ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

«ΤΑ ΑΔΙΚΗΜΑΤΑ ΤΗΣ ΠΛΑΣΤΟΓΡΑΦΙΑΣ ΚΑΙ ΤΗΣ ΑΠΑΤΗΣ ΜΕ ΥΠΟΛΟΓΙΣΤΗ ΣΗΜΕΡΑ»

Επιβλέπων Καθηγητής: κος ΔΑΛΑΚΟΥΡΑΣ ΘΕΟΧΑΡΗΣ
Διπλωματική Εργασία του: ΠΑΝΤΑΛΩΝΑ ΕΥΑΓΓΕΛΟΥ (ΑΜ: mli18016)

Θεσσαλονίκη, Δεκέμβριος 2020

«ΤΑ ΑΔΙΚΗΜΑΤΑ ΤΗΣ ΠΛΑΣΤΟΓΡΑΦΙΑΣ ΚΑΙ ΤΗΣ ΑΠΑΤΗΣ ΜΕ ΥΠΟΛΟΓΙΣΤΗ ΣΗΜΕΡΑ»

Ευάγγελος Ν. Πανταλώνας
Απόφοιτος Νομικής ΑΠΘ, 2014

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 27η/02/2021

Θεοχάρης Δαλακούρας	Μαστροκώστας Χρήστος	Δαγκλής Νικόλαος
.....	.....	.....

Ευάγγελος Πανταλώνας

Περίληψη

Η παρούσα εργασία ασχολείται με την ερμηνεία του αδικήματος της απάτης με υπολογιστή από τη θέσπισή του έως σήμερα, με τη μελέτη του αδικήματος της πλαστογραφίας και τη δυνητική του εφαρμογή στις περιπτώσεις πλαστοποίησης συγκεκριμένων ψηφιακών εγγράφων, καθώς και με τις σύγχρονες μορφές απάτης στο διαδίκτυο, όταν και τελούνται περισσότερα ποινικά αδικήματα με απώτερο σκοπό τον παράνομο προσπορισμό περιουσιακού οφέλους.

Λέξεις Κλειδιά: απάτη, πλαστογραφία, υπολογιστής, διαδίκτυο

Στην Αργυρώ

Περιεχόμενα

Κεφάλαιο 1ο: Εισαγωγή - Σκοπός Μελέτης

Η διάδοση της χρήσης των ηλεκτρονικών υπολογιστών, η ταχύτατη διασπορά της πρόσβασης στο διαδίκτυο, η έκρηξη της νέας ψηφιακής οικονομίας σε συνδυασμό με την εκτόξευση της ταχύτητας της εξέλιξης των σχετιζόμενων με το διαδίκτυο τεχνολογιών (Big Data, IoT) οδήγησε μεταξύ άλλων και στον πολλαπλασιασμό και την εμφάνιση νέων μορφών ηλεκτρονικής εγκληματικότητας (π.χ. απάτης με υπολογιστή, hacking/cracking, πλαστογραφία, που γίνεται μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών)[1]. Και αυτό συνέβη είτε επειδή με την ανάπτυξη της τεχνολογίας και της πληροφορικής κατέστη πλέον ευκολότερη η τέλεση των «συμβατικών εγκλημάτων» (τα κοινά εγκλήματα που διαπράττονται μέσω η/υ), είτε επειδή εμφανίστηκαν νέες μορφές εγκλημάτων με αμιγώς ψηφιακό χαρακτήρα (τα λεγόμενα γνήσια εγκλήματα κυβερνοχώρου)[2].

Σύμφωνα δε με τα στατιστικά στοιχεία της Eurostat[3], 87% των Ευρωπαϊκών νοικοκυριών έχουν πρόσβαση στο Διαδίκτυο, ενώ το αντίστοιχο ποσοστό για τα Ελληνικά νοικοκυριά ανέρχεται στο 71%. Περισσότεροι επομένως από 7 στους 10 Έλληνες είναι τουλάχιστον συμβατικοί χρήστες του Διαδικτύου, ήτοι κάνουν χρήση ιστοσελίδων, e-mail, ηλεκτρονικών καταστημάτων κ.ο.κ.. Δεδομένου δε του ότι οι περισσότεροι εκ των χρηστών ήταν ήδη ενήλικες όταν η χρήση του διαδικτύου κατέστη προσβάσιμη στο ευρύ κοινό (λίγο μετά το 2000) είναι σαφές ότι η πλειοψηφία των χρηστών αυτών είναι αυτοδίδακτοι και ελάχιστα γνωρίζουν περί των κινδύνων που υφίστανται κατά τη χρήση του διαδικτύου. Βέβαια, η «ηλεκτρονική εγκληματικότητα» δεν εμφανίστηκε ταυτόχρονα με την διάδοση της χρήσης του διαδικτύου, αλλά ταυτόχρονα με την έναρξη ευρύτερης χρήσης των ηλεκτρονικών υπολογιστών, περί τα τέλη της δεκαετίας του ’80, όταν και οι χρήση ηλεκτρονικών υπολογιστών και αντίστοιχων συστημάτων άρχισε να εδραιώνεται στις μεγάλες επιχειρήσεις, στα πιστωτικά ιδρύματα κτλ.

Όπως συμβαίνει πάντοτε, και είναι και λογικό λόγω της αρχής “nullum crimen sine lege”, η ποινικοποίηση των εγκληματικών συμπεριφορών έπεται της εμφάνισής

---

[1] *Σιδηρόπουλος Θ.,* Το δίκαιο του διαδικτύου (internet), 2η έκδ., σ. 33 επ.

[2] *Σιδηρόπουλος Θ.,* ό.π. σ. 33 επ. Για τη διάκριση των ηλεκτρονικών εγκλημάτων (computer crime, cyber crime, internet related crime κλπ) βλ. *Αγγελή Ι.*, Διαδίκτυο και Ποινικό δίκαιο. Έγκλημα στον κυβερνοχώρο, ΠοινΧρον Ν΄, σ. 676 -677.

[3] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals/el

τους[4]. Όταν επομένως εμφανίστηκαν συγκεκριμένες συμπεριφορές, όπου κάποιος επενέβαινε σε υπολογιστικά προγράμματα με δόλιο τρόπο, επηρεάζοντας δεδομένα ή/και διαδικασίες, προκειμένου να αποκομίσει οποιοδήποτε όφελος (περιουσιακό ή και όχι), αλλά οι συγκεκριμένες συμπεριφορές και πράξεις δεν πληρούσαν στο σύνολό τους την αντικειμενική υπόσταση κάποια ποινικής διάταξης, έγινε αντιληπτό από το σύνολο του νομικού κόσμου ότι είχε έρθει η ώρα να καθορίσει ο νόμος τα όρια των ανθρώπινων συμπεριφορών και στον ηλεκτρονικό κόσμο. Έτσι, ο Έλληνας νομοθέτης, με το Ν. 1805/1988 εισήγαγε στον ποινικό μας κώδικα νέες διατάξεις, που θα κάλυπταν τα διάφορα κενά του νόμου ως προς συγκεκριμένες συμπεριφορές. Μεταξύ άλλων λοιπόν θεσπίσθηκε και η διάταξη του άρθρου 386^{Α} ΠΚ με τίτλο «Απάτη με Υπολογιστή», η οποία θα αποτελεί και το θέμα της παρούσας εργασίας στα πρώτα κεφάλαιά της. Η συγκεκριμένη διάταξη θεσπίσθηκε προκειμένου να καλυφθούν εκείνα τα κενά νόμου που δεν επέτρεπαν να εφαρμοσθεί η διάταξη της απάτης (386 ΠΚ)[5].

Αντίστοιχα και όταν εμφανίστηκαν συγκεκριμένες συμπεριφορές, όπου κάποιος άνευ δικαιώματος είτε αντέγραφε ή αλλοίωνε λογισμικά (λ.χ. προγράμματα ηλεκτρονικών υπολογιστών/ιστοσελίδες) με αποτέλεσμα την παραγωγή μη αυθεντικών δεδομένων με σκοπό να λαμβάνονται υπόψη ως αυθεντικά, είτε κατήρτιζε πλαστά ηλεκτρονικά έγγραφα και λογισμικά κλπ., έγινε αντιληπτό από το σύνολο του νομικού κόσμου ότι είχε έρθει η ώρα, εξαιτίας της ραγδαίας ανάπτυξης της τεχνολογίας και της υποκατάστασης της γραφής από σύγχρονα μέσα αποτύπωσης της ανθρώπινης σκέψης, να επέμβει ο νομοθέτης διευρύνοντας την έννοια του εγγράφου κατά τη διάταξη του άρθρου 13γ ΠΚ, ώστε να περιλαμβάνονται πλέον σε αυτήν και τα ψηφιακά δεδομένα. Αυτό έχει ως αποτέλεσμα, κατά την πλαστογράφηση των δεδομένων, ιστοσελίδων κλπ, να αντιμετωπίζονται τέτοιου είδους συμπεριφορές βάσει των εγκλημάτων σχετικά με τα υπομνήματα και να επιτυγχάνεται έτσι μία πλήρης προστασία από τέτοιες συμπεριφορές, που πριν την εν λόγω τροποποίηση ίσως παρέμεναν ατιμώρητες.

Ειδικότερα, στο 2^{ο} και 3^{ο} κεφάλαιο της παρούσας θα αναφερθούν τα νομικά εκείνα ζητήματα που οδήγησαν το νομοθέτη στη θέσπιση του ιδιώνυμου εγκλήματος

[4] βλ. συναφώς *Αγγελή Ι.*, ΠοινΧρον Ν΄, σ. 678, όπου αναφέρεται: *«στο ποινικό δίκαιο οι έννομες τάξεις έρχονται εκ των υστέρων να ρυθμίσουν νομοθετικώς τις καταστάσεις, πιεζόμενες από τα πράγματα… Πολλά από τα εγκλήματα που έχουν παρουσιαστεί στο διαδίκτυο, δεν μπορούν να αντιμετωπιστούν με την συμβατική νομοθεσία, στο χώρο τουλάχιστον του ποινικού δικαίου».*

[5] *Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σελ. 180

της απάτης με υπολογιστή (386^{A} ΠΚ) στην αρχική και στη σημερινή του μορφή, ενώ στο 4^{ο} κεφάλαιο θα αναλυθεί εκτενώς η αντικειμενική και η υποκειμενική του υπόσταση (386Α ΠΚ) καθώς και η σχέση του με την κοινή απάτη (386 ΠΚ). Στο κεφάλαιο δε που ακολουθεί (5^{ο}) θα αναλυθεί το αδίκημα της πλαστογραφίας και η διευρυμένη πλέον έννοια του εγγράφου κατά το άρθρο 13 γ ΠΚ, ενώ στο 6^{ο} κεφάλαιο θα αναφερθούμε στην πλαστογραφία ως μέσο τέλεσης της απάτης και της απάτης με η/υ στις σύγχρονες μορφές εγκληματικότητας. Τέλος, στο 7^{ο} κεφάλαιο θα καταγραφούν τα συμπεράσματα του γράφοντος σχετικά με τα διάφορα ζητήματα που θα αναφερθούν.

Κεφάλαιο 2ο: Η Εισαγωγή του άρθρου 386Α ΠΚ (Ν. 1805/1988) – Η επιρροή του Γερμανού Νομοθέτη

Το άρθρο 386Α ΠΚ, όπως προστέθηκε στον Ποινικό μας Κώδικα με το άρθρο 5 του Ν. 1805/1988 (ΦΕΚ Α 199) και εφαρμόσθηκε έως την αντικατάστασή του με το άρθρο δεύτερο παρ.11 Ν.4411/2016, ΦΕΚ Α 142/3.8.2016, είχε την εξής μορφή:

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

2.1. Εισαγωγή

Η θεσμοθέτηση της διάταξης του άρθρου 386Α ΠΚ (απάτης με η/υ), που εισήχθη με το ν. 1805/1988, κρίθηκε αναγκαία προκειμένου να καλυφθούν τα κενά νόμου που ανέκυψαν στην πράξη με τη ραγδαία ανάπτυξη της τεχνολογίας και των συστημάτων ηλεκτρονικών πληρωμών, και που συνίσταντο στην αδυναμία της διάταξης της κοινής απάτης (386 ΠΚ) να καλύψει παράνομες συμπεριφορές, που διαπιστώνονταν ολοένα και συχνότερα στις σύγχρονες μορφές οικονομικής ηλεκτρονικής εγκληματικότητας, δηλαδή περιπτώσεις προσβολών της περιουσίας με τη χρήση ηλεκτρονικού υπολογιστή στις οποίες δεν παρενέβαινε εξαπάτηση φυσικού προσώπου[6].

Πιο συγκεκριμένα, στο διάστημα προ της θέσπισης του ανωτέρω νόμου, τόσο η θεωρία όσο και η νομολογία κλήθηκαν να χαρακτηρίσουν ποινικά συγκεκριμένες, φανερά έκνομες συμπεριφορές, οι οποίες σχετίζονταν με ηλεκτρονικούς υπολογιστές. Λόγω όμως της αρχής «κανένα έγκλημα δίχως νόμο», καλούνταν να αντιμετωπίσουν τις συμπεριφορές αυτές με το τότε υφιστάμενο ποινικό οπλοστάσιο, το οποίο όμως είχε καταστεί πλέον «ξεπερασμένο», σε σχέση με το «οπλοστάσιο» των ηλεκτρονικών εγκληματιών.

[6] *Νούσκαλης Γ.,* ΠοινΔικ 2003, σελ. 180· *Ναμίας Ο.,* Σύγχρονες μορφές ηλεκτρονικής απάτης στις Τραπεζικές συναλλαγές, ΠοινΧρ 2003,489.

2.2. Η νομική πραγματικότητα προ της θέσπισης του εγκλήματος της «Απάτης με Υπολογιστή»

Μετά την τοποθέτηση των πρώτων Αυτόματων Ταμειολογιστικών Μηχανών (Automated Teller Machine- εφεξής ATM) στην Ελλάδα το έτος 1983 από την Alpha Bank[7], και την σταδιακή τους εξάπλωση, ήταν φυσικό επακόλουθο να αρχίσουν να εμφανίζονται και οι πρώτες «απάτες» σχετικές με τις μηχανές αυτές.

Έτσι, τα Ελληνικά Δικαστήρια εκλήθησαν να ερμηνεύσουν υπό το πρίσμα του ποινικού δικαίου δύο συχνά εμφανιζόμενες στην πράξη περιπτώσεις: τη λήψη χρημάτων από ATM, είτε με τη χρήση ξένης μαγνητικής κάρτας και του μυστικού κωδικού αριθμού της χωρίς εξουσιοδότηση από τον δικαιούχο, είτε με τη χρήση μαγνητικής κάρτας από τον ίδιο τον δικαιούχο πλην όμως καθ' υπέρβαση του πιστωτικού υπολοίπου της κάρτας.

Κατά το ίδιο χρονικό διάστημα (δεκαετία 1980-1990), και η θεωρία είχε προβληματιστεί για τα συγκεκριμένα ζητήματα, καθώς και με το εάν πράγματι μπορούσε να διωχθεί ποινικά ο μη δικαιούχος χρήστης κάρτας με το ισχύον τότε ποινικό οπλοστάσιο[8]. Αντίστοιχα, έως τη θέσπιση του Ν. 1805/1988, συμπεριφορές όπως η ενέργεια τραπεζικού υπαλλήλου να μεταφέρει λογιστικές μονάδες από λογαριασμό κάποιου πελάτη της τράπεζας σε λογαριασμό άλλου πελάτη της τράπεζας και η ανάληψή τους από τον δεύτερο, ήταν δύσκολο να διωχθούν ποινικά, αφού δεν πληρούταν η αντικειμενική υπόσταση των κατά το χρόνο εκείνο σχετικών τυποποιημένων αδικημάτων (κλοπή, υπεξαίρεση ή απάτη).

Το μείζον νομικό ζήτημα, το οποίο καθιστούσε την ανωτέρω πράξη μη διώξιμη ποινικά, τουλάχιστον ως προς το αδίκημα της απάτης, ήταν ότι στις συμπεριφορές, που κάποιος «εξαπατούσε» έναν η/υ (κλασσικό παράδειγμα η μη δήλωση της αποφοίτησης ενός τέκνου προκειμένου να συνεχίζεται η είσπραξη φοιτητικού επιδόματος από τον γονέα[9]), εξέλιπε τόσο το στοιχείο της «πλάνης του φυσικού προσώπου», όσο και της «πράξης παράλειψης ή ανοχής» του παραπλανώμενου φυσικού προσώπου, η οποία ενείχε περιουσιακή διάθεση, αμφότερα τα οποία αποτελούσαν στοιχεία της αντικειμενικής υπόστασης της συμβατικής απάτης του 386ΠΚ[10]. Εφόσον λοιπόν, προ του Ν. 1805/1988, κάποιος παρέμβαινε αθεμίτως στην πορεία μιας διαδικασίας

[7] https://www.sansimera.gr/articles/1252 -προσπέλαση στις 14-11-2020
[8] *Γιαννόπουλος Θ.,* Όψεις και προβλήματα της ηλεκτρονικής εγκληματικότητας ΝοΒ 34(1986), 173
[9] *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 3η έκδ., άρθρ. 386Α, αρ 7
[10] *Ναμίας Ο.,* Σύγχρονες μορφές ηλεκτρονικής απάτης στις Τραπεζικές συναλλαγές, ΠοινΧρ 2003,489.

επεξεργασίας δεδομένων σε η/υ, η οποία από μόνη της επέφερε ζημία εις βάρος τίνος (δεν επέμβαινε δηλαδή φυσικό πρόσωπο μετά τη λήξη της διαδικασίας στον η/υ και πριν την περιουσιακή διάθεση), η πράξη αυτή παρέμενε ατιμώρητη.

2.3. Η θέσπιση του εγκλήματος της «Απάτης με Υπολογιστή»: Οι τυποποιούμενοι τρόποι τέλεσης και η σύγκριση με την αντίστοιχη Γερμανική διάταξη.

Προκειμένου να μην μένουν ατιμώρητες στην ελληνική έννομη τάξη πράξεις ηλεκτρονικής εγκληματικότητας πρωτόγνωρες για την εποχή, διαμορφώθηκε και θεσπίστηκε το ιδιώνυμο[11] έγκλημα της απάτης με υπολογιστή (386^{A} ΠΚ), ακολουθώντας ως πρότυπο την αντίστοιχη γερμανική διάταξη του άρθρου 263a του Γερμανικού Ποινικού Κώδικα (263a StGB), η οποία είχε εισαχθεί στη Γερμανία νωρίτερα κατά δύο χρόνια[12].

Ως πράξη απάτης με υπολογιστή, κατά την έννοια του άρθρου 386^{A} ΠΚ –στην αρχική του μορφή- ήταν η πρόκληση βλάβης με τον «επηρεασμό των στοιχείων του υπολογιστή». Αυτός δε ο επηρεασμός με την σειρά του μπορούσε να τελεστεί με έναν από τους διαζευκτικά αναφερόμενους τρόπους: α) της μη ορθής διαμόρφωσης του προγράμματος, β) της επέμβασης κατά την εφαρμογή του, γ) της χρησιμοποίησης μη ορθών ή ελλιπών στοιχείων και δ) με οποιονδήποτε άλλον τρόπο. Με απώτερο επομένως σκοπό να τιμωρηθούν και οι στο μέλλον αναφυόμενες πράξεις, που απορρέουν από τις δυνατότητες της τεχνολογίας της πληροφορικής, ο νομοθέτης θέσπισε ως τρόπο τέλεσης και τον «με οποιονδήποτε άλλο τρόπο» επηρεασμό των στοιχείων του υπολογιστή. Διαφοροποιήθηκε κατά τον τρόπο αυτόν από τον γερμανό νομοθέτη, ο οποίος όχι μόνο δεν είχε προβεί στην ευρεία αυτή αόριστη διατύπωση, αλλά αντιθέτως είχε προβλέψει ρητά ως τρόπο τέλεσης στην αντίστοιχη γερμανική διάταξη την περίπτωση της χωρίς δικαίωμα χρήσης στοιχείων/δεδομένων.

Ενόψει της παράλειψης αυτής του Έλληνα νομοθέτη να προβλέψει ρητά ως τρόπο τέλεσης της απάτης με η/υ «τη χωρίς δικαίωμα χρήση στοιχείων ή δεδομένων», διατυπώθηκαν σοβαρές αντιρρήσεις ως προς την εφαρμογή της εν λόγω διάταξης (απάτης με η/υ) για την αντιμετώπιση του ήδη γνωστού τότε ζητήματος της ανάληψης χρημάτων από ΑΤΜ με κλεμμένη μαγνητική κάρτα ή από τον ίδιο τον δικαιούχο καθ' υπέρβαση του πιστωτικού υπολοίπου της κάρτας. Χαρακτηρίστηκε έτσι ατυχώς η πρώτη πράξη (ανάληψη χρημάτων από ΑΤΜ με κλεμμένη μαγνητική κάρτα) ενίοτε ως

[11] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, 2000, σ. 182· *Κουράκης Ν,* Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001, σ. 2591.

[12] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, 2000, σ. 182-183· *Ναμίας Ο.,* ό.π., ΠοινΧρ 2003, 489.

κλοπή[13], ενίοτε ως υπεξαίρεση[14], ενώ η δεύτερη (ανάληψη χρημάτων από ΑΤΜ από τον ίδιο τον δικαιούχο καθ' υπέρβαση του πιστωτικού υπολοίπου της κάρτας) ως κλοπή[15]. Κοινή δε αφετηρία όλων των αντιρρήσεων και των διαφοροποιημένων απόψεων –ενόψει και της ανυπαρξίας ρητής πρόβλεψης της «χωρίς δικαίωμα χρήσης» ως τρόπο τέλεσης-, αποτελεί η αμφιβόλου κατ' αρχήν ορθότητας θέση, ότι στις περιπτώσεις αυτές (: χωρίς δικαίωμα χρήση) δεν υπάρχει «επηρεασμός» των στοιχείων του υπολογιστή[16]. Βέβαια πολλούς υποστηρικτές βρήκε ήδη από τότε και η, ορθή κατά τη γνώμη του γράφοντος, θέση ότι «η χωρίς δικαίωμα χρήση δεδομένων» συνιστά απάτη με υπολογιστή[17].

---

[13] ΕφΑθ 1904/1991 ΠοινΧρ 1992, 196 (παρατ. Αναγνωστόπουλου), όπου έκρινε ότι η χωρίς δικαίωμα χρήση συνιστά κλοπή και όχι απάτη. Συνιστά δηλαδή αφαίρεση ξένου κινητού πράγματος (χρημάτων) από την κατοχή άλλου (της Τράπεζας) · Ομοίως και ΑΠ 2530 / 2008 –ΝΟΜΟΣ. Αντιθ. *Μυλωνόπουλος*, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, σελ. 58, όπου αναφέρει ότι εν προκειμένω ελλείπει το απαραίτητο για τη στοιχειοθέτηση του εγκλήματος της κλοπής στοιχείο, δηλαδή η αφαίρεση (θραύση ξένης κατοχής και θεμελίωση νέας), αφού η τράπεζα στην πραγματικότητα συγκατατίθεται στην παράδοση των χρημάτων μέσω του ΑΤΜ, αφού το μηχάνημα λειτούργησε «κανονικά», όπως εξαρχής είχε προγραμματιστεί, και όπως ακριβώς θα γινόταν και αν ο χρήστης της κάρτας ήταν ο πραγματικός δικαιούχος.

[14]ΔιαρκΣτρατΑθ 2897/1994 ΠοινΧρ 1994, 1465 (με σύμφωνη πρόταση Κονιδάρη), όπου το δικαστήριο δέχτηκε ότι η πράξη αυτή συνιστά υπεξαίρεση και όχι απάτη με υπολόγιστή, διότι δεν προκαλεί επηρεασμό των στοιχείων του υπολογιστή κατά το άρθρο 386^{Α} ΠΚ, ως «απόκλιση από την κανονική και σύννομη εκτέλεση του προγράμματος», διότι ο «υπολογιστής με βάση τα δεδομένα και τον προγραμματισμό του αναγνωρίζει ως δικαιούχο κάθε χρήστη ορθών δεδομένων…».

[15] Διαρκές Στρατοδικείο Θεσσαλονίκης 401/1986Συμβ, Ποιν Χρ. ΛΣΤ, 776

[16]Η θέση αυτή φαίνεται να ήταν και η κρατούσα, βλ. συναφώς *Παπαδαμάκης Α.,* ό.π. σ. 189-190· *Αναγνωστόπουλου Ηλ.,* Παρατηρήσεις στην ΕφΑθ 1904/1991, ΠοινΧρον ΜΒ΄(1992), 197 · ΒουλΣυμβΔΣΑθ 2897/1994 με πρόταση Κονιδάρη Κ., ΠοινΧρον ΜΔ΄(1994), 1464 ·ΒουλΣυμβΔΣΘες 401/1986, ΠοινΧρον ΛΣΤ΄(1986), 774 με πρόταση Αδ. Παπαδαμάκη · *Ναμίας Ο.,* ό.π., ΠοινΧρ 2003, 490. Αντιθ. Συμβ.Ναυτ.Πειραιώς 418/1996: όπου κρίνει ότι η από μη δικαιούχο ανάληψη χρημάτων από μηχάνημα αυτόματης συναλλαγής τραπέζης συνιστά απάτη με υπολογιστή. Αναφέρει χαρακτηριστικά: *«ο δράστης «πληροφορεί» κατά συμπερασματικά συναγόμενο τρόπο τον υπολογιστή ότι έχει ένα δικαίωμα είτε ως προς την πιστωτική κάρτα είτε ως προς το ποσό αυτό, το οποίο στην πραγματικότητα δεν έχει. Με άλλα λόγια «δηλώνει» έμμεσα ότι έχει δικαίωμα να εισάγει τα πιο πάνω δεδομένα και να προκαλέσει αντίστοιχη επεξεργασία τους με τη συναίνεση του δικαιούχου, πράγμα που δεν συμβαίνει στην πραγματικότητα έτσι υπάρχει συμπεριφορά εγκείμενη σε επηρεασμό της επεξεργασίας των στοιχείων και πρόσφορη να βλάψει την περιουσία του τελικά ζημιωμένου» (την άποψη αυτή διατύπωσε ως ανωτέρω ο Χρ. Μυλωνόπουλος, ό.π. σ. 66-67»).*

[17]*Μυλωνόπουλος,* Ποινικό Δίκαιο – Ειδικό Μέρος,2016, σ. 552: όπου αναφέρει χαρακτηριστικά ότι η ευρεία διατύπωση της διάταξης -«με οποιονδήποτε άλλο τρόπο»-, επιτρέπει την υπαγωγή σ' αυτήν και περιπτώσεων επηρεασμού ακόμη και με σύννομη χρήση ορθών στοιχείων (= κανονική αλλά χωρίς δικαίωμα εκτέλεση προγράμματος. Ομοίως και *Κουράκης*, ό.π., ΠοινΛογ 2001, σ. 2594 όπου ωστόσο αναφέρει ότι κατά την γνώμη του θα ήταν σκόπιμο η υπό συζήτηση περίπτωση (της «χωρίς δικαίωμα χρήση») να ενταχθεί στην υποπερίπτωση γ΄ του άρθρου 686^{Α} ΠΚ, δηλαδή αυτή που αφορά χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, άρα στοιχείων που δεν ανταποκρίνονται εν όλω ή εν μέρει στην πραγματικότητα. Τούτο διότι ο ίδιος θεωρεί ότι η τελευταία υποπερίπτωση («με οποιονδήποτε άλλο τρόπο») θα πρέπει να αποτελέσει ασφαλιστική δικλείδα για καταστάσεις επηρεασμού στοιχείων του υπολογιστή που δεν έχουν ακόμα μορφοποιηθεί, και ούτε θα μπορούσαν να προβλεφθούν από τον ιστορικό νομοθέτη, αλλά ανάγονται στο μέλλον, ενόψει της πιθανολογούμενης μελλοντικής τεχνολογικής ανάπτυξης στον τομέα της πληροφορικής.

Ενώ λοιπόν στον γερμανικό ποινικό κώδικα, προβλέφθηκε ρητά ως τρόπος τέλεσης της απάτης με η/υ, ήδη από το 1986, η ήδη γνωστή τότε περίπτωση «ανάληψης χρημάτων από ΑΤΜ τραπέζης με χρήση κλεμμένης μαγνητικής κάρτας» (:*χωρίς δικαίωμα χρήση δεδομένων*), κάτι τέτοιο δεν συνέβη με την αντίστοιχη ελληνική διάταξη, που προέβλεψε -στην αρχική μορφή της- την γενική, αόριστη και ως εκ τούτου προβληματική και αμφίβολης συνταγματικότητας[18], διατύπωση *«επηρεασμός στοιχείων υπολογιστή με οποιονδήποτε άλλο τρόπο».*

Η αστοχία της διατύπωσης της διάταξης από τον Έλληνα νομοθέτη γίνεται ιδιαίτερα αντιληπτή, εάν αναλογιστεί κανείς ότι η πράξη «ανάληψης χρημάτων από ΑΤΜ με χρήση κάρτας από μη νόμιμο δικαιούχο», που θα μελετηθεί σε επόμενο κεφάλαιο, ήτοι η πράξη της «*χωρίς δικαίωμα χρήσης δεδομένων»*, ήταν από τις πρώτες περιπτώσεις που κλήθηκε να αντιμετωπίσει η ελληνική νομολογία. Πλην όμως η αντιμετώπιση της συγκεκριμένης «αστοχίας» καθυστέρησε αρκετά.

Ενόψει δε των παραπάνω παρατηρήσεων, δεν θα έπρεπε να αποκλειστεί το ενδεχόμενο να αποδοθεί η διαφοροποίηση της ελληνικής διάταξης στην αρχική μορφή της σε σχέση με την «πρότυπη» γερμανική, στην προχειρότητα και ατυχή επιλογή του Έλληνα νομοθέτη[19].

2.4. Ειδικά περί της γενικής ρήτρας *«με οποιοδήποτε άλλο τρόπο»* ως επιμέρους τρόπο τέλεσης του εγκλήματος.

Η επιλογή του Έλληνα νομοθέτη να καθιερώσει ως επιμέρους τρόπο τέλεσης τον «*με οποιοδήποτε άλλο τρόπο* - πέραν των ρητώς αναφερόμενων στη διάταξη- *επηρεασμό των στοιχείων υπολογιστή»*, ήταν αυτή που προκάλεσε θεωρητικές και νομολογιακές διχογνωμίες, τροφοδοτώντας τη νομική συζήτηση γύρω από το έγκλημα της απάτης με υπολογιστή, έως και την αντικατάσταση της διάταξης το 2016. Ειδικότερα, η συζήτηση και οι διχογνωμίες περιστρέφονταν αφενός γύρω από το ποιες συγκεκριμένες πράξεις μπορεί να θεωρηθεί ότι εμπίπτουν στον «*οποιονδήποτε άλλο τρόπο»,* αφετέρου γύρω από το αν η ένταξη στον «*οποιοδήποτε άλλο τρόπο»* οποιασδήποτε πράξης που δε τυποποιείται ρητά στο νόμο θα οδηγούσε σε

[18]Βλ. *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 3η έκδ., άρθρ. 386Α, αρ 8: *«το οριζόμενο «είτε με οποιονδήποτε άλλο τρόπο»: φαίνεται αμφίβολης συνταγματικότητας, αφού δεν φαίνεται να ανταποκρίνεται πλήρως στην lege certa.».*

[19] *Ναμίας Ο.,* Σύγχρονες μορφές ηλεκτρονικής απάτης στις Τραπεζικές συναλλαγές, ΠοινΧρ 2003,492-493.

απαγορευμένη διασταλτική συμπλήρωση του γράμματος της διάταξης και άρα παραβίαση της αρχής «καμιά ποινή δίχως νόμο»[20].

2.5. Η χαρακτηριστική περίπτωση της «Χρήσης κλεμμένης κάρτας ΑΤΜ». Θεωρητικές και νομολογιακές προσεγγίσεις.

Όπως προελέχθη, η ύπαρξη στη διάταξη του 386Α του *«με οποιοδήποτε άλλο τρόπο»* τρόπου τέλεσης του συγκεκριμένου αδικήματος, οδήγησε σε θεωρητικές συγκρούσεις αλλά και διαφορετικές δικαστικές κρίσεις. Χαρακτηριστικότερο παράδειγμα των διαφορών αυτών που εκκινούσαν από την αόριστη διατύπωση του νόμου, ήταν ο νομικός χαρακτηρισμός της χρήσης κλεμμένης χρεωστικής ή πιστωτικής κάρτας για ανάληψη χρημάτων ή αγορές, περίπτωση που όπως προαναφέρθηκε είχε κληθεί να αντιμετωπιστεί η νομολογία και προ της εισαγωγής του άρθρου 386Α στον Ποινικό μας Κώδικα[21].

Ειδικότερα, ο Μυλωνόπουλος στην ερμηνεία που δίνει για το συγκεκριμένο τρόπο τέλεσης (: «με οποιοδήποτε άλλο τρόπο») αναφέρει ότι η ευρεία διατύπωση που δίνει ο νόμος «*επιτρέπει την υπαγωγή σε αυτήν και περιπτώσεων επηρεασμού ακόμη και με μη σύννομη χρήση ορθών στοιχείων (=κανονική αλλά χωρίς δικαίωμα εκτέλεση προγράμματος)»*, φέροντας ως παράδειγμα την κλεμμένη μαγνητική κάρτα και την κανονική αλλά μη σύννομη έναρξη διαδικασίας επεξεργασίας των στοιχείων υπολογιστή.[22] Κατά τον ίδιο, στην περίπτωση της κλεμμένης μαγνητικής κάρτας, ο δράστης «πληροφορεί» κατά συμπερασματικά συναγόμενο τρόπο τον υπολογιστή ότι έχει ένα δικαίωμα ως προς την πιστωτική κάρτα, το οποίο στην πραγματικότητα δεν έχει. Με άλλα λόγια «δηλώνει» έμμεσα ότι έχει δικαίωμα να εισάγει τα πιο πάνω δεδομένα και να προκαλέσει αντίστοιχη επεξεργασία τους με τη συναίνεση του δικαιούχου, πράγμα που δεν συμβαίνει στην πραγματικότητα, με αποτέλεσμα να υπάρχει έτσι συμπεριφορά εγκείμενη σε επηρεασμό της επεξεργασίας των στοιχείων και πρόσφορη να βλάψει την περιουσία του τελικά ζημιωμένου[23]. Κατά την άποψη συνεπώς αυτή όντως υφίσταται επηρεασμός, με την έννοια ότι εισάγονται στοιχεία τα οποία ναι μεν είναι γνήσια και ορθά καθ' εαυτά, αλλά όχι σε σχέση με τον νόμιμο

[20] *Παπαδαμάκης Α,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σελ 187

[21] Βλ. ανωτέρω, κεφάλαιο 2.2.

[22] *Μυλωνόπουλος,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ 552-553. Αντιθ. *Κουράκης Ν,* ΠοινΛογ 2001, σ. 2594, ο οποίος υιοθετεί δική του θέση, υποστηρίζοντας ότι θα ήταν σκόπιμο η συγκεκριμένη περίπτωση (της κλεμμένης μαγνητικής κάρτας) να ενταχθεί στην υποπερίπτωση (γ) του α. 386Α, δηλ. σε αυτή που αφορά χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, στοιχείων δηλαδή που δεν ανταποκρίνονται εν όλω ή εν μέρει στην πραγματικότητα.

[23] *Μυλωνόπουλος Χ.,* Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ. 66επ.

σύνδεσμο που πρέπει να υπάρχει ανάμεσα στον κομιστή της κάρτας και στον δικαιούχο της, ώστε τελικά να υπάρχει διάσταση με την πραγματικότητα. Την άποψη αυτή φαίνεται να ενστερνίζονται και άλλοι θεωρητικοί, που δέχονται την δομική ομοιότητα της απάτης με η/υ προς την απάτη[24].

Αντίθετα, ο Παπαδαμάκης θεωρούσε ότι οι περιπτώσεις που θα πρέπει να εμπίπτουν στο συγκεκριμένο τρόπο τέλεσης θα πρέπει να αφορούν «τρόπο- μεθόδευση επηρεασμού του υπολογιστή και όχι απλή εκμετάλλευση των δυνατοτήτων του», αναφέροντας ρητά ότι η χρήση κλεμμένης κάρτας αποτελεί απλή εκμετάλλευση της αυτοματοποιημένης μηχανικής λειτουργίας του υπολογιστή, αφού, κατά τη γνώμη του, δεν είναι ο υπολογιστής που, κατ' απόκλιση του προγραμματισμού του, προκαλεί την περιουσιακή βλάβη[25], καθώς αυτός (ο υπολογιστής) συνεχίζει να λειτουργεί, όπως εξαρχής προγραμματίστηκε[26]. Προσθέτει δε στην ανωτέρω άποψη, ότι «*τυχόν ταύτιση της απλής εκμετάλλευσης με τον επηρεασμό ίσως οδηγεί και σε απαγορευμένη διασταλτική συμπλήρωση του γράμματος διάταξης*»[27]. Την άποψη αυτή ακολούθησαν, κατά τη δεκαετία 1990-2000 και άλλοι θεωρητικοί, όπως ο Αναγνωστόπουλος (Παρατηρήσεις στην ΕφΑθ 1904/1991, ΠοινΧρον 1992.197) και ο Παύλου (Παρατηρήσεις στο ΣυμβΝαυτΠειρ 418/1996, Υπεράσπιση 1997.111 επ.).

Αντίστοιχες διακυμάνσεις παρατηρήθηκαν και στη νομολογία. Για παράδειγμα, η υπ' αριθμ. 2897/1994 απόφαση του Διαρκούς Στρατοδικείου Αθηνών (σε συμβούλιο) έκρινε ότι η ανάληψη από μη δικαιούχο χρημάτων από ΑΤΜ συνιστά υπεξαίρεση και όχι απάτη με υπολογιστή, θεωρώντας ότι (σ.σ. ο κατηγορούμενος) «*δεν επηρέασε τα στοιχεία υπολογιστή για να προσπορίσει στον εαυτό του παράνομο περιουσιακό όφελος*[28].

---

[24] Ότι δηλαδή ο δράστης «εξαπατά» τον η/υ με μία ψευδή πληροφορία για δικαίωμα που δεν έχει, όπως αντίστοιχα με τη συμπεριφορά του αυτή θα εξαπατούσε τον υπάλληλο της Τράπεζας, εάν είχε τελεστεί με συναφή συναγόμενη βούληση ενώπιον του, βλ. *Κιούπη,* Ποινικό Δίκαιο και ίντερνετ, σελ. 116· *Βασιλάκη,* Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, σελ. 213.

[25] *Παπαδαμάκης,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σ. 189 επ.· βλ. όμως *Νούσκαλη,* ΠοινΔικ 2003, σελ. 186, όπου διατύπωσε έντονες επιφυλάξεις, αναφέροντας ότι ο ισχυρισμός αυτός δεν προσφέρει ικανοποιητική απάντηση, αφού ποια είναι τα όρια ανάμεσα στην «εκμετάλλευση» και στην «επίδραση των στοιχείων». «Εκμετάλλευση» των δυνατοτήτων της τεχνολογίας υπάρχει σε κάθε μορφή της σύγχρονης ηλεκτρονικής οικονομικής εγκληματικότητας μέσω αυτοματοποιημένων συστημάτων πληρωμών. Πάντοτε το πρόγραμμα λειτουργεί κανονικά βάσει εντολών. Εκείνο που είναι αντικανονικό είναι η χρήση χωρίς δικαίωμα ορισμένων δεδομένων και το εξ' αυτών παραγόμενο αποτέλεσμα, δηλαδή η παράνομη περιουσιακή βλάβη.

[26] *Παπαδαμάκης,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σ. 190.

[27] *Παπαδαμάκης,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σ. 191.

[28] Ποινικός Λόγος 6/2001, σελ 2584. Βέβαια στη συγκεκριμένη περίπτωση το θύμα είχε δώσει στον κατηγορούμενο την κάρτα και το μυστικό pin προκειμένου ο τελευταίος να του φέρει χρήματα μετά από ανάληψη, πλην όμως ο κατηγορούμενος έκανε ανάληψη περισσότερων χρημάτων και ιδιοποιήθηκε το σύνολό τους. Επομένως, κατά τη γνώμη του γράφοντος, ακόμη και με τη σημερινή

Αντίθετα το υπ' αριθμ. 54/2012 βούλευμα του Συμβουλίου Πλημμελειοδικείου Κιλκίς έκρινε ότι ««*η διάταξη που ορίζει περαιτέρω «είτε με οποιονδήποτε άλλο τρόπο» ιδίως αναφέρεται στη χρησιμοποίηση στοιχείων ξένου υπολογιστή από πρόσωπο μη δικαιούμενο…*»», αναφέροντας περαιτέρω ότι στην περίπτωση της ανάληψης χρημάτων από ΑΤΜ από μη δικαιούμενο πρόσωπο *«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»*[29]. Ομοίως η υπ' αριθμ. 1087/2019 Απόφαση του Αρείου Πάγου, έκρινε ότι ειδικά ως προς τον *«με οποιοδήποτε άλλο τρόπο»* τρόπο τέλεσης της απάτης με η/υ *«θα πρέπει να λεχθεί ότι λόγω της ευρείας αυτής διατύπωσης του νόμου επιτρέπεται η υπαγωγή σ` αυτήν και των περιπτώσεων επηρεασμού ακόμη και με μη σύννομη χρήση ορθών στοιχείων (δηλαδή κανονική αλλά χωρίς δικαίωμα εκτέλεσης προγράμματος). Στην περίπτωση αυτή υπάγεται και η ανάληψη χρημάτων από ΑΤΜ Τράπεζας από μη δικαιούμενο πρόσωπο (πχ με κλεμμένη μαγνητική κάρτα). Επομένως επηρεασμό συνιστά και οποιαδήποτε χωρίς δικαίωμα επεξεργασία των δεδομένων του υπολογιστή που οδηγεί σε αποτέλεσμα διαφορετικό από εκείνο που προσδοκάται με τη νόμιμη χρήση, όπως η περίπτωση που αναφέρεται διεθνώς υπό τον όρο "skimming"»*[30]. Η δε υπ' αριθμ. 131/2013[31] Απόφαση του Αρείου Πάγου είχε κρίνει ότι η παράνομη υποκλοπή στοιχείων κάρτας μέσω αντιγραφής της μαγνητικής λωρίδας και η εν συνεχεία δημιουργία πλαστών αντιγράφων των καρτών αυτών και η εκμετάλλευσή τους για ανάληψη ποσών από τα ΑΤΜ είναι απάτη με υπολογιστή, ενώ ομοίως κρίθηκαν και οι περιπτώσεις της υποκλοπής κάρτας και αριθμού pin[32] και υποκλοπής στοιχείων κάρτας (16ψήφιος αριθμός κάρτας, όνομα κατόχου, ημερομηνία λήξης και

μορφή της διάταξης του 386[A], η συγκεκριμένη πράξη θα έπρεπε να χαρακτηριστεί ως υπεξαίρεση και όχι ως απάτη με υπολογιστή, και τούτο γιατί ο κατηγορούμενος εισήγαγε τα «ορθά» στοιχεία προκειμένου να προβεί σε ανάληψη, έχοντας κατά το χρόνο εισαγωγής τους δικαίωμα προς τούτο κατόπιν εντολής και συγκατάθεσης του θύματος, ενώ στη συνέχεια, έχοντας πλέον στη κατοχή του το σύνολο των καταθέσεων του θύματος, ανέλαβε μεγαλύτερο από το ποσό για το οποίο είχε εντολή και συναίνεση, ιδιοποιήθηκε δε τόσο το ποσό για το οποίο είχε εντολή, όσο και το υπερβάλλον.

[29] ΣυμβΠλημμΚιλκίς 54/2012 Ποιν Δνη 2014, 238.

[30] ΑΠ (ΠΟΙΝ) 1087/2019 –ΝΟΜΟΣ. Ομοίως έκρινε η ΕφΣτερΕλλ68/2014- ΝΟΜΟΣ όπου δέχτηκε: *«Η διάταξη που ορίζει περαιτέρω «είτε με οποιονδήποτε άλλο τρόπο» ιδίως αναφέρεται στη χρησιμοποίηση στοιχείων ξένου υπολογιστή από πρόσωπο μη δικαιούμενο, εφόσον υπάρχουν και τα λοιπά στοιχεία του αδικήματος και με τη σύννομη ακόμη χρήση ορθών στοιχείων του υπολογιστή.»*

[31] ΠοινΧρ 2014 σελ. 185.

[32] ΑΠ 813/2015, ΠοινΧρ 2017, 179 - ΝΟΜΟΣ

κωδικός αριθμός ασφαλείας -cvv) και η χρήση τους, χωρίς το σώμα της κάρτας, για αγορά μέσω διαδικτύου[33].

Αντίστοιχη με την χωρίς δικαίωμα χρήση κάρτας, θα έλεγε κανείς ότι είναι και η χωρίς δικαίωμα χρήση κωδικών e-banking τρίτου προσώπου. Αίσθηση επομένως προκαλεί η υπ' αριθμ. 742/2012 απόφαση του Αρείου Πάγου[34], σύμφωνα με την οποία χαρακτηρίστηκε ως κλοπή, η χωρίς δικαίωμα μεταφορά ποσών από τον κατηγορούμενο μέσω του e-banking του θύματος στο δικό του λογαριασμό, και τούτο διότι εν προκειμένω δεν μπορεί να θεωρηθεί, κατά τη γνώμη του γράφοντος, ως «θραύση κατοχής» η εισαγωγή των κωδικών του e-banking στο σύστημα.

Από την μελέτη των ανωτέρω θεωρητικών απόψεων αλλά και των αντικρουόμενων δικαστικών αποφάσεων γίνεται εύκολα αντιληπτό ότι η επιλογή του Έλληνα νομοθέτη να μην ακολουθήσει επακριβώς την πορεία που χάραξε το 1986 ο Γερμανός νομοθέτης, αλλά να εντάξει και τη γενική ρήτρα «με οποιοδήποτε άλλο τρόπο» ως τρόπο τέλεσης της απάτης με υπολογιστή, ναι μεν μπορεί να συνέβαλε, για όσα χρόνια λειτούργησε, στην αντιμετώπιση και στον περιορισμό των «απατεώνων του διαδικτύου», διευρύνοντας το πλήθος των συμπεριφορών που μπορούσαν να χαρακτηριστούν ως «ποινικές», εντούτοις όμως το έπραξε αυτό κατά τρόπο προβληματικό, αφού δημιουργήθηκε τέτοια ασάφεια, όπως αποδείχθηκε από την ανακολουθία της νομολογίας των προηγούμενων ετών, τόσο των δικαστηρίων της ουσίας όσο και του Ακυρωτικού.

[33] ΑΠ 367/2017 - ΝΟΜΟΣ
[34] ΠοινΧρ 2013/677.

Κεφάλαιο 3ο: Η τροποποίηση του άρθρου 386Α ΠΚ με το Ν. 4411/2016

3.1. Η Σύμβαση της Βουδαπέστης (23 Νοεμβρίου 2001) και το από 28 Ιανουαρίου 2003 Πρόσθετο Πρωτόκολλο αυτής

Η εφεύρεση του Παγκόσμιου Ιστού το έτος 1989 και η δημιουργία του πρώτου web server και του πρώτου web browser από τον Tim Burners-Lee[35], αποτέλεσε το έναυσμα για την έναρξη χρήσης του διαδικτύου και από την ευρύτερη κοινωνία. Στην ανατολή της δεκαετίας των «90's» οι χρήστες του διαδικτύου άρχισαν να αυξάνονται με εκθετικό ρυθμό, φτάνοντας στη δύση της προηγούμενης χιλιετίας τους 361.00.000 χρήστες, ποσοστό 5,8% του παγκόσμιου πληθυσμού[36]. Είναι σαφές ότι η έκρηξη αυτή, που είχε ως φυσικό συνεπακόλουθο την αύξηση της νεοπαγούς, διαδικτυακής εγκληματικότητας, δε μπορούσε να αφήσει ασυγκίνητη την Ευρωπαϊκή κοινότητα[37], η οποία αναγνώρισε ότι οι νέες τεχνολογικές δυνατότητες ταχύτατης διάδοσης των πληροφοριών, πέραν των πάμπολλων θετικών συνεπειών στο σύνολο της κοινωνίας, έχουν και μία «σκοτεινή πλευρά»[38].

Βασιζόμενη, μεταξύ άλλων, στην έκθεση του καθηγητή Dr. HWK Kaspersen, ο οποίος θεώρησε ότι το θέμα της ηλεκτρονικής εγκληματικότητας πρέπει να αντιμετωπιστεί με ένα ισχυρότερο από Ευρωπαϊκή Οδηγία νομικό όπλο, το Νοέμβριο του 1996, η Ευρωπαϊκή Επιτροπή περί Ποινικών Θεμάτων (European Committee on Crime Problems), με την υπ' αρ. CDPC/103/211196 Απόφασή της, αποφάσισε τη δημιουργία μιας επιτροπής ειδικών εμπειρογνωμόνων για την αντιμετώπιση του Κυβερνοεγκλήματος. Η εν λόγω επιτροπή συστάθηκε από το Συμβούλιο των Υπουργών, με την υπ' αρ. CM/Del/Dec(97)583 απόφαση, και ονομάστηκε «Επιτροπή Εμπειρογνωμόνων για το Έγκλημα στο Διαδίκτυο»[39]. Σκοπός της η σύνταξη ενός «σχεδίου νόμου» αντιμετώπισης του διαδικτυακού εγκλήματος και των επιμέρους διαδικαστικών (δικονομικών) προβλημάτων που αναφύονται. Έμφαση έπρεπε να δοθεί αφενός στα επιμέρους «εγκλήματα στο διαδίκτυο ή μέσω αυτού» ("cyber-space offences") όπως παράνομες μεταφορές χρημάτων, προσφορά παράνομων υπηρεσιών, παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας κτλ,, αφετέρου στις τυχόν δυνατότητες των Αρχών να επέμβουν στα τεχνολογικά δίκτυα (πχ. Με επιβολή

[35] https://en.wikipedia.org/wiki/Tim_Berners-Lee -Προσπέλαση την 14η-11-2020
[36] https://www.internetworldstats.com/emarketing.htm -Προσπέλαση την 14η-11-2020
[37] Αγγελής Ι., Διαδίκτυο και Ποινικό Δίκαιο, ΝοΒ, 2000, σ. 680
[38] Explenatory Report to the Convention on Cybercrime, Council of Europe Treaty Series- No 185, Introduction, https://rm.coe.int/16800cce5b - Προσπέλαση 14-11-2020
[39] Ακριβής μετάφραση του «Committee of Experts on Crime in Cyber-Space» (PC-CY)

επιμέρους υποχρεώσεων στους παρόχους Υπηρεσιών Διαδικτύου), και εκ τρίτου στα ζητήματα ποινικής δικαιοδοσίας που αναφύονται λόγω της ιδιαιτερότητας των ποινικών αδικημάτων που τελούνται στο διαδίκτυο ή μέσω διαδικτύου.

Έτσι, μετά από τέσσερα χρόνια μελετών, η ανωτέρω Επιτροπή Εμπειρογνωμόνων κατέθεσε τον Ιούνιο του 2001 ενώπιον της Ευρωπαϊκής Επιτροπής περί Ποινικών Θεμάτων το τελικό σχέδιο του νομικού της κειμένου, που έμελλε να υπογραφεί από τριάντα μία χώρες στις 23 Νοεμβρίου 2001 στη Βουδαπέστη[40], υπό τον τίτλο «Διεθνής Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο». Καθιερώθηκε δε στον Ευρωπαϊκό νομικό κόσμο και με τον τίτλο «Σύμβαση της Βουδαπέστης»[41]. Δύο χρόνια αργότερα, τον Ιανουάριο του 2003, υπεγράφη και το Πρόσθετο Πρωτόκολλο αυτής, σχετικά με την ποινικοποίηση της εξάπλωσης του ρατσισμού μέσω διαδικτύου. Η Σύμβαση τέθηκε σε ισχύ το 2004[42].

Με την εν λόγω σύμβαση, που για να εφαρμοστεί στην εσωτερική έννομη τάξη κάθε υπογράφοντος Κράτους, απαιτούνταν κύρωσή της με νόμο, τα κράτη ανέλαβαν την υποχρέωση να θεσπίσουν επιμέρους ποινικές διατάξεις τόσο Ουσιαστικού, όσο και Δικονομικού Δικαίου.

Πιο συγκεκριμένα, πέραν των επιμέρους Ορισμών που θεσπίσθηκαν με το 1ο Κεφάλαιο αυτής, των Δικονομικών Διατάξεων που αναφέρονται στο 2ο Τμήμα του 2ου Κεφαλαίου αυτής, και των περί Διεθνούς Συνεργασίας διατάξεων που αναφέρονται στο 3ο Κεφάλαιο αυτής, αποφασίστηκε ότι τα Συμβαλλόμενα Μέρη, υπό την επιφύλαξη διατύπωσης συγκεκριμένων Επιφυλάξεων και Δηλώσεων, οφείλουν να συμπεριλάβουν, στην εσωτερική τους έννομη τάξη διατάξεις Ουσιαστικού Ποινικού Δικαίου που αφορούν:

α) Την ποινικοποίηση πράξεων που στρέφονται κατά της «Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας των δεδομένων και συστημάτων υπολογιστών -1ος Τίτλος του 1ου Τμήματος του 2ου Κεφαλαίου-,

β) Την ποινικοποίηση πράξεων, από πρόθεση και άνευ δικαιώματος εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων, που έχουν ως αποτέλεσμα είτε την παραγωγή μη αυθεντικών δεδομένων («πλαστογραφία σχετική με υπολογιστές»), είτε

---

[40] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=fhgQsqgK - προσπέλαση 14-11-2020

[41] Explenatory Report to the Convention on Cybercrime, Council of Europe Treaty Series- No 185, The preparatory work, https://rm.coe.int/16800cce5b - προσπέλαση 14-11-2020

[42] *Ζέκος Γ.*, Κυβερνοέγκλημα & Νόμος 4411/2016, Διαδίκτυο, Η/Υ και Τηλεπικοινωνίες στο ελληνικό δίκαιο, σ. 385-398

την πρόκληση απώλειας ξένης περιουσίας («απάτη σχετικά με υπολογιστές»)-2ος Τίτλος του 1ου Τμήματος του 2ου Κεφαλαίου-,

γ) Την ποινικοποίηση πράξεων σχετικών με την παραγωγή, διακίνηση, διανομή κτλ υλικού παιδικής πορνογραφίας -3ος Τίτλος του 1ου Τμήματος του 2ου Κεφαλαίου- και

δ) Την ποινικοποίηση πράξεων σχετικών με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας-4ος Τίτλος του 1ου Τμήματος του 2ου Κεφαλαίου-.

Την ανωτέρω Σύμβαση η Ελλάδα κύρωσε με τον Ν. 4411/2016 (ΦΕΚ Α 142/3-8-2020), γενόμενη έτσι η τελευταία χρονολογικά χώρα (από αυτές που υπέγραψαν εξαρχής τη Σύμβαση στις 23-11-2001) που την κυρώνει. Άξιο αναφοράς είναι ότι η Νότια Αφρική, παρόλο που έχει υπογράψει τη Σύμβαση εξαρχής, έως σήμερα δεν την έχει κυρώσει[43].

Δυνάμει του άρθρου 8 της Σύμβασης, η χώρα μας ανέλαβε την υποχρέωση «*να λάβει 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 α. εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή, 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*», ήτοι ανέλαβε την υποχρέωση να ποινικοποιήσει πράξεις «απάτης σχετικής με υπολογιστές». Τα συγκεκριμένα «νομοθετικά μέτρα», η χώρα μας τα έλαβε αντικαθιστώντας (επί της ουσίας τροποποιώντας) το ήδη υφιστάμενο άρθρο 386Α ΠΚ, δυνάμει του ως άνω κυρωτικού της Σύμβασης της Βουδαπέστης Νόμου 4411/2016, το οποίο μελετάται αμέσως κατωτέρω.

<u>3.2. Η μελέτη του άρθρο 386Α ΠΚ μετά την τροποποίησή του με το Ν.4411/2016.</u>

Το άρθρο 386Α ΠΚ, όπως αντικαταστάθηκε με το άρθρο δεύτερο παρ. 11 του Ν. 4411/2016 (ΦΕΚ Α 142/3-8-2016) και εφαρμόσθηκε έως την κατάργησή του με την ταυτόχρονη θέση σε εφαρμογή του Νέου Ποινικού Κώδικα (Ν4619/2019), είχε την εξής μορφή:

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς

[43] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=fhgQsqgK – προσπέλαση στις 14-11-2020

δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα».

Συγκρίνοντας τη μορφή της διάταξης του 386^{A} (όπως αυτή αναδιατυπώθηκε με το ν. 4411/2016 και ίσχυσε έως τις 30-6-2019) με την προϊσχύσασα, αντιλαμβάνεται κανείς δύο θεμελιώδεις αλλαγές. Αφενός την αντικατάσταση της φράσης «στοιχεία υπολογιστή» με τη φράση «αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων», αφετέρου την απάλειψη δύο τυποποιούμενων τρόπων τέλεσης της πράξης και την εισαγωγή δύο καινούριων. Μετά τις ανωτέρω αλλαγές, η διάταξη έγινε πολύ πιο σαφής και εύστοχη. Τις εν λόγω αλλαγές θα μελετήσουμε στο παρόν κεφάλαιο.

3.2.1. Η αντικατάσταση του γενικού τρόπου τέλεσης του αδικήματος

Ως προελέχθη, η πρώτη αλλαγή που παρατηρείται στο άρθρο 386^{A}, μετά την αντικατάστασή του κατ' άρθρο 2§11 Ν.4411/2016, είναι η αντικατάσταση του αντικειμένου της μετοχής «επηρεάζοντας», τροποποιώντας έτσι τον γενικό τρόπο τέλεσης της «βλάβης ξένης περιουσίας». Η φράση «στοιχεία υπολογιστή» αντικαταστάθηκε με τη φράση «αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων», διαμορφώνοντας έτσι τον γενικό τρόπο τέλεσης του αδικήματος σε «βλάβη ξένης περιουσίας δια επηρεασμού του αποτελέσματος διαδικασίας επεξεργασίας ψηφιακών δεδομένων».

Θα έλεγε κανείς ότι ο όρος «στοιχεία υπολογιστή» που υπήρχε στην προϋφιστάμενη διάταξη ήταν σχεδόν αόριστος, αφού πουθενά στο νόμο δεν ορίζονταν ποια ήταν τα «στοιχεία αυτά του υπολογιστή» που ενέπιπταν στην εν λόγω διάταξη, ενώ και η ορολογία αυτή σε καμία περίπτωση δεν ανταποκρινόταν στην αντίστοιχη ορολογία της επιστήμης των υπολογιστών.

Βέβαια η εισαγωγή της έννοιας των «ψηφιακών δεδομένων» θα ήταν παντελώς ανούσια, αν δεν είχε συνοδευτεί με τον νομοθετικό ορισμό της. Ο ορισμός αυτός εισήχθη στον Ποινικό μας Κώδικα με την προσθήκη περίπτωσης -θ- στο (περί ορισμών εννοιών) άρθρο 13[44]. Η συγκεκριμένη προσθήκη έγινε με την 1^{η} παράγραφο του 2^{ου} άρθρου του Ν.4411/2016, κατά τη μεταφορά στο Ελληνικό Δίκαιο της Ευρωπαϊκής Οδηγίας 2013/40/ΕΕ περί επιθέσεων σε πληροφοριακά συστήματα κτλ., ενώ όπως

[44] Αρ. 13 περ. θ' ΠΚ/1950: *«θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μία λειτουργία»*

προαναφέρθηκε, με το άρθρο 1ο του ίδιου νόμου κυρώθηκε η Σύμβαση της Βουδαπέστης. Παρόλο που η προσθήκη της περίπτωσης -θ- στο άρθρο 13 ΠΚ έγινε με το άρθρο δεύτερο του Ν. 4411/2016, που μετέφερε την ανωτέρω Ευρωπαϊκή Οδηγία στο Ελληνικό Δίκαιο, από τη συγκριτική μελέτη του περιγραφόμενου στην ίδια την 2013/40/ΕΕ Οδηγία ορισμού (όπου γίνεται λόγος για «ηλεκτρονικά δεδομένα»)[45], του περιγραφόμενου στο αρ. 1 περ. β' της Σύμβασης της Βουδαπέστης ορισμού (όπου γίνεται λόγος για «δεδομένα υπολογιστών»)[46], και του τελικού ορισμού που εισήχθη εν τέλει στο άρθρο 13 ΠΚ/1950, γίνεται αντιληπτό ότι η τελική διάταξη χρησιμοποιεί έναν νέο όρο, σε σχέση με τις πρότυπες διατάξεις, τον όρο «ψηφιακά». Η ουσία βέβαια και των τριών ορισμών παραμένει ίδια, αφού περιγράφουν το ίδιο αντικείμενο με χρήση συνώνυμων φράσεων ή λέξεων, πλην όμως δε μπορεί παρά να επισημανθεί η επιλογή του Έλληνα νομοθέτη να διαφοροποιηθεί από την ακριβή μετάφραση των αντίστοιχων ορισμών που έδωσαν το Συμβούλιο της Ευρώπης από το 2001 και η Ευρωπαϊκή Ένωση από το 2013.

Σε κάθε περίπτωση, με την εισαγωγή πλέον του νομοθετικού ορισμού της έννοιας των «ψηφιακών δεδομένων», η διάταξη του άρθρου 386Α ΠΚ γίνεται περισσότερο σαφής, συγκεκριμένη και κατανοητή, αφού γίνεται αντιληπτό ότι για να τελεστεί το εν λόγω έγκλημα, απαιτείται ο δράστης να επηρεάσει το *«αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων»*, έννοια πολύ πιο «ειδική» από τη γενική, αόριστη και δυσερμήνευτη έννοια των «στοιχείων υπολογιστή».

3.2.2. Οι παρεμβάσεις στους επιμέρους τρόπους τέλεσης του αδικήματος της 386Α ΠΚ/1950

Η δεύτερη θεμελιώδης αλλαγή που επήλθε στο άρθρο 386Α με τον Ν. 4411/2016 ήταν η επέμβαση του νομοθέτη στους επιμέρους τρόπους τέλεσης της πράξης του «επηρεασμού του αποτελέσματος της διαδικασίας επεξεργασίας ψηφιακών δεδομένων». Συγκεκριμένα:

- προστέθηκε η πράξη της *«χωρίς δικαίωμα χρήσης δεδομένων»*,

[45] Άρθρο 2 περ. β 2013/40/ΕΕ Οδηγίας: «*β)"ηλεκτρονικά δεδομένα" : η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία»*

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

-αφαιρέθηκε η υπαλλαγή της «*επέμβασης κατά την εφαρμογή του* (σ.σ. προγράμματος)»,
-προστέθηκε η πράξη της *«χωρίς δικαίωμα παρέμβασης σε πληροφοριακό σύστημα»*[47] -και αφαιρέθηκε η γενική ρήτρα *«με οποιονδήποτε άλλο τρόπο»*.

Το εδάφιο περί «επέμβασης κατά την εφαρμογή του προγράμματος», απαλείφθηκε, κατά τη γνώμη του γράφοντος, γιατί ο συγκεκριμένος τρόπος τέλεσης θα μπορούσε να θεωρηθεί είτε ως υποπερίπτωση του ήδη υφιστάμενου 1ου τρόπου, (: της *«μη ορθής διαμόρφωσης του προγράμματος»)*, είτε, πιο εύστοχα, ως υποπερίπτωση του νεοπαγούς 4ου τρόπου τέλεσης, ήτοι της *«χωρίς δικαίωμα παρέμβασης σε πληροφοριακό σύστημα*», ίσως και σε συνδυασμό με τον 2ο και τον 3ο τρόπο τέλεσης όπως εφαρμόστηκαν (χρήση μη ορθών ή ελλιπών δεδομένων και χωρίς δικαίωμα ορθών δεδομένων – ανάλογα με την περίπτωση). Αναζητώντας στη βιβλιογραφία την ερμηνεία του συγκεκριμένου τρόπου, ως ίσχυε προ της απαλοιφής του, παρατηρούμε ότι εννοείται η «επέμβαση κατά την εφαρμογή (ροή) προγράμματος με επεξεργασία δεδομένων από το πληκτρολόγιο ή επέμβαση στα μηχανικά μέρη του υπολογιστή που επηρεάζουν τη λειτουργία του προγράμματος»[48]. Είναι επομένως σαφές ότι ως επέμβαση κατά την εφαρμογή του προγράμματος με επεξεργασία δεδομένων από το πληκτρολόγιο μπορεί να θεωρηθεί η επέμβαση μέσω πληκτρολογίου στις εντολές του προγράμματος (backend) ή και ως επέμβαση με εισαγωγή μη ορθών/ ελλιπών δεδομένων ή χωρίς δικαίωμα ορθών δεδομένων. Αντιστοίχως, δεδομένου του ότι βάσει του κατά το χρόνο εκείνο προστεθέντος με το Ν.4411/2016 νέου, εδαφίου η΄ του άρθρου 13ΠΚ[49], ο υπολογιστής θεωρείται «πληροφοριακό σύστημα» για τον ποινικό κώδικα, η επέμβαση σε μηχανικά μέρη του υπολογιστή μπορεί να ενταχθεί στον (τότε) νέο τέταρτο κατά σειρά τρόπο τέλεσης (: «*χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα»*). Ως εκ τούτου, η *«επέμβαση κατά την εφαρμογή του προγράμματος»* ως τυποποιούμενος τρόπος τέλεσης καλύφθηκε από τους νέους τυποποιημένους τρόπους, και καθώς δεν είχε πλέον λόγο ύπαρξης, ορθώς απαλείφθηκε.

---

[47] *Μοροζίνης Ι.* σε *Δαλακούρα Θ.*, Ηλεκτρονικό Έγκλημα, 2019 ό.π. σ. 170.
[48] *Μυλωνόπουλος Χ.*, Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ 550 · *Παπαδαμάκης,* ο.π, σελ 187.
[49] Αρ. 13 περ. η΄ ΠΚ/1950: *«η) 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.*

Το έτερο απαλειφθέν εδάφιο, ήτοι η γενική ρήτρα του «με οποιοδήποτε άλλο τρόπο» επηρεασμού των στοιχείων υπολογιστή, ήταν, όπως αναλύθηκε σε προηγούμενα κεφάλαια[50], η διάταξη που, όπως προαναφέρθηκε, δημιούργησε λόγω της ασάφειάς της διχασμό στη θεωρία και ανακολουθία στη νομολογία. Δεδομένου όμως του ότι, με τον Ν.4411/2016 τυποποιήθηκαν ως τρόποι τέλεσης η *«χωρίς δικαίωμα χρήση δεδομένων», και η «χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα»*, με αποτέλεσμα να καλυφθούν εκείνες οι συγκεκριμένες συμπεριφορές που έως τότε δεν μπορούσαν να υπαχθούν σε κάποιον από τους άλλους τρόπους τέλεσης, αναγκάζοντας τα δικαστήρια να προσφύγουν στη γενική αυτή ρήτρα, κρίθηκε από το νομοθέτη ότι πλέον δεν υφίστατο λόγος περαιτέρω ύπαρξής της.

Κατόπιν λοιπόν της αντικατάστασης της διάταξης του 386^{A} με τον ν. 4411/2016 και παρατηρώντας τη νέα του μορφή, διαπιστώνουμε ότι οι ανωτέρω θεωρητικές διχογνωμίες και νομολογιακές διαφορές εξαλείφονται πλήρως, αφού οι νεοπαγείς τρόποι τέλεσης περιλαμβάνουν ρητώς πλέον την «χωρίς δικαίωμα» χρήση δεδομένων και επέμβαση σε πληροφοριακό σύστημα, όπου και υπάγονται πλέον οι περιπτώσεις της ανάληψης χρημάτων με κλεμμένη κάρτα, η χρήση στοιχείων ξένης κάρτας για αγορές στο διαδίκτυο ή η χρήση υποκλαπέντων κωδικών εισόδου σε τραπεζικά συστήματα e-banking[51].

Αξίζει πάντως να υπογραμμισθεί ότι, από τις σε προηγούμενο κεφάλαιο αναφερόμενες θεωρητικές απόψεις και ερμηνείες[52], αυτή του Μυλωνόπουλου αποδείχθηκε η πιο εύστοχη, αφού ήταν αυτός που ρητά είχε εκθέσει την άποψη ότι η «χωρίς δικαίωμα» χρήση ορθών δεδομένων εμπίπτει στον «με οποιοδήποτε άλλο τρόπο» τρόπο τέλεσης της πράξης του 386^{A}.

Η ανωτέρω όμως αυτή αναδιατυπωμένη μορφή της διάταξης της απάτης με υπολογιστή δεν διατηρείται αυτούσια σήμερα. Τούτο διότι ο ΠΚ/1950 καταργήθηκε, και από 1-7-2019 τέθηκε σε ισχύ ο Νέος Ποινικός Κώδικας, με το Ν.4619/2019. Η διάταξη του άρθρου 386^{A} ΠΚ όπως ισχύει σήμερα, μελετάται στο αμέσως επόμενο κεφάλαιο.

---

[50] Βλ. ανωτέρω κεφάλαια 2.4 και 2.5

[51] Βλ. συναφώς *Δαλακούρα Θ.,* Ηλεκτρονικό Έγκλημα, σ. 14, όπου αναφέρεται ότι *«σύμφωνα με το επεξηγηματικό Υπόμνημα που συνοδεύει τη Σύμβαση, η ρύθμιση του άρθρου 8 τίθεται με σκοπό να συμπεριλάβει οποιαδήποτε, χωρίς δικαίωμα επέμβαση σε σύστημα η/υ, συνοδευόμενη από σκοπό πρόκλησης παράνομου περιουσιακού οφέλους, έτσι ώστε να καταλαμβάνονται και οι περιπτώσεις του «ηλεκτρονικού χρήματος» και κυρίως της απάτης με πιστωτικές κάρτες».*

[52] Βλ. ανωτέρω κεφάλαιο 2.5

Κεφάλαιο 4ο: Η Απάτη με Υπολογιστή (386Α) στο Νέο Ποινικό Κώδικα

4.1. Εισαγωγή

Η σημερινή μορφή της διάταξης της απάτης με υπολογιστή, όπως αυτή αναδιατυπώθηκε με τον πρόσφατο νόμο 4619/2019 (νέος Ποινικός Κώδικας) απαριθμεί πλέον περιοριστικά τους τρόπους τέλεσης του αδικήματος (αφού αφαιρέθηκε ο διαζευκτικός σύνδεσμος «*είτε»*), ενώ περιλαμβάνει πλέον και έναν πέμπτο τρόπο τέλεσης. Πιο συγκεκριμένα, η διάταξη υπό την ισχύουσα σήμερα μορφή της έχει ως εξής:

«1.Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή: α) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή, β) με τη χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή, γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, ή ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων τιμωρείται με φυλάκιση και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000 ευρώ, επιβάλλεται κάθειρξη έως δέκα έτη και χρηματική ποινή.

2. Όποιος κατασκευάζει, διαθέτει ή κατέχει πρόγραμμα ή σύστημα υπολογιστή που προορίζεται για τη διάπραξη του εγκλήματος της παραγράφου 1 τιμωρείται με φυλάκιση έως δύο έτη και χρηματική ποινή. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή σύστημα υπολογιστή πριν το χρησιμοποιήσει για τη διάπραξη του εγκλήματος της παραγράφου 1.

3. Αν η απάτη με υπολογιστή στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000 ευρώ επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή έως χίλιες ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά είκοσι έτη».

4.2 Σύντομη Ερμηνεία της 386Α ΠΚ- Σχέση της με την κοινή απάτη (386 ΠΚ)

Η ανάγνωση της διάταξης του άρθρου 386Α ΠΚ, δημιουργεί την εντύπωση ότι η αντικειμενική υπόσταση της απάτης με η/υ παρουσιάζει δομική ομοιότητα με αυτήν της κοινής απάτης του 386, ώστε να προκρίνεται η ερμηνεία της πρώτης παράλληλα με την δεύτερη[53]. Έτσι υποστηρίζεται ότι η πράξη/«επέμβαση» του δράστη στα

[53] Υπέρ της άποψης αυτής, που εμφανίζεται ως κρατούσα βλ. *Μυλωνόπουλο Χ.,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ.548, όπου αναφέρει μάλιστα ότι η ομοιότητα προς την

δεδομένα του υπολογιστή (:«επηρεάζοντας» τα στοιχεία του υπολογιστή με έναν από τους προβλεπόμενους τρόπους τέλεσης), βρίσκει αντιστοιχία στην πράξη της εξαπάτησης του άρθρου 386 ΠΚ (:«πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με έναν από τους προβλεπόμενους τρόπους τέλεσης)[54]. Ως εκ τούτου θα πρέπει δηλαδή, με τον «επηρεασμό» να δημιουργείται μία κατάσταση ανάλογη με εκείνη που συνεπάγεται η παραπλάνηση στην απάτη[55].

Εντούτοις η κρατούσα αυτή άποψη που προκρίνει την ερμηνευτική ταύτιση μεταξύ της απάτης με η/υ (386^{A} ΠΚ) και της κοινής απάτης (386 ΠΚ), παρουσιάζει αδυναμίες και εμφανίζεται αντιφατική, όταν εμμένει στην «αντίστοιχη» μεταφορά του στοιχείου «πείθοντας κάποιον» και στην απάτη με υπολογιστή, ενώ την ίδια στιγμή δέχεται ότι η έλλειψη του στοιχείου αυτού ήταν ακριβώς αυτό που οδήγησε το νομοθέτη να θεσπίσει τη νέα διάταξη[56]. Και τούτο ειδικότερα διότι, το να αντιστοιχεί η κρατούσα άποψη τον όρο «επηρεασμός των στοιχείων» με την παραπλάνηση ανθρώπου, είναι σχήμα εκ των πραγμάτων αδύνατο, εάν αναλογιστεί κανείς πως λειτουργούν τα αυτοματοποιημένα συστήματα ηλεκτρονικής διακίνησης περιουσίας[57]. Στην απάτη με η/υ εκλείπει το στοιχείο της ανθρώπινης παραπλάνησης ώστε να οδηγείται ο παραπλανημένος σε περιουσιακή «αυτοπροσβολή», η δε έλλειψη αυτή δεν μπορεί να αντικατασταθεί απλώς από μία «κατάσταση παραπλάνησης του υπολογιστή»[58]. Αντιθέτως στην απάτη με η/υ, η ζημία-περιουσιακή βλάβη προκαλείται εξαρχής από την πράξη του ίδιου του δράστη, αφού με μόνο τον επηρεασμό του αυτοματοποιημένου προγράμματος η/υ προκαλεί την περιουσιακή μετατόπιση, με

απάτη δεν υπήρξε τυχαία αλλά σκόπιμη επιλογή του νομοθέτη, ο οποίος είχε την πρόθεση να αποτελέσει αυτή σοβαρό ερμηνευτικό βοήθημα· *Κιούπη,* ό.π., σελ. 116· *Βασιλάκη,* Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σελ. 213· βλ. και *Παπαδαμάκη, Α.,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σελ 182-183, όπου αναφέρει ότι η διάταξη του άρθρου 386ΑΠΚ είναι ευθυγραμμισμένη με τους όρους στοιχειοθέτησης της απάτης του άρθρου 386 ΠΚ.

[54] *Παπαδαμάκης,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σελ 183.

[55] *Παπαδαμάκης,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σελ 185, όπου αναφέρει ότι για τον λόγο αυτό η ενεργοποίηση διαφόρων αυτόματων μηχανών με πλαστά κέρματα δεν αποτελεί απάτη με η/υ, διότι η συμπεριφορά του δράστη δεν επηρεάζει τη διαδικασία επεξεργασίας στοιχείων υπολογιστή, αλλά μία τεχνική του λειτουργία.

[56] Βλ. συναφώς *Νούσκαλη Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 184 επ.

[57] *Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 185.

[58] *Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 188.

συνέπεια να αποτελεί περίπτωση «ετεροπροσβολής» του έννομου αγαθού της περιουσίας[59]. Η δε διαφοροποίηση αυτή δεν καθιστά την απάτη με υπολογιστή ειδικότερη μορφή της παραδοσιακής απάτης, αλλά κατά τη σύσσωμη αποδοχή της θεωρίας, η απάτη του 386^{A} είναι ένα ιδιώνυμο έγκλημα και μεταξύ των δύο διατάξεων υπάρχει σχέση αμοιβαίου αποκλεισμού[60].

Ενόψει των ανωτέρω, από την απλή και μόνο αντιπαραβολή του λεκτικού των διατάξεων της απάτης με η/υ και της κοινής απάτης, γίνεται αντιληπτό ότι η διάταξη της 386^{A} ΠΚ είναι πρόσφορη να αντιμετωπίσει περιπτώσεις, στις οποίες η κρίσιμη για το αδίκημα της απάτης παράνομη περιουσιακή διάθεση επιτυγχάνεται δια του επηρεασμού των στοιχείων του υπολογιστή, χωρίς την παρεμβολή φυσικού προσώπου (που να ελέγχει τα δεδομένα και να αποφασίζει για την περιουσιακή διάθεση)[61]. Και εκεί είναι που εντοπίζεται η βασική διαφορά μεταξύ των δύο διατάξεων, 386 και 386^{A} ΠΚ, αλλά πολύ περισσότερο και ο λόγος θέσπισης της τελευταίας.

4.3. Ανάλυση της διάταξης 386^{A} ΠΚ

4.3.1 Αντικειμενική Υπόσταση

Το έγκλημα της απάτης με η/υ (386Α ΠΚ), αποτελεί ένα υπαλλακτικώς[62] μικτό αδίκημα, πολύτροπο, το οποίο μπορεί να τελεστεί με πλείστους –αλλά περιοριστικά αναφερόμενους τρόπους, οι οποίοι πρέπει να κατατείνουν στον επηρεασμό του αποτελέσματος μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή[63]. Έτσι ο «επηρεασμός» του αποτελέσματος μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή, που επιφέρει παράνομη περιουσιακή μετατόπιση, συνιστά κατά κάποιο τρόπο το άμεσο αποτέλεσμα της εγκληματικής συμπεριφοράς[64].

---

[59] *Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386^{A} ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 188- 189 · *Κουράκης*, ό.π., ΠοινΛογ 2001, σ. 2592.

[60] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000 σελ 182· *Μυλωνόπουλος* , Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ. 558· *Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386^{A} ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 180 (και εκεί περαιτέρω παραπομπές και σε Βασιλάκη, Καϊάφα – Γκμπάντι) · *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 3^{η} έκδ., άρθρ. 386^{A}, αρ 12 · *Κουράκης*, ό.π., ΠοινΛογ 2001, σ. 2591.

[61] *Ναμίας Ο.,* ό.π., ΠοινΧρ 2003,489.

[62] ΑΠ (ΠΟΙΝ) 1087/2019 –ΝΟΜΟΣ. Πραγματώνεται υπαλλακτικώς όπως και το έγκλημα της κοινής απάτης, βλ.ΑΠ 1246/1990, ΠοινΧρ1991, 538.

[63] *Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο 386^{A}. Απάτη με υπολογιστή, sakkoulas online,αρ. 1.

[64] *Μυλωνόπουλος* , ο.π. σελ. 549.

Υποκείμενο τέλεσης της πράξης μπορεί να είναι και εδώ, όπως και στην κοινή απάτη, ο οποιοσδήποτε («*όποιος»).*

Αντικείμενο της εγκληματικής πράξης είναι η περιουσία[65]. Συνεπώς, προστατευόμενο έννομο αγαθό από τη συγκεκριμένη διάταξη είναι και εδώ η «περιουσία»[66], η οποία όμως δεν απαιτείται να συνδέεται με συγκεκριμένο άτομο[67]. Η σκέψη αυτή επιβεβαιώνεται και από το τελευταίο εδάφιο που είχε η διάταξη αυτή στην αμέσως προϊσχύουσα μορφή της, αφού προέβλεπε ρητά ότι ήταν «αδιάφορο», αν οι παθόντες από την πράξη είναι ένας ή περισσότερα άτομα. Σύμφωνα δε με τον Παπαδαμάκη[68] *«πρόκειται για διατύπωση νόμου με «θυματολογικό χαρακτήρα»,* με την έννοια ότι με την πράξη του 386^{A} μπορεί να επέλθει απειροελάχιστη ζημία σε πολλούς ανθρώπους (θύματα), κάτι που όμως καθιστά την ζημία της «συνολικής συλλογικής περιουσίας» (ως έννομο αγαθό) εξαιρετικά μεγάλη. Επικαλείται δε ο ανωτέρω συγγραφέας την κοινή πείρα, αναφέροντας ότι στην πλειονότητα των περιπτώσεων ο δράστης του εγκλήματος της απάτης με υπολογιστή βλάπτει την συνολική περιουσία μιας ομάδας ατόμων ή εταιριών ή πιστωτικών ιδρυμάτων. Έχουν βέβαια διατυπωθεί και απόψεις και για άλλα, δευτερευόντως προστατευόμενα με τη συγκεκριμένη διάταξη έννομα αγαθά[69], τα οποία είναι προφανώς πολύ ειδικότερα του γενικότερου εννόμου αγαθού της περιουσίας.

Η πράξη επομένως που ποινικοποιεί η διάταξη του 386^{A} είναι η «*βλάβη ξένης περιουσίας»*, όπως ακριβώς συμβαίνει και με την απάτη του 386 ΠΚ. Αυτό όμως που διαφοροποιεί τις δύο διατάξεις, όπως αναφέρθηκε ήδη και θα αναλυθεί κατωτέρω είναι

---

[65] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σελ 183.

[66] Έτσι *Μυλωνόπουλος Χ.,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ.548· *Παπαδαμάκης Α,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000*,* σελ 183-184. Βλ. όμως και *Νούσκαλη,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386^{A} ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 179, όπου αναφέρει ότι το πρόγραμμα Η/Υ υπό την ιδιότητα του να διακινεί και να διασφαλίζει την περιουσία είναι το έννομο αγαθό που προσβάλλεται καταρχήν, προτού επέλθει η βλάβη στο έννομο αγαθό της περιουσίας.

[67] *Παπαδαμάκης,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σελ 183· *Μυλωνόπουλος Χ.,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016,. σελ.556 · *Κουράκης Ν.*, Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001, ΠοινΛογ 2001, σ. 2593, όπου αναφέρει ότι το γεγονός ότι η απάτη με η/υ στοιχειοθετείται πλήρως ακόμα και εάν τα πρόσωπα, στα οποία επέρχεται η ζημία, είναι άδηλα, αποτελεί απόκλιση σε σχέση με τα όσα προβλέπονται για την κοινή απάτη.

[68] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000,. σελ 183.

[69] *Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386^{A} ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, σ. 179, όπου υπάρχουν παραπομπές σε γερμανικές απόψεις που υποστήριξαν ως δευτερευόντως προστατευόμενα έννομα αγαθά από τη διάταξη αυτή τα «συστήματα συναλλαγών χωρίς μετρητά» και την «εμπιστοσύνη στην ασφάλεια μεταφοράς κεφαλαίων μέσω επεξεργασίας δεδομένων».

ο τρόπος που επιφέρεται η βλάβη στην ξένη περιουσία από το δράστη. Εν προκειμένω, η πράξη αυτή καθεαυτή του δράστη, που οδηγεί εν συνεχεία στην βλάβη ξένης περιουσίας είναι ο «επηρεασμός του αποτελέσματος της διαδικασίας επεξεργασίας ψηφιακών δεδομένων». Ως «επηρεασμός» νοείται, όταν το αποτέλεσμα της επεξεργασίας των δεδομένων αποκλίνει λόγω της συμπεριφοράς του δράστη από εκείνο που θα επιτυγχανόταν με κανονική και σύννομη εκτέλεση του προγράμματος[70].

Στο σημείο αυτό κρίνεται σκόπιμο να αναφερθούν οι ορισμοί των όρων «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα», όπως εισήχθησαν στη διάταξη του άρθρου 13 ΠΚ το πρώτον με το ν. 4411/2016, και όπως προβλέπονται σήμερα στο άρθρο 13 ΠΚ του ν. 4619/2019.

Ειδικότερα, κατά το στοιχείο στ΄ του άρθρου 13 ΠΚ, όπως αυτό ισχύει σήμερα:

«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»,

ενώ κατά το στοιχείο ζ΄ του ίδιου άρθρου:

«*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*».

Φαίνεται, από την ανάγνωση και μόνο των ορισμών αυτών, ότι δεν μπορεί να υπάρξει πληροφοριακό σύστημα χωρίς ψηφιακά δεδομένα, αφού το αντικείμενο που διαχειρίζονται τα πληροφοριακά συστήματα είναι τα ψηφιακά δεδομένα.

Αναγιγνώσκοντας επομένως εκ νέου την ανωτέρω διάταξη του άρθρου 386^{A} ΠΚ, σε συνδυασμό με τον ορισμό του 13 περ. στ΄ περί πληροφοριακών συστημάτων, κατά τη γνώμη του γράφοντος, ένας εναλλακτικός τρόπος διατύπωσης της φράσης *«επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας δεδομένων υπολογιστή»* θα μπορούσε να είναι «*παρεμβαίνοντας σε πληροφοριακό σύστημα εν γένει»* αφού η έννοια του πληροφοριακού συστήματος περιλαμβάνει την έννοια της επεξεργασίας ψηφιακών δεδομένων και του αποτελέσματος της επεξεργασίας αυτής, ειδικά αν αναλογιστεί

[70]*Μυλωνόπουλος,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σ. 556 · *Μυλωνόπουλος,* Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ. 57.

κανείς ότι και οι πέντε τυποποιούμενοι «τρόποι τέλεσης» του επηρεασμού του αποτελέσματος της διαδικασίας επεξεργασίας δεδομένων υπολογιστή συσχετίζονται με την έννοια του πληροφοριακού συστήματος, απαιτούν δηλαδή μια εμπλοκή του δράστη με ένα πληροφοριακό σύστημα.

Οι τρόποι τέλεσης της πράξης του επηρεασμού του *«αποτελέσματος επεξεργασίας δεδομένων υπολογιστή»* είναι πέντε, εξαντλητικά πλέον απαριθμούμενοι στο νόμο. Ως εκ τούτου, οποιαδήποτε πράξη διωκόμενη διά του συγκεκριμένου άρθρου, δια της οποίας επέρχεται επηρεασμός του αποτελέσματος επεξεργασίας δεδομένων υπολογιστή, πρέπει να υπαγάγεται σε έναν από τους συγκεκριμένους τρόπους τέλεσης, όπως αυτοί αναλύονται αμέσως μετά.

Στο σημείο αυτό πρέπει να σημειωθεί ότι, προκειμένου να υπάρξει εφαρμογή της μελετούμενης διάταξης, ο *«επηρεασμός τους αποτελέσματος διαδικασίας επεξεργασίας δεδομένων υπολογιστή»*, με όποιον τρόπο από τους απαριθμούμενους στο νόμο και αν τελείται, πρέπει να οδηγεί άμεσα και απευθείας σε περιουσιακή διάθεση, χωρίς να παρεμβληθεί άλλη ενέργεια ή άνθρωπος[71]. Με άλλα λόγια πρέπει να είναι αυτή καθ' εαυτή η παρέμβαση του δράστη που οδηγεί τον ηλεκτρονικό υπολογιστή να συντελέσει αυτόματα, τρόπον τινά, την περιουσιακή διάθεση[72].

Σε περίπτωση που, στην αλυσίδα των γεγονότων, που ξεκινά με την συμπεριφορά του δράστη (παρεμβολή σε διαδικασία επεξεργασίας δεδομένων υπολογιστή) και τελειώνει με την επέλευση περιουσιακής βλάβης τινός, παρεμβάλλεται φυσικό πρόσωπο το οποίο «παραπλανάται», τότε δεν μπορεί να τύχει εφαρμογής η συγκεκριμένη διάταξη, αλλά αυτή της κοινής απάτης (386 ΠΚ), για την τέλεση της οποίας χρησιμοποιείται ως «μέσο τέλεσης» ο υπολογιστής («απάτη μέσω υπολογιστή»)[73].

---

[71]*Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386[Α] ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σελ. 185- 189, αναφέρει μάλιστα, ότι απλώς σε κάποιες περιπτώσεις παρεμβάλλεται η εντελώς τυπική αποδοχή του αποτελέσματος αυτού από ανθρώπους · *Μυλωνόπουλος ,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σ. 556· *Μπουρμάς Γ.,* Στοιχεία απάτης με υπολογιστή κατ'άρθρο 386 α ΠΚ και διάκριση αυτής από την κοινή απάτη του άρθρου 386 ΠΚ, ΠοινΧρον ΝΑ΄, σελ.471επ, όπου αναφέρει ότι εάν παρεμβληθεί ενέργεια φυσικού προσώπου, το οποίο ενεργεί απλώς στο πλαίσιο δέσμιας αρμοδιότητας εκτελώντας μηχανικά τις «εντολές» που δίνει σ' αυτόν ο υπολογιστής, τότε δεν αποτελεί τα πρόσωπο αυτό τίποτε άλλο από ένα «προεκτεινόμενο χέρι» του υπολογιστή.

[72] *Μπουρμάς Γ.,* Στοιχεία απάτης με υπολογιστή κατ'άρθρο 386 α ΠΚ και διάκριση αυτής από την κοινή απάτη του άρθρου 386 ΠΚ, ΠοινΧρον ΝΑ΄, σελ.469

[73]ΑΠ 367/2017 - ΝΟΜΟΣ· ΑΠ 813/2015 -ΝΟΜΟΣ· ΑΠ 1152/1999 ΠραξΛογΠΔ 2000, σ. 327επ. · ΣυμβΕφΠατρ 244/2001 ΠραξΛογΠΔ 2004, σ. 107 επ.

Επιπλέον, κατά την κρατούσα άποψη, πρέπει να υπάρχει και αντιστοιχία (προσδοκώμενου) οφέλους και περιουσιακής βλάβης[74], με την έννοια ότι δε τιμωρείται με τη συγκεκριμένη διάταξη κάποιος που επηρεάζει αποτέλεσμα επεξεργασίας δεδομένων υπολογιστή προκειμένου να λάβει αμοιβή από τρίτο για την πράξη του αυτή[75].

4.3.1.1. Οι Τρόποι Τέλεσης

Από την ανάγνωση της διάταξης, υπό την ισχύουσα σήμερα μορφή της, διαπιστώνει κανείς ότι αναγνωρίζονται πλέον πέντε, διαζευκτικά αναφερόμενοι (αρίθμηση από α΄ έως ε΄ και χρήση του «ή») τρόποι τέλεσης της πράξης του επηρεασμού αποτελέσματος επεξεργασίας δεδομένων υπολογιστή. Δεν αποκλείεται βέβαια μια ενιαία πράξη να γίνεται με περισσότερων του ενός τρόπους τέλεσης. Οι τρόποι αυτοί είναι οι εξής:

Α. «Η μη ορθή διαμόρφωση προγράμματος υπολογιστή»:

Απαραίτητο για να αντιληφθεί κανείς τον συγκεκριμένο τρόπο τέλεσης είναι να γνωρίζει τι είναι «πρόγραμμα υπολογιστή» και πως αυτό δουλεύει. Ως πρόγραμμα χαρακτηρίζεται ένα «*σύνολο δεδομένων με τα οποία παρέχονται εντολές στον υπολογιστή»*[76] (ορθότερα «*δεδομένα με τη μορφή εντολών σε συγκεκριμένη ακολουθία»)*. Επομένως, για να συνιστά μια συμπεριφορά «μη ορθή διαμόρφωση προγράμματος» πρέπει ο δράστης να παρέμβει, εξ αρχής ή μεταγενέστερα[77, 78] με τέτοιο τρόπο στην ακολουθία των εντολών του προγράμματος, να διαφοροποιήσει με τέτοιο τρόπο τα δεδομένα του προγράμματος[79] ώστε η διαμόρφωση αυτού, να είναι μη ορθή. Ως προς το πως κρίνεται αν ένα πρόγραμμα διαμορφώνεται/λειτουργεί «ορθά» κατά την έννοια του συγκεκριμένου άρθρου αναπτύχθηκαν τρεις θεωρίες. Σύμφωνα με

[74] *Παπαδαμάκης Α,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000, σελ 186· *Μυλωνόπουλος Χ.*, Ποινικό Δίκαιο-Ειδικό Μέρος, ΠΝ Σάκκουλας, 2016, σελ. 556.

[75] Αντιθ. *Βασιλάκη Ε.,* Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σ. 215 επ. · *Κουράκης*, ό.π., ΠοινΛογ 2001, σ. 2593, όπου αναφέρει ότι μία ακόμα διαφορά μεταξύ της απάτης με η/υ και της κοινής απάτης, είναι και το γεγονός ότι στην πρώτη (απάτη με η/υ) δεν απαιτείται συσχετισμός του επιδιωκόμενου οφέλους με τη βλάβη της ξένης περιουσίας, φέροντας ως παράδειγμα την περίπτωση που κάποιος βλάπτει το σύστημα στοιχείων μίας επιχείρησης (δολιοφθορά) για να εισπράξει αμοιβή από τους ανταγωνιστές της.

[76] *Μυλωνόπουλος Χ.,* Ποινικό Δίκαιο-Ειδικό Μέρος, ΠΝ Σάκκουλας, 2016, σελ. 549

[77] *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 4η έκδ., άρθρ. 386Α, αρ 4.

[78] Αντίθετα, ο Παπαδαμάκης θεωρεί ότι *«μη ορθή διαμόρφωση προγράμματος»* υπάρχει όταν το πρόγραμμα *«εκ κατασκευής» είναι πρόσφορο («εμπεριέχει εγγενώς τον κίνδυνο») να επιφέρει περιουσιακή βλάβη τρίτου»»*, βλ. *Παπαδαμάκη Α.*, Τα Περιουσιακά Εγκλήματα, 3η εκδ, 2020, 156.

[79] Μπορεί να έχουμε εκπόνηση νέου, ολικά η μερικά, προγράμματος, ή μετέπειτα αλλοίωση του υπάρχοντος προγράμματος, ή με την απόκρυψη δεδομένων (holding back), *Μυλωνόπουλος Χ.*, Ποινικό Δίκαιο-Ειδικό Μέρος, ΠΝ Σάκκουλας, 2016, 549.

την υποκειμενική θεωρία «*το πρόγραμμα λειτουργεί ορθά όταν ανταποκρίνεται στη βούληση του νόμιμου κατόχου του*» ενώ σύμφωνα με την αντικειμενική θεωρία «*το πρόγραμμα λειτουργεί ορθά όταν εκπληρώνει την αποστολή του*». Αμφότερες αυτές οι θεωρίες εμφανίζονται προβληματικές στις περιπτώσεις που ο δράστης της απάτης είναι ταυτόχρονα και ο ιδιοκτήτης ή ο κατασκευαστής του προγράμματος, και αφενός η βούληση του κατόχου και αφετέρου η αποστολή του προγράμματος είναι ακριβώς το μη αποδεκτό από την έννομη τάξη αποτέλεσμα[80]. Ορθότερη εμφανίζεται η κανονιστική θεωρία (κανονιστικό κριτήριο), εκφρασμένη από τον Μυλωνόπουλο, σύμφωνα με την οποία «μη *ορθό είναι το πρόγραμμα όταν δεν ανταποκρίνεται στην κοινωνικά αποδεκτή αποστολή για την οποία προορίζεται».* Το πότε δε συμβαίνει αυτό, ο ίδιος το συναρτά με την προσφορότητα του να προκαλέσει βλάβη στην περιουσία τρίτου, σύμφωνα με την αρχή της επίτασης του κινδύνου[81].

Β. «Με χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή»:

Ο τυποποιούμενος αυτός στο νόμο τρόπος τέλεσης του 386^{A} αναφέρεται στην παράνομη παρέμβαση στο σύστημα του υπολογιστή. Η έννοια «σύστημα υπολογιστή», προφανώς αντιστοιχεί στην προϋφιστάμενη έννοια του «πληροφοριακού συστήματος», όπως αυτή ενυπήρχε στην αμέσως προϊσχύουσα μορφή της διάταξης (ν. 4411/2016), και η οποία έννοια ορίζεται στο άρθρο 13 ΠΚ παρ. στ΄. Κρίσιμο στοιχείο εν προκειμένω είναι το πως θα ερμηνευθεί ο όρος «παρέμβαση».

Ο Παπαδαμάκης περιγράφει αρκετά απλοϊκά το συγκεκριμένο τρόπο τέλεσης, ως «*επηρεασμό της διαδικασίας επεξεργασίας δεδομένων από το πληκτρολόγιο ή απορρύθμισης των μηχανικών μερών του υπολογιστή, που έχει ως αποτέλεσμα τη μεταβολή της λειτουργίας του»* σημειώνοντας μάλιστα[82] ότι ο τρόπος τέλεσης αυτός αφορά «*ένα πρόγραμμα που ήδη χρησιμοποιείται»*[83].

---

[80] Παράδειγμα τραπεζίτη που αλλοιώνει το πρόγραμμα τοκοφορίας *Μυλωνόπουλος Χ*., Ποινικό Δίκαιο-Ειδικό Μέρος, ΠΝ Σάκκουλας, 2016, σελ. 549-550, Μπουρμάς Γ., Στοιχεία απάτης με υπολογιστή κατ'άρθρο 386 α ΠΚ και διάκριση αυτής από την κοινή απάτη του άρθρου 386 ΠΚ, ΠοινΧρον ΝΑ΄, σελ.469

[81] *Μυλωνόπουλος ,* Ποινικό Δίκαιο-Ειδικό Μέρος, ΠΝ Σάκκουλας, 2016, σ. 549· βλ. και *Βασιλάκη Ε.*, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σ. 223, όπου θεωρεί ότι μη ορθό είναι ένα πρόγραμμα, όταν τα αποτελέσματα της εφαρμογής του έρχονται σε αντίθεση με μία νόμιμη κατάσταση.

[82] *Παπαδαμάκης Α*., Τα Περιουσιακά Εγκλήματα, 3^{η} εκδ, 2020, 158

[83] Σε αντίθεση δηλαδή με τη γνώμη του περί του πρώτου τρόπου τέλεσης που εφαρμόζεται σε πράξεις που αφορούν την εξαρχής μη ορθή κατασκευή του προγράμματος, βλ. υποσημ. 94

Κατά τη γνώμη του γράφοντος, και με δεδομένο τον ορισμό του πληροφοριακού συστήματος στο άρθρο 13 ΠΚ, στην οποία εμπεριέχεται η έννοια του «υπολογιστή»[84], ως «παρέμβαση στη λειτουργία προγράμματος/συστήματος υπολογιστή» μπορεί να νοηθεί: i) η εξωτερική παρέμβαση σε πληροφοριακό σύστημα/υπολογιστή, π.χ. η απορρύθμιση των μηχανικών μερών, όπως αναφέρει και ο Παπαδαμάκης, αλλά και η με οποιοδήποτε τρόπο σύνδεση εξωτερικής συσκευής σε πληροφοριακό σύστημα, που υποκλέπτει, αποκρυπτογραφεί και διανέμει τηλεοπτικό συνδρομητικό σήμα[85], ii) η εσωτερική παρέμβαση σε πληροφοριακό σύστημα/υπολογιστή, με την έννοια της back-end παρέμβασης, π.χ. διάσπαση της ασφάλειας πληροφοριακού συστήματος τράπεζας και η πίστωση λογιστικών μονάδων σε συγκεκριμένο λογαριασμό, χωρίς όμως ο δράστης να κάνει χρήση παρανόμως κτηθέντων ορθών στοιχείων τρίτου προσώπου και iii) η χωρίς δικαίωμα, front-end πρόσβαση σε πληροφοριακό σύστημα/υπολογιστή με χρήση παρανόμως κτηθέντων ορθών στοιχείων, όπως το παράδειγμα της αιτιολογικής έκθεσης του ν. 4411/2016 – παράνομη απόκτηση username και password τρίτου προσώπου, είσοδος στο e-banking και μεταφορά ποσών[86].

Εστιάζοντας καλύτερα σε κάθε μία από τις τρεις ανωτέρω περιπτώσεις συμπεριφορών, υπό στοιχεία -i-, -ii- και -iii-, διαπιστώνουμε ότι, η υπό στοιχείο -ii- συμπεριφορά (*back-end εσωτερική παρέμβαση με διάσπαση των συστημάτων ασφαλείας -firewalls)* αλλά και η υπό στοιχείο -iii- συμπεριφορά (*front end εξωτερική παρέμβαση με χρήση παρανόμως κτηθέντων ορθών στοιχείων)* θα μπορούσαν να υπαχθούν και στον κατωτέρω, υπό -Δ- τρόπο τέλεσης (*χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή)*, αφού χωρίς *άνευ δικαιώματος εισαγωγής κτλ δεδομένων υπολογιστή* δεν νοείται *επηρεασμός μιας διαδικασίας επεξεργασίας δεδομένων* και άρα δεν είναι δυνατή η επέλευση οποιασδήποτε περιουσιακής βλάβης.

---

[84] Ο ορισμός του «πληροφοριακού συστήματος» δεν άλλαξε στο Νέο Ποινικό Κώδικα, και επομένως, δεδομένου του ότι δεν υπήρξε άλλος, ειδικότερος ορισμός, για την έννοια του υπολογιστή, θεωρείται αυτονόητο ότι η έννοια του «υπολογιστή» εντάσσεται στην ευρύτερη έννοια του «πληροφοριακού συστήματος».

[85] ΣυμβΠλημΚιλκις 54/2012 ΠοινΔνη 2014 σ. 238. Υπό το προηγούμενο καθεστώς η συγκεκριμένη συμπεριφορά εντάχθηκε στον (τότε) δεύτερο τυποποιούμενο τρόπο τέλεσης της απάτης 386^{α}, την «επέμβαση κατά την εφαρμογή του προγράμματος», έτσι *Μυλωνόπουλος Χ.*, Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ 550

[86] «*Τροποποιείται το άρθρο 386Α Π.Κ. (απάτη υπολογιστή) κατά τα οριζόμενα στο άρθρο 8 της Σύμβασης. Σύμφωνα με τη νέα διάταξη περιλαμβάνεται πλέον ρητά στις περιπτώσεις απάτης με υπολογιστή και η χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα, όπως π.χ. στην περίπτωση του δράστη που έχει αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου.»*, σελ. 6 Αιτιολογικής έκθεσης.

Από το συνδυασμό των ανωτέρω σκέψεων προκύπτει ότι ο συγκεκριμένος τρόπος τέλεσης είναι αρκετά γενικός σε σχέση με τους άλλους τέσσερις. Για την ακρίβεια, οι άλλοι τέσσερις τρόποι τέλεσης είτε είναι ειδικότερες εκφάνσεις του 2ου μελετούμενου τρόπου τέλεσης, είτε προαπαιτούν το 2ο τρόπο τέλεσης για να είναι αποτελεσματικοί. Έτσι, δε νοείται επέλευση αποτελέσματος βλαπτικού για ξένη περιουσία, λόγω μη ορθής διαμόρφωσης προγράμματος από τον δράστη, αν ο ίδιος ο δράστης δεν «παρέμβει χωρίς δικαίωμα» στο σύστημα του υπολογιστή. Αντίστοιχα δε νοείται «εισαγωγή, αλλοίωση κτλ δεδομένων», αν πρώτα ο δράστης δεν «παρέμβει» στο σύστημα.

Εύλογα λοιπόν, δημιουργήθηκε στον γράφοντα η πεποίθηση ότι, η τυποποίηση από το νομοθέτη του συγκεκριμένου, αρκετά γενικού τρόπου τέλεσης, σε αντικατάσταση του αντίστοιχου *«χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα»*, όπως υπήρχε στην διά του Ν.4411/2016 μορφή του 386Α ΠΚ[87], είχε ως απώτερο σκοπό να δίδεται η δυνατότητα στους εφαρμοστές του Ποινικού Κώδικα, όταν θα κληθούν να αντιμετωπίσουν νέες μορφές απάτης με υπολογιστή, που δεν θα μπορούν να υπαχθούν σε κάποιον άλλο τρόπο τέλεσης, να μπορούν να τις υπαγάγουν στο συγκεκριμένο τρόπο, αφού δε νοείται απάτη με υπολογιστή χωρίς κάποιας μορφής παρέμβαση στο σύστημα του υπολογιστή.

Γ. «Με χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας»:

Σύμφωνα με τον τρίτο διαζευκτικό τρόπο τέλεσης του αδικήματος του 386Α, ο δράστης πρέπει να εισαγάγει στον υπολογιστή «μη ορθά ή ελλιπή δεδομένα[88]», με αποτέλεσμα να επέλθει η περιουσιακή μεταβίβαση. Είναι κοινώς αποδεκτό στη θεωρία[89] ότι τα «μη ορθά» και τα «ελλιπή» δεδομένα προσομοιάζουν με την

[87] Που με τη σειρά του είχε αντικαταστήσει το «*με οποιοδήποτε άλλο τρόπο»* που υπήρχε στην αρχική μορφή της διάταξης.

[88] Αντί του όρου «στοιχείων», που χρησιμοποιούνταν στην προισχύουσα μορφή της διάταξης. Ο δε όρος «στοιχεία» του υπολογιστή, ως έννοια, δεν ορίζονταν στον νόμο. Στον τεχνικό DIN-Norm 44300 Nr 19 (επεξεργασία δεδομένων), «στοιχεία» είναι «σημεία ή συνεχείς λειτουργίες με βάση γνωστές ή αποδεδειγμένες συμβάσεις, προς το σκοπό επεξεργασίας περιγεγραμμένων πληροφοριών. Σ' αυτά περιλαμβάνονται και τα προγράμματα του η/υ για την επεξεργασία δεδομένων. Στοιχεία του η/υ είναι όχι μόνο πληροφορίες που είναι προορισμένες να εξυπηρετούν τη διαδικασία επεξεργασίας, αλλά και άλλους σκοπούς (λ.χ. την προστασία κατά της εισόδου στα δεδομένα μ εξουσιοδοτημένων προσώπων, ως συνθηματικοί κώδικες), βλ. συναφώς *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 3η έκδ., άρθρ. 386Α, αρ 4.

[89]*Μυλωνόπουλος, Χ.,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ. 550, όπου παραπέμπει σε έτερο σύγγραμμα του · *Παπαδαμάκης Α,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις

«παράσταση ψευδών γεγονότων» και την «απόκρυψη ή παρασιώπηση αληθινών γεγονότων» που οδηγούν στην πλάνη του προσώπου στην κλασική απάτη του 386ΠΚ αντίστοιχα, με την έννοια ότι *«μη ορθά»* είναι τα δεδομένα εκείνα που εισάγει ο χρήστης χωρίς να είναι αληθή[90], ενώ *«ελλιπή»* είναι τα δεδομένα εκείνα που *«εκφράζουν την πραγματικότητα στην οποία αναφέρονται και η οποία έχει αποφασιστική σημασία για την επεξεργασία των δεδομένων»*[91, 92]. Ελλιπή είναι τα δεδομένα και όταν παρασιωπούνται κατά παράβαση υποχρέωσης αληθινά γεγονότα (λ.χ. η ενημέρωση για την περάτωση των σπουδών του τέκνου)[93]. Δεν είναι απαραίτητο η εισαγωγή των μη ορθών/ελλιπών δεδομένων στον να γίνεται από τον ίδιο το δράστη, αλλά μπορεί να γίνεται και μέσω τρίτου προσώπου που ενεργεί χωρίς δόλο και χωρίς αποφασιστική αρμοδιότητα, οπότε γίνεται λόγος για «έμμεση αυτουργία». Αν και ο χειριστής έχει τον απαιτούμενο από την μελετούμενη διάταξη δόλο, τότε εκείνος είναι ο αυτουργός και ο παρακινήσας ο ηθικός αυτουργός[94].

Κρίσιμο στοιχείο επίσης, στο συγκεκριμένο τρόπο τέλεσης είναι αν τα συγκεκριμένα μη ορθά ή ελλιπή δεδομένα, ελέγχονται από κάποιο φυσικό πρόσωπο στην πορεία από την εισαγωγή τους έως και πριν την περιουσιακή διάθεση, και αν ελέγχονται, πόσο αποφασιστικός είναι ο έλεγχος αυτός[95]. Με άλλα λόγια διαφοροποιείται το αδίκημα (και εφαρμόζεται η διάταξη του 386 ΠΚ) σε περίπτωση που εμπλακεί φυσικό πρόσωπο με αποφασιστική αρμοδιότητα για να διατάξει ή να απαγορεύσει την περιουσιακή διάθεση, και επί της ουσίας η «χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων» οδηγήσει στην πλάνη του προσώπου αυτού που εν συνεχεία διατάξει την περιουσιακή διάθεση[96]. Σε τέτοια περίπτωση μιλάμε για «απάτη μέσω υπολογιστή», αφού εν προκειμένω ο υπολογιστής αποτέλεσε το μέσο δια του οποίου ο

Σάκκουλα, 2000, σελ 188 · *Μπουρμάς,* Στοιχεία απάτης με υπολογιστή κατ'άρθρο 386 α ΠΚ και διάκριση αυτής από την κοινή απάτη του άρθρου 386 ΠΚ, ΠοινΧρον ΝΑ΄, σελ 470.

[90] π.χ. εισαγωγή στο σύστημα μεγαλύτερου αριθμού τέκνων από την πραγματικότητα για να εισπραχθεί επίδομα πολυτέκνου, παράδειγμα αναφερόμενο από αμφότερους τους Μυλωνόπουλο και Παπαδαμάκη, οι οποίοι παραπέμπουν στην *Βασιλάκη, Ε.*, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, Π.Ν. Σάκκουλας, 1993.

[91] «*και η οποία έχει αποφασιστική σημασία για την επεξεργασία των δεδομένων», Μυλωνόπουλος Χ.,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016 σελ. 550

[92] π.χ. η παράλειψη εισαγωγής στο σύστημα του διαζυγίου για να εισπράττεται το επίδομα συζύγου, *Μυλωνόπουλος Χ.,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ. 551

[93] *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 3η έκδ., άρθρ. 386Α, αρ 7.

[94] *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 4η έκδ., άρθρ. 386Α, αρ 6.

[95] Βλ. και *Μυλωνόπουλο*, Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ. 551.

[96] πχ όταν εργαζόμενος συμπληρώνει σε εφαρμογή της εργοδότριάς του τις ώρες που εργάστηκε επιπλέον του ωραρίου του (αντί της παλιάς μεθόδου να στέλνει έγγραφο με υπογραφή), και τα δεδομένα αυτά (επιπλέον ώρες) ελέγχονται από τον υπεύθυνο του λογιστηρίου

δράστης επικοινώνησε στο αποφασίζον φυσικό πρόσωπο τα δεδομένα που το παραπλάνησαν.

Στο συγκεκριμένο τρόπο τέλεσης (όπως και στον κατωτέρω, υπό -Δ-) προστέθηκε το πρώτον με το Νέο Ποινικό Κώδικα και ένα ειδικό εδάφιο, προσδιοριστικό του είδους των μη ορθών/ελλιπών δεδομένων, που αφορά τα «δεδομένα αναγνώρισης της ταυτότητας». Εν αντιθέσει με τον επόμενο, υπό στοιχείο -Δ- τρόπο τέλεσης, η προσθήκη στον παρόντα τρόπο τέλεσης του συγκεκριμένου προσδιοριστικού εδαφίου είναι, κατά τη γνώμη του γράφοντος, ατυχής ως αλυσιτελής. Ειδικότερα, για να γίνει λόγος για χρησιμοποίηση «δεδομένων αναγνώρισης της ταυτότητας» προϋποτίθεται ότι στη μνήμη του «προς εξαπάτηση» υπολογιστή υπάρχουν ήδη αποθηκευμένα τα συγκεκριμένα «ορθά» δεδομένα αναγνώρισης της ταυτότητας του χρήστη (π.χ. ονοματεπώνυμο, username και password), στα οποία ο υπολογιστής ανατρέχει, ακριβώς για να ταυτοποιήσει ότι αυτός που εισάγει τα συγκεκριμένα δεδομένα είναι το ίδιο πρόσωπο με αυτό του οποίου τα στοιχεία έχει στη μνήμη του και να του επιτρέψει ακολούθως να εισάγει συγκεκριμένα δεδομένα που δυνητικά μπορούν να οδηγήσουν σε περιουσιακή διάθεση. Αν επομένως ο χρήστης του υπολογιστή εισάγει *μη ορθά ή ελλιπή δεδομένα αναγνώρισης ταυτότητας*, όπως η διάταξη αναφέρει, εξ υπαρχής δε θα υπάρχει ταυτοποίηση της ταυτότητάς του και άρα το ίδιο το σύστημα του υπολογιστή θα αρνηθεί οποιαδήποτε πρόσβαση. Φαίνεται επομένως ότι εν προκειμένω ο νομοθέτης παρασύρθηκε και εισήγαγε τη συγκεκριμένη φράση και στο συγκεκριμένο εδάφιο, αφού η λογική υποδεικνύει ότι η χρήση μη ορθών/ελλιπων δεδομένων αναγνώρισης ταυτότητας οδηγεί ακριβώς στη μη αναγνώριση της ταυτότητας.

Δ. *«Με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας»:*

Ο τέταρτος κατά σειρά τυποποιούμενος τρόπος τέλεσης του υπό μελέτη αδικήματος ήρθε σε αντικατάσταση προς το πληρέστερο του αντίστοιχου τρόπου της προϋφιστάμενης διάταξης (*«χωρίς δικαίωμα χρήση δεδομένων»*). Βαρύτητα πρέπει να δοθεί στους όρους «δεδομένα» και «χωρίς δικαίωμα». Ο όρος «δεδομένα» θα μπορούσε να ερμηνευθεί ως «ορθά και πλήρη δεδομένα»[97], καθώς η χρήση μη ορθών ή ελλιπών δεδομένων τυποποιείται ήδη στο προηγούμενο εδάφιο, πλην όμως, κατά τη

[97] Σύμφωνα με την εκ της αιτιολογικής έκθεσης του Ν. 4411/2016 αντλούμενης ερμηνείας, όπου για τον τότε αντίστοιχο τρόπο τέλεσης (*«χωρίς δικαίωμα χρήση δεδομένων»)* γίνονταν ρητή αναφορά σε χρήση «ορθών» δεδομένων. Βλ. και παρακάτω υποσημείωση 115.

γνώμη του γράφοντος, τέτοια ερμηνεία θα λειτουργούσε συσταλτικά, αφού σκοπός της διάταξης είναι η ποινικοποίηση οποιουδήποτε είδους χωρίς δικαίωμα επεξεργασίας (*εισαγωγή, αλλοίωση κτλ)* δεδομένων, που έχουν ως αποτέλεσμα περιουσιακή βλάβη. Η προϋπόθεση *«χωρίς δικαίωμα»* αναλύεται εκτενώς παρακάτω[98]. Τέλος, η προσθήκη στη συγκεκριμένη διάταξη του όρου «*ιδίως δεδομένων αναγνώρισης ταυτότητας»*, εν αντιθέσει με ανωτέρω, έχει αντίκρισμα, ειδικά όταν γίνεται λόγος για «χωρίς δικαίωμα εισαγωγή ορθών δεδομένων αναγνώρισης ταυτότητας», ενέργεια που από μόνη της μπορεί να επιφέρει περιουσιακή διάθεση[99]. Σημειωτέον ότι στην αιτιολογική έκθεση του Ν. 4411/2016[100], όταν και είχε πρωτοεισαχθεί ως τρόπος τέλεσης η «χωρίς δικαίωμα χρήση δεδομένων», που είναι αντίστοιχη με τον υπό μελέτη τρόπο, φέρονταν ως παράδειγμα η χωρίς δικαίωμα χρήση username και password. Λόγω της ομοιότητας της προηγούμενης με την παρούσα διάταξη, το εν λόγω παράδειγμα θα μπορούσε να αναφερθεί εκ νέου, ειδικά λόγω και της προσθήκης των «δεδομένων αναγνώρισης ταυτότητας» ως «ειδικής κατηγορίας δεδομένων» που εμπίπτουν στο συγκεκριμένο τρόπο. Σε κάθε περίπτωση, πρέπει να σημειωθεί ότι στην έως σήμερα εκδοθείσα βιβλιογραφία που τέθηκε υπόψη του γράφοντος και αφορά τον 386^{A} Νέου ΠΚ, δεν βρέθηκαν αναφορές ή σχόλια ή ερμηνείες σχετικά με την επιλογή του νομοθέτη να εντάξει τα «δεδομένα αναγνώρισης ταυτότητας» στο πραγματικό της διάταξης. Σε κάθε περίπτωση, καθώς δεν προκύπτει ότι η χωρίς δικαίωμα εισαγωγή/αλλοίωση κτλ δεδομένων αναγνώρισης ταυτότητας αλλάζει κάτι ως προς την εφαρμογή της διάταξης (π.χ. θα μπορούσε να είναι επιβαρυντική περίσταση), συμπεραίνουμε ότι η αναφορά του συγκεκριμένου είδους δεδομένων αποτελεί απλώς ενδεικτική απαρίθμηση/παράδειγμα.

Το ιδανικότερο παράδειγμα που ταιριάζει στο συγκεκριμένο τρόπο τέλεσης είναι αυτό της χρήσης από το δράστη (κλεμμένης/απωλεσθείσας) πιστωτικής ή χρεωστικής κάρτας τρίτου προσώπου[101], αφού στην συγκεκριμένη περίπτωση αρκεί η χωρίς δικαίωμα εισαγωγή στο υπολογιστικό σύστημα των (ορθών) στοιχείων προκειμένου να επηρεαστεί το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών

[98] Κεφάλαιο 4.3.1.2.

[99] π.χ. χωρίς δικαίωμα χρήση από το δράστη του username και password του MyTaxisNet τρίτου προσώπου, για υποβολή αίτησης λήψης έκτακτου επιδόματος, δηλώνοντας ταυτόχρονα δικό του (του δράστη) τραπεζικό λογαριασμό. Εν προκειμένω, όλα τα δεδομένα που εισάγονται είναι «ορθά» - ιδίως αυτά της «αναγνώρισης ταυτότητας»- πλην όμως η περιουσιακή διάθεση επέρχεται «χωρίς δικαίωμα» λόγω της «αλλοίωσης» του δηλωμένου τραπεζικού λογαριασμού.

[100] *Βλ.* παραπάνω, υποσημείωση 92.

[101] *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 4^{η} έκδ., άρθρ. 386^{A}, αρ 7.

δεδομένων και να επέλθει περιουσιακή διάθεση. Η συγκεκριμένη συμπεριφορά και ο χαρακτηρισμός της ως ποινικά κολάσιμη πράξη που εμπίπτει στην διάταξη του 386^{A} είχε δημιουργήσει θεωρητικές έριδες, όπως αναλύθηκε ανωτέρω και υπό το πρίσμα του προϊσχύσαντος δικαίου σε προηγούμενο κεφάλαιο (2.5.). Όπως μάλιστα ήδη σημειώθηκε (στο Κεφάλαιο 3.2.2.), η τυποποίηση της «χωρίς δικαίωμα χρήσης δεδομένων» με τον Ν. 4411/2016 είχε τερματίσει αυτές τις έριδες, αφού πλέον δε φαινόταν ότι τίθεται το ερώτημα αν η «χρήση κλεμμένης κάρτας» υπάγεται ή όχι στο 386^{A}. Γι' αυτό και είναι άξιο αναφοράς ότι ο Παπαδαμάκης εμμένει έως και σήμερα[102] στην ίδια (και αντίθετη με τους λοιπούς θεωρητικούς[103] και τη νομολογία του Αρείου Πάγου[104]) άποψη, ότι δηλαδή «*η χρήση* (σ.σ. εισαγωγή, αλλοίωση κτλ) *δεδομένων δεν πρέπει να εξαντλείται στην απλή εκμετάλλευση των δυνατοτήτων του υπολογιστή, αλλά να εμπεριέχει μεθόδευση»*, καταλήγοντας ότι «*η χρήση κλεμμένης πιστωτικής κάρτας δεν συνιστά επηρεασμό του προγράμματος ή των δεδομένων υπολογιστή αλλά εκμετάλλευση της λειτουργίας του υπολογιστή»*.

Ε. «Με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων»:

Ο πέμπτος τρόπος τέλεσης του αδικήματος της απάτης με υπολογιστή, αποτελεί μία νεοεισαχθείσα διάταξη του νέο Ποινικού Κώδικα, η οποία εισήχθη το πρώτον με το ν. 4619/2019. Με τον τρόπο αυτό τέλεσης και την ευρεία διατύπωση που χρησιμοποιεί (σκόπιμη επιλογή του όρου «αξιοποίησης»), ο Έλληνας νομοθέτης επιχειρεί να συμπεριλάβει κάθε είδους παρεμβολή του δράστη σε εφαρμογές ηλεκτρονικών πληρωμών, όπως το Internet Banking και το Phone Banking[105]. Κατά τη γνώμη του γράφοντος, η συγκεκριμένη διάταξη είναι «όσο γενική χρειάζεται να είναι», σε μία ύστατη προσπάθεια του νομοθέτη να ποινικοποιηθεί οποιαδήποτε πράξη παράνομης (χωρίς δικαίωμα) χρήσης εφαρμογών ηλεκτρονικής πληρωμής. Δεδομένης δε της ταχύτατης εξέλιξης του είδους των «παράνομων παρεμβολών», είναι σαφές ότι η γενικότητα της διάταξης αποσκοπούσε στην δημιουργία του απαραίτητου οπλοστασίου για να αντιμετωπιστούν και όσες συμπεριφορές θα εμφανιστούν το

[102] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, 3η εκδ, 2020, σελ. 159-160

[103] Όπως αναφέρθηκαν στα ανωτέρω Κεφάλαια 2.5. και 3.2.2. και απαριθμούνται και στο έργο των *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 4η έκδ., άρθρ. 386^{A}, αρ 7, όπου γίνεται παραπομπή σε «*Μυλωνόπουλο ΠοινΔ ΕιδΜ αρθρ. 372-406 σ. 54,602 • Κιούπης, Ποιν.Δίκαιο και Ίντερνετ, σ. 116 • Ναμίας Ο., ΠΧ ΝΓ 490*

[104] Ενδεικτικά ΑΠ 131/2013, 813/2015, 1414/2017 - ΝΟΜΟΣ

[105] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, 3η εκδ, 2020, 162

πρώτον στο μέλλον, ως συνέπεια της πιθανολογούμενης ακόμη μεγαλύτερης τεχνολογικής ανάπτυξης της πληροφορικής.

Τέλος, παρόλο που γίνεται αναφορά σε λογισμικά που αφορούν μετακίνηση «*χρημάτων*», στο συγκεκριμένο τρόπο τέλεσης πρέπει να υπαχθούν, κατά τη γνώμη του γράφοντος, και τυχόν παρεμβολές σε αξιοποίηση λογισμικού που προορίζεται για συναλλαγές μέσω κρυπτονομισμάτων. Είναι βέβαιο ότι τα επόμενα χρόνια, και όσο αυξάνονται οι χρήστες κρυπτονομισμάτων αλλά και οι έμποροι και πάροχοι υπηρεσιών που θα δέχονται τιμήματα και αμοιβές σε κρυπτονομίσματα, μοιραία θα αυξηθούν και οι εγκληματικές συμπεριφορές που θα στρέφονται εναντίον των αντίστοιχων λογισμικών. Και μπορεί, έως σήμερα, η μεν Ευρωπαϊκή Ένωση να μην έχει δημιουργήσει ένα νομικό πλαίσιο γύρω από την ολοένα αυξανόμενη χρήση των κρυπτονομισμάτων, το δε Δικαστήριο της Ευρωπαϊκής Ένωσης να απέρριψε την σκέψη τα κρυπτονομίσματα να θεωρηθούν «χρήματα»[106] κατά την έννοια της Οδηγίας 2009/110/ΕΚ[107], όμως δε μπορεί κανείς να αμφισβητήσει ότι αφού τα κρυπτονομίσματα και οι εφαρμογές διακίνησης αυτών αποτελούν πλέον μέρος της κοινωνικοοικονομικής ζωής, τυχόν περιπτώσεις «χωρίς δικαίωμα χρήσης» του λογισμικού που προορίζεται για τη μετακίνηση και τις συναλλαγές με κρυπτονομίσματα, δε μπορούν παρά να εμπίπτουν στο αδίκημα της «απάτης με υπολογιστή», αφού σαφέστατα μπορεί να υπάρξει περιουσιακή διάθεση και άρα βλάβη ξένης περιουσίας. Παρόλο που η περιουσιακή αυτή βλάβη δε συνίσταται σε ευρώ ή άλλο νόμιμο νόμισμα, αφ' ης στιγμής μπορεί να αποδοθεί και να έχει αντίστοιχο αντίκρισμα, μέσω της ισοτιμίας, στα γνωστά στο νομοθέτη και στο δικαστήριο νομίσματα, η συμπεριφορά που την επέφερε (τη βλάβη), πρέπει επομένως να διώκεται ποινικά[108].

---

[106] ΔικΕΕ, Skatteverket v David Hedqvist, C 264/14, σκέψη 42

[107] Ενσωματώθηκε στην ελληνική νομοθεσία με το Ν. 4261/2014.

[108] Υπό το ανωτέρω πρίσμα είναι σαφές ότι ορθά κινήθηκε το Συμβούλιο Εφετών Θεσσαλονίκης, με την υπ' αρ. 690/2017 απόφασή του, γνωμοδοτώντας επί αιτήματος του Εισαγγελέα Εφετών ως προς το αν πρέπει ή όχι να εκδοθεί στις ΗΠΑ κατηγορούμενος στον οποίο αποδίδονταν πράξεις σχετιζόμενες με διατήρηση ιστοσελίδας ανταλλαγής κρυπτονομισμάτων και μέσω αυτής ξεπλύματος βρώμικου χρήματος, όταν και έκρινε ότι, *όλες οι αποδιδόμενες πράξεις (εκτός από αυτήν της λειτουργίας μη αδειοδοτημένης επιχείρησης χρηματικών συναλλαγών) ανεξάρτητα από την κατηγορία εγκλημάτων στην οποία κατατάσσονται, τον τρόπο περιγραφής τους και την χρησιμοποιούμενη γι' αυτές ορολογία στο ποινικό δίκαιο των Η.Π.Α., είναι αξιόποινες και κατά την ελληνική νομοθεσία και στοιχειοθετούν, κατ' αντιστοιχία, τη νομοτυπική μορφή του εγκλήματος της…., της διακεκριμένης απάτης με υπολογιστή (άρθρο 386Α σε συνδυασμό με το άρθρο 386 παρ. 2 του Ποινικού Κώδικα)*. Βλ. ΣΤΕ (ολομ) 110/2020, 15η σκεψη, ΝΟΜΟΣ.

4.3.1.2: Ο όρος «χωρίς δικαίωμα» που αναφέρεται τρόπους τέλεσης

Σκόπιμο κρίνεται εν προκειμένω να δοθεί ο ορισμός του όρου *«χωρίς δικαίωμα»* που αναφέρεται στους ανωτέρω τρόπος τέλεσης του επηρεασμού. Καθώς στο συγκεκριμένο άρθρο δεν ορίζεται η συγκεκριμένη έννοια, οδηγούμαστε αρχικά στο ν. 4411/2016 με τον οποίο εισήχθησαν το πρώτον η συγκεκριμένη έννοια, και εν συνεχεία στην Οδηγία 2013/40/ΕΕ η οποία μεταφέρθηκε στο εθνικό μας δίκαιο με τον συγκεκριμένο νόμο και συγκεκριμένα το άρθρο 2 αυτού. Στο άρθρο 2 περ. δ΄ της οδηγίας βρίσκουμε τον παρακάτω ορισμό: *«χωρίς δικαίωμα»: η αναφερόμενη στην παρούσα οδηγία 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.*

Προκύπτει επομένως ότι χωρίς δικαίωμα στο άρθρο 386^{Α} ΠΚ ενεργεί όποιος χρησιμοποιεί δεδομένα ή παρεμβαίνει σε πληροφοριακό σύστημα/ηλεκτρονικό υπολογιστή, χωρίς να έχει συναίνεση του ιδιοκτήτη ή άλλου νόμιμου δικαιούχου ή η συγκεκριμένη συμπεριφορά απαγορεύεται εν γένει από άλλη διάταξη νόμου. Είναι δε το στοιχείο αυτό ειδικό στοιχείο του αδίκου, *«που οριστικοποιεί τον άδικο χαρακτήρα της σχετικής συμπεριφοράς, μόνο όταν αυτή γίνεται χωρίς δικαίωμα»*[109].

4.3.2. Υποκειμενική Υπόσταση

Για την πράξη της απάτης του 386^{Α}, ήτοι την βλάβη ξένης περιουσίας με επηρεασμό του αποτελέσματος της διαδικασίας επεξεργασίας ψηφιακών δεδομένων αρκεί ο ενδεχόμενος δόλος. Στο σημείο αυτό εντοπίζεται και μία ακόμη διαφορά της ηλεκτρονικής απάτης από την κοινή απάτη: Τούτο διότι ενώ στην ηλεκτρονική απάτη αρκεί, ως προς όλα τα στοιχεία της αντικειμενικής υπόστασης ενδεχόμενος δόλος, στην κοινή απάτη και δη στην παράσταση ψευδών γεγονότων ως αληθών απαιτείται δόλος β΄ βαθμού («εν γνώσει»)[110].

Για να καταφαθεί όμως αρχικός καταλογισμός της πράξης πρέπει να υφίσταται και άμεσος δόλος α' βαθμού ως προς τον προσπορισμό στο δράστη ή σε τρίτο περιουσιακού οφέλους. Επομένως, ακριβώς όπως και στην κλασική απάτη του 386 ΠΚ, συζητάμε για έγκλημα σκοπού και «*υπερχειλούς υποκειμενικής υπόστασης»*[111].

---

[109] *Παπαδαμάκης Α.*, Τα Περιουσιακά Εγκλήματα, 3η εκδ, 2020, 162

[110] *Κουράκης Ν,* Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001, σ. 2593.

[111] *Μυλωνόπουλος Χ,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ 557. Άξιο αναφοράς είναι το παράδειγμα που δίνεται εδώ από τον Μυλωνόπουλο, καθώς προκύπτει ένα ιδιαίτερο κενό που υπήρχε στο Νόμο πριν τον Ν. 4411/2016. Αναφέρει λοιπόν το παράδειγμα εργαζομένου, που για

4.3.3. Απόπειρα – Συμμετοχή – Ποινές

Με το Νέο Ποινικό Κώδικα τροποποιήθηκε και η παράγραφος 1 του άρθρου 42 ΠΚ, που περιέχει τον ορισμό της απόπειρας. Έτσι αντικαθιστώντας ο νομοθέτης τη φράση «*επιχειρεί πράξη που περιέχει τουλάχιστον αρχή εκτέλεσης*», με την εμπεριέχουσα σήμερα στη διάταξη αυτή φράση «*αρχίζει να εκτελεί την περιγραφόμενη στον νόμο πράξη*», συρρίκνωσε την έννοια της απόπειρας. Έτσι σε αντίθεση με την ευρύτερη έννοια που είχε η απόπειρα στην προγενέστερη μορφή του άρθρου[112], σήμερα προσδιορίζεται το περιεχόμενο της αρχής εκτέλεσης του εγκλήματος στο πλαίσιο της απόπειρας κατά τρόπο, ώστε να είναι σαφές ότι για να θεμελιωθεί αξιόποινο πρέπει να έχει αρχίσει να πραγματώνεται ένα μέρος της αντικειμενικής υπόστασης του εγκλήματος[113].

Ως αρχή δε εκτέλεσης του εγκλήματος της απάτης με υπολογιστή χαρακτηρίζονταν, προ της τροποποιήσεως της διάταξης της απάτης με υπολογιστή, από τους συγγραφείς η «*έναρξη του επηρεασμού των στοιχείων του υπολογιστή*»[114]. Πλέον, με την ύπαρξη της φράσης «αποτέλεσμα της διαδικασίας επεξεργασίας δεδομένων υπολογιστή» ως αντικείμενο της μετοχής «επηρεάζοντας», ορθότερο θα ήταν να πούμε ότι αρχή εκτέλεσης υπάρχει όταν ο δράστης τελεί εκείνη την ενέργεια - έναν δηλαδή από τους προαναφερόμενους τρόπους τέλεσης ή με τμήμα αυτού-, που αναπόδραστα θα οδηγήσει τη διαδικασία της επεξεργασίας στο αποτέλεσμα που επιδιώκει ο δράστης και κατά συνέπεια και στην περιουσιακή βλάβη, χωρίς ωστόσο να κατορθώσει να επέλθει η βλάβη στην ξένη περιουσία[115]. Τούτο διότι το έγκλημα θεωρείται

να εκδικηθεί τον εργοδότη του εισάγει ψευδή στοιχεία στο σύστημα της επιχείρησης, ώστε αυτή να παραλύσει, χωρίς να προσδοκά περιουσιακό όφελος. Η συγκεκριμένη πράξη, λόγω έλλειψης του ειδικού σκοπού δε θα τιμωρούνταν βάσει 386^{A}. Δε θα μπορούσε να τιμωρηθεί όμως ούτε με το 389ΠΚ (απατηλή πρόκληση βλάβης), αφού το τελευταίο απαιτεί παραπλάνηση φυσικού προσώπου! Βέβαια, η συγκεκριμένη πράξη, μετά το Ν. 4411/2016, και πριν την θέση σε εφαρμογή του Νέου Ποινικού Κώδικα, θα μπορούσε να ενταχθεί στο 381^{A} ΠΚ (Φθορά ηλεκτρονικών δεδομένων) · *Κουράκης Ν*, Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001, σ. 2593.

[112]Ως αρχή εκτελέσεως οριζόταν από την νομολογία –στην προϊσχύουσα μορφή της υπό εξέταση διάταξης- κάθε ενέργεια, η οποία αποτελούσα τμήμα εν όλω ή εν μέρει της αντικειμενικής υποστάσεως του εγκλήματος, άγει αναμφισβητήτως και ευθέως στην πραγμάτωση αυτού ή τελεί προς αυτή σε τέτοια αναγκαία και άμεση σχέση συνάφειας, ώστε κατά κοινή αντίληψη να θεωρείται τμήμα αυτής, οδηγώντας άμεσα σε αυτήν, αν δεν ανακοπεί για οποιοδήποτε λόγο, βλ. *Χαραλαμπάκη Α.,* Ο Νέος Ποινικός Κώδικας, σελ. 15.

[113] βλ. συναφώς και Αιτιολογική έκθεση ν. 4619/2019, όπου αναφέρει περαιτέρω ότι με τον τρόπο αυτό η ποινή της απόπειρας συναρτάται με την πράξη που έχει τελεστεί και όχι με τον δόλο του υπαιτίου.

[114] *Μυλωνόπουλος*, Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ 558.

[115] Βλ. συναφώς *Παπαδαμάκη Α,* Τα Περιουσιακά Εγκλήματα, 3^{η} εκδ, 2020, σελ 192.

τετελεσμένο όταν επέλθει η περιουσιακή βλάβη. Εξυπακούεται δε ότι για την ολοκλήρωση του εγκλήματος δεν απαιτείται να προσποριστεί και το προσδοκώμενο όφελος.

Ιδιαίτερα ζητήματα συμμετοχής δεν τίθενται[116]. Η πράξη τελείται και κατά συναυτουργία[117], ενώ είναι δυνατή και η έμμεση αυτουργία, όταν σε επαφή με τον ηλεκτρονικό υπολογιστή (π.χ. εισαγωγή δεδομένων) έρχεται καλόπιστος τρίτος που ενεργεί εν αγνοία του[118].

Η υπό μελέτη αξιόποινη πράξη αποτελεί στη βασική της μορφή πλημμέλημα. Ως προς τις ποινές που απειλούνται σε βάρος του δράστη της συγκεκριμένης αξιόποινης πράξης (στη βασική της μορφή), αξίζει να αναφερθεί ότι η διάταξη δεν κάνει καμία αναφορά στο πλαίσιο ποινής του, παραχωρώντας κατ' αυτόν τον τρόπο το δικαίωμα στον εκάστοτε δικαστή, να εξαντλήσει τα ανώτατα όρια φυλάκισης, ανάλογα με το βαθμό της προσβολής. Αν όμως η ζημία είναι ιδιαίτερα μεγάλη, και συγκεκριμένα εάν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000 ευρώ, επιβάλλεται κάθειρξη έως δέκα έτη και χρηματική ποινή. Συνάγεται ως εκ τούτου ότι η κακουργηματική μορφή του βασικού εγκλήματος στηρίζεται σε ενιαίο ποσοτικό κριτήριο (ζημία άνω των 120.000€)[119].

4.3.4. Η ποινικοποίηση των προπαρασκευαστικών πράξεων

Με το Νέο Ποινικό Κώδικα θεσμοθετήθηκε το πρώτον ως ποινικό αδίκημα η πράξη κατασκευής, διάθεσης και κατοχής προγραμμάτων ή συστημάτων υπολογιστή, που εκ φύσεως προορίζονται για την τέλεση του αδικήματος της απάτης με υπολογιστή, με την πρόσθεση 2ης παραγράφου στο άρθρο 386Α.

Με την δεύτερη αυτή παράγραφο, ο Έλληνας νομοθέτης διεύρυνε το αξιόποινο και τιμώρησε κατ' εξαίρεση, τις συγκεκριμένες πράξεις, ως προπαρασκευαστικές του

[116] Βλ. και *Παπαδαμάκη Α.,* Τα Περιουσιακά Εγκλήματα, 3η εκδ, 2020, σελ 192, όπου αναφέρει ότι όλες οι μορφές συμμετοχής και η συναυτουργία είναι δυνατές στο έγκλημα · *Μυλωνόπουλο Χ,* Ποινικό Δίκαιο- Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ 558.

[117] Βλ. συναφώς ΑΠ (ΠΟΙΝ) 1166/2019 –ΝΟΜΟΣ, όπου αναφέρει ότι: *«Ειδικότερα, απάτη με υπολογιστή μπορεί να τελεστεί και κατά συναυτουργία όταν περισσότεροι επεμβαίνουν ευθέως, είτε συγχρόνως από κοινού είτε διαδοχικά, μετά όμως από συναπόφασή, δηλαδή με κοινό δόλο και με σκοπό παράνομου περιουσιακού οφέλους, στην εξέλιξη του προγράμματος ή και στα μηχανικά μέρη του υπολογιστή και με μη ορθή διαμόρφωση του προγράμματος ή με τη χρησιμοποίηση κατά τον προγραμματισμό του συστήματος μη ορθών ή ελλιπών στοιχείων, προκαλούν αποτέλεσμα διαφορετικό από εκείνο που θα προέκυπτε από τη διαδικασία της επεξεργασίας των στοιχείων».*

[118] *Μυλωνόπουλος,* Ποινικό Δίκαιο- Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016, σελ 558.

[119] βλ. συναφώς και Αιτιολογική έκθεση ν. 4619/2019.

κύριου αδικήματος πράξεις[120, 121] προφανώς θεωρώντας ότι αυτές ενέχουν ιδιαίτερη επικινδυνότητα, που η έννομη τάξη αδυνατεί να ανεχθεί και κατ' αναλογία και άλλων διατάξεων του ΠΚ, οι οποίες επίσης τιμωρούν τις προπαρασκευαστικές πράξεις. Εξάλλου η ρύθμιση αυτή φαίνεται να συμβαδίζει με διεθνή κείμενα, αφού συναφή πρόβλεψη υπάρχει και εντός της Οδηγίας 2013/40/ΕΕ και του άρθρου 6 της Σύμβασης της Βουδαπέστης, όπου γίνεται και εκεί αναφορά στην ποινικοποίηση των προπαρασκευαστικών πράξεων εγκλημάτων όπως η παράνομη πρόσβαση, υποκλοπή, παρεμβολές σε δεδομένα και σε συστήματα[122]. Στο δε δράστη τέλεσης αυτών απειλείται ποινή φυλάκισης έως και δύο ετών.

Παρόλο που στη νεότερη βιβλιογραφία δε γίνεται ιδιαίτερη ανάλυση των όρων του συγκεκριμένου αδικήματος, οφείλουμε να παρατηρήσουμε ότι η επιλογή του νομοθέτη να χρησιμοποιήσει διαζευκτικά τους όρους «*πρόγραμμα»* και *«σύστημα υπολογιστή»*, δε μπορεί παρά να σημαίνει ότι τιμωρητέα είναι η κατασκευή, κατοχή κτλ τόσο λογισμικού (software) όσο και συσκευών (hardware).

Τέλος, προσοχή πρέπει να δοθεί στην ερμηνεία του όρου «*προορίζεται»*, υπό την έννοια ότι κατά την απαγγελία κατηγορίας σε κάτοχο τέτοιου προγράμματος ή συστήματος υπολογιστή πρέπει να γίνεται σαφής αναφορά στις δυνατότητες του συγκεκριμένου προγράμματος, άλλως, όπως εύστοχα παρατηρείται και από τον Παπαδαμάκη, πολύς κόσμος που ασχολείται με υπολογιστές θα μπορούσε «*να έρθει αντιμέτωπος με εύκολες και πρόχειρες ποινικοποιήσεις»*[123].

4.3.5. Απάτη με Υπολογιστή κατά του Δημοσίου

Είναι αξιοσημείωτο ότι, έως τη θέση σε ισχύ του Νέου Ποινικού Κώδικα, με το άρθρο 462 του οποίου και καταργήθηκε ο «Νόμος Περί Καταχραστών του Δημοσίου» (Ν. 1608/1950), είχε αναπτυχθεί μία σημαντική διχογνωμία, αν και κατά πόσο οι επιβαρυντικές διατάξεις του νόμου αυτού εφαρμόζονται και στην απάτη με

[120] *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 4η έκδ., άρθρ. 386Α, αρ 12

[121] *Παπαδαμάκης Α.*, Τα Περιουσιακά Εγκλήματα, 3η εκδ, 2020, 163

[122] Το άρθρο 6 της Σύμβασης τα Βουδαπέστης αναφέρεται στην υποχρέωση των κρατών να ποινικοποιήσουν τις προπαρασκευαστικές πράξεις των περιγραφόμενων στα άρθρα 2 έως 5 περί παράνομων προσβάσεων, παρεμβολών σε συστήματα κτλ, πλην όμως είναι σαφές ότι, τελολογικά ερμηνευόμενης της διάταξης, σκοπός ήταν η λήψη μέτρων ποινικοποίησης της παραγωγής, κατοχής και διάθεσης οποιουδήποτε είδους software και hardware προορίζεται για παράνομες δραστηριότητες.

[123] *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, 3η εκδ, 2020, 163

υπολογιστή, δεδομένου του ότι ενώ στο άρθρο 1 δε γινόταν ρητή αναφορά περί τούτου[124].

Με την κατάργηση του ανωτέρω νόμου και τη θέση σε ισχύ του Νέου Ποινικού Κώδικα, ο Έλληνας Νομοθέτης φρόντισε να εντάξει, σε όποιο αδίκημα έκρινε τούτο σκόπιμο, επιμέρους επιβαρυντική διάταξη για τις περιπτώσεις που τελείται εις βάρος του δημοσίου. Έτσι σήμερα προβλέπεται ρητά στην παράγραφο 3 ότι εάν η απάτη με υπολογιστή στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000 ευρώ, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή έως χίλιες ημερήσιες μονάδες, με την πράξη να παραγράφεται μετά είκοσι έτη[125].

[124] Υπέρ της άποψης ότι χωρεί εφαρμογή: ΠεντΕφΑθ 678, 751/1988, ΠοινΛογ 2001, όπου δέχεται ότι το έγκλημα της απάτης με υπολογιστή είναι κλασσική απάτη, διαφέρει δε μόνο στο ότι η βλάβη της ξένης περιουσίας προκαλείται όχι από εξαπάτηση φυσικού προσώπου, αλλά από επέμβαση σε Η/Υ και ως εκ τούτου η απάτη με υπολογιστή, μπορεί να υπαχθεί στο ν. 1608/1950. Αντιθ. ΑΠ 1270/1993, ΠοινΛογ 2001, σελ. 2586, όπου δέχεται ότι η απάτη με υπολογιστή δεν περιλαμβάνεται στα εγκλήματα που προβλέπει το α. 1 του ν. 1608/1950 · *Κουράκης Ν*, Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001, σελ. 2594, όπου αναφέρει ότι η διατύπωση του ν. 1608/1950 δεν επιτρέπει επέκταση της εφαρμογής του στην ηλεκτρονική απάτη, αφού κάτι τέτοιο θα αποτελούσε συνταγματικά απαγορευμένη αναλογική επέκταση του αξιοποίνου.

[125]Βλ συναφώς και Αιτιολογική έκθεση ν. 4619/2019 όπου αναφέρει, ότι η ρητή πρόβλεψη αυτή του εδαφίου α΄, της παραγράφου 3 του άρθρου 386^{Α} σε συνδυασμό με την επιμήκυνση του χρόνου της παραγραφής (είκοσι έτη αντί δεκαπέντε), εξασφαλίζει την μείζονα προστασία της πράγματι δημόσιας περιουσίας και καθιστά περιττό τον απαρχαιωμένο και άκρως προβληματικό Ν. 1608/50, ο οποίος καταργήθηκε.

Κεφάλαιο 5ο: Το αδίκημα της Πλαστογραφίας (216 ΠΚ)

5.1 Σύντομη ανάλυση της διάταξης

Η διάταξη του αδικήματος της πλαστογραφίας υπό την ισχύουσα σήμερα μορφή της έχει ως εξής:

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

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

3. Αν ο υπαίτιος αυτών των πράξεων (παράγραφοι 1-2) σκόπευε να προσπορίσει στον εαυτό του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, και το συνολικό όφελος ή η συνολική ζημία υπερβαίνει τις 120.000 ευρώ τιμωρείται με κάθειρξη έως δέκα έτη και χρηματική ποινή.

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

5.1.1. Αντικειμενική υπόσταση

Από τη διάταξη αυτή της παραγράφου 1 του άρθρου 216 ΠΚ, που αποβλέπει στην προστασία της ασφάλειας και ακεραιότητας των εγγράφων συναλλαγών[126], προκύπτει ότι για τη στοιχειοθέτηση του βασικού εγκλήματος της πλαστογραφίας απαιτείται αντικειμενικώς, είτε η εξαρχής κατάρτιση από το δράστη εγγράφου, που να εμφανίζεται ότι καταρτίστηκε δήθεν από άλλον[127], είτε η νόθευση γνησίου εγγράφου, δηλαδή η μεταγενέστερη της κατάρτισης του αλλοίωση της εννοίας του περιεχομένου

---

[126] Βλ. *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 2, όπου αναφέρει ότι η διάταξη αποβλέπει στην προστασία της δημόσιας πίστης περί τα υπομνήματα και την ασφάλεια των εγγράφων και όχι στην προστασία της περιουσίας ή άλλων εννόμων αγαθών· ΟλΑΠ 3/2008 - ΝΟΜΟΣ, ΟλΑΠ (ΠΟΙΝ) 179/1990 ΝοΒ 1990, 328, ΑΠ 160/2020 ΝΟΜΟΣ, ΑΠ (ΠΟΙΝ) 332/2020 –ΝΟΜΟΣ, ΑΠ (ΠΟΝ) 397/2020–ΝΟΜΟΣ, ΑΠ (ΠΟΙΝ) 163/2019–ΝΟΜΟΣ· ΑΠ (ΠΟΙΝ) 625/2019 –ΝΟΜΟΣ· ΑΠ 902/2017 ΝΟΜΟΣ, ΑΠ 932/2009 ΙΣΟΚΡΑΤΗΣ.

[127] Ως κατάρτιση πλαστού εγγράφου νοείται η εξ' υπαρχής δημιουργία κάποιου εγγράφου, που δεν υπήρχε και το οποίο φέρεται ότι προέρχεται από ορισμένο φυσικό ή νομικό πρόσωπο, ενώ στην πραγματικότητα δεν προέρχεται από αυτό. Απαιτείται δηλαδή να υπάρχει διάσταση μεταξύ του πραγματικού και του φερόμενου εκδότη, βλ. *Μυλωνόπουλου*, Ποινικό Δίκαιο, Ειδικό Μέρος, Τα εγκλήματα σχετικά με τα υπομνήματα (άρθρα 216 - 223 ΠΚ), σελ. 41 · Να δημιουργείται δηλαδή παραπλάνηση περί της ταυτότητας του εκδότη · ΑΠ 317/2015 ΝΟΜΟΣ· ΑΠ (ΠΟΙΝ) 336/2013- ΝΟΜΟΣ· ΑΠ (ΠΟΙΝ) 55/2011- ΝΟΜΟΣ · ΑΠ (ΠΟΙΝ) 209/2011- ΝΟΜΟΣ · ΑΠ (ΠΟΙΝ) 1486/2011- ΝΟΜΟΣ · ΑΠ 2463/2008 –ΝΟΜΟΣ.

του, η οποία μπορεί να γίνει με την προσθήκη ή εξάλειψη ή τροποποίηση λέξεων, αριθμών ή σημείων, ώστε να παρέχεται η εντύπωση ότι η δήλωση του εκδότη είχε εξαρχής το περιεχόμενο που της προσδόθηκε μετά την αλλοίωση[128]. Η κατάρτιση και η νόθευση αποτελούν δύο διαφορετικές μορφές του εγκλήματος της πλαστογραφίας[129]. Υλικό δε αντικείμενο τους είναι το έγγραφο[130], όπως αυτό προσδιορίζεται στη διάταξη του άρθρου 13γ ΠΚ[131].

Πρόκειται για ένα σωρευτικά μικτό έγκλημα, αφού οι περισσότεροι τρόποι πραγματώσεως του, που αναφέρονται στο νόμο, δεν μπορούν να εναλλαχθούν μεταξύ τους πάνω στην ίδια μονάδα του εννόμου αγαθού[132]. Αξίζει δε να επισημανθεί ότι δεν στοιχειοθετείται το αδίκημα της πλαστογραφίας, εάν αυτός που καταρτίζει έγγραφο ή νοθεύει το περιεχόμενο του, ενεργεί κατ' εντολή ή με τη συναίνεση του εκδότη[133].

Από το συνδυασμό όμως της παραγράφου 1 και της παραγράφου 2 της ανωτέρω διάταξης, προκύπτει ότι καθιερώνονται δύο αυτοτελή εγκλήματα, δηλαδή αυτό της πλαστογραφίας και το άλλο της χρήσεως πλαστού ή νοθευμένου εγγράφου[134]. Το έγκλημα δε της χρήσης πλαστού εγγράφου στοιχειοθετείται αντικειμενικώς, όταν ο δράστης καταστήσει προσιτό το πλαστό ή νοθευμένο έγγραφο στον μέλλοντα να παραπλανηθεί από το περιεχόμενο του τρίτο και δώσει σ' αυτόν τη δυνατότητα να λάβει γνώση του περιεχομένου του, χωρίς να απαιτείται και να λάβει πράγματι γνώση, πολύ περισσότερο χωρίς να απαιτείται να παραπλανηθεί[135]. Το δε έγγραφο καθίσταται

---

[128]ΑΠ (ΠΟΙΝ) 1711/2010- ΝΟΜΟΣ· ΑΠ 217/2003 ΠοινΧρ ΝΓ` σ. 929· ΑΠ 1224/2001 ΠοινΧρ ΝΒ` σ. 426· *Μυλωνόπουλου*, Ποινικό Δίκαιο, Ειδικό Μέρος, Τα εγκλήματα σχετικά με τα υπομνήματα (άρθρα 216 - 223 ΠΚ), σελ. 56 · *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 45-46, όπου αναφέρεται ότι η έκταση της νόθευσης είναι αδιάφορη. Αρκεί να θίγεται η «αποδεικτική σημαντικότητα» · ΑΠ 752/2018, ΑΠ 902/2017 ΝΟΜΟΣ.

[129] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 48.

[130] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 2.

[131]ΟλΑΠ 3/2008, ΝΟΜΟΣ · ΑΠ (ΠΟΙΝ) 1503/2016 ΝΟΜΟΣ, όπου αναφέρεται «ως έγγραφο, που αποτελεί το υλικό αντικείμενο της πλαστογραφίας, νοείται, κατά το άρθρ. 13 εδ. γ' του ΠΚ, κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός, που έχει έννομη σημασία. Το έγγραφο πρέπει να είναι αντικειμενικά πρόσφορο να παράγει με την χρήση του έννομες συνέπειες · ΑΠ 317/2015 ΝΟΜΟΣ.

[132] *Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο216, sakkoulas online,αρ. 87 ·

[133] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 40-41 ·*Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρ. 216, sakkoulas online,αρ. 90.

[134] ΟλΑΠ 1284/1992, ΠοινΧρ 1992, 923.

[135]*Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 62· *Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο216, sakkoulas online,αρ. 108 · ΑΠ 671/2017 ΝΟΜΟΣ ·ΑΠ (ΠΟΙΝ) 1413/2013 ·ΑΠ (ΠΟΙΝ) 1711/2010- ΝΟΜΟΣ · ΑΠ (ΠΟΙΝ) 184/2002 ΠοινΛογ 2002, 155.

«προσιτό», όταν ο δράστης το μεταφέρει στην σφαίρα κυριαρχίας του τρίτου, χωρίς δηλαδή να αρκεί η απλή κατοχή του από τον δράστη[136].

Αξίζει όμως στο σημείο αυτό να διευκρινιστεί ότι ο Νέος Ποινικός Κώδικας (Ν. 4619/2019) ανάγει πλέον σε αυτοτελές έγκλημα τη χρήση του πλαστού εγγράφου, όχι μόνο στην περίπτωση που αυτή γίνεται από τρίτο πρόσωπο -υπό τον όρο βέβαια ότι ο τρίτος διατελεί εν γνώσει της πλαστότητας του εγγράφου-[137], αλλά και στην περίπτωση που αυτή γίνεται από τον αυτουργό της πλαστογραφίας[138]. Συνεπώς, η χρήση του πλαστού εγγράφου όταν τελείται από τον αυτουργό της πλαστογραφίας, δεν αποτελεί πλέον «επιβαρυντική περίπτωση»[139], αλλά αυτοτελή πράξη, που συρρέει φαινομενικά όταν ακολουθεί την πλαστοποιητική ενέργεια και απορροφάται από αυτήν[140].

5.1.2. Υποκειμενική υπόσταση

Για τη στοιχειοθέτηση του εγκλήματος της πλαστογραφίας υποκειμενικώς απαιτείται δόλος του δράστη, ο οποίος περιλαμβάνει τη γνώση και τη θέληση των πραγματικών περιστατικών, που απαρτίζουν την πράξη της πλαστογραφίας και επιπροσθέτως σκοπός του υπαιτίου να παραπλανήσει με τη χρήση του πλαστού ή νοθευμένου εγγράφου άλλον, για γεγονός που μπορεί να έχει έννομες συνέπειες, δηλαδή που είναι σημαντικό για την παραγωγή, διατήρηση, μεταβολή ή απόσβεση δικαιώματος ή έννομης σχέσης ή κατάστασης, δημόσιας ή ιδιωτικής φύσης[141].

---

[136] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 62·

[137] ΑΠ 217/2003 ΠοινΧρ ΝΓ` σελ. 929.

[138] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 1.

[139] Βλ. αντίθετα υπό το προϊσχύσαν δίκαιο, όπου, δυνάμει του τότε τελευταίου εδαφίου της παραγράφου 1, θεωρούνταν ως επιβαρυντική περίπτωση της πλαστογραφίας, υπό την έννοια ότι λαμβανόταν υπόψη κατά την επιμέτρηση της ποινής και επαυξανόταν το ελάχιστο όριο αυτής, μη υποκειμένου σε αυτοτελή κύρωση. Δεν προβλεπόταν δηλαδή ρητά επίταση της ποινής αλλά ασκούσε επιρροή μόνο κατά την επιμέτρηση της ποινής, βλ. *Μαργαρίτη Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 67. Η δε αυτοτέλεια αυτή της χρήσης από τον πλαστογράφο ως εγκλήματος έπαυε μόνον εφόσον η χρήση τιμωρούνταν ως επιβαρυντική περίπτωση, δηλαδή μόνον όταν τιμωρούνταν και η πλαστογραφία. Αντίθετα όταν η τελευταία, για οποιοδήποτε λόγο έμενε ατιμώρητη, τότε η χρήση και στην περίπτωση που έγινε από τον πλαστογράφο ανακτά την αυτοτέλεια της και τιμωρούνταν ως αυτοτελές έγκλημα, βλ. συναφώς ΟλΑΠ 1284/1992, ΠοινΧρ 1992, 923.

[140] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 1 · βλ. και Αιτιολογική έκθεση νέου Ποινικού Κώδικα.

[141] ΟλΑΠ 3/2008, ΤΝΠ ΝΟΜΟΣ ·ΑΠ (ΠΟΙΝ) 1711/2010- ΝΟΜΟΣ· *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ.54.

Το αδίκημα της πλαστογραφίας είναι υπερχειλούς υποκειμενικής υπόστασης[142]. Απαιτείται συνεπώς επιπλέον σκοπός του δράστη να παραπλανήσει άλλον για γεγονός που μπορεί να έχει έννομες συνέπειες, ενώ είναι αδιάφορο εάν επιτεύχθηκε τελικώς η παραπλάνηση, ή εάν σκοπείται η παραπλάνηση κάποιου συγκεκριμένου προσώπου ή όποιου ευκαιριακά εμφανιστεί[143]. Επιπροσθέτως αξίζει να επισημανθεί ότι ομοίως αδιάφορα είναι και τα κίνητρα κι απώτερα ελατήρια του δράστη[144].

5.1.3. Αιτιώδης σύνδεσμος- προσφορότητα προς απόδειξη

Η πλαστή δήλωση του φερόμενου εκδότη ή η νοθευμένη δήλωση του εκδότη πρέπει να είναι πρόσφορη να αποδείξει γεγονός που μπορεί να έχει έννομη συνέπεια ή να αποτελεί σημείο προοριζόμενο για τέτοια απόδειξη[145]. Η δήλωση αυτή (πλαστή/ νοθευμένη) θα πρέπει συνεπώς να μπορεί αντικειμενικά να παραπλανήσει άλλον για γεγονός, που μπορεί να έχει έννομες συνέπειες, δηλαδή να είναι πρόσφορη να παράγει έννομες συνέπειες, το δε γεγονός να προκύπτει από το περιεχόμενο του εγγράφου στο οποίο ενσωματώνεται ή σε συνδυασμό με άλλα στοιχεία, ενώ είναι παντελώς αδιάφορο, εάν ο σκοπός της παραπλανήσεως θα επιτυγχανόταν και χωρίς το έγγραφο αυτό[146].

5.1.4. Η κακουργηματική πλαστογραφία και χρήση πλαστού (παρ. 3 και 4 άρθρ. 216 ΠΚ)

Από την απλή ανάγνωση των παραγράφων 3 και 4 άρθρου 216 ΠΚ προκύπτει ότι υπάρχουν δυο μορφές κακουργηματικής πλαστογραφίας και χρήσης πλαστού: η επί σκοπώ προσπορισμού οφέλους ή βλάβης με όφελος ή ζημία άνω των 120.000 ευρώ και η πλαστογραφία ή η χρήση πλαστού, που στρέφεται κατά του Δημοσίου, ΝΠΔΔ ή ΟΤΑ με το ίδιο ποσό οφέλους ή ζημία[147]. Αν η χρήση γίνεται από τρίτο και όχι από τον

---

[142] *Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο216, sakkoulas online, αρ. 123 · ΑΠ (ΠΟΙΝ) 317/2020 –ΝΟΜΟΣ · ΑΠ (ΠΟΙΝ)397/2020 –ΝΟΜΟΣ.

[143] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 54 ·ΑΠ 317/2015 ΤΝΠ ΝΟΜΟΣ· ΑΠ 867/2006 ΠοινΧρ ΝΖ, 244.

[144] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 55.

[145] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 56.

[146] ΑΠ 317/2015 ΝΟΜΟΣ: *«Το πλαστό έγγραφο να μπορεί αντικειμενικά με τη χρήση του να παραπλανήσει άλλον για γεγονός, που μπορεί να έχει έννομες συνέπειες, δηλαδή να είναι πρόσφορο να παράγει έννομες συνέπειες, το δε γεγονός να προκύπτει από το περιεχόμενο του εγγράφου ή σε συνδυασμό με άλλα στοιχεία και είναι αδιάφορο, εάν ο σκοπός της παραπλανήσεως θα επιτυγχανόταν και χωρίς το έγγραφο ή, εάν προοριζόταν αυτό για το παρόν ή το μέλλον ή για συγκεκριμένη περίπτωση»* · ΑΠ (ΠΟΙΝ) 423/2020–ΝΟΜΟΣ· ΑΠ (ΠΟΙΝ) 163/2019–ΝΟΜΟΣ· ΑΠ (ΠΟΙΝ))1503/2016 ΝΟΜΟΣ.

[147] Συνεπώς δεν αποτελεί πλέον κακούργημα η πλαστογραφία κατ' επάγγελμα ή κατ' συνήθεια, όπως προβλεπόταν στον προϊσχύοντα ΠΚ.

πλαστογράφο για να είναι κακουργηματική η χρήση απαιτείται να έχει και ο τρίτος το σκοπό οφέλους ή βλάβης[148]. Με δεδομένο δε ότι πρόκειται για έγκλημα σκοπού, είναι αδιάφορο εάν ο σκοπός αυτός επιτεύχθηκε ή όχι[149].

Ειδικά δε ως προς την πλαστογραφία ή τη χρήση πλαστού με σκοπό οφέλους ή βλάβης τρίτου, αξίας άνω των 120.000 ευρώ, αξίζει να αναφερθεί ότι δεν είναι απαραίτητο η περιουσιακή μετακίνηση να είναι άμεσα συνδεδεμένη με την πλαστογραφία ή τη χρήση πλαστού, με την έννοια να πρέπει να προέρχεται απευθείας από αυτή, δια μόνης της υλικής πράξης της κατάρτισης ή της νόθευσης ή της χρήσης του πλαστού, αλλά αρκεί ότι το περιουσιακό όφελος ή η περιουσιακή βλάβη έχει ενταχθεί στο εν γένει δια της πλαστογραφίας παραπλανητικό σχέδιο του δράστη και διαμορφώνονται με την πλαστογραφία ή τη χρήση πλαστού οι προϋποθέσεις για να υπάρχει στη συνέχεια η δυνατότητα (: ο κίνδυνος), έστω και με την παρεμβολή άλλων ενεργειών του δράστη, να επέλθει το επιδιωκόμενο περιουσιακό όφελος ή η σκοπούμενη περιουσιακή βλάβη[150]. Οι τυχόν επιπρόσθετες και επόμενες ενέργειες του δράστη δεν αναιρούν το πρόσφορο της πλαστογραφίας ή της νόθευσης να επιφέρει το περιουσιακό όφελος ή την περιουσιακή ζημία την οποία επιδιώκει ο δράστης, αφού κατά την έννοια της ερμηνευόμενης διάταξης για τη θεμελίωση του αξιοποίνου ο νόμος απέβλεψε όχι στην αμεσότητα της ενεργείας του δράστη σε σχέση με το αποτέλεσμα της περιουσιακής βλάβης ή του οφέλους, αλλά στην αμεσότητα του κινδύνου τον οποίο ενέχει αυτή καθ` εαυτή η υλική πράξη της πλαστογραφίας έστω και αν πρέπει να ακολουθήσει ενδεχομένως και περαιτέρω ενέργεια αυτού, η οποία ουσιαστικώς ενεργοποιεί τον κίνδυνο της επέλευσης του οφέλους ή της βλάβης[151].

5.2. Η έννοια του εγγράφου – Η προβληματική για τα ηλεκτρονικά έγγραφα

Όπως ήδη αναφέρθηκε, υλικό αντικείμενο της πλαστογραφίας είναι το έγγραφο. Στο άρθρο 13γ ΠΚ, όπως αυτό ισχύει σήμερα, στοιχειοθετείται η έννοια του εγγράφου, η οποία αναλύεται ως εξής: *«γ) Έγγραφο είναι κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό*

[148]*Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 76.
[149] ΟλΑΠ 3/2008 ΝΟΜΟΣ · ΑΠ (ΠΟΙΝ) 1211/2017 ΝΟΜΟΣ· *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 74.
[150]ΟλΑΠ 3/2008 ΝΟΜΟΣ, ΑΠ (ΠΟΙΝ) 761/2019 ΝΟΜΟΣ, ΑΠ (ΠΟΙΝ)122/2016, ΝΟΜΟΣ, *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 72.
[151] ΑΠ (ΠΟΙΝ) 761/2019 ΝΟΜΟΣ, ΑΠ (ΠΟΙΝ)122/2016 ΝΟΜΟΣ.

ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή αναπαραγωγή στοιχείων που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφόσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία». Αξίζει δε να επισημανθεί ότι το τελευταίο εδάφιο της περίπτωσης γ του άρθρου 13 προστέθηκε με το άρθρο 2 του ν. 1805/1988, προκειμένου να διευρυνθεί η έννοια του εγγράφου στο ποινικό δίκαιο, κυρίως προς αντιμετώπιση των αναγκών που προέκυπταν από τη χρήση των ηλεκτρονικών μέσων συναλλαγής και συνακόλουθα την ποινική τους μεταχείριση, καθόσον η μέχρι τότε έννοια του εγγράφου δεν αρκούσε για την στοιχειοθέτηση του αδικήματος της πλαστογραφίας[152]. Στην έννοια συνεπώς του εγγράφου περιλαμβάνονται πλέον και τα ψηφιακά δεδομένα, οι μαγνητικές ταινίες πιστωτικών καρτών, βάσεις δεδομένων και αρχεία, εφόσον πρόκειται για ηλεκτρονικά αρχεία[153]. Η σημασία λοιπόν της διεύρυνσης της έννοιας του εγγράφου είναι προφανής, καθ' όσον δηλώνεται ότι οι υλικοί φορείς δεδομένων είναι έγγραφα κατά την έννοια του νόμου, ακόμα και όταν τα δεδομένα που περιέχουν είναι δημιούργημα μιας μηχανής, εφόσον όμως έχει προηγηθεί ο προγραμματισμός της από κάποιο πρόσωπο[154]. Έτσι με τη διευρυμένη αυτή έννοια του εγγράφου, το αδίκημα

---

[152] *Πανταζόπουλος Σ.,* Αναψηλάφηση της απόφασης λόγω ψευδών αποδεικτικών μέσων, σ. 78 επ, *Γιαννόπουλος Θ.*, Η έννοια του εγγράφου μετά τη «συμπλήρωση» του άρθρου 13 γ΄ ΠΚ και η σημασία του Αστικού και Αστικού Δικονομικού Δικαίου, ΕλλΔνη 1990, σ. 1399 επ.

[153] *Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., σ. 340-341· Για το ότι στην έννοια του εγγράφου περιλαμβάνονται και τα δεδομένα υπολογιστή, βλ. ΑΠ (ΠΟΝ) 1237/2010 –ΝΟΜΟΣ, όπου αναφέρεται: *«το Δικαστήριο πείθεται ότι ο κατηγορούμενος, όπως και οι εντοπισθέντες πριν από αυτόν να έχουν λάβει, με βάση αναληθή στοιχεία του Η/Υ της Σχολής, πτυχίο χωρίς να έχουν ολοκληρώσει τις σπουδές τους, προσέγγισε υπάλληλο της γραμματείας της, ο οποίος δεν κατέστη δυνατόν να εντοπισθεί και στον οποίο, ως εκ της υπηρεσίας του, ήταν προσιτές οι καταχωρημένες στη βάση δεδομένων του ηλεκτρονικό υπολογιστή της γραμματείας αναλυτικές καταστάσεις βαθμολογίας των φοιτητών της Σχολής και τον έπεισε να νοθεύσει την αφορώσα τον ίδιο αναλυτική κατάσταση βαθμολογίας, κατά τρόπο ώστε να εμφανίζεται ότι έλαβε προακτέο βαθμό και στα αναφερόμενα στο διατακτικό εννέα συνολικά μαθήματα, στα οποία, όπως εκεί ειδικότερα διευκρινίζεται, είτε δεν είχε καν συμμετάσχει, είτε δεν είχε λάβει προακτέο βαθμό, με συνέπεια η Ιατρική Σχολή να παραπεισθεί εκ των νοθευμένων δεδομένων του Η/Υ της Γραμματείας της και να θεωρήσει τον κατηγορούμενο επιτυχώς ολοκληρώσαντα ης σπουδές του και να του χορηγήσει πτυχίο…. Εξ άλλου, είναι επίσης πρόδηλο ότι το αποδιδόμενο στον κατηγορούμενο αδίκημα δεν μπορεί να συγχέεται με το εκ της διατάξεως του άρθρου 217 του Π.Κ. προβλεπόμενο, ήτοι αυτό της πλαστογραφίας πιστοποιητικού, αφού δεν πρόκειται εδώ τοιαύτη περίπτωση αλλά αληθής νόθευση εγγράφου, ως τοιούτου νοουμένου και των δεδομένων του Η/Υ της άνω Σχολής, το οποίο, ασχέτως του ότι προορίζεται για την έκδοση πιστοποιητικών, δεν είναι το ίδιο πιστοποιητικό κατά την έννοια της διατάξεως του άρθρου 217 Π.Κ., αλλά κοινό έγγραφο, υποκείμενο σε νόθευση, πράξη για την οποία προσήκει η υπαγωγή της στη διάταξη του άρθρου 216 του Π.Κ».*

[154] *Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., σ. 341.

της πλαστογραφίας, βρίσκει εφαρμογή στα ηλεκτρονικά έγγραφα και στο λογισμικό[155]. Ως εκ τούτου η παράνομη αντιγραφή δεδομένων ή λογισμικού συνιστά πλαστογραφία, αν ο δράστης ενεργεί με σκοπό παραπλάνησης άλλου για γεγονός που μπορεί να έχει έννομη σημασία, ενώ η χρήση του αντιγραμμένου λογισμικού συνιστά πλαστογραφία μετά χρήσεως[156]. Επιπροσθέτως, η αλλοίωση των δεδομένων ενδέχεται να συνιστά νόθευση εγγράφου[157].

Καθίσταται όμως σαφές από τον νομοθέτη ότι προστατεύονται μόνο τα δεδομένα ή τα προγράμματα που έχουν αποδεικτική σημασία, όπως π.χ. εγγραφές στο μαγνητικό τμήμα καρτών[158]. Ενώ όμως από την διατύπωση του ανωτέρω άρθρου φαίνεται να προκύπτει ότι για την κατάφαση της πλήρωσης της έννοιας του εγγράφου είναι απαραίτητη μόνο η αποδεικτική λειτουργία του εγγράφου, κρίνεται σκόπιμο να αναφερθεί ότι υιοθετείται μια συσταλτική ερμηνεία της έννοιας αυτής, όπου απαιτείται να πληρούνται και άλλες δύο λειτουργίες του εγγράφου, δηλαδή η σταθερή ενσωμάτωση του σε υλικό φορέα (διαιωνιστική λειτουργία) καθώς και να προκύπτει ο εκδότης του εγγράφου (εγγυητική λειτουργία)[159] . Ως εκ τούτου δεν συνιστά έγγραφο,

---

[155] *Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., σ. 340-341, ΣυμβΠλημΘε 3204/1993, Υπεράσπιση 1994, 1132, με παρατηρήσεις Γ. Νούσκαλη, σ.1139 επ., η οποία δέχτηκε ότι η παράνομη αντιγραφή λογισμικού συνιστά πλαστογραφία μετά χρήσεως.

[156] *Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., σ. 341 επ.

[157] *Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., σ. 341.

[158] *Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., σ. 341.

[159] *Μυλωνόπουλος Χ.,* Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, σ. 42 σε συνδυασμό με σ. 46 · Χαρακτηριστική είναι η ΠλημμΧίου 53/2007, ΠοινΧρ2008, 270, όπου αναφέρει: *«Περαιτέρω για την στοιχειοθέτηση της κατ` άρ. 13 περ. γ` του ΠΚ εννοίας του εγγράφου πρέπει να συντρέχουν οπωσδήποτε και τα εξής τρία απαραίτητα στοιχεία: α) η διαιωνιστική λειτουργία του εγγράφου, η οποία διασφαλίζεται με την σταθερή ενσωμάτωση του ανθρωπίνου διανοήματος σε κάποιον υλικό φορέα έτσι ώστε το ενσωματούμενο διανόημα να δύναται ανά πάσα στιγμή να αναπαραχθεί προκείμενου να χρησιμεύσει προς απόδειξη, β) η εγγυητική λειτουργία του εγγράφου, η οποία, προϋποθέτει την ύπαρξη εκδότη επαρκώς εξατομικευμένου, δηλαδή απαιτείται όπως ο εκδότης που αναγνωρίζει το ενσωματούμενο στον υλικό φορέα διανόημα ως δικό του και δεσμεύεται από αυτό είτε να κατονομάζεται ευθέως ή τουλάχιστον να προκύπτει και να καθίσταται αναγνωρίσιμος μέσω του εγγράφου, άλλως το διανόημα δεν μπορεί να αναγνωρισθεί ως έγγραφο ούτε να λειτουργήσει ως θεμέλιο παραγωγής εννόμων συνεπειών και δημόσιας πίστης. Γίνεται παγίως δεκτόν ότι δεν απαιτείται όπως ο εκδότης υπογράφει ιδιοχείρως το έγγραφο, αλλά έγγραφο υφίσταται ακόμη και όταν ο εκδότης έχει θέσει την υπογραφή του με μηχανικό μέσο, σε κάθε περίπτωση δε αρκεί όπως το πρόσωπο του εκδότη προκύπτει από το έγγραφο ή τουλάχιστον καθίσταται εμφανές από το περιεχόμενο του εγγράφου, όπως π.χ. όταν συνάγεται από το είδος ή από τα στοιχεία του εγγράφου (ΑΠ 238/2000 ΠοινΧρ Ν΄/694), από σφραγίδα, αναγνωρίσιμες συντμήσεις, λογότυπο κ.λπ., χωρίς να απαιτείται οπωσδήποτε "εγχάρτωση" του εκδότη. Αντιθέτως δεν υπάρχει έγγραφο όταν το πρόσωπο του εκδότη καθίσταται γνωστό αποκλειστικά και μόνον με την προσφυγή σε αλλότριο, τρίτο, υλικό φορέα κείμενο εκτός και πέραν του υλικού φορέα του διανοήματος, όταν δηλαδή για την διαπίστωση ή την συναγωγή του προσώπου του εκδότη απαιτείται προσφυγή σε πρόσθετη απόδειξη, από την οποία και μόνον προκύπτει το πρώτον το πρόσωπο του, όταν δηλαδή για την συναγωγή του προσώπου του εκδότη ενός εγγράφου πρέπει κάποιος να αναφερθεί σε άλλο έγγραφο, όπως π.χ. σε μαρτυρική κατάθεση, γραφολογική πραγματογνωμοσύνη, προτάσεις διαδίκου κ.λπ. Στην περίπτωση αυτή γίνεται*

μια απλή εγγραφή στη μνήμη RAM η/υ, αλλά πρέπει τα δεδομένα να έχουν εγγραφτεί σε μία σταθερή μνήμη και να είναι σταθερά ενσωματωμένα στους υλικούς φορείς τους[160]. Συναφώς δεν συνιστούν έγγραφα, η stratch pad memory, η οθόνη του υπολογιστή, το ενσύρματο λογισμικό ή οι φορείς προγραμμάτων bootstrap διότι δεν προκύπτει ο εκδότης τους, αλλά και δεν έχουν αποδεικτική σημασία[161].

Μάλιστα υποστηρίζεται ότι στο έγκλημα της πλαστογραφίας προέχουσα είναι η εγγυητική λειτουργία του εγγράφου, που συνίσταται στο αναγνωρίσιμο του εκδότη του (να προσδιορίζεται δηλαδή το πρόσωπο που δεσμεύεται από το έγγραφο), διότι διαφορετικά δεν είναι νοητή η παραγωγή εννόμων συνεπειών από αυτό[162].

Ενόψει των παραπάνω προκύπτει ότι μόνο σε όποιο μέτρο το επιτρέπει η έννοια του ηλεκτρονικού εγγράφου (άρθρο 13γ ΠΚ) κατά τα ανωτέρω, μπορεί να στοιχειοθετηθεί τα αδίκημα της πλαστογραφίας, διότι δεν είναι πάντοτε εύκολο να αναγνωριστεί ο εκδότης ενός ψηφιακού εγγράφου, ενώ ενδέχεται να εκλείπει η αποδεικτική ή η διαιωνιστική λειτουργία των δεδομένων. Έτσι για παράδειγμα γίνεται δεκτό ότι η ιστοσελίδα, που συνιστά μορφή ψηφιακού κειμένου, θεωρείται έγγραφο, αν η αποτύπωση των δεδομένων στον υλικό φορέα έχει τον χαρακτήρα της σταθερής ενσωμάτωσης και ταυτόχρονα τα δεδομένα προσδιορίζουν τον συγκεκριμένο εκδότη από την ηλεκτρονική του διεύθυνση[163].

Ακριβώς όμως επειδή δεν συγκεντρώνουν όλα τα ηλεκτρονικά δεδομένα τα στοιχεία του «εγγράφου», αλλά εντούτοις ανακύπτει ανάγκη ποινικοποίησης της πλαστοποίησης τους, στο άρθρο 7 της Σύμβασης για το Κυβερνοέγκλημα προβλέφθηκε ρητά ότι κάθε συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά μέτρα για να ποινικοποιηθεί η από πρόθεση και άνευ δικαιώματος εισαγωγή, αλλοίωση, διαγραφή ή

κατηγορηματικά δεκτόν ότι δεν υφίσταται κατά νόμον έγγραφο και γ) η αποδεικτική λειτουργία του εγγράφου, η οποία πληρούται όταν το ενσωματωμένο στον υλικό φορέα διανόημα είναι προορισμένο ή πρόσφορο, κατά τις διακρίσεις του άρ. 13 περ. γ` του ΠΚ, να αποδείξει γεγονός που μπορεί να έχει έννομες συνέπειες, έχει δε το έγγραφο αποδεικτικό προορισμό (Beweisbestimmung), όταν καταρτίσθηκε εξ υπαρχής συνειδητά από τον εκδότη με σκοπό να αποδεικνύει ένα νομικά σημαντικά γεγονός, ενώ έχει αποδεικτική προσφορότητα (Beweiseignung), όταν, ανεξαρτήτως της ενδόμυχης διάθεσης του εκδότη του κατά το χρόνο συντάξεως του εγγράφου, μπορεί αντικειμενικά να χρησιμεύσει προς απόδειξη ενός νομικά σημαντικού γεγονότος (Χ. Μυλωνόπουλος, Ποινικό Δίκαιο, Ειδικό Μέρος, Τα εγκλήματα σχετικά με τα υπομνήματα, 2005, σ. 3-4, 8 έως 17)» · Φράγκος Κ., Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο216, sakkoulas online, αρ. 26.

[160] *Μυλωνόπουλος Χ.,* Η ποινική προστασία του λογισμικού κατά το ελληνικό δίκαιο, ΠοινΧρ ΛΗ΄,σ. 10 επ.·*Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., σ. 341.

[161]*Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 18.

[162] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ. 6.

[163] *Πανταζόπουλος Σ,* Αναψηλάφηση της απόφασης λόγω ψευδών αποδεικτικών μέσων, σ. 78 επ. · *Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο216, sakkoulas online, αρ. 57-58.

καταστολή δεδομένων υπολογιστή που καταλήγουν σε παραγωγή μη αυθεντικών δεδομένων με σκοπό να λαμβάνονται υπόψη ή να χρησιμοποιούνται για νόμιμους σκοπούς σαν να ήταν αυθεντικά, ασχέτως του εάν αυτά τα δεδομένα είναι ή όχι άμεσα αναγνώσιμα ή αντιληπτά[164].

Παρά όμως την ρητή αυτή πρόβλεψη στο άρθρο 7 της Σύμβασης, ο Έλληνας νομοθέτης παρέλειψε να εισάγει με το ν. 4411/2016 ή με τον νέο Ποινικό Κώδικα αντίστοιχη ρύθμιση, που να δημιουργεί στην ουσία ένα παράλληλο αδίκημα με αυτό της πλαστογραφίας, το οποίο να μην στρέφεται κατά «εγγράφου» κατά τον ορισμό του 13ΠΚ (και άρα να μην απαιτείται -όπως επί της παραδοσιακής πλαστογραφίας- το «πλαστό» να πληροί τα στοιχεία του «εγγράφου»), αλλά να στρέφεται κατά της πλαστοποίησης ηλεκτρονικών δεδομένων εν γένει, κατά την έννοια του άρθρου 7 της Σύμβασης της Βουδαπέστης. Φαίνεται επομένως ότι ο Έλληνας νομοθέτης επέδειξε αβλεψία, αρκούμενος απλώς στην από το έτος 1998 διεύρυνση της έννοιας του εγγράφου για να συμπεριλάβει και τα ηλεκτρονικά έγγραφα, χωρίς όμως διασφαλίσει, ούτε τότε, ούτε το έτος 2016, ούτε και το έτος 2019 την ποινικοποίηση της πλαστοποίησης εκείνων των ηλεκτρονικών δεδομένων, τα οποία δεν πληρούν σωρευτικά και τις τρεις λειτουργίες - στοιχεία της έννοιας του «εγγράφου», που αποτελεί το αντικείμενο της παραδοσιακής πλαστογραφίας.

Επιπλέον, αστοχία του Έλληνα νομοθέτη ήταν και η αβλεψία του να ποινικοποιήσει αυτοτελώς τη συμπεριφορά κάποιου προσώπου, που καταρτίζει πλαστά ηλεκτρονικά έγγραφα για να τα χρησιμοποιήσει ως μέσο τέλεσης απάτης με υπολογιστή, ήτοι προκειμένου να επηρεάσει άμεσα τη λειτουργία ενός η/υ με σκοπό περιουσιακή διάθεση, χωρίς όμως να έχει πρόθεση να παραπλανήσει κάποιο πρόσωπο (λ.χ. του προσώπου που καταρτίζει πλαστές μαγνητικές κάρτες ανάληψης από ΑΤΜ). Δεδομένου ότι η παραδοσιακή πλαστογραφία απαιτεί σκοπό παραπλάνησης «άλλου» σχετικά με γεγονός που μπορεί να έχει έννομες συνέπειες, ως «άλλος» δε, θεωρείται οποιοδήποτε φυσικό πρόσωπο, γίνεται αντιληπτό ότι δεν μπορεί να καταφάσκεται ο σκοπός ή προσφορότητα παραπλάνησης κάποιου προσώπου, στις περιπτώσεις που κάποιος καταρτίζει πλαστά ηλεκτρονικά έγγραφα για να τα χρησιμοποιήσει προκειμένου να επηρεάσει άμεσα τη λειτουργία ενός μηχανήματος ή γενικότερα κάποιου η/υ. Ως εκ τούτου, δεδομένου ότι το γράμμα της διάταξης 216 ΠΚ δεν μπορεί να καλύψει περιπτώσεις όπου τα πλαστά έγγραφα προορίζονται να αναγνωστούν από

[164] *Δαλακούρας Θ.,* Ηλεκτρονικό Έγκλημα, σ. 15.

πρόγραμμα η/υ, καθώς ο όρος «παραπλανώ» συνδέεται πάντοτε με κάποιο πρόσωπο, θα έπρεπε ίσως να λάβει χώρα μία ανάλογη πρόβλεψη σαν αυτή που έγινε στην περίπτωση της κοινής απάτης και της απάτης με υπολογιστή κατά τα ανωτέρω.

Με την ανωτέρω λογική επομένως, οδηγούμαστε στο παράδοξο συμπέρασμα ότι: Α) Δράστης που εισάγει παρανόμως κτηθέντα ψηφιακά δεδομένα σε μαγνητική ταινία πλαστικής κάρτας (τα οποία δεδομένα αντιστοιχούν σε «χρεωστική κάρτα»), δημιουργώντας «πλαστές κάρτες αναλήψεως από ΑΤΜ», δε τελεί το ποινικό αδίκημα του 216§1 ΠΚ, αφού η πράξη του αυτή δεν είναι πρόσφορη να παραπλανήσει άλλον, αλλά αποτελεί απλώς προπαρασκευαστική πράξη του 386^{Α} ΠΚ (που δεν εμπίπτει καν στο 386^{Α}§2, ώστε να είναι και τιμωρητέα). Αν ο ίδιος δράστης όντως χρησιμοποιήσει την πλαστή κάρτα ανάληψης, και αναλάβει χρήματα από ΑΤΜ και δη με χρέωση λογαριασμού του πραγματικού δικαιούχου των δεδομένων που αντέγραψε στην πλαστική κάρτα, τότε τελεί και το αδίκημα του 386^{Α}. Β) Αντιθέτως, δράστης που εισάγει παρανόμως κτηθέντα ψηφιακά δεδομένα σε μαγνητική ταινία πλαστικής κάρτας (τα οποία δεδομένα αντιστοιχούν σε «πιστωτική κάρτα»), δημιουργώντας «πλαστές πιστωτικές κάρτες», τελεί το ποινικό αδίκημα του 216§1 ΠΚ, αφού η πράξη του αυτή είναι πρόσφορη να παραπλανήσει άλλον (τον επιχειρηματία ο οποίος πρόκειται να εισάγει την πλαστή πιστωτική στο POS του). Αν ο ίδιος δράστης όντως χρησιμοποιήσει την πλαστή πιστωτική κάρτα για να αγοράσει αγαθά από κατάστημα, παραπλανώντας τον επιχειρηματία ότι είναι νόμιμος κάτοχος της κάρτας, τότε, πέρα από το αδίκημα του 216§1, τελεί και τα αδικήματα του 216§2 και του 386 ΠΚ[165].

Συμπερασματικά, σημειώνουμε ότι ενώ με τον Ν. 4411/2016 είχε γίνει μία σημαντική προσπάθεια από τον νομοθέτη να αντιμετωπιστούν πολλές από τις εκφάνσεις της ηλεκτρονικής εγκληματικότητας (εισαγωγή στον Ποινικό Κώδικα των άρθρων 292^{Β} και 292^{Γ} περί παρεμβολής σε σύστημα, αναδιαμόρφωση του άρθρου 370^{Γ}, προσθήκη των 370^{Δ} και 370^{Ε} και του 381^{Α} περί της φθοράς ηλεκτρονικών δεδομένων [166]), η παράλειψη ποινικοποίησης των πράξεων πλαστοποίησης ηλεκτρονικών δεδομένων άφησε ένα σημαντικό κενό, με αποτέλεσμα οι συγκεκριμένες πράξεις να τιμωρούνται μόνον από το άρθρο 216 ΠΚ, ήτοι όποτε θεωρείται ότι τα δεδομένα που πλαστοποιήθηκαν μπορούσαν να θεωρηθούν «έγγραφα» και μόνο όποτε τα έγγραφα αυτά ήταν πρόσφορα να παραπλανήσουν «άλλον».

---

[165] Βλ. ΕφΘεσσ 2322/2010 - ΝΟΜΟΣ

[166] *Καϊάφα-Γκμπάντι Μ./ Παπακυριάκου Θ.,* Στοιχεία Ενωσιακού Ποινικού Δικαίου, 2^{η} έκδ., σ. 163 επ.

Κεφάλαιο 6ο: Η Πλαστογραφία ως μέσο τέλεσης της απάτης και της απάτης με η/υ στις σύγχρονες μορφές εγκληματικότητας

6.1. Γενική θεώρηση

Τα πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου (email) καθώς και οι πλαστές ιστοσελίδες (ως ψηφιακά κείμενα), χρησιμοποιούνται όλο και συχνότερα ως μέσο παραπλάνησης των χρηστών του διαδικτύου από δράστες με σκοπό τέλεσης κάθε είδους απάτης (με τη γενική έννοια του όρου) στο διαδίκτυο. Αμφότερες δε οι κατηγορίες, δηλαδή τόσο οι ηλεκτρονικές επιστολές όσο και οι ιστοσελίδες μπορούν, σύμφωνα με τη θεωρία, να θεωρηθούν έγγραφα κατά την έννοια του άρθρου 13γ ΠΚ, ανάλογα με τον τρόπο λειτουργίας τους[167] και εφόσον πληρούν τις τρείς λειτουργίες του «εγγράφου» (αποδεικτική, εγγυητική, διαιωνιστική) κατά τα ανωτέρω[168].

Πιο συγκεκριμένα, γίνεται δεκτό ότι τόσο το ηλεκτρονικό μήνυμα που αποστέλλεται μέσω διαδικτύου (e-mail) όσο και οι ιστοσελίδες, που συνιστούν και αυτές μορφές ψηφιακού κειμένου, συνιστούν έγγραφα, εφόσον ενσωματώνουν πνευματικό διανόημα που μπορεί να αποδοθεί σε ορισμένο εκδότη και είναι προορισμένο ή πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία[169]. Μάλιστα έχει υποστηριχθεί ότι οι ηλεκτρονικές επιστολές είναι έγγραφα, κατά την ανωτέρω έννοια, εάν έχουν χαρακτηριστικά όπως πραγματικό όνομα, ψηφιακή διεύθυνση, ψηφιακή υπογραφή και στοιχεία για την διαδρομή που έχει κάνει, ώστε να μπορεί ο παραλήπτης να ελέγξει αν μία επιστολή είναι αυθεντική ή όχι[170, 171]. Ομοίως και οι ιστοσελίδες είναι έγγραφα από την στιγμή που είναι αποθηκευμένες στον υπολογιστή του παρόχου, ώστε να συνδέονται ηλεκτρονικά με αυτόν που κατέχει την ιστοσελίδα και κατά συνέπεια να υπάρχει σύνδεση με τον εκδότη της[172]. Στην αντίθετη περίπτωση, δηλαδή αν υπάρχει ψευδώνυμο και δεν μπορεί η ιστοσελίδα να συσχετίζεται με τον

---

[167] *Ζέκος Γ.,* Διαδίκτυο, Η/Υ και τηλεπικοινωνίες στο ελληνικό δίκαιο, 2017, σ. 84επ.

[168]βλ. και *Μυλωνόπουλο Χ.*, Ποινικό Δίκαιο, Ειδικό Μέρος, Τα εγκλήματα σχετικά με τα υπομνήματα (άρθρα 216 - 223 ΠΚ), σελ. 31 επ.

[169] *Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο216, sakkoulas online, αρ. 57-58. Για το ότι το ηλεκτρονικό μήνυμα που αποστέλλεται μέσω διαδικτύου (e-mail) μπορεί να αποτελέσει το υλικό αντικείμενο της πλαστογραφίας, αφού πληροί την έννοια του εγγράφου, βλ. και ΑΠ (ΠΟΙΝ) 471/2017- ΝΟΜΟΣ: *«Ειδικότερα, κατάρτισε εξ ολοκλήρου δύο (2) πλαστά έγγραφα ηλεκτρονικής αλληλογραφίας (e- mails)..»* · ΑΠ 546/2011 -ΝΟΜΟΣ · ΠλημμΑθ 594/2014 ΝοΒ 2014, 1683.

[170] *Ζέκος Γ.,* Διαδίκτυο, Η/Υ και τηλεπικοινωνίες στο ελληνικό δίκαιο, 2017, σ. 84 επ.

[171] Κατά τη γνώμη του γράφοντος, η δυνατότητα *«αντίληψης του παραλήπτη περί της αυθεντικότητας του e-mail»* πρέπει να κριθεί με βάση τις ελάχιστες γνώσεις περί ηλεκτρονικών υπολογιστών που έχει ο μέσος χρήστης, που περιορίζονται στην αντίληψη του φερόμενου «ονόματος αποστολέα» και της φερόμενης διεύθυνσης ηλεκτρονικού ταχυδρομείου προέλευσης και όχι στο αν υπάρχει ψηφιακή υπογραφή ή στη δυνατότητα ελέγχου της διαδρομής του ηλεκτρονικού μηνύματος

[172] *Ζέκος Γ.,* Διαδίκτυο, Η/Υ και τηλεπικοινωνίες στο ελληνικό δίκαιο, 2017, σ. 84 επ.

εκδότη της δεν θεωρείται έγγραφο[173]. Πάντως, διατυπώθηκαν πολλές επιφυλάξεις αναφορικά με το εάν η ιστοσελίδα ως ψηφιακό κείμενο πληροί ή όχι την εγγυητική λειτουργία του «εγγράφου», υπό την έννοια της δυνατότητας σύνδεσής της με τον «εκδότη της». Γίνεται δεκτό ότι η εγγυητική λειτουργία του εγγράφου μπορεί να καταφαθεί και στην περίπτωση αυτή, αφού ο «εκδότης» της ιστοσελίδας (που επί της ουσίας είναι ένα έγγραφο «html»), αφού την «φορτώσει» σε συγκεκριμένο ηλεκτρονικό υπολογιστή / διακομιστή (web-server) και λάβει (σταθερή) διεύθυνση IP (ώστε να μπορούν οι λοιποί η/υ του δικτύου να συνδεθούν με τη σελίδα), ζητά από τον πάροχο Domain Names να συνδέσει την IP του με την καταχωρημένο στο πρόσωπό του ηλεκτρονική διεύθυνση (domain name)[174].

Ενόψει των ανωτέρω, γίνεται αντιληπτό ότι ενδεχόμενη πλαστογράφηση τέτοιων ηλεκτρονικών δεδομένων, ήτοι δημιουργία πλαστών ηλεκτρονικών μηνυμάτων και πλαστών ιστοσελίδων προκειμένου να χρησιμοποιηθούν ως μέσο τέλεσης απάτης, μπορεί να αντιμετωπιστεί και βάσει των εγκλημάτων σχετικά με τα υπομνήματα.

6.2. Σύγχρονες μορφές εγκληματικότητας και η προβληματισμοί ως προς την ποινική τους αντιμετώπιση

Στο υποκεφάλαιο αυτό θα πραγματευτούμε τρία από τα πιο γνωστά φαινόμενα εγκληματικότητας στο σύγχρονο ψηφιακό κόσμο. Δύο εξ αυτών, το «phishing» και το «pharming», έχουν γράψει ήδη σημαντική ιστορία στο χώρο του εγκλήματος[175, 176], ενώ το τρίτο, το sim-swapping, εμφανίστηκε μόλις τα τελευταία χρόνια. Στις σύγχρονες αυτές μορφές εγκληματικότητας ο δράστης τελεί το αδίκημα της πλαστογραφίας ηλεκτρονικού εγγράφου ως προπαρασκευαστική πράξη τέλεσης απάτης ή απάτης με υπολογιστή. Στα πλαίσια της μελέτης των φαινομένων αυτών, θα αναφερθούμε τόσο στις τεχνικές των εγκληματιών, όσο και στις ποινικές διατάξεις που παραβιάζονται στις περιπτώσεις αυτές, καθώς και τους εν γένει νομικούς προβληματισμούς που γεννώνται.

---

[173] *Ζέκος Γ.,* Διαδίκτυο, Η/Υ και τηλεπικοινωνίες στο ελληνικό δίκαιο, 2017, σ. 84 επ.

[174] Κωνσταντινίδης Α, Η έννοια και η λειτουργία του εγγράφου στο ουσιαστικό και δικονομικό ποινικό δίκαιο, σελ 118.

[175] Η πρώτη αναφορά σε τεχνική «Phising» έγινε ήδη από το 1980, με την αναφορά των Jerry Felix και Chris Hauck, σε μία παρουσίαση περί Συστημάτων Ασφαλείας, στα πλαίσια ενός διεθνούς συνεδρίου μεταξύ χρηστών των προϊόντων της εταιρίας Hewlett-Packard - https://en.wikipedia.org/wiki/Phishing#1980s – προσπέλαση 30-11-2020

[176] Η πρώτη επίθεση από «Pharmers» έλαβε χώρα γύρω στον Ιανουάριο 2005 εις βάρος της εταιρίας Panix, μίας εταιρίας παροχής Υπηρεσιών Διαδικτύου, με έδρα τη Νέα Υόρκη - http://www.technicalinfo.net/papers/Pharming.html - προσπέλαση 30-11-2020

6.2.1. Το φαινόμενο «phishing» και η ποινική του αντιμετώπιση

Το φαινόμενο «phishing» ως όρος αναφέρεται στην αθέμιτη απόκτηση δεδομένων, άλλως στην διάπραξη απάτης στο διαδίκτυο[177]. Για να αποκτήσουν οι δράστες τα δεδομένα, μπορούν να χρησιμοποιήσουν διάφορες τεχνικές, οι οποίες τις περισσότερες φορές συνδυάζονται μεταξύ τους. Ενδεικτικά αναφέρουμε τις εξής: α) «Spray and Pray»[178], β) «Spear Phishing»[179], γ) «Phishing through Search Engines»[180] δ) «via Keylogger Malware»[181], ε) «Vishing (Voice Phishing)»[182] στ) «via Trojans»[183] ζ) «Link Manipulation» κτλ[184].

Στο παρόν υποκεφάλαιο θα μελετήσουμε μία από τις παραδοσιακές περιπτώσεις phishing που ξεκινούν μέσω ηλεκτρονικών μηνυμάτων (e-mails), τα οποία υποτίθεται ότι προέρχονται από αξιόπιστους οργανισμούς, κατά κανόνα από μεγάλα πιστωτικά ιδρύματα. Τα ηλεκτρονικά αυτά μηνύματα, που συνήθως περιέχουν επίσημα λογότυπα ή άλλες αναφορές ενός αξιόπιστου οργανισμού (ακόμη και πραγματικά ονόματα γνωστών στο θύμα υπαλλήλων), αποστέλλονται στον ανυποψίαστο παραλήπτη και άλλοτε ζητούν από αυτόν με διάφορες δικαιολογίες (λ.χ. επιβεβαίωση εγκατάστασης νέων τεχνικών συστημάτων ασφαλείας) την αποκάλυψη μέσω απάντησης στο e-mail ευαίσθητων δεδομένων, όπως δεδομένα εκτέλεσης συναλλαγών

[177] *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860

[178] Μαζική αποστολή e-mail σε υποψήφια θύματα, με φαινομενικό αποστολέα «γνωστή» στο θύμα εταιρία, με αίτημα τη συμπλήρωση στοιχείων, επιβεβαίωση λογαριασμού κτλ.

[179] Επιλεκτική αποστολή e-mail σε υποψήφια θύματα, των οποίων όμως ήδη γνωρίζουν κάποιες πληροφορίες (π.χ. ότι είναι πελάτες συγκεκριμένου τραπεζικού ιδρύματος), ώστε να πεισθούν ευκολότερα.

[180] Εμφάνιση πλαστών ιστοσελίδων που φέρονται να προσφέρουν φθηνά προϊόντα/υπηρεσίες ως αποτελέσματα έρευνας μέσω μηχανής αναζήτησης

[181] Κακόβουλο λογισμικό που με οποιοδήποτε τρόπο έχει εγκατασταθεί στον υπολογιστή του χρήστη και «παρακολουθεί» το πληκτρολόγιο, ήτοι συγκεντρώνει πληροφορίες περί των πλήκτρων που πατά ο χρήστης όταν επιχειρεί να εισέλθει σε συγκεκριμένη ιστοσελίδα, τις οποίες αποστέλλει στους δράστες.

[182] Απόπειρα «ψαρέματος» του θύματος μέσω social engineering, ώστε να χορηγήσει τηλεφωνικά προσωπικές του πληροφορίες στους δράστες. Αντίστοιχη με την παραδοσιακή απάτη όπου ο δράστης καλεί το θύμα, συνήθως ηλικιωμένο, και παριστάνει ότι είναι αστυνομικός ο οποίος ζητά κάποιο χρηματικό ποσό για να «σώσει» μέλος της οικογένειας του θύματος από νομικές εμπλοκές λόγω δήθεν τροχαίου ή άλλου ατυχήματος

[183] Οι «Trojan Horses» είναι είδος κακόβουλου λογισμικού που εγκαθίσταται στον υπολογιστή του χρήστη και συγκεντρώνει πληροφορίες τις οποίες αποστέλλει στους δράστες. Συνήθως εγκαθίσταται με το άνοιγμα ενός μολυσμένου αρχείου, το οποίο βρίσκεται συνημμένο σε παραπλανητικό e-mail και φέρεται να έχει γνωστή για το χρήστη «επέκταση» (πχ. ".doc" ή ".pdf"), πλην όμως στην πραγματικότητα είναι αρχείο τύπου ".exe", το οποίο, όταν ανοιχθεί από σφάλμα, εγκαθιστά το κακόβουλο λογισμικό.

[184] https://www.phishing.org/phishing-techniques - προσπέλαση 3-12-2020

μέσω διαδικτύου (λ.χ. PIN και TAN[185]), άλλοτε (ειδικά στις περιπτώσεις «Spear Phishing») έχουν ως «συνημμένο» ένα δήθεν «φορολογικό παραστατικό» συναλλαγής ή άλλο έγγραφο, το οποίο όμως στην πραγματικότητα είναι «κακόβουλο λογισμικό» όπως οι «Trojan Horses» και άλλοτε περιέχουν έναν παραπλανητικό σύνδεσμο («Link Manipulation»)[186] που παραπέμπει τον παραλήπτη σε έναν σύνδεσμο επιφανειακά αξιόπιστο, που όμως είναι φτιαγμένος κατά τέτοιο τρόπο, ώστε να τον οδηγεί σε διαφορετική ιστοσελίδα από αυτή που προβλέπεται και συγκεκριμένα σε μία πλαστή, αλλά οπτικά πανομοιότυπη με την αυθεντική, η οποία ωστόσο ανήκει στον server του δράστη[187].

Παρακάτω θα προσπαθήσουμε να χαρακτηρίσουμε από ποινικής άποψης όλες τις συμπεριφορές ενός «Phisher», στις περιπτώσεις που το e-mail του προς το υποψήφιο θύμα χρησιμοποιεί την τακτική του «Link Manipulation».

Το σύνθετο αυτό εγκληματικό φαινόμενο, φαίνεται να απαρτίζεται από δύο τουλάχιστον αυτοτελώς τυποποιούμενες εγκληματικές συμπεριφορές. Πιο συγκεκριμένα, προηγείται η αποστολή του παραπλανητικού e-mail, με φερόμενο αποστολέα κάποιο γνωστό στο θύμα τραπεζικό ίδρυμα, στο οποίο αναφέρεται ο δήθεν λόγος για τον οποίο το θύμα πρέπει να επισκεφθεί την ιστοσελίδα της τράπεζας και να βάλει τα προσωπικά του στοιχεία (username και password). Στο «ύποπτο e-mail» αναφέρεται επίσης και κάποιος «υπερσύνδεσμος» («hyperlink») που φαινομενικά θα παρέπεμπε το θύμα απευθείας στην «ιστοσελίδα της τράπεζας», πλην όμως παραπέμπει το θύμα σε κάποια «πλαστή» ιστοσελίδα, παρόμοια με τη γνωστή στο θύμα πραγματική. Με τον τρόπο αυτό με το οποίο ο δράστης αποβλέπει στην κτήση των ευαίσθητων δεδομένων του θύματος, το οποίο, εάν παραπλανηθεί από το e-mail, αποκαλύπτει τα προσωπικά του ευαίσθητα στοιχεία απευθείας στον δράστη, μέσω της καταχώρισής τους στην πλαστή ιστοσελίδα στην οποία παραπέμφθηκε διά του ανωτέρω υπερσυνδέσμου. Στη συνέχεια, αφότου πλέον ο δράστης κατέχει τα απαραίτητα «credentials», τα χρησιμοποιεί για να εισέλθει στο πληροφοριακό σύστημα της τράπεζας, ώστε μέσω της χωρίς δικαίωμα χρήσης του ειδικού λογισμικού περί μεταφοράς χρημάτων, να προκαλέσει κάποια περιουσιακή μετατόπιση.

---

[185] *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860.

[186] https://el.wikipedia.org/wiki/Phishing - προσπέλαση 3-12-2020

[187] https://el.wikipedia.org/wiki/Phishing - προσπέλαση 3-12-2020

Το ανωτέρω σύνθετο εγκληματικό φαινόμενο, παρά την τεράστια άνθησή του παγκοσμίως[188] δεν φαίνεται να έχει απασχολήσει μέχρι σήμερα την ελληνική νομολογία, ώστε να υφίσταται μία ομοιόμορφη ποινική αντιμετώπιση των ανωτέρω περιγραφόμενων συμπεριφορών. Υποστηρίζεται απλώς από μερίδα της θεωρίας ότι επειδή η ανωτέρω τεχνική του «phishing» βασίζεται στην δημιουργία πλάνης του θύματος με απώτερο σκοπό την περιουσιακή του ζημία, μέσω παράστασης ενός ψεύτικου γεγονότος (: αποστολή παραπλανητικού ηλεκτρονικού μηνύματος από τον Phisher) ως αληθινού, θα πρέπει να αντιμετωπιστεί ποινικά με τη διάταξη της κοινής απάτης (386 ΠΚ)[189]. Ωστόσο, προκειμένου να καταλήξουμε στον ορθό ποινικό χαρακτηρισμό της ανωτέρω σύνθεσης εγκληματικής συμπεριφοράς του δράστη, θα ήταν καλύτερο να εξετάσουμε χωριστά τις επιμέρους εγκληματικές του συμπεριφορές.

Πιο συγκεκριμένα, όταν ο δράστης καταρτίζει το παραπλανητικό ηλεκτρονικό μήνυμα (e-mail), με το οποίο αποσκοπά να παραπλανήσει τον παραλήπτη για το πρόσωπο του εκδότη, αφού εμφανίζει ως εκδότη του ηλεκτρονικού μηνύματος κάποιο γνωστό στο θύμα οργανισμό (π.χ. την Τράπεζα), δημιουργείται η εύλογη πεποίθηση ότι πληρείται η νομοτυπική υπόσταση της πλαστογραφίας. Εξάλλου γίνεται δεκτό ότι πλαστογραφία διαπράττεται και με την αποστολή e-mail ως δήθεν προερχόμενο από άλλο πρόσωπο, όπως εν προκειμένω[190], ενώ ο σκοπός παραπλάνησης για γεγονός που έχει έννομη σημασία είναι προφανής στην περίπτωση αυτή. Όσον αφορά δε το κρίσιμο ζήτημα του εάν το e-mail πληροί την έννοια του «εγγράφου», που είναι το (αναγκαίο) αντικείμενο της πλαστογραφίας, όπως ήδη αναλύθηκε εκτενώς ανωτέρω, γίνεται δεκτό ότι αυτό είναι έγγραφο κατά την έννοια του άρθρου 13γ ΠΚ[191]. Συνεπώς εφόσον το ηλεκτρονικό αυτό μήνυμα αποθηκεύεται αρχικά στο σκληρό δίσκο του υπολογιστή του αποστολέα, αλλά σε κάθε περίπτωση και στο σκληρό δίσκο του παρόχου υπηρεσιών ηλ. αλληλογραφίας που είναι αρμόδιος για τη διαχείριση ηλεκτρονικών μηνυμάτων του θύματος, πληρούται και η προϋπόθεση της διαιωνιστικής λειτουργίας του εγγράφου[192]. Περαιτέρω, εφόσον εμφανίζεται ως φερόμενος εκδότης του μηνύματος ένα νομικό

[188] Μια επίθεση "Spear Phising" κοστίζει μέσω όρο στον οργανισμό-θύμα περί το 1,6 εκατομμύριο δολάρια / το 85% των εταιριών/οργανισμών παγκοσμίως έχουν γίνει στόχος επιθέσεων "phising" / βλ. https://www.keepnetlabs.com/phishing-statistics-you-need-to-know-to-protect-your-organization/ αρ. 6 & 8, -προσπέλαση 3-12-2020

[189] *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ.

[190]*Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 216, αρ.17.

[191] Βλ. παραπάνω κεφάλαιο 6.1.

[192]Το απεσταλμένο ηλεκτρονικό μήνυμα περιέχεται και στο σκληρό δίσκο του παραλήπτη, βλ. ΕφΑΘ 32/2011, ΔΕΕ 2011, σ. 591, ΜΠρΧαλκ 89/2014 ΕλΔνη 2015, σ.251,

πρόσωπο, όπως για παράδειγμα ένα πιστωτικό ίδρυμα και ενσωματώνεται στο έγγραφο όνομα φυσικού προσώπου που ενεργεί ως όργανο και για λογαριασμό του νομικού προσώπου πληρείται και η εγγυητική λειτουργία του[193]. Τέλος πληρείται και η αποδεικτική του λειτουργία, αφού το e-mail είναι πρόσφορο να αποδείξει γεγονότα όπως συναλλαγές μεταξύ πελάτη και Τράπεζας[194]. Ενόψει των ανωτέρω προκύπτει ότι η κατάρτιση πλαστού e-mail κατά τα ανωτέρω, μπορεί να τιμωρηθεί ως πλαστογραφία, εφόσον πληρείται υπό τις ανωτέρω προϋποθέσεις η αντικειμενική και υποκειμενική υπόσταση της πλαστογραφίας.

Ομοίως και η κατάρτιση από το δράστη (Phisher) της πλαστής, αλλά πανομοιότυπης με την αυθεντική, ιστοσελίδας, στην οποία παραπέμπει τον παραλήπτη το παραπλανητικό e-mail, ενδέχεται να πληροί τη νομοτυπική υπόσταση της πλαστογραφίας. Και τούτο ειδικότερα διότι, όπως ήδη αναλύθηκε[195], η ιστοσελίδα υπό τις παραπάνω προϋποθέσεις πληροί την έννοια του «εγγράφου», που είναι το (αναγκαίο) αντικείμενο της πλαστογραφίας. Μάλιστα εάν ληφθεί υπόψη ότι η κατάρτιση της πλαστής αυτής ιστοσελίδας από το δράστη (:πραγματικός εκδότης), αποσκοπεί να παραπλανήσει τον παραλήπτη για το πρόσωπο του εκδότη, αφού εμφανίζει ως εκδότη της ιστοσελίδας την αξιόπιστη Τράπεζα, και για γεγονός το οποίο έχει έννομη σημασία, αντιλαμβάνεται κανείς ότι πληρείται η νομοτυπική μορφή της πλαστογραφίας.

Περαιτέρω η συμπεριφορά του δράστη, ο οποίος, αφότου αποκτήσει τα ευαίσθητα δεδομένα του παραπλανημένου θύματος, τα χρησιμοποιεί ο ίδιος, ώστε με μόνο τον επηρεασμό του αυτοματοποιημένου προγράμματος η/υ να προκαλεί ο ίδιος ο δράστης την περιουσιακή μετατόπιση από το λογαριασμό του θύματος, θα πρέπει κατά την γνώμη του γράφοντος να τιμωρείται με τις διατάξεις για την απάτη με υπολογιστή (386^{A} ΠΚ). Τούτο διότι στην προκείμενη περίπτωση η ζημία-περιουσιακή βλάβη

---

[193] *Μυλωνόπουλο Χ.*, Ποινικό Δίκαιο, Ειδικό Μέρος, Τα εγκλήματα σχετικά με τα υπομνήματα (άρθρα 216 - 223 ΠΚ), σελ. 48 επ.

[194] Ο καθορισμός της ηλεκτρονικής διεύθυνσης κατά τρόπο μοναδικό από τον ίδιο χρήστη και η δήλωση της σε κάθε αποστελλόμενο ηλεκτρονικό μήνυμα συνιστά απόδειξη της ταυτότητας του εκδότη του και κατ' αναλογία για τα οριζόμενα για το παραδοσιακό έγγραφο του άρθρου 443 ΚΠολΔ, η μηχανική του απεικόνιση σε έντυπο εμπίπτει, σύμφωνα με τη διάταξη του άρθρου 444 περ. 3 ΚΠολΔ, στην έννοια του ιδιωτικού εγγράφου, με αποδεικτική δύναμη σε βάρος του εκδότη του (συνδυασμός των άρθρων 443, 444 και 445 ΚΠολΔ), διότι αυτή ακριβώς η μοναδική για κάθε χρήστη ηλεκτρονική διεύθυνση, που έχει ορισθεί και εφαρμοσθεί από τον ίδιο τον αποστολέα, έχει τον χαρακτήρα της ιδιόχειρης υπογραφής, έστω και αν δεν έχει την παραδοσιακή μορφή της τελευταίας, ΜΠρΑΘ 1327/2001, ΔΕΕ 2001, 377επ.

[195] Βλ. παραπάνω κεφάλαιο 6.1.

προκαλείται από την πράξη του ίδιου του δράστη, αφού με μόνο τον επηρεασμό του αυτοματοποιημένου προγράμματος η/υ και συγκεκριμένα με τη χωρίς δικαίωμα εισαγωγή ορθών δεδομένων στον υπολογιστή και τη χρήση προγράμματος προορισμένου για μεταφορά χρημάτων, προκαλεί την περιουσιακή μετατόπιση, επιφέροντας με τον τρόπο αυτό μείωση της περιουσίας της τράπεζας (ή του παραλήπτη-θύματος), με συνέπεια να αποτελεί περίπτωση «ετεροπροσβολής» του έννομου αγαθού της περιουσίας του τελευταίου.

Αντιθέτως, εσφαλμένη κρίνεται από τον γράφοντα η θέση[196], βάσει της οποίας η ανωτέρω σύνθεση συμπεριφορά αυτή του δράστη, που βασίζεται στη δημιουργία πλάνης στο θύμα, θα έπρεπε να τιμωρείται ως απάτη σύμφωνα με το άρθρο 386 ΠΚ. Τούτο διότι, ναι μεν πράγματι, εάν ο παραλήπτης πειστεί ότι το e- mail είναι αυθεντικό του προκαλείται πλάνη, εντούτοις γνωστοποιώντας ο παραπλανημένος παραλήπτης τα ευαίσθητα δεδομένα του (π.χ. το username και το password ή τον αριθμό της πιστωτικής κάρτας μετά του αριθμού CVV και της ημερομηνίας λήξης) στον phisher (είτε απευθείας είτε δια της πλαστής ιστοσελίδας), δεν προβαίνει ο ίδιος (ο παραπλανημένος παραλήπτης) σε καμία άμεση περιουσιακή διάθεση, ήτοι δεν συντρέχει το στοιχείο της αυτοβλάβης. Αντιθέτως, προκειμένου να επέλθει η περιουσιακή βλάβη του θύματος, απαιτείται η παρεμβολή μίας περαιτέρω πράξης, η οποία πραγματοποιείται από τον ίδιο τον δράστη, ο οποίος είναι αυτός που, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή, μεταβιβάζει τα χρήματα από τον λογαριασμό του θύματος σε δικό του λογαριασμό ή κάνει χρήση των στοιχείων της πιστωτικής κάρτας του θύματος.. Η δε χρησιμοποίηση των ευαίσθητων αυτών δεδομένων από το δράστη για την πραγματοποίηση μεταβιβάσεων χρηματικών ποσών από τον τραπεζικό λογαριασμό του θύματος είναι αναμφισβήτητα μία αυτοτελής ενέργεια. Ως εκ τούτου, επειδή η περιουσιακή βλάβη επέρχεται με πράξη του δράστη, και όχι με πράξη του ίδιου του θύματος, δεν στοιχειοθετείται η κοινή απάτη, η οποία είναι κατεξοχήν έγκλημα αυτοζημίωσης-αυτοπροσβολής. Όλα δε τα παραπάνω επιρρώνονται και από το γεγονός ότι μόνη η κοινοποίηση των ευαίσθητων στοιχείων από το θύμα, δεν είναι απόλυτο ότι θα οδηγήσει αναγκαστικά σε βλάβη της περιουσίας του[197]. Εξάλλου το γεγονός ότι μετά

[196] *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ.

[197] *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ., υποσ. 8.

το «ψάρεμα» των ευαίσθητων στοιχείων ακολουθεί η με πράξη του δράστη περιουσιακή βλάβη του θύματος, σημαίνει απλώς ότι ο δράστης χρησιμοποιεί χωρίς δικαίωμα τα στοιχεία που πέτυχε να έχει στη διάθεση του[198]. Εξάλλου, δε μπορεί να αποκλειστούν και οι περιπτώσεις που ο phisher συγκεντρώνει τα δεδομένα από τα θύματά του, όχι για να τα χρησιμοποιήσει ο ίδιος, αλλά για να τα πουλήσει στη «μαύρη αγορά». Αντίθετα επιχειρήματα και θέσεις, που επιχειρούν να διευρύνουν το αξιόποινο του εγκλήματος της απάτης, θεωρώντας ότι, με μόνο την γνωστοποίηση των ευαίσθητων στοιχείων από το θύμα στον δράστη, προβαίνει το ίδιο το θύμα σε άμεση περιουσιακή διάθεση, δεν φαίνονται πειστικά[199].

6.2.2. Το φαινόμενο «pharming» και η ποινική του αντιμετώπιση

Από το «phishing» θα πρέπει να διακριθεί η εγκληματική συμπεριφορά του «pharming». Ως «pharming» χαρακτηρίζεται μία μέθοδος εξαπάτησης μέσω διαδικτύου, η οποία δε στοχεύει σε ευθεία παραπλάνηση του θύματος, αλλά σε «παραπλάνηση του υπολογιστή του». «Όχημα» αυτής της απάτης είναι συνήθως κάποιο είδος κακόβουλου λογισμικού (virus ή trojan horse), που «μολύνει» είτε τον υπολογιστή του θύματος[200] είτε κάποιον Domain Name Server (αν και η «μόλυνση» μπορεί να επέλθει και από ανθρώπινο χέρι – πχ του συντηρητή του server). Αποτέλεσμα της μόλυνσης είναι ότι ο συγκεκριμένος υπολογιστής επισκέπτεται μόνο πλαστές ιστοσελίδες, ακόμη και εάν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου. Έτσι το θύμα, αν και αναγράφει τη σωστή ονομασία του διαδικτυακού χώρου, παραπέμπεται σε άλλη IP διεύθυνση και καταλήγει να βλέπει στην οθόνη του μία πανομοιότυπη με την αυθεντική, αλλά πλαστή ιστοσελίδα. Ακολούθως, νομίζοντας ότι βρίσκεται σε χώρο εμπιστοσύνης, πραγματοποιεί φερ' ειπείν τις συναλλαγές του μέσω online-banking, οι οποίες ωστόσο καταλήγουν στην μεταφορά των κεφαλαίων του στους δράστες[201].

Το pharming μπορεί να πραγματοποιηθεί με ποικίλους τεχνικά τρόπους. Γενικά στρέφεται εναντίον της λειτουργίας του Domain Name System (DNS), ήτοι του Πρωτοκόλλου βάσει του οποίου κάθε domain name (π.χ. "www.abcd.com")

[198] Βλ. και *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ., υποσ. 10.
[199] Αντιθ. *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ.
[200] *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ.
[201] *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ.

αντιστοιχείται στην IP του διακομιστή της εκάστοτε ιστοσελίδας. Ειδικά δύναται να στραφεί εναντίον κάθε επιπέδου του DNS, με απώτερο σκοπό την ανακατεύθυνση του προγράμματος περιήγησης σε ψεύτικες ιστοσελίδες[202] που θα προσομοιάζουν με τις «αυθεντικές», ώστε το θύμα να πεισθεί και να συμπληρώσει τις ευαίσθητες πληροφορίες του. Το pharming μπορεί να πραγματοποιηθεί επιφέροντας αλλοίωση: είτε α) του αρχείου «host» ενός Η/Υ[203], αντιστοιχώντας το γνωστό στο χρήστη «domain name» (πχ. www.ΤΡΑΠΕΖΑ.gr) σε IP διεύθυνση που αντιστοιχεί σε πλαστή (αλλά πανομοιότυπη με την αυθεντική) ιστοσελίδα, είτε β) των ρυθμίσεων ή του firmware του δρομολογητή (router) ενός δικτύου LAN[204] ή/και WAN[205], με αποτέλεσμα όλοι οι υπολογιστές-μέλη του συγκεκριμένου δικτύου να ανακατευθύνονται σε άλλες διευθύνσεις IP από αυτές που πραγματικά επιθυμούν, είτε γ) των δεδομένων ενός DNS Server[206], με αποτέλεσμα ο συγκεκριμένος DNS Server να ανακατευθύνει λάθος όλους τους χρήστες του Διαδικτύου που έτυχε κατά το συγκεκριμένο χρόνο να εξυπηρετηθούν από αυτόν[207].

Όσον αφορά την ποινική αντιμετώπιση αυτής της εγκληματικής συμπεριφοράς, είναι προφανές ότι η αρχική συμπεριφορά, της παρέμβασης στα αρχεία εκείνα του Η/Υ ή του εκάστοτε DNS Server για να προκληθεί λανθασμένη ανακατεύθυνση μπορεί να χαρακτηριστεί ως «hacking», κατά το σημερινό άρθρο 370Δ ΠΚ[208]. Η διάταξη αυτή τιμωρεί την χωρίς δικαίωμα (: χωρίς τη συναίνεση του νόμιμου κατόχου των δεδομένων) πρόσβαση σε ηλεκτρονικούς υπολογιστές. Επειδή εν προκειμένω η τεχνική των pharmers συνιστά ένα είδος διείσδυσης μέσω διαδικτύου στον υπολογιστή του θύματος ή στον DNS Server μιας εταιρίας, η οποία αναμφισβήτητα γίνεται με δόλο

---

[202] http://www.technicalinfo.net/papers/Pharming2.html - προσπέλαση 3-12-2020

[203] "Host File" είναι το αρχείο – «ατομικός τηλεφωνικός κατάλογος», υπό την έννοια ότι αντιστοιχεί διευθύνσεις IP σε domain names. Ο περιηγητής (browser) ελέγχει πάντα πρώτα αυτό το αρχείο όταν ο χρήστης πληκτρολογεί μία διεύθυνση (domain name), και αν το domain name υπάρχει στη λίστα, τότε ο περιηγητής απλώς παραπέμπεται στην καταχωρημένη IP.

[204] LAN: Συντομογραφία για «Τοπικά Δίκτυα» - Local Area Network

[205] WAN: Συντομογραφία για «Δίκτυα Ευρείας Περιοχής» - Wide Area Network

[206] DNS Servers είναι οι διακομιστές των τοπικών, μικρότερων ή μεγαλύτερων δικτύων, στους οποίους απευθύνεται ένας Η/Υ όταν δε γνωρίζει (ήτοι δεν έχει τέτοιες εγγραφές στο «host file» του) σε ποια IP διεύθυνση αντιστοιχείται κάποιο domain name. Όσο πιο «μικρό» το δίκτυο που εξυπηρετεί ο κάθε DNS Server, προφανώς και τόσο λιγότερες οι «εγγραφές» σε αυτόν. Αν επομένως ένας Η/Υ «ρωτήσει» τον DNS Server του παρόχου υπηρεσιών διαδικτύου για κάποιο domain namekαι αυτός δεν γνωρίζει, θα απευθυνθεί σε κάποιον «μεγαλύτερο» DNS Server κ.ο.κ..

[207] http://www.technicalinfo.net/papers/Pharming2.html - προσπέλαση 3-12-2020

[208] *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., άρθρ. 370Δ, αρ. 4, όπου παραπέμπει και σε *Βασιλάκη Ε.,* ό.π., ΠοινΧρ 2007, σ. 860 επ.

και χωρίς τη συγκατάθεση του θύματος, πληρούται η νομοτυπική μορφή της ανωτέρω διάταξης[209].

Περαιτέρω, αξίζει να εξεταστεί, εάν το τμήμα της ανωτέρω συμπεριφοράς που αφορά την κατασκευή πλαστών ιστοσελίδων στις οποίες παραπέμπεται εν αγνοία του το θύμα και δηλώνει τα credentials του (username, password, pin κτλ), μπορεί να τιμωρηθεί και βάσει των διατάξεων περί πλαστογραφίας[210]. Τούτο διότι η κατάρτιση πλαστής ιστοσελίδας, πανομοιότυπης με την αυθεντική, με την οποία αποσκοπείται η παραπλάνηση ενός προσώπου όσον αφορά τον εκδότη της ιστοσελίδας και για γεγονός για το οποίο έχει έννομη συνέπεια, πληροί τη νομοτυπική μορφή της πλαστογραφίας. Το κρίσιμο δε ζήτημα της πλήρωσης της έννοιας του «εγγράφου» στην περίπτωση της ιστοσελίδας, που είναι το (αναγκαίο) αντικείμενο της πλαστογραφίας, έχει ήδη αναλυθεί εκτενώς ανωτέρω.

Όπως επομένως γίνεται σαφές, σε αμφότερες τις ανωτέρω μεθόδους (phishing και pharming) έχουμε κατασκευή πλαστών ιστοσελίδων στις οποίες τα θύματα, εν αγνοία τους, δηλώνουν ευαίσθητα στοιχεία τους, νομίζοντας ότι απευθύνονται σε έμπιστους οργανισμούς. Αυτό που τις διαφοροποιεί είναι ο τρόπος με τον οποίο τα θύματα παραπέμπονται στις ιστοσελίδες αυτές• μέσω παραπλανητικού e-mail ή μέσω παρέμβασης στον υπολογιστή ή στο δίκτυο.

6.2.3. Το φαινόμενο του «Sim Swapping» και η ποινική του αντιμετώπιση

Η έξαρση των φαινομένων υποκλοπής ευαίσθητων δεδομένων και άλλων προσωπικών στοιχείων, μεταξύ άλλων και με τις ανωτέρω μεθόδους phishing και pharming, δε μπορούσε να αφήσει αδιάφορες τις Αρχές. Πέραν των διάφορων μέτρων που ελήφθησαν από ποινικής σκοπιάς, ο ευρωπαίος νομοθέτης έπρεπε να λάβει και προληπτικά μέτρα, ώστε να περιοριστούν τα φαινόμενα διαδικτυακής απάτης που ήταν απόρροια υποκλοπής ευαίσθητων δεδομένων ηλεκτρονικής τραπεζικής (web-banking) και πιστωτικών/χρεωστικών καρτών. Τα μέτρα αυτά συμπεριελήφθησαν στην Ευρωπαϊκή Οδηγία 2015/2366/ΕΕ[211], που ενσωματώθηκε στο Ελληνικό Δίκαιο με τον Ν. 4537/2018. Μεταξύ αυτών, θεσπίσθηκε στο άρθρο 96 (αρ. 97 της Οδηγίας) η

[209] *Βασιλάκη Ε.,* , Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860 επ.

[210] βλ. *Κιούπης Δ.,* Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ευρωπαϊκή Ένωση, Δικηγορικός Σύλλογος Πειραιά – Ένωση Ελλήνων Ποινικολόγων – Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, 2010, σελ. 205-206 με εκεί παραπομπή αναφορικά με την ιστοσελίδα ως έγγραφο.

[211] Γνωστή και ως «PSD2».

υποχρέωση των «παρόχων υπηρεσιών πληρωμής»[212] να εφαρμόζουν «ισχυρή ταυτοποίηση πελάτη» στις περιπτώσεις που κάποιος *«α) αποκτά πρόσβαση online στο λογαριασμό πληρωμών του, β) εκκινεί πράξη ηλεκτρονικής πληρωμής ή γ) εκτελεί οποιαδήποτε ενέργεια εξ αποστάσεως που μπορεί να ενέχει κίνδυνο απάτης στις πληρωμές ή άλλες παραβάσεις»*. Ως ισχυρή ταυτοποίηση ορίστηκε, στο άρ. 4 περ. 30 Ν. 4537/2018 η υποχρέωση των παρόχων υπηρεσιών πληρωμής να επιβεβαιώνουν ότι ο χρήστης του web-banking ή ο χρήστης της χρεωστικής/πιστωτικής είναι ο πραγματικός δικαιούχος, «*με βάση τη χρήση δύο ή περισσότερων στοιχείων που αφορούν γνώση (στοιχείο το οποίο μόνο ο χρήστης υπηρεσίας πληρωμών γνωρίζει)* (σ.σ. οι κωδικοί εισόδου στο e-banking/ο αριθμός, η ημερομηνία λήξης και το CVV της πιστωτικής/χρεωστικής κάρτας)*, κατοχή (στοιχείο το οποίο μόνο ο χρήστης κατέχει)*(σ.σ. το κινητό του τηλέφωνο ή κάποιο φορητό αξεσουάρ όπως έξυπνο ρολόι) *και κάποιο μοναδικό εγγενές χαρακτηριστικό του (στοιχείο το οποίο ο χρήστης είναι)* (σ.σ. το δακτυλικό αποτύπωμα ή χαρακτηριστικά προσώπου)*, 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»*. Η εν λόγω διάταξη, περί υποχρέωσης ισχυρής ταυτοποίησης των χρηστών σε συγκεκριμένες συναλλαγές, τέθηκε σε ισχύ στις 14 Σεπτεμβρίου 2019, κατ' εφαρμογή του άρθρου 110 Ν. 4537/2018 (αρ. 115§4 Οδηγίας), ήτοι 18 μήνες μετά την έκδοση του ΕΕ/2018/389 κατ' εξουσιοδότηση κανονισμού της Ευρωπαϊκής Επιτροπής[213]. Επομένως, από την 14η Σεπτεμβρίου και έπειτα, για τις περισσότερες (αν όχι για όλες) τις εξ αποστάσεως συναλλαγές, είτε δια ηλεκτρονικής τραπεζικής ή άλλων υπηρεσιών διαδικτυακής πληρωμής, είτε δια απομακρυσμένης χρήσεως χρεωστικής/πιστωτικής κάρτας, οι χρήστες είναι υποχρεωμένοι να χρησιμοποιούν περισσότερους από έναν τρόπους ταυτοποίησης, έτσι ώστε, αν για οποιοδήποτε λόγο είτε υποκλαπούν τα ευαίσθητα στοιχεία τους (username/password) είτε κλαπεί η πιστωτική/χρεωστική τους κάρτα, οι δράστες να μη μπορούν να προκαλέσουν περιουσιακή ζημία δια απάτης με υπολογιστή, ήτοι να μη μπορέσουν να μεταφέρουν κονδύλια από ένα λογαριασμό σε άλλον ή να

[212] Όπως ορίζονται στο αρ. 4 περ. 11 σε συνδυασμό με το αρ. 1§2 Ν.4537/2018, ήτοι πιστωτικά ιδρύματα, ιδρύματα ηλεκτρονικού χρήματος, γραφεία ταχυδρομικών επιταγών με εξουσιοδότηση παροχής υπηρεσιών πληρωμών, ιδρύματα πληρωμών, η Ευρωπαϊκή Κεντρική Τράπεζα, το Ελληνικό Δημόσιο κτλ.

[213] Εκδοθέντος την 27η-11-2017 και δημοσιευθέντος στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης την 13η-3-2018.

αγοράσουν εμπορεύματα με χρέωση της κλεμμένης κάρτας. Στην πράξη αυτό μεταφράστηκε ως εξής: σε οποιαδήποτε μεταφορά ποσού δια web banking σε λογαριασμό τρίτου ή διαδικτυακή αγορά με χρεωστική/πιστωτική κάρτα, ο χρήστης είτε συμπληρώνει έναν «κωδικό μιας χρήσης» που έρχεται ως SMS στον τηλεφωνικό του αριθμό (που έχει ήδη δηλώσει στον πάροχο των υπηρεσιών web-banking ή/και της κάρτας), είτε εγκρίνει στο έξυπνο κινητό του τηλέφωνο την αρξάμενη συναλλαγή δια του δακτυλικού του αποτυπώματος ή της τεχνολογίας αναγνώρισης προσώπου. Η θέσπιση των ανωτέρω διαδικασιών κατέστησε σχεδόν ανέφικτη την τέλεση διαδικτυακής απάτης με τη γενική (και όχι την ποινική) του όρου έννοια, με αποτέλεσμα οι επίδοξοι δράστες να πρέπει να εξελιχθούν. Γεννήθηκε έτσι η απάτη τύπου «Sim Swapping».

Επί της ουσίας, η συμπεριφορά «Sim Swapping» είναι ο τρόπος που βρήκαν όσοι ήταν ήδη εξοικειωμένοι με την υποκλοπή δεδομένων (δια μεθόδων phishing, pharming κλπ.), προκειμένου να ξεπεράσουν το εμπόδιο της διπλής ταυτοποίησης. Προτού μελετήσουμε επομένως τις επιμέρους πράξεις των δραστών ως προς τη συγκεκριμένη συμπεριφορά, πρέπει να λάβουμε ως δεδομένο, ότι ο δράστης της «Sim Swapping» συμπεριφοράς έχει ήδη στην κατοχή του, μέσω υποκλοπής με οποιανδήποτε τρόπο, τα ευαίσθητα δεδομένα του θύματος[214]. Επομένως, ως προς την υποκλοπή των ανωτέρω δεδομένων, ανάλογα με τον τρόπο που αυτή έγινε εφικτή, ισχύουν, από ποινικής θεώρησης, όσα αναφέρθηκαν ανωτέρω περί phishing και pharming.

Έχοντας επομένως στη διάθεση του ο δράστης τα ευαίσθητα δεδομένα του θύματος (στοιχείο της γνώσης, άρθρο 4 περ. 30 του ν. 4537/2018), πρέπει να βρει ένα τρόπο να αποκτήσει πρόσβαση είτε στο στοιχείο της «κατοχής», είτε στο στοιχείο του «εγγενούς χαρακτηριστικού». Και επειδή το τελευταίο είναι αδύνατο, στόχος του δράστη καθίσταται η πρόσβαση στο αντικείμενο εκείνο που έχει μόνο το θύμα στα χέρια του, το κινητό του τηλέφωνο, ο αριθμός του οποίου, ως γνωστόν είναι μοναδικός, και αντιστοιχεί στην «κάρτα sim[215]» που είναι τοποθετημένη σε αυτό. Ως εκ τούτου, για να αποφύγει ο δράστης να κλέψει το κινητό τηλέφωνο του θύματος (το οποίο

[214] Είτε κωδικούς ταυτοποίησης (e-banking ή άλλων εφαρμογών οικονομικών συναλλαγών) είτε αριθμό, ημερομηνία λήξης και cvv χρεωστικής/πιστωτικής κάρτας.

[215] SIM: Subscriber Identity Module -το μικρό αυτό κύκλωμα, της μικρής αυτής κάρτας, περιέχει ως πληροφορίες: α) τον μοναδικό σειριακό αριθμό (ICCID), β) τον μοναδικό τηλεφωνικό αριθμό που είναι συνδεδεμένη (IMSI), τις υπηρεσίες που ο χρήστης της έχει πρόσβαση και δ) τους κωδικούς ξεκλειδώματος της (PIN και PUK)https://en.wikipedia.org/wiki/SIM_card- προσπέλαση 12-12-2020.

ενδεχομένως θα είναι και κλειδωμένο, θα γίνει δε άμεσα αντιληπτό το γεγονός της απώλειας), επιχειρεί να αποκτήσει μία κάρτα sim, η οποία αντιστοιχεί στον αριθμό του θύματος. Μόνος τρόπος γι' αυτό είναι μέσω της εκμετάλλευσης της δυνατότητας των παρόχων υπηρεσιών τηλεπικοινωνιών να «συνδέσουν» έναν τηλεφωνικό αριθμό με μία νέα κάρτα sim (ώστε αν π.χ. χαθεί το κινητό τηλέφωνο, ο πραγματικός δικαιούχος να μπορεί να διατηρήσει τον ίδιο τηλεφωνικό αριθμό και β) τα στοιχεία ταυτοποίησης του θύματος, τα οποία αποκτά είτε μέσω μεθόδων phishing είτε μέσω αγοράς στο σκοτεινό διαδίκτυο από άλλους εγκληματίες (που τα έχουν αποσπάσει με διαδικτυακές επιθέσεις μεγάλων οργανισμών/εταιριών), είτε από το ίδιο το θύμα μέσω κοινωνικής μηχανικής (social engineering). Ακολούθως, δημιουργεί πλαστά έγγραφα ταυτοποίησης (π.χ. ταυτότητα/δίπλωμα οδήγησης) και παριστάνει στους υπαλλήλους του παρόχου τηλεπικοινωνιών το ίδιο το θύμα, παραπλανώντας τους, ώστε να του χορηγήσουν μία νέα κάρτα sim, με συνδεδεμένο τον τηλεφωνικό αριθμό του θύματος, διαπράττοντας πέραν πάσης αμφιβολίας το αδίκημα της πλαστογραφίας και της πλαστογραφίας με χρήση. Με το κινητό του θύματος πλέον στην κατοχή του, ο δράστης είναι ελεύθερος να πράξει κάθε είδους απάτης με υπολογιστή, είτε «αδειάζοντας» τον λογαριασμό πληρωμών του θύματος, είτε χρεώνοντας αυτόν ή την πιστωτική/χρεωστική του κάρτα, αφού πλέον το sms για την διπλή ταυτοποίηση «προσγειώνεται» μεν στον τηλεφωνικό αριθμό του θύματος, που όμως βρίσκεται στην κατοχή του δράστη.

6.3. Συμπεράσματα ως προς τις σύγχρονες μορφές εγκληματικότητας.

Από τη μελέτη των ανωτέρω περιπτώσεων σύγχρονων μορφών διαδικτυακής εγκληματικότητας, διαπιστώνουμε ότι όσο η τεχνολογία εξελίσσεται και οι οικονομικές συναλλαγές με φυσική παρουσία μειώνονται, τόσο τα εγκληματικά στοιχεία θα στρέφονται προς το διαδίκτυο για να τελέσουν τις πράξεις τους, αφού και τα υποψήφια θύματα αυξάνονται, και το ρίσκο να γίνου αντιληπτοί και να τιμωρηθούν μειώνεται. Από ποινικής σκοπιάς, παρατηρούμε ότι σε όλες τις ανωτέρω συμπεριφορές, ο δράστης τελεί διάφορα αδικήματα (πλαστογραφία, πλαστογραφία με χρήση, hacking) για να υποκλέψει τα ευαίσθητα και μη στοιχεία του θύματος, όπως κωδικούς πρόσβασης, αριθμούς κάρτας, στοιχεία ταυτότητας, τηλέφωνα κλπ., πλην όμως ως προπαρασκευαστικές πράξεις, ως μέσα, για να μπορέσει ο δράστης εν τέλει να αποκτήσει παράνομο οικονομικό όφελος, είτε διαπράττοντας απάτης του άρθρου 386 ΠΚ και οδηγώντας το ίδιο το θύμα σε αυτοβλάβη (περιπτώσεις που φθίνουν

πλέον), είτε διαπράττοντας απάτη με υπολογιστή του άρθρου 386[Α] ΠΚ, κάνοντας χρήση των χωρίς δικαίωμα αποκτηθέντων ευαίσθητων και μη δεδομένων του θύματος.

Κεφάλαιο 7ο: Συμπέρασμα

Με την παρούσα εργασία επιχειρήθηκε η μελέτη της προσέγγισης του Έλληνα νομοθέτη ως προς την ποινική αντιμετώπιση των διάφορων μορφών ηλεκτρονικής εγκληματικότητας, που έχουν ως σκοπό τον προσπορισμό στον δράστη παράνομου περιουσιακού οφέλους. Από την εκτενή ανάλυση της εξέλιξης της μορφής της βασικής νομοθετικής διάταξης ως προς τα συγκεκριμένα αδικήματα, ήτοι του άρθρου 386Α ΠΚ, διαπιστώσαμε ότι ενώ ο Έλληνας νομοθέτης κινήθηκε γρήγορα το έτος 1988 και θέσπισε την εν λόγω διάταξη προτού καν γίνει ευρέως διαδεδομένη η χρήση του διαδικτύου στη χώρα, έπραξε τούτο σχετικά προβληματικά, όπως αποδεικνύεται από τις διάφορες διαφωνίες που παρατηρήθηκαν σε θεωρία και νομολογία. Ακολούθως, προσπάθησε να διορθώσει τις αστοχίες αυτές, κυρώνοντας (πολύ καθυστερημένα) τη Σύμβαση της Βουδαπέστης και μεταφέροντας στο Εθνικό Δίκαιο (επίσης καθυστερημένα) την Ευρωπαϊκή Οδηγία 2013/40/ΕΕ, βάσει της οποίας το ανωτέρω άρθρο κατέστη νομικά ορθότερο, ενώ με το Νέο Ποινικό Κώδικα, που τέθηκε σε ισχύ μετά την έναρξη και πριν τη λήξη συγγραφής της παρούσας, επήλθαν επιπλέον αλλαγές στην εν λόγω διάταξη, τα αποτελέσματα των οποίων μένει να φανούν τα επόμενα έτη.

Στην πορεία της έρευνας, και κατά τη μελέτη των επιμέρους εγκληματικών συμπεριφορών (ασχέτως του νομικού χαρακτηρισμού τους) κατέστη σαφές ότι οι περισσότερες μορφές ηλεκτρονικής απάτης (με τη γενική του όρου έννοια) απαιτούν από την πλευρά των επίδοξων δραστών συγκεκριμένες «προπαρασκευαστικές πράξεις» ώστε να καταφέρουν να υποκλέψουν τα απαραίτητα εκείνα ψηφιακά δεδομένα, που θα τους επιτρέψουν την περιουσιακή μεταβίβαση, μεταξύ των οποίων συμπεριλαμβάνεται και η παντί τρόπω πλαστοποίηση ψηφιακών δεδομένων. Για το λόγο αυτό και αφιερώθηκε ένα τμήμα της παρούσας στην ανάλυση της διάταξης της πλαστογραφίας (216 ΠΚ), ώστε να καταστεί σαφές πότε, και υπό ποιες προϋποθέσεις, μπορεί (ή δε μπορεί λόγω νομοθετικού κενού) να τύχει εφαρμογής και η συγκεκριμένη διάταξη κατά τον ποινικό έλεγχο των εγκληματικών αυτών συμπεριφορών, ενώ έγινε και μία προσπάθεια επεξήγησης των εφαρμοστέων ποινικών διατάξεων σε κάποιες κλασσικές περιπτώσεις ηλεκτρονικής απάτης και των τεχνικών τους.

Συμπερασματικά, θα έλεγε κανείς ότι ο Έλληνας νομοθέτης, ακολουθώντας και τις διεθνείς εξελίξεις, έκανε μια ιδιαίτερα σημαντική προσπάθεια να αποτυπώσει στον Ποινικό Κώδικα τις βασικότερες έννοιες περί πληροφοριακών συστημάτων και ψηφιακών δεδομένων, ώστε να μπορούν οι διατάξεις του να εφαρμοσθούν και στα

εγκλήματα που τελούνται στον ψηφιακό κόσμο. Από τη διαχρονική πορεία όμως της Ελληνικής ποινικής νομοθεσίας, δημιουργείται η αίσθηση ότι ο Έλληνας νομοθέτης αδυνατεί να συλλάβει τον τρόπο λειτουργίας και τις έννοιες της πληροφορικής επιστήμης, με αποτέλεσμα οι νομοθετικές του παρεμβάσεις, όταν γίνονται, να γίνονται καθυστερημένα και σχετικά κακότεχνα. Βέβαια δε μπορεί να παραγνωριστεί ότι η επιστήμη της πληροφορικής εξελίσσεται καθημερινά και οι τεχνικές των εγκληματιών αλλάζουν συνεχώς, με αποτέλεσμα να είναι δύσκολο να υπαχθούν στις προδιατυπωμένες, γενικές ποινικές διατάξεις.

Επομένως, το γενικό συμπέρασμα που προκύπτει είναι ότι καλώς θεσπίσθηκαν (έστω και καθυστερημένα) οι εκάστοτε ποινικές διατάξεις, πλην όμως δεν είναι αρκετές για να περιοριστούν οι συγκεκριμένες συμπεριφορές. Αυτό που πρέπει να λάβουν υπόψη τους όλες οι κρατικές και διακρατικές αρχές είναι ότι μόνο με την θέσπιση υποχρεωτικής λήψης προληπτικών μέτρων και κανόνων ασφαλείας από τους φορείς που διακινούν ψηφιακό χρήμα, ο χώρος των ηλεκτρονικών συναλλαγών θα γίνει ασφαλέστερος για την περιουσία του απλού χρήστη, ο οποίος βέβαια από την πλευρά του οφείλει να είναι ιδιαίτερα προσεκτικός κατά τη χρήση των πολύ σημαντικών αλλά και συνάμα ιδιαίτερα επικίνδυνων υπηρεσιών που είναι διαθέσιμες στο διαδίκτυο.

Βιβλιογραφία

- *Αγγελής Ι.,* Διαδίκτυο και Ποινικό δίκαιο. Έγκλημα στον κυβερνοχώρο, ΠοινΧρον Ν΄, σ. 675επ.
- *Αναγνωστόπουλος Η.,* Παρατηρήσεις στην ΕφΑθ 1904/1991, ΠοινΧρον ΜΒ΄(1992), 197
- *Βασιλάκη Ε.,* Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σελ. 201 επ.
- *Βασιλάκη Ε.,* Τα φαινόμενα «Phising», «Pharming» και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σ. 860
- *Γιαννόπουλος Θ.,* Όψεις και προβλήματα της ηλεκτρονικής εγκληματικότητας, NoB 1986, 170 επ.
- *Γιαννόπουλος Θ.,* Η έννοια του εγγράφου μετά τη «συμπλήρωση» του άρθρου 13γ ΠΚ και η σημασία του αστικού και αστικού δικονομικού δικαίου, Ελλ Δνη 1990
- *Δαλακούρας Θ.,* Ηλεκτρονικό Έγκλημα, 2019
- *Δούβλης Β./ Μπώλος Α.,* Δίκαιο προστασίας καταναλωτών, τομ. 2, 2008
- *Ζέκος Γ.,* Διαδίκτυο, Η/Υ και τηλεπικοινωνίες στο ελληνικό δίκαιο, 2017
- *Ιγγλεζάκης Ι.,* Δίκαιο πληροφορικής, 3η έκδ., 2018
- *Καϊάφα-Γκμπάντι Μ./ Παπακυριάκου Θ.,* Στοιχεία Ενωσιακού Ποινικού Δικαίου, 2η έκδ., 2019.
- *Κιούπης Δ.,* Ποινικό Δίκαιο και ίντερνετ, *Σάκκουλας* 1999
- *Κιούπης Δ.,* Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ευρωπαϊκή Ένωση, Δικηγορικός Σύλλογος Πειραιά – Ένωση Ελλήνων Ποινικολόγων – Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, 2010
- *Κουράκης Ν,* Κριτική επισκόπηση της νομολογίας κατά θέματα: Απάτη με ηλεκτρονικό υπολογιστή, ΠοινΛογ 2001
- *Κωνσταντινίδης Α.,* Η έννοια και λειτουργία του εγγράφου στο ουσιαστικό και δικονομικό ποινικό δίκαιο, 2000.
- *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ερμηνεία και εφαρμογή ΠΚ, 3η έκδ., Π.Ν. Σάκκουλας, 2014
- *Μαργαρίτης Μ./Μαργαρίτη Α.,* Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή, 4η έκδ., Π.Ν. Σάκκουλας, 2020
- *Μπουρμάς Γ.,* Στοιχεία απάτης με υπολογιστή κατ'άρθρο 386 α ΠΚ και διάκριση αυτής από την κοινή απάτη του άρθρου 386 ΠΚ, ΠοινΧρον ΝΑ΄
- *Μυλωνόπουλος Χ.,* Ποινικό Δίκαιο – Ειδικό Μέρος, Π.Ν. Σάκκουλας, 2016.
- *Μυλωνόπουλος Χ.,* Ποινικό Δίκαιο, Ειδικό Μέρος, Τα εγκλήματα σχετικά με τα υπομνήματα (άρθρα 216 - 223 ΠΚ), Π.Ν. Σάκκουλας, 2005.
- *Μυλωνόπουλος Χ.,* Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ. 55 επ.
- *Μυλωνόπουλος Χ.,* Η ποινική προστασία του λογισμικού κατά το Ελληνικό Ποινικό Δίκαιο, ΠοινΧρον ΛΗ΄

- *Ναμίας Ο.,* Σύγχρονες μορφές ηλεκτρονικής απάτης στις Τραπεζικές συναλλαγές, Ποιν.Χρ. 2003,487
- *Νούσκαλης Γ.,* Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386^{Α} ΠΚ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, σ. 178 επ.
- *Πανταζόπουλος Σ.,* Αναψηλάφηση της απόφασης λόγω ψευδών αποδεικτικών μέσων, 2009.
- *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, Εκδόσεις Σάκκουλα, 2000
- *Παπαδαμάκης Α.,* Τα Περιουσιακά Εγκλήματα, 3^{η} εκδ, 2020
- *Σιδηρόπουλος Θ.,* Το δίκαιο του διαδικτύου (internet), 2^{η} έκδ., 2008
- *Φράγκος Κ.,* Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα/ Άρθρο 216/ 396^{Α} ΠΚ
- *Χαραλαμπάκης Α.,* Ο Νέος Ποινικός Κώδικας, Νομική Βιβλιοθήκη, 2019
- *Jougleux P.,* Ευρωπαϊκό Δίκαιο του Διαδικτύου, 2016

Ιστοσελίδες

- https://www.sansimera.gr/articles/1252 (Προσπέλαση στις 14-11-2020)
- https://en.wikipedia.org/wiki/Tim_Berners-Lee (Προσπέλαση στις 14-11-2020)
- https://www.internetworldstats.com/emarketing.htm (Προσπέλαση στις 14-11-2020)
- https://rm.coe.int/16800cce5b Explenatory Report to the Convention on Cybercrime, Council of Europe Treaty Series- No 185, Introduction – (Προσπέλαση στις 14-11-2020)
- https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=fhgQsqgK (Προσπέλαση στις 14-11-2020)
- https://en.wikipedia.org/wiki/Phishing#1980s (Προσπέλαση στις 30-11-2020)
- http://www.technicalinfo.net/papers/Pharming.html (Προσπέλαση στις 30-11-2020)
- https://www.phishing.org/phishing-techniques (Προσπέλαση στις 3-12-2020)
- https://www.keepnetlabs.com/phishing-statistics-you-need-to-know-to-protect-your-organization (Προσπέλαση στις 3-12-2020)
- http://www.technicalinfo.net/papers/Pharming2.html (Προσπέλαση στις 3-12-2020)
- https://en.wikipedia.org/wiki/SIM_card (Προσπέλαση στις 12-12-2020)

Νομολογία

- ΟλΑΠ (ΠΟΙΝ) 179/1990, ΝοΒ 1990, 328
- ΟλΑΠ 1284/1992, ΠοινΧρ 1992, 923
- ΟλΑΠ 3/2008 – ΝΟΜΟΣ
- ΑΠ 1246/1990, ΠοινΧρ 1991, 538
- ΑΠ 1270/1993, ΠοινΛογ 2001, 2586
- ΑΠ 1152/1999 ΠραξΛογΠΔ 2000, σ. 327επ.
- ΑΠ 1224/2001 ΠοινΧρ ΝΒ` , 426
- ΑΠ (ΠΟΙΝ) 184/2002 ΠοινΛογ 2002, 155

- ΑΠ 217/2003 ΠοινΧρ ΝΓ`, 929
- ΑΠ 867/2006 ΠοινΧρ ΝΖ, 244
- ΑΠ 2530 / 2008 –ΝΟΜΟΣ
- ΑΠ 2463/2008 –ΝΟΜΟΣ
- ΑΠ 932/2009 ΙΣΟΚΡΑΤΗΣ
- ΑΠ (ΠΟΝ) 1237/2010 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 1711/2010- ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 55/2011- ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 209/2011- ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 1486/2011- ΝΟΜΟΣ
- ΑΠ 546/2011 -ΝΟΜΟΣ
- ΑΠ 742/2012 ΠοινΧρ 2013, 677
- ΑΠ 131/2013 ΠοινΧρ 2014, 185
- ΑΠ (ΠΟΙΝ) 336/2013- ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 1413/2013- ΝΟΜΟΣ
- ΑΠ 813/2015, ΠοινΧρ 2017, 179
- ΑΠ 317/2015 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ)122/2016- ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 1503/2016 -ΝΟΜΟΣ
- ΑΠ 367/2017 – ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 471/2017- ΝΟΜΟΣ
- ΑΠ 671/2017 -ΝΟΜΟΣ
- ΑΠ 902/2017 ΝΟΜΟΣ,
- ΑΠ 1414/2017 – ΝΟΜΟΣ
- ΑΠ 752/2018- ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 761/2019 -ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 1087/2019 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 1166/2019 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 790/2019 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 163/2019–ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 367/2019–ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 625/2019 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ)160/2020 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 332/2020 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ)397/2020 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 423/2020 –ΝΟΜΟΣ
- ΑΠ (ΠΟΙΝ) 317/2020 –ΝΟΜΟΣ
- ΣΤΕ (ολομ) 110/2020- ΝΟΜΟΣ.
- ΠεντΕφΑθ 678, 751/1988, ΠοινΛογ 2001
- ΕφΑθ 1904/1991 ΠοινΧρ 1992, 196 (παρατ. Αναγνωστόπουλου)
- ΕφΘεσσ 2322/2010 – ΝΟΜΟΣ
- ΕφΑΘ 32/2011, ΔΕΕ 2011, σ. 591
- ΕφΣτερΕλλ 68/2014- ΝΟΜΟΣ
- ΜΠρΑΘ 1327/2001, ΔΕΕ 2001, 377επ.
- ΠλημμΧίου 53/2007, ΠοινΧρ2008, 270
- ΜΠρΧαλκ 89/2014 ΕλλΔνη 2015, σ.251

- ΠλημμΑθ 594/2014 ΝοΒ 2014, 1683.
- ΒουλΣυμβΔΣΘες 401/1986, ΠοινΧρον ΛΣΤ΄(1986), 774 με πρόταση Αδ. Παπαδαμάκη
- ΣυμβΠλημΘε 3204/1993, Υπεράσπιση 1994, 1132
- Συμβ.Ναυτ.Πειραιώς 418/1996
- ΔιαρκΣτρατΑθ 2897/1994 ΠοινΧρ 1994, 1465 (με σύμφωνη πρόταση Κονιδάρη)
- ΣυμβΕφΠατρ 244/2001 ΠραξΛογΠΔ 2004, σ. 107 επ.
- ΣυμβΠλημμΚιλκίς 54/2012 Ποιν Δνη 2014, 238.
- ΣυμβΕφΘεσς 690/2017- ΝΟΜΟΣ