζονται με το κρυπτοχρήμα

Ως σχήμα Ponzi νοείται οποιαδήποτε χρηματική απάτη στηρίζεται σε «πυραμίδα» επενδυτών. Η πυραμίδα επενδυτών αποτελεί παράνομο επενδυτικό σχήμα καθόσον η πληρωμή των παλαιών επενδυτών γίνεται από τα κεφάλαια που εισφέρουν οι νέοι. Στο πεδίο του κρυπτοχρήματος, έχουν εξαπατηθεί εκατομμύρια επενδυτών με απώλειες δισεκατομμυρίων. Ιδιαίτερα γνωστή έγινε η περίπτωση της απάτης του Onecoin. Η ιδρύτριά του έπεισε το επενδυτικό κοινό ότι το Onecoin «θα γίνει το πιο ισχυρό κρυπτονόμισμα»[286] και οι συμμετέχοντες κέρδιζαν ανταμοιβή για κάθε άτομο που προσκαλούσαν. Τελικά το συγκεκριμένο δε διέθετε καν δικό του blockchain, η ιδρύτρια συγκέντρωσε έως 4 δις δολάρια και είναι καταζητούμενη από την Europol.

---

[283] Σύμφωνα με την έκθεση της FATF βλ. ό.π. σελ. 7, το ψηφιακό πορτοφόλι είναι ένα μέσο (εφαρμογή λογισμικού ή άλλος μηχανισμός) που χρησιμεύει για την κατοχή, αποθήκευση, ή μεταφορά εικονικής νομισματικής αξίας.

[284] Η ευρωπαϊκή έννομη τάξη έχει κρίνει το κρυπτοχρήμα άξιο ποινικής προστασίας, όπως προκύπτει από το συνδυασμό των περ. α', β', γ' της Οδηγίας (ΕΕ) 2019/713. Βλ. Ι. Μοροζίνη σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, 2023, σελ. 156.

[285] Χρησιμοποιείται ως μέσο πληρωμής λύτρων σε επιθέσεις ransomware (λυτρισμικό), καθώς και για πληρωμές σε καταστήματα του σκοτεινού διαδικτύου. Αποτελεί επίσης μέσο για τη χρηματοδότηση της τρομοκρατίας.

[286] Η συγκεκριμένη υπόσχεση αφορά σε κάτι μέλλον και αβέβαιο, οπότε δεν εμπίπτει στην έννοια του γεγονότος κατά τον ΠΚ και δεν αρκούσε από μόνη της για τη στοιχειοθέτηση της απάτης.

Η ιδρύτρια παρίστανε εν γνώσει της ψευδώς, ότι έχει εξειδικευμένες χρηματοοικονομικές γνώσεις στα κρυπτονομίσματα και έπεισε τους ενδιαφερομένους επενδυτές να επενδύσουν μεγάλα χρηματικά ποσά στις εκάστοτε επενδυτικές δομές που είχε συστήσει για το σκοπό αυτό. Επίσης υποσχόταν μεγάλα κέρδη χωρίς ανάληψη σοβαρού ρίσκου και σταθερές αποδόσεις, με σκοπό να προσποριστεί παράνομο περιουσιακό όφελος, ενώ εξ' αρχής γνώριζε ότι δεν διέθετε τη δυνατότητα να εξασφαλίσει τόσο υψηλή και σταθερή απόδοση. Ακόμα δεν είχε καν την πρόθεση να επενδύσει τα χρήματα για την ανάπτυξη δικτύου blockchain, αλλά εξ' αρχής αποσκοπούσε να καρπωθεί τα χρηματικά ποσά και να αποκομίσει αντίστοιχο παράνομο περιουσιακό όφελος. Με βάση αυτά τα δεδομένα πληρούνταν η αντικειμενική υπόσταση της απάτης (386 ΠΚ).

6.8.5.2 Η ποινική αξιολόγηση της αφαίρεσης μονάδων κρυπτοχρήματος

Τα αποθηκευμένα στη μνήμη flash ιδιωτικά και δημόσια κλειδιά και γενικότερα τα αποθηκευμένα σε αυτή τη μνήμη δεδομένα δεν μπορούν να αποτελέσουν αντικείμενο κλοπής ενέργειας. Τούτο διότι σε περίπτωση αθέμιτης αντιγραφής των κλειδιών (ψηφιακών δεδομένων[287]) δεν σημαίνει παράλληλα αφαίρεση[288] ηλεκτρονίων από την αστραπιαία μνήμη[289]. Συνεπώς αν κάποιος αφαιρέσει ηλεκτρονικό υπολογιστή που περιέχει ιδιωτικά και δημόσια κλειδιά, θα διωχθεί δυνάμει του ΠΚ 372 μόνο για την κλοπή του υπολογιστή αλλά όχι για τις περιεχόμενες μονάδες σε αυτόν κρυπτοχρήματος. Για πρόσβαση χωρίς δικαίωμα θα τιμωρηθεί δυνάμει του ΠΚ 370Β, ενώ αν τα κλειδιά θεωρηθούν απόρρητα δυνάμει του 370Γ[290]. Επίσης, αν κάνει χρήση των κλειδιών για να μεταφέρει σε δικό του πορτοφόλι τις μονάδες κρυπτοχρήματος, τότε θα έχει διαπράξει το έγκλημα του 386Α ΠΚ[291]. Τέλος, αν παραποιεί έναν άυλο μηχανισμό, ο οποίος χρησιμεύει στη μεταφορά νομισματικής αξίας κρυπτοχρήματος και προστατεύεται από την απομίμηση ή τη δόλια χρήση, τότε θα τελεί το έγκλημα του 209 ΠΚ.

---

[287] Το κρυπτοχρήμα συνίσταται σε ψηφιακά δεδομένα, οπότε η ποινική του αντιμετώπιση παραλλάσσει από περίπτωση σε περίπτωση. Έτσι μπορεί να αποτελεί αντικείμενο συναλλαγών ή μέσο απόδειξης. Βλ. Γ. Ναζίρη σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα, 2023, σελ. 458.

[288] Τα ψηφιακά δεδομένα είναι άυλα και δεν μπορούν να θεωρηθούν πράγματα σε οποιοδήποτε σταθερό μέσο και αν είναι αποθηκευμένα.

[289] Ε. Μεταξάκης, Bitcoin – Κρυπτοχρήμα και κυβερνοέγκλημα, 2017, σελ. 98.

[290] Ό.π., σελ. 237.

[291] Ι. Μοροζίνης σε Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, 2023, σελ. 167. Βούλευμα 828/2022, Ποιν.Δνη, σελ. 1228.

6.9 Η απάτη στο πεδίο των NFT's

Τα μη εναλλάξιμα κρυπτοπαραστατικά (Non Fungible Tokens – NFT's), στηρίζονται και πάλι στην τεχνολογία του blockchain, όπως και το κρυπτοχρήμα. Διαφέρουν από το τελευταίο κατά το ότι τα NFT's είναι μοναδικά[292], ενώ οι μονάδες συγκεκριμένου τύπου κρυπτοχρήματος (πχ bitcoin), δε διαφέρουν σε τίποτα η μία από την άλλη. Στην πράξη, τα NFT's χρησιμοποιούνται για να αποδείξουν τη γνησιότητα έργων τέχνης, λειτουργώντας ως «ψηφιακά πιστοποιητικά πνευματικής ιδιοκτησίας» τα οποία αποθηκεύονται μέσα στην αλυσίδα τμημάτων[293].

Η εγκληματική δράση στον χώρο τον NFT's ομοιάζει με εκείνη του κρυπτοχρήματος, περιλαμβάνοντας συνήθως επενδυτικές απάτες ή παράνομη πρόσβαση στο ψηφιακό πορτοφόλι του χρήστη στο οποίο περιέχονται τα ψηφιακά περιουσιακά στοιχεία. Έτσι, στην τελευταία περίπτωση υπάρχει μη εξουσιοδοτημένη πρόσβαση σε ψηφιακό πορτοφόλι (με χρησιμοποίηση δεδομένων χωρίς δικαίωμα) και τελείται το 370Β ΠΚ. Επιπλέον, σε περίπτωση μεταφοράς των NFT's σε άλλα πορτοφόλια, ο νόμιμος δικαιούχος δεν μπορεί να έχει πρόσβαση στα ψηφιακά περιουσιακά του στοιχεία. Συνακόλουθα, υπάρχει αυταπόδεικτη περιουσιακή ζημία και τελείται το έγκλημα του 386Α ΠΚ. Έτσι και πάλι η αθέμιτη μεταφορά NFT, θα αντιμετωπίζεται ως απάτη με υπολογιστή[294].

Για τη μεταφορά των NFT's μπορεί να απαιτηθούν μεγάλα τέλη, τα λεγόμενα «gas fees», με σκοπό την αμοιβή εκείνων που επαληθεύουν τις συναλλαγές στο δίκτυο blockchain. Συνεπώς, για την εντελή ικανοποίηση του θύματος, ο δράστης θα πρέπει να καταβάλλει και αυτά τα ποσά (ΠΚ 405 παρ. 2,3 ΠΚ).

---

[292] Λ. Κανέλλος, Smart Contracts, 2022, σελ. 104.

[293] Για την αλυσίδα τμημάτων βλ. παραπάνω 6.8.3.1 και την αξιοπιστία που προσφέρει 6.8.3.2.

[294] Βλ. Γ. Νούσκαλη σε ΠοινΔικ 2/2003, σελ. 187 «το αποτέλεσμα είναι η χωρίς δικαίωμα μείωση της περιουσίας του θύματος και η αύξηση, αντίστοιχα της περιουσίας του δράστη, ο οποίος μετά την ηλεκτρονική αυτή διακίνηση περιουσιακών στοιχείων … οι ανωτέρω πράξεις θα μπορούσαν να υπαχθούν ασφαλώς στη διάταξη της απάτης με υπολογιστή».

7 Επίλογος

Συνοψίζοντας, τα τελευταία έτη συντελέστηκαν σημαντικές τεχνολογικές εξελίξεις, οι οποίες με τη σειρά τους συνέτειναν στην ανάπτυξη νέων μορφών ηλεκτρονικής οικονομικής εγκληματικότητας. Η ανάγκη για διαρκή επαγρύπνηση του νομοθέτη, ώστε η ποινική νομοθεσία να ανταποκρίνεται στις νέες τεχνολογικές εξελίξεις είναι προφανής. Το ίδιο αναγκαία είναι και η συνεχής επιμόρφωση των συντελεστών απονομής της δικαιοσύνης, σχετικά με την ερμηνεία και εφαρμογή των σχετικών διατάξεων. Για την πληρέστερη κατανόηση αυτών των -πολλές φορές περίπλοκων- διατάξεων, απαιτείται διαρκής τριβή τόσο με τη νέα νομοθεσία όσο και με τη νέα τεχνολογία.

Δεν αρκεί, βέβαια, από μόνη της η σύγχρονη νομοθεσία και η ορθή εφαρμογή της. Χρειάζεται επιπλέον, η αποτελεσματική και συντονισμένη δράση των ερευνητικών και διωκτικών αρχών, όχι μόνο των εγχώριων αλλά και στη βάση διεθνούς συνεργασίας. Πολλώ δε μάλλον, όταν η απάτη συνδέεται με εγκλήματα ιδιαίτερης ποινικής απαξίας - ξέπλυμα μαύρου χρήματος και χρηματοδότηση της τρομοκρατίας. Η απάτη στις ηλεκτρονικές συναλλαγές αποτελεί από τη φύση της μια δυναμική, διασυνοριακή και ευρεία μορφή εγκληματικής δραστηριότητας που συνεχώς μεταβάλλεται παράλληλα με τις τεχνολογικές εξελίξεις. Αναμένουμε τις νέες προκλήσεις με το βλέμμα στραμμένο στο μέλλον.

Βιβλιογραφία

Ε. Αλεξανδροπούλου – Αιγυπτιάδου, Προσωπικά Δεδομένα, εκδ. Νομική Βιβλιοθήκη, 2016.

Α. Αργυρόπουλος, Ηλεκτρονική εγκληματικότητα, εκδ. Αντ. Ν. Σάκκουλα, 2001.

Κ. Βλαχόπουλος, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2007.

Θ. Δαλακούρας, Ο Νέος Κώδικας Ποινικής Δικονομίας, εκδ. Νομική Βιβλιοθήκη, 2020.

Θ. Δαλακούρας, Ηλεκτρονικό Έγκλημα, εκδ. Νομική Βιβλιοθήκη, 2023.

Α. Ζάννη, Το διαδικτυακό έγκλημα, εκδ. Αντ. Ν. Σάκκουλα, 2005.

Β. Ζησιάδης, Η οικονομική εγκληματικότητα, εκδ. Σάκκουλα, 2002.

Λ. Κανέλλος, Smart Contracts, εκδ. Νομική Βιβλιοθήκη, 2022.

Ι. Καρακώστας, Δίκαιο και Internet, εκδ. Π.Ν. Σάκκουλα - Δίκαιο και Οικονομία, 2009.

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

Ν. Κουράκης, Το έγκλημα της απάτης, εκδ. Νομική Βιβλιοθήκη, 2001.

Θ. Κριθαράς, Ποινικό δίκαιο και διαδίκτυο, εκδ. Νομική Βιβλιοθήκη, 2009.

Ι. Μανωλεδάκης, Η διαλεκτική των εννόμων αγαθών, εκδ. Σάκκουλα, 1973.

Ι. Μανωλεδάκης, Εγκλήματα κατά της ιδιοκτησίας, εκδ. Σάκκουλα, 2002.

Μ. Μαργαρίτης – Α. Μαργαρίτη, Ποινικός Κώδικας Ερμηνεία – Εφαρμογή, εκδ. Π.Ν. Σάκκουλα, 2020.

Ε. Μεταξάκης, Bitcoin – Κρυπτοχρήμα και κυβερνοέγκλημα, εκδ. Αντ. Ν. Σάκκουλα, 2017.

Ε. Μεταξάκης, Κυβερνοέγκλημα, εκδ. Π.Ν. Σάκκουλα, 2022.

Ε. Μπακιρλή, Σύγχρονη Τεχνολογία και Αντεγκληματική Πολιτική, εκδ. Νομική Βιβλιοθήκη, 2019.

Γ. Μπουρμάς σε Α. Χαραλαμπάκη, Ο νέος ποινικός κώδικας, εκδ. Νομική Βιβλιοθήκη, 2020.

Χ. Μυλωνόπουλος, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, εκδ. Αντ. Ν. Σάκκουλα, 1991.

Χ. Μυλωνόπουλος, Ποινικό Δίκαιο - Ειδικό Μέρος, εκδ. Π.Ν. Σάκκουλα, 2016.

Χ. Μυλωνόπουλος, Ποινικό Δίκαιο – Ειδικό Μέρος, εκδ. Νομική Βιβλιοθήκη, 2021.

Ο. Ναμίας, Σύγχρονες μορφές (ηλεκτρονικής) απάτης στις τραπεζικές συναλλαγές, σε Τιμητικό Τόμο Ανδρουλάκη, εκδ. Αντ. Ν. Σάκκουλα, 2003, σελ. 467 επ.

Π. Παναγιωτόπουλος σε Επίκαιρα ζητήματα οικονομικού ποινικού δικαίου, εκδ. Νομική Βιβλιοθήκη, 2021, σελ. 57 επ.

Α. Παπαδαμάκης, Τα περιουσιακά εγκλήματα, εκδ. Σάκκουλα, 2020.

Στ. Παύλου, Τα εγκλήματα περί το νόμισμα, εκδ. Σάκκουλα, 1989.

Στ. Παύλου, Εγκλήματα κατά της ιδιοκτησίας, εκδ. Π.Ν. Σάκκουλα, 2006.

Στ. Παύλου – Ι. Μπέκας, Αν. Αποστολίδου, Ποινικό Δίκαιο – Ειδικό Μέρος, εκδ. Π.Ν. Σάκκουλα, 2020.

Θ. Σάμιος σε Ποινικές Επιστήμες - θεωρία και πράξη: Προσφορά τιμής στην Άννα Μπενάκη Ψαρούδα, Τόμος Β, εκδ. Αντ. Ν. Σάκκουλα, 2008, σελ. 517επ.

Θ. Σάμιος, Κάρτες αυτόματης συναλλαγής και ποινικό δίκαιο, Π.Ν. Σάκκουλα, 2010.

Φ. Σπυρόπουλος, Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking), εκδ. Αντ. Ν. Σάκκουλα, 2016.

Α. Συκιώτου, Το διαδίκτυο ως σύγχρονο όχημα θυματοποίησης, εκδ. Αντ. Ν. Σάκκουλα, 2009.

Σ. Συρμακέζης σε 3ο Πανελλήνιο Συνέδριο της Ε.Ε.Ν. e-Θέμις «Το δίκαιο στην ψηφιακή εποχή», σελ. 109επ. εκδ. Νομική Βιβλιοθήκη, 2012.

Κ. Φράγκος, Ποινικός Κώδικας (Ν. 4619/2019 και Ν. 4637/2019), εκδ. Σάκκουλα, 2020.

Α. Χαραλαμπάκης συν. Γ. Μπουρμάς, Οι αλλαγές του νέου ποινικού κώδικα, εκδ. Νομική Βιβλιοθήκη, 2022.

R. Doswell – G.L. Simons, Πληροφορική και εγκληματικότητα, NCC Publications, 1986.

M. Yar, Cybercrime and society, SAGE Publications, 2013.

Αρθρογραφία:

Ηλ. Αναγνωστόπουλος, ΠοινΧρ ΜΒ (1992), σελ. 197 (παρατηρήσεις επί της εφετειακής απόφασης 1904/1991 του Τριμελούς Εφετείου Αθηνών).

Μ. Καϊάφα – Γκμπάντι, Αρμενόπουλος 61 (2007), σελ. 1080επ.

Γ. Νούσκαλης, Ποινική Δικαιοσύνη 2/2003, σελ. 178επ.

Ε. Συμεωνίδου-Καστανίδου, Υπεράσπιση 8 (1998), σελ. 937επ.

Γ. Μπουρμάς, Ποινικά Χρονικά ΝΑ’ (2001), σελ. 470επ.

Ο. Ναμίας, Ποινικά Χρονικά ΝΓ’ (2003), σελ. 487επ.

Χ. Νικολαΐδης, Αρχείο Νομολογίας ΝΕ' (2004), σελ. 465 επ.

Συμβ.Διαρκ.Στρατ.Θεσ 401/1986 (Ποινικά Χρονικά ΛΣΤ/1986, σελ. 776).

Πλημμ.Αθ. 3668/2006 (Ποινικά Χρονικά ΝΖ/2007, σελ. 271).

Πλημμ.Αθ.1213/2007 (Ποινικά Χρονικά ΝΗ/2008, σελ. 634).

Πλημμ.Αθ. 638/2008 (Ποινικά Χρονικά Ξ/2010, σελ. 775).

Συμβ.Πλημ.Κιλκίς 54/2012 (Ποινική Δικαιοσύνη 2014, σελ. 238).

Ηλεκτρονικά:

Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος, Ιανουάριος 2021, διαθέσιμη σε https://www.bankofgreece.gr/enimerosi/grafeio-typoy/anazhthsh-enhmerwsewn/enhmerwseis?announcement=3933ea6b-1bcd-4a9f-8d7d-caf1a0b2f32e.

Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος, Δεκέμβριος 2021, διαθέσιμη σε https://www.bankofgreece.gr/enimerosi/grafeio-typoy/anazhthsh-enhmerwsewn/enhmerwseis?announcement=fe474159-8c69-4616-94c9-f71674e8bf15.

Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος, Μάϊος 2022, διαθέσιμη σε https://doi.org/10.52903/finsta.gr202205.

Έκθεση Χρηματοπιστωτικής Σταθερότητας της Τράπεζας της Ελλάδος, Νοέμβριος 2022, διαθέσιμη σε https://doi.org/10.52903/finsta.gr202211.

The European Financial and Economic Crime Centre (EFECC): https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc.

Payment Fraud: A low-risk, high-profit criminal activity, payment card fraud can be split into two distinct types: card-not-present fraud, which occurs largely online, and card-present fraud, which typically occurs at retail outlets and ATMs, POS, NFC (Skimming) Sim Swapping: https://www.europol.europa.eu/media-press/newsroom/news/ten-hackers-arrested-for-string-of-sim-swapping-attacks-against-celebrities.

Directive on the fight against fraud to the Union's financial interests by means of criminal law (σελ. 12, 17, 37) Anti money laundering action: The fourth directive EU conclusion. https://uwe-repository.worktribe.com/output/883459/the-robustness-of-eu-financial-crimes-legislation-a-critical-review-of-the-eu-and-uk-anti-fraud-and-money-laundering-scheme.

The scope of the new EU authority explicitly includes crypto assets, given that this is one of the fields more prone to money-laundering activities https://markets.businessinsider.com/news/currencies/crypto-regulator-eu-financial-crime-oversight-money-laundering-exchange-illicit-2022-2.

AML, Money Laundering using NFT's: https://www.acfcs.org/acfcs-special-contributor-report-it-starts-with-art-nfts-money-laundering-and-terrorist-financing/.

The New Digital Art Trade Is Ideal for Criminals: https://news.bloomberglaw.com/white-collar-and-criminal-law/the-new-digital-art-trade-is-ideal-for-criminals.

Financial Crime & Fraud Detection Using AI Computing https://arxiv.org/abs/2103.01854.

https://www.consilium.europa.eu, https://curia.europa.eu, https://www.legifrance.gouv.fr, https://bafin.de, https://www.chd.lu, https://www.cssf.lu, https://www.sif.admin.ch, https://www.irs.gov, https://crsreports.congress.gov, https://www.fatf-gafi.org, https://lawfilesext.leg.wa.gov.

Νομολογία:

ΑΠ 1152/1999

ΑΠ 127/2004

ΑΠ 2530/2008

ΑΠ 355/2009

ΑΠ 1700/2010

ΑΠ 737/2012

ΑΠ 742/2012

ΑΠ 131/2013

ΑΠ 813/2015

ΑΠ 367/2017

ΑΠ 1087/2019

ΑΠ 1726/2019

ΑΠ 562/2020

ΑΠ 734/2021

ΑΠ 1071/2021

ΕφΑθ. 1904/1991

ΕφΑθ. 9474/2002

ΕφΑθ. 5224/2007

ΕφΑθ. 1081/2008

Πλημμ.Αθ. 3668/2006

Πλημμ.Αθ. 1213/2007

Πλημμ.Αθ. 638/2008

ΔιαρκΣτρατΘεσ. 401/1986

ΔιαρκΣτρατΑθ. 2897/1994

Συμβ.Ναυτ.Πειραιώς 418/1996

Συμβ.Πλημμ.Καστοριάς 196/1999

Συμβ.Πλημμ.Κιλκίς 54/2012