ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

ΝΟΜΙΚΗ ΣΧΟΛΗ

Π.Μ.Σ.: ΠΟΙΝΙΚΕΣ ΕΠΙΣΤΗΜΕΣ (Criminal law and Criminology)

ΕΙΔΙΚΕΥΣΗ: ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΠΟΙΝΙΚΗ ΔΙΚΟΝΟΜΙΑ (Criminal law and Criminal Procedure)

ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2022-2023

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Βέρα Ζόγκαϊ του Καστριότ
Α.Μ.: 7340162201005

Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων

(Ερμηνεία των άρθρων 370Β-ΣΤ, 292Β-Ε και 379 ΠΚ)

Επιβλέποντες:

α) Γεώργιος Τριανταφύλλου, Αναπληρωτής Καθηγητής Νομικής Σχολής ΕΚΠΑ (επιβλέπων)

β) Νικόλαος Δημητράτος, Αναπληρωτής Καθηγητής Νομικής Σχολής ΕΚΠΑ

γ) Αθανασία Διονυσοπούλου, Επίκουρη καθηγήτρια Νομικής Σχολής ΕΚΠΑ

Αθήνα, 2023

Στους γονείς μου

Πίνακας περιεχομένων

1. Εισαγωγικά

Τα εγκλήματα του λεγόμενου κυβερνοχώρου (cybercrimes) είναι εγκλήματα που διαπράττονται στο διαδίκτυο (internet) με τη χρήση Η/Υ ή ηλεκτρονικού ταχυδρομείου, με αναρτήσεις σε ιστοσελίδες, με αποστολή ηλεκτρονικών μηνυμάτων (e-mails) σε κάποιο τρίτο κ.λπ.. [1] Πρόκειται για εγκλήματα χωρίς πατρίδα καθώς καθίσταται δύσκολο να εντοπιστεί ο τόπος τέλεσής τους, όπως ενίοτε και ο δράστης. [2] Η έννοια του «εγκλήματος στον κυβερνοχώρο» έχει την έννοια του εγκλήματος στο οποίο η τεχνολογία διαδραματίζει σπουδαίο ρόλο όντας ή το μέσο ή/και το αντικείμενο του εγκλήματος. [3] Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση ηλεκτρονικών υπολογιστών (computer crime) και σε κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκαν μέσω του διαδικτύου. Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες με κυριότερες τις κακόβουλες εισβολές σε δίκτυα (hacking και cracking), επιθέσεις άρνησης εξυπηρέτησης, το κακόβουλο λογισμικό (όπως ιούς, (viruses), "σκουλήκια" (worms), δούρειους ίππους (Trojan Horses) κ.λπ.), πειρατεία λογισμικού ή ψηφιακών δεδομένων. [4] Τα αδικήματα που αποτελούν αντικείμενο ανάλυσης της παρούσης εργασίας είναι τα εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων των ηλεκτρονικών υπολογιστών.

2. Διεθνές και ευρωπαϊκό νομοθετικό πλαίσιο για την ποινική αντιμετώπιση των επιθέσεων κατά της ασφάλειας των πληροφοριακών συστημάτων και ψηφιακών δεδομένων

Σε διεθνές επίπεδο οι επιθέσεις κατά συστημάτων πληροφοριών ρυθμίζονται από τις σχετικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα [CETS No. 185, Budapest, 23.XI.2001, σε ισχύ από τις 01.07.2004].

Σε Ενωσιακό επίπεδο οι επιθέσεις κατά συστημάτων πληροφοριών ρυθμίζονται από τις σχετικές διατάξεις της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου («Οδηγία»).

Η επικύρωση της Σύμβασης της Βουδαπέστης και εν ταυτώ η ενσωμάτωση της ως άνω 2013/40/ΕΕ Οδηγίας έλαβαν χώρα στην ελληνική έννομη τάξη με τον Ν. 4411/2016 (ΦΕΚ 142/Α΄/3.8.2016).

---

[1] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 413, αρ. 676 = sakkoulas-online
Στη Διεθνή και Ενωσιακή νομοθεσία δεν έχει νομοθετηθεί κοινά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο. Κατά συνέπεια, οι όροι «έγκλημα που διαπράττεται μέσω ηλεκτρονικών υπολογιστών» [computer crime], «ηλεκτρονικό έγκλημα» [electronic crime] ή «έγκλημα στον κυβερνοχώρο» [cybercrime] χρησιμοποιούνται κατ' εναλλαγή, για να περιγράψουν «αξιόποινες πράξεις που διαπράττονται με χρήση [μέσω] ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή εναντίον αυτών των δικτύων και συστημάτων» [Ευρωπαϊκή Επιτροπή, Ανακοίνωση προς μία Γενική Πολιτική σχετικά με την Καταπολέμηση του Εγκλήματος στον Κυβερνοχώρο, COM(2007) 267, § 1.1].

[2] Σε αντίθεση με τα «παραδοσιακά εγκλήματα» του «φυσικού χώρου», τα εγκλήματα τα οποία έχουν ως μέσο τέλεσης έναν ηλεκτρονικό υπολογιστή ή γενικότερα κάποιο πληροφοριακό σύστημα είναι κατά κανόνα «εγκλήματα αποστάσεως» (βλ. σχετικώς: Χ. Μυλωνόπουλος, Διεθνές Ποινικό Δίκαιο, 1993, σελ. 160 επ.), εγκλήματα δηλαδή, κατά τα οποία η συμπεριφορά του δράστη εκδηλώνεται σε διαφορετικό σημείο από το αξιόποινο αποτέλεσμά της.

[3] MAH Strafverteidigung, § 50 Cybercrime und Datenkriminalität Rn. 8o, beck-online

[4] Η. Σεφερίδης, Ηλεκτρονικά εγκλήματα, ΠραξΛογΠΔ 4/2021.1004 = sakkoulas-online

2.1 Ιστορική αναδρομή της νομικής αντιμετώπισης

Εν έτει 2001 τα κράτη μέλη του Συμβουλίου της Ευρώπης υπέγραψαν τη Σύμβαση για το Κυβερνοέγκλημα στη Βουδαπέστη. Το Ευρωπαϊκό Συμβούλιο το 2003 εξέδωσε την Απόφαση-Πλαίσιο 2005/222/ΔΕΥ, η οποία έμελλε να καταπολεμήσει το κυβερνοέγκλημα και να προωθήσει την ασφάλεια των πληροφοριακών συστημάτων, η οποία ωστόσο δεν είχε ενσωματωθεί στην ελληνική έννομη τάξη.

Στο εγχώριο δίκαιο μια πρωτόλεια προσπάθεια καταπολέμησης του φαινομένου επιχειρήθηκε με το Ν. 1805/1988, ο οποίος εισήγαγε στα άρθρα 370Β, 370Γ και 386Α του πΠΚ τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes), εφόσον είχαν διαπραχθεί online. Με το Ν 4411/2016 κυρώθηκε η Σύμβαση της Ευρώπης για το έγκλημα στον Κυβερνοχώρο μαζί με το Πρόσθετο Πρωτόκολλο αυτής, το οποίο αφορά στην ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσεως, καθώς επίσης ενσωματώθηκε στην Ελληνική έννομη τάξη η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών. Με τον ως άνω νόμο προσετέθη το άρθρο 381Α και 381Β πΠΚ. Αμφότερες οι ως άνω διατάξεις, ενώ καταργήθηκαν με το Ν 4619/2019 (νέο ΠΚ), επανήλθαν με τα άρθρα 13 και 14 του Ν 4947/2022.

3. Το αδίκημα της παράνομης πρόσβασης σε σύστημα πληροφοριών (370Β ΠΚ)

Η ποινική αντιμετώπιση του «hacking»[5] κρίθηκε επιβεβλημένη από τη Σύμβαση της Βουδαπέστης, λόγω της αποτρεπτικής λειτουργίας που επιτελεί αυτή, προκειμένου να προστατευτούν αποτελεσματικά τα πληροφοριακά συστήματα και τα πληροφοριακά δεδομένα από τις απειλές και τους σχετικούς κινδύνους που ελλοχεύει η μη εξουσιοδοτημένη πρόσβαση. [6]

[5] Η έννοια του «hacking» αναφέρεται στη μη εξουσιοδοτημένη πρόσβαση (διείσδυση) σε σύστημα πληροφοριών ή σε στοιχεία εισαχθέντα σε υπολογιστή ή σύστημα υπολογιστών ή σε στοιχεία που μεταδίδονται με σύστημα υπολογιστών, διότι το hacking με τη μορφή της χωρίς εξουσιοδότησης πρόσβασης σε ηλεκτρονικές πληροφορίες συνθέτει τις περισσότερες πληροφορίες το πρώτο αναγκαίο βήμα για την αλλοίωση ή καταστροφή ή οποιαδήποτε άλλη κακόβουλη και καταστροφική επενέργεια επί ηλεκτρονικών πληροφοριών, όπως επί παραδείγματι τη χρησιμοποίησή του για ηλεκτρονικές απάτες. Για περαιτέρω ανάλυση επί της έννοιας βλ. Michael Bachmann, 'What Makes Them Click? Applying The Rational Choice Perspective To The Hacking Underground' (2008) <https://www.semanticscholar.org/paper/What-Makes-Them-Click-Applying-The-Rational-Choice-Bachmann/933802d90a244766e33f78f250f93e95ac9d81b3 > accessed 18 September 2023.
Οι «hackers» διαφοροποιούνται από τους «crackers» διότι οι πρώτοι συγκεντρώνουν πληροφορίες για το σύστημα το οποίο σκοπούν να παραβιάσουν προσπαθώντας να αποκτήσουν πρόσβαση σε αυτά βρίσκοντας ή "σπάζοντας" τους κωδικούς εισόδου, κατακτώντας κατ' αποτέλεσμα τα δικαιώματα του νόμιμου χρήστη του συστήματος, ενώ η δεύτερη κατηγορία πραγματοποιεί επιβλαβείς πράξεις στα συστήματα. (Γεώργιος Ζέκος, Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, 2022, σ. 363 = sakkoulas-online)

[6] Αιτιολογική Έκθεση Σύμβασης της Βουδαπέστης, σκέψη 45: «Το πιο αποτελεσματικό μέσο για την πρόληψη της μη εξουσιοδοτημένης πρόσβασης είναι, καταρχήν, η εισαγωγή και η ανάπτυξη αποτελεσματικών μέτρων ασφαλείας. Ωστόσο, μια ολοκληρωμένη απάντηση πρέπει να περιλαμβάνει επίσης την απειλή και τη χρήση μέτρων ποινικού δικαίου. Η ποινική απαγόρευση της μη

Το αδίκημα της παράνομης πρόσβασης σε συστήματα πληροφοριών ή σε δεδομένα, το οποίο εδράζεται στο άρθρο 370Β ΠΚ και το οποίο μετουσιώνει το σκοπό εναρμόνισης του ισχύοντος ελληνικού πλαισίου με το άρθρο 2 της Σύμβασης και το άρθρο 3 της Οδηγίας, έχει το ακόλουθο περιεχόμενο:

*1. Όποιος κατά παράβαση μέτρου προστασίας και χωρίς δικαίωμα αποκτά πρόσβαση σε μέρος ή στο σύνολο **συστήματος πληροφοριών ή σε ηλεκτρονικά δεδομένα** τιμωρείται με φυλάκιση έως δύο έτη ή χρηματική ποινή. Σε ιδιαίτερα ελαφρές περιπτώσεις η πράξη μένει ατιμώρητη.*

2. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του συστήματος πληροφοριών ή των δεδομένων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.

3. Αν η πράξη της παραγράφου 1 αναφέρεται σε επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή.

4. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής αξίας, επιβάλλεται φυλάκιση και χρηματική ποινή.

5. Για την ποινική δίωξη των πράξεων των παραγράφων 1 και 4 απαιτείται έγκληση.

3.1. Προστατευόμενο έννομο αγαθό

Αντικείμενο προστασίας της υπό εξέταση διάταξης συνιστά αφενός μεν το απόρρητο των ηλεκτρονικών δεδομένων (στην παρ. 1) και αφετέρου η πνευματική ιδιοκτησία (στην παρ. 3).[7] Φορέας του εννόμου αγαθού είναι το εξουσιοδοτημένο πρόσωπο, δηλαδή το πρόσωπο που δικαιούται να διαθέτει τα δεδομένα.[8] Λόγω της ιδιαιτερότητας της έννοιας των δεδομένων, το δικαίωμα διάθεσης δεν μπορεί να εξισωθεί με την ιδιοκτησία του υπολογιστή, του μέσου αποθήκευσης ή του φορέα δεδομένων.[9] Τουτέστιν η κυριότητα επί του υλικού φορέα δεν συνεπάγεται και εξουσία διάθεσης.

Το απόρρητο νοείται υπό την τυπική του έννοια, δηλαδή το τυπικό δικαίωμα του νόμιμου κατόχου των δεδομένων να αποκλείει άλλους από την πρόσβαση σε αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου υπό ουσιαστική έννοια. [10] Τα προστατευόμενα δεδομένα δεν χρειάζεται να είναι μυστικά – απόρρητα κατά την έννοια άλλων ποινικών αδικημάτων και στο αντίστοιχο άρθρο 202a StGB κατά την έννοια που νοείται αυτό στα άρθρα 203 , 206 , 353b. [11]

εξουσιοδοτημένης πρόσβασης είναι σε θέση να παράσχει πρόσθετη προστασία στο σύστημα και τα δεδομένα καθαυτά και σε πρώιμο στάδιο από τους κινδύνους που περιγράφονται ανωτέρω.»

[7] Κωστάρας Α., *ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ – ΕΠΙΤΟΜΗ ΕΙΔΙΚΟΥ ΜΕΡΟΥΣ (Άρθρα 134-410 ΠΚ)* (4η, Νομική Βιβλιοθήκη 2014). Σελ. 1153

[8] Lackner/Kühl/Heger/Heger, 30η έκδοση 2023, StGB § 202a Rn. 1

[9] MüKoStGB/Graf, 4η έκδοση 2021, StGB § 202a Rn. 2

[10] Χρίστος Μυλωνόπουλος, *ΗΛΕΚΤΡΟΝΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ Συμβολή Στην Ερμηνεία Των Άρθρων 13γ, 370Β, 370Γ Και 386Α ΠΚ (Άρθρα 2-5 Ν. 1805/1988)* (ΑΝΤ Ν ΣΑΚΚΟΥΛΑ 1991).Σελ. 92

[11] NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202a Rn. 26

Το απόρρητο υπό τυπική έννοια συνιστά ένα δικαίωμα πάνω στο πνευματικό περιεχόμενο των δεδομένων που είναι ανεξάρτητο από την κυριότητα επί του υλικού φορέα των δεδομένων και δεν συνδέεται απαραιτήτως με κάποιο οικονομικό συμφέρον.

Η διάταξη αυτή προστατεύει και το δικαίωμα στο απόρρητο της επικοινωνίας που κατοχυρώνεται στο άρθρο 19 παρ. 1 του Συντάγματος σε ό,τι αφορά, ειδικά, τις επικοινωνίες δεδομένων και αποτελεί το αντίστοιχο του άρθρου 370Α ΠΚ που αναφέρεται στην παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας.[12]

Έχει υποστηριχθεί και η άποψη [13] ότι το προστατευόμενο έννομο αγαθό συνιστά η περιουσία ως σύνολο.[14] Σε διεθνές επίπεδο η εν λόγω θεώρηση εγκαταλείφθηκε [15] καθώς η άυλη έννοια της πληροφορίας αυτονομείται από την ύλη και την ενέργεια και συμπεριλαμβάνει κάθε λογής δεδομένα, και όχι μόνο αυτά που ενέχουν προσωπική ή οικονομική αξία. [16]

Ωστόσο η διάταξη του άρθρου 370Β ΠΚ δεν αναφέρει ως απαραίτητο στοιχείο την οικονομική αξία των προστατευόμενων απορρήτων και συνεπώς αποσυνδέεται ή άλλως ανεξαρτητοποιείται το απόρρητο από την περιουσιακή του ιδιότητα .[17] Αυτό επιρρωνύεται από το γεγονός ότι κρίνεται αξιόμεμπτη η παράνομη πρόσβαση στους ηλεκτρονικούς λογαριασμούς της συζύγου, συμπεριλαμβανομένου του λογαριασμού της στο Facebook, και η δημιουργία αντιγράφων των ιδιωτικών συνομιλιών, εγγράφων και φωτογραφιών της.[18]

Άξια αναφοράς κρίνεται η απόφαση της 27ης Φεβρουαρίου 2008 - 1 BvR 370/07- του Ανώτατου Ακυρωτικού της Γερμανίας,[19] η οποία εξεδόθη στο πλαίσιο συνταγματικού ελέγχου ενός νόμου για την προστασία του Συντάγματος του κρατιδίου Βόρειας Ρηνανίας-

[12] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 418, αρ. 688 = sakkoulas-online

[13] Άγγελος Κωνσταντινίδης, Η διακεκριμένη παραβίαση απορρήτων στοιχείων (άρθρο 370Β παρ. 2 περ. β' ΠΚ, ΠοινΧρον 1997, σελ. 1216 επ.

[14] Χαρακτηριστικά το Βούλευμα του Συμβουλίου Πλημμελειοδικών Θεσσαλονίκης υπ' αριθμόν 3204/1993 (δημοσιευμένη σε Υπερ. 1994, σελ. 1133 με σχόλιο Γ. Νούσκαλη) όπου διαβάζουμε την ακόλουθη σκέψη «στην περίπτωση της παραβάσεως του άρθρου 370 ΠΚ -αθέμιτη αντιγραφή προγραμμάτων υπολογιστών-το προστατευόμενο έννομο αγαθό αποτελεί το περιουσιακό αγαθό της πληροφορίας, όπως ανευρίσκεται στο λογισμικό ενός υπολογιστή».

[15] Ιδίως μετά τη θέση σε ισχύ της Σύμβασης της Βουδαπέστης και δη από την Αιτιολογική έκθεση του άρθρου 2 της Σύμβασης, όπου ιστορικοβουλητικά συνάγεται μετά βεβαιότητας η κρίση περί ανάγκης αυτοτελούς προστασίας των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων από μη εξουσιοδοτημένη πρόσβαση σε αυτά.

[16] Κατόπιν της τροποποίησης του γερμανικού ποινικού νόμου για την καταπολέμηση του εγκλήματος ηλεκτρονικών υπολογιστών που είχε τεθεί σε ισχύ από τις 11 Αυγούστου 2007 (BGBl I, 1786), καθίσταται σαφές ότι το άρθρο 202a StGB προστατεύει το δικαίωμα διάθεσης δεδομένων ανεξάρτητα από το περιεχόμενο ή την αξία τους (Stefan Ernst, 'Το Νέο Ποινικό Δίκαιο Των Υπολογιστών, NJW 2007 , 2661). Ωστόσο στη Γερμανία ακόμη και σήμερα υποστηρίζεται ότι το 202a StGB προστατεύει κυρίως το τυπικό απόρρητο των δεδομένων, ωστόσο δευτερευόντως συμπροστατεύεται και η περιουσία (T. Fischer, § 202a StGB, σελ. 1398). Ωστόσο στα πλαίσια του ελληνικού δικαίου που η διάταξη αρκείται στη διείσδυση και δεν απαιτεί κτήση ή σκοπό κτήσης της γνώσης η εν λόγω μειοψηφούδα διάταξη κρίνεται άνευ σημασίας

[17] Ειρήνη Βασιλάκη, Η ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ ΜΕΣΩ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ Η Αντιμετώπιση Του Προβλήματος Ιδιαίτερα Μετά Την Εισαγωγή Του Ν 1805/88 (ΑΝΤ Ν ΣΑΚΚΟΥΛΑ 1993). Σελ. 159-162

[18] CASE OF BUTURUGĂ v. ROMANIA, Η διαδικτυακή βία ως μορφή ενδοοικογενειακής βίας, 11-02-2020

[19] BVerfG, Urt. v.27/02/2008, BvR 370/07, 595/07

Βεστφαλίας (Art. 5 Abs. II Nr. 11 NWVerfSchG), που παρείχε δικαιολογητικό έρεισμα κρυφής διείσδυσης για online-ανακρι έρευνα (Online-Durchsuchung) των κρατικών αρχών σε πληροφοριακά συστήματα και βάσεις δεδομένων υπόπτου για εγκληματική δραστηριότητα.

Ο νόμος αυτός κρίθηκε ανίσχυρος από το Δικαστήριο, διότι προσέβαλλε το συνταγματικό δικαίωμα ελεύθερης ανάπτυξης της προσωπικότητας, στην ιδιαίτερη πτυχή του ως συνταγματικό δικαίωμα διασφάλισης της εμπιστευτικότητας και ακεραιότητας των πλημοφοριακών συστημάτων (Grundrecht auf Gewährleistung der Vertraulichkeit und Integritāt Informationstechnischer Systeme, GVIIS), που κατοχυρώνεται, όπως επισημαίνεται, στο άρθρ. 2 παρ.1 σε συνδ. με άρθρ. 1 παρ.1 του Θεμελιώδους Νόμου (Art. 2 I i.V.m Art. 1 I GG).

Η σπουδαιότητα της απόφασης αυτής συνίσταται αφενός στο ότι για πρώτη φορά ανεγνωρίσθη ως ιδιαίτερο συνταγματικό δικαίωμα η πληροφοριακή ασφάλεια (IT-Sicherheit) για την άμεση προστασία των πληροφοριακών συστημάτων, προκειμένου να αντιμετωπιστούν οι νέοι αναδυόμενοι «ψηφιακοί κίνδυνου» και αφετέρου διαπλάσσεται αυθεντικά στην απόφαση του Συνταγματικού Δικαστηρίου το περιεχόμενο του δικαιώματος αυτού, το οποίο διακρίνεται τόσο από το δικαίωμα πληροφοριακού αυτοκαθορισμού (Recht auf informationelle Selbstbestimmung), όσο και από το απόρρητο των τηλεπικοινωνιών (Telekommunikationsgeheimnis).

3.2. Χαρακτηρολογικά γνωρίσματα

Το αδίκημα συνιστά εν μέρει κοινό και εν μέρει μη γνήσιο ιδιαίτερο (στις παρ. 2 και 4, όπου ο δράστης είναι στην υπηρεσία του κατόχου), απλό, γνήσιο πολύτροπο ή διαζευκτικώς μικτό, ενέργειας, συγκεκριμένης διακινδύνευσης,[20] απλής συμπεριφοράς (τυπικό)[21], στιγμιαίο, μη ιδιόχειρο και τέλος πλημμέλημα, το οποίο υπόκειται σε παραγραφή μετά την πάροδο 5 ετών (άρθρο 111 παρ. 3 ΠΚ).[22]

Υποστηρίζεται ότι το αδίκημα που τυποποιείται με το άρθρο 370Β ΠΚ συνιστά έγκλημα βλάβης της ασφάλειας των πληροφοριακών συστημάτων και δεδομένων, καθώς δια μέσου μίας μη εξουσιοδοτημένης πρόσβασης (unauthorized access) δεν τίθεται απλώς υπό διακινδύνευση, αλλά πλήττεται η στενότερη σφαίρα του εννόμου αγαθού της ασφάλειας

[20] Άποψη ερειδόμενη στην Αιτιολογική Έκθεση του Ν 1805/1988 για το αδίκημα της παράνομης πρόσβασης που το χαρακτήριζε ως διακινδύνευσης.
[21] Κωστάρας (n 3). Σελ. 1153
[22] ibid. Σελ. 1153 καθώς και Χ. Μυλωνόπουλος, *ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ – ΓΕΝΙΚΟ ΜΕΡΟΣ* (2η, Π Ν Σάκκουλας 2020).Σελ. 1018

(IT security).[23] [24] Η επιχειρηματολογία ερείδεται στο γεγονός ότι, με δεδομένο ότι το προστατευόμενο έννομο αγαθό της υπό εξέταση διάταξης συνιστά η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων και συστημάτων υπολογιστών, με την αθέμιτη πρόσβαση έχει ήδη προκαλέσει τη τρώση του εννόμου αγαθού της εμπιστευτικότητας του εννόμου αγαθού.[25]

Μολονότι η κρατούσα στη θεωρία άποψη ορίζει το αδίκημα της παράνομης πρόσβασης (illegal access) ως έγκλημα συμπεριφοράς, υποστηρίζεται ότι συνιστά έγκλημα αποτελέσματος, η επέλευση του οποίου συντελείται με την ολοκλήρωση της τεχνικής εισόδου στο προσβαλλόμενο πληροφοριακό σύστημα. Προς επίρρωση αυτής της άποψης, ήτοι ότι το αποτέλεσμα νομοτυπικά αυτονομείται από τη συμπεριφορά του δράστη, εισφέρεται το παράδειγμα της απόκρουσης από αντιικό λογισμικό (antivirus software) μιας επιχειρούμενης «τεχνικής επικοινωνίας» μεταξύ του συστήματος που διαχειρίζεται ο δράστης και του κατασκοπευτικού λογισμικού, που εγκατέστησε το ίδιο το θύμα, θεωρώντας το ως υγιές λογισμικό. Στο ως άνω παράδειγμα ο δράστης έχει ολοκληρώσει την εγκληματική του συμπεριφορά και αναμένει «κάτι άλλο» ως εξωτερικό γεγονός, δηλαδή το αποτέλεσμα της πράξης του αυτής, που είναι η χωρίς δικαίωμα είσοδος στο πληροφοριακό σύστημα του δικαιούχου. [26]

---

[23] Παναγιώτης Τουργέλης, Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων: συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ' (Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ), Σχολή Νομικής 2022) με παραπομπή σε C. Schwarzenegger, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001 am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Femmeldegeimnisses, σε: Festschrift für Stefan Trechsel zum 65. Geburtstag. Zürich, 2002, σελ. 316. (https://www.zora.uzh.ch/id/eprint/23961/8/Schwarzenegger_FS_Trechsel_2002.pdf), όπου ο συγγραφέας δεχόμενος ως προστατευόμενο έννομο αγαθό του άρθρου 2 της Σύμβασης την ακώλυτη εξουσία διάθεσης και ελέγχου, υποστηρίζει ότι το αδίκημα δεν είναι απλά ένα αδίκημα διακινδύνευσης. Περαιτέρω παραπέμπει και σε Ν. Ανδρουλάκη, ΠΔ, ΓενΜ ΙΙ, σελ. 36 επ., που επεξηγεί την άποψη, ότι κάθε προστατευόμενο από τον ποινικό νομοθέτη έννομο αγαθό περιβάλλεται από τρεις «σφαίρες επιρροής», δηλαδή τρεις ειρηνευμένες ζώνες, τις οποίες σχηματοποιεί σε ομόκεντρους κύκλους. Η «θραύση» της ευρύτερης σφαίρας επέρχεται με μία αθέμιτη συμπεριφορά του δράστη, η οποία δίχως να ενέχει επικινδυνότητα, διαταράσσει την ειρηνευμένη κατάσταση του έννομου αγαθού. Η άποψη αυτή για τις τρεις ζώνες προστασίας αποτελεί το δογματικό θεμέλιο της θεωρίας της εντύπωσης (Eindrucks theorie), που χρησιμοποιείται στην επιστημονική βιβλιογραφία για τη σύλληψη του αδίκου της απρόσφορης απόπειρας.

[24] Κωνσταντίνος Χατζηιωάννου, Η ποινική αντιμετώπιση των προσβολών ηλεκτρονικών δεδομένων και συστημάτων πληροφοριών: ευρωπαϊκή και εθνική διάσταση, διδακτορική διατριβή 2013, (https://freader.ekt.gr/eadd/index.php?doc=39060&lang=el#p=321), σελ. 320

[25] Την άποψη ότι πρόκειται για έγκλημα βλάβης ενστερνίζεται και ο Εμμανουήλ Μεταξάκης, ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ Βασικές έννοιες – Ερμηνεία διεθνούς, ενωσιακής και ημεδαπής νομοθεσίας – Τυπολογία, (Π. Ν. Σάκκουλας 2022) σελ. 557, με περαιτέρω παραπομπή για τη δυνατότητα ένα έγκλημα να είναι βλάβης, ακόμα και όταν δεν είναι έγκλημα αποτελέσματος, ως στερούμενου υλικού αντικειμένου σε Χ. Μυλωνόπουλος, *Ποινικό Δίκαιο - ΓΕΝΙΚΟ ΜΕΡΟΣ* (2η, Π Ν Σάκκουλας 2020) σελ. 1011.

[26] Τουργέλης Τουργέλης (n 19). Σελ. 245, με περαιτέρω παραπομπές σε Pfister, Christa, Hacking. Die Schweizer Hacking-Strafnorm (Art. 143bis StGB) im Vergleich mit den Bestimmungen der Cybercrime Convention, des Rechts der Europaischen Union, des deutschen und des österreichischen Strafrechts, Dissertation der Rechtswissenschaftlichen Fakultat Universitat Zürich, 2008, σελ. 163 όπου παρατίθεται το εδάφιο 233 της Αιτιολογικής έκθεσης της Σύμβασης της Βουδαπέστης ως εργαλείο για την ερμηνεία και επιχειρηματολογία υπέρ της θέσης ότι το αδίκημα του αντίστοιχου άρθρου 143bis ελβΠΚ συνιστά έγκλημα αποτελέσματος. Συγκεκριμένα, σύμφωνα με το άρθρο 22 της Σύμβασης της Βουδαπέστης,

3.3. Δομή και στοιχεία του εγκλήματος

Στο άρθρο 370Β ΠΚ περιέχονται τέσσερις κυρωτικοί κανόνες στις αντίστοιχες παραγράφους 1 έως 4.

3.3.1. Τα στοιχεία της αντικειμενικής υπόστασης του βασικού αδικήματος

Στην πρώτη παράγραφο στοιχειοθετείται το αδίκημα στη βασική του μορφή. Συγκεκριμένα πρόκειται για έγκλημα κοινό, η αντικειμενική υπόσταση του οποίου πληρούται αφενός με τη χωρίς δικαίωμα και κατά παράβαση μέτρου ασφαλείας απόκτηση πρόσβασης σε μέρος ή στο σύνολο συστήματος πληροφοριών και αφετέρου με τη χωρίς δικαίωμα και κατά παράβαση μέτρου προστασίας απόκτησης πρόσβασης σε ηλεκτρονικά δεδομένα.

Ευθύς εξαρχής επισημαίνεται ότι δεν προστατεύεται το μηχανικό μέρος (hardware) του Η/Υ, αλλά το λογισμικό (software), δηλαδή τα προγράμματα και τα δεδομένα που έχουν αποθηκευτεί στη μνήμη του Η/Υ, στοιχείων και προγραμμάτων. [27]

Στο σημείο αυτό σκόπιμο κρίνεται να ανατρέξουμε στον αυθεντικό ορισμό που δίδεται από το άρθρο 13 στοιχείο στ΄ ΠΚ (σε αντιστοιχία με το άρθρο 2 στοιχ. β' της Οδηγίας) όσον αφορά τον όρο πληροφοριακό σύστημα, ο οποίος είναι ταυτόσημος με τον όρο **σύστημα πληροφοριών**.[28] Συγκεκριμένα προβλέπεται ότι *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.*[29]

Η έννοια του πληροφοριακού συστήματος καλύπτει, πέραν από τους παραδοσιακούς υπολογιστές, τα έξυπνα κινητά, τους προσωπικούς ψηφιακούς οδηγούς («PDA» : Personal Digital Assistants), τις ταμπλέτες (Tablets) και παρόμοιες συσκευές, οι οποίες παράγουν, επεξεργάζονται και διαβιβάζουν ψηφιακά δεδομένα και συνδεόμενες με το διαδίκτυο («Internet»), δέχονται και στέλνουν ηλεκτρονικές επιστολές («e-mails»), μεταφέρουν αρχεία, φορτώνουν έγγραφα κ.ο.κ..

Επομένως, με τη χρήση του όρου «σύστημα πληροφοριών», δηλαδή πληροφοριακό σύστημα, στο άρθρο 370Β ΠΚ αποσαφηνίζεται ότι αντικείμενο προστασίας είναι α) η ίδια η

για τη θεμελίωση της ποινικής δικαιοδοσίας του κράτους-μέλους, βάσει της αρχής της εδαφικότητας, λαμβάνεται υπόψη, τόσο ο τόπος στον οποίο βρίσκεται το πληροφοριακό σύστημα του επιτιθέμενου (attacker), όσο και ο τόπος όπου βρίσκεται το πληροφοριακό σύστημα του θύματος. Συνεπώς, δυνάμει της διάκρισης αυτής συνάγεται ότι υφίσταται και ένας τόπος αποτελέσματος. Προς τεκμηρίωση της ως άνω θέσης αξιοποιείται επίσης η ετυμολογική προέλευση του όρου «πρόσβαση» (Γ. Μπαμπινιώτη, Λεξικό της νέας ελληνικής γλώσσας, Σελ. 1506) και εξάγεται το συμπέρασμα ότι η έννοιά της παραπέμπει σε ένα εξωτερικό γεγονός, αυτοτελές σε σχέση με την ανθρώπινη συμπεριφορά, το οποίο απαιτείται να επέλθει για να επιτευχθεί η τεχνική είσοδος του δράστη στο σύστημα και στα δεδομένα του δικαιούχου.

[27] Μιχαήλ Μαργαρίτης and Άντα Μαργαρίτη, *ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ Ερμηνεία – Εφαρμογές* (4η, Π Ν Σάκκουλας 2020). Σελ. 1084

[28] Σύστημα υπολογιστή σύμφωνα με τη Σύμβαση είναι μια συσκευή που αποτελείται από υλισμικό και λογισμικό, η οποία έχει αναπτυχθεί για την αυτόματη επεξεργασία ψηφιακών δεδομένων. Περιλαμβάνει εγκαταστάσεις εισόδου, εξόδου και αποθήκευσης και μπορεί να είναι συνδεδεμένο σε δίκτυο με άλλες παρόμοιες συσκευές ή και όχι. Convention on Cybercrime (ETS No. 185) Explanatory Report, https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf , σκέψη 23

[29] Άρθρο 13 στοιχείο στ' ΠΚ (Ν. 4619/2019)

συσκευή ή η ομάδα των διασυνδεδεμένων ή σχετικών συσκευών, που μπορεί να συνδέονται μεταξύ τους είτε ενσύρματα είτε ασύρματα και που μπορεί να αποτελούν μέρος ενός γεωγραφικά τοπικού ή ευρύτερου δικτύου και μέσω των οποίων εκτελείται αυτόματη επεξεργασία ψηφιακών δεδομένων, β) όσο και αυτά τα ίδια τα ψηφιακά δεδομένα, των οποίων η αυτόματη επεξεργασία τελείται μέσω της ως άνω συσκευής ή διασυνδεδεμένης ομάδας συσκευών. Οι ηλεκτρονικοί υπολογιστές, που αποτελούν ένα σύστημα, μπορεί να είναι συνδεδεμένοι στο δίκτυο είτε ως τερματικά σημεία είτε ως μέσα υποβοήθησης της επικοινωνίας σε ένα δίκτυο. Το καθοριστικό στοιχείο από ποινικής πλευράς είναι ότι μέσω του εν λόγω δικτύου υπολογιστών ανταλλάσσονται ψηφιακά (ηλεκτρονικά) δεδομένα ή γίνεται επεξεργασία τέτοιων δεδομένων. [30]

Από την άλλη πλευρά, ως ηλεκτρονικά δεδομένα τα οποία εννοιολογικά ταυτίζονται με την έννοια των ψηφιακών δεδομένων,[31] όπως αυθεντικά προσδιορίζονται στο άρθρο 13 στοιχείο ζ' ΠΚ, *νοούνται 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.* Στην έννοια των ψηφιακών δεδομένων δεν περιλαμβάνονται μόνο οι απλές ή σύνθετες μεμονωμένες πληροφορίες, αλλά και περίπλοκα συμπλέγματα πληροφοριών, όπως τα προγράμματα ηλεκτρονικών υπολογιστών.

Στη γλώσσα της πληροφορικής, τα δεδομένα είναι όρος ταυτόσημος με την πληροφορία, που αποτελεί αγαθό («asset») που έχει επιστημονική, τεχνολογική ή οικονομική αξία για το νόμιμο κάτοχό της, αλλά και για το κοινωνικό σύνολο και για το λόγο αυτό πρέπει να διασφαλιστεί η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητά της.[32] Κατά τον Φιλόπουλο, απαιτείται συσταλτική ερμηνεία της έννοιας των δεδομένων, ώστε να εμπίπτουν στην διάταξη μόνο δεδομένα, τα οποία περιέχουν πληροφορίες, για την γνώση των οποίων ο κάτοχός τους έχει αποκλειστικό έννομο συμφέρον. [33]

Τα εν λόγω δεδομένα, νοούνται μόνον σε σχέση με ένα πληροφοριακό σύστημα, εντάσσονται σε αυτό και μπορούν να αποθηκεύονται, να αποτελούν αντικείμενο επεξεργασίας, να ανακτώνται ή να διαβιβάζονται από τη συσκευή ή την ομάδα συσκευών, που αποτελούν το πληροφοριακό σύστημα, με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή του. Επομένως προστατεύονται από την εν λόγω διάταξη τα ψηφιακά δεδομένα τα οποία αποθηκεύονται στην κύρια μνήμη του ηλεκτρονικού υπολογιστή, που αποτελείται από τη μνήμη τυχαίας προσπέλασης («ram») και τη μνήμη μόνο για ανάγνωση («rom»). Επίσης προστασίας τυγχάνουν και εκείνα τα ψηφιακά δεδομένα που αποθηκεύονται στην περιφερειακή μνήμη του υπολογιστή, από την οποία υπάρχει επίσης η δυνατότητα ανάκτησης, επεξεργασίας και διαβίβασής τους, όταν όμως συνδέονται με ηλεκτρονικό υπολογιστή. Κύρια είδη της περιφερειακής μνήμης είναι:

α) ο σκληρός δίσκος, που είναι τοποθετημένος εσωτερικά στην κεντρική μονάδα του υπολογιστή και συνδέεται με τη μητρική κάρτα με καλώδιο

[30] Ελένη Καμπέρου σε Αριστοτέλης Χαραλαμπάκης and Ελένη Καμπέρου (eds), *Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469*, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2738

[31] Κωστάρας (n 3). Και άρθρο 13 στοιχείο ζ' ΠΚ (Ν. 4619/2019)

[32] Μαυρίδης, ό.π., 209

[33] Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021, σελ. 477

β) τα «flash drives ή usb drives», τα οποία συνδέονται απευθείας σε μια usb θύρα του υπολογιστή και προσφέρουν εύκολη μεταφορά δεδομένων

γ) οι οπτικοί δίσκοι οδηγοί («drives»), που βρίσκονται στην πρόσοψη της κεντρικής μονάδας του υπολογιστή και συνδέονται με τη μητρική κάρτα με παράλληλο κωδικό, με κυριότερα είδη τα («cd-rom») (μόνο για ανάγνωση), («cdr») (μιας εγγραφής), («cdrw») (επανεγγράψιμο) και («dvd»).

δ) Είδος περιφερειακής μνήμης του υπολογιστή του μέλλοντος είναι οι «έξυπνες κάρτες» με ενσωματωμένους μικροεπεξεργαστές. Συνεπώς δεν μένουν εκτός ποινικής προστασίας τα ηλεκτρονικά (ψηφιακά) δεδομένα που έχουν αποθηκευτεί σε οποιονδήποτε υλικό φορέα από τους προαναφερόμενους ή άλλον παρεμφερή, αφού όλοι έχουν τα γνωρίσματα του πληροφοριακού συστήματος, από τη χρονική στιγμή που συνδέονται με τον ηλεκτρονικό υπολογιστή, αποτελώντας τότε τμήμα του συγκεκριμένου πληροφοριακού συστήματος (λ.χ. η «usb» θύρα του υπολογιστή με το στικάκι «usb», η θύρα drive του υπολογιστή με το «cd-rom» ή το «dvd») και μέσω των οποίων γίνεται επεξεργασία, ανάκτηση ή διαβίβαση των ψηφιακών δεδομένων που περιλαμβάνουν οι εν λόγοι

3.3.1.2. Δράστης του εγκλήματος

Δράστης του αδικήματος μπορεί να είναι ο οποιοσδήποτε, επομένως το αδίκημα καταρχήν είναι κοινό. Στις παραγράφους 2 και 4 τυποποιείται ένα μη γνήσιο ιδιαίτερο έγκλημα (49 παρ.2 ΠΚ), καθώς η ιδιαίτερη ιδιότητα του δράστη (insider) δεν θεμελιώνει το πρώτον τον άδικο χαρακτήρα της πράξης της αθέμιτης πρόσβασης. [34] Σύμφωνα με το γράμμα του νόμου, αν ο δράστης όμως είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των ηλεκτρονικών δεδομένων, η πράξη τιμωρείται μόνο εάν η πρόσβαση απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του (παράγραφος 2 του άρθρου 370Β ΠΚ).[35]

Υποκείμενο τέλεσης του αδικήματος φυσικά δεν καθίσταται ο δικαιούχος διαχείρισης του πληροφοριακού συστήματος και των ψηφιακών δεδομένων ή το εξουσιοδοτημένο από το δικαιούχο πρόσωπο.[36] Ως εξουσιοδοτημένος σε πρόσβαση σε πληροφοριακό σύστημα νοείται λόγου χάρη ο εκτελών μια επεξεργασία δεδομένων βάσει εντολής του προϊσταμένου μιας επιχείρησης.

Εξ αντιδιαστολής γίνεται αντιληπτό ότι η κυριότητα ή η κατοχή των υλικών φορέων (hardware) αν δεν συνοδεύεται και από το αντίστοιχο δικαίωμα διαχείρισης του συστήματος και των δεδομένων ή σχετική εξουσιοδότηση από το δικαιούχο κάλλιστα μπορεί να καταστήσει αυτουργό του αδικήματος της αθέμιτης πρόσβασης τον πράττοντα τοιουτοτρόπως.[37] Σημαντικό ρόλο διαδραματίζει επί του παρόντος το άρθρο 31 του ΠΚ, για τη νομική πλάνη, η οποία αν θεωρηθεί συγγνωστή (παρ. 2) αποκλείει τον καταλογισμό σε ενοχή του πεπεισμένου υποκειμένου των προσωπικών δεδομένων ότι δικαιούται να

[34] Μυλωνόπουλος, *ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ – ΓΕΝΙΚΟ ΜΕΡΟΣ* (n 18). Σελ. 177

[35] Καμπέρου σε Αριστοτέλη Χαραλαμπάκη (n 22). Σελ. 2737

[36] Σε αντιστοιχία με το άρθρο 202a γερμ. ΠΚ (Ausspähen von Daten), όπου στην αντικειμενική υπόσταση ορίζεται «Όποιος αποκτά μη εξουσιοδοτημένη πρόσβαση για τον εαυτό του ή άλλο πρόσωπο σε δεδομένα που δεν προορίζονται για αυτόν..»

[37] Αθανάσιος Κονταξής, ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ – Συνδυασμός θεωρίας και πράξης, τόμος Β΄, 3η έκδοση, (Αντ. Ν. Σάκκουλας, 2000), σελ. 3155 στα πλαίσια ερμηνείας του 370Β προϊσχ.ΠΚ

αποκτήσει ηλεκτρονική πρόσβαση σε διαχειριζόμενο σύστημα από άλλο πρόσωπο-δικαιούχο καθ' υπέρβαση μέτρων τεχνικής προστασίας.

Στα πλαίσια νομολογιακής επεξεργασίας του άρθρου 202 a StGB κρίθηκε ότι αυτουργός του αδικήματος μπορεί να καταστεί και ο διαχειριστής ενός συστήματος, ο οποίος αποκτά πρόσβαση σε αποθηκευμένα στο σύστημα μη δημόσια ψηφιακά δεδομένα τρίτου προσώπου-δικαιούχου, υπερβαίνοντας μέτρα προστασίας (εν προκειμένω κωδικών ασφαλείας) που ετέθησαν για τον αποκλεισμό του.[38]

Στο μείζονος ενδιαφέροντος ζήτημα του εάν ο πάροχος διαδικτυακής πρόσβασης (Access Provider) καθώς και ο διαχειριστής ενός δικτύου (Network Provider) δύνανται να συνιστούν υποκείμενα τέλεσης του αδικήματος, ερευνητέο καθίσταται καταρχάς το εάν εκείνοι θεωρούνται τρίτοι απέναντι στον έχοντα την εξουσία αποκλειστικής διαχείρισης και κατ' επέκταση εάν υφίσταται η προσδοκία εμπιστευτικότητας του συστήματος και των ψηφιακών δεδομένων, τα οποία μεταδίδονται μέσω του δικτύου που διαχειρίζονται. Μολονότι η παλαιότερη στη γερμανική θεωρία άποψη τάχθηκε υπέρ της άποψης ότι δεν νοούνται ως τρίτοι, εφόσον πράγματι υφίσταται αντικειμενική τεχνολογική δυνατότητα του διαχειριστή (Administrator) να γνωρίζει λεπτομέρειες ως προς τη διαδικτυακή δραστηριότητα του χρήστη μέσω της διεύθυνσης διαδικτυακού πρωτοκόλλου (IP-Adress) χωρίς να υπάρχει κάποιο μέτρο πληροφοριακής ασφάλειας το οποίο πρέπει να υπερκεράσουν και συνεπώς απέκλειε a priori την ιδιότητα του δράστη.[39]

Παρ' ημίν υποστηρίζεται ότι καθόσον στοιχείο της αντικειμενικής υπόστασης της ποινικά άδικα πράξης της αθέμιτης πρόσβασης συνιστά η υπέρβαση τεχνικών μέτρων πληροφορικής ασφάλειας και ως τέτοια δεν νοούνται μόνον τα διατεθέντα από τον πάροχο μέτρα, αλλά και μέτρα προστασίας που έθεσε επιπροσθέτως ο ίδιος ο δικαιούχος, όπως επί παραδείγματι η κρυπτογράφηση (encryption) των μεταδιδόμενων μέσω του δικτύου δεδομένων[40], η άνευ

---

[38] *BGH, 13 Μαΐου 2020 - 5 StR 614/19 - Παράνομη πρόσβαση σε γραμματοκιβώτια από τον διαχειριστή του συστήματος* [2020] BGH 5 StR 614/19, 2020 NStZ-RR 278. Η εν λόγω απόφαση σχολιασμένη από Νικόλα Γανιάρη, στο περιοδικό Art of Crime, Νοέμβριος 2021, στο σύνδεσμο: (https://theartofcrime.gr/%CF%80%CE%B1%CF%81%CE%AC%CE%BD%CE%BF%CE%BC%CE%B7-%CE%B1%CF%80%CF%8C%CE%BA%CF%84%CE%B7%CF%83%CE%B7-%CF%80%CF%81%CF%8C%CF%83%CE%B2%CE%B1%CF%83%CE%B7%CF%82-%CF%83%CE%B5-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC/#:~:text=%CE%A3%CF%84%CE%BF%20%CE%AC%CF%81%CE%B8%CF%81%CE%BF%20370%CE%92%20%CF%80%CE%B1%CF%81.,%CE%BA%CE%B1%CF%84%CF%8C%CF%87%CE%BF%CF%85%20%CE%AE%20%CE%B1%CF%81%CE%BC%CE%BF%CE%B4%CE%AF%CE%BF%CF%85%20%CF%85%CF%80%CE%B1%CE%BB%CE%BB%CE%AE%CE%BB%CE%BF%CF%85%20%CF%84%CE%BF%CF%85%C2%BB.)

[39] Η άποψη αυτή συνυφαίνεται με το γεγονός ότι η υπέρβαση μέτρων ασφαλείας συνιστά τμήμα της αντικειμενικής υπόστασης του δράστη της αθέμιτης πρόσβασης σε αποθηκευμένα σε σύστημα πληροφορικής ή μεταδιδόμενα μέσω αυτών ηλεκτρονικά δεδομένα, όπως υποδεικνύεται από την Αιτιολογική Σκέψη του Γερμανού νομοθέτη.

[40] Τα Εικονικά Ιδιωτικά Δίκτυα (VPN) παρέχουν μια κρυπτογραφημένη σύνδεση μεταξύ της συσκευής ενός χρήστη και ενός απομακρυσμένου διακομιστή, αποκρύπτοντας την αρχική διεύθυνση IP. Το VPN λειτουργεί με τη δημιουργία μιας κρυπτογραφημένης σήραγγας (encrypted tunnel) μεταξύ της συσκευής του χρήστη και ενός απομακρυσμένου διακομιστή VPN, διασφαλίζοντας ότι όλα τα δεδομένα που μεταδίδονται είναι ασφαλή από υποκλοπές και χάκερ. Για περαιτέρω ανάλυση των τεχνικών τρόπων διαδικτυακής ανωνυμίας: Raymond Andrè Hagen ' Tools for Achieving Anonymity on the Internet | LinkedIn' <https://www.linkedin.com/pulse/tools-achieving-anonymity-internet-raymond-andr%C3%A8-hagen/> accessed 20 September 2023.

εξουσιοδότησης αποκρυπτογράφηση των δεδομένων από τον πάροχο του δικτύου ηλεκτρονικών επικοινωνιών πληροί την αντικειμενική υπόσταση. [41]

Από τα ανωτέρω συνάγεται ότι ο πάροχος πρόσβασης σε δίκτυο πληροφοριών (access/network provider) μπορεί να αποτελεί τρίτο πρόσωπο σε σχέση με τον δικαιούχο διαχείρισης ενός πληροφοριακού συστήματος καθώς και των μεταδιδόμενων ψηφιακών δεδομένων.

Όπως αναφέρθηκε εκ προοιμίου, σε αντίθεση με την παράγραφο 1, στις παραγράφους 2 και 4 ο νομοθέτης τυποποιεί ένα μη γνήσιο ιδιαίτερο έγκλημα, στο οποίο δράστης μπορεί να είναι μόνο εκείνο το πρόσωπο που ευρίσκεται στην υπηρεσία του νόμιμου κατόχου του παραβιαζόμενου πληροφοριακού συστήματος ή ηλεκτρονικών δεδομένων και νόμιμου κατόχου των παραβιαζόμενων στοιχείων αντιστοίχως.

Η ιδιότητα του εσωτερικού δράστη θεμελιώνεται στο πλαίσιο μιας εξαρτημένης ή ανεξάρτητης εργασιακής σχέσης, καθώς και σύμβασης έργου τόσο του δημοσίου όσο και του ιδιωτικού τομέα, ανεξάρτητα από τη βαθμίδα της υπαλληλικής σχέσης και τη φύση των καθηκόντων. [42] Στην εν λόγω περίπτωση υπάγονται επίσης τόσο ο διευθυντής μίας εταιρείας, που δεν έχει δικαίωμα πρόσβασης σε συγκεκριμένα αποθηκευμένα αρχεία δεδομένων του συστήματος πληροφοριών της επιχείρησης, όσο και η καθαρίστρια αλλά και προγραμματιστές, αναλυτές, χειριστές η/υ και ηλεκτρολόγοι, ακόμα και αν δεν τελούν σε προσωρινή υπαλληλική σχέση. [43]

Η απαγόρευση πρόσβασης του υπαλλήλου στο πληροφοριακό σύστημα ή στα ψηφιακά δεδομένα πρέπει να προκύπτει ρητά και μάλιστα εγγράφως από τον εσωτερικό κανονισμό ή απόφαση του νόμιμου κατόχου ή αρμόδιου υπαλλήλου. Ο εσωτερικός κανονισμός του οργανισμού ή της επιχείρησης περιέχει την εταιρική πολιτική ασφάλειας (corporate security policy), η οποία είναι σε έγγραφη μορφή και εκτός από τους μηχανισμούς ασφαλείας για την προστασία των πληροφοριακών αγαθών του οργανισμού της επιχείρησης, περιγράφει αναλυτικά τους δικαιούμενους σε πρόσβαση στα πληροφοριακά δεδομένα, το είδος της πρόσβασης, τον τύπο των δεδομένων καθώς και το χρονικό διάστημα και την αιτία της παροχής πρόσβασης. Το έγγραφο αυτό κρίνεται υψίστης σημασίας για κάθε φυσικό ή νομικό πρόσωπο που διατηρεί αυτοματοποιημένα συστήματα επεξεργασίας δεδομένων, διότι σε αυτό καθορίζονται τα πρόσωπα των δικαιούμενων πρόσβασης στο πληροφοριακό σύστημα, αλλά και το είδος και η έκταση πρόσβασης του καθενός εργαζομένου. Αν δεν υφίσταται τέτοιος γραπτός εσωτερικός κανονισμός ή έγγραφη απόφαση του νόμιμου κατόχου του πληροφοριακού συστήματος, που να απαγορεύει ρητά την πρόσβαση του υπαλλήλου στο σύνολο ή σε συγκεκριμένο μέρος του πληροφοριακού συστήματος ή των δεδομένων του, η πρόσβαση είναι ελεύθερη και συνεπώς δεν συγκροτείται η αντικειμενική υπόσταση του εγκλήματος. [44] Κατά συνέπεια, αφής στιγμής ο νόμος απαιτεί να είναι διατυπωμένη εγγράφως και ρητά η σχετική απαγόρευση πρόσβασης, δεν αρκεί ούτε η προφορική απαγόρευση ούτε και η από τις περιστάσεις ή το κείμενο του εσωτερικού κανονισμού ή της

[41] Τουργέλης (n 19). Σελ. 248

[42] Κωστάρας (n 3). Σελ. 249 στα πλαίσια ερμηνείας του προϊσχύσαντος άρθρου 370Β ΠΚ

[43] Μυλωνόπουλος, *ΗΛΕΚΤΡΟΝΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ Συμβολή Στην Ερμηνεία Των Άρθρων 13γ, 370Β, 370Γ Και 386Α ΠΚ (Άρθρα 2-5 Ν. 1805/1988)* (n 6) 84 έως 85. Βασιλάκη (n 11) 183–184.

[44] Ελένη Καμπέρου σε Αριστοτέλη Χαραλαμπάκη (ed), *Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469*, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2737

απόφασης του κατόχου ή του αρμοδίου υπαλλήλου του έμμεσα συμπερασματικά συναγόμενη απαγόρευση πρόσβασης.

3.3.1.3. Υλικό αντικείμενο του εγκλήματος

Υλικό αντικείμενο του εγκλήματος αποτελούν το σύνολο ή μέρος, ήγουν ένα αρχείο ή ο φάκελος, ενός πληροφοριακού συστήματος πληροφοριών ή των ηλεκτρονικών του δεδομένων του. Ποινικά υπόλογος καθίσταται εκείνος που παράνομα αποκτά πρόσβαση σε ένα αυτόνομο πληροφοριακό σύστημα που λειτουργεί απομονωμένα μέσω ενός ηλεκτρονικού υπολογιστή, χωρίς να επικοινωνεί με άλλα συστήματα, αλλά και εκείνος που αποκτά πρόσβαση σε ένα δίκτυο υπολογιστών που διασυνδέονται μεταξύ τους μέσω κόμβων (υπολογιστές, εκτυπωτές, δρομολογητές), γραμμών μεταφοράς δεδομένων μεταξύ των κόμβων και κατάλληλου λογισμικού και πρωτοκόλλων δικτύωσης. Επομένως, υλικό αντικείμενο του εγκλήματος μπορούν να είναι κατ' αρχήν οι κόμβοι, οι γραμμές μεταφοράς των δεδομένων μεταξύ τους, το λογισμικό και τα πρωτόκολλα δικτύωσης, τα πρωτόκολλα επικοινωνίας μεταξύ των κόμβων και τα πρωτόκολλα του επιπέδου εφαρμογής, ιδίως το «DNS» που αποτελεί ένα είδος τηλεφωνικού καταλόγου του διαδικτύου, το «SMTP», που είναι το βασικό στοιχείο του «email» και το «HTPP», που χρησιμοποιείται από τις περισσότερες διαδικτυακές εφαρμογές. [45]

Δεν μπορεί όμως να αποτελούν υλικό αντικείμενο του εγκλήματος τα «στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών», τα οποία προστατεύονται από τη χωρίς δικαίωμα πρόσβαση σε αυτά κατ΄ εφαρμογή της διάταξης του άρθρου 370Δ παρ. 2 του νέου ΠΚ.

3.3.1.4. Χωρίς δικαίωμα πρόσβαση

3.3.1.4.1. Πρόσβαση

Ως **πρόσβαση** λογίζεται η είσοδος σε σύστημα πληροφοριών, χωρίς να απαιτείται η επεξεργασία, η αντιγραφή ή η χρήση των στοιχείων. Το αξιόποινο του δράστη συνίσταται στη διείσδυση στο σύστημα μέσω μιας μη ηθελημένης παραβίασης των μηχανισμών ελέγχου του συστήματος χωρίς να έχει άδεια πρόσβασης, ενώ δεν αποτελεί στοιχείο της νομοτυπικής υπόστασης και ο σκοπός δολιοφθοράς, καταστροφής, ή αποκόμισης οικονομικού οφέλους. [46]

Π.χ. Παρακολουθείτε το φίλο σας να συμπληρώνει το όνομα χρήστη και τον κωδικό πρόσβασης. Γνωστό και ως shoulder surfing («κρυφοκοίταγμα» - «κοίταγμα πάνω από τον ώμο»). [47] Θυμάστε τα στοιχεία σύνδεσής του και χωρίς την άδειά του, αργότερα συνδέεστε και διαβάζετε όλα τα μηνύματά του.

Με άλλα λόγια η μη εξουσιοδοτημένη πρόσβαση σε ξένο ηλεκτρονικό υπολογιστή ή σύστημα υπολογιστών δεν είναι αναγκαίο να γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας, αλλά αρκεί να πραγματοποιείται λ.χ. μόνο για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας.[48] Αυτή καθεαυτή η διείσδυση είναι

---

[45] Μαυρίδης Ι., Ασφάλεια πληροφοριών στο διαδίκτυο, σελ. 40 επ., Κεφάλαιο 2.6. «Το επίπεδο Εφαρμογής», Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα, www.kallipos.gr, ΣΕΑΒ, 2015.

[46] Καμπέρου σε Αριστοτέλη Χαραλαμπάκη (n 23) 2739.Με περαιτέρω παραπομπές.

[47] Βλ. για το shoulder surfing στον ακόλουθο ιστότοπο: https://www.techtarget.com/searchsecurity/definition/shoulder-surfing

[48] Ήδη από την Αιτιολογική έκθεση της Σύμβασης της Βουδαπέστης, εντοπίζουμε την επισήμανση ότι «η απλή μη εξουσιοδοτημένη διείσδυση, δηλαδή το "hacking", το "cracking" ή η "καταπάτηση

φορέας αυτοτελούς αδίκου, με τη μορφή έντονης διακινδύνευσης περαιτέρω εννόμων αγαθών, καθώς δημιουργεί τη δυνατότητα άπειρων περαιτέρω καταχρήσεων: εξάλειψη δεδομένων, μεταβολή ξένων κωδικών λέξεων, αποστολή εξυβριστικών ή απειλητικών κειμένων με ξένο όνομα, διάπραξη απατών κ.τ.λ..[49] Αυτό καθίσταται ιδιαίτερα αντιληπτό λόγω της εξάπλωσης του IoT[50] και την άμεση επίδραση του ψηφιακού περιβάλλοντος πάνω στο φυσικό, όπου ο δράστης αποκτά απεριόριστες δυνατότητες βλάβης ή διακινδύνευσης πολλών εννόμων αγαθών. [51]

Για το λόγο αυτό συμπεριλαμβάνονται και επιθέσεις κατά πληροφοριακών συστημάτων ήσσονος σημασίας, όπως και πράξεις κυβερνοακτιβισμού (hacktivism) που τελούνται για πολιτικούς ή συμβολικούς λόγους, χωρίς να διακινδυνεύουν τη λειτουργία των πληροφοριακών συστημάτων. [52]

Από τεχνικής πλευράς, η πρόσβαση ονομάζεται «παρείσφρηση» και μπορεί να γίνει με διάφορους τρόπους όπως λ.χ. με την αξιοποίηση πληροφοριών που προέρχονται από υπαλλήλους ή συνεργάτες του παρόχου, με εκμετάλλευση της τάσης των χρηστών να επιλέγουν προβλέψιμα συνθηματική ή της τάσης τους να αποκαλύπτουν πληροφορίες σε φαινομενικά αξιόπιστα άτομα.

Κατεξοχήν περιπτώσεις μιας τέτοιας πρόσβασης συνιστούν το <<hacking>> , το οποίο συνίσταται στη μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή σύστημα υπολογιστών, η οποία καταρχήν δεν γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της

υπολογιστή" θα πρέπει κατ' αρχήν να είναι παράνομη από μόνη της» και Ελένη Καμπέρου σε Αριστοτέλη Χαραλαμπάκη (ed), *Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469*, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2734

[49] Μυλωνόπουλος (n 2), σελ. 93. Με περαιτέρω παραπομπή σε Sieber Inf Tech 19/20, 53 και Βασιλάκη (n 4), σελ.86-87

[50] Οι επιθέσεις στο Διαδίκτυο των Πραγμάτων (IoT): Το Διαδίκτυο των πραγμάτων εξαπλώνεται μέρα με τη μέρα. Αυτές περιλαμβάνουν φορητούς υπολογιστές και tablet, δρομολογητές, διαδικτυακές κάμερες, έξυπνα ρολόγια, ιατρικές συσκευές, κατασκευαστικό εξοπλισμό, αυτοκίνητα, ακόμη και συστήματα οικιακής ασφάλειας. Οι καταναλωτές επίσης αλλά και οι επιχειρήσεις επωφελούνται από αυτές τις συσκευές που συνδέονται με το διαδίκτυο, καθώς εξοικονομούν χρήματα από συλλέγοντας τεράστιες ποσότητες δεδομένων και απλοποιώντας τις επιχειρηματικές διαδικασίες. Ωστόσο, η σύνδεση με αυτόν τον όγκο ηλεκτρονικών συσκευών δεν σημαίνει ασφάλεια, αλλά μάλλον την το αντίθετο, καθώς η σύνδεση με περισσότερα Internet of Things πραγμάτων σημαίνει ότι είμαστε ευάλωτοι σε ηλεκτρονικές εισβολές. Μόλις οι χάκερς αποκτήσουν τον έλεγχο των συσκευών IoT, οι συσκευές μπορούν να χρησιμοποιηθούν για να "διαταράξουν", να υπερφορτώσουν δίκτυα, ή να κλειδώσουν βασικό εξοπλισμό για οικονομικό όφελος. Ismail Humied, Common Risks and Challenges in Cybercrime (May 2023) DOI:10.13140/RG.2.2.34392.67840 (file:///C:/Users/User/Downloads/9-21CommonRisksandChallengesinCybercrime.pdf)

[51] Γεώργιος Ζέκος, Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, (Εκδόσεις Σάκκουλα 2022), σ. 360 = sakkoulas-online

[52] Μολονότι η εν λόγω πρόβλεψη δεν ήταν υποχρεωτική κατά την Οδηγία 2013/46/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου κατά το άρθρο 50 της Επεξηγηματικής Έκθεσης του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα και συγκεκριμένα, «*Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system. The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems (including public networks provided by telecommunication services and private networks, such as Intranets or Extranets)*.»

κατασκοπείας, αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Υ/Η, [53] το <<cracking>> που αποτελεί το σπάσιμο συστημάτων ασφαλείας και το <<pharming>>, που αποτελεί ένα ειδικό πρόγραμμα το οποίο διεισδύει στον υπολογιστή του θύματος ούτως ώστε ο συγκεκριμένος υπολογιστής να μπορεί να επισκέπτεται μόνο πλαστές σελίδες, ακόμα και αν ο χρήστης αναγράφει τη σωστή διεύθυνση του διαδικτυακού τόπου. [54] [55]

Η «ηλεκτρονική είσοδος» στο σύστημα ή σε αποθηκευμένο αρχείο ψηφιακών δεδομένων του δικαιούχου μπορεί να γίνει με τη βοήθεια τεχνικών εργαλείων, όπως λογισμικών ανίχνευσης «αδύνατων σημείων» του συστήματος και κατασκοπευτικών λογισμικών,[56] δούρειου ίππου (Trojan horse) και καταγραφέα πληκτρολογίου (keylogger), μέσω των οποίων παρέχεται η δυνατότητα στο δράστη να παρακολουθεί την ηλεκτρονική δραστηριότητα του θιγόμενου προσώπου.

Χρήζει ιδιαίτερης προσοχής η ποινική αξιολόγηση της εγκατάστασης από το ίδιο το πλανώμενο θύμα των μολυσματικών λογισμικών, που επιτρέπουν στο δράστη, κατόπιν διασύνδεσής του με το εγκατεστημένο λογισμικό, να αποκτήσει πρόσβαση. Στη γερμανική επιστήμη κατ' εφαρμογή της θεωρίας της κυριαρχίας επί της πράξης (Tatherrschaft), [57] υποστηρίζεται ότι η ποινική ευθύνη του δράστη (hacker) για αθέμιτη πρόσβαση κατ' έμμεση αυτουργία θεμελιώνεται στη χειραγώγηση και παραπλάνηση του θύματος, που καθίσταται όργανο των εγκληματικών σχεδίων του.

Στο ελληνικό ποινικό δίκαιο η έμμεση αυτουργία,[58] επιτελεί «εμβαλωματική» λειτουργία για την ποινική αντιμετώπιση περιπτώσεων , μη τιμωρούμενων υπό το κράτος του συστήματος της περιορισμένης εξάρτησης της συμμετοχικής δράσης από τον αυτουργό. [59] Στην ελληνική επιστημονική θεωρία συνιστά περίπτωση έμμεσης αυτουργίας η παραπλήνηση του θύματος

---

[53] Ανδρέας Αργυρόπουλος, Ηλεκτρονική εγκληματικότητα, Τα αδικήματα της χωρίς άδεια απόκτησης δεδομένων (202a StGB), της παραποίησης δεδομένων (303a StGB) και της δολιοφθοράς Η/Υ (303b StGB) σε σχέση με το hacking και τη μετάδοση των ηλεκτρονικών ιών στο Internet (ΑΝΤ. Ν. Σάκκουλα 2001). Σελ. 34-36.

[54] Καμπέρου σε Αριστοτέλη Χαραλαμπάκη (n 9). Σελ

[55] Μυλωνόπουλος, *ΗΛΕΚΤΡΟΝΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ Συμβολή Στην Ερμηνεία Των Άρθρων 13γ, 370Β, 370Γ Και 386Α ΠΚ (Άρθρα 2-5 Ν. 1805/1988)* (n 6).

[56] Επί παραδείγματι, το exploit που είναι ένα πρόγραμμα ή ένα κομμάτι κώδικα που έχει σχεδιαστεί για να βρίσκει και να εκμεταλλεύεται ένα ελάττωμα ασφαλείας ή μια ευπάθεια σε μια εφαρμογή ή ένα σύστημα υπολογιστή, συνήθως για κακόβουλους σκοπούς, όπως η εγκατάσταση κακόβουλου λογισμικού. Ένα exploit δεν είναι το ίδιο το κακόβουλο λογισμικό, αλλά μάλλον είναι μια μέθοδος που χρησιμοποιείται από τους εγκληματίες του κυβερνοχώρου για την παράδοση κακόβουλου λογισμικού. Για περισσότερα βλ. ενδεικτικά: 'What Is an Exploit?' (*Cisco*) <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html> accessed 20 September 2023.

[57] Claus Roxin, Täterschaft und Tatherrschaft, Schönke/Schröder, StGB vor § 25 Rn. 57, beck-online, NK-StGB/Schild/Kretschmer, 6. Aufl. 2023, StGB § 25 Rn. 29, και παρ' ημίν Νικόλαος Ανδρουλάκης, Ποινικό Δίκαιο- Γενικό Μέρος, ΙΙ Απόπειρα και Συμμετοχή, (Π.Ν. Σάκκουλας 2004) σελ. 137 έως 139

[58] Η θεωρία της "κυριαρχίας επί της πράξης" συνιστά παρ' ημίν μια θεωρία για την έμμεση αυτουργία, όπως εισήχθη στην Ελληνική Επιστήμη η περί Tatherrschaft θεωρία του Roxin, από τον Χαραλαμπάκη με τίτλο "Η έμμεση αυτουργία – Σκέψεις σε βασικά προβλήματα της συμμετοχής στο ελληνικό ποινικό δίκαιο" (ΑΝΤ. Ν. Σάκκουλα Αθήνα- Κομοτηνή 1998)

[59] Νικόλαος Ανδρουλάκης, Ποινικό Δίκαιο- Γενικό Μέρος, ΙΙ Απόπειρα και Συμμετοχή, (Π.Ν. Σάκκουλας 2004) σελ. 142- 143 (ο ρόλος του έμμεσου αυτουργού)

από το δράστη, η οποία οδηγεί σε αυτοκαταστροφική ενέργεια του παραπλανηθέντος.[60] Ως τέτοια παραπλάνηση μπορεί να ιδωθεί και η αναληθής παρουσίαση από το δράστη ενός κατασκοπευτικού λογισμικού ενός «υγιούς» για τη λειτουργία του πληροφοριακού συστήματος του δικαιούχου ή ακόμη και επωφελούς, ώστε το θύμα, που δεν γνωρίζει, να κατεβάσει (download) από το διαδίκτυο το λογισμικό αυτό (π.χ. δούρειο ίππο[61]), επιτρέποντας έτσι, στο δράστη να αποκτήσει πρόσβαση στο σύστημα και στα δεδομένα που διαχειρίζεται.

3.3.1.4.2. «Χωρίς δικαίωμα»

Προκειμένου να πληρούται ο όρος της αθέμιτης πρόσβασης θα πρέπει εκείνη να λαμβάνει χώρα άνευ δικαιώματος. Καταρχάς, δυνάμει της Αιτιολογικής Έκθεσης της Σύμβασης της Βουδαπέστης, [62] αυτό σημαίνει ότι δεν ποινικοποιείται η πρόσβαση που έχει επιτραπεί από τον ιδιοκτήτη ή άλλο δικαιούχο του συστήματος ή μέρους αυτού (όπως για τους σκοπούς της εγκεκριμένης δοκιμής ή της προστασίας του εν λόγω συστήματος πληροφορικής). Συνεπώς, ο εντοπισμός κενών ασφαλείας στο σύστημα πληροφορικής μιας εταιρείας, δεν τιμωρείται εάν στον «χάκερ» είχε ανατεθεί αυτό το καθήκον από τον ιδιοκτήτη της εταιρείας. [63] Κατά συνέπεια, μπορεί να εξαχθεί το συμπέρασμα ότι η συγκατάθεση του δικαιούχου, αποκλείει ήδη την πλήρωση της αντικειμενικής υπόστασης.[64]

Ως περίπτωση «δικαιωματικής πρόσβασης» σταχυολογείται η ελεύθερη και ανοικτή πρόσβαση σε δημόσια δίκτυα (public networks).[65]

---

[60] Στοιχειοθετείται η έμμεση αυτουργία όταν ελλείπει η άδικη κυρία πράξη, στην περίπτωση που ο δράστης εκμεταλλεύεται την αδυναμία του πράττοντος να αντιληφθεί τη σημασία της πράξης του και έτσι κυριαρχεί επ' αυτής λόγω της υπέρτερης γνώσης του (Irrtumsherrschaft) Χρίστος Μυλωνόπουλος, *Ποινικό Δίκαιο - ΓΕΝΙΚΟ ΜΕΡΟΣ* (2η, Π Ν Σάκκουλας 2020) 914–919.

[61] Το κακόβουλο λογισμικό (malware)"δούρειος ίππος" είναι ένας τύπος λογισμικού που "κατεβαίνει" σε έναν υπολογιστή μεταμφιεσμένος ως νόμιμο πρόγραμμα. Σε αντίθεση με υπόλοιπα κακόβουλα λογισμικά υπολογιστών (computer viruses, computer worms), ένας δούρειος ίππος δεν μπορεί να ενεργοποιηθεί από μόνος του, οπότε απαιτείται να το κατεβάσει ο χρήστης. Για περισσότερες λεπτομέρειες βλ. Εμμανουήλ Μεταξάκης, ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ Βασικές έννοιες – Ερμηνεία διεθνούς, ενωσιακής και ημεδαπής νομοθεσίας – Τυπολογία, (Π. Ν. Σάκκουλας 2022) σελ. 122-124 και Benutzung „Trojanischer Pferde" und anderer Spionageprogramme (MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a) με περαιτέρω παραπομπή στην εξαιρετικά ενδιαφέρουσα απόφαση BGH, 27 Ιουλίου 2017 − 1 StR 412/16 (LG Kempten) για την ποινική ευθύνη της παράνομης εξόρυξης Bitcoin με χρήση υπολογιστών τρίτων. (NStZ 2018, 401, beck-online)

[62] Explanatory Report Convention on Cybercrime (ETS No. 185), Nr. 47 «it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned).»

[63] BeckOK StGB/Weidemann, 58. Ed. 1.8.2023, StGB § 202a Rn. 20 (B. Objektiver Tatbestand (Rn. 3-11)-V. Unbefugt (Rn. 11) Το αυτό παράδειγμα ανευρίσκουμε στην Αιτιολογική Σκέψη του 41ου Τροποποιητικού Νόμου με τον οποίο αναδιατυπώθηκε η παρ. 202a γερμΠΚ, Drucksache 16/3656, σελ.10 (https://dserver.bundestag.de/btd/16/036/1603656.pdf) accessed 20 September 2023.

[64] Αυτονοήτως, συγκατάθεση που λαμβάνεται με παραπλάνηση είναι άκυρη, γεγονός που είναι σημαντικό για περιπτώσεις phishing και pharming. Επίσης, η συγκατάθεση του ατόμου στο οποίο αφορούν τα δεδομένα είναι άσχετη εάν δεν είναι εξουσιοδοτημένο να τα διαθέσει. (MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a Rn. 70)

Πολύ ενδιαφέρουσα η ανάλυση Arne Klaas, '"White Hat Hacking" – Αποκάλυψη Τρωτών Σημείων Ασφαλείας Σε Δομές Πληροφορικής Όρια Ποινικής Ευθύνης Για Ηθικές Επιθέσεις Hacking' [2022] Multimedia und Recht 187. (MMR 2022, 187, beck-online)

[65] Explanatory Report Convention on Cybercrime (ETS No. 185), Nr. 47 « Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."»

Η ιδιοκτησία του μέσου αποθήκευσης των δεδομένων ή το γεγονός ότι τα δεδομένα σχετίζονται με τον ίδιο τον δράστη δεν συνεπάγεται άνευ ετέρου ότι υφίσταται και η αντίστοιχη εξουσία διάθεσης.[66]

Η παραβίαση του παρόντος άρθρου προϋποθέτει γενικά ότι ο κατηγορούμενος πράγματι απέκτησε πρόσβαση σε υπολογιστή χωρίς ή καθ' υπέρβαση τυχόν εξουσιοδότησης.

3.3.1.4.3. Περίπτωση υπέρβασης εξουσιοδότησης

Ο όρος της υπέρβασης την εξουσιοδοτημένης πρόσβασης, που δεν απαντάται στην αντικειμενική υπόσταση του άρθρου 370Β ΠΚ, σημαίνει μεν πρόσβαση σε υπολογιστή με εξουσιοδότηση ωστόσο αξιοποίηση αυτής της πρόσβασης για να αποκτήσει (ή να τροποποιήσει και τότε πληρούται η αντικειμενική υπόσταση του 379) ο δράστης πληροφορίες στον υπολογιστή που εκείνος δεν έχει το δικαίωμα να αποκτήσει ή να τροποποιήσει.[67]

Εάν κάποιος έχει δικαίωμα να έχει πρόσβαση σε ένα πληροφοριακό σύστημα, αλλά υπερβεί αυτό του το δικαίωμα πληροί τις προϋποθέσεις και συνεπώς καθίσταται ποινικά υπόλογος για την παραβίαση του άρθρου 370Β ΠΚ; [68]

Στο σημείο αυτό να εξετάσουμε την ακόλουθη υπόθεση.

Ο πρώην αρχιφύλακας της αστυνομίας της Τζόρτζια (State of Georgia) Νέιθαν Βαν Μπούρεν χρησιμοποίησε τον υπολογιστή του περιπολικού του για να αποκτήσει πρόσβαση σε μια βάση δεδομένων των αρχών επιβολής του νόμου για να ανακτήσει πληροφορίες για έναν συγκεκριμένο αριθμό πινακίδων κυκλοφορίας με αντάλλαγμα χρήματα.

Ο Βαν Μπούρεν χρησιμοποίησε μεν τα δικά του, έγκυρα διαπιστευτήρια για να εκτελέσει την την έρευνα, η συμπεριφορά του παραβίασε όμως την πολιτική του τμήματος κατά της απόκτησης πληροφοριών από τη βάση δεδομένων για σκοπούς που δεν αφορούν την επιβολή του νόμου.

Ο Νόμος περί απάτης και κατάχρησης υπολογιστών του 1986 ή άλλως CFAA (Computer Fraud and Abuse Act of 1986) υποβάλλει σε ποινική και αστική ευθύνη οποιονδήποτε "αποκτά σκόπιμα πρόσβαση σε υπολογιστή χωρίς εξουσιοδότηση ή υπερβαίνει την εξουσιοδοτημένη πρόσβαση" σύμφωνα με το άρθρο 18 U.S.C. § 1030(α)(2).

Εδώ και δεκαετίες, τα δικαστήρια διχάζονταν ως προς το αν ο CFAA απαγορεύει επίσης την πρόσβαση σε συστήματα ή αρχεία υπολογιστών με άδεια αλλά για απαγορευμένο λόγο. Μήπως ένας εργαζόμενος "υπερβαίνει[] την εξουσιοδοτημένη πρόσβαση" κατεβάζοντας, για

---

[66] BeckOK StGB/Weidemann, 58th Ed. 1 Αυγούστου 2023, StGB § 202a Rn. 8-11.3

[67] Σύμφωνα με το άρθρο 18 παρ. 2 U.S. Code § 1030 - Απάτη και συναφείς δραστηριότητες σε σχέση με υπολογιστές, στοιχείο της αντικειμενικής υπόστασης συνιστά είτε η πρόσβαση σε υπολογιστή χωρίς εξουσιοδότηση ή καθ' υπέρβαση της εξουσιοδοτημένης πρόσβασης «(2)intentionally accesses a computer without authorization or exceeds authorized access, …». Όσον αφορά το δεύτερο όρο η ερμηνεία που δίδεται είναι η ακόλουθη: « The term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;». The Department of Justice has published its own manual on "Prosecuting Computer Crimes" which is available at the following link, page 11: https://www.justice.gov/criminal/file/442156/download

[68] 19-783 Van Buren v. United States (06/03/2021)

παράδειγμα, υλικό στο οποίο ο εργαζόμενος επιτρέπεται να έχει πρόσβαση για την εργασία του, αλλά με την πρόθεση να παραιτηθεί και να μεταφέρει το υλικό αυτό σε άλλον εργοδότη;

Τα γεγονότα του Van Buren αποτελούν ένα τρανταχτό παράδειγμα. Σε έναν αστυνομικό, στον Nathan Van Buren, προσφέρθηκαν 5.000 δολάρια για να ελέγξει αν κάποιος ήταν μυστικός αστυνομικός χρησιμοποιώντας τον αριθμό κυκλοφορίας. Ο Van Buren αναζήτησε τον αριθμό σε μια βάση δεδομένων πινακίδων στην οποία είχε πρόσβαση, αλλά μόνο για νόμιμους σκοπούς επιβολής του νόμου.

Το Δικαστήριο βασίστηκε κυρίως στο γράμμα του νόμου, ιδίως στον χωρίο "υπερβαίνει την εξουσιοδοτημένη πρόσβαση", για να καταλήξει στο συμπέρασμα ότι ο Van Buren είχε "δικαίωμα" να αποκτήσει το υλικό που απέκτησε και με τον τρόπο που το απέκτησε. Το γεγονός ότι απέκτησε πρόσβαση στο υλικό για αθέμιτο σκοπό δεν άλλαξε την ανάλυση του κειμένου.

Η απόφαση στην υπόθεση Van Buren είναι αξιοσημείωτη επειδή περιορίζει το πεδίο εφαρμογής της CFAA για την αναγνώριση ποινική ευθύνης.[69]

3.3.1.5. Υπέρβαση μέτρου προστασίας

Η περιγραφείσα πράξη προσβολής πρέπει να τελείται με τον συγκεκριμένο τρόπο που απαιτεί ο νόμος, ήτοι με την «παραβίαση μέτρων προστασίας» που έχει λάβει ο νόμιμος δικαιούχος του πληροφοριακού συστήματος ή των ηλεκτρονικών δεδομένων.

Η εν λόγω ασφάλεια πρέπει να έχει ως σκοπό την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στα προστατευόμενα δεδομένα ή τουλάχιστον να τη δυσκολεύει σημαντικά. Η προστασία που επιτυγχάνεται δεν χρειάζεται να είναι ανυπέρβλητη. Από την άλλη πλευρά, δεν πρέπει να είναι υπέρμετρα εύκολο για έναν εισβολέα να διαρρήξει την ασφάλεια.[70]

Από αυτό μπορεί να συναχθεί ότι η προστασία πρόσβασης πρέπει να είναι κατάλληλη για να προσφέρει ένα πραγματικό εμπόδιο στις διαδικασίες που αναμένονται βάσει της εμπειρίας ζωής. [71]

Επί τη βάσει των ανωτέρων συνάγεται ότι δεν εμπίπτει στο εφαρμοστικό πεδίο της διάταξης του άρθρου 370Β ΠΚ η είσοδος σε ένα ανοικτό ιδιωτικό ασύρματο δίκτυο (Wifi, Wlan) με σκοπό μέσω αυτού την πλοήγηση στο διαδίκτυο (Schwarz-surfen).[72]

---

[69] Υπόθεση Van Buren v. United States, 141 S. Ct. 1648 (2021)
'Van Buren v. United States, 141 S. Ct. 1648 | Casetext Search + Citator' <https://casetext.com/case/van-buren-v-united-states-5> accessed 21 September 2023.

[70] MüKoStGB/Graf, 4η έκδοση 2021, StGB § 202a Rn. 39-53, καθώς και Αιτιολογική Σκέψη του 41ου Τροποποιητικού Νόμου με τον οποίο αναδιατυπώθηκε η παρ. 202a γερμΠΚ, Drucksache 16/3656, σελ.10 (https://dserver.bundestag.de/btd/16/036/1603656.pdf) accessed 20 September.

[71] *BGH, 21ης Ιουλίου 2015 - 1 StR 16/15 - Δημιουργία Bitcoin* [2015] BGH 1 StR 16/15, 2015 NJW 3463. «Der erreichte Schutz muss also kein unüberwindbarer sein; andererseits darf die Durchbrechung der Sicherung einem Angreifer auch nicht ohne Weiteres möglich sein (BT-Drs. 16/3656, 10). Daraus lässt sich ableiten, dass die Zugangssicherung geeignet sein muss, bei den nach der Lebenserfahrung zu erwartenden Vorgehensweisen ein tatsächliches Hindernis zu bieten»

[72] Zur Straflosigkeit des sogenannten »Schwarz-Surfens« Anmerkung zu LG Wuppertal ZUM 2011, 190 Von Frank Michael Höfinger*, Köln (ZUM 2011, 212, beck-online) Η απόφαση αφορά στην ποινική αξιολόγηση του λεγόμενου «μαύρου σέρφινγκ». Αυτό περιλαμβάνει μη εξουσιοδοτημένη κλήση σε ένα «ανοιχτό» ασύρματο δίκτυο (WLAN – Ασύρματο τοπικό δίκτυο). Εν προκειμένω, ο κατηγορούμενος

Οι συσκευές που προορίζονται αποκλειστικά για τη διατήρηση αποδεικτικών στοιχείων (π.χ. βιντεοκάμερες, συσκευές εγγραφής ή δημιουργία πρωτοκόλλων πρόσβασης/αρχείων καταγραφής) δεν συνιστούν καμία ειδική ασφάλεια για την προστασία πρόσβασης.[73] Η ειδική ασφάλεια πρόσβασης μπορεί να επιτευχθεί τόσο μέσω φυσικών προστατευτικών μέτρων (κλειδαριές, σφράγιση) όσο και μέσω τεχνικών, εγγενών μέτρων ασφαλείας του συστήματος σε επίπεδο υλικού ή λογισμικού προφυλάξεων όπως κρυπτογράφηση, κωδικός πρόσβασης, τείχος προστασίας...[74]

Η έννοια της διασφάλισης της πρόσβασης περιλαμβάνει, ειδικότερα, προγράμματα προστασίας που δεν μπορούν να ξεπεραστούν χωρίς εξειδικευμένες γνώσεις και επομένως αναγκάζουν τον δράστη να έχει πρόσβαση σε κάτι που το εξουσιοδοτημένο άτομο ήθελε σαφώς να αποτρέψει (BGH NJW 2015, 3463) . [75]

Με γνώμονα συνεπώς το συμπέρασμα ότι η υπέρβαση της προστασίας πρόσβασης πρέπει να απαιτεί διόλου ασήμαντο χρόνο ή τεχνική προσπάθεια, για αυτό δεν απαξιολογούνται ποινικά περιπτώσεις στις οποίες η παραβίαση της προστασίας είναι εύκολα δυνατή. Ως υπέρβαση, όπως έχει αναλυθεί ανωτέρω, νοείται η ενέργεια που είναι ικανή να απενεργοποιήσει ή να παρακάμψει την αντίστοιχη διάταξη ασφαλείας (πρβλ. Fischer, ό.π. παρ. 11α). Ωστόσο εάν η προστασία πρόσβασης παρακαμφθεί γρήγορα και χωρίς ιδιαίτερη προσπάθεια λόγω ειδικών γνώσεων, δεξιοτήτων ή δυνατοτήτων, ο όρος της παράβασης των μέτρων προστασίας πληρούται, διότι το νομικά κρίσιμο δεν συνίσταται στο εάν η προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση μπορεί να υπερκεραστεί γρήγορα ή αργά, με μεγάλη ή μικρή προσπάθεια.[76]

Η ύπαρξη προστασίας πρόσβασης πρέπει να βασίζεται στη γενική προστασία των δεδομένων από την πρόσβαση μη εξουσιοδοτημένων προσώπων και όχι στο αν οι εμπειρογνώμονες ή οι εμπειρογνώμονες μπορούν εύκολα να έχουν πρόσβαση στα δεδομένα. [77]

Προϋποτίθεται ότι έχουν ληφθεί μέτρα που είναι αντικειμενικά κατάλληλα και, σύμφωνα με τη βούληση του εξουσιοδοτημένου μέρους και έχουν σκοπό να εμποδίσουν την πρόσβαση στα δεδομένα. Η εν λόγω απαίτηση υπέρβασης μέτρων προστασίας λειτουργεί ως έμπρακτη

δεν παρεισέφρησε σε δεδομένα ειδικά προστατευμένα από μη εξουσιοδοτημένη πρόσβαση στο ξένο δίκτυο δεδομένων (§ 202 α παράγρ. 1 StGB), αλλά απλώς χρησιμοποίησε τη σύνδεση στο Διαδίκτυο που άνοιξε μέσω αυτού του WLAN για να εξοικονομήσει τα έξοδα της πρόσβασης στο Διαδίκτυο.

[73] MüKoStGB/Graf, 4η έκδοση 2021, StGB § 202a Rn. 39-53

[74] BeckOK StGB/Weidemann, 58th Ed. 1 Αυγούστου 2023, StGB § 202a Rn. 12-16.1

[75] StGB § 202a κατασκοπεία δεδομένων Kargl Kindhäuser/Neumann/Paeffgen/Saliger, Ποινικός Κώδικας, 6η έκδοση, 2023 (Unter den Begriff der Zugangssicherung fallen insbesondere Schutzprogramme, die nicht ohne fachliche Kenntnisse überwunden werden können und daher den Täter zu einem Zugriff zwingen, den der Verfügungsberechtigte erkennbar verhindern wollte BGH NJW 2015, 3463)

[76] BGH, 5 StR 614/19BGH : Παράνομη πρόσβαση σε γραμματοκιβώτια από διαχειριστές συστήματος, NStZ-RR 2020, 278

[77] βλ. *Valerius,* στο: *Graf/Jäger/Wittig,* WirtschaftsStrR, 2nd ed. , § 202 a StGB Rn 26, όπου επίσης ορίζεται ότι δεν είναι απαραίτητο η ασφάλεια να είναι αποτελεσματική έναντι του δράστη.

εξωτερίκευση της βούλησης του δικαιούχου να παραμείνουν μυστικά απέναντι στους τρίτους το περιεχόμενο των ψηφιακών δεδομένων. [78]

Οι ως άνω επισημάνσεις αφορούν στην παράγραφο 1 του άρθρου 370Β ΠΚ, όπου ο νομοθέτης διαπλάθει ένα κοινό έγκλημα. Για την παράγραφο 2, το ως άνω μέτρο προστασίας συνίσταται στην απαίτηση του νομοθέτη για ρητή και έγγραφη απαγόρευση πρόσβασης του δράστη βάσει εσωτερικού κανονισμού ή έγγραφης απόφασης του κατόχου ή αρμόδιου υπαλλήλου, με την οποία εξωτερικεύεται η βούληση του δικαιούχου για αποκλεισμού του υπαλλήλου από τη διαχείριση του συστήματος και των δεδομένων.

3.4. Λόγοι άρσης του αδίκου

Ισχύουν οι γενικές διατάξεις του γενικού μέρους. Στα πλαίσια του γερμ ΠΚ εφαρμογής τυγχάνουν οι διατάξεις των άρθρων 100α και 100β του Κώδικα Ποινικής Δικονομίας μπορούν να θεωρηθούν ως δικαιολογία για τα όργανα επιβολής του νόμου. [79]

3.5. Υποκειμενική υπόσταση

Η απαιτούμενη μορφή υπαιτιότητας του δράστη, με γνώμονα το γεγονός ότι ελλείπει ειδική νομοθετική αναφορά, βάσει των άρθρων 18 ΠΚ (όπου διχοτομούνται τα αδικήματα σε κακουργήματα και πλημμελήματα βάσει της αφηρημένα απειλούμενης στο νόμο ποινής) και 26 ΠΚ συνάγεται ότι συνίσταται στο δόλο (27 παρ. 1 ΠΚ), αρκούντος και του ενδεχόμενου, που πρέπει να επικαλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.[80] Συγκεκριμένα ο δράστης πρέπει να γνωρίζει (wissen) και να θέλει (wollen) να πραγματώσει όλα τα στοιχεία της αντικειμενικής υπόστασης, ήγουν να αποκτήσει πρόσβαση σε πληροφοριακό σύστημα ή σε ηλεκτρονικά δεδομένα του δικαιούχου καθ' υπέρβαση μέτρων προστασίας και χωρίς δικαίωμα.

Όσον αφορά στην παράγραφο 2, όπου ποινικά αξιόμεμπτη συμπεριφορά του δράστη θεμελιώνεται στη ρητή απαγόρευση κανονισμού ή απόφασης του δικαιούχου ή ενός εξουσιοδοτημένου υπαλλήλου του, όπου ο δράστης πρέπει να γνωρίζει και να θέλει να εισβάλλει στο σύστημα και στα δεδομένα του δικαιούχου-εργοδότη του, έχοντας τουλάχιστον ενδεχόμενο δόλο για την απαγόρευση αυτή.

3.6. Διακεκριμένες παραλλαγές του βασικού αδικήματος

Στην παράγραφο 3 του άρθρου 370Β ΠΚ διαμορφώνεται από το νομοθέτη απλώς διακεκριμένη παραλλαγή του βασικού αδικήματος της αθέμιτης πρόσβασης (illegal access), με βαρύνον στοιχείο της ποινικής απαξίας τη προσβολή συγκεκριμένων μορφών απορρήτου επισύροντας και αυστηρότερη ποινή φυλάκισης από 10 ημέρες έως 3 έτη ή διαζευκτικά χρηματική ποινή. Η επίταση της ποινικής απαξίας συγκεκριμένα συνίσταται στο γεγονός ότι ο δράστης παρεισφρέοντας στο πληροφοριακό σύστημα ή στα ψηφιακά δεδομένα λαμβάνει γνώση του περιεχομένου των ηλεκτρονικών δεδομένων, τα οποία συνιστούν επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του δημοσίου ή του ιδιωτικού τομέα.

---

[78] Andreas Popp σε Hilgendorf/Kudlich/Valerius, Handbuch des Strafrechts Bd. 4 (C.F. Müller GmbH, Jan 1, 2019), σελ.700 "sondern darf zugleich auch als sinnfällige Manifestation des Willens gelten, die gespeicherten oder übermittelten Daten vor nicht zur Kenntnis berufenen anderen Personen geheim zu halten" με τεκμηρίωση από τις Αιτιολογικές Εκθέσεις α)BT-Drs. 10/5058, Σελ. 29, β) 16/3656, Σελ. 10

[79] MAH Strafverteidigung, § 50 Cybercrime und Datenkriminalität Rn. 38, beck-online

[80] Ομοίως και στην αντίστοιχη γερμανική διάταξη απαιτείται τουλάχιστον ενδεχόμενος δόλος, Αρκεί να αντιληφθεί ότι υπάρχει εμπόδιο στην πρόσβαση στα δεδομένα με το οποίο το εξουσιοδοτημένο μέρος ήθελε να προστατεύσει τα δεδομένα. (MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a Rn. 80)

Συγκεκριμένα πρόκειται για τη χωρίς δικαίωμα και κατά παράβαση μέτρου προστασίας απόκτησης πρόσβασης σε μέρος ή στο σύνολο συστήματος πληροφοριών ή σε ηλεκτρονικά δεδομένα που αναφέρονται σε επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα.[81]

Ως επιστημονικά απόρρητα νοούνται εκείνες που συνιστούν συστηματικές γνώσεις, αναγόμενες σε κάποιο γνωστικό αντικείμενο και τα οποία πρέπει να παραμείνουν μυστικά. Ως επιχειρηματικά απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα αποτελούν όλα εκείνα τα στοιχεία, όπως οικονομικές συναλλαγές, πελατολόγιο, αντικείμενο εργασιών της, που ο δικαιούχος κρίνει ως απόρρητα και συνεπώς δεν επιθυμεί τη γνωστοποίηση σε τρίτους και δη ανταγωνιστές. [82]

Σκοπός του άρθρου 370Β ΠΚ συνιστά η διαφύλαξη του απορρήτου με τη μορφή του στοιχείου ή προγράμματος ηλεκτρονικού υπολογιστή, ενώ με το άρθρο 370Γ ΠΚ η προστασία κάθε άλλου στοιχείου ή προγράμματος Η/Υ.[83]

Στη τέταρτη παράγραφο του υπό εξέταση άρθρου, τυποποιούνται δύο ιδιαιτέρως διακεκριμένες παραλλαγές του βασικού εγκλήματος της αθέμιτης πρόσβασης. Στην προκειμένη περίπτωση ο ιθύνων λόγος επίτασης της ποινής συνίσταται είτε στην ιδιαίτερη ιδιότητα του δράστη, που ευρίσκεται στην υπηρεσία του νόμιμου κατόχου των στοιχείων και καταχράται την ιδιότητά του αυτή είτε στην ιδιαίτερα μεγάλη οικονομική αξία του απορρήτου των παραβιαζόμενων ψηφιακών δεδομένων, συμπροσβάλλοντας κατ' αποτέλεσμα και το έννομο αγαθό της περιουσίας και αξιολογούμενη η ιδιαίτερη οικονομική αξία σε συνάρτηση με τα έννομα αγαθά του παθόντος. [84] Η ποινική κύρωση που επισύρει η πλήρωση των όρων της εν λόγω παραγράφου είναι φυλάκιση από 10 ημέρες έως 5 έτη και σωρευτικά χρηματική ποινή.

3.7. Ποινικές κυρώσεις

Για το βασικό αδίκημα της παράνομης πρόσβασης σε σύστημα πληροφοριών ή σε δεδομένα, που τυποποιείται στην παράγραφο 1 του άρθρου 370Β ΠΚ, απειλείται ποινή φυλάκισης με μέγιστο όριο απειλούμενης ποινής τα δύο έτη ή διαζευκτικά χρηματική ποινή. Στην απλώς διακεκριμένη παραλλαγή της παραγράφου 3 του εν λόγω άρθρου, το μέγιστο της απειλούμενης ποινής διαμορφώνεται στα 3 έτη, επιλογή που κρίνεται δικαιολογημένη καθώς συμπροστατεύονται τα επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα.

Αξιοσημείωτο να παρατηρήσουμε το γεγονός ότι ο νομοθέτης επέλεξε να κρίνει ατιμώρητες τις ιδιαίτερα ελαφρές περιπτώσεις αθέμιτης πρόσβασης σε σύστημα πληροφοριών ή σε ηλεκτρονικά δεδομένα. Τέτοια δυνατότητα άλλωστε παρέχετε και από το άρθρο 3 της Οδηγίας 2013/40/ΕΕ, όπου ορίζεται ότι για ήσσονος σημασίας περιπτώσεις δεν απαιτείται η λήψη ποινικών μέτρων από μέρους του εκάστου κράτους. Ως ιδιαίτερα ελαφρές περιπτώσεις

[81] Για το ιδιωτικό απόρρητο χρήσιμη η ερμηνεία στα πλαίσια του 371 ΠΚ, ενώ για το δημόσιο του άρθρου 252 αρ. 4 ΠΚ.

[82] Βλ. Καμπέρου Ελ., σε Χαραλαμπάκη σελ. 2741, καθώς και Μ. Μαργαρίτης – Άντα Μαργαρίτη, ό.π., σελ. 1084

[83] Μαργαρίτης and Μαργαρίτη (n 23). Σελ. 1084 με περαιτέρω παραπομπή για τεκμηρίωση στην απόφαση ΑΠ 121/2003 (το οποίο αφορά στο προϊσχύον άρθρο 370Β που πλέον μετετέθη στο 370 Γ).

[84]Κωνσταντινίδης, Η διακεκριμένη παραβίαση απορρήτων στοιχείων, ΠΧρ. 1997, σελ. 1216 επ. και Καϊάφα – Γκμπάντι, Παρατηρήσεις στην ΕφΑθ 217/1997, Υπερ 1997, σελ. 850

νοούνται εκείνες, στις οποίες η χωρίς δικαίωμα πρόσβαση του δράστη ενέχει ασήμαντη ηθικοκοινωνική απαξία, όπως επί παραδείγματι πράξεις κυβερνοακτιβισμού που τελούνται για πολιτικούς ή συμβολικούς λόγους.Βάσει του γράμματος του νόμου η πράξη μένει ατιμώρητη. Η διατύπωση αυτή συνεπάγεται ότι η αντικειμενική και η υποκειμενική υπόσταση πληρούται, ωστόσο δεν επιβάλλεται ποινή (άρθρο 14 ΠΚ). Υποστηρίζεται ότι πρόκειται για δυνητικό λόγο δικαστικής άφεσης της ποινής (104Β ΠΚ), καθώς η μη επιβολή της εξαρτάται από το εάν το δικαστήριο κρίνει την υπόθεση ως ιδιαίτερα ελαφρά.[85] Ωστόσο η αδιάστικτη γραμματική διατύπωση της διατάξεως τυποποιεί υποχρεωτικό λόγο απαλλαγής από την ποινή.

Βάσει της τελευταίας παραγράφου, απαιτείται για την ποινική δίωξη προηγούμενη έγκληση του παθόντος, δηλαδή του δικαιούχου διαχείρισης του πληροφοριακού συστήματος ή/και των ψηφιακών δεδομένων, τόσο για το βασικό αδίκημα της παραγράφου 1, όσο και για τις ιδιαιτέρως διακεκριμένες παραλλαγές της παραγράφου 4. Συμπερασματικά συνάγουμε ότι για την απλώς διακεκριμένη παραλλαγή της παραγράφου 3 η ποινική δίωξη κινείται αυτεπαγγέλτως.

3.8. Ειδικές μορφές εμφάνισης του εγκλήματος

3.8.1. Απόπειρα

Το άρθρο 11 παράγραφος 2 της Σύμβασης της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο, αλλά και το αντίστοιχο άρθρο 8 παράγραφος 2 της Οδηγίας 2013/40/ΕΕ δεν επέτασσε την ποινικοποίηση της απόπειρας.[86]

Στην ελληνική Ποινική Νομολογία, έχει επικρατήσει η ουσιαστική-αντικειμενική θεωρία, η οποία αποκρυσταλλώθηκε με την ΑΠ 285/1965 και ορίζει: Πράξη που στοιχειοθετεί αρχή εκτέλεσης εγκλήματος συγκροτεί α) είτε πράξη που συνιστά τυποποιημένο στο νόμο στοιχείο της αντικειμενικής υπόστασης ή β) αναγκαίο οργανικό και λειτουργικό τμήμα της πράξης αντικειμενικής υπόστασης, ώστε να οδηγεί σε πραγμάτωσή της, αν δεν ανακοπεί άμεσα. Όσον αφορά τον πυρήνα (το α΄) ουδεμία αντίρρησις εγείρεται, η θεωρητική διαμάχη, που αναζωπυρώθηκε με τον νΠΚ, αφορά την <<περιφέρεια>> (το β΄).

Επί της ουσίας και παρά το γράμμα του 42, ο νέος Ποινικός κώδικας, δεν ενστερνίστηκε την τυπική αντικειμενική θεωρία, διότι για τα άτυπα εγκλήματα στην αιτιολογική έκθεση (που συνιστά αυθεντική ερμηνευτική πηγή) εξακολουθεί να εντάσσει την <<περιφέρεια>>, [87]προκειμένου να ορίσει την αρχή εκτελέσης.

Εξίσου υποστηριζόμενη είναι και η θεωρία της εντύπωσης, βάσει της οποίας στοιχειοθετείται αρχή εκτέλεσης του εγκλήματος, όταν ήδη δημιουργείται αντικειμενικά η εντύπωση διατάραξης της ειρήνευσης του εννόμου αγαθού, με αποτέλεσμα να κλονίζεται η

[85] Ελένη Καμπέρου σε Αριστοτέλης Χαραλαμπάκης and Ελένη Καμπέρου (eds), Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2743

[86] Explanatory Report Convention on Cybercrime (ETS No. 185), Nr. 120 « …, απαιτείται η ποινικοποίηση της απόπειρας μόνο όσον αφορά τα αδικήματα που θεσπίζονται σύμφωνα με τα άρθρα 3, 4, 5, 7, 8, 9 παράγραφος 1 στοιχείο α και 9 παράγραφος 1 στοιχείο γ», ενώ το αδίκημα της παράνομης πρόσβασης προβλέπεται στο άρθρο 2. Ομοίως και στην Οδηγία «Τα κράτη μέλη εξασφαλίζουν ότι η απόπειρα διάπραξης αδικήματος που αναφέρεται στα άρθρα 4 και 5 να τιμωρείται ως ποινικό αδίκημα», ενώ η παράνομη πρόσβαση σε συστήματα πληροφοριών προβλέπεται στο άρθρο 3.

[87] Από Νομολογία ενδεικτική η υπ΄αριθμόν 441/2020 που ορίζει << από τη διάταξη αυτή, (42 παρ. 1 ν ΠΚ), με τη νέα της διατύπωση δεν υπάρχει ουσιώδης μεταβολή ως προς την ερμηνεία του όρου της αρχής της εκτέλεσης...>>

εμπιστοσύνη του κοινωνικού συνόλου στην ισχύ της εννόμου τάξεως, πλήττοντας το αίσθημα της ασφάλειας του δικαίου. [88]

Ως παράδειγμα αρχής εκτέλεσης του αδικήματος μπορούμε να εισφέρουμε την περίπτωση της εισαγωγής του αναγνωριστικού (password). [89]

3.8.2. Συμμετοχή

Αναφορικά με την ποινική ευθύνη του παρόχου υπηρεσιών πρόσβασης στον παγκόσμιο ιστό (access provider), ο οποίος προβαίνει σε χωρίς δικαίωμα διάθεση της διαδικτυακής διεύθυνσης (IP-address) του χρήστη σε τρίτο πρόσωπο, προκειμένου να αποκτήσει αθέμιτη πρόσβαση στο σύστημα και στα δεδομένα του παθόντος, μπορεί να καταφαθεί συμμετοχική με τη στενή έννοια ποινική ευθύνη του. Συγκεκριμένα, η συμπεριφορά του θα απαξιολογηθεί στα πλαίσια του άρθρου 47 ΠΚ, όπου προβλέπεται η συνέργεια ως μορφή συμμετοχής, και η ποινική του ευθύνη εξαρτάται από τη μορφή της συνδρομής που παρέσχε, εφόσον φυσικά συντρέχει και ο διπλός συμμετοχικός δόλος (Doppelter Gehilfenvorsatz).

Της ίδιας ποινικής μεταχείρισης τυγχάνει και ένας «χάκερ γκρι καπέλου» (gray-hat hacker) ή ένας ερευνητής πληροφορικής ασφάλειας, που αντί να ενημερώσει το δικαιούχο του πληροφοριακού συστήματος ή των ψηφιακών δεδομένων τουναντίον «πωλεί» τις πληροφορίες σχετικά με τα «αδύναμα σημεία» (weak points) που ανακάλυψε σε «χάκερς μαύρου καπέλου» (black-hat).

Ομοίως, ο κατασκευαστής υλισμικού/λογισμικού (IT- producer), ο οποίος διαθέτει στο δράστη το κλειδί αποκρυπτογράφησης για τη δυνατότητα πρόσβασης, χωρίς τη συγκατάθεση του δικαιούχου διαχείρισης, ευθύνεται ποινικά εφόσον έχει τον απαιτούμενο δόλο.

3.8.3. Συρροές

Μέσω της ποινικοποίησης της παράνομης πρόσβασης ορίζεται ότι αντιμετωπίζονται βασικές επιθέσεις κατά της ασφάλειας συστημάτων πληροφορικής και ηλεκτρονικών δεδομένων. [90]

Ωστόσο αυτό επ' ουδενί λόγω δεν συνεπάγεται ότι το αδίκημα του άρθρου 370Β ΠΚ συνιστά το βασικό έγκλημα κατά του εννόμου αγαθού της ασφάλειας συστημάτων πληροφορικής και ηλεκτρονικών δεδομένων, καθώς οι υπόλοιπες εγκληματικές συμπεριφορές κατά της ασφάλειας δεν εμπεριέχουν όλα απαραιτήτως το στοιχείο της αθέμιτης πρόσβασης, ώστε να θεωρηθούν εγκληματικές παραλλαγές του. Τωόντι, τόσο η πράξη της υποκλοπής, όσο και η πράξη της παρεμβολής αποτελούν διακριτές συμπεριφορές έναντι της πρόσβασης (access), την οποία δεν προαπαιτούν οπωσδήποτε.

Το άρθρο 370Β ΠΚ εντάσσεται σε ένα κανονιστικό πλέγμα με το οποίο προστατεύεται το ίδιο έννομο αγαθό, ήτοι η ασφάλεια των πληροφοριακών συστημάτων και δεδομένων,

---

[88] Αλέξανδρος Κωστάρας, *ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ Έννοιες και Θεσμοί του Γενικού Μέρους* (3η, Νομική Βιβλιοθήκη 2019) σελ. 488.

[89] Βασιλάκη (n 11) σελ. 88.

[90] Βάσει της σκέψης 44 της Αιτιολογικής Έκθεσης της Βουδαπέστης, όπου αναφέρει επί λέξει: «Η "παράνομη πρόσβαση" καλύπτει το βασικό αδίκημα των επικίνδυνων απειλών και επιθέσεων κατά της ασφάλειας (δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας) των συστημάτων υπολογιστών και των δεδομένων.»

συγκεκριμενοποιούμενο ωστόσο στην προστασία του δικαιώματος διαχείρισης το συστήματος και τω δεδομένων.

Τούτου δοθέντος, το έγκλημα της αθέμιτης πρόσβασης συρρέει φαινομενικά με τα εγκλήματα που περιγράφονται στις διατάξεις των άρθρων 292Β, 370Ε αλλά και 292Γ ΠΚ λόγω της ταυτότητας του προσβαλλομένου εννόμου αγαθού.

Μεταξύ των αδικημάτων των άρθρων 370Β και 370Ε υφίσταται φαινομενική πραγματική συρροή στις περιπτώσεις στις οποίες ο δράστης εισέρχεται χωρίς δικαίωμα στο σύστημα του παθόντος εγκαθιστώντας παράλληλα κατασκοπευτικό λογισμικό (π.χ. sniffer-programm, keylogger), μέσω του οποίου βαθαίνει η εγκληματική δράση προβαίνοντας εν συνεχεία σε υποκλοπή, δηλαδή χωρίς δικαίωμα ακρόαση ή και καταγραφή των μη δημόσια μεταδιδόμενων δεδομένων (π.χ. δεδομένων επικοινωνίας μέσω viber, ή διαμοιρασμό αρχείων μέσω dropbox) ή «παγίδευση» των ηλεκτρομαγνητικών εκπομπών του συστήματος.

4. Το αδίκημα της παραβίασης απορρήτων σχετιζομένων με ηλεκτρονικό υπολογιστή (370Γ ΠΚ)

Παραβίαση απορρήτων σχετιζόμενη με η/υ (άρθρο 370Γ ΠΚ)

Στο παρόν άρθρο 370Γ του νέου ΠΚ έχει ενταχθεί το έγκλημα που τυποποιείτο μέχρι πρότινος στο προϊσχύσαν άρθρο 370Β. Τιμωρείται όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα. Επίσης διευκρινίζεται το περιεχόμενο της έννοιας των απορρήτων (εδ. β' παρ. 1) και αυξάνεται η ποινή όταν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων και το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής αξίας (παρ. 2). [91] Πέρα από τις διατάξεις του δικαίου που προστατεύουν τα εμπορικά και βιομηχανικά απόρρητα (βλ. φέρ' ειπείν Νόμο 146/1914, περί αθεμίτου ανταγωνισμού), ειδικά όσον αφορά τα απόρρητα που σχετίζονται με η/υ προβλέπεται ειδική προστασία στο άρθρο 370Γ ΠΚ.

Η νομοτυπική υπόσταση του αδικήματος του άρθρου 370Γ ΠΚ διαπλάσσεται ως ακολούθως:

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Οι πράξεις που προβλέπονται στο άρθρο αυτό διώκονται με έγκληση.

4.1. Προστατευόμενο έννομο αγαθό

Κατά μια άποψη, το προστατευόμενο έννομο αγαθό εξειδικεύεται στην τυπική εξουσία διάθεσης εκείνου, ο οποίος ως «κύριος των στοιχείων», δηλαδή δυνάμει του δικαιώματός του στο πνευματικό περιεχόμενο και ανεξάρτητα από περιουσιακές σχέσεις του φορέα του στοιχείου, να ορίζει σε ποιον μπορούν να γίνουν προσιτά. [92]

Κατά την κρατούσα άποψη, στο άρθρο 370Γ ΠΚ προστατεύεται το απόρρητο, που έχει τη μορφή στοιχείου ή προγράμματος ηλεκτρονικού υπολογιστή, υπό την προϋπόθεση ότι είναι κρατικό, επιστημονικό, επαγγελματικό απόρρητο ή απόρρητο επιχείρησης του δημοσίου ή του ιδιωτικού τομέα. [93]

---

[91] Κ. Φράγκος, Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 370Γ, αρ. 1, Ενημέρωση:10/12/2019, sakkoulas-online

[92] Π. Φιλόπουλος, Ποινική Προστασία Απορρήτου, 2015, άρθ. 370Β, σ. 145, αρ. 7 = sakkoulas-online

[93] ΤρΠλημΑθ 2484/2019 ΠοινΔικ, 5/2020, σελ. 461 – 462 (ΤΝΠ QUALEX), ΠλημΚαλαμ 127/2016 ΠΧρ 2016 σελ. 387, ΣυμβΑΠ 1294/2007 ΠραξΛογΠΔ 2007 σελ. 333, ΑΠ 121/2003 ΠοινΔικ, 6/2003, σελ. 619 – 620 (παρατ. Γ. Νούσκαλης), Α. Ζήσης, Από τον πολιτικώς ενάγοντα στον παριστάμενο για την υποστήριξη της κατηγορίας, 2023, σ. 213-216, υποσ. 391 = sakkoulas-online. Από τη θεωρία ομοίως

Έχει υποστηριχθεί ότι εφόσον το απόρρητο έχει οικονομική αξία, προστατεύεται και το έννομο αγαθό της περιουσίας. [94] Ωστόσο η διάταξη του άρθρου δεν αναφέρει ως απαραίτητο στοιχείο την οικονομική αξία των προστατευόμενων απορρήτων και συνακόλουθα αποσυνδέει τα απόρρητα από την περιουσιακή τους ιδιότητα. [95]

4.2. Χαρακτηρολογικά γνωρίσματα του εγκλήματος

Το αδίκημα της παραβίασης απορρήτων σχετιζόμενων με ηλεκτρονικό υπολογιστή συνιστά πλημμέλημα, στιγμιαίο και βλάβης[96]. Στην παράγραφο 1 διαπλάσσεται ως κοινό έγκλημα, ενώ στη 2 ως μη γνήσιο ιδιαίτερο, όταν ο δράστης βρίσκεται στην υπηρεσία του κατόχου, λόγω της ιδιαίτερης σχέσης του δράστη με τον κάτοχο των στοιχείων, που λειτουργεί ως επιβαρυντική περίσταση και επαυξάνει το αξιόποινο της πρώτης παραγράφου του κοινού εγκλήματος της διάταξης του 370Γ ΠΚ. [97]

Με την παρούσα διάταξη εισάγεται ένα έγκλημα υπαλλακτικώς μικτό, [98] καθώς οι διάφοροι τρόποι τέλεσης του αδικήματος (αντιγραφή, αποτύπωση, χρησιμοποίηση, αποκάλυψη, παραβίαση) μπορούν να εναλλαχθούν και παρά ταύτα θα τιμωρείται ο δράστης μια φορά.

Ορίζεται ως έγκλημα ενέργειας καταρχήν, ωστόσο δύναται να τελεστεί και με παράλειψη, αν ο δράστης έχει ιδιαίτερη νομική υποχρέωση αποτροπής του αποτελέσματος σύμφωνα με το άρθρο 15 ΠΚ. [99]

4.3. Δομή και στοιχεία του αδικήματος

Στοιχεία του εγκλήματος:

Α. Στην παράγραφο 1 του άρθρου 370Γ ΠΚ μνημονεύονται πέντε τρόποι τέλεσης του αδικήματος (αντιγραφή, αποτύπωση, χρησιμοποίηση, αποκάλυψη και παραβίαση στοιχείων ή προγραμμάτων υπολογιστών), τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα.

4.3.1. Δράστης

Δράστης του αδικήματος μπορεί να είναι ο οιοσδήποτε. Όταν όμως ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, εφαρμόζεται η παράγραφος 2 του άρθρου 370Γ ΠΚ.

Αλέξανδρος Κωστάρας, *ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ – ΕΠΙΤΟΜΗ ΕΙΔΙΚΟΥ ΜΕΡΟΥΣ (Άρθρα 134-410 ΠΚ)* (4η, Νομική Βιβλιοθήκη 2014) 1148.

[94] Άγγελος Κωνσταντινίδης, Η διακεκριμένη παραβίαση απορρήτων στοιχείων (άρ. 370Β παρ. 2 περ. β' ΠΚ), ΠΧΡ 1997, σελ. 1216

[95] Λαμπράκης Χ., σε Χαραλαμπάκη Α., Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, τόμος Β', άρθρα 207-473, σελ. 1722, στα πλαίσια ερμηνεία του παλαιού 370Β ΠΚ

[96] Ενδέχεται όμως το έγκλημα να τελείται και με τρόπο που προσιδιάζει σε διακινδύνευση του εννόμου αγαθού, εφόσον εντάσσεται στην έννοια του «οπωσδήποτε παραβιάζει» Λαπράκης Χ., ό.π.

[97] Κωστάρας, ό.π., σελ. 1146

[98] ΑΠ 1294/2007 «… συντελείται δε η παραβίαση των προγραμμάτων είτε με την αντιγραφή ή την αποτύπωση ή τη χρησιμοποίηση ή την αποκάλυψη σε τρίτο, δηλαδή με υπαλλακτικώς μικτούς τρόπους τέλεσης οι οποίοι εννοιολογικά διαφέρουν» (https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=Z0ZgV0KruNiNdUlNRuIjl8KimOmvod&apof=1294_2007&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%C6), ΠλημΚαλαμ 127/2016, σελ. 387, ΣυμβΕφΑθ 217/1997 Υπερ σελ. 846, ΣυμβΠλημΑθ 4742/2004, ΠοινΔικ 2005, σελ. 407 και Π. Φιλόπουλος, Ποινική Προστασία Απορρήτου, 2015, άρθ. 370Β, σ. 146, αρ. 10 = sakkoulas-online

[99] Καμπέρου, ό.π. σελ. 2746

4.3.2.Αθέμιτα

Η διάταξη του άρθρου 370Β ΠΚ προϋποθέτει ότι η παραβίαση του απορρήτου τελείται αθέμιτα. Αθέμιτα είναι εκείνα τα απόρρητα που αποκτήθηκαν χωρίς δικαίωμα[100] ή χωρίς τη συναίνεση του δικαιούχου, του κατόχου, του πνευματικού ή υλικού ιδιοκτήτη. Συνεπώς, δεν είναι αθέμιτη πράξη όταν έχει δώσει τη ρητή συναίνεσή του ο νόμιμος κάτοχος του στοιχείου του προγράμματος του ηλεκτρονικού υπολογιστή σε τρίτον, για να το αντιγράψει, αποτυπώσει και τα λοιπά. Αν όμως η ρητή συναίνεση αφορά μόνο λόγου χάρη την αντιγραφή ή την αποτύπωση του προγράμματος ή του στοιχείου, αν ο τρίτος το αποκαλύψει σε άλλον, τότε η πράξη του τελείται αθέμιτα, διότι δεν περιλαμβάνεται στη συναίνεση.[101] Ήγουν η συγκατάθεση του νόμιμου κατόχου αποκλείει την αντικειμενική υπόσταση του εγκλήματος.[102] Επίσης, δεν είναι αθέμιτη πράξη όταν έχει τηρηθεί η νόμιμη διαδικασία άρση του απορρήτου.[103]

Η τέλεση της πράξης πραγματοποιείται όταν αντιβαίνει σε διάταξη νόμου, ενώ στην περίπτωση «κοινωνικά πρόσφορων» πράξεων πρέπει να συντρέχουν και άλλα στοιχεία, λ.χ., η εμφάνιση λογισμικού στην οθόνη ή η χρήση του λογισμικού δεν είναι πράξεις αθέμιτες, αλλά αποδοκιμάζονται από το δίκαιο μόνο όταν συντρέχουν και άλλα στοιχεία, π.χ. γίνονται παρά τη θέληση του δικαιούχου. [104]

Νόμιμος κάτοχος του απορρήτου είναι εκείνος ο οποίος, με βάση τον νόμο ή σύμβαση, το έχει στη φυσική του εξουσία και πρέπει να διακρίνεται από τον δικαιούχο του απορρήτου.[105] Επί παραδείγματι, ο γιατρός που έχει την προσωπική καρτέλα του ασθενούς με τα στοιχεία της ασθένειάς του, είναι κάτοχος του απορρήτου, ενώ ο ασθενής είναι ο δικαιούχος.[106] Εύστοχα υποστηρίζεται, πάντως, σε σχέση με τα στοιχεία ή τα προγράμματα ηλεκτρονικών υπολογιστών ότι, εφόσον αυτά δεν είναι ενσώματα, ως κατοχή νοείται η δυνατότητα εξουσίασης των στοιχείων ενός προγράμματος, η οποία συνίσταται στη δυνατότητα προσπέλασης, χρήσης ή διάθεσης των στοιχείων αυτού και στηρίζεται σε ένα νόμιμο δικαίωμα. [107]

Η προστασία που παρέχει το άρθρο 370Β ΠΚ στα απόρρητα προγράμματα ή δεδομένα η/υ είναι ευρύτατη και δεν ελέγχεται εάν ο δράστης ενήργησε με πρόθεση βλάβης ή όχι. Πάντως, η προστασία δεν εκτείνεται στο υλικό η/υ, το οποίο προστατεύεται ενδεχομένως κατά τις διατάξεις περί απορρήτων του νόμου 146/14 περί αθεμίτου ανταγωνισμού.[108] Ακόμα, το

---

[100] Μανωλεδάκης, Ερμηνεία κατ᾽ άρθρο των όρων του ειδικού μέρους του Ποινικού Κώδικα,(Σάκκουλα 1996), σελ. 131

[101] Χ. Λαμπάκη/Ε.Καμπέρου-Νταλτα, ό.π., σελ. 1726 και 2749 αντίστοιχα

[102] Έτσι ΣυμβΕφΑθ 2949/2003, ΠοινΔικ 2004, σελ. 1110

[103] Νόμος 5002/2022 "Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών".

[104] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 412, αρ. 676 = sakkoulas-online

[105] Χ. Λαμπάκη/Ε.Καμπέρου-Νταλτα, ό.π., σελ. 1726 και 2749 αντίστοιχα

[106] Α. Κωστάρα, ό.π., σελ. 1027, Ι. Μανωλεδάκη, ό.π., σελ. 13

[107] Έτσι ΣυμβΕφΑθ 2949/2003, ΠοινΔικ 2004, σελ. 1110 καθώς βλ. και Χ. Λαμπάκη/Ε.Καμπέρου-Νταλτα, ό.π., σελ. 1726 και 2749 αντίστοιχα

[108] Άρθρο 16 του νόμου περί αθεμίτου ανταγωνισμού: «Με φυλάκισιν μέχρις εξ μηνών και με χρηματικήν ποινήν (μέχρι τριών χιλιάδων δραχμών) ή με μίαν των ποινών τούτων τιμωρείται όστις, ως υπάλληλος, εργάτης ή μαθητευόμενος παρά τινι εμπορικώ ή βιομηχανικώ καταστήματι ή επιχειρήσει, ανακοινώνει άνευ δικαιώματος εις τρίτους, κατά το χρονικόν διάστημα της υπηρεσίας του, απόρρητα του καταστήματος ή της επιχειρήσεως εμπεπιστευμένα αυτώ ως εκ της υπηρεσίας του, ή άλλως

άρθρο 370Β ΠΚ εφαρμόζεται ανεξάρτητα εάν το απόρρητο είναι αποθηκευμένο στη μνήμη η/υ. [109]

4.3.3. Η αντιγραφή κ.λπ. στοιχείων ή προγραμμάτων υπολογιστών που συνιστούν απόρρητα (370Γ παρ. 1 ΠΚ)

Η εγκληματική συμπεριφορά πραγματώνεται με την αθέμιτη αντιγραφή, χρησιμοποίηση, αποκάλυψη σε τρίτον ή παραβίαση απόρρητων στοιχείων ή προγραμμάτων η/υ.

Αντιγραφή, δηλαδή αναπαραγωγή, είναι η ενσωμάτωση του στοιχείου ή του προγράμματος σε έναν υλικό φορέα, ακόμα και όταν γίνεται χωρίς τη χρήση τεχνικών μέσων (με σχεδιασμό ή γραφή),[110] αλλά και γενικότερα, η δημιουργία αντιγράφων, η οποία το καθιστά προσιτό στις αισθήσεις άμεσα ή έμμεσα. [111] Η φόρτωση ενός προγράμματος σε έναν εξωτερικό φορέα από την εσωτερική μνήμη του ηλεκτρονικού υπολογιστή θεωρείται αντιγραφή.[112] Από τη Νομολογία έχει κριθεί ως αντιγραφή η ενσωμάτωση σε δισκέτες του πελατολογίου της εταιρείας, το οποίο ήταν καταχωρημένο σε πρόγραμμα ηλεκτρονικού υπολογιστή και αποτελούσε επαγγελματικό απόρρητο. [113] Επιπλέον, αντιγραφή συντρέχει και όταν ο υπάλληλος μεταδίδει, μέσω του ηλεκτρονικού ταχυδρομείου της επιχείρησης που εργάζεται, τα ηλεκτρονικά κατοχυρωμένα στοιχεία που συνιστούν επαγγελματικά απόρρητα της επιχείρησης, στο προσωπικό του email.[114] Οι υλικοί φορείς στους οποίους αντιγράφονται οι πληροφορίες, που είναι αποθηκευμένες στη μνήμη ενός ηλεκτρονικού υπολογιστή, μπορούν να συνιστούν τα «στικάκια» (usb) ή οι δίσκοι τύπου «cd» «dvd». [115]

Αποτύπωση σημαίνει αναπαραγωγή ενός ενσώματου αντιγράφου του προγράμματος ή των δεδομένων από κάποιο προϋπάρχον πρωτότυπο μέσω φωτοτύπησης ή μεταφοράς σε δισκέτα, ή «σκαναρίσματος» του πρωτοτύπου και εκτύπωσης κατόπιν κ.λπ.. [116] Η αποτύπωση συνιστά ένα είδος αντιγραφής. [117] Ως νομολογιακό παράδειγμα εισφέρεται η (αναιρεθείσα, λόγω έλλειψης αιτιολογίας) απόφαση, όπου ο κατηγορούμενος, πρώην διευθυντής λογιστηρίου της εγκαλούσας εταιρείας φέρεται να είχε πρόσβαση στα γραφεία της εταιρείας και να αποτύπωνε εξακολουθητικά και σε μεταγενέστερο της απόλυσής του χρόνο, στοιχεία από το ηλεκτρονικό αρχείο του υπολογιστή αυτής. [118]

περιελθόντα εις την αντίληψίν του, προς τον σκοπόν ανταγωνισμού ή επί τη προθέσει βλάβης του κυρίου του καταστήματος ή της επιχειρήσεως. Με την αυτήν ποινήν τιμωρείται και ο χρησιμοποιών ή ανακοινών εις τρίτους άνευ δικαιώματος, προς τον σκοπόν ανταγωνισμού, τα τοιαύτα απόρρητα, ων έλαβε γνώσιν διά τινός των εν τω προηγουμένω εδαφίω ανακοινώσεων ή δι᾽ ιδίας αυτού πράξεως αντικειμένης εις τους νόμους ή τα χρηστά ήθη.»

[109] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 413, αρ. 676 = sakkoulas-online

[110] Μανωλεδάκης, Ερμηνεία κατ' άρθρον , 1996, σελ. 134

[111] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 412, αρ. 676 = sakkoulas-online

[112] Μυλωνόπουλος, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ. 74

[113] ΑΠ 121/2003 ΣΤ'Τμ. [Αντιγραφή και χρήση προγραμμάτων Η/Υ] (παρατ. Γ. Νούσκαλης), ΠοινΔικ, 6/2003, σελ. 619 – 620, ΤΝΠ QUALEX

[114] ΜονΠρωτΠειρ 4137/2019 (Ειδ.) σε ΤΝΠ QUALEX, και σε ΙΣΟΚΡΑΤΗ «https://www.dsanet.gr/Epikairothta/Nomologia/mprpeir%204137_2019.htm»

[115] Καμπέρου, ό.π., σελ. 2746

[116] Βασιλάκη, ό.π. 1993, σελ. 178, Μανωλεδάκης ό.π., σελ. 134, Μυλωνόπουλος, ό.π. σελ. 75

[117] Κονταξής, 2000, σελ. 3151

[118] ΣυμβΑΠ 1294/2007 ΠοινΧρ 2008, σελ. 346

Χρησιμοποίηση των απόρρητων στοιχείων ή προγραμμάτων υπολογιστών συνιστά η χρήση σύμφωνα με τον προορισμό τους, [119] ή η εμπορική τους εκμετάλλευση με σκοπό το όφελος. [120]

Ως **αποκάλυψη** σε τρίτο νοείται η ολική ή μερική γνωστοποίηση του λογισμικού ή των δεδομένων σε τρίτο, που δεν έχει δικαίωμα πρόσβασης σε αυτά, έτσι ώστε να γίνεται δυνατή η εκμετάλλευση τους,[121] όχι όμως και η περιγραφή τους. Αποκάλυψη θα μπορούσε να συντελεσθεί με γνωστοποίηση στον τρίτο του μυστικού κωδικού πρόσβασης στον ηλεκτρονικό υπολογιστή (password), όπου είναι αποθηκευμένα τα κρίσιμα απόρρητα, με τον οποίο κωδικό ο τρίτος αποκτά απευθείας πρόσβαση σε αυτά και μπορεί να τα αντιγράψει, αποθηκεύσει ή χρησιμοποιήσει κατά το δοκούν. [122] Νομολογιακό παράδειγμα συνιστά η έναντι αμοιβής παραχώρηση σε διαφημιστή, που έχει αναλάβει τη διαφημιστική καμπάνια, του πελατολογίου της εγκαλούσης εταιρείας.[123] Περαιτέρω, είναι δυνατή και η αποκάλυψη των απορρήτων δεδομένων με παράλειψη.

Το αδίκημα του άρθρου 370Γ ΠΚ τελεί όποιος, εκτός από τους παραπάνω τρόπους «οπωσδήποτε παραβιάζει» τα απόρρητα. Προκειμένου να πληρούται η αρχή της νομιμότητας και δη η επιταγή σαφούς περιγραφής της αξιόποινης συμπεριφοράς [124] και να αποφευχθεί ο κίνδυνος υπερβολικής διεύρυνσης του αξιοποίνου, ο εν λόγω όρος πρέπει να ερμηνευθεί περιοριστικά, ώστε να αναφέρεται σε πράξεις ανάλογης βαρύτητας και απαξίας με εκείνες των άλλων τεσσάρων τρόπων τέλεσης του αδικήματος.[125] Ήγουν, δέον να μην εντάσσεται στην αντικειμενική υπόσταση του υπό ανάλυση άρθρου η απλή πρόσβαση σε δεδομένα και προγράμματα ηλεκτρονικών υπολογιστών χωρίς ο δράστης να αποκτά και τα παραβιαζόμενα απόρρητα, διότι η εν λόγω συμπεριφορά πληροί τους όρους του άρθρου 370Β ΠΚ για την παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα και επαπειλεί ποινή ηπιότερη (φυλάκιση έως 2 έτη ή χρηματική ποινή) συγκριτικά με αυτή του άρθρου 370Γ (φυλάκιση τουλάχιστον 3 μήνες).

4.3.4. Στοιχεία ή προγράμματα υπολογιστών

Αντικείμενο του εγκλήματος είναι «τα στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα».

Όσον αφορά την έννοια των όρων «**στοιχεία ή προγράμματα υπολογιστών**», ως τέτοια νοούνται τα στοιχεία που έχουν άμεση σύνδεση μόνο με την έννοια του λογισμικού (software), στο οποίο περιλαμβάνονται το σύνολο πληροφοριών ή δεδομένων των προγραμμάτων των ηλεκτρονικών υπολογιστών. Με το άρθρ. 370Γ ΠΚ προστατεύεται λοιπόν μόνο το λογισμικό, ενόψει της ρητής αναφοράς σε «στοιχεία ή προγράμματα υπολογιστών»

[119] Κονταξής, 2000 σελ. 3152
[120] Μυλωνόπουλος, ό.π. σελ. 76
[121] Για την έννοια «της ανακοίνωσης σε τρίτον» στο άρθρο 16 Ν 146/1914 βλ. Βασιλάκη, ΝοΒ 1988, σελ. 1341
[122] Καμπέρου, ό.π., σελ. 2747
[123] ΣυμβΕφΑθ 217/1997, σελ. 846
[124] άρθρο 7 παρ. 1 του Συντάγματος που ρητά απαιτείται ο ποινικός νόμος να <<ορίζει τα στοιχεία της αξιόποινης πράξης>>. Έτσι, τα στοιχεία του εγκλήματος και οι προϋποθέσεις του αξιοποίνου εν γένει πρέπει όχι απλώς να περιγράφονται στο νόμο, αλλά και να είναι επαρκώς προσδιορίσιμα για να πληρούν τους όρους της αρχής nullum crimen nulla poena sine lege certa (Μυλωνόπουλος Χ., Γενικό Μέρος, όπ, σελ, 122-123)
[125] Κιούπης, ό.π., σελ. 129

όχι και το μηχανικό μέρος του υπολογιστή «hardware», το οποίο καλύπτεται από τις άλλες διατάξεις του ειδικού μέρους του ΠΚ, όπως π.χ. οι διατάξεις των άρθρ. 372 (κλοπή) και 378 ΠΚ (φθορά ξένης ιδιοκτησίας) κλπ. [126] Άρα, η αποκάλυψη λόγου χάρη ενός βιομηχανικού απορρήτου, που δεν είναι αποθηκευμένου στη μνήμη ηλεκτρονικού υπολογιστή, δεν εντάσσεται στο άρθρο 370Β ΠΚ.

4.3.5. Απόρρητα

Τα προστατευόμενα απόρρητα υπό του άρθρου 370Γ περιορίζονται ήγουν μόνο στις περιπτώσεις της «παράνομης διείσδυσης» σε κρατικά, επιστημονικά, επαγγελματικά ή επιχειρηματικά απόρρητα, καλύπτοντας τις περιπτώσεις της διαδεδομένης εμπορικής ή βιομηχανικής κατασκοπείας.[127]

Ως **απόρρητα** θεωρούνται, κατά το εδάφιο β', και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους, χωρίς ωστόσο να έκταση εφαρμογής της διάταξης και σε άλλα είδη απορρήτων που δεν συμπεριλαμβάνονται στο α' εδάφιο. [128]

Προστατεύονται απόρρητα τόσο ιδιωτικά όσο και δημόσια. Ως προς τον ορισμό του απορρήτου γίνεται δεκτό, σύμφωνα με τη μικτή θεωρία,[129] ότι τα στοιχεία του υπολογιστή θεωρούνται απόρρητα όταν: α) είναι προσιτά σε περιορισμένο κύκλο προσώπων χωρίς να είναι κοινώς γνωστά, β) συνδέονται με τη λειτουργία μιας επιχείρησης, πράγμα που γνωρίζουν τα πιο πάνω πρόσωπα και γ) η πρόσβαση σε αυτά είναι δυσχερής και τηρούνται απόρρητα με τη βούληση του κατόχου τους, ο οποίος έχει δικαιολογημένο ενδιαφέρον για αυτό. [130]

Ωστόσο, δεν αποκλείεται η προστασία προγραμμάτων και δεδομένων, ως προς τα οποία ο κάτοχός τους δεν έχει εκδηλώσει ρητά τη βούληση του να τα τηρήσει απόρρητα ή το ενδιαφέρον να τηρηθούν απόρρητα δεν είναι δικαιολογημένο, όπως προκύπτει από τη διατύπωση του νόμου («ως απόρρητα θεωρούνται και εκείνα που…»).[131] Ωστόσο έχει επισημανθεί ότι το αξιόποινο πρέπει να μην εξαρτάται μόνο από το υποκειμενικό στοιχείο

---

[126] ΣυμβλΕφΑθ 2949/2003, ΠοινΔικ 2004, σελ. 1110· ΣυμβλΠλημΑθ 4742/2004, ΠοινΔικ 2005, σελ. 407· ΑΠ 121/2003 Ποιν 2003, σελ. 619 και Ε. Βασιλάκη, ό.π., σελ. 222, Α. Κονταξής, ΠΚ, Τόμ. Β΄, σελ. 3145, Α. Κωστάρας, ό.π., σελ. 1149 επ., Χ. Λαμπάκης, ό.π., σελ. 1724, Μ. Μαργαρίτης, ΠΚ, σ. 1033 αριθμ. 2· Χ. Μυλωνόπουλος, ΠοινΧρ 1991, 81

[127] Μ. Καϊάφα-Γκμπάντι, Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, Αρμ 7/2007, σελ. 1068 = sakkoulas-online, Κιούπης, ό.π. (1999), σελ. 132, Μυλωνόπουλος, ό.π., σελ. 81. Αντίθετοι Βασιλάκη, σελ. 174 και Μαργαρίτης, ό.π. (2009), σελ. 1033

[128] Όπως προκύπτει από την Αιτιολογική Έκθεση του Ν. 4919/2019 (σελ. 71), ο νομοθέτης δεν θέλησε στο δεύτερο εδάφιο της παραγράφου 1 να διευρύνει την έκταση εφαρμογής της διάταξης και σε άλλα είδη απορρήτων, εκτός από τα οριζόμενα στο εδάφιο α, αλλά «(δ)ιευκρινίζεται το περιεχόμενο της έννοιας των απορρήτων» (https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/k-poinkod-eis-NEO.pdf)

[129] ΑΠ 121/2003 ΣΤ'Τμ. [Αντιγραφή και χρήση προγραμμάτων Η/Υ] (παρατ. Γ. Νούσκαλης), ΠοινΔικ, 6/2003, σελ. 619 – 620, (ΤΝΠ QUALEX), Βλ. Μυλωνόπουλου, ό.π., σελ. 72· Ρόκα, Αθέμιτος ανταγωνισμός, σελ. 127· Κοτσίρη, Δίκαιο ανταγωνισμού, σελ. 1 Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 411-413, υποσ. 949 = sakkoulas-online

[130] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 411, αρ. 674 = sakkoulas-online και Μυλωνόπουλος, ό.π. σελ. 72-73, Βασιλάκη, ό.π. (1993) σελ. 165

[131] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 412, αρ. 674 = sakkoulas-online

της θέλησης του κατόχου των πληροφοριών, αλλά το δικαιολογημένο ενδιαφέρον του να είναι αντικειμενικό. [132]

Συνοψίζοντας, βασική προϋπόθεση για το χαρακτηρισμό στοιχείων (δεδομένων) ως απορρήτων είναι, το αν αυτά είναι προσιτά ή όχι σε κάθε τρίτο, ενώ όσον αφορά τα προγράμματα η/υ, η ιδιότητα του απορρήτου, με βάση την παραπάνω διάταξη, αποδίδεται σε αυτά που συνδέονται με ορισμένο κάτοχο και ο κύκλος των προσώπων που γνωρίζουν το πρόγραμμα είναι περιορισμένος. Από την προστασία που παρέχει ο νόμος αποκλείεται, συνεπώς, το τυποποιημένο λογισμικό ή στοιχεία και προγράμματα υπολογιστών, τα οποία κυκλοφορούν ελεύθερα στο διαδίκτυο ή γενικότερα είναι προσβάσιμα στον οποιοδήποτε, διότι αν συνέβαινε αυτό, τότε το ενδιαφέρον του κατόχου τους να παραμείνουν μυστικά δεν θα ήτο δικαιολογημένο. Ο χαρακτήρας του προγράμματος είναι αδιάφορος, ενώ κρίσιμο είναι αν η διάθεσή του περιορίζεται σε έναν ορισμένο κύκλο αποδεκτών-χρηστών και προβλέπονται ρήτρες διαφύλαξης του προγράμματος, προκειμένου να θεωρηθεί ως απόρρητο, ενώ όταν ο κύκλος των αποδεκτών του προγράμματος είναι μεγάλος, η ύπαρξη τεχνικών μέτρων ασφαλείας δηλώνει την πρόθεση του δημιουργού να παραμείνει το πρόγραμμα απόρρητο. [133]

Κρατικά απόρρητα είναι τα στοιχεία ή περιστατικά, με πρωτογενή σπουδαιότητα για την ίδια την κρατική υπόσταση, [134] τα οποία βάσει βουλήσεως των εκπροσώπων του κράτους και λόγω της φύσης τους, απαγορεύεται να γνωστοποιηθούν σε πρόσωπα που βρίσκονται έξω από το στενό υπηρεσιακό κύκλο.[135] Ενόψει των ειδικότερων διατάξεων 146 έως 152 ΠΚ στο Κεφάλαιο IV για τις προσβολές κρατικών απορρήτων, στη διάταξη δεν συμπεριλαμβάνονται, μολονότι αποτελούν όψεις κρατικών απορρήτων, τα στρατιωτικά και διπλωματικά απόρρητα ή τα απόρρητα που αναφέρονται στην ασφάλεια του Κράτους. [136]

Επιστημονικά απόρρητα θεωρούνται τα στοιχεία εκείνα που περιέχουν συστηματικές γνώσεις, συνιστούν βιβλία ή μελέτες ή πορίσματα ερευνών, όταν βρίσκονται στο στάδιο γραφής ή υπό έκδοση, αναφερόμενα στην ερμηνεία ή την προβολή ορισμένου γνωστικού αντικειμένου (π.χ. διδακτορική διατριβή, μελέτη, άρθρα) και πρέπει βάσει βουλήσεως του ίδιου του συγγραφέα ή δημιουργού να μείνουν απόρρητα μέχρι και την δημοσίευσή τους.[137]

---

[132] Καμπέρου, ό.π., με παραπομπή σε Νούσκαλη, ΠοινΔικ 2003, σελ. 621 ΑΠ 121/2003 ΣΤ'Τμ. [Αντιγραφή και χρήση προγραμμάτων Η/Υ] (παρατ. Γ. Νούσκαλης)

[133] Σύμφωνα με το γράμμα του νόμου, με τη χρήση του επιρρήματος «ιδίως» στο εδάφιο β, συνεκτιμάται από το Δικαστήριο εάν ο νόμιμος κάτοχος έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση, προκειμένου να βεβαιωθεί η βούλησή του να διατηρηθεί το στοιχείο ή το πρόγραμμα του υπολογιστή απόρρητο. Κατά τη συνήθη πρακτική των χρηστών του Διαδικτύου, ο νόμιμος κάτοχος ενός στοιχείου ή προγράμματος υπολογιστή που το έχει αφήσει ελεύθερα προσπελάσιμο στον οποιονδήποτε τρίτο χωρίς λήψη οποιουδήποτε, έστω και στοιχειώδους μέτρου ασφαλείας ή προστασίας, εκφράζει με τον τρόπο αυτό τη βούλησή του να καθίστανται τα εν λόγω στοιχεία γνωστά στον οποιονδήποτε. Το ενδιαφέρον το να μη λάβουν γνώση οι άλλοι δεν θα μπορούσε να αξιολογηθεί ως δικαιολογημένο. Βλ. Καμπέρου, ό.π., σελ. 2748, Βασιλάκη, ό.π., σελ. 168-171. Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 411-413, υποσ. 950 = sakkoulas-online

[134] Α. Παπαδαμάκης, Στρατιωτικό Ποινικό Δίκαιο, Θεωρητική θεμελίωση και συστηματική ερμηνεία του νέου στρατιωτικού ποινικού κώδικα: Εισαγωγή, θεμελιώδεις έννοιες, ουσιαστικό μέρος, δικονομικό μέρος, (Σάκκουλας 2008), σελ. 354 έως 355 και δη υποσημείωση 3

[135] Βλ. Α. Κωστάρα, ό.π., σελ. 1150 επ., Α. Κονταξή, ό.π., σελ. 3149, Χ. Λαμπάκη, ό.π., σελ. 1725

[136] Καμπέρου, ό.π., σελ. 2749

[137] Α. Κωστάρα, ο.π. σελ. 1150 επ, με παραπομπή σε Α. Κονταξή, ΠΚ, Τόμος Β, σελ. 3149

Επαγγελματικά απόρρητα είναι οι μέθοδοι παραγωγής ενός προϊόντος, το πελατολόγιο, το συνταγολόγιο και άλλα επαγγελματικά μυστικά. [138] **Απόρρητο επιχείρησης** του δημοσίου ή ιδιωτικού τομέα είναι εκείνα που αναφέρονται στην κάτοχό τους επιχείρηση[139] και αποτελούν συνήθως και επαγγελματικό απόρρητο.

Νομολογιακά έχει κριθεί ότι απόρρητο συνιστούν τα στοιχεία που αφορούν τις συναλλαγές της εγκαλούσας εταιρείας με άλλες εταιρείες ή αναφέρονται στη διάρθρωση του μετοχικού της κεφαλαίου και απεικονίζουν τους Έλληνες του και ξένους επενδυτές ή αναφέρονται σε επιταγές εισπρακτέες από την εταιρία ή σχετίζονται με το θέμα του διακανονισμού του ΦΠΑ ή αναφέρονται σε ισοζύγια, είναι καταστάσεις που αφορούν σε λήξη επιταγών ή είναι καρτέλες λογαριασμών, οι οποίες περιέχουν επιταγές και αφορούν σε συναλλαγές της εταιρείας.[140] Επίσης έχει κριθεί ως επαγγελματικό απόρρητο ο κατάλογος ασφαλιστικών συμβολαίων στον οποίον αναγράφονταν ο αριθμός του κάθε συμβολαίου, το όνομα και η επωνυμία του ασφαλιζόμενου, η διάρκεια της ασφάλισης, η μάρκα του ασφαλιζόμενου οχήματος και ο αριθμός κυκλοφορίας του, τα οποία τηρούνταν στους ηλεκτρονικούς υπολογιστές της εταιρείας.[141]

Δέον να επισημανθεί ότι το απόρρητο δεν αφορά αυτά καθαυτά τα ονόματα ή τις διευθύνσεις που είναι καταχυρωμένα στον ηλεκτρονικό υπολογιστή, αλλά την ιδιότητά των ατόμων αυτών ως πελατών της συγκεκριμένης επιχείρησης. [142]

Τα **εμπορικά απόρρητα** ανήκουν στα απόρρητα μιας επιχείρησης ιδιωτικού ή δημοσίου τομέα, καθώς συνιστούν πληροφορίες που δεν είναι ευρέως γνωστές, έχουν εμπορική αξία που απορρέει από τον απόρρητο χαρακτήρα τους και ο κάτοχος των πληροφοριών αυτών έχει καταβάλει εύλογες προσπάθειες για την προστασία του απόρρητου χαρακτήρα τους.[143]

Ο δόλος θα πρέπει να περιλαμβάνει τη γνώση του δράστη ότι πρόκειται για απόρρητα άλλου, δημόσιου ή ιδιωτικού τομέα.[144]

---

[138] Κ. Φράγκος, Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 370Γ, αρ. 7, Ενημέρωση:10/12/2019, sakkoulas-online

[139] ΑΠ 121/2003 ΣΤ'Τμ. [Αντιγραφή και χρήση προγραμμάτων Η/Υ] (παρατ. Γ. Νούσκαλης) ΠοινΔικ, 6/2003, σελ. 619 – 620 (ΤΝΠ QUALEX) στην εν λόγω υπόθεση οι κατηγορούμενοι αντέγραψαν αθεμίτως σε δισκέτες το πελατολόγιο της εν λόγω επιχείρησης (επαγγελματικό της απόρρητο) και αποχωρώντας από αυτήν, ίδρυσαν άλλη, ανταγωνιστική εταιρία με όμοιο αντικείμενο, χρησιμοποιώντας τα στοιχεία που είχαν αντιγράψει.

[140] ΣυμβΑΠ 1294/2007 προσπελάσιμη στο διαδικτυακό ιστότοπο του ΑΠ (https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=Z0ZgV0KruNiNdUlNRuIjl8KimOmvod&apof=1294_2007&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%C6)

[141] ΤρΠλημΑθ 2484/2019 (Παραβίαση επαγγελματικού απορρήτου ιδιαίτερα μεγάλης οικονομικής σημασίας - Υφ' όρον παύση ποινικής δίωξης) ΠοινΔικ, 5/2020, σελ. 461 – 462 (ΤΝΠ QUALEX)

[142] Όπως φέρ' ειπείν των ενδιαφερομένων να πραγματοποιήσουν ταξίδια (ΑΠ 121/2003)

[143] Άρθρο 22Α Ν 1733/1987 (σχετικά με την προστασία της τεχνογνωσίας και των επιχειρηματικών πληροφοριών που δεν έχουν αποκαλυφθεί -εμπορικό απόρρητο- από την παράνομη απόκτηση, χρήση και αποκάλυψη) όπως τροποποιήθηκε με το άρθρο 1 Ν.4605/2019, ΦΕΚ Α 52/1.4.2019 με το σκοπό εναρμόνιση με την Οδηγία (ΕΕ) 2016/943).

[144] Κ. Φράγκος, Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 370Γ, αρ. 8, Ενημέρωση:10/12/2019, sakkoulas-online

4.4. Οι διακεκριμένες μορφές του εγκλήματος (370Γ παρ. 2)

Με την παρ. 2 τιμωρείται βαρύτερα, σε βαθμό πλημμελήματος, ο δράστης αν είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, οπότε επιβάλλεται φυλάκιση τουλάχιστον ενός έτους. Τουτέστιν, τυποποιούνται δύο διακεκριμένες παραλλαγές και υπάλληλοι του κατόχου υπό ευρεία έννοια μπορεί να είναι και υπάλληλοι του δικαιούχου μη κατόχου, ενώ η οικονομική αξία του απόρρητου στοιχείου ή προγράμματος συναρτάται με την αξία που έχει για τον δικαιούχο παθόντα.

Εν προκειμένω, ο νομοθέτης απαξιολογεί ως ειδεχθέστερη την «κατασκοπεία εκ των έσω». Συγκεκριμένα, στην **υπηρεσία του κατόχου των στοιχείων** θεωρείται ότι βρίσκεται ο δράστης, όταν συνδέεται με το νόμιμο κάτοχο των στοιχείων με οποιαδήποτε σχέση εξαρτημένης ή ανεξάρτητης εργασίας ή ακόμη και με σύμβαση έργου. Ο γενικός διευθυντής μιας επιχείρησης είναι εργαζόμενος υπό αυτή την έννοια, όπως και η καθαρίστρια ενός μικρού συνεργείου. [145] Ωστόσο, η έκφραση «στην υπηρεσία του κατόχου των δεδομένων» δέον να ερμηνεύεται περιοριστικά, καθώς μέλη του ΔΣ ή πρώην εργαζόμενοι υπόκεινται μόνο στο πλαίσιο ποινής της παραγράφου 1, αφού δεν τελούν (ή δεν τελούν πια) σε σχέση οποιασδήποτε μορφής εργασίας και κατ' επέκταση δεν πληρούται ο όρος της απασχόλησης στην υπηρεσία του κατόχου. [146] Οι εξωτερικοί συνεργάτες καθώς και οι τεχνικοί που εργάζονται για λίγο χρονικό διάστημα και για συγκεκριμένη εργασία σε μια επιχείρηση, πρέπει να αποκλείονται από την υπό εξέταση επιβαρυντική περίσταση, εάν δεν προκύπτει η υποχρέωση διαφύλαξης του απορρήτου από ρητή συμβατική υποχρέωση ή από τις περιστάσεις ή υποχρέωση πίστης που απορρέει από το εργατικό δίκαιο. [147]

Νομολογιακά έχει κριθεί ότι στην υπηρεσία του κατόχου των στοιχείων είναι ο υπάλληλος της εγκαλούσας εταιρίας, ο οποίος εργαζόταν ως αναλυτής - προγραμματιστής και λόγω της ιδιότητάς του αυτής είχε τη δυνατότητα πρόσβασης στα καταχωρημένα στον ηλεκτρονικό υπολογιστή της εταιρίας στοιχεία. [148]

Επιπλέον, στοιχειοθετείται η διακεκριμένη παραλλαγή του αδικήματος όταν το απόρρητο είναι μεγάλης οικονομικής σημασίας. Εν προκειμένω, η ιδιαίτερη ποινική απαξία βασίζεται στην οικονομική ζημία που υπέστη ο νόμιμος κάτοχος των απορρήτων, γεγονός που μπορεί να δικαιολογηθεί ιδίως ενόψει των επενδύσεων που γίνονται στο χώρο του λογισμικού και την μεγάλη οικονομική αξία που ενυλώνουν πολλές φορές στοιχεία που είναι αποθηκευμένα στον υπολογιστή.

[145] Στα πλαίσια ανάλυσης του άρθρου 370Β παλαιού ΠΚ Κωστάρας, ό.π. σελ. 1149. Βασιλάκη, ό.π. (η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993), σελ. 184 και Κωνσταντινίδης, Καθήκον μαρτυρίας και επαγγελματικό απόρρητο στην ποινική δίκη, τεύχος β', (ΑΝΤ. Ν. ΣΑΚΚΟΥΛΑΣ 1991), σελ. 174

[146] Χ. Μυλωνόπουλος, ό.π. (ηλεκτρονικοί υπολογιστές και διαδίκτυο 1991), σελ. 84

[147] Βασιλάκη, ό.π., σελ. 184

[148] ΕφΑθ 217/1997, Υπερ 1997, σελ. 846

4.5. Ποινικές κυρώσεις

Η πράξη της παραγράφου 1 τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών με μέγιστο επιβλητέας ποινής τα 5 έτη. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους (1 έως 5 έτη φυλάκισης). Η ιδιαίτερη οικονομική σημασία κρίνεται σε συνάρτηση με τα έννομα αγαθά του παθόντος, φέρ' ειπείν η παράδοση λίστας πελατών σε ανταγωνιστή ή προγραμμάτων για την εκπόνηση των οποίων έγινε πολυδάπανη έρευνα. [149]

Κατά την παρ. 3 ορίζεται ότι οι πράξεις που προβλέπονται στις παραγράφους 1 και 2, που είναι πλημμελήματα, διώκονται ύστερα από έγκληση.

4.6. Ειδικές μορφές εμφάνισης του εγκλήματος

4.6.1.Απόπειρα

Με το νόμο 4619/2019, ο νέος Ποινικός Κώδικας φαίνεται, μολονότι ουσιαστικώς η διατύπωση του άρθρου 42ΠΚ δεν διαφέρει από την προγενέστερη, [150] να απεμπόλησε τη διευρυμένη-ουσιαστική αντικειμενική θεωρία αναφορικά με την αρχή εκτέλεσης στην απόπειρα, όπως είχε υιοθετηθεί από τη Νομολογία κατόπιν της υπ' αριθμόν 285/1665[151] του Ανωτάτου Ακυρωτικού της Χώρας και εφαρμόζεται ομοιόμορφα επί σειρά ετών. Στην αιτιολογική έκθεση ορίζεται πως στο πλαίσιο του νέου ΠΚ, εφεξής, ακολουθείται η τυπική αντικειμενική θεωρία,[152] προκειμένου στην αρχή εκτέλεσης να μην παρεισφρέουν στοιχεία εκτός της αντικειμενικής υπόστασης, κάτι που ουδέποτε υποστηρίχθηκε βάσει του τύπου του Frank.[153] Βεβαίως, η ίδια η αιτιολογική αντιφάσκει όσον αφορά τα άτυπα εγκλήματα επιστρέφοντας στην ακολουθητέα θεωρία του Frank [154] και αποδεικνύοντας πόσο επικίνδυνη μπορεί να αποβεί η αναδιατύπωση παγιωμένων θέσεων.

---

[149] Μιχαήλ Μαργαρίτης και Άντα Μαργαρίτη, *ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ Ερμηνεία – Εφαρμογές* (4η, Π Ν Σάκκουλας 2020) σελ. 1086. Περαιτέρω παραπομπές σε Καϊάφα – Γκμπάντι, Παρατηρήσεις στην ΕφΑθ 217/1997, Υπερ 1997, σελ. 850

[150] πΠΚ : « ...επιχειρεί πράξη που περιέχει τουλάχιστον αρχή εκτέλεσης...»
νΠΚ: « ...αρχίζει να εκτελεί την περιγραφόμενη στον νόμο αξιόποινη πράξη..»

[151] ΑΠ 285/1965, ΠοινΧρ 1965, σελ. 592 << αρχή εκτέλεσης υπάρχει, όταν ο δράστης προβεί σε ενέργεια, η οποία αποτελεί μέρος της αντικειμενικής υποστάσεως του εγκλήματος και οδηγεί κατ' ευθείαν στην πραγμάτωση αυτού, ή τελεί προς αυτή σε τέτοια αναγκαία και άμεση σχέση συνάφειας, ώστε κατά την κοινή αντίληψη να θεωρείται σαν τμήμα αυτής, στην οποία αμέσως οδηγεί, αν δεν ήθελε ανακοπεί από οποιονδήποτε λόγο>>

[152] Αιτιολογική του Ν. 4619/2019 «14. Προσδιορίζεται το περιεχόμενο της αρχής εκτέλεσης του εγκλήματος στο πλαίσιο της απόπειρας, ώστε να είναι σαφές ότι για να θεμελιωθεί αξιόποινο πρέπει να έχει αρχίσει να πραγματώνεται ένα μέρος της αντικειμενικής υπόστασης του εγκλήματος (άρθρο 42 παρ. 1)»

[153] Μυλωνόπουλος Χ., «Ζητήματα Απόπειρας κατά τον νέο Ποινικό Κώδικα» Ποινική Δικαιοσύνη 2020, σελίδα 321

[154] Αιτιολογική του Ν. 4619/2019: «Τούτο είναι εφικτό ακόμα κι όταν ο ακριβής τρόπος τέλεσης δεν περιγράφεται στον νόμο, όπως λ.χ. συμβαίνει στο έγκλημα της ανθρωποκτονίας ή της σωματικής βλάβης. Στις περιπτώσεις αυτές ο δράστης αρχίζει να εκτελεί την περιγραφόμενη στον νόμο πράξη όταν έχει εξαπολύσει κατά του εννόμου αγαθού την ενέργεια η οποία, κατά την συνήθη πορεία των πραγμάτων, είναι ικανή να επιφέρει την αξιόποινη βλάβη αν δεν ανακοπεί από άλλη πράξη του ιδίου ή τρίτου ή από επιγενόμενο τυχαίο γεγονός, όπως λ.χ. όταν πυροβολεί προς την πλευρά του θύματος, του επιτίθεται με μαχαίρι κλπ.»

Απόπειρα τέλεσης του αδικήματος του άρθρου 370Γ ΠΚ είναι νοητή με οποιονδήποτε τρόπο και αν τελείται αυτό. Συγκεκριμένα, το αδίκημα είναι τετελεσμένο από τη στιγμή, που θα γίνει αντιγραφή, αποτύπωση, αποκάλυψη, παραβίαση ή χρήση των στοιχείων ή του προγράμματος ηλεκτρονικού υπολογιστή. Πριν από αυτές τις χρονικές στιγμές, εφόσον ο δράστης έχει προβεί σε αρχή εκτέλεσης, το αδίκημα βρίσκεται σε στάδιο απόπειρας.[155] Επί παραδείγματι, αρχή εκτέλεσης συνιστά το πάτημα του πλήκτρου, που δίνει την εντολή για την αντιγραφή και όχι η τοποθέτηση της δισκέτας ή του USB στον ηλεκτρονικό υπολογιστή[156] ή το πάτημα του πλήκτρου, που δίνει την εντολή για εκτύπωση των δεδομένων, αλλά για λόγους ανεξάρτητους από τη θέληση του δράστη δεν ολοκλήρωσε τη σκοπούμενη ενέργεια, διότι εμφανίστηκε απροειδοποίητα κάποιος. [157]

4.6.2. Συμμετοχή

Η συμμετοχή στο αδίκημα παρίσταται δυνατή σε όλες τις κατά τα άρθρα 45 επόμενα του ΠΚ μορφές της. Ειδικά όσον αφορά την ηθική αυτουργία και τη συνέργεια αξιοσημείωτο είναι το ότι, εφόσον το αδίκημα της παραγράφου 2 (περίπτωση πρώτη) διαπλάσσεται ως μη γνήσιο ιδιαίτερο, τότε για το συμμέτοχο που δεν έχει τη τυποποιημένη ιδιότητα, τυγχάνει εφαρμογής η παράγραφος 1, κατ' εφαρμογή του άρθρου 49 παρ. 2 ΠΚ. [158]

4.6.3. Συρροές

Η εν λόγω διάταξη είναι νέα και ειδική εν σχέσει με το άρθρο 16 του Ν. 146/1914 για τον αθέμιτο ανταγωνισμό και εξ ου η συρροή είναι φαινομενική κατ' ιδέαν, όταν πρόκειται για εμπορικό ή βιομηχανικό απόρρητο και βάσει της αρχής της ειδικότητας εφαρμόζεται το άρθρο 370Γ ΠΚ.[159]

Το άρθρο 72 του Ν 2121/1993 καλύπτει μόνο το πρωτότυπο πνευματικό δημιούργημα, κάτι που στα πλαίσια ανάλυσης του άρθρου καταδείχθηκε ότι δεν είναι απαραίτητο.

Άρθρο 29. Κυρώσεις και διοικητικά πρόστιμα. (Ν. 4850/2021)

«β. Όποιος, χωρίς δικαίωμα, αποκτά πρόσβαση, ή όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί ή αποκαλύπτει σε τρίτον μέρος ή σύνολο ηλεκτρονικών δεδομένων του άρθρου 15, διώκεται σύμφωνα με τα άρθρα 370Β και 370Γ του Ποινικού Κώδικα (ν. 4619/2019, Α' 95), κατά περίπτωση».

[155] Αλέξανδρος Κωστάρας, *ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ – ΕΠΙΤΟΜΗ ΕΙΔΙΚΟΥ ΜΕΡΟΥΣ (Άρθρα 134-410 ΠΚ)* (4η, Νομική Βιβλιοθήκη 2014) 1151

[156] Λαμπράκης Χ., σε Χαραλαμπάκη Α., Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, τόμος Β', άρθρα 207-473, σελ. 1727, στα πλαίσια ερμηνεία του παλαιού 370Β ΠΚ

[157] Καμπέρου, ό.π. σελ. 2751

[158] Κωστάρας, ό.π. σελ. 1152 και Χ. Λαμπάκη/Ε.Καμπέρου-Νταλτα, ό.π., σελ. 1728 και 2751 αντίστοιχα, Α. Κονταξής, ΠΚ, Τόμ. Β΄, Έκδοση Γ', 2000 σελ. 3153

[159] Κονταξής, ό.π. στα πλαίσια ερμηνεία του 370Β Πτκ, σελ. 3152

5. Η παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και η χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα ή σε στοιχεία μεταδιδόμενα με συστήματα τηλεπικοινωνιών (370Δ ΠΚ)

Η νομοτυπική υπόσταση του αδικήματος 370Δ ΠΚ διαπλάσσεται ως ακολούθως.

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.

2. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του, τιμωρείται με φυλάκιση.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου.

Προλεγόμενα

Με το ν. 4411/2016 εισήχθη μια νέα διάταξη, το άρθρο 370Δ ΠΚ με το οποίο τιμωρείτο αυτοτελώς η παραβίαση του επικοινωνιών μέσω πληροφοριακών συστημάτων ως κακούργημα. Η διάταξη αυτή μεταφέρθηκε στο άρθρο 370Ε ΠΚ και τιμωρείται μετά το Ν. 5002/2022 ως κακούργημα.

Η διάταξη του άρθρου 370Δ του νέου ΠΚ (που αντιστοιχεί στο 370Γ προϊσχύσαντος ΠΚ) τιμωρεί όποιον χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών (παρ. 1), καθώς και όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση (παρ. 2).

Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου (παρ. 3).

Αν η ανωτέρω πράξη αναφέρεται σε στοιχεία που αφορούν στις διεθνείς σχέσεις της χώρας ή στην ασφάλεια του κράτους, ο δράστης τιμωρείται, κατά το άρθρο 148 παρ. 2 του νέου ΠΚ, για κακουργηματική κατασκοπεία.[160]

[160] Στο νέο ΠΚ δεν συμπεριελήφθη στη διάταξη διακεκριμένη παραλλαγή, όπως στο άρθρο 370Γ 2 προϊσχύσαντος ΠΚ, όταν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, καθότι παρέχεται επαρκής προστασία στα κρατικά απόρρητα μέσω των διατάξεων 146-152 ΠΚ (IV.Προσβολές κρατικών απορρήτων)

Ενώ το άρθρο 370Β αφορά στη διαφύλαξη απορρήτων με τη μορφή του στοιχείου ή προγράμματος Η/Υ, το παρόν άρθρο αφορά κάθε άλλο στοιχείο ή πρόγραμμα. [161]

5.1. Προστατευόμενο έννομο αγαθό

Υποστηρίζεται ότι με την παρούσα διάταξη προστατεύεται η εξουσία του δικαιούχου να διαθέτει τα στοιχεία και τα προγράμματα Η/Υ κατ' αρέσκεια, λόγω της επαγγελματικής και οικονομικής τους αξίας.[162]

Η κρατούσα άποψη θεωρεί ότι έννομο αγαθό της διατάξεως του άρθρου 370Δ ΠΚ (όπως και του άρθρου 370 Β), συνιστά το απόρρητο υπό τυπική έννοια, δηλαδή το τυπικό δικαίωμα του νομίμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου υπό ουσιαστική έννοια.[163] Προστατεύονται τα προγράμματα ως αποτελέσματα οικονομικών επενδύσεων, λόγω της μεγάλης οικονομικής-περιουσιακής αξίας αυτών. [164] Κατά συνέπεια, η ίδια η πληροφορία έχει ουσιαστική αξία και αυτή εν τέλει προστατεύεται, [165] καθόσον προσλαμβάνει υπόσταση και αξία κατόπιν αξιολογήσεως από τον φορέα της, ο οποίος με τον τρόπο αυτόν αποκτά την εξουσία διαθέσεώς της, τη δυνατότητα εξουσιάσεώς της και το δικαίωμα να αποκλείει κάθε ανάμειξη τρίτου με αυτή χωρίς τη συγκατάθεσή του.[166]

Συνεπώς, η ως άνω διάταξη έχει θεσπιστεί για την προστασία του ιδιωτικού συμφέροντος και όχι του κοινωνικού, από την παράβασή της δε προσβάλλονται ιδιωτικά συμφέροντα και δεν γεννάται αξίωση αποζημιώσεως ή χρηματικής ικανοποιήσεως λόγω ηθικής βλάβης του Ελληνικού Δημοσίου. [167]

Ειδικά για την παρ. 2, έννομο αγαθό συνιστά και το απόρρητο των ψηφιακών δεδομένων, [168] όπως αυτά περιγράφονται στο άρ. 13 περ. ζ ΠΚ, και των στοιχείων που μεταδίδονται μέσω συστημάτων επικοινωνιών. Ούτως, προασπίζεται το ''ψηφιακό άσυλο'' του νόμιμου

---

[161] ΑΠ 121/2003 «(οι) διατάξεις αυτές, (370 Β΄ παρ.1 και 2 του παλαιού ΠΚ) οι οποίες θεσπίστηκαν για τη διαφύλαξη των αναφερόμενων απορρήτων που έχουν τη μορφή στοιχείου ή προγράμματος υπολογιστή, σε αντίθεση με το άρθρο 370 Γ ΠΚ που αφορά κάθε άλλο στοιχείο ή πρόγραμμα υπολογιστή»

[162] Κ. Φράγκος, Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 370Δ, αρ. 2, Ενημέρωση:10/12/2019, sakkoulas-online

[163] Δαλακούρας Θ., Ηλεκτρονικό έγκλημα, 2023, σελ. 36 με περαιτέρω παραπομπή σε Μυλωνόπουλο, ό.π., 1991, σελ. 92 επ. κ.λπ.

[164] Ιδ. ΝαυτΠειρ 530/2003, ΠοινΧρ 2014, σελ. 75 επ., στην οποία μνημονεύεται ότι προασπίζονται τα προγράμματα ως αποτελέσματα οικονομικών επενδύσεων.

[165] Η πληροφορία αξιολογείται ως ένα νέο έννομο αγαθό στο χώρο του ποινικού δικαίου. Ειδικότερα, τα ηλεκτρονικά δεδομένα και τα συστήματα πληροφοριών έχουν αναδειχθεί πλέον σε αγαθά με τα οποία οι νόμιμοι κάτοχοί τους συνδέουν σημαντικά συμφέροντα. Το ελληνικό Σύνταγμα προστατεύει ρητά το δικαίωμα πρόσβασης στην πληροφορία στο άρθρο (άρθρο 5 Α του Σ). Α. Παπαδοπούλου, Το επιχειρηματικό απόρρητο, 2007, § 18, σ. 241 = sakkoulas-online με παραπομπή σε Μυλωνόπολου, ό.π. σελ. 83 αναφέρεται στη φράση του Fr. Bacon: «η γνώση είναι δύναμη»· για τη φύση της πληροφορίας, την οικονομική της αξία και για την πληροφορία από την άποψη της επικοινωνίας.

[166] Α. Ζήσης, Από τον πολιτικώς ενάγοντα στον παριστάμενο για την υποστήριξη της κατηγορίας, 2023, σ. 216 = sakkoulas-online

[167] Βλ. ΝαυτΠειρ 530/2003, ό.π., όπου, το Ελληνικό Δημόσιο, δήλωσε παράσταση πολιτικής αγωγής για ικανοποίηση ηθικής βλάβης, και τελικά κηρύχθηκε απαράδεκτη, λόγω έλλειψης ενεργητικής νομιμοποίησης και διατάχθηκε η αποβολή της πολιτικής αγωγής.

[168] Κιούπης Δ., Ποινικό δίκαιο και Internet, Ποινικά 57, 1999, σελ. 127

κατόχου. [169] Χρήζει αναφοράς και η άποψη ότι η παρ. 2 προστατεύει την ασφάλεια των ηλεκτρονικών πληροφοριών και το δικαίωμα του έχοντος την εξουσία διάθεσης επ' αυτών στην ακώλυτη και απόλυτη χρήση τους, η οποία εμπεριέχει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των στοιχείων. [170]

Επιπλέον, ως προς τον ειδικότερο τρόπο τέλεσης της αντιγραφής, έχει υποστηριχθεί ότι έννομο αγαθό αποτελεί και η πνευματική ιδιοκτησία. Αναφορικά με τον τρόπο τέλεσης της χρήσης, έχει προκριθεί και η προστασία της ιδιοκτησίας ως προστατευτέο έννομο αγαθό, με γνώμονα την υπ' αρ. ΝαυτΠειρ 530/2003 απόφαση. Στην προαναφερθείσα υπόθεση, μη εξουσιοδοτημένος προς τούτο κελευστής, εισήλθε στο γραφείο ανωτέρου του και χρησιμοποιώντας το νομίμως αποκτηθέν λογισμικό του υπολογιστή του, εκτύπωσε κάποια έγγραφα. Από την πράξη του καθίσταται αντιληπτό ότι δεν παραβίασε κάποιο δικαίωμα πνευματικής ιδιοκτησίας.[171]

5.2. Χαρακτηρολογικά γνωρίσματα του εγκλήματος

Το αδίκημα του άρθρου 370Δ ΠΚ συνιστά έγκλημα στιγμιαίο, ενεργείας, μη ιδιόχειρο και γνήσιο πολύτροπο ή διαζευκτικώς μικτό. Το αδίκημα είναι κοινό ως προς τις παραγράφους 1 και 2 και μη γνήσιο ιδιαίτερο ως προς την παράγραφο 3.[172]

Στην παράγραφο 1 το έγκλημα είναι βλάβης, ενώ στην παράγραφο 2 αφηρημένης διακινδύνευσης, καθώς η τυποποιημένη εγκληματική συμπεριφορά κρίνεται από τον νομοθέτη αυτή καθεαυτή επικίνδυνη για το έννομο αγαθό του απορρήτου του πληροφοριακού συστήματος και των μεταδιδόμενων με τηλεπικοινωνιακό σύστημα στοιχείων, χωρίς να απαιτείται από τον νόμο να επέλθει κάποιο εμπειρικό αποτέλεσμα κινδύνου. [173] Ωστόσο, έχει διατυπωθεί και η άποψη ότι στη παράγραφο 2 το αδίκημα διαπλάσσεται ως βλάβης, καθώς έχει επέλθει τρώση του εννόμου αγαθού ήδη με την πρόσβαση. [174]

Όπως προανεφέρθη και ανωτέρω, στα πλαίσια ανάλυσης του άρθρου 370Β ΠΚ, το αδίκημα του 370Δ ΠΚ χαρακτηρίζεται ως έγκλημα διατάραξης της ψηφιακής ειρήνης, καθώς προσιδιάζει με την παραβίαση της φυσικής εξουσίας τινός στην οικία του όπως προβλέπεται στο άρθρο 334 ΠΚ (διατάραξη οικιακής ειρήνης). [175]

---

[169] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2754

[170] Σπυρόπουλος Φ., Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking), 2016, σελ. 180

[171] Μεταξάκης Εμ., Κυβερνοέγκλημα, ό.π., 2022, σελ. 558- 559

[172] Κωστάρας Αλέξανδρος, Ποινικό Δίκαιο: Επιτομή Ειδικού Μέρους, (Νομική Βιβλιοθήκη 2014), σελ. 1153

[173] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2754

[174] Σπυρόπουλος Φ., Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking), 2016, σελ. 184

[175] Κιούπης Δ., Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, Υπερ. 2000, σελ. 970

5.3. Δομή και στοιχεία του εγκλήματος

Στο άρθρο 370Δ ΠΚ τυποποιούνται δυο αυτοτελή αδικήματα. Αφενός, (α) η άνευ δικαιώματος παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών, που επισύρει χρηματική ποινή ή παροχή κοινωφελούς εργασίας [176] (παρ.1) και αφετέρου (β) η χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα ή σε στοιχεία μεταδιδόμενα με συστήματα τηλεπικοινωνιών, που τιμωρείται με φυλάκιση (παρ. 2).

Από τη διάταξη του άρθρου 370Γ παρ. 2 του προϊσχύσαντος ΠΚ και 370 Δ παρ. 2 του ήδη ισχύοντος ΠΚ, προκύπτει ότι για τη στοιχειοθέτηση του εγκλήματος απαιτείται η πρόσβαση στα στοιχεία που μεταδίδονται με συστήματα πληροφοριών να γίνεται χωρίς δικαίωμα και δη με την παραβίαση των απαγορεύσεων ή μέτρων ασφαλείας που έχει θέσει ο νόμιμος κάτοχος όπως μεταξύ άλλων η καθιέρωση κωδικού (password), που καταδεικνύει τη βούληση του κατόχου να αποκλείσει άλλους από την πρόσβαση σ' αυτά. [177]

5.3.1. Η χωρίς δικαίωμα αντιγραφή ή χρήση προγραμμάτων υπολογιστών (άρθρο 370Δ παρ. 1 ΠΚ)

5.3.1.1 Αντικειμενική υπόσταση

Η φράση «χωρίς δικαίωμα» σημαίνει την απουσία οποιασδήποτε μορφής συγκαταθέσεως από μέρους του νομίμου κατόχου των προγραμμάτων, η οποία αποκλείει την αντικειμενική υπόσταση του εγκλήματος και δεν αίρει απλώς τον άδικο χαρακτήρα της πράξεως. [178]

Δεν τιμωρείται η πρόσβαση που έχει επιτραπεί κατόπιν εξουσιοδότησης από τον κάτοχο, επί παραδείγματι η εξουσιοδότηση να χρησιμοποιήσει το σύστημα ή μέρος του για σκοπούς ελέγχου του πληροφοριακού συστήματος. Επιπλέον, δεν είναι αξιόποινη η πρόσβαση σε ένα σύστημα Η/Υ, που επιτρέπει την ελεύθερη και ανοιχτή πρόσβαση στο κοινό, καθώς η πρόσβαση αυτή θεωρείται «με δικαίωμα.»[179]

Χρήζει επισήμανσης ότι το δικαίωμα διάθεσης του συστήματος δεν συνεπάγεται άνευ ετέρου την ύπαρξη δικαιώματος διάθεσης επί των δεδομένων. [180] Κατ' επέκταση, όταν το δικαίωμα διάθεσης ανήκει σε περισσότερα άτομα, χρειάζεται η συγκατάθεση όλων για την νομότυπη διάθεση του προγράμματος, άλλως η πράξη θεωρείται ότι τελείται χωρίς δικαίωμα.[181]

---

[176] Η κοινωφελής εργασία, ως κύρια ποινή, προβλέπεται στο άρθρο 55 ΠΚ, ωστόσο με τον Ν. 4623/2019 και συγκεκριμένα με το άρθρο 98 του εν λόγω νόμου, ορίζεται ότι «1 (α)ναστέλλεται η ισχύς των διατάξεων του Ποινικού Κώδικα, ο οποίος κυρώθηκε με τον Ν. 4619/2019 (Α' 95), κατά το μέρος που προβλέπουν την παροχή κοινωφελούς εργασίας είτε ως κύρια ποινή είτε ως μετατροπή στερητικής της ελευθερίας ποινής ή χρηματικής ποινής…». Βάσει της Αιτιολογικής « (η) αναστολή αυτή επιβάλλεται για να υπάρξει καλύτερη προετοιμασία των σχετικών διαδικασιών καθώς και διαβούλευση με τους αρμόδιους φορείς για την αποτελεσματικότερη εφαρμογή του νόμου».

[177] ΑΠ 954/2020

[178] Α. Ζήσης, Ποινικός Κώδικας, 2022, άρθ. 370Δ, σ. 741 = sakkoulas-online, και ΝαυτΠειρ 530/2003 ΠοινΧρ 2004, 75

[179] Convention on Cybercrime (ETS No. 185) Explanatory Report, https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf, σκέψη 47

[180] Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021, σελ. 478

[181] Φιλόπουλος Π., Ποινική Προστασία του Απορρήτου-Συστηματική Ερμηνεία Άρθρων 370-371 ΠΚ, 2015, σελ. 176

5.3.1.2. Δράστης του εγκλήματος

Με βάση τα προαναφερθέντα το αδίκημα συνιστά έγκλημα κοινό και κατ' επέκταση δράστης του εγκλήματος μπορεί να είναι ο οιοσδήποτε, ακόμη και εκείνος που εργάζεται για το νόμιμο κάτοχο του προγράμματος υπολογιστή, το οποίο χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί. [182]

5.3.1.3. Εγκληματική συμπεριφορά

Αναφορικά με την **εγκληματική συμπεριφορά** που στοιχειοθετεί ποινική ευθύνη δυνάμει του άρθρου 370Δ ΠΚ, πράξη προσβολής είναι η χωρίς δικαίωμα αντιγραφή προγράμματος υπολογιστή ή η χωρίς δικαίωμα χρήση τέτοιου προγράμματος.

Η διάταξη αυτή είναι η βάση για την ποινική προστασία του λογισμικού. Αντίστοιχα, η διάταξη του άρθρου 66 ν. 2121/1993 είναι η βασική διάταξη για την προστασία της πνευματικής ιδιοκτησίας, γενικά. Με βάση το άρθρο 66 ν. 2121/1993, όπως ισχύει σήμερα, τιμωρείται ποινικά, μεταξύ άλλων, η αναπαραγωγή ενός έργου που γίνεται άμεσα ή έμμεσα, προσωρινά ή μόνιμα, με οποιαδήποτε μορφή, εν όλω ή εν μέρει. Στο προϊσχύσαν δίκαιο, προβλεπόταν απαγόρευση του πολλαπλασιασμού με αντιγραφή (άρθρο 16 ν. 2378/20) και ο σχετικός όρος είχε στενότερο περιεχόμενο από τον αντίστοιχο όρο της αναπαραγωγής, στο ν. 2121/1993. Η ερμηνεία του όρου «αντιγραφή» στο άρθρο 370Δ παρ. 1 ΠΚ, θα πρέπει, συνεπώς, να λάβει χώρα κατ' αναλογία με τον αντίστοιχο όρο της της «αναπαραγωγής» του ν. 2121/1993. Ο ν. 2121/1993 δεν περιέχει έναν ορισμό της αναπαραγωγής και το κενό έρχεται να καλύψει η επιστήμη, ορίζοντας ως τέτοια την παραγωγή ενός ή περισσοτέρων σταθερών αντιτύπων ή αντιγράφων ενός έργου, η οποία το καθιστά προσιτό στις αισθήσεις άμεσα ή μέσω τεχνικών συσκευών. [183]

Ως αντιγραφή νοείται η ενσωμάτωση του στοιχείου ή του προγράμματος σε υλικό φορέα, ανεξαρτήτως αν γίνεται με ή χωρίς τεχνικά μέσα, όπως με σχεδιασμό, ή γραφή. Στην έννοια υπάγεται η μεταφορά ενός προγράμματος σε χαρτί, μαγνητικούς δίσκους, ταινίες, usb ή φορητό σκληρό δίσκο. [184] Στην έννοια της αντιγραφής εμπίπτει και η απλή αποθήκευση, εφόσον είναι σταθερή και επιτρέπει σε κάποιον την εκ νέου πρόσβαση στο πρόγραμμα.[185] Έτσι, αντιγραφή αποτελεί η μεταφορά προγραμμάτων σε χαρτί, μαγνητικούς ή οπτικούς δίσκους, όπως και η αποθήκευσή του σε μνήμη ενός υπολογιστή, ακόμα και όταν αυτή γίνεται προσωρινά. [186]

Στο σημείο αυτό δέον να διευκρινιστεί ότι η τέλεση του αδικήματος υπό αυτό το τρόπο δεν συνεπάγεται αυτοδίκαια και ότι έχει λάβει γνώση των δεδομένων ο δράστης. [187]

Πέρα από την αντιγραφή, ο νόμος απαγορεύει και τη **χρήση** ενός προγράμματος η/υ χωρίς δικαίωμα. Εδώ εμπίπτει η εκτέλεση του λογισμικού από το σύστημα επεξεργασίας του υπολογιστή, φόρτωση του προγράμματος στη μνήμη RAM κ.ο.κ., ενώ δεν εμπίπτει η απλή

---

[182] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2755

[183] Βλ. Μαρίνου, Πνευματική ιδιοκτησία, σελ. 152· επίσης, βλ. Κουμάντου, Πνευματική ιδιοκτησία, σελ. 218, ο οποίος ορίζει την αναπαραγωγή ως την παραγωγή νέων υλικών υποστρωμάτων όπου επαναλαμβάνεται η αρχική ενσωμάτωση του έργου

[184] Βασιλάκη, ό.π., σελ. 115

[185] Φιλόπουλος Π., Ποινική Προστασία του Απορρήτου-Συστηματική Ερμηνεία Άρθρων 370-371 ΠΚ, 2015, σελ. 175

[186] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 414, αρ. 678 = sakkoulas-online

[187] Κιούπης Δ., Ποινικό δίκαιο και Internet, Ποινικά 57, 1999, σελ. 129

παραλαβή από τρίτο των υλικών φορέων του λογισμικού, η οποία αποτελεί προπαρασκευαστική πράξη που δεν τιμωρείται, το ίδιο όπως και η μελέτη του συνοδευτικού υλικού ή της περιγραφής του προγράμματος.[188] Ως χρήση από την άλλη νοείται ακόμα και η απλή εκτέλεση του προγράμματος, κατά την οποία ο δράστης εκτύπωσε κάποια έγγραφα. [189] Έχει κριθεί νομολογιακά ως χρησιμοποίηση του προγράμματος και η πώλησή του σε τρίτους.[190]

Δεν θεωρείται χρήση η απλή παραλαβή των υλικών φορέων που περιέχουν λογισμικό. Αν υπάρχει συγκατάθεση του δικαιούχου του προγράμματος δεν τελείται το αδίκημα. [191]

Αξιόποινη κατά την παρ. 1 είναι και η λεγόμενη κλοπή χρόνου (time theft), δηλ. όταν ο χρήστης συστήματος πληροφορικής, χρησιμοποιεί τον ηλεκτρονικό υπολογιστή για διεκπεραίωση υποθέσεων που δεν ανήκουν στον κύκλο των εργασιών του εργοδότη του [192]

Στον τρόπο τέλεσης της χρήσης Η/Υ εμπίπτει μεταξύ άλλων, η τροποποίηση λογισμικού, η οποία όμως τιμωρείται και κατά τις διατάξεις της πνευματικής ιδιοκτησίας (άρ. 66 Ν. 2121/1993), καθώς προσβάλλει το δικαίωμα του δημιουργού και η μεταβίβασή του, που πλήττει έμμεσα το περιουσιακό δικαίωμα του δικαιούχου.193

Υλικό αντικείμενο επίθεσης είναι μόνο τα προγράμματα Η/Υ και όχι τα στοιχεία ως τέτοια.

Πρόγραμμα είναι μία ενότητα οδηγιών και κανονισμών που περιέχουν τα αναγκαία στοιχεία για τη λύση ενός προβλήματος [πηγαίο πρόγραμμα –Source programm γραμμένο σε γλώσσες Basic, Cobol, Fortan κ.λπ.– και αντικειμενικό πρόγραμμα –object programm– που προέρχεται από ένα μεταγλωττιστή.[194] Ειδικότερα, ως πρόγραμμα (πρόγραμμα εφαρμογών και πρόγραμμα βάσης) νοείται ένα σύνολο, ικανό, όταν ενσωματωθεί σε ένα μέσο που μπορεί να αναγνωσθεί από μία μηχανή, να οδηγήσει τη μηχανή που έχει δυνατότητα επεξεργασίας πληροφοριών στην υπόδειξη, παράσταση και επίτευξη μιας συγκεκριμένης λειτουργίας, αποστολής ή αποτελέσματος.[195] Στην έννοια των προγραμμάτων Η/Υ εμπίπτουν όλες οι πληροφορίες που έχουν αποθηκευτεί ψηφιακά, ειδικότερα τα δεδομένα μουσικής (όπως λ.χ. avi-, mpg-, vcd-, svcdδεδομένα και άλλα δεδομένα, εφόσον πληρούνται οι λοιπές προϋποθέσεις). [196]

Είναι αδιάφορο, αν το πρόγραμμα είναι απόρρητο, δηλ. αν έχει γνωστοποιηθεί. Ούτε απαιτείται να είναι πρωτότυπο ή να έχει δημιουργικό ύφος, ώστε να θεωρηθεί έργο κατά το δίκαιο της πνευματικής ιδιοκτησίας ή εφεύρεση ή πνευματική δημιουργία. [197]

---

[188] Ι. Ιγγλεζάκης, Δίκαιο Πληροφορικής, 4η έκδ., 2021, σ. 414, αρ. 679 = sakkoulas-online

[189] Μιχαήλ Μαργαρίτης and Άντα Μαργαρίτη, ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ Ερμηνεία – Εφαρμογές (4η, Π Ν Σάκκουλας 2020). Σελ. 1087 με παραπομπή στην απόφαση ΝαυτΠειρ 530/2003 ΠοινΧρ 2004, 75

[190] ΣυμβΠλημΘεσσ 3204/2003

[191] ΝαυτΠειρ 3204/1993 από Α. Ζήσης, Ποινικός Κώδικας, 2022, άρθ. 370Δ, σ. 742 = sakkoulas-online

[192] Π. Φιλόπουλος, Ποινική Προστασία Απορρήτου, 2015, άρθ. 370Γ, σ. 177, αρ. 13 = sakkoulas-online

[193] Ιγγλεζάκης Ι., Δίκαιο της Πληροφορικής, 4η έκδ., 2021, σελ. 414

[194] Βασιλάκη, ό.π., 98 επ., με τη διάκριση σε προγράμματα συστημάτων, προγράμματα εφαρμογών, πηγαίο πρόγραμμα, ατομικά προγράμματα και προγράμματα για πολλούς χρήστες

[195] Μυλωνόπουλου, ΠοινΧρ 1998, 3· εδώ περιλαμβάνονται όχι μόνο τα προγράμματα που φτιάχτηκαν σε μία νέα εγκατάσταση, αλλά και όσα αναπλάστηκαν (έτσι η Schlüchter, Wirtschaftskriminalität, σ.88)

[196] MK-Graf, 2003, § 202 a, αρ. 9

[197] ΣυμβΠλημΘεσ 3201/1993, Υπερ. 1994, 1137· ά.ά. ο Μυλωνόπουλος, Ποινικά, σ. 88, με γνώμονα το συνταγματικό κανόνα που κατοχυρώνει την ελεύθερη ανάπτυξη της προσωπικότητας· προς την ίδια κατεύθυνση η κριτική του Μαρίνου, Software, Ι, σ. 87

Η ratio της διάταξης ερείδεται στη μεγάλη δαπάνη που απαιτείται για την ανάπτυξη των προγραμμάτων.[198] Όμως δεν απαιτείται οικονομική αξία των προγραμμάτων.

Υφίσταται διχογνωμία αναφορικά με το εάν το εν λόγω πρόγραμμα πρέπει να είναι έργο πρωτότυπο, ήτοι προσωπικό δημιούργημα ως αποτέλεσμα της προσωπικής, πνευματικής του εργασίας και να εμπίπτει στην προστασία του νόμου για την πνευματική ιδιοκτησία ως έργο λόγου (ή διάνοιας). [199] Η επιχειρηματολογία υπέρ αυτής της άποψης στηρίζεται στην παραδοχή ότι ένα έργο που δεν συγκεντρώνει τα χαρακτηριστικά του έργου λόγου είναι ελεύθερο, με βάση την διεθνώς αναγνωρισμένη αρχή της ελεύθερης ροής της πληροφορίας και του διεθνούς και ευρωπαϊκού πλαισίου για την πνευματική ιδιοκτησία. [200] Ωστόσο, αντικρούεται η εν λόγω θέση με το επιχείρημα ότι εφόσον ο νόμος δεν διακρίνει σχετικά, πρέπει να προστατεύεται οποιοδήποτε είδος προγράμματος, ανεξάρτητα από την ιδιότητά του ως «έργου» κατά τις διατάξεις του Ν. 2121/1993. [201]

5.3.2. Η χωρίς δικαίωμα πρόσβαση σε πληροφοριακό σύστημα ή σε στοιχεία μεταδιδόμενα με συστήματα τηλεπικοινωνιών (370Δ παρ. 2 ΠΚ)

Το αδίκημα του άρθρου προσομοιάζει με την αντικειμενική υπόσταση του αδικήματος 370Β παρ. 1 ΠΚ με κύριες διαφορές ότι στο υπό εξέταση αδίκημα δεν απαιτείται η υπερκέραση μέτρων προστασίας αφενός και αφετέρου εν προκειμένω δεν γίνεται αναφορά σε ηλεκτρονικά δεδομένα. Το άρθρο ποινικοποιεί κάθε είδους πρόσβαση σε συστήματα πληροφοριών και δη το “hacking” που λαμβάνει χώρα χωρίς άδεια του νόμιμου δικαιούχου, ανεξάρτητα από το σκοπό του δράστη ή την επέλευση ή μη της ζημίας.

---

[198] Βασιλάκη, ό.π., σ. 96, 103 με αναφορά στην ΕισΕκθ Ν. 1805/1988

[199] Άρθρο 2 παρ. 3 Ν. 2121/1993, όπως διαμορφώθηκε ως άνω με το άρθρο 53 παρ. 1 του Ν.4961/2022 (ΦΕΚ Α 146/27.07.2022.) : «3. Με την επιφύλαξη των διατάξεων του Κεφαλαίου 7 του παρόντος νόμου, θεωρούνται ως έργα λόγου προστατευόμενα κατά τις διατάξεις περί πνευματικής ιδιοκτησίας τα προγράμματα ηλεκτρονικών υπολογιστών και το προπαρασκευαστικό υλικό του σχεδιασμού τους. Η προστασία παρέχεται σε κάθε μορφή έκφρασης ενός προγράμματος ηλεκτρονικού υπολογιστή. Οι ιδέες και οι αρχές στις οποίες βασίζεται οποιοδήποτε στοιχείο προγράμματος ηλεκτρονικού υπολογιστή, περιλαμβανομένων και εκείνων στις οποίες βασίζονται τα συστήματα διασύνδεσής του, δεν προστατεύονται κατά τον παρόντα νόμο. Ένα πρόγραμμα ηλεκτρονικού υπολογιστή θεωρείται πρωτότυπο εφόσον είναι προσωπικό πνευματικό δημιούργημα του δημιουργού του. Αντικείμενο προστασίας είναι και το ψηφιακό αρχείο σχεδιασμού με τη βοήθεια ηλεκτρονικού υπολογιστή (Computer Aided Design File - C.A.D. File), εφόσον περιλαμβάνει πηγαίο κώδικα.»»

[200] Σύμφωνα με το Μυλωνόπουλο, ό.π. (Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο), σελ. 88, η αντίθετη άποψη θα οδηγούσε σε υπερβολική διεύρυνση του αξιοποίνου και σε δικαιοσυστηματικές αντιφάσεις, καθώς πώς η αντιγραφή ενός κοινότυπου προγράμματος επιτρέπεται από το Δίκαιο της Πνευματικής Ιδιοκτησίας, αλλά απαγορεύεται από τη διάταξη 370Δ ΠΚ; Διεθνώς υπόψη η Σύμβαση της Στοκχόλμης 1967 για τη για τη σύσταση παγκόσμιας οργάνωσης προστασίας της ιδιοκτησίας επί των έργων διανοίας, Σύμβαση της Βέρνης. Ευρωπαϊκό πλαίσιο υπόψη ο Κανονισμός (ΕΕ) 2018/1807 για την ελεύθερη ροή δεδομένων μη προσωπικού χαρακτήρα και Κανονισμός (ΕΕ) 2015/2120 (θέσπιση μέτρων για την πρόσβαση στο διαδίκτυο).

[201] Βασιλάκη, ό.π., σελ. 96, με πρόσθετο επιχείρημα απορρέον από την Εισηγητική Έκθεση του Ν. 1805/88, όπου αναφέρεται ότι θέσπιση της εν λόγω διάταξης κρίθηκε αναγκαία, λόγω της μεγάλης δαπάνης που απαιτείται για την παραγωγή προγραμμάτων καθώς και του μεγάλου ανταγωνισμού που επικρατεί στο χώρο αυτό. Η διάταξη δεν επιτελεί συμπληρωματική ρύθμιση του δικαίου της πνευματικής ιδιοκτησίας, παρέχεται ήγουν μια sui generis προστασία του λογισμικού ενός υπολογιστή κατά τις προτάσεις της WIPO (World Intellectual Property Organization) και δη publication Nr 814 Genf 1978 σελ. 7 επ. https://www.wipo.int/edocs/pubdocs/en/copyright/120/wipo_pub_120_1978_01.pdf

5.3.2.1. Δράστης

Δράστης του εγκλήματος της παραγράφου 2 του άρθρου 370Δ ΠΚ καταρχήν μπορεί να είναι οιοσδήποτε. Αν ωστόσο ο δράστης βρίσκεται στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη τιμωρείται μόνο εφόσον η πρόσβαση απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του, δυνάμει της τρίτης παραγράφου του άρθρου. [202]

5.3.2.2. Υλικό αντικείμενο

Εν προκειμένω, υλικό αντικείμενο του εγκλήματος συνιστά το σύνολο η τμήμα πληροφοριακού συστήματος ή τα στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνίων. Προστατεύονται και τα ψηφιακά δεδομένα, τα οποία εντάσσονται στην έννοια του πληροφοριακού συστήματος. [203]

Η χωρίς δικαίωμα παρακολούθηση εκπομπών σε ένα PC της επί πληρωμή τηλεόρασης μέσω internet, λ.χ. με μία πειρατική κάρτα, συνιστά χωρίς δικαίωμα πρόσβαση σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών.[204]

Τα στοιχεία αυτά συνιστούν πληροφοριακά δεδομένα, ή άλλως πληροφορίες, τα οποία μεταδίδονται με ένα σύστημα τηλεπικοινωνίας. Ως τηλεπικοινωνία νοείται κάθε μορφή ενσύρματης ή ασύρματης, ηλεκτρικής, ηλεκτρομαγνητικής, ακουστικής ή οπτικής επικοινωνίας που πραγματοποιείται ανεξαρτήτως απόστασης, μέσω κατάλληλων συσκευών, όπως το τηλέφωνο, το ραδιοτηλέφωνο, ο ασύρματος, το τηλέτυπο, το φαξ, το ραδιόφωνο, η τηλεόραση κ.λπ.. Αυτές οι συσκευές, συνδέονται μεταξύ τους με δίκτυα. Ένα σύστημα τηλεπικοινωνιών περιλαμβάνει τον πομπό που μετατρέπει την πληροφορία από φυσική σε ηλεκτρική μορφή, την κωδικοποιεί και τη διαμορφώνει καταλλήλως προκειμένου να διασχίσει με τη μορφή σήματος ένα κανάλι και να καταλήξει στο δέκτη της, όπου αποκωδικοποιείται.[205] Επομένως, οποιαδήποτε πρόσβαση σε πληροφοριακά συστήματα τα οποία μεταδίδονται μέσω ενός τηλεπικοινωνιακού συστήματος κατά τον προαναφερόμενο τρόπο, εμπίπτει στο πεδίο εφαρμογής του άρθρου 370Δ παρ. 2 ΠΚ.

Άξια αναφοράς κρίνεται η ιδιαίτερη σύνδεση της 292Α ΠΚ με τη χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα, η οποία εντοπίζεται στην αναφορά της αντικειμενικής υπόστασης της διάταξης σε σύστημα λογισμικού. Το «λογισμικό» (software) αποτελεί ουσιαστικά το πρόγραμμα βάσει του οποίου λειτουργούν οι υπολογιστές του παρόχου αναφορικά με τις υπηρεσίες που παρέχουν.[206] Ειδικότερα, λειτουργικό σύστημα (Operating System ή OS) ονομάζεται στην επιστήμη της πληροφορικής το λογισμικό του υπολογιστή που είναι υπεύθυνο για τη διαχείριση και τον συντονισμό των εργασιών, καθώς και την κατανομή των διαθέσιμων πόρων. Το λειτουργικό σύστημα παρέχει ένα θεμέλιο, ένα μεσολαβητικό επίπεδο λογικής διασύνδεσης μεταξύ λογισμικού και υλικού, διαμέσου του οποίου οι εφαρμογές αντιλαμβάνονται εμμέσως τον υπολογιστή. Στο βαθμό που οι τηλεπικοινωνίες (όπως περιορίστηκε η εφαρμογή της διάταξης ανωτέρω) παρέχονται και ασκείται η όποια διαχείρισή τους μέσω ηλεκτρονικών προγραμμάτων (π.χ. το γνωστό πρόγραμμα “skype”),

[202] Η ανάλυση επί της απαίτησης έγγραφης και σαφούς απαγόρευσης είναι όμοια με αυτή της ανάλυσης της παραγράφου 2 του άρθρου 370Β ΠΚ.

[203] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2757

[204] Π. Φιλόπουλος, Ποινική Προστασία Απορρήτου, 2015, άρθ. 370Γ, σ. 187, αρ. 26 = sakkoulas-online

[205] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2757

[206] Γ. Ζέκος, Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, 2022, σ. 450 = sakkoulas-online

τότε πράγματι μιλούμε για ηλεκτρονικές πληροφορίες των οποίων η προστασία καλύπτεται από τη διάταξη του άρθρο 292Α ΠΚ.[207]

Περιπτώσεις υπαγόμενες στον εν λόγω κυρωτικό κανόνα συνιστούν, κατεξοχήν, το "hacking", που ορίζεται ως η χωρίς δικαίωμα πρόσβαση σε σύνολο ή τμήμα πληροφοριακού συστήματος, η παραβίαση τράπεζας δεδομένων («databank»), το cracking που είναι το «σπάσιμο» προγραμμάτων ασφαλείας και το «pharming».

Παράδειγμα που θα ενέπιπτε στην εν λόγω νομοτυπική υπόσταση συνιστά η επίτευξη λήψης των στοιχείων σύνδεσης έξυπνου κινητού (smart phone) μέσω απατηλού σύντομου μηνύματος (phishing sms)[208], τα οποία εν συνεχεία ο δράστης χρησιμοποιεί για να αποκτήσει πρόσβαση στα πληροφοριακά δεδομένα του συγκεκριμένου κινητού. [209]

Ο δράστης μπορεί επίσης να παρεισφρήσει στην επικοινωνία και να τροποποιήσει τα μεταδιδόμενα δεδομένα , να υποκλέψει τα στοιχεία πρόσβασης των επικοινωνούντων ή να αποκρυπτογραφήσει τα δεδομένα που διακινούνται και να πληροφορηθεί το περιεχόμενό τους. [210]

5.4. Υποκειμενική υπόσταση

Ελλείψει ειδικής αναφοράς σε αμφότερες τις παραγράφους βάσει των διατάξεων 18, 26 και 27 ΠΚ, απαιτείται δόλος, αρκούντος και του ενδεχόμενου, που πρέπει να επικαλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

5.5. Ποινικές κυρώσεις

Τα αδικήματα της παραγράφου 1 του άρθρου 370Δ ΠΚ επισύρει χρηματική ποινή (άρθρο 57 ΠΚ), ενώ το αδίκημα της παραγράφου 2 επαπειλεί ποινή φυλάκισης (53 ΠΚ) από 10 ημέρες έως 5 έτη.

Τα αδικήματα του άρθρου 370Δ ΠΚ, που τελούνται μετά την έναρξη ισχύος του νέου Ποινικού Κώδικα (1.7.2019), διώκονται αυτεπαγγέλτως. Όσα όμως τελέστηκαν μέχρι και πριν την ως άνω ημερομηνία διώκονται αποκλειστικά κατ' έγκληση του παθόντος -νόμιμου κατόχου του προγράμματος ηλεκτρονικού υπολογιστή (παρ.1) ή του πληροφοριακού συστήματος ή των μεταδιδόμενων στοιχείων (παρ. 2) κατ' εφαρμογή της παραγράφου 4 του άρθρου 370Γ πΠΚ, η οποία είναι ευμενέστερη για το κατηγορούμενο και βάσει του 2 ΠΚ εφαρμόζεται.

---

[207] Φαινομενική συρροή της διάταξης του άρθρο 292Α παρ. 1 α΄ ΠΚ με τη διάταξη του άρθρο 370Γ παρ. 2 ΠΚ. Το έννομο αγαθό που προστατεύεται από το άρθρο 292Α είναι το υπερατομικό έννομο αγαθό του απορρήτου των επικοινωνιών. Επομένως, σε περίπτωση πρόσβασης σε λογισμικό παροχής υπηρεσιών τηλεφωνίας θα εφαρμοστεί το άρθρο 292Α παρ. 1α΄ ΠΚ ως ειδικότερη της διάταξης του άρθρο 370Γ παρ. 2 ΠΚ (αρχή της ειδικότητας) – στις υπόλοιπες περιπτώσεις (π.χ. σε λογισμικό που δεν χρησιμοποιείται από πάροχο τηλεφωνικών υπηρεσιών για την παροχή των υπηρεσιών αυτών) εφαρμογής τυγχάνει το άρθρο 370Γ παρ. 2. Γ. Ζέκος, Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, 2022, σ. 451 = sakkoulas-online

[208] Ή άλλως "smishing", που ένας συνδυασμός των λέξεων "SMS" -ή "short message service", της τεχνολογίας που βρίσκεται πίσω από τα μηνύματα κειμένου- και "phishing". Το Smishing είναι μια επίθεση κοινωνικής μηχανικής που χρησιμοποιεί ψεύτικα μηνύματα κειμένου στο κινητό για να εξαπατήσει τους χρήστες ώστε να κατεβάσουν κακόβουλο λογισμικό, να μοιραστούν ευαίσθητες πληροφορίες ή να στείλουν χρήματα σε εγκληματίες του κυβερνοχώρου. (https://www.ibm.com/topics/smishing)

[209] Καμπέρου, ό.π. σελ. 2758

[210] Μαυρίδης, Ασφάλεια πληροφοριών στο διαδίκτυο, 2015, σελ. 62 επ. (https://repository.kallipos.gr/bitstream/11419/1024/3/00_master_document-KOY.pdf)

5.6. Ειδικές μορφές εμφάνισης των εν 370Δ προβλεπόμενων αδικημάτων

5.6.1. Απόπειρα

Τα αδικήματα των παραγράφων 1 και 2 δύνανται να παραμείνουν στο στάδιο της απόπειρας. Φέρ' ειπείν, παραμένει το αδίκημα της παραγράφου 1 σε στάδιο απόπειρας όταν ο δράστης ξεκίνησε να αντιγράφει σε υλικό φορέα λ.χ. σε στικάκι «usb» το πρόγραμμα, αλλά δεν ολοκλήρωσε την εγγραφή, διότι έγινε αντιληπτός από τρίτο.

5.6.2. Συμμετοχή

Κάθε μορφή συμμετοχής είναι δυνατή στα εγκλήματα των άρθρων 370Δ ΠΚ.

5.6.3. Συρροές

Λόγω της ετερότητας των εννόμων αγαθών υφίσταται κατ' ιδέα αληθής συρροή μεταξύ των εγκλημάτων της **πλαστογραφίας** (216 ΠΚ) και της παραβάσεως του άρθρου 370Δ ΠΚ. [211]

Όσον αφορά στο είδος της συρροής μεταξύ των εγκλημάτων της **κλοπής πνευματικής ιδιοκτησίας** και της παραβάσεως του άρθρου 370Δ ΠΚ, προκρίνεται ότι ομοίως υφίσταται αληθής, κατ' ιδέα η συρροή λόγω ακριβώς της ετερότητας των πληττομένων αγαθών αφού στην περίπτωση της παραβάσεως του άρθρου 370Δ ΠΚ, το προστατευόμενο έννομο αγαθό αποτελεί το περιουσιακό αγαθό της πληροφορίας όπως ευρίσκεται στο λογισμικό ενός υπολογιστή. [212]

Με την ίδια λογική, αληθινή κατ' ιδέαν ορίζεται και η συρροή με το αδίκημα της εκβίασης (385 ΠΚ), αν ο δράστης – χρήστης του διαδικτύου απέκτησε χωρίς δικαίωμα πρόσβαση στο πληροφοριακό σύστημα του παθόντος, κρυπτογράφησε τα αρχεία του συστήματος και στη συνέχεια εκβίασε τον παθόντα για να του αποστείλει κωδικούς και οδηγίες αποκρυπτογράφησης.

Αναφορικά με τη σχέση του άρθρου 370Δ ΠΚ με το άρθρο 370Ε ΠΚ, όταν πρόκειται για παράνομη πρόσβαση, με τη μορφή της παρακολούθησης, της αποτύπωσης σε υλικό φορέα (παρ.1) ή παρέμβασης, σε ηλεκτρονική αλληλογραφία (e mail) κατά το χρόνο που αυτή διαβιβάζεται από τον αποστολέα προς τον παραλήπτη και αποδεικνύεται ότι ο δράστης είχε σκοπό να πληροφορηθεί το περιεχόμενό της, εφαρμόζεται μόνον η αυστηρότερη διάταξη του άρθρου 370Ε παρ. 1 ως ειδική, έναντι τόσο εκείνης του άρθρου 370Δ ΠΚ παρ. 2 ΠΚ, η οποία δεν απαιτεί τον επιπρόσθετο σκοπό πληροφόρησης του περιεχομένου της μεταδιδόμενης ηλεκτρονικής αλληλογραφίας, όσο και έναντι εκείνης του άρθρου 370Γ παρ. 2 ΠΚ, η οποία δεν εφαρμόζεται όταν το ηλεκτρονικό μήνυμα «υποκλέπτεται» κατά το χρόνο που διαβιβάζεται. [213]

Όσον αφορά τη σχέση του άρθρου 370Δ παρ. 2 εδ. α' ΠΚ με το άρθρο 370Β παρ. 1 εδ. α' ΠΚ, όταν υλικό αντικείμενο του εγκλήματος είναι το σύνολο ή τμήμα του πληροφοριακού συστήματος, συρρέουν φαινομενικά κατ' ιδέαν και εφαρμόζεται το άρθρο 370Δ παρ. 2 εδ. α' ΠΚ, με βάση την αρχή της σιωπηρής επικουρικότητας που υπερισχύει το αδίκημα που απειλεί βαρύτερη ποινή.

---

[211] ΣυμβΠλημΘες 3204/1993 Υπερ 1994, σελ. 1133

[212] ΣυμβΠλημΘεσ 3204/1993 Υπερ 1994, 1133 από Α. Ζήσης, Ποινικός Κώδικας, 2022, άρθ. 370Δ, σ. 742 = sakkoulas-online)

[213] Καμπέρου, ό.π. σελ. 2759

6. Το αδίκημα της παράνομης υποκλοπής δεδομένων (37ΟΕ ΠΚ)

Το αδίκημα της υποκλοπής δεδομένων, που εδράζεται στο άρθρο 37ΟΕ ΠΚ, βρίσκεται σε συστοιχία με το άρθρο 3 της Σύμβασης της Βουδαπέστης και το άρθρο 6 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

Βάσει του άρθρου 3 της Σύμβασης, τα κράτη μέλη κλήθηκαν να ποινικοποιήσουν την μέσω τεχνικών μέσων και άνευ εξουσιοδοτήσεως υποκλοπή που αφορά μη δημόσιες διαβιβάσεις των δεδομένων υπολογιστή από, προς ή εντός ενός πληροφοριακού συστήματος, συμπεριλαμβανομένων και των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστή που περιέχει ηλεκτρονικά δεδομένα. [214]

Το άρθρο 370Ε υπέστη εκ βάθρων αναδιαμόρφωση με το άρθρο 11 του Ν.5002/2022 (ΦΕΚ Α` 228/09.12.2022). Η σπουδαία διαφοροποίηση που επέφερε ο ως άνω νόμος συνίσταται στην αναβίβαση της εγκληματικής συμπεριφοράς της παραβίασης των μη δημόσιων διαβιβάσεων δεδομένων ή ηλεκτρομαγνητικών δεδομένων σε κακούργημα (ο νομοθέτης επενέβη κατ' όμοιο τρόπο και στο άρθρο 370Α ΠΚ όπου τυποποιείται το αδίκημα της παραβίασης του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας).[215]

Το νομοθετικό κείμενο του άρθρου 370Ε έχει το ακόλουθο περιεχόμενο:

1. Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.

2. Με την ποινή της παραγράφου 1 τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπεται στην παράγραφο 1.

3. Αν οι πράξεις των παραγράφων 1 και 2 συνιστούν παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου, επιβάλλεται κάθειρξη.

6.1. Προστατευόμενο έννομο αγαθό

Αναφορικά με το σκοπό της διάταξης του άρθρου 370Ε ΠΚ, δεν υφίσταται ομοφωνία και οι απόψεις διίστανται, έχοντας ωστόσο όλες την ίδια αφετηρία. Συγκεκριμένα, σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης της Βουδαπέστης, η διάταξη προστατεύει το δικαίωμα του απορρήτου της επικοινωνίας δεδομένων, υπό την έννοια του δικαιώματος του προσώπου

[214] Η Σύμβαση της Βουδαπέστης προσπελάσιμη στον ακόλουθο σύνδεσμο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32013L0040 accessed 18 September 2023.

[215] Η επιλογή του νομοθέτη να αναβιβάσει εκ νέου το αδίκημα σε κακούργημα επικρίνεται από τη θεωρία κυρίως διότι η εν λόγω παλινδρόμηση εγείρει ζητήματα αναλογικότητας και ασφάλειας δικαίου. Βλ. Θεοχάρη Δαλακούρα, Ορισμοί και ουσιαστικές διατάξεις ποινικής αντιμετώπισης του ηλεκτρονικού εγκλήματος σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα - Ουσιαστικές και δικονομικές όψεις, 2η έκδοση, (Νομική Βιβλιοθήκη 2023), σελ. 38

που επικοινωνεί στη μη δημόσια διαβίβαση των δεδομένων του (non-public transmission of computer data). [216]

Κατά μια άλλη θεώρηση, με το έγκλημα της υποκλοπής δεδομένων προσβάλλεται το συμφέρον διατήρησης του τυπικού απορρήτου του έχοντος την εξουσία διαθέσεως των δεδομένων, εντασσόμενο στο γενικότερο δικαίωμα μη δημοσιότητας της ιδιωτικής επικοινωνίας, με αναγωγή στο συνταγματικά κατοχυρωμένο δικαίωμα, στο άρθρο 19 παρ. 1 Συντ., του εμπιστευτικού χαρακτήρα του περιεχομένου της επικοινωνίας. [217] Η εν λόγω ωστόσο θεώρηση περιορίζει την προστατευτική εμβέλεια της διάταξης εξίσου.

Αντίστοιχα υποστηρίζεται και η άποψη που προάγει το συμφέρον διατήρησης τυπικού απορρήτου του έχοντος την εξουσία διαθέσεως των δεδομένων, ως έκφανση του δικαιώματος μη δημοσιότητας της ιδιωτικής επικοινωνίας. [218]

Το προστατευόμενο έννομο αγαθό της υπό εξέταση διάταξης σύμφωνα με τη σύγχρονη θεώρηση συνίσταται στην ευρύτερη προστασία του απορρήτου των επικοινωνιών και δεδομένων, (καθώς δεν συνιστά απλώς ένα νομοθετικό σύστοιχο της διάταξης του άρθρου 370Α ΠΚ) που είναι η ασφάλεια του διαχειριζόμενου συστήματος και των δεδομένων του δικαιούχου, τόσο κατά το χρονικό στάδιο διαβίβασής τους σε άλλο πληροφοριακό σύστημα όσο και κατά την εσωτερική τους επεξεργασίας. Η ασφάλεια αυτή ερείδεται στην εμπιστευτικότητα (confidentiality), που επιτελείται μέσω της μη δημόσιας διαβίβασης των δεδομένων και στην ακεραιότητα (integrity), που συνίσταται σε μη τροποποίηση της ταυτότητας των διαχειριζομένων δεδομένων. [219]

---

[216] Convention on Cybercrime (ETS No. 185) Explanatory Report, https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf , σκέψη 51, όπου ορίζεται επί λέξει «Η διάταξη αυτή αποσκοπεί στην προστασία του δικαιώματος προστασίας της ιδιωτικής ζωής της επικοινωνίας δεδομένων. Το αδίκημα έχει την ίδια απαξία όπως η παραβίαση του απορρήτου των επικοινωνιών με την παραδοσιακή υποκλοπή και καταγραφή προφορικών τηλεφωνικών συνδιαλέξεων μεταξύ προσώπων. Το δικαίωμα του απορρήτου της αλληλογραφίας κατοχυρώνεται στο άρθρο 8 της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα. Το αδίκημα που θεσπίζεται βάσει του άρθρου 3 εφαρμόζει την αρχή αυτή σε όλες τις μορφές ηλεκτρονικής διαβίβασης δεδομένων, είτε μέσω τηλεφώνου, φαξ, ηλεκτρονικού ταχυδρομείου ή μεταφοράς αρχείων.»
Την εν λόγω θέση ασπάζεται και ο Θ. Δαλακούρας, ό.π. σελ. 37

[217] Ελένη Καμπέρου σε Αριστοτέλης Χαραλαμπάκης and Ελένη Καμπέρου (eds), *Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469*, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2761

[218] Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021, σελ. 473

[219] Παναγιώτης Τουργέλης, 'Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων: συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ' (Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ), Σχολή Νομικής 2022) 279 <http://didaktorika.gr/eadd/handle/10442/52558> . Ο ως άνω συγγραφεύς προς τεκμηρίωση της άποψής του (ότι προστατεύεται η εμπιστευτικότητα και η διαθεσιμότητα μέσω της ποινικοποίησης), παραπέμπει στο επίσημο κείμενο της Συγκριτικής Μελέτης του ΟΗΕ για την αντιμετώπιση του κυβερνοεγκλήματος, όπου χαρακτηριστικά αναφέρεται ότι «η ποινικοποίηση της παράνομης υποκλοπής επεκτείνει την προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων υπολογιστών από τα δεδομένα που βρίσκονται σε ένα σύστημα σε όλα τα μεταδιδόμενα δεδομένα» Ομοίως και Ε. Μεταξάκης, ο οποίος συμπεριλαμβάνει και τη διαθεσιμότητα των δεδομένων και συστημάτων υπολογιστών ως προστατευόμενο έννομο αγαθό σε ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ Βασικές έννοιες – Ερμηνεία διεθνούς, ενωσιακής και ημεδαπής νομοθεσίας – Τυπολογία, (Π. Ν. Σάκκουλας 2022) σελ. 557

6.2. Χαρακτηρολογικά γνωρίσματα του εγκλήματος

Το αδίκημα της υποκλοπής δεδομένων συνιστά κοινό έγκλημα, καθόσον δράστης μπορεί να είναι οποιοσδήποτε, εκτός του δικαιούχου διαχείρισης του πληροφοριακού συστήματος και των δεδομένων.

Επιπρόσθετα το αδίκημα χαρακτηρίζεται ως γνήσιο πολύτροπο ή άλλως υπαλλακτικώς μικτό, δεδομένου ότι οι πλείονες τρόποι τέλεσης (παρακολούθηση, αποτύπωση, παρέμβαση) μπορούν να εναλλαχθούν και παρά ταύτα ο δράστης θα τιμωρηθεί μία φορά.

Πρόκειται επίσης για έγκλημα απλής συμπεριφοράς, αφού η ηθικοκοινωνική απαξία της συμπεριφοράς εντοπίζεται ήδη στην πράξη με την οποία ο δράστης προσβάλλει την αποκλειστική διαχείριση των ψηφιακών δεδομένων κατά τη διαβίβασή τους ή με παγίδευση των ηλεκτρομαγνητικών εκπομπών του συστήματος. Με άλλα λόγια, η συμπεριφορά του δράστη συνδέεται αναπόσπαστα με το υλικό αντικείμενο στο οποίο εκείνος επενεργεί.[220] Το ίδιο ισχύει και για την παρ. 2, όπου αποδοκιμάζεται η χρήση της πληροφορίας ή του υλικού φορέα ως συμπεριφορά του δράστη.

Έχει υποστηριχθεί ότι πρόκειται για αδίκημα που παρουσιάζει αναλογίες με το έγκλημα της διατάραξης οικιακής ειρήνης (334 ΠΚ), καθώς τωόντι υφίσταται το δικαίωμα του πληροφοριακού αυτοκαθορισμού και της ελεύθερης ανάπτυξης της προσωπικότητας, το οποίο βάλλεται στην περίπτωση της υποκλοπής δεδομένων (όπως επίσης και στο άρθρο 370Β). [221]

Το αδίκημα χαρακτηρίζεται ως βλάβης[222] για τους πρώτους δύο τρόπους τέλεσης του αδικήματος,(παρακολούθησης και αποτύπωσης) καθώς δια μέσου της υποκλοπής των ψηφιακών δεδομένων επέρχεται άμεση, πραγματική και οριστική τρώση του εννόμου αγαθού του απορρήτου και της ελεύθερης επικοινωνίας, αλλά όσον αφορά την παρέμβαση στη διαβίβαση των δεδομένων με σκοπό πληροφόρησης του περιεχομένου της είναι αφηρημένης διακινδύνευσης. [223]

Όσον αφορά το τρίτο τρόπο τέλεσης του αδικήματος και συγκεκριμένα την παρέμβαση στη διαβίβαση των δεδομένων με σκοπό πληροφόρησης του περιεχομένου, γίνεται αντιληπτό ότι τυποποιείται ένα έγκλημα υπερχειλούς υποκειμενικής υπόστασης, ή άλλως έγκλημα σκοπού.

Το αδίκημα όταν τελείται με τις μορφές τις αποτύπωσης σε υλικό φορέα και της παρέμβασης (παρ. 1), καθώς και στην περίπτωση της χρήσης της πληροφορίας ή του υλικού φορέα (παρ. 2) χαρακτηρίζεται ως στιγμιαίο, ενώ αντιθέτως στην περίπτωση που τελείται με τη μορφή της

---

[220] Χρίστος Μυλωνόπουλος, *Ποινικό Δίκαιο - ΓΕΝΙΚΟ ΜΕΡΟΣ* (2η, Π Ν Σάκκουλας 2020) 177.

[221] Χαρακτηρίζεται ως έγκλημα διατάραξης ψηφιακής οικιακής ειρήνης, Δ. Κιούπης, Ποινικό Δίκαιο και Internet (ΑΝΤ. Ν. Σάκκουλα 1999), σελ. 125

[222] Σύμφωνα με τη θέση του Τουργέλη και με δεδομένη τη θέση του ότι πληττόμενο έννομο αγαθό συνιστά τόσο η εμπιστευτικότητα όσο και η ακεραιότητα, το αδίκημα μπορεί να σκιαγραφηθεί ως έγκλημα βλάβης του πρώτου στοιχείου (της εμπιστευτικότητας), αλλά συνάμα και ως έγκλημα αφηρημένης διακινδύνευσης του στοιχείου της ακεραιότητας των ψηφιακών δεδομένων ως μέρους ενός πληροφοριακού συστήματος. Ως παράδειγμα εισφέρεται η επίθεση «man-in-the-middle», την οποία ο δράστης μπορεί να αξιοποιήσει για λαθρακρόαση (eavesdropping) των ηλεκτρονικών δεδομένων, αλλά και για μια τροποποίηση του περιεχομένου ηλεκτρονικών μηνυμάτων κατά τη διαβίβασή τους. Ό.π. σελ. 280

[223] Ελένη Καμπέρου σε Αριστοτέλης Χαραλαμπάκης and Ελένη Καμπέρου (eds), Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2761 και 2762

παρακολούθησης των διαβιβαζόμενων δεδομένων ή εκπομπών αξιολογείται ως διαρκές για όσο χρόνο διαρκεί η παρακολούθηση. [224]

6.3. Αντικειμενική υπόσταση

6.3.1. Ο δράστης του εγκλήματος

Όπως αναλύθηκε ανωτέρω, το αδίκημα της υποκλοπής δεδομένων συνιστά κοινό έγκλημα, γεγονός που συνεπάγεται ότι δράστης μπορεί να είναι ο οιοσδήποτε που δεν απολαμβάνει του δικαιώματος διαχείρισης του συστήματος και των δεδομένων.

Στην παράγραφο 2 του άρθρου 370Ε ΠΚ δράστης μπορεί να είναι ο οιοσδήποτε. Ωστόσο, ως δράστης του εγκλήματος νοείται και εκείνος που διέπραξε το αδίκημα της υποκλοπής ψηφιακών δεδομένων, οπότε η χρήση της υποκλαπείσας πληροφορίας ή του υλικού φορέα, στον οποίο αποτυπώθηκε, συνιστά εν τοις πράγμασι την ουσιαστική αποπεράτωση του πρότερου αδικήματος. [225]

Στην έννοια του δράστη συγκαταλέγεται και ο διαχειριστής (DSP) ή ο εργαζόμενος σε υποδομές ψηφιακών υπηρεσιών. [226] Επί παραδείγματι δράστης υποκλοπής μπορεί να είναι και ο πάροχος νεφοϋπολογιστικών υπηρεσιών (cloud service provider) που παρεμβαίνει χωρίς δικαίωμα με κατασκοπευτικό λογισμικό (spionage-software) κατά τη μη δημόσια διαβίβαση δεδομένων ή/και αποτυπώνει σε υλικό φορέα δεδομένα του δικαιούχου διαχείρισης κατά το διαμοιρασμό αρχείων με τον παραλήπτη.[227]

Ποινική ευθύνη στοιχειοθετείται επίσης και στην περίπτωση που ο διαχειριστής υπηρεσιών μετάδοσης πληροφοριών και πρόσβασης στο διαδίκτυο (access provider), με τη βοήθεια ειδικών τεχνολογικών εργαλείων, παρακολουθεί και καταγράφει χωρίς εξουσιοδότηση τη μη

---

[224] Καμπέρου, ό.π. σελ 2762

[225] Αξιοσημείωτο το γεγονός ότι στη γερμανική έννομη τάξη, η λόγω συμπεριφορά τυποποιείται αυτοτελώς, ήγουν ο αθέμιτος προσπορισμός δεδομένων που αποκτήθηκαν μέσω μιας προηγούμενης αξιόποινης πράξης, Συγκεκριμένα, πρόκειται για το άρθρο 202d StGB, υπό το τίτλο «Datenhehlerei», όπου το δικαιολογητικό έρεισμα για τη θέσπισή του εντοπίζεται στο ότι διατηρείται και βαθαίνει η προσβολή του εννόμου αγαθού (MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202d Rn. 2α).

[226] Βλ. υπόθεση φερόμενων υποκλοπών ηλεκτρονικών δεδομένων από υπάλληλο της εταιρίας Google INC.. Christian Hoffmann, Die Verletzung der Vertraulichkeit informationstechnischer Systemedurch Google Street View (https://www.degruyter.com/document/doi/10.9785/ovs-cr-2010-514/html) accessed 22 September 2023. Στην περί ης πολύκροτη υπόθεση, έγινε γνωστό ότι κατά τη διάρκεια των ταξιδιών στις πόλεις, ο οδηγός ενός από τα διερχόμενα οχήματα της γνωστής εταιρείας όχι μόνο φωτογράφιζε δρόμους, αλλά και συνέλεγε, με τη βοήθεια ειδικού λογισμικού, πληροφορίες για ιδιωτικά ασύρματα δίκτυα για τα ασύρματα δίκτυα, με σκοπό τον μετέπειτα εντοπισμό κινητών συσκευών, π.χ. κινητών τηλεφώνων.(Πρόκειται για τον λεγόμενο εντοπισμό με βάση το WLAN, κατά τον οποίο η θέση ενός κινητού θέσης υπολογίζεται με βάση τα πρότυπα μετάδοσης WLAN). Παρ' ημίν η συμπεριφορά του υπαλλήλου πληροί το αδίκημα της υποκλοπής μη δημόσια μεταδιδόμενων ηλεκτρονικών δεδομένων, με τη βοήθεια ειδικών τεχνικών εργαλείων (370Ε ΠΚ)

[227] Daniel Müller, *Der strafrechtliche Schutz der Datenvertraulichkeit vor potentiellen Insiderangriffen* (file:///C:/Users/User/Downloads/s11623-017-0794-z.pdf) accessed 20 September 2023. Το υπολογιστικό νέφος είναι η παροχή υπολογιστικών υπηρεσιών -συμπεριλαμβανομένων των διακομιστών, της αποθήκευσης, των βάσεων δεδομένων, της δικτύωσης, του λογισμικού, της ανάλυσης και της νοημοσύνης- μέσω του διαδικτύου ("το νέφος") που προσφέρει ταχύτερη καινοτομία, ευέλικτους πόρους και οικονομίες κλίμακας. Το cloud computing μολονότι προσφέρει ένα ευρύ φάσμα δυνατοτήτων ανάπτυξης, δημιουργεί επίσης νέους τύπους κινδύνων. Ενώ οι παραβιάσεις από εξωτερικούς δράστες μπορούν να εντοπιστούν, στην περίπτωση παροχής νεφοϋπολογιστικών υπηρεσιών, όπου ένας μεγάλος αριθμός ατόμων εμπλέκεται στην παροχή και τη χρήση του, ο κίνδυνος μιας επίθεσης εκ των έσω αποτελεί τον μεγαλύτερο κίνδυνο για την ασφάλεια.

δημόσια ηλεκτρονική επικοινωνία, προκειμένου να διαθέσει τα σχετικά ηλεκτρονικά δεδομένα έναντι οικονομικού ανταλλάγματος σε ενδιαφερόμενους «αγοραστές». Οι δε τελευταίοι, εφόσον προβαίνουν σε χρήση αυτών, πληρούν την αντικειμενική υπόσταση της παραγράφου 2 του άρθρου 370 Ε ΠΚ.

Αντικείμενο του εγκλήματος συνιστούν τα ψηφιακά δεδομένα επί των οποίων υφίσταται μία εξουσία αποκλειστικής διαχείρισης και διαμόρφωσης της υπόστασής τους.

Η πράξη υποκλοπής

6.3.2. Η αθέμιτη παρακολούθηση ή αποτύπωση μη δημοσίων διαβιβάσεων δεδομένων ή ηλεκτρομαγνητικών εκπομπών ή η παρέμβαση σε αυτές (370Ε παρ. 1 ΠΚ)

Αναφορικά με την έννοια της υποκλοπής ηλεκτρονικών δεδομένων, όπως προβλέπεται στο άρθρο 3 της Σύμβασης της Βουδαπέστης για το Κυβερνοέγκλημα, γίνεται αναφορά σε κάθε πράξη οπτικοακουστικής παρακολούθησης των δεδομένων και συγκεκριμένα κάθε πράξη που αφορά στην ακρόαση, παρακολούθηση ή επιτήρηση του περιεχομένου των επικοινωνιών είτε άμεσα μέσω της πρόσβασης και χρήσης του υπολογιστή είτε έμμεσα μέσω της χρήσης λαθρακρόασης ή μηχανισμών καταγραφής. [228]

Στο άρθρο 370Ε ΠΚ, δεν υιοθετήθηκε η παρεχόμενη από τη Σύμβαση δυνατότητα περιστολής της αντικειμενικής υπόστασης του αδικήματος. Αναλυτικότερα, στο τελευταίο εδάφιο του άρθρου 3 της Σύμβασης προβλέπεται « (έ)να Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση της διάπραξης του εγκλήματος … την επίτευξη σύνδεσης ενός συστήματος υπολογιστή με ένα άλλο σύστημα υπολογιστή». Τέτοια περίπτωση συνιστά η ένταξη του πληττόμενου συστήματος σε μολυσματικό ρομποτικό δίκτυο (botnet)[229]. Η επιλογή αυτή του νομοθέτη, να καταστήσει αξιόποινες και τις υποκλοπές που λαμβάνουν χώρα μέσω σύνδεσης ενός συστήματος υπολογιστή με ένα άλλο σύστημα υπολογιστή, κρίνεται ορθή, καθώς επιτυγχάνεται πληρέστερη προστασία των μη δημόσια διαβιβαζόμενων σε άλλο πληροφοριακό σύστημα δεδομένων.

Η τυποποίηση της πράξης της υποκλοπής (interception), με τεχνικά μέσα, ψηφιακών δεδομένων ή ηλεκτρομαγνητικών εκπομπών, κατά το χρόνο που αυτά διαβιβάζονται από, προς ή εντός πληροφοριακού συστήματος πληροί τους όρους της αρχής της νομιμότητας, όσον αφορά το και ορισμένο της αντικειμενικής υπόστασης (nullum crimen nulla poena sile lege certa), [230] καθώς οι πράξεις υποκλοπής μπορούν να λάβουν αποκλειστικά και μόνο τις ακόλουθες μορφές : α) *παρακολούθησης* μη δημόσια διαβιβαζόμενων δεδομένων από, προς ή εντός πληροφοριακού συστήματος ή ηλεκτρομαγνητικών εκπομπών του, β) *αποτύπωσης*

---

[228] Explanatory Report to the Convention on Cybercrime, Nr. 53 (https://rm.coe.int/16800cce5b) και συγκεκριμένα: « Interception by "technical means" relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. »

[229] Ο όρος “botnet” συντίθεται από τις λέξεις robot (ρομπότ) και network (δίκτυο) και κάθε μολυσμένη συσκευή ονομάζεται bot. Ένα botnet αναφέρεται σε μια ομάδα υπολογιστών που έχουν μολυνθεί από κακόβουλο λογισμικό και έχουν τεθεί υπό τον έλεγχο ενός κακόβουλου δράστη. (https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/) accessed 19 September 2023

[230] Η απαγόρευση της αοριστίας καθιερώνεται με ιδιαίτερη έμφαση στο άρθρο 7 παρ. 1 του Συντάγματος που ρητά απαιτείται ο ποινικός νόμος να <<ορίζει τα στοιχεία της αξιόποινης πράξης>>. Έτσι, τα στοιχεία του εγκλήματος και οι προϋποθέσεις του αξιοποίνου εν γένει πρέπει όχι απλώς να περιγράφονται στο νόμο, αλλά και να είναι επαρκώς προσδιορίσιμα. (Μυλωνόπουλος Χ., Γενικό Μέρος, όπ, σελ, 122-123)

σε υλικό φορέα μη δημόσια διαβιβαζόμενων δεδομένων από, προς ή εντός πληροφοριακού συστήματος ή ηλεκτρομαγνητικών εκπομπών του, γ) *παρέμβασης* κατά τη μη δημόσια διαβίβαση δεδομένων από, προς ή εντός πληροφοριακού συστήματος και δ) *χρήσης* της πληροφορίας ή του υλικού φορέα επί του οποίου έγινε η αποτύπωση με έναν από τους ανωτέρω «τρόπους».

Αναλυτικότερα, ως *παρακολούθηση (surveillance*) νοείται η οργανωμένη, με τεχνικά μέσα, ακρόαση ή η επιτήρηση του περιεχομένου της ηλεκτρονικής επικοινωνίας, χωρίς να χρειάζεται καταγραφή ή αποθήκευση των δεδομένων που παρακολουθούνται. Εξάλλου, η αποτύπωση των δεδομένων τιμωρείται αυτοτελώς ως τρόπος τέλεσης από την διάταξη. [231] Στον παρόντα τρόπο τέλεσης εντάσσονται και οι επιθέσεις «πλαγίου μονοπατιού» (side channel-attacks), με τις οποίες ο δράστης παρακολουθεί, μεταξύ άλλων, το χρόνο, τον ήχο και την κατανάλωση ενέργειας. [232]

Η έννοια της *αποτύπωσης* ερμηνεύεται ως αναπαραγωγή ενός ενσώματου μόνιμου αντιγράφου των πρωτοτύπων δεδομένων ή εκπομπών που διαβιβάζονται στο πληροφοριακό σύστημα. Στην έννοια εμπίπτει η εκτύπωση σε χαρτί και η αποθήκευση των ψηφιακών δεδομένων σε κάποιο μέσο αποθήκευσης (σκληρός δίσκος, DVD, Cd-Rom κλπ.), εφόσον καθίσταται δυνατή η μεταγενέστερη ανάκτηση, επεξεργασία ή περαιτέρω διαβίβασή τους. Σημειωτέον ότι με τους τρόπους τέλεσης της παρακολούθησης και της αποτύπωσης δεν απαιτείται η λήψη γνώσης του περιεχομένου της μετάδοσης.[233]

Ως *παρέμβαση* με ειδικά τεχνικά εργαλεία νοείται η «παρείσφρηση» στα διαβιβαζόμενα εντός του πληροφοριακού συστήματος δεδομένα ή στις ηλεκτρομαγνητικές εκπομπές, χωρίς να απαιτείται ούτε ο δράστης να παρακολούθησε στη συνέχεια το περιεχόμενο της ηλεκτρονικής επικοινωνίας και έτσι να το πληροφορήθηκε ούτε να το αποτύπωσε σε υλικό φορέα. Απαιτείται ωστόσο να είχε ο δράστης, κατά το χρόνο της παρέμβασης (17 ΠΚ), σκοπό να πληροφορηθεί αυτός ή άλλος το περιεχόμενο των δεδομένων ή εκπομπών και ασφαλώς να γνώριζε ότι παρεμβαίνει σε ξένο πληροφοριακό σύστημα, καθώς το αδίκημα διαπλάθεται ως υπερχειλούς υποκειμενικής υπόστασης όταν τελείται υπό αυτό το τρόπο.

Όπως είχε επισημανθεί και στο κεφάλαιο για την ανάλυση του αδικήματος της παράνομης πρόσβασης σε συστήματα πληροφοριών ή σε δεδομένα (370Β), δύναται ο δράστης να παρέμβει στη μετάδοση των ψηφιακών δεδομένων χωρίς να εισέλθει στην «ψηφιακή οικία» του παθόντος, όπως συμβαίνει στην «επίθεση παρεμβαλλόμενου προσώπου» (Man-in-the-Middle Attack)[234]. Συνεπώς, η «παρέμβαση» ως τρόπος τέλεσης υποκλοπής δεν πρέπει να

[231] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2763

[232] Τουργέλης, ό.π. 285 με περαιτέρω παραπομπές

[233] Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021, σελ. 483

[234] Ένα τυπικό παράδειγμα παραβάσεων επιθέσεων man-in-the-middle, είναι όταν ο δράστης παρεμβάλλεται μεταξύ δύο επικοινωνιακών μερών. Αυτό μπορεί να γίνει, για παράδειγμα, με το να εγκαθιστά ο δράστης το δικό του σημείο πρόσβασης WiFi σε μια τοποθεσία με ένα σημείο πρόσβασης WiFi, όπως ένα καφέ ή ένα ξενοδοχείο, που χρησιμοποιεί το ίδιο όνομα (Evil Twin hotspot). Το θύμα χρησιμοποιεί το σημείο πρόσβασης WiFi του δράστη με τη λανθασμένη πεποίθηση ότι πρόκειται για το ασφαλές δίκτυο WiFi της αντίστοιχης τοποθεσίας. Στην πραγματικότητα, το θύμα αποκτά πρόσβαση στο διαδίκτυο μέσω του υπολογιστή του δράστη, γεγονός που δίνει στον δράστη τη δυνατότητα να καταγράφει ή/και να χειραγωγεί όλες τις διαδικτυακές δραστηριότητες του θύματος. Συχνά, στόχος του δράστη είναι να αποκτήσει δεδομένα πρόσβασης στις ηλεκτρονικές τραπεζικές συναλλαγές του θύματος. (Το παράδειγμα από MAH Strafverteidigung, § 50 Cybercrime und Datenkriminalität Rn. 44, beck-online)

συγχέεται με την «πρόσβαση», ήτοι την εισβολή σε ένα πληροφοριακό σύστημα, όπου στη τελευταία αυτή κατηγορία υπάγεται το «hacking».[235]

Τέλος, ως χρήση της πληροφορίας ή του υλικού φορέα νοείται κάθε ενέργεια που κατατείνει στην απόκτηση γνώσης του περιεχομένου της υποκλαπείσας πληροφορίας.

Το παρόν άρθρο δεν περιλαμβάνει στην αντικειμενική υπόσταση την υπερκέραση μέτρων προστασίας, γεγονός που ευνοεί την πληρέστερη προστασία του εννόμου αγαθού (όπως το άρθρο 370Β ΠΚ). Εν προκειμένω, δεν απαιτείται η θωράκιση των δεδομένων με τυχόν μέτρα ασφαλείας, προκειμένου να εξωτερικευθεί η αντίστοιχη βούληση του δικαιούχου, αντίθετα, η ανάγκη προστασίας βασίζεται στο γεγονός ότι ο καθένας απολαύει του δικαιώματος στην επικοινωνία, η οποία θα πρέπει κατ' αρχήν να παραμένει μη δημόσια, εκτός εάν οι συμμετέχοντες επιθυμούν το αντίθετο.[236]

6.3.3. Αθεμίτως- χωρίς δικαίωμα

Η πράξη της υποκλοπής πρέπει να γίνει αθεμίτως, ήγουν χωρίς δικαίωμα. Τα δεδομένα δεν θα πρέπει να προορίζονται για τον δράστη, διαφορετικά, δεν πληρούται η αντικειμενική υπόσταση. Όπως και με το άρθρο 370Β ΠΚ, το στοιχείο του «άνευ δικαιώματος» βασίζεται στη βούληση του προσώπου που είναι εξουσιοδοτημένο να διαθέτει τα δεδομένα.[237]

6.3.4. Διαβίβαση δεδομένων ή ηλεκτρομαγνητικές εκπομπές

Σύμφωνα με την Αιτιολογική Έκθεση για τη Σύμβαση της Βουδαπέστης, ως διαβιβαζόμενα δεδομένα νοούνται μόνο τα δεδομένα που μεταδίδονται ηλεκτρονικά από, προς ή εντός του ίδιου συστήματος πληροφορικής.[238] Υπάγονται δηλαδή οι ηλεκτρονικές διαβιβάσεις δεδομένων μέσω ασύρματων δικτύων (WLAN), καθώς και η ηλεκτρονική συνομιλία μεταξύ δύο φυσικών προσώπων μέσω εφαρμογών, όπως το Skype και Viber (με τη τεχνολογική μέθοδο VoLP).

Η διαβίβαση των δεδομένων διακρίνεται σε εσωτερική και εξωτερική.

Προκειμένου να επιτευχθεί επικοινωνία, προϋποτίθεται η παρουσία δύο τουλάχιστον προσώπων, αφενός του πομπού και αφετέρου του δέκτη των ψηφιακών δεδομένων, τα οποία επικοινωνούν μεταξύ τους, είτε διαδικτυακά ή δορυφορικά ή άλλως μέσω πληροφοριακού συστήματος , ανταλλάσσοντας πληροφορίες που αντιμετωπίζονται από τα μέρη ως ιδιωτικά.[239] Η εξωτερική διαβίβαση των ψηφιακών δεδομένων (data transfer

---

[235] Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021, σελ. 483

[236] Ομοίως και για το αντίστοιχο άρθρο 202b Abfangen von Daten, MüKoStGB/Graf, 4η έκδοση 2021, StGB § 202b Rn. 1-5

[237] MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202b Rn. 8

[238] Explanatory Report to the Convention on Cybercrime, Nr. 51 (https://rm.coe.int/16800cce5b) και συγκεκριμένα: «The communication in the form of transmission of computer data can take place inside a *single* computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the *same* person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard).»

[239] Θεοχάρη Δαλακούρα, Ορισμοί και ουσιαστικές διατάξεις ποινικής αντιμετώπισης του ηλεκτρονικού εγκλήματος σε Θ. Δαλακούρα, Ηλεκτρονικό Έγκλημα - Ουσιαστικές και δικονομικές όψεις, 2η έκδοση, (Νομική Βιβλιοθήκη 2023), σελ. 37

process) εκτείνεται χρονικά από τη τεχνική αποστολή[240] των ψηφιακών δεδομένων από το πληροφοριακό σύστημα του αποστολέα-δικαιούχου διαχείρισής τους έως της λήψη των ψηφιακών δεδομένων από τον παραλήπτη-διαχειριστή του «επικοινωνούντος» πληροφοριακού συστήματος. [241]

Ωστόσο δεν αποκλείεται η ταύτιση του προσώπου αποστολέα – λήπτη κατά την εξωτερική διαβίβαση των δεδομένων από το ένα πληροφοριακό σύστημα στο άλλο, όπως συμβαίνει στην περίπτωση της μεταφοράς δεδομένων από το κινητό τηλέφωνο (smartphone) του δικαιούχου στο φορητό υπολογιστή (laptop) στο πλαίσιο ενός κλειστού δικτύου πληροφοριών (Wi-Fi λ.χ.).

Ως εσωτερική μετάδοση, από την άλλη, δυνάμει του άρθρου 3 της Σύμβασης και του άρθρου 6 της Οδηγίας, νοείται αυτή που λαμβάνει χώρα εντός του ίδιου πληροφοριακού συστήματος με τη ροή (flowing) των ηλεκτρονικών δεδομένων από το ένα εξάρτημα του μηχανικού μέρους (hardware) προς το άλλο. [242]

Τέλος, ως ηλεκτρομαγνητικές εκπομπές[243] νοούνται τα διάφορα ηλεκτρομαγνητικά κύματα, που εκπέμπει ένα πληροφοριακό σύστημα κατά τη λειτουργία του, τα οποία παγιδεύονται από το δράστη με την αξιοποίηση τεχνικού εξοπλισμού.[244] Μεταξύ αυτών συγκαταλέγονται, όπως αναφέρεται και στις Επεξηγήσεις σχετικά με τη Σύμβαση,[245] οι διάφορες ηλεκτρομαγνητικές εκπομπές από τις τεχνικές εργασίες αποθήκευσης ψηφιακών δεδομένων σε ένα πληροφοριακό σύστημα χωρίς να υφίσταται σε εξέλιξη κάποια διαδικασία

---

[240] Η χρήση συσκευών καταγραφής πλήκτρων, οι οποίες κατασκοπεύουν δεδομένα κατά την πληκτρολόγησή τους στο πληκτρολόγιο, δεν επαρκεί για το τη στοιχειοθέτηση του αδικήματος 202b του γερμανικού Ποινικού Κώδικα, δεδομένου ότι στην περίπτωση αυτή τα δεδομένα δημιουργούνται μόνο κατά την πληκτρολόγησή τους στο πληκτρολόγιο και, επομένως, δεν μεταφέρονται από μια θέση αποθήκευσης σε μια θέση-στόχο. Kusnik: Abfangen von Daten - Straftatbestand des § 202b StGB auf dem Prüfstand MMR 2011, 720

[241] Η διαβίβαση δεδομένων κατά την έννοια του άρθρου 202b του γερμανικού Ποινικού Κώδικα νοείται επίσης υπό την προϋπόθεση ότι δεν έχει ακόμη ολοκληρωθεί, δηλαδή τα δεδομένα εξακολουθούν να φορτώνονται. Ακόμα και στην περίπτωση ενδιάμεσης αποθήκευσης (Zwischenspeicher), στην οποία ο αποστολέας δεν έχει καμία επιρροή, μπορεί υπό προϋποθέσεις να θεωρηθεί διαβίβαση. Ωστόσο, από τη στιγμή που ο παραλήπτης αποκτά τον έλεγχο των δεδομένων, καθώς του δίνεται η δυνατότητα να λάβει γνώση τους, η διαδικασία διαβίβασης έχει ολοκληρωθεί και το άρθρο 202b δεν εφαρμόζεται πλέον. Κατά συνέπεια, τα δεδομένα που διαβιβάστηκαν σε προγενέστερη χρονική στιγμή δεν προστατεύονται. Kusnik: Abfangen von Daten - Straftatbestand des § 202b StGB auf dem Prüfstand MMR 2011, 720

[242] Το παράδειγμα από την Επεξηγηματική έκθεση για τη Σύμβαση για το έγκλημα στον κυβερνοχώρο, Nr. 51 (https://rm.coe.int/16800cce5b) : "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example…)."

[243] Για πληρέστερη ανάλυση βλ. MMR 2011, 720, beck-online (και συγκεκριμένα ενότητα 2. Με τίτλο Elektromagnetische Abstrahlung επόμενα)

[244] Ως παράδειγμα μη εξουσιοδοτημένη απόκτηση δεδομένων από ηλεκτρομαγνητικές εκπομπές θα μπορούσε να χρησιμοποιηθεί η χρήση κατευθυντικών μικροφώνων (Einsatz von Richtmikrofonen) και οι λεγόμενες επιθέσεις πλευρικού καναλιού (side channel Angriffe). MAH Strafverteidigung, § 50 Cybercrime und Datenkriminalität Rn. 46, beck-online

[245] Επεξηγηματική έκθεση για τη Σύμβαση για το έγκλημα στον κυβερνοχώρο, Nr. 57 (https://rm.coe.int/16800cce5b) : "The creation of an offence in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision."

διαβίβασης των δεδομένων σε άλλο πληροφοριακό σύστημα. Το ηλεκτρομαγνητικές εκπομπές ενός πληροφοριακού συστήματος δεν αποτελούν καθ' αυτές δεδομένα, μπορούν όμως κατά την ανάλυσή τους, μέσω επιθέσεων να ανασκευαστούν σε πληροφορία, η οποία αποδίδει το νοηματικό περιεχόμενο των διαχειριζόμενων από τον παθόντα ψηφιακών δεδομένων.

6.3.5. Μη δημοσίως

Η αντικειμενική υπόσταση του αδικήματος καταλαμβάνει μόνο τη μη δημόσια διαβίβαση των δεδομένων από, προς ή εντός ενός πληροφοριακού συστήματος. Ο καθοριστικός παράγοντας για τη «μη δημοσιότητα» μιας μεταφοράς δεδομένων δεν είναι ο τύπος ή το περιεχόμενο των μεταφερόμενων δεδομένων, αλλά ο τύπος της διαδικασίας μεταφοράς.[246] Όπως προκύπτει και από τις Επεξηγήσεις σχετικά με τη Σύμβαση, η μη δημοσιότητα αναφέρεται στον τρόπο μετάδοσης και όχι στο είδος των ψηφιακών δεδομένων. [247] Μια μετάδοση μέσω του Διαδικτύου μπορεί επίσης να είναι μη δημόσια, ακόμη και αν τα δεδομένα που μεταδίδονται είναι πληροφορίες δημόσιας πρόσβασης ή μη προσωπικά δεδομένα. [248] Συνεπώς, οποιαδήποτε μη δημόσια μεταφορά δεδομένων, ανεξαρτήτως περιεχομένου, προστατεύεται από την καταγραφή ή τη λήψη των μεταδιδόμενων δεδομένων,[249] όταν αυτά διαβιβάζονται με εμπιστευτικό τρόπο σε ένα συγκεκριμένο παραλήπτη.[250]

Κρίσιμο κριτήριο για τη διάγνωση του «μη δημοσίου» τρόπου μετάδοσης των δεδομένων συνιστά η εξωτερίκευση της βούλησης των επικοινωνούντων φυσικών προσώπων για διατήρηση της εμπιστευτικότητας στη διαχείριση των μεταδιδόμενων ψηφιακών δεδομένων έναντι τρίτου προσώπου, όπως ο εργοδότης. [251]

Η εξωτερίκευση της βούλησης για εμπιστευτικότητα των μεταδιδόμενων δεδομένων πρέπει να καθίσταται αντιληπτή στον τρίτο μέσω συγκεκριμένων πράξεων του εξωτερικού κόσμου. Άλλως, ο τύπος της διαδικασίας μετάδοσης που επιλέχθηκε εκδηλώνει τη βούληση επικοινωνίας μόνο με ορισμένα άτομα ή μια συγκεκριμένη ομάδα ανθρώπων. [252] Επί

---

[246] Ομοίως και για το αντίστοιχο 202b StGB σε MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202b Rn. 10

[247] Explanatory Report to the Convention on Cybercrime, Nr. 54 (https://rm.coe.int/16800cce5b) "...(t)he term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted."

[248] MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202b Rn. 10, με έρεισμα τη σκέψη 54 της Επεξηγηματικής έκθεσης της Σύμβασης «The data communicated may be publicly available information, but the parties wish to communicate confidentially.»

[249] Οι λεγόμενες διαβιβάσεις VPN (Virtual Private Network), καθώς και οι διαβιβάσεις σε ενδοεταιρικά ή εσωτερικά δίκτυα εταιρειών ή αρχών αναφέρονται ως παραδείγματα διαβίβασης μη δημόσιων δεδομένων. Επιπλέον, η διαβίβαση μη κρυπτογραφημένων δεδομένων μέσω του διαδικτύου θεωρείται επίσης μη δημόσια, ακόμη και αν τα διαβιβαζόμενα δεδομένα είναι πληροφορίες δημόσια προσβάσιμες. Οι διαβιβάσεις στα λεγόμενα "ανοικτά" και μη κρυπτογραφημένα δίκτυα WLAN θεωρούνται επίσης προστατευόμενες. StGB § 202β Υποκλοπή δεδομένων, Kargl Kindhäuser/Neumann/Paeffgen/Saliger, έκδοση 2023 7, 8

[250] Όπως επισημαίνει και ο Τουργέλης (ό.π. σελ. 289) η νομοθετική αυτή επιλογή επιρρωνύει τη θέση ότι με τη διάταξη αυτή δεν προστατεύεται το απόρρητο των δεδομένων.

[251] Στο συγκεκριμένο παράδειγμα γίνεται αναφορά στη σκέψη 54 της Επεξηγηματικής έκθεσης της Σύμβασης «Communications of employees, whether or not for business purposes, which constitute "non-public transmissions of computer data" are also protected against interception without right under Article 3 (see e.g. ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92).»

[252] Στα πλαίσια ερμηνείας της διάταξης 202d StGB, υποστηρίζεται ότι μια μετάδοση που δεν απευθύνεται στο κοινό μπορεί να διαγνωστεί αντικειμενικά, κυρίως από την προσπάθεια που

παραδείγματι, εξωτερίκευση της βούλησης για εμπιστευτικότητα των μεταδιδόμενων μέσω δημόσιων δικτύων δεδομένων αποτελεί η κρυπτογράφησή τους με ιδιωτικό κλειδί (private key), το οποίο χρησιμοποιεί συγκεκριμένος παραλήπτης για την αποκρυπτογράφηση και ανάγνωση των παραληφθέντων δεδομένων. [253] Προς διασαφήνιση επισημαίνεται ότι η εν λόγω λήψη μέτρων προστασίας μολονότι θεμιτή για την εμπέδωση του μη δημόσιου τρόπου μετάδοσης των ψηφιακών δεδομένων, δεν συνιστά στοιχείο της αντικειμενικής υπόστασης. [254]

6.3.6. Χρήση ειδικών εργαλείων

Ένας περαιτέρω όρος για την πλήρωση της αντικειμενικής υπόστασης του αδικήματος συνιστά η απαίτηση επίτευξής της με την χρήση « τεχνικών μέσων », προκειμένου να αποτραπεί η υπερβολική ποινικοποίηση. [255] Όπως και στο άρθρο 370Α ΠΚ, η χρήση ειδικών τεχνικών μέσων συνθεμελιώνει το άδικο της συμπεριφοράς του δράστη. [256] Ως ειδικά τεχνολογικά εργαλεία λογίζονται αυτά που συνίστανται σε κάποιο μολυσματικό λογισμικό (malware), όπως το "Lokibot", ή ειδικά κατασκοπευτικά προγράμματα (sniffer), μεταξύ των οποίων ο «καταγραφέας πληκτρολογίου» (keylogger[257]).

6.4. Λόγοι άρσης του αδίκου

Οι επεξηγήσεις σχετικά με τη Σύμβαση της Βουδαπέστης για το Κυβερνοέγκλημα, διευκρινίζουν πως καταλείπεται η διακριτική ευχέρεια στα Συμβαλλόμενα Κράτη να καθιερώσουν νομικούς λόγους αποκλεισμού του αδίκου χαρακτήρα της υποκλοπής ηλεκτρονικών δεδομένων, υπό αυστηρές προϋποθέσεις. [258] Παρ' ημίν, η παρεχόμενη αυτή

απαιτείται για την υποκλοπή της. Στην περίπτωση δεδομένων που μπορούν να υποκλαπούν με χρήση συσκευής, που μπορεί να αγοραστεί νόμιμα (για παράδειγμα, δέκτες WLAN, ραδιοφωνικούς δέκτες ή walki-talkies), τότε η μετάδοση δεδομένων θα κρίνεται δημόσια (NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202b Rn. 8ο). Ομοίως και § 43 Strafrecht im Bereich der Informationstechnologien, Hassemer Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht 3. Auflage 2019 Rn. 92-102 «Die Feststellung ob es sich um eine nichtöffentliche Datenübermittlung handelt, kann im Einzelfall kaum ohne IT-Spezifisches Fachwissen geklärt werden.»

[253] Για περαιτέρω βλέπε Τουργέλη ό.π. σελ. 289

[254] MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202b Rn. 9: «(d)ie übertragenen Daten können verschlüsselt sein; der Tatbestand erfordert dies aber nicht», επίσης Βλ. NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202b Rn. 7 ανάλυση των υποστηριζόμενων θέσεων αναφορικά με την εννοιοδότηση του όρου «μη δημόσια» υπό την υποκειμενική και αντικειμενική θεώρηση.

[255] Explanatory Report to the Convention on Cybercrime, Nr. 53 (https://rm.coe.int/16800cce5b) καθώς και Αιτιολογική Έκθεση τροποποιηθεισών διατάξεων για την καταπολέμηση των εγκλημάτων κατά ηλεκτρονικών υπολογιστών γερμανικού ΠΚ (BT-Drs. 16/3565, σελίδα 11) (https://dserver.bundestag.de/btd/16/036/1603656.pdf) «Eine weitere Einschränkung des Tatbestandes soll durch die Voraussetzung der Anwendung „technischer Mittel" erreicht werden, um eine Überkriminalisierung zu verhindern. Technische Mittel können neben Vorrichtungen zur Erfassung und Aufzeichnung drahtloser Kommunikationen auch Software, Codes oder Passwörter sein.»

[256] Επισημαίνεται ότι υπό τις σημερινές συνθήκες αυτός ο «περιορισμός» δεν υφίσταται πλέον. Η εποχή των «έξυπνων συσκευών» δίνει τη δυνατότητα σε κάθε χρήστη χωρίς ιδιαίτερες τεχνικές γνώσεις να χαρτογραφεί τα ραδιοσήματα χρησιμοποιώντας το δικό του smartphone μέσω μιας δωρεάν διαθέσιμης εφαρμογής, για παράδειγμα. (Auer-Reinsdorff/Conrad IT-R-HdB, § 43 Strafrecht im Bereich der Informationstechnologien Rn. 106, beck-online)

[257] MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202b Rn. 9

[258] Explanatory Report to the Convention on Cybercrime, Nr. 58 (https://rm.coe.int/16800cce5b) «(t)he act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection

δυνατότητα μετουσιώνεται στις πρόβλεψεις του Ν. 5002/22, όπου θεσμοθετείται η ανακριτική πράξη της άρσης του απορρήτου επικοινωνιών, διενεργούμενη (κατ' απαίτηση του άρθρου 19Σ[259]), μόνο για τη διακρίβωση σοβαρών εγκλημάτων.[260] [261]

Μολονότι υποστηρίζεται ότι όλες οι γενικές διατάξεις 21-25 ΠΚ μπορούν να τύχουν εφαρμογής και να οδηγήσουν σε άρση του άδικου χαρακτήρα των πράξεων που προβλέπονται στο 370Ε, [262] εντούτοις, έχει κριθεί νομολογιακά ότι λόγος άρσης του αδίκου της υποκλοπής δεν μπορεί να αποτελέσει η κατάσταση ανάγκης (άρθρο 25 ΠΚ), διότι το έννομο αγαθό της ελεύθερης επικοινωνίας δεν είναι "σημαντικά κατώτερο αγαθό" έναντι της ελευθερίας, της τιμής ή της περιουσίας που πλήττονται μέσω της υποκλοπής.[263]

6.5. Υποκειμενική υπόσταση του εγκλήματος

Προκειμένου να αποδοθεί μομφή στο δράστη της πράξης της υποκλοπής θα πρέπει να καταφαθεί η συνδρομή τουλάχιστον ενδεχόμενου δόλου σε εναρμόνιση με την απαίτηση του ενωσιακού νομοθέτη της Οδηγίας για περιορισμό του αξιοποίνου μόνο σε περιπτώσεις εκ προθέσεως υποκλοπής ηλεκτρονικών δεδομένων. [264] Πρέπει δηλαδή ο δράστης να γνωρίζει και να θέλει να πραγματώσει όλα τα στοιχεία της αντικειμενικής υπόστασης.

Όσον αφορά το σκοπό πληροφόρησης του περιεχομένου υποστηρίζεται ότι συνυφαίνεται με το τρίτο τρόπο τέλεσης του αδικήματος, ήτοι την παρέμβαση και συνεπώς απαιτείται η συνδρομή μόνο στην ως άνω περίπτωση. [265]

Στην παράγραφο 2 του άρθρου απαιτείται ο δράστης της χρήσης της πληροφορίας ή του υλικού φορέα να γνωρίζει ότι η συγκεκριμένη πληροφορία ή ο υλικός φορέας στον οποίο αποτυπώθηκε και εκείνος χρησιμοποιεί, είναι προϊόν κάποιας αξιόποινης πράξης της πρώτης

---

activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities.»

[259] Στο άρθρο 19 του Συντάγματος ορίζεται ότι το απόρρητο της επικοινωνίας, συμπεριλαμβανομένης της ηλεκτρονικής, είναι απόλυτα απαραβίαστο.

[260] Πλέον, το βασικό νομοθέτημα το οποίο ρυθμίζει εξαντλητικά και ειδικά την άρση του απορρήτου των επικοινωνιών είναι ο Ν. 5002/22, με ισχύ από την 9-12-22, οπότε και καταργήθηκε ο Ν. 2225/1994. Στο άρθρο 6 του ως άνω νόμου περιλαμβάνεται ο κατάλογος των αδικημάτων
για τα οποία επιτρέπεται η διενέργεια της ανακριτικής πράξης της άρσης του απορρήτου. Η απαρίθμηση του νόμου είναι περιοριστική. Θα πρέπει σε βάρος του προσώπου κατά του οποίου διατάσσεται η άρση να υφίστανται σοβαρές ενδείξεις ενοχής (α. 6 § 4 περ. β) Ν. 5002/22 και α. 254 § 3 περ. β) ΚΠΔ). Η διαδικασία της άρσης στην περίπτωση της διακρίβωσης εγκλημάτων ρυθμίζεται στην παρ. 3 του άρθρου 6.

[261] Αντίστοιχα και στη γερμανική έννομη τάξη παρέχεται αντίστοιχη δυνατότητα βάσει των άρθρων 100a, 100g και επόμενα του Κώδικα Ποινικής Δικονομίας, κατά περίπτωση σε συνδυασμό με τα άρθρα 100f και 100h. (MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202b Rn. 20, 21)

[262] Ελένη Καμπέρου σε Αριστοτέλης Χαραλαμπάκης and Ελένη Καμπέρου (eds), *Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469*, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2766

[263] ΑΠ 453/2016

[264] Explanatory Report to the Convention on Cybercrime, Nr. 58 (https://rm.coe.int/16800cce5b)
"(f)or criminal liability to attach, the illegal interception must be committed "intentionally…""

[265] Ε. Καμπέρου, ό.π. σελ. 2765. Ωστόσο αντίθετος ο Τουργέλης, ο οποίος επικαλούμενος την αρχή "in dubio pro mitiore" που πρεσβεύει ότι μεταξύ δύο ερμηνευτικών εκδοχών θα πρέπει να επιλέγεται η ευμενέστερη, ισχυρίζεται ότι πρέπει να γίνει δεκτό ότι ο δόλος σκοπού πληροφόρησης αφορά όλους τους τρόπους τέλεσης, καθώς περιστέλλει την εμβέλεια του άρθρου και για το λόγο αυτό είναι ευμενέστερο για τον κατηγορούμενο. (σελ. 292, ό.π.)

παραγράφου, δηλαδή είτε παρακολούθησης είτε παρέμβασης είτε αποτύπωσης σε υλικό φορέα υποκλαπέντων δεδομένων. [266]

6.6. Η χρήση της πληροφορίας ή του υλικού φορέα (370Ε παρ. 2 ΠΚ)

Η χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στην παρ. 1 του ίδιου άρθρου τιμωρείται. Ήγουν, απαιτείται η πληροφορία ή ο υλικός της φορέας να αποτελούν αιτιωδώς και άμεσα το προϊόν του εγκλήματος της «υποκλοπής» που προβλέπεται στην παρ. 1. Στη έννοια της χρήσης εμπίπτουν συμπεριφορές, όπως η αποστολή «cd» ή «dvd» ή «usb» ή έγγραφη επιστολή ή αποστολή «e-mail», που περιέχει τις παράνομα κτηθείσες πληροφορίες, σε κάποιο πρόσωπο, χωρίς όμως να απαιτείται να έλαβε και γνώση ο τελευταίος των πληροφοριών. Εδώ εμπίπτει και η δημοσίευση του περιεχομένου του υλικού φορέα σε έντυπο ή σε ιστοσελίδα στο διαδίκτυο, η ακρόαση και η αναπαραγωγή του περιεχομένου του υλικού φορέα επί του οποίου αποτυπώθηκαν οι πληροφορίες, η μεταβίβαση του υλικού φορέα σε τρίτο, η πώληση της πληροφορίας ή και του υλικού φορέα σε τρίτο. [267]

6.7. Ποινικές κυρώσεις

Με την τροποποίηση του άρθρου 370Ε ΠΚ με το άρθρο 11 Ν. 5002/2022, τα εγκλήματα της διάταξης αυτής έγιναν κακουργήματα και συνεπώς το άρθρο αυτό υπό την νέα του μορφή εφαρμόζονται μόνο για πράξεις που τελούνται μετά την έναρξη ισχύος του Ν. 5002/2022.

Συγκεκριμένα για τις πράξεις των παραγράφων 1 και 2 η επαπειλούμενη ποινή συνίσταται σε κάθειρξη έως 10 έτη, ενώ εάν οι ως άνω πράξεις συνιστούν παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που άπτεται της ασφάλειας του Κράτους, η ποινή διαμορφώνεται σε κάθειρξη από 5 έως και 15 έτη (52 παρ. 2 ΠΚ).

6.8. Ειδικές μορφές εμφάνισης του εγκλήματος

6.8.1. Απόπειρα

Είναι νοητή η απόπειρα στο αδίκημα της υποκλοπής δεδομένων. Χαρακτηριστικό παράδειγμα αποτελεί η εγκατάσταση του «καταγραφέα πληκτρολογίου» (keylogging-malware) στον υπολογιστή του δικαιούχου, ο οποίος αντιλαμβάνεται την ενέργεια του δράστη, προτού ενεργοποιηθεί η λειτουργία του κατασκοπευτικού αυτού λογισμικού. Εν προκειμένω, ο δράστης βρίσκεται σε στάδιο αρχής εκτέλεσης καθώς έχει προβεί ήδη σε μία συμπεριφορά, η οποία τελεί άμεση συνάφεια με την πράξη υποκλοπής. [268]

6.8.2.Συμμετοχή

Στο έγκλημα του άρθρου 370Ε ΠΚ είναι δυνατή κάθε μορφή συμμετοχής. Ενδεικτικά, ως συνεργός θα τιμωρηθεί ο πάροχος διαδικτυακής πρόσβασης που καθιστά διαθέσιμη χωρίς δικαίωμα τη διαδικτυακή διεύθυνση (IP- address) στο δράστη, προκειμένου ο τελευταίος να προβεί σε πράξη υποκλοπής.

Δυνατή καθίσταται και η δια παραλείψεως συνέργεια στην περίπτωση μη λήψης μέτρων ασφαλείας μιας νεφοϋπολογιστικής υποδομής, που χρησιμοποιείται για την αποθήκευση

[266] Ελένη Καμπέρου σε Αριστοτέλης Χαραλαμπάκης and Ελένη Καμπέρου (eds), *Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469*, vol 2 (Νομική Βιβλιοθήκη 2021). Σελ. 2766

[267] Ε. Καμπέρου, ό.π., σελ. 2765-2766

[268] Βάσει της ουσιαστικής-αντικειμενικής θεωρίας , ό.π. αναλύθηκε στο αντίστοιχο κεφάλαιο για την απόπειρα στο αδίκημα 370Β ΠΚ

ψηφιακών δεδομένων του δικαιούχου, προκειμένου να διευκολυνθεί η αθέμιτη παρέμβαση του δράστη κατά τον επιμερισμό των ψηφιακών δεδομένων. [269]

6.8.3. Συρροές

Η συρροή των αδικημάτων που προβλέπονται στο άρθρο 370Ε ΠΚ στην περίπτωση που ο ίδιος δράστης πραγματώσει τόσο την παρ. 1 όσο και την παρ. 2 της διατάξεως υποστηρίζεται ότι θα είναι σχέση πραγματικής αληθινής συρροής, διότι δεν καλύπτεται η απαξία της παρ. 2 από την παρ. 1.[270] Έχει όμως υποστηριχθεί ότι στην περίπτωση που ο ίδιος δράστης πραγματώσει την παρ. 1 και την παρ. 2 της διατάξεως, η χρήση της πληροφορίας ή του φορέα (παρ. 2) θα αποτελεί την ουσιαστική αποπεράτωση του εγκλήματος και ότι η σχέση συρροής μεταξύ της παρ. 1 και 2 του άρ. 370Ε νΠΚ είναι κατ' ιδέαν φαινομενική και η πράξη της παρ. 1 θα εφαρμοστεί ως ειδικότερη. Έχει όμως υποστηριχθεί και η αντίθετη άποψη, ότι στην περίπτωση που ο ίδιος δράστης πραγματώσει την παρ. 1 και την παρ. 2 της διατάξεως, η χρήση της πληροφορίας ή του φορέα (παρ. 2) θα αποτελεί την ουσιαστική αποπεράτωση του εγκλήματος και ότι η σχέση συρροής μεταξύ της παρ. 1 και 2 του άρθρου 370Ε ΠΚ είναι κατ' ιδέαν φαινομενική και η πράξη της παρ. 2 θα απορροφηθεί ως συντιμωρητή ύστερη πράξη.[271]

Αναφορικά με τη σχέση του αδικήματος 370Ε ΠΚ με το αδίκημα της αθέμιτης πρόσβασης γίνεται αντιληπτό ότι συρρέουν φαινομενικά, λόγω ταυτότητας του προσβαλλομένου εννόμου αγαθού, καθώς με αμφότερες προστατεύεται η ασφάλεια των πληροφοριακών συστημάτων και ψηφιακών δεδομένων. Συγκεκριμένα, εφαρμόζεται η αρχή της σιωπηρής επικουρικότητας υπέρ της διάταξης του άρθρου 370Ε στις περιπτώσεις εκείνες, στις οποίες ο δράστης εισχωρεί χωρίς δικαίωμα και καθ' υπέρβαση μέτρων ασφαλείας στο σύστημα του δικαιούχου, υποκλέπτοντας στη συνέχεια δεδομένα, διαβιβαζόμενα τόσο εντός του πληροφοριακού συστήματος (εσωτερική ροή των δεδομένων) όσο και μη δημοσίως διαβιβαζόμενα προς ένα άλλο πληροφοριακό σύστημα (εξωτερική ροή των δεδομένων). Συνεπώς, η πράξη της αθέμιτης πρόσβασης συνιστά το προστάδιο μίας περαιτέρω εμβάθυνσης της προσβολής του εννόμου αγαθού της ασφάλειας πληροφοριακών συστημάτων και δεδομένων που συντελείται με την υποκλοπή ηλεκτρονικών δεδομένων του δικαιούχου-παθόντος. [272]

Το αδίκημα της παραγράφου 1 του άρθρου 370Ε ΠΚ συρρέει φαινομενικά κατ' ιδέαν με τη διάταξη του άρθρου 370Δ παρ. 2 ΠΚ. Θα τύχει εφαρμογής το άρθρο 370Ε ΠΚ ως ειδικότερο, διότι αναφέρεται στα δεδομένα που διαβιβάζονται μεταξύ δύο επικοινωνούντων προσώπων, τα οποία συνιστούν ένα τμήμα εκ του συνόλου των στοιχείων που μεταδίδονται με συστήματα τηλεπικοινωνιών. [273] Κατ' άλλη άποψη, εφαρμόζεται το άρθρο 370Ε ΠΚ, βάσει

---

[269] Τουργέλης, ό.π. σελ. 293

[270] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2765, όπου προς τεκμηρίωση της θέσεώς της αναφέρει ότι η κοινωνικοηθική απαξία της χρήσης της υποκλαπείσας πληροφορίας της παρ. 2, δεν καλύπτεται από την εγκληματική πράξη της παραγράφου 1, ώστε να απορροφηθεί από αυτή.

[271] Τουργέλης Π., Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων. Συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ, Διδακτορική Διατριβή, 2022, σελ. 294

[272] Τουργέλης, ό.π. με επιχειρηματολογία από το αντίστοιχο ελβετικό άρθρο 143ΠΚ (Unbefugte Datenbeschaffung) που επικρατεί του άρθρου του αφορώντος την αθέμιτη πρόσβαση κατ' εφαρμογή της αρχής της επικουρικότητας.

[273] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2766

της αρχής της σιωπηρής επικουρικότητας, καθώς η πράξη υποκλοπής βαθαίνει την τρώση του εννόμου αγαθού που προκάλεσε η πράξη της αθέμιτης πρόσβασης.[274]

Σχετικά με την ηλεκτρονική αλληλογραφία, το αδίκημα του άρθρου 370Ε παρ. 1 ΠΚ συρρέει φαινομενικά κατ' ιδέαν με τη διάταξη του άρθρου 370 παρ. 2 και εφαρμόζεται το πρώτο ως ειδικό, διότι απαιτεί ένα πρόσθετο στοιχείο, τον σκοπό πληροφόρησης του περιεχομένου του e-mail, όταν πρόκειται για παρέμβαση, ενώ απαιτείται η παρέμβαση να γίνει κατά τον χρόνο διαβίβασής του από τον αποστολέα στον παραλήπτη. Αντίθετα, το άρθρο 370 παρ. 2 ΠΚ δεν θέτει τις ως άνω προϋποθέσεις. [275]

Επιπρόσθετα, όταν η υποκλοπή λαμβάνει χώρα με παρέμβαση κατά την διαβίβαση των δεδομένων, γίνεται δεκτή η εφαρμογή του άρθρου 370Ε ΠΚ ως ειδικότερο έναντι του άρθρου 370Α ΠΚ.[276]

Το άρθρο 15 παρ. 1 Ν. 3471/2006 είναι επικουρικό σε σχέση με το άρθρο 370Ε παρ. 1 ΠΚ, εάν πρόκειται για διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών. Το άρθρο 38 παρ. 1 β Ν. 4624/2019 συρρέει αληθινά με το άρθρο 370Ε παρ. 1 ΠΚ.[277]

Σε περίπτωση που ο αυτουργός ή συμμέτοχος τελέσει πρώτα την πράξη του άρθρου 292Γ ΠΚ και, κατόπιν, το έγκλημα του άρθρου 370Ε παρ. 1 ΠΚ, τότε το άρθρο 292Γ ΠΚ είναι επικουρικό έναντι του άρθρου 370Ε ΠΚ. [278] Συμπληρωματικά, το άρ. 370Ε νΠΚ συρρέει αληθινά πραγματικά με το άρ. 292Δ ΠΚ. [279]

Το αδίκημα χρήσης της παρ. 2 συρρέει πραγματικά αληθινά με τα εγκλήματα κατά της τιμής, με την εκβίαση (385 ΠΚ) και την απάτη (386 ΠΚ). [280]

Ανακεφαλαιώνοντας, εάν οι πράξεις των άρθρων 370Δ ή 370Ε ΠΚ έχουν τελεστεί προς όφελος ή για λογαριασμό νομικού προσώπου ή ενώσεως προσώπου ο νομοθέτης, μεταφέροντας την σχετική ρύθμιση της Οδηγίας προβλέπει διοικητικές κυρώσεις σε βάρος τους, οι οποίες κυμαίνονται από χρηματικά πρόστιμα έως και την απαγόρευση άσκησης επαγγελματικής δραστηριότητας.[281]

[274] Τουργέλης Π., Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων. Συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ, Διδακτορική Διατριβή, 2022, σελ. 293

[275] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2766

[276] Τουργέλης Π., Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων. Συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ, Διδακτορική Διατριβή, 2022, σελ. 294

[277] Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021, σελ. 486

[278] Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021, σελ. 490

[279] Τουργέλης Π., Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων. Συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ, Διδακτορική Διατριβή, 2022, σελ. 295

[280] Καμπέρου Ε. σε: Χαραλαμπάκη, Ο νέος ΠΚ, Ερμηνεία κατ΄ άρ. του Ν. 4619/2019, τόμος Β, 2021, σελ. 2766

[281] Μυλωνόπουλος Χ., Διεθνές & Ευρωπαϊκό Ποινικό Δίκαιο, 2021, σελ. 500

7. Απαγόρευση διακίνησης λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων (370ΣΤ ΠΚ)

Το άρθρο 370ΣΤ προστέθηκε ως άνω με το άρθρο 12 Ν. 5002/2022 (ΦΕΚ Α` 228/09.12.2022). Το αδίκημα που προβλέπεται στο υπό εξέταση άρθρο έχει το ακόλουθο περιεχόμενο:

Απαγόρευση διακίνησης λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων

1. Με φυλάκιση τουλάχιστον δύο (2) ετών τιμωρείται όποιος παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, εξάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί λογισμικά ή συσκευές παρακολούθησης, με δυνατότητα υποκλοπής, καταγραφής και κάθε είδους άντλησης περιεχομένου ή και δεδομένων επικοινωνίας (κίνησης και θέσης), με τα οποία μπορούν να τελεσθούν οι πράξεις του άρθρου 370Α.

2. Με φυλάκιση τουλάχιστον δύο (2) ετών τιμωρείται όποιος, χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ, των παραγράφων 2 και 3 του άρθρου 370Δ και του άρθρου 370Ε, παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, εξάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα, με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος.

Κρίσιμη κρίνεται η αναφορά στο άρθρο 13 Ν. 5002/2022 προβλέπει τη διαδικασία καθορισμού των προϋποθέσεων για την προμήθεια από το Δημόσιο λογισμικών και συσκευών παρακολούθησης. Ειδικότερα το άρθρο αυτό με τίτλο «Προμήθεια λογισμικών και συσκευών παρακολούθησης από το Δημόσιο» έχει ως εξής:

«Με προεδρικό διάταγμα, *που εκδίδεται εντός τριών (3) μηνών από την έναρξη ισχύος του παρόντος, μετά από πρόταση των Υπουργών Προστασίας του Πολίτη, Εθνικής Άμυνας, Δικαιοσύνης και Ψηφιακής Διακυβέρνησης, καθορίζονται οι προϋποθέσεις υπό τις οποίες είναι επιτρεπτή η σύναψη συμβάσεων εκ μέρους κρατικών δομών για την προμήθεια λογισμικών ή συσκευών παρακολούθησης του άρθρου 370ΣΤ του Ποινικού Κώδικα για την εκπλήρωση των σκοπών τους, καθώς και επιπρόσθετοι όροι της χρήσης τους».*

Σε σχέση με το άρθρο 13 Ν. 5002/2022 η Επιστημονική Υπηρεσία της Βουλής επισημαίνει, μεταξύ άλλων, τα εξής: *«Δεδομένου ότι, σύμφωνα με το άρθρο 370 ΣΤ ΠΚ, τιμωρείται η παρα- γωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, εξαγωγή, κατοχή διανομή ή με άλλο τρόπο διακίνηση λογισμικών ή συσκευών παρακολούθησης καθώς και συνθηματικών ή κωδικών πρόσβασης ή άλλων παρεμφερών δεδομένων, με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος, θα ήταν νομο- τεχνικώς ορθότερο να προβλέπεται ειδικός λόγος άρσης του αδίκου για τους συμβαλλόμενους (ιδιώτες και κρατικούς υπαλλήλους) στις συμβάσεις που αναφέρει το άρθρο 13».*

Με τη θέσπιση του ως άνω άρθρου ιάται η πλημμέλεια του νομοθέτη του νέου Ποινικού Κώδικα να τυποποιήσει στο άρθρο 292Γ ΠΚ ως αξιόποινες προπαρασκευαστικές πράξεις τη διάθεση, παραγωγή και εμπορία εργαλείων και συνθηματικών πρόσβασης, προοριζόμενων

μόνο για την παρακώλυση λειτουργίας πληροφοριακών συστημάτων αντί της σφαιρικότερης ποινικής προστασίας της πληροφορικής ασφάλειας. [282]

8. Παρακώλυση λειτουργίας πληροφοριακών συστημάτων (292Β ΠΚ)

Μετά το άρθρο 292Α[283] εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών, τυποποιείται το υπό εξέταση άρθρο.

Το άρθρο 292Β ΠΚ θεσπίστηκε κατ' ενσωμάτωση των άρθρων 5 [284] της Σύμβασης της Βουδαπέστης[285] και αντιστοίχως 4 [286] της Οδηγίας 2013/40/ΕΕ, όπου οι υπερεθνικές αυτές διατάξεις διαγράφουν το γενικό πλαίσιο ποινικοποίησης των παρεμβολών σε συστήματα (System Interference) μέσω παρεμβάσεων σε δεδομένα. Ο σκοπός της ως άνω διάταξης συνίσταται στην προστασία του εννόμου συμφέροντος του διαχειριστή και χρήστη για αδιατάρακτη λειτουργικότητα του πληροφοριακού συστήματος και μάλιστα οποιασδήποτε μορφής σχετικά με τη δυνατότητα επεξεργασίας δεδομένων. [287] Ωστόσο το ακριβές νομικό

[282] Παναγιώτης Τουργέλης, Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων: συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ' (Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ), Σχολή Νομικής 2022) <http://didaktorika.gr/eadd/handle/10442/52558> accessed 7 September 2023.

[283] Όπως διαμορφώθηκε η διάταξη με τι άρθρο 95 περ. ιά Ν.4623/2019,ΦΕΚ Α 134/9.8.2019, σε συνδυασμό με το άρθρο 61 Ν.4855/2021, ΦΕΚ Α` 215/12.11.2021.

[284] Το ακριβές περιεχόμενο της διάταξης έχει ως ακολούθως: (άρθρο 5 - Παρεμβολές σε συστήματα), «Κάθε συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος σοβαρή παρακώλυση της λειτουργίας ενός συστήματος υπολογιστή δια της εισαγωγής, διαβίβασης, βλάβης, διαγραφής, φθοράς, αλλοίωσης ή καταστολής δεδομένων υπολογιστή, όταν αυτή διαπράττεται από πρόθεση.»

[285] Σύμφωνα με τη σκέψη 65 της Αιτιολογικής Έκθεσης της Σύμβασης, η περιγραφόμενη στο άρθρο 5 συμπεριφοράς αναφέρεται στη Σύσταση του Συμβουλίου της Ευρώπης υπ' αριθμόν (89) 9 ως δολιοφθορά των υπολογιστών (computer sabotage). Η διάταξη αποσκοπεί στην ποινικοποίηση της σκόπιμης παρεμπόδισης της νόμιμης χρήσης συστημάτων υπολογιστών, συμπεριλαμβανομένων των τηλεπικοινωνιακών εγκαταστάσεων, με τη χρήση ή τον επηρεασμό δεδομένων υπολογιστή. Το προστατευόμενο έννομο συμφέρον συνίσταται στο συμφέρον των διαχειριστών και των χρηστών υπολογιστικών ή τηλεπικοινωνιακών συστημάτων να απολαμβάνουν την ορθή λειτουργία τους. Το κείμενο είναι διατυπωμένο με ουδέτερο τρόπο ώστε να μπορούν να προστατευθούν από αυτό όλα τα είδη λειτουργιών.

[286] Το ακριβές περιεχόμενο του εν λόγω άρθρου έχει ως ακολούθως: (άρθρο 4 - Παράνομη παρεμβολή σε σύστημα), «Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.»

[287] Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης και δη τη σκέψη 65, αναφέρεται ότι αποσκοπείται «η ποινικοποίηση της δόλιας παρεμπόδισης νόμιμης χρήσης υπολογιστικών συστημάτων συμπεριλαμβανομένων τηλεπικοινωνιακών εγκαταστάσεων με τη χρήση ή επιρροή των δεδομένων». Εξ αντιδιαστολής επομένως δεν προωθείται με το υπερεθνικό αυτό πλαίσιο η προστασία από αθέμιτες παρεμβολές σε συστήματα πληροφοριών μέσω επεμβάσεων στο υλισμικό τους (hardware), που εμπίπτει στο προστατευτικό πεδίο των διατάξεων, με τις οποίες αντιμετωπίζεται η φθορά ξένης ιδιοκτησίας. Επίσης, βάσει της ίδιας ως άνω σκέψης «Το κείμενο είναι διατυπωμένο με ουδέτερο τρόπο ώστε να μπορούν να προστατεύονται από αυτό όλα τα είδη λειτουργιών».

περιεχόμενο «της αδιατάρακτης λειτουργικότητας» δεν αποσαφηνίζεται σε τι συνίσταται, πρόκειται δηλαδή για όρο περιγραφικό. [288]

Άρθρο 292Β Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

1. Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση και χρηματική ποινή.

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

8.1. Προστατευόμενο έννομο αγαθό

Η θέση που έχει επικρατήσει αναφορικά με το προστατευόμενο έννομο αγαθό ενστερνίζεται ότι ο σκοπός της της διάταξης του άρθρου 292Β, είναι αφενός η προστασία της ακεραιότητας (integrity), η οποία αντιστοιχεί in concreto στην άσκηση της εξουσίας διαμόρφωσης της υπόστασης των δεδομένων, ως μέρους του συστήματος από το δικαιούχο και αφετέρου η προστασία της διαθεσιμότητας (availability), δηλαδή της συνεχούς (ακώλυτης) δυνατότητας χρήσης του πληροφοριακού συστήματος.[289] Η ακεραιότητα και η διαθεσιμότητα συνιστούν, διακριτές αλλά και συνάμα συσχετιζόμενες λειτουργικές πτυχές του εννόμου αγαθού της ασφάλειας των πληροφοριακών συστημάτων και δεδομένων. [290]

Είχε υποστηριχθεί στο παρελθόν, ενόψει της ιστορικής δικαιοσυστηματικής μεταχείρισης της ηλεκτρονικής εγκληματικότητας ως ιδιαίτερου τμήματος της οικονομικής εγκληματικότητας,

[288] Η διάταξη 303b γερμΠΚ προστατεύει το συμφέρον όλων των χειριστών και των χρηστών για την απρόσκοπτη λειτουργία της επεξεργασίας των δεδομένων τους, βάσει BT-Drs. 16/3656 σελ. 13, (Schönke/Schröder/Stree/Hecker, 29. Aufl. 2014, StGB § 303b Rn. 1, beck-online)

[289] Η ακεραιότητα εντάσσεται στην «αρνητική», ενώ η διαθεσιμότητα στη «θετική λειτουργία» της πληροφοριακής ασφάλειας.

[290] Ε. Καμπέρου, ο.π., σελ. 2095, Π. Τουργέλης, Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων: συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε Π.Κ., 2022, σελ.: 306, Ν. Χατζηνικολάου, Ποινικό Δίκαιο, Ειδικό Μέρος, Εγκλήματα κατά της ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών, των κοινωφελών εγκαταστάσεων, της λειτουργίας πληροφοριακών συστημάτων, άρθρα 290 – 298, 2017, σελ. 183

η άποψη ότι με τις διατάξεις ποινικής αντιμετώπισης των δολιοφθορών πληροφοριακών συστημάτων (computer sabotage) [291] αντιμετωπίζονται εγκληματικές συμπεριφορές, που συνιστούν «περιπτώσεις καταστροφής συστημάτων επεξεργασίας ηλεκτρονικών δεδομένων, διαπραττόμενες με δόλο περιουσιακής ζημίας» και επομένως ότι προστατεύεται ως έννομο αγαθό η περιουσία. [292]

Ωστόσο, το έννομο αγαθό της περιουσίας ενίοτε τυγχάνει συμπροστατευόμενο παρ' ημίν. Συγκεκριμένα, από τη νομοτυπική διάπλαση της διακεκριμένης παραλλαγής του άρθρου 292Β παρ.2 στοιχ. β ΠΚ, όπου επιλέχθηκε από τον Έλληνα νομοθέτη η «οικονομική ζημία ιδιαίτερα μεγάλης αξίας» ως μία από τις ενδεικτικά αναφερόμενες περιπτώσεις της αόριστης νομικής έννοιας «σοβαρή ζημία» ως στοιχείο της αντικειμενικής υπόστασης, συνάγεται ότι συμπροστατευόμενο έννομο αγαθό με την επίμαχη διάταξη είναι και η περιουσία. Τούτο μάλιστα ισχύει και για το εδ. α' της παρ. 2, όπου ο κίνδυνος προσβολής της περιουσίας συνιστά το λόγο αυτοτελούς νομοτυπικής διάπλασης μίας σχετικά διακεκριμένης παραλλαγής, τυποποιώντας, έτσι, ένα έγκλημα αφηρημένης διακινδύνευσης της περιουσίας.

8.2. Χαρακτηρολογικά στοιχεία του εγκλήματος

Πρόκειται για πλημμέλημα, αυτεπαγγέλτως διωκόμενο (μετά την κύρωση του νέου ΠΚ), και για έγκλημα κοινό, καθώς δράστης του εγκλήματος μπορεί να είναι οποιοδήποτε πρόσωπο, ακόμη και ο ίδιος ο νόμιμος ιδιοκτήτης του πληροφοριακού συστήματος, εφόσον παρεμβάλλεται σε αυτό χωρίς δικαίωμα, δηλαδή χωρίς εξουσιοδότηση από το δικαιούχο διαχείρισης (σε περίπτωση ετερότητας του προσώπου) ή από την έννομη τάξη (lawful excuse)[293].

Το αδίκημα του άρθρου 292Β ΠΚ είναι δε *έγκλημα αποτελέσματος*, δεδομένου ότι ο δράστης δεν αρκεί να προβεί απλά σε μία συμπεριφορά, που κατατείνει τεχνολογικά στη σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας του πληττόμενου συστήματος πληροφοριών, αλλά απαιτείται να επέλθει αιτιωδώς, από τη συμπεριφορά αυτή και το αποτέλεσμά της, τυποποιούμενο αυτοτελώς ως στοιχείο της αντικειμενικής υπόστασης του εγκλήματος. [294]

Περαιτέρω, με τις διατάξεις του άρθρου 292Β νέου ΠΚ περιγράφεται ένα *γνήσιο πολύτροπο ή υπαλλακτικώς μικτό έγκλημα*, [295] δεδομένου ότι οι τυποποιημένοι στην αντικειμενική

[291] Η ανάγκη προστασίας από τις οποίες αναφέρεται ήδη σε πρώιμο χρονικά στάδιο, στην υπ'αρ. (89) 9 Σύσταση του Συμβουλίου της Ευρώπης, όπου στο κείμενο αυτό γίνεται λόγος για «ηλεκτρονικό βανδαλισμό».

[292] Τουργέλης, όπ με περαιτέρω παραπομπή σε K.Kühne, Die Entwicklung des Internetstrafrechts, σελ.55. Πάντως, η άποψη αυτή υποστηρίζεται ακόμη και σήμερα για τη ερμηνεία αντίστοιχων διατάξεων σε ξένες έννομες τάξεις, όπως η αυστριακή, αναφορικά με την παρ. 126b αυστρ.ΠΚ (Störung der Funktionsfähigkeit eines Computersystems), που εντάσσεται στο κεφάλαιο για την αντιμετώπιση περιουσιακών εγκλημάτων.

[293] Βλ. άρθρο 2 στοιχ.δ' της Οδηγίας 2013/40/ΕΕ, για τον ορισμό του «χωρίς δικαίωμα». Η ζημία σε λογισμικό ή υλικό από τον μοναδικό εξουσιοδοτημένο χρήστη δεν αποτελεί παράβαση, ομοίως για 303b γερμΠΚ (MüKoStGB/Wieck-Noodt, 4. Aufl. 2022, StGB § 303b Rn. 6)

[294] Από τη γερμανική θεωρία και νομολογία για την ερμηνεία της αντίστοιχης παρ.303b γερμ.ΠΚ, όπου για την πλήρωση της αντικειμενικής υπόστασης του αδικήματος απαιτείται αιτιώδης συνάφεια μεταξύ της αντίστοιχης πράξης δολιοφθοράς και της σημαντικής διακοπής της επεξεργασίας δεδομένων, από Schönke/Schröder/Stree/Hecker, 29. Aufl. 2014, StGB § 303b, beck-online και από Νομολογία, LG Düsseldorf: DDoS-Attacken als Erpressung und Computersabotage, (MMR 2011, Seite 624, beck-online)

[295] Ν. Χατζηνικολάου, ό.π., σελ. 186, αναφορικά με το άρθρο 292Β του προϊσχύοντος πλέον Ποινικού Κώδικα

υπόσταση του εγκλήματος τρόποι τέλεσης μπορούν να εναλλαχθούν στο ίδιο αντικείμενο, ήτοι το προσβαλλόμενο πληροφοριακό σύστημα ή τα ψηφιακά δεδομένα, αποτελώντας όμως πάντα μία αξιόποινη πράξη. Τούτο συνεπάγεται πως ακόμη και αν ο δράστης επιλέξει να προσβάλει την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability), πτυχές του εννόμου αγαθού της πληροφορικής ασφάλειας με όλους τους δυνατούς τρόπους, που τυποποιούνται στην αντικειμενική υπόσταση του άρθρου 292Β ΠΚ, θα τιμωρηθεί για ένα μόνο έγκλημα «παρακώλυσης λειτουργίας πληροφοριακών συστημάτων».

Επιπρόσθετα, τυποποιείται ένα *έγκλημα βλάβης* του εννόμου αγαθού της ασφάλειας των πληροφοριακών συστημάτων και δεδομένων,[296] καθότι για την στοιχειοθέτηση της αντικειμενικής υπόστασης δεν αρκεί η διακινδύνευση της ομαλής λειτουργίας του πληροφοριακού συστήματος, αλλά απαιτείται να επέλθει παρακώλυση (σοβαρή παρεμπόδιση ή διακοπή) της λειτουργίας του. Το αποτέλεσμα δηλαδή της συμπεριφοράς του δράστη, ως αυτοτελές στοιχείο της αντικειμενικής υπόστασης του εγκλήματος, δεν συνίσταται σε κίνδυνο, αλλά σε βλάβη της ακεραιότητας και διαθεσιμότητας του συστήματος του δικαιούχου. Ωστόσο, στο άρθρο 292Β παρ.2 στοιχ. α' ΠΚ τυποποιείται από το νομοθέτη, επιπλέον, ένα έγκλημα αφηρημένης διακινδύνευσης της ακεραιότητας και διαθεσιμότητας, δηλαδή της ασφάλειας, ενός αόριστου αριθμού (μεγάλου αριθμού) πληροφοριακών συστημάτων μέσω της αξιοποίησης ειδικού εργαλείου. Πέραν αυτών, μάλιστα, στα εδάφια α' και β' της παρ.2 περιγράφεται από τον Έλληνα νομοθέτη και ένα έγκλημα αφηρημένης διακινδύνευσης (στοιχ. α') και βλάβης (στοιχ. β') αντίστοιχα του εννόμου αγαθού της περιουσίας. [297]

Πρόκειται καταρχήν για *στιγμιαίο* έγκλημα ανεξάρτητα από τη χρονική διάρκεια της διακοπής ή της σοβαρής παρεμπόδισης χρήσης του πληροφοριακού συστήματος από το δικαιούχο. Κατ' εξαίρεση όμως το «πληροφορικό σαμποτάζ» αποτελεί *διαρκές* έγκλημα, όταν η σοβαρή παρεμπόδιση του συστήματος τελείται με αποκλεισμό της πρόσβασης στα ψηφιακά δεδομένα του δικαιούχου, διότι τότε η αντικειμενική υπόσταση του εγκλήματος περιλαμβάνει όχι μόνο τη δημιουργία αλλά και τη διατήρηση της παράνομης κατάστασης από το δράστη.

8.3. Αντικειμενική υπόσταση

8.3.1. Δράστης

Όπως προαναφέρθηκε, το αδίκημα χαρακτηρίζεται ως κοινό. Αναλυτικότερα, κατωτέρω σταχυολογούνται κάποιες περιπτώσεις.

Στην έννοια του δράστη παρακώλυσης λειτουργίας πληροφοριακού συστήματος υπάγεται και ο διαχειριστής ενός μολυσματικού δικτύου "Botnet" και όχι ο ανυποψίαστος χρήστης αυτού. [298]

[296] Καμπέρου Ε., ό.π., σελ. 2095

[297] Τουργέλης Π., ό.π., σελ. 308

[298] Η προσβολή μέσω ενός υπολογιστή "Zombie" αποτελεί πράξη, κατά ποινικό δίκαιο, του διαχειριστή του δικτύου "Botnet" και όχι του (νόμιμου) διαχειριστή του «χειραγωγούμενου» αυτού υπολογιστή. Συχνά μάλιστα η λειτουργία των δικτύων "Botnet" συνδυάζεται με τη δημιουργία ιστοσελίδας στο «σκοτεινό διαδίκτυο» για τη διενέργεια κατανεμημένων επιθέσεων επ' αμοιβή (DDoS-as-a-service). Βλ.

Επίσης δράστης του εγκλήματος μπορεί να είναι και ο διαχειριστής ενός δικτύου πληροφοριών (network), που «ανακατευθύνει» τη διαδικτυακή σύνδεση σε ιστοσελίδα με μολυσματικό λογισμικό (malware), το οποίο εγκαθίσταται αυτομάτως σε υπολογιστικό σύστημα προκαλώντας δυσλειτουργία του. Η ανωτέρω συμπεριφορά του παρόχου και συγκεκριμένα του διαχειριστή-φυσικού προσώπου, κατά την θεμελιώδη ποινική αρχή της ενοχής, συνιστά πράξη προσβολής και δη βλάβης του έννομου αγαθού της ασφάλειας των συστημάτων πληροφορικής και ηλεκτρονικών δεδομένων στις ειδικότερες πτυχές της διαθεσιμότητάς και ακεραιότητάς τους. Στοιχειοθετείται έτσι, υπό την αίρεση πλήρωσης και των υπόλοιπων όρων, ποινική ευθύνη για τέλεση της αξιόποινης πράξης «παρακώλυσης λειτουργίας πληροφοριακών συστημάτων (292Β ΠΚ)»[299]

8.3.2. Αντικείμενο του εγκλήματος

Αντικείμενο του εγκλήματος είναι το πληροφοριακό σύστημα ως σύνολο επί του οποίου υφίσταται δικαίωμα διαχείρισης στις ειδικότερες πτυχές αφενός της εξουσίας διαμόρφωσης της υπόστασης των ψηφιακών δεδομένων ως μέρους του πληροφοριακού συστήματος και αφετέρου της εξουσίας ακώλυτης χρήσης του πληροφοριακού συστήματος ως ολότητας. Η προσβολή αυτού του δικαιώματος διαχείρισης συνιστά τη συγκεκριμενοποίηση της προσβολής του εννόμου αγαθού της πληροφορικής ασφάλειας.

8.3.3. Πράξη σοβαρής παρεμπόδισης ή διακοπής της λειτουργίας χωρίς δικαίωμα.

Ο Έλληνας νομοθέτης, επί τη βάσει του άρθρου 4 της Οδηγίας, επέλεξε ορθά μία ευρύτερη διάπλαση του εγκλήματος του πληροφορικού σαμποτάζ, τυποποιώντας ως πράξη προσβολής όχι μόνο την πράξη που επιφέρει «σοβαρή παρεμπόδιση» του συστήματος αλλά και την πράξη που κατατείνει σε «διακοπή», εν αντιθέσει με το άρθρο 5 της Σύμβασης, στο οποίο η πράξη τέλεσης του εγκλήματος περιγράφεται αποκλειστικά με τον όρο «παρεμπόδιση» (hindering).

8.3.4. Χωρίς δικαίωμα

Η συμπεριφορά του δράστη του περιγραφόμενου εγκλήματος πρέπει να τελείται «χωρίς δικαίωμα» (without right), δηλαδή χωρίς να είναι δικαιούχος διαχείρισης του συστήματος ως ολότητας ή να έχει σχετική εξουσιοδότηση για παρεμβολή στο σύστημα από το δικαιούχο ή από την έννομη τάξη. Όπως αναφέρεται σχετικά στην Αιτιολογική Έκθεση της Σύμβασης,[300] συμπεριφορές, όπως νόμιμες καθημερινές δραστηριότητες, συνδεόμενες με το σχεδιασμό δικτύων, δοκιμές (τεστ) της ασφάλειας του συστήματος και ενέργειες ενίσχυσης της πληροφορικής προστασίας ή προσθαφαίρεσης προγραμμάτων κατόπιν εξουσιοδότησης του δικαιούχου, δεν πρέπει να αντιμετωπίζονται ποινικά ακόμη και εάν επέρχεται σοβαρή παρεμπόδιση του συστήματος.[301]

---

https://encyclopedia.kaspersky.com/glossary/ddos-as-a-service/ (accessed 19 September 2023)

[299] Τουργέλης Π., ό.π., σελ. 309

[300] Ιδίως βλ. σκέψεις 68 και 38 της Αιτιολογικής Έκθεσης της Σύμβασης και τον επίσης τον ορισμό που δίνεται στο άρθρο 2 εδ'δ΄ της Οδηγίας.

[301] Ε. Καμπέρου, ό.π., σελ. 2097

Για την αξιολόγηση της νομικής φύσης του στοιχείου αυτού έχουν υποστηριχθεί διαφορετικές απόψεις. [302]Ο όρος «χωρίς δικαίωμα» επιτελεί και στην παρούσα εξέταση ποινικής ευθύνης «διπλή λειτουργία», εξεταζόμενος πρώτα σε σχέση με την έννοια του δικαιούχου [303]ή τη συγκατάθεσή του τελευταίου σε μία παρεμβολή στο σύστημα, οπότε αποκλείεται ήδη η αντικειμενική υπόσταση και έπειτα σε επίπεδο αδίκου.

8.3.5. Εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή αποκλεισμός της πρόσβασης στα δεδομένα του συστήματος

Η περιγραφείσα πράξη προσβολής πρέπει να τελείται με κάποιον από τους περιοριστικά αναφερόμενους στο νόμο τρόπους, οι οποίοι μάλιστα μπορούν να εναλλαχθούν από το δράστη οδηγώντας, όμως, πάντα σε μία εγκληματική πράξη, εφόσον προσβλήθηκε η ίδια μονάδα εννόμου αγαθού, δηλαδή το ίδιο σύστημα πληροφοριών π.χ. ο ίδιος ηλεκτρονικός υπολογιστής ή το ίδιο δίκτυο ηλεκτρονικών υπολογιστών. Χαρακτηριστικό παράδειγμα αποτελεί η εισαγωγή από το δράστη εξελιγμένων-μορφών μολυσματικού λογισμικού (malware) με πολλαπλή λειτουργία, που επιφέρει αφενός αλλοίωση ή/και διαγραφή ψηφιακών δεδομένων του δικαιούχου, πλήττοντας έτσι την ακεραιότητα του συστήματος ως ολότητας και αφετέρου αποκλεισμό της πρόσβασης του δικαιούχου με κρυπτογράφηση (encryption) ψηφιακών δεδομένων που διαχειρίζεται ο τελευταίος, πλήττοντας έτσι και τη διαθεσιμότητα του συστήματος ως ολότητας, αποτελώντας μία εγκληματική συμπεριφορά απαξιολούμενη κατ' άρθρο 292Β ΠΚ.[304]

Οι ως άνω περιγραφόμενοι τρόποι τέλεσης του αδικήματος μπορούν να ομαδοποιηθούν σε δύο μεγάλες κατηγορίες. Στην πρώτη κατηγορία τοποθετούνται εκείνοι οι τρόποι παρεμβολής στο σύστημα του δικαιούχου, που προσβάλλουν την ακεραιότητα του συστήματος και συγκεκριμένα οι παρεμβολές με διαγραφή, καταστροφή και αλλοίωση ψηφιακών δεδομένων, που επεξεργάζεται ο δικαιούχος του συστήματος. Στη δεύτερη κατηγορία εντάσσονται εκείνοι οι τρόποι παρεμβολής του δράστη που προσβάλλουν τη διαθεσιμότητα του συστήματος, ήτοι η εισαγωγή, διαβίβαση ψηφιακών δεδομένων καθώς και ο αποκλεισμός του δικαιούχου από την πρόσβαση και επομένως τη δυνατότητα ακώλυτης χρήσης του πληροφοριακού συστήματος ως ολότητας.[305]

Ειδικότερα, ως εισαγωγή δεδομένων (input of data) νοείται κατά την επιστημονική βιβλιογραφία,[306] τόσο η με φυσικό τρόπο «διοχέτευση» ηλεκτρονικών δεδομένων σε εξωτερικό αποθηκευτικό φορέα (πχ. usb) συνδεδεμένο με πληροφοριακό σύστημα, όσο και η ηλεκτρονική (εξ αποστάσεως) αποστολή ηλεκτρονικών δεδομένων στο πληροφοριακό

[302] Σύμφωνα με Ε. Καμπέρου (ό.π. 2097), ο όρος «χωρίς δικαίωμα» δηλώνει την έλλειψη συγκατάθεσης του νομίμου κατόχου του πληροφοριακού συστήματος, η οποία αποκλείει την αντικειμενική υπόσταση του εγκλήματος και δεν αίρει απλώς τον άδικο χαρακτήρα του, ενώ σύμφωνα με Ν. Χατζηνικολάου(ό.π. σελ. 192) η με δικαίωμα» – νόμιμη παρακώλυση θεμελιώνει τον αρχικό άδικο χαρακτήρα της πράξης, ο οποίος ωστόσο αίρεται στη βάση του εκάστοτε στοιχείου που δικαιολογεί τη συμπεριφορά του δράστη.

[303] Εδώ εντάσσεται ο συνδικαιούχος διαχείρισης του πληροφοριακού συστήματος ως ολότητας αλλά και ο δικαιούχος διαχείρισης ψηφιακών δεδομένων, που νομίμως έτσι παρεμβαίνει στην επεξεργασία τους.

[304] Ε. Καμπέρου, ό.π., σελ. 2097

[305] Π. Τουργέλης, ό.π., σελ. 311-312

[306] M.Gercke, Understanding Cybercrime (https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf)

σύστημα, που πλήττει την ακεραιότητά επεξεργαζόμενων ψηφιακών δεδομένων ως μέρους ή/και τη διαθεσιμότητα του συστήματος, νοούμενη ως αδιάλειπτη δυνατότητα χρήσης του.

Χαρακτηριστικό παράδειγμα αποτελεί η εγκατάσταση ηλεκτρονικού ιού (computervirus), αλλά όχι και «δούρειου ίππου» (trojan horse), καθώς αυτός επιτελεί κατά βάση κατασκοπευτική λειτουργία και δεν κατατείνει στην διατάραξη της λειτουργίας του συστήματος, μέσω σημαντικής μείωσης της ταχύτητας του πληροφοριακού συστήματος. [307]

Η διαβίβαση δεδομένων (transmission of data) διακρίνεται, καθώς συνίσταται στη μεταφορά δεδομένων από υπολογιστή σε υπολογιστή στο πλαίσιο ενός δικτύου (Network), όπως ασύρματου δικτύου ευρείας εμβέλειας.

Μετάδοση είναι η προώθηση τέτοιων ερεθισμάτων με μη φυσικά, π.χ. ηλεκτρονικά μέσα σε άλλους υπολογιστές ή συσκευές αποθήκευσης δεδομένων. Παραδείγματα συνιστούν οι "επιθέσεις άρνησης παροχής υπηρεσιών" (DoS attacks)[308], κατά τις οποίες οι υπηρεσίες ενός διακομιστή επιβαρύνονται τόσο πολύ από μεγάλο αριθμό αιτημάτων, ώστε η ικανότητα λήψης και επεξεργασίας τους να μην επαρκεί και έτσι να εμποδίζεται ή τουλάχιστον να δυσχεραίνεται η πρόσβαση για νόμιμη επαφή με τον διακομιστή. Τέτοιες επιθέσεις DoS περιλαμβάνουν επίσης τις λεγόμενες διαδικτυακές διαδηλώσεις με σκοπό την πολιτική διαμαρτυρία. [309]

Στο σημείο αυτό αξιοσημείωτη είναι η απόφαση του Εφετείου της Φρανκφούρτης αναφορικά με το αξιόποινο χαρακτήρα της διαδικτυακής διαμαρτυρίας υπό το πρίσμα του άρθρου 303a του γερμ ΠΚ. [310]

Συγκεκριμένα το Δικαστήριο έκρινε ότι η μη προσβασιμότητα για χρονικό διάστημα δύο ωρών από τον έχοντα την εξουσία διαθέσεως των δεδομένων (Verfugungsberechtigte), χωρίς να είναι νομικά σημαντικό, εάν παρεμποδίστηκαν και τρίτοι-διαδικτυακοί επισκέπτες, δεν εμπίπτει στην έννοια της «αποστέρησης των δεδομένων» (Datenunterdrückung) λόγω του πολύ μικρού χρονικού διαστήματος, που έλαβε χώρα η διαδικτυακή αυτή διαμαρτυρία και επομένως δεν στοιχειοθετείται η αντικειμενική υπόσταση της παρ. 303a γερμ ΠΚ

[307] Βάσει της σκέψη 67 της Αιτιολογικής Έκθεσης της Σύμβασης ως σοβαρή παρεμπόδιση νοείται η αποστολή δεδομένων σε ένα συγκεκριμένο σύστημα με τέτοια μορφή, μέγεθος ή συχνότητα ώστε να επηρεάζει σημαντικά την ικανότητα του ιδιοκτήτη ή του φορέα εκμετάλλευσης να χρησιμοποιεί το σύστημα ή να επικοινωνεί με άλλα συστήματα (π.χ. μέσω προγραμμάτων που δημιουργούν επιθέσεις "άρνησης εξυπηρέτησης", κακόβουλους κώδικες όπως ιούς που εμποδίζουν ή επιβραδύνουν σημαντικά τη λειτουργία του συστήματος ή προγράμματα που στέλνουν τεράστιες ποσότητες ηλεκτρονικής αλληλογραφίας σε έναν παραλήπτη προκειμένου να μπλοκάρουν τις λειτουργίες επικοινωνίας του συστήματος).

[308] Denial-of-service (DoS), φαινόμενο που καταγράφεται πλέον με την πιο συστηματική του μορφή ως Distributed Denial-of-service (DDos). Βλ. McLaurin, Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service, σελ. 216 (https://openyls.law.yale.edu/bitstream/handle/20.500.13051/17179/08_30YaleL_PolyRev211_2011_2012_.pdf?sequence=2&isAllowed=y) σελ. 216

[309] MüKoStGB/Wieck-Noodt, 4. Aufl. 2022, StGB § 303b Rn. 12

[310] OLG Frankfurt/M.: Strafbarkeit einer „Online-Demo" (MMR 2006, 547, beck-online). Πάντως δεν εξετάστηκε από το γερμανικό Εφετείο (OLG) η στοιχειοθέτηση της αντικειμενικής υπόστασης της παρ. 303b γερμ.ΠΚ (αντίστοιχο άρθρο 292Β ισχ.ΠΚ), λόγω της νομοθετικής αντιμετώπισης, πριν τον 41° τροποποιητικό νόμο, όχι ως αυτόνομου εγκλήματος, αλλά ως διακεκριμένης παραλλαγής της παρ. 303a γερμ.ΠΚ.

(Datenveränderung). Η νομολογιακή αυτή άποψη ωστόσο, για εξαίρεση από το πεδίο εφαρμογής της παρ. 303a γερμ.ΠΚ περιπτώσεων αδυναμίας πρόσβασης στα δεδομένα για πολύ μικρή χρονική διάρκεια , απορρίπτεται ορθά από την κρατούσα άποψη στη θεωρία καθόσον δεν ερείδεται στο γράμμα του νόμου. [311]

Ως «διαβίβαση δεδομένων» νοείται και η μαζική αποστολή μηνυμάτων ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (spam e-mails). Σχετικά με την αντιμετώπιση της μαζικής αποστολής μηνυμάτων ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (spam mails) που επιφέρουν μεν βλάβη στη λειτουργικότητα του συστήματος, αποστελλόμενα ωστόσο για εμπορικούς ή διαφημιστικούς σκοπούς υποστηρίζεται ότι οι συμπεριφορές αυτές δεν ενέχουν ουσιαστικό εγκληματικό άδικο, διότι συνιστούν καθημερινές συμπεριφορές προώθησης επιχειρηματικής δραστηριότητας. [312] Επομένως, σε περίπτωση σοβαρής προσβολής της λειτουργικότητας του συστήματος, θα πρέπει να αντιμετωπιστούν μόνο με την επιβολή αστικών κυρώσεων, προτείνοντας μάλιστα τη ρητή εξαίρεσή τους από το πεδίο εφαρμογής του άρθρου 292Β.

Ως διαγραφή ψηφιακών δεδομένων (deletion) νοείται εκείνη η επεμβατική στα δεδομένα ενέργεια που οδηγεί σε ανεπανόρθωτη απώλεια του περιεχομένου τους. Εν προκειμένω απαιτείται μία ερμηνευτική συστολή του γράμματος, ώστε στην έννοια της διαγραφής να υπαχθούν μόνο οι περιπτώσεις οριστικής διαγραφής.[313]

Ως καταστροφή ψηφιακών δεδομένων (damage) νοείται η ενέργεια εκείνη του δράστη, που επιφέρει βλάβη της άυλης υπόστασής τους και επομένως αδυναμία της δυνατότητας χρήσης τους τη δεδομένη χρονική στιγμή. Στην έννοια της καταστροφής ψηφιακών δεδομένων πρέπει να υπαχθεί και η διαγραφή ψηφιακών δεδομένων, τα οποία όμως μπορούν να «ανακτηθούν» με τη χρήση ειδικού λογισμικού, όπως επίσης και με την αξιοποίηση αντιγράφου ασφαλείας (back-up). Εάν μάλιστα η καταστροφή των ψηφιακών δεδομένων επέρχεται αντανακλαστικά μέσω της καταστροφής του υλικού αποθηκευτικού τους φορέα, που συνιστά αξιόποινη πράξη κατ' άρθρο 381 ΠΚ, τότε συντρέχει αληθινή συρροή, διότι ο δράστης πραγματώνει την αντικειμενική υπόσταση διαφορετικών εγκλημάτων.

Ως αλλοίωση ψηφιακών δεδομένων νοείται η τροποποίηση του περιεχομένου των ψηφιακών δεδομένων. Εδώ εμπίπτουν όλες εκείνες οι ενέργειες του δράστη, όπως η αντικατάσταση του αρχικού τους περιεχομένου και η παραποίησή του με προσθήκη νέων,

[311] Είναι νομικά αδιάφορη ήτοι η διάρκεια του αποκλεισμού του διαχειριστή για τη στοιχειοθέτηση της αντικειμενικής υπόστασης της αξιόποινης πράξης του για αλλοίωσης ψηφιακών δεδομένων, εφόσον ο δικαιούχος διαχειριστής διατηρεί το ενδιαφέρον ακώλυτη πρόσβαση σε αυτά μεταξύ άλλων Valerius, επίσης Gercke/Bruns.

[312] Συμεωνίδου – Καστανίδου, Επιθέσεις κατά συστημάτων πληροφοριών, σελ. 73 προς την ίδια κατεύθυνση (σκέψη 69) της Επεξηγηματικής Έκθεσης της Σύμβασης της Βουδαπέστης, που ορίζει ότι η αποστολή μη ζητηθέντων μηνυμάτων ηλεκτρονικού ταχυδρομείου (unsolicited e-mail), για εμπορικούς ή άλλους σκοπούς, μπορεί να προκαλέσει ενόχληση στον παραλήπτη, ιδίως όταν τα μηνύματα αυτά αποστέλλονται σε μεγάλες ποσότητες ή με μεγάλη συχνότητα ("spamming"). Κατά τη γνώμη των εκπονούντων το κείμενο της Σύμβασης, η συμπεριφορά αυτή θα πρέπει να ποινικοποιείται μόνο όταν η επικοινωνία παρεμποδίζεται σκόπιμα και σοβαρά.

[313] Α. Αργυρόπουλο, ό.π., σελ.98, ο οποίος αντιδιαστέλλει τη «λογική» αυτή διαγραφή (logisches Löschen) από τη φυσική διαγραφή (physisches Löschen), επερχόμενη με την εξαφάνιση ή βλάβη του υλικού φορέα. Για την έννοια της διαγραφής επίσης βλ. MüKoStGB/Wieck-Noodt, 4η έκδοση 2022, StGB § 303a Rn. 12

με τις οποίες προσβάλλεται η ακεραιότητα του περιεχομένου των δεδομένων ως μέρους του συστήματος.[314]

Τέλος, τρόπο τέλεσης της πράξης σοβαρής παρεμπόδισης ή διακοπής συνιστά και ο *αποκλεισμός της πρόσβασης (access*) του δικαιούχου στα δεδομένα, που επεξεργάζεται μέσω του συστήματος. [315]

Χαρακτηριστικά παραδείγματα αποτελούν η αθέμιτη κρυπτογράφηση (encryption) και το «κλείδωμα» των ψηφιακών δεδομένων με αλλαγή χωρίς δικαίωμα του συνθηματικού (password) ή άλλου κωδικού ασφαλείας προκαλώντας έτσι αδυναμία χρήσης τους (Unbrauchbarmachen). Επίσης εδώ υπάγεται και η κρυφή εγκατάσταση από το δράστη «λυτρισμικού» (Ransomware), καθώς και το κατέβασμά του (download) από το ίδιο το θύμα, παραπλανώμενο ωστόσο από τον πρώτο για τη φύση και τις ιδιότητες του λογισμικού αυτού, που έχει ως αποτέλεσμα την κρυπτογράφηση (encryption) και επομένως τον αποκλεισμό της πρόσβασης του δικαιούχου. [316]

8.3.6. Σοβαρή παρεμπόδιση ή διακοπή ως αποτέλεσμα

Ως παρεμπόδιση [317] νοείται «κάθε πράξη παρεμβολής στη λειτουργικότητα ενός υπολογιστικού συστήματος», δηλαδή στην ικανότητά του να επεξεργάζεται με ορθό τρόπο ψηφιακά δεδομένα και επομένως κάθε πράξη με την οποία δυσχεραίνεται η ομαλή λειτουργία του συστήματος.

Ωστόσο, για τη θεμελίωση του ποινικά άδικου χαρακτήρα της πράξης του δράστη τίθεται ως προϋπόθεση η σοβαρή παρεμπόδιση (serious hindering) σε εναρμόνιση, εξαιρουμένων έτσι εξ ορισμού από την αντικειμενική υπόσταση του εγκλήματος περιπτώσεων ήσσονος σημασίας παρεμβολών, όπως η απλή διακινδύνευση και η ελαφριά παρακώλυση της λειτουργίας του συστήματος. Τούτο άλλωστε ευθυγραμμίζεται και με τη βασική αρχή λειτουργίας του ποινικού δικαίου ως έσχατου μέσου προστασίας (ultima-ratio-principle).

Στην Αιτιολογική Έκθεση της Σύμβασης καταγράφεται ως ενδεικτικό κριτήριο, που συνιστά ερμηνευτικό εργαλείο για τον εθνικό εφαρμοστή του δικαίου, η αποστολή δεδομένων από το δράστη (πχ εισαγωγή μολυσματικού ιού ή υποβολή ερωτημάτων διαδικτυακής σύνδεσης στο πλαίσιο επιθέσεων που επιφέρουν αδυναμία εξυπηρέτησης) σε τέτοια μορφή, μέγεθος και συχνότητα, ώστε να επηρεάζεται σημαντικά η δυνατότητα του δικαιούχου να χρησιμοποιήσει το σύστημα ή να επικοινωνήσει με άλλα συστήματα. Αναφέρεται μάλιστα ότι τα κράτη-μέλη μπορούν να ορίσουν μία ελάχιστη ποσότητα (minimum amount) δεδομένων, υπαγόμενη στην έννοια της «σοβαρής παρεμπόδισης».[318]

---

[314] Βλ. και Α. Αργυρόπουλο, ό.π., σελ. 103.

[315] Η τυποποίηση αυτού του τρόπου τέλεσης έγινε κατ΄ εναρμόνιση του Έλληνα νομοθέτη με το άρθρο 5 Οδηγίας όπου περιλαμβάνεται στους ποινικά αποδοκιμαστέους τρόπους παρεμβολής και ο συγκεκριμένος τρόπος τέλεσης εν αντιθέσει με το αντίστοιχο άρθρο 5 της Σύμβασης, στο οποίο δε γίνεται σχετική αναφορά.

[316] Π. Τουργέλης, ό.π., σελ. 317

[317] Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης, σκέψη 66

[318] Σκέψη 67 Αιτιολογικής Έκθεσης της Σύμβασης. Αντίθετα στο γερμανικό νομοσχέδιο του 41ου Τροποποιητικού νόμου, BT-Drs 16/3656, σελ. 13, για την ερμηνεία του όρου σημαντική διατάραξη (erhebliche Störung) εσφαλμένα επιλέχθηκε ο όρος "nicht unerhebliche Beeinträchtigung", δηλαδή «όχι ασήμαντη προσβολή», επιτρέποντας έτσι την υπαγωγή και ενδιάμεσων περιπτώσεων παρεμπόδισης λειτουργίας, που δεν επηρεάζουν αποφασιστικά την ικανότητα του συστήματος για επεξεργασία ψηφιακών δεδομένων.

Μεταξύ των κριτηρίων εξειδίκευσης της έννοιας της «σοβαρής παρεμπόδισης» πρέπει να συμπεριληφθεί από τον εφαρμοστή του δικαίου και η ένταση [319] της παρακώλυσης λειτουργίας, δηλαδή ο βαθμός δυσχέρανσης της δυνατότητας του δικαιούχου για την αξιοποίηση της λειτουργικότητας του συστήματος, καθώς επίσης και η ουσιώδης σημασία για το δικαιούχο διαχείρισης[320] του πληροφοριακού συστήματος. Αντίθετα, η διάρκεια της παρεμπόδισης χρήσης του συστήματος δεν συνιστά εξ ορισμού αποφασιστικό κριτήριο συνδρομής της έννοιας «σοβαρή παρεμπόδιση» και επομένως συνθεμελιωτικό στοιχείο του αδίκου της συμπεριφοράς του δράστη.

Περαιτέρω, η διακοπή του συστήματος αναφέρεται στον ολικό τερματισμό της λειτουργίας του συστήματος, δηλαδή σε μία βαρύτερης μορφής βλάβη του έννομου αγαθού της ασφάλειας, στις ειδικότερες εκφάνσεις της ακεραιότητας και διαθεσιμότητας, την οποία ωστόσο ο Έλληνας νομοθέτης αξιολόγησε ως αποτέλεσμα, που έχει ανάλογη ηθικοκοινωνική απαξία σε σχέση με την παρεμπόδιση, απειλώντας με το ίδιο πλαίσιο ποινής, ήτοι φυλάκιση (από 10 ημέρες έως 5 έτη) και χρηματική ποινή.

8.3.7. Αιτιώδης συνάφεια

Η σοβαρή παρεμπόδιση ή διακοπή του συστήματος θα πρέπει να συνιστά αποτέλεσμα της συμπεριφοράς του δράστη, σύμφωνα με την κρατούσα θεωρία του ισοδυνάμου των όρων. Επομένως, δεν υφίσταται αιτιώδης συνάφεια, όταν το αποτέλεσμα επέρχεται τελικά από μία απρόσμενη διακοπή ηλεκτροδότησης ή οφείλεται σε βλάβη του υλισμικού από παρένθετη ενέργεια του δικαιούχου.

8.4. Λόγοι άρσης του αδίκου

Εν προκειμένω τυγχάνουν εφαρμογής γενικοί λόγοι άρσης που συνιστούν εξουσιοδότηση από την έννομη τάξη για την παρεμβολή σε πληροφοριακό σύστημα που διαχειρίζεται άλλο πρόσωπο, όπως η άμυνα (άρθρο 22 ΠΚ) και η κατάσταση ανάγκης (άρθρο 25 ΠΚ).

8.5. Υποκειμενική υπόσταση

Του νόμου μη διακρίνοντος και δεδομένης της πλημμελληματικής φύσεως του εγκλήματος, για την πλήρωση της υποκειμενικής υπόστασης του εγκλήματος του άρθρου 292Β ΠΚ απαιτείται δόλος, οποιουδήποτε βαθμού, αρκούντος και του ενδεχόμενου, ο οποίος να αναφέρεται στα στοιχεία της αντικειμενικής υπόστασης.

8.6. Διακεκριμένες παραλλαγές

Στην παράγραφο 2 τυποποιούνται τρεις διακεκριμένες παραλλαγές του βασικού εγκλήματος.

Α) Χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημιές. Η επίταση της ποινικής απαξίας της περιγραφόμενης εγκληματικής συμπεριφοράς θεμελιώνεται στη χρήση από το δράστη «εργαλείου που έχει σχεδιαστεί κατά

[319] Ν.Χατζηνικολάου, ό.π., σελ. 189. Επομένως μία ελαφριά μείωση της ταχύτητας του συστήματος δεν μπορεί να θεωρηθεί «σοβαρή παρεμπόδιση»

[320] Στο 303b γερμ.ΠΚ (Computersabotage), η ουσιώδης σημασία (wesentliche Bedeutung) για το δικαιούχο συνιστά στοιχείο της αντικειμενικής υπόστασης και επομένως συνθεμελιωτικό στοιχείο του ποινικού αδίκου της συμπεριφοράς του δράστη.

κύριο λόγο για πραγματοποίηση επιθέσεων, που επηρεάζουν μεγάλο αριθμό [321] συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημιές».

Η ratio του βαρύτερου ποινικού αδίκου της πράξης εντοπίζεται σε ένα αφηρημένο κίνδυνο προσβολής τους μέσω αξιοποίησης από το δράστη ενός τεχνικού εργαλείου που έχει ως κύριο λειτουργικό προορισμό τη διενέργεια μαζικών επιθέσεων κατά της ακεραιότητας και διαθεσιμότητας. Δεν απαιτείται όμως για να συγκροτηθεί η διακεκριμένη μορφή το εγκλήματος, να επήλθε κάποιο από τα προαναφερόμενα αποτελέσματα, δηλαδή ούτε να επηρεάστηκε μεγάλος αριθμός πληροφοριακών συστημάτων ούτε να προκλήθηκε οικονομική ζημία ιδιαίτερα μεγάλης αξίας[322] κ.λπ. Παράδειγμα αποτελεί η χρήση μολυσματικού λογισμικού (malware) για την παρεμπόδιση ή τη διακοπή της λειτουργίας χιλιάδων πληροφοριακών συστημάτων ατόμων ή κρατικών υπηρεσιών σε παγκόσμια κλίμακα, [323] σε εναρμόνιση έτσι του νομοθέτη με το πλαίσιο ποινικοποίησης της Οδηγίας για την αναγκαία αντιμετώπισή τους με την υιοθέτηση βαρύτερων ποινικών κυρώσεων.

Ως «εργαλεία» νοούνται συσκευές ή προγράμματα υπολογιστή τα οποία χρησιμοποιεί ο δράστης για να παρεμποδίσει σοβαρά ή να διακόψει τη λειτουργία ενός πληροφοριακού συστήματος, εισάγοντας, διαγράφοντας, καταστρέφοντας ή αλλοιώνοντας τα ψηφιακά του δεδομένα ή αποκλείοντας την πρόσβαση στα δεδομένα αυτά. Συμπεριλαμβάνονται τα εργαλεία που μπορούν να δημιουργούν «botnet», δηλαδή δίκτυα προγραμμάτων ρομπότ που προσβάλλουν σημαντικό αριθμό υπολογιστών μέσω της μόλυνσης τους με το κακόβουλο λογισμικό, με συνέπεια ο δράστης να αποκτά από απόσταση έλεγχο των προσβεβλημένων υπολογιστών, εν αγνοία των χρηστών τους και με σκοπό την εξαπόλυση επιθέσεων στον κυβερνοχώρο μεγάλης κλίμακας, η οποία μπορεί να προκαλέσει σοβαρές ζημίες. [324]

Β) Πρόκληση σοβαρής ζημίας

Η αναγκαιότητα ποινικής αντιμετώπισης επιθέσεων, που προκαλούν σοβαρή ζημία, καταδείχθηκε στην Οδηγία 2013/40/ΕΕ, με την οποία καταλείπεται διακριτική ευχέρεια στα κράτη -μέλη για τον προσδιορισμό της έννοιας αυτής. [325] Ομοίως, σναφορά στην ποινική μεταχείριση επιθέσεων κατά πληροφοριακών συστημάτων με περαιτέρω συνέπεια την πρόκληση σοβαρής ζημίας, γίνεται και στη Σύμβαση της Βουδαπέστης, όπου παρέχεται η διακριτική ευχέρεια θεμελίωσης του ποινικού αδίκου της συμπεριφοράς του δράστη στην πρόκληση σοβαρής ζημίας, στο πλαίσιο ωστόσο της παρ. 2 του άρθρου 4, με το οποίο προωθείται η αυτοτελής ποινικοποίηση των πράξεων παρεμβολών σε δεδομένα και όχι σε

[321] Ενώ στο άρθρο 9 παρ.3 της Οδηγίας, γίνεται λόγος για «σημαντικό» αριθμό, δηλαδή μία ευρύτερη έννοια σε σχέση με αυτή του «μεγάλου αριθμού» που επελέγη από τον Έλληνα νομοθέτη.

[322] Στο άρθρο 303b παρ.4 αρ. 1 γερμ.ΠΚ (Computersabotage), ορίζεται αυθεντικά, με ενδεικτική ερμηνεία, το εννοιολογικό πλάτος της έννοιας της «σοβαρής ζημίας», όπου ορίζει "μια ιδιαίτερα σοβαρή περίπτωση συντρέχει κατά κανόνα, όταν ο δράστης προκαλεί μεγάλης έκτασης περιουσιακή απώλεια".

[323] Εδώ εντάσσεται η προσβολή της λειτουργίας υπολογιστικών συστημάτων, που έχουν καταστεί «νεκροζώντανα» (zombies), ενταχθέντα από το δράστη σε μολυσματικό ρομποτικό δίκτυο, όπως αναφέρεται ενδεικτικά στην υπ' άρ 13 Αιτιολογική Σκέψη.

[324] Βλ. άρθρο 5 προοιμίου Οδηγίας 2013/40/ΕΕ.

[325] Σύμφωνα με τη 13η Αιτιολογική Σκέψη της Οδηγίας: «(ε)ίναι σκόπιμο να προβλεφθούν αυστηρότερες κυρώσεις … όταν η επίθεση στον κυβερνοχώρο διαπράττεται σε μεγάλη κλίμακα και πλήττει έτσι σημαντικό αριθμό συστημάτων πληροφοριών, συμπεριλαμβανομένης της επίθεσης που έχει ως στόχο τη δημιουργία «botnet» ή όταν η επίθεση στον κυβερνοχώρο προκαλεί σοβαρές ζημίες, μεταξύ άλλων όταν η επίθεση εκτελείται μέσω «botnet»…»

αυτό του άρθρου 5, όπου προωθείται η ποινικοποίηση των παρεμβολών σε συστήματα πληροφοριών.

Ο όρος «σοβαρή ζημία» παραπέμπει σε μία αξιολογική έννοια, [326] για τον προσδιορισμό της οποίας ο Έλληνας νομοθέτης προέβη σε μία αυθεντική, ενδεικτική ερμηνεία, εντάσσοντας στο εννοιολογικό της πλάτος, μεταξύ άλλων, και την πρόκληση «οικονομικής ζημίας ιδιαίτερα μεγάλης αξίας», κατ' αντιστοιχία με άλλες έννομες τάξεις του ηπειρωτικού ευρωπαϊκού χώρου και της μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, όπως στις περιπτώσεις πολύμηνης δυσλειτουργίας συστημάτων πληροφοριών μίας εταιρείας που έχει καταστεί στόχος κατανεμημένων επιθέσεων άρνησης εξυπηρέτησης (DDoS-Attacks). Τέλος, ως σοβαρή ζημία κατά τον Έλληνα νομοθέτη νοείται και η σημαντική απώλεια δεδομένων του δικαιούχου. Πρόκειται για τη λογική βλάβη (logical damage) του συστήματος που επέρχεται με τη διαγραφή, καταστροφή [327] και βλάβη μίας σημαντικής ποσότητας επεξεργαζόμενων ψηφιακών δεδομένων. Εδώ θα πρέπει να υπαχθεί η διαγραφή ή βλάβη ενός δοκιμίου, επιστημονικού συγγράμματος, ιατρικού φακέλου και αρχείου πολυσέλιδης δικογραφίας σε ψηφιακή μορφή.

Γ) Παρακώλυση λειτουργίας συστήματος πληροφοριών που αποτελεί μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες

Ιδιαίτερα διακεκριμένη παραλλαγή διαπλάσσεται στο στοιχείο γ' της παραγράφου 2 του άρθρου 292Β ΠΚ, σε εναρμόνιση ιδίως με το ενωσιακό πλαίσιο, όπου επισημαίνεται η ανάγκη αυξημένης προστασίας υποδομών ζωτικής σημασίας από τα κράτη μέλη. [328]

Η ως άνω διάταξη αναφέρεται στο έγκλημα εκείνο που τελείται κατά ζωτικής σημασίας αγαθών ή υπηρεσιών, όπως, ιδίως: η εθνική άμυνα (π.χ. συστήματα επικοινωνίας των Ενόπλων Δυνάμεων), η υγεία (π.χ. δίκτυα δημόσιων νοσοκομείων), οι συγκοινωνίες (π.χ. δίκτυα δημόσιων συγκοιινωνιών), οι μεταφορές (π.χ. δίκτυα μεταφορών) και η ενέργεια (π.χ. δίκτυα εγκαταστάσεων παραγωγής ενέργειας), σε περιπτώσεις, δηλαδή, όπου υπάρχει σοβαρός κίνδυνος διάχυσης των αποτελεσμάτων της αξιόποινης συμπεριφοράς στον ευρύ κοινωνικό χώρο, με την τρώση ενός πληροφοριακού συστήματος ενταγμένου σε υποδομή, που εξυπηρετεί την μαζική προμήθεια σε αόριστο αριθμό ανθρώπων των ως άνω αγαθών.

8.7. Ειδικές μορφές εμφάνισης του εγκλήματος

8.7.1. Απόπειρα

Δοθέντος ότι η διάταξη θεσπίζει έγκλημα αποτελέσματος που είναι δεκτικό απόπειρας, στην περίπτωση π.χ. που ο δράστης αποστέλλει σε ηλεκτρονικό σύστημα ψηφιακά αρχεία που είναι πράγματι δυνατό να προκαλέσουν τη σοβαρή παρεμπόδιση της λειτουργίας του, τούτο

[326] Οι αξιολογικές έννοιες αντιδιαστέλλονται όμως από τις περιγραφικές έννοιες, διότι «αναφέρονται σε δεδομένα που δεν είναι αισθητά ή αντιληπτά από μόνα τους, αλλά μπορεί κανείς να τα φανταστεί και να τα καταλάβει μόνο σε συσχετισμό με τον κόσμο των κανόνων. (K. Engisch, Εισαγωγή στη νομική σκέψη, μετάφραση Δ.Σπινέλλη, σελ. 133 επ.).

[327] Εισφέρεται από Τουργέλη το βιβλιογραφικό παράδειγμα από E.Hilgendorf, Grundfalle zum Computerstrafrecht, JuS 1996, σελ. 1082: «Ο Α είναι ένας φοροτεχνικός σύμβουλος, που διαχειρίζεται τα λογιστικά θέματα της εταιρείας του Χ. Όταν ο τελευταίος κατήγγειλε της μεταξύ τους εργασιακή σχέση, ο Α αποφάσισε να τον εκδικηθεί, καταστρέφοντας όλα τα δεδομένα του υπολογιστικού συστήματος της εταιρείας του. Με τον τρόπο αυτό προέκυψε για τον Χ μία σημαντική περιουσιακή ζημία».

[328] Βλ. την υπ' αρ. 4 σε συνδυασμό με την υπ' αρ 13 Αιτιολ. Σκέψη της Οδηγίας 2013/40/ΕΕ και την υπ' αρ. 8 Αιτιολ. Σκέψη της Οδηγίας 2008/114/ΕΚ.

όμως δεν συμβαίνει επειδή ο χρήστης αντιλαμβάνεται την επικινδυνότητα του ηλεκτρονικού μηνύματος και δεν ανοίγει το συνημμένο μολυσμένο αρχείο ή ακόμη όταν η επίθεση αποκρούεται από την έγκαιρη κινητοποίηση των υπευθύνων ασφαλείας του συστήματος. Αν πάντως επρόκειτο για επίθεση που αποκρούστηκε ευχερώς από διαθέσιμο «τείχος προστασίας» του συστήματος θα πρόκειται για απρόσφορη απόπειρα, αφού το αποτέλεσμα δεν ήταν εξ αρχής δυνατό να επέλθει. [329]

8.7.2. Συμμετοχή

Στο έγκλημα είναι νοητή κάθε μορφή συμμετοχής κατά τα άρθρα 45 – 47 ΠΚ. Η παροχή από μέρους ενός προγραμματιστή σε ένα τρίτο πρόσωπο ενός εργαλείου διπλής χρήσης (dual use tool), παύει να συνιστά αξιολογικά ουδέτερη συμπεριφορά, εφόσον ο πρώτος γνωρίζει την αξιοποίηση του τεχνικού εργαλείου από το δράστη για τη τέλεση πληροφοριακού «σαμποτάζ» στοιχειοθετώντας ποινική ευθύνη για συνέργεια, εφόσον πληρούται ο απαιτούμενος διπλός δόλος. [330]

8.7.3. Συρροή

Όπως έχει αναλυθεί, με το άρθρο 292Β ΠΚ προστατεύεται ως κοινωνικό έννομο αγαθό[331], δηλαδή ως αγαθό του κοινωνικού συνόλου, οποιοδήποτε πληροφοριακό σύστημα, στο επιμέρους συστατικό στοιχείο της διαθεσιμότητάς του, όπως και δευτερευόντως η ακεραιότητα των ίδιων των ψηφιακών δεδομένων του συστήματος. Τούτου δοθέντος, η διάταξη συρρέει αληθινά με άλλες διατάξεις που προστατεύουν ατομικά έννομα αγαθά. Στα πλαίσια αυτά, η εξέταση της συρροής μεταξύ του εγκλήματος του πληροφορικού σαμποτάζ και της αθέμιτης πρόσβασης, που ανακύπτει στις περιπτώσεις εκείνες, στις οποίες ο δράστης με την αθέμιτη πρόσβαση επιφέρει περαιτέρω και σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας του πληροφοριακού συστήματος του δικαιούχου. Μεταξύ των δύο εγκλημάτων, λόγω ταυτότητας του προσβαλλόμενου έννομου αγαθού, δηλαδή της ασφάλειας των πληροφοριακών συστημάτων και δεδομένων, πρέπει να γίνει δεκτή η φαινομενική πραγματική συρροή. Συγκεκριμένα, η διάταξη του άρθρου 292Β θα απωθήσει αυτήν του άρθρου 370Β κατά την αρχή της (σιωπηρής) επικουρικότητας (λογική-αξιολογική σχέση), αφού η παρακώλυση λειτουργίας του συστήματος συνιστά «εμβάθυνση» της εγκληματικής προσβολής του ίδιου έννομου αγαθού, δηλαδή της πληροφορικής ασφάλειας, στις ειδικότερες λειτουργικές πτυχές της ακεραιότητας και διαθεσιμότητας του συστήματος.

Σε περίπτωση όμως που παρεμποδίζεται σοβαρά ή διακόπτεται η λειτουργία πληροφοριακού συστήματος, το οποίο αποτελεί μέρος εγκατάστασης παροχής στο κοινό τηλεφωνικών ή ηλεκτρονικών επικοινωνιών (κοινωφελής εγκατάσταση), η διάταξη του άρθρου 292Β ΠΚ συρρέει κατ' ιδέαν φαινομενικά με εκείνη του άρθρου 292Ε ΠΚ, οπότε θα εφαρμόζεται η τελευταία, η οποία αφενός μεν τιμωρεί την πράξη με βαρύτερη ποινή (φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή) σε σύγκριση με εκείνη του άρθρου 292Β παρ. 1 ΠΚ (φυλάκιση και χρηματική ποινή), αφετέρου δε αποτελεί ειδική διάταξη σε

[329] Ν. Χατζηνικολάου, ό.π, σελ. 192

[330] Τουργέλης με περαιτέρω παραπομπή σε A.Böken

[331] Κοινωνικό αγαθό δηλαδή μπορεί να είναι υλικό αντικείμενο, φυσική ιδιότητα υλικού αντικειμένου ή κοινωνική ιδιότητα υλικού αντικειμένου για τη διατήρηση του οποίου (κοινωνικού αγαθού) υπάρχει ουσιώδες ατομικό ή συλλογικό συμφέρον. Α. Τσέτουρα, Το θεσμικό πλαίσιο της κοινωνικής εργασίας, 2022, σ. 10 = sakkoulas-online με περαιτέρω παραπομπή σε Ι. Μανωλεδάκης, Επιτομή Γενικού Μέρους, ζ΄ έκδοση, Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2005, σ. 13.

σχέση με εκείνη του άρθρου 292Β ΠΚ, διότι αναφέρεται σε συγκεκριμένο είδος πληροφοριακών συστημάτων και δη εκείνων που εξυπηρετούν τις τηλεφωνικές και ηλεκτρονικές επικοινωνίες του κοινού.[332]

Ομοίως φαινομενική κατ' ιδέαν συρροή υφίσταται μεταξύ του εγκλήματος της παρακώλυσης λειτουργίας πληροφοριακών συστημάτων που αποτελούν μέρος υποδομών ζωτικής σημασίας για το κοινωνικό σύνολο (292Β παρ. 2 στ. γ΄) και του εγκλήματος που τυποποιείται στο άρθρο 293 παρ.1 ΠΚ, λόγω κάλυψης της εγκληματικής απαξίας τους από μία διάταξη. Συγκεκριμένα, θα επικρατήσει ως αυστηρότερη η διάταξη του άρθρου 292Β παρ.2 στοιχ.γ' ΠΚ έναντι της διάταξης του άρθρου 293 παρ.1 ΠΚ με βάση την αρχή της σιωπηρής επικουρικότητας (λογική-αξιολογική σχέση). Η τελευταία διάταξη θα εφαρμόζεται στις υπόλοιπες περιπτώσεις, δηλαδή όταν η παρακώλυση λειτουργίας κοινωφελών εγκαταστάσεων δεν τελείται με αθέμιτη παρέμβαση σε σύστημα πληροφοριών.[333]

Τέλος, αξιολογείται η σχέση της «ψηφιακής εκβίασης» (cyber extortion/digitale Erpressung) με το αδίκημα της παρακώλυσης πληροφοριακών συστημάτων. Στο πλαίσιο της παρούσας προβληματικής, ο όρος αυτός αναφέρεται στην τέλεση δύο αξιόποινων πράξεων από το δράστη, που αντιμετωπίζονται στον ισχύοντα ποινικό κώδικα με τις διατάξεις των άρθρων 292Β και 385 ΠΚ. Η συνηθέστερη περίπτωση συρροής ανακύπτει στη χρήση λυτρισμικού (ransomware), το οποίο ο δράστης εγκαθιστά στο πληροφοριακό σύστημα του παθόντος προβαίνοντας χωρίς δικαίωμα σε κρυπτογράφηση ψηφιακών δεδομένων του τελευταίου. Η παρακώλυση λειτουργίας του προσβαλλόμενου πληροφοριακού συστήματος (292Β παρ.1 ΠΚ) τελείται εν προκειμένω με αποστέρηση της δυνατότητας πρόσβασής του παθόντος στα δεδομένα που διαχειρίζεται. Εν συνεχεία ο δράστης προβαίνει σε απειλή διαγραφής ψηφιακών δεδομένων για να εξαναγκάσει το θύμα να προβεί σε μία πράξη, δηλαδή να καταβάλει «λύτρα», συνήθως σε κρυπτονόμισμα, προκειμένου να αποκρυπτογραφηθούν τα δεδομένα του και να αποκτήσει έτσι εκ νέου πρόσβαση σε αυτά, έχοντας σκοπό παράνομου περιουσιακού οφέλους, που αντιστοιχεί σε περιουσιακή ζημία του τελευταίου ή άλλου προσώπου. [334] Η συρροή των ως άνω αδικημάτων κρίνεται αληθινή, διότι το προστατευόμενο έννομο αγαθό εκάστης διάταξης διαφέρει.

8.8. Ποινική δίωξη – υποστήριξη της κατηγορίας

Το έγκλημα εφεξής είναι αυτεπαγγέλτως διωκόμενο, καθώς κρίθηκε ότι δύναται να πλήξει σημαντικό αριθμό ατόμων. [335] Για εκκρεμείς υποθέσεις προ της εφαρμογής του νέου Π.Κ., εφαρμόζεται, δυνάμει του άρθρου 2 ΠΚ, η προϊσχύσασα διάταξη, που απαιτούσε έγκληση του παθόντος, ως ευμενέστερη για τον κατηγορούμενο. Κατ' αντιστοιχία με τα ανωτέρω, δικαίωμα υποβολής εγκλήσεως είχαν ο νόμιμος κάτοχος του πληροφοριακού συστήματος, καθώς και ο δικαιούχος των πληττόμενων δεδομένων.

Δικαίωμα παράστασης προς υποστήριξη της κατηγορίας έχει ο νόμιμος κάτοχος του πληροφοριακού συστήματος (όχι απαραίτητα και του υλικού φορέα του, καθώς το εμπράγματο, περιουσιακό δικαίωμα επ' αυτού είναι αδιάφορο εν προκειμένω). [336]Το ίδιο

[332] Ε. Καμπέρου, ό.π., σελ. 2100
[333] Π. Τουργέλης, ό.π., σελ. 333
[334] Π. Τουργέλης, ό.π., σελ. 333
[335] Αιτολογική Έκθεση Νέου Π.Κ., σελ. 59 (https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/k-poinkod-eis-NEO.pdf)
[336] Ν. Χατζηνικολάου, ο.π., σελ. 200

δικαίωμα έχει και ο δικαιούχος των ψηφιακών δεδομένων, τα οποία ο δράστης καταστρέφει, αλλοιώνει, κ.λπ.. [337]

9. Η ποινικοποίηση των προπαρασκευαστικών πράξεων τέλεσης επιθέσεων κατά πληροφοριακών συστημάτων και δεδομένων στον ισχύοντα ποινικό κώδικα (292Γ ΠΚ).

Η ρύθμιση αποτελεί μεταφορά του άρθρου 6 της Σύμβασης της Βουδαπέστης και του άρθρου 7 της Οδηγίας 2013/40/ΕΕ.

Η διάταξη του άρθρου 292Γ ΠΚ προσετέθη με το άρθρο 2 παρ. 8 του Ν. 4411/2016 (ΦΕΚ Α/142/03-08-2016) και παρέμεινε απαράλλαχτη, ως προς την ειδική υπόσταση του εγκλήματος και μετά την εισαγωγή του νέου ΠΚ (Ν. 4619/2019, ΦΕΚ 95/Α/11-06-2019), αλλά μετεβλήθη προς επιεικέστερο πλαίσιο ποινής, με την πρόβλεψη της διαζευκτικής δυνατότητας επιβολής χρηματικής ποινής αντί φυλάκισης έως δύο (2) έτη.

Με την ποινικοποίηση συμπεριφορών κατασκευής, κατοχής και εν γένει διάθεσης εργαλείων “hacking” εμφαίνεται η πρόθεση του νομοθέτη να καταστείλει τις επικίνδυνες συμπεριφορές, που δεν συνιστούν αξιόποινη συνέργεια λόγω μη τέλεσης κύριας πράξης αθέμιτης πρόσβασης, υποκλοπής ή παρεμβολής στο σύστημα και στα δεδομένα του δικαιούχου και να προασπίσει το έννομο αγαθό της ασφάλειας πληροφοριακών συστημάτων και δεδομένων πληρέστερα.

Η δικαιοπολιτική επιλογή πρωθύστερης ποινικής αντιμετώπισης (Vorfeldkriminalisierung) επιθέσεων κατά της ασφάλειας πληροφοριακών συστημάτων και δεδομένων, εντάσσεται στο πλαίσιο μίας εξελισσόμενης δικαιοπολιτικής μετατροπής του ποινικού δικαίου «από κατασταλτικό εργαλείο τιμώρησης ex post σε προληπτικό εργαλείο αποτροπής κινδύνων ex ante», δηλαδή από κλασικό σε προληπτικό ποινικό δίκαιο (Präventionsstrafrecht) που έχει ως αποστολή, όχι την ποινική αντιμετώπιση κοινωνικά επιβλαβών συμπεριφορών, αλλά την παρεμπόδισή τους.[338]

9.1. Χαρακτηρολογικά γνωρίσματα

Με το άρθρο 292Γ ΠΚ τυποποιείται αδίκημα *αφηρημένης διακινδύνευσης* (abstrakte Gefährdungsdelikte), [339] θέση που επιρρωνύεται από τη δικαιοπολιτική επιλογή του νομοθέτη για αυτεπάγγελτη (και όχι κατ' έγκληση) δίωξη της πράξης και ενδεικνύει την αντίληψή του για τη διακινδύνευση ενός αόριστου αριθμού μονάδων εννόμου αγαθού της ασφάλειας πληροφοριακών συστημάτων και δεδομένων.[340]

[337] Ε. Καμπέρου, ό.π., σελ. 2101

[338] Π. Τουργέλης, ό.π., σελ. 337. Αντίστοιχη διάταξη εντοπίζεται στο γερμΠΚ και συγκεκριμένα στο άρθρο 202c StGB “Vorbereiten des Ausspähens und Abfangens von Daten”

[339] Ομοίως και το 202c γερμ ΠΚ όπως προκύπτει από BT-Drs. 16/3656 και BeckOK StGB/Weidemann, 58. Ed. 1.8.2023, StGB § 202c Rn. 3 ή αντίστοιχα το άρθρο 126c αυστρ.ΠΚ ή 144bis παρ. 2 ελβΠΚ.

[340] Ε. Καμπέρου, ό.π., σελ. 2102

Επιπροσθέτως, το αδίκημα συνιστά *υπαλλακτικώς μικτό* έγκλημα, δεδομένου ότι τυποποιούνται πλείονες μορφές τέλεσης του εγκλήματος, οι οποίες μάλιστα μπορούν να τελεστούν σωρευτικά από το δράστη, αποδίδοντας ωστόσο πάντα ένα έγκλημα.

Επιπλέον, με τη διάταξη του άρθρου 292Γ ΠΚ περιγράφεται ένα έγκλημα *απλής συμπεριφοράς*. Τούτο δε, διότι η ηθικοκοινωνική απαξία του εγκλήματος εντοπίζεται στην ενέργεια του δράστη, χωρίς να τυποποιείται κάποιο αποτέλεσμα αυτής ως ξεχωριστό στοιχείο της αντικειμενικής υπόστασης του εγκλήματος.

Τέλος, με την ως άνω διάταξη στοιχειοθετείται ένα έγκλημα υπερχειλούς υποκειμενικής υπόστασης, διότι για τη θεμελίωση ποινικής ευθύνης του δράστη της αξιόποινης προπαρασκευαστικής πράξης δεν αρκεί μία δόλια συμπεριφορά παραγωγής, πώλησης, προμήθειας προς χρήση, εισαγωγής, κατοχής, διανομής ή με άλλο τρόπο διακίνησης τεχνικών εργαλείων, αλλά απαιτείται επιπλέον σκοπός τέλεσης του εγκλήματος του άρθρου 292Β.

9.2. Αντικειμενική υπόσταση

9.2.1. Δράστης του εγκλήματος

Το αδίκημα χαρακτηρίζεται ως κοινό, γεγονός που συνεπάγεται ότι δράστης του εγκλήματος δύναται να είναι ο οιοσδήποτε. Αν όμως ο ίδιος ο δράστης του εγκλήματος του άρθρου 292Β ΠΚ, παρήγαγε, προμηθεύτηκε, εισήγαγε ή κατείχε εργαλεία από τα αναφερόμενα στην περ. α΄ ή β΄ του άρθρου 292Γ ΠΚ, με τη χρήση των οποίων τέλεσε κάποιο από τα προαναφερόμενα εγκλήματα, το έγκλημα του άρθρου 292Γ ΠΚ θα συρρέει πραγματικά φαινομενικά με το τελεσθέν έγκλημα και θα απορροφάται από αυτό με βάση τον κανόνα της προηγούμενης συντιμωρητής πράξης.[341]

9.2.2. Αντικείμενο του εγκλήματος

Αντικείμενο του εγκλήματος είναι το πληροφοριακό σύστημα και τα ψηφιακά δεδομένα επί των οποίων υφίσταται δικαίωμα διαχείρισης, που συνιστά τη «συγκεκριμενοποίηση» του εννόμου αγαθού της πληροφορικής ασφάλειας.

9.2.3. Πράξη προσβολής

Καταρχάς, αντικείμενο προστασίας της διάταξης συνιστά το έννομο αγαθό που μπορεί να διακινδυνεύσει μέσω των τιμωρητέων προπαρασκευαστικών πράξεων, δηλαδή εν προκειμένω το κοινωνικό έννομο αγαθό της διαθεσιμότητας και δευτερευόντως της ακεραιότητας του πληροφοριακού συστήματος και των δεδομένων του. Ήγουν, η ποινική προστασία του εννόμου αγαθού της ασφάλειας των πληροφοριακών συστημάτων και δεδομένων παρέχεται σε ένα προωθημένο στάδιο μέσω της τυποποίησης αξιολογικά ουδέτερων συμπεριφορών (neutrale Handlungen),[342] οι οποίες όμως τελούμενες με σκοπό τη διάπραξη επιθέσεων κατά των πληροφοριακών συστημάτων και δεδομένων, αποκτούν ουσιαστικό ποινικό άδικο.

Ειδικότερα, ως «*παραγωγή*» νοείται ο σχεδιασμός (design) και η δημιουργία των υπό 292Γ στοιχείο α’ συσκευών ή προγραμμάτων υπολογιστών και υπό στοιχείο β’ δεδομένων πρόσβασης, πρόσφορων για την τέλεση επιθέσεων κατά πληροφοριακών συστημάτων και ψηφιακών δεδομένων. Στη γερμανική θεωρία για τη στοιχειοθέτηση της ποινικής ευθύνης

[341] Ε. Καμπέρου, ό.π., σελ. 2102

[342] S. Ernst (επιμέλεια), Hacker, Cracker & Computerviren, Κολωνία: O. Schmidt Verlag, 2004, περιθωριακός αριθμός 393.

του δράστη παραγωγής «λογισμικού εργαλείου» (Software-Tool) κατά την αντίστοιχη παράγραφο 202c γερμ.ΠΚ, απαιτείται η δημιουργία λογισμικού να γίνεται όχι για ιδία χρήση, αλλά με πρόθεση περαιτέρω διάθεσης του προγράμματος σε τρίτον για την τέλεση μίας επίθεσης σε πληροφοριακό σύστημα. Η άποψη αυτή ερείδεται στην γενική ποινική διδασκαλία για κοινωνική έννοια της πράξης (sozialer Handlungsbegriff), η οποία πρέπει να ενέχει κοινωνικό νόημα, δηλαδή να αποτελεί «πράξη προς έτερον».[343]

Ως «*πώληση*» τεχνικών εργαλείων νοείται η συμφωνία διάθεσης επ' ανταλλάγματι των ως άνω συσκευών ή δεδομένων πρόσβασης σε τρίτο πρόσωπο, το οποίο αποσκοπεί στην χρήση τους για την διάπραξη επιθέσεων κατά πληροφοριακών συστημάτων.

Ως «*προμήθεια*» προς χρήση νοείται η με οποιονδήποτε τρόπο απόκτηση ή διάθεση της εξουσίας διαχείρισης των τεχνικών εργαλείων ή δεδομένων πρόσβασης για την τέλεση επιθέσεων.

Ως «*εισαγωγή*» νοείται η διάθεση στην Ελληνική Επικράτεια των ως άνω τεχνικών εργαλείων ή δεδομένων πρόσβασης από το δράστη με απώτερο σκοπό την χρήση αυτών για την διενέργεια επιθέσεων κατά της λειτουργικότητας συστημάτων πληροφοριών.

Ειδικά όσον αφορά την *κατοχή*, σημειώνεται αρχικά ότι ο ενωσιακός νομοθέτης δεν το συγκαταλέγει στις αξιόποινες μορφές τέλεσης των προπαρασκευαστικών αυτών πράξεων, [344] ενώ αντίθετα η Σύμβαση της Βουδαπέστης το περιλαμβάνει στο άρθρο 6. [345]

Ως κατοχή πρέπει να νοηθεί μία πραγματική σχέση φυσικής εξουσίασης ενός πράγματος από ένα πρόσωπο, αποτελώντας αυτονομημένη έννοια σε σχέση με την αντίστοιχη του αστικού δικαίου. Αναγκαίο εννοιολογικό στοιχείο της κατοχής συνιστά η φυσική βούληση και εξουσίασης. Παρά το γεγονός δε, ότι η πληροφορία λόγω της άυλης φύσης της δεν μπορεί να υπαχθεί, μέσω μίας απαγορευμένης αναλογικής ερμηνείας, στην έννοια του πράγματος, πρέπει να γίνει δεκτό ότι δίπλα στην έννοια της «κλασικής» κατοχής ενυπάρχει και μία διευρυμένη έννοια κατοχής, αναφερόμενη στην κυριαρχική εξουσία (Herrschaftsmacht) επί των δεδομένων, [346] διακριτή σε σχέση με την εξουσία επί του υλικού φορέα, όπως αντίστοιχα διακριτή έννοια συνιστά και η κυριότητα επί του υλισμικού (hardware) σε σχέση με το δικαίωμα διαχείρισης του συστήματος και των δεδομένων.

Η θεώρηση της κατοχής ως πράξης και κατ' επέκτασιν την ποινικοποίησή της εγείρει σημαντικά δογματικά προβλήματα παραβίασης της αρχής της αναλογικότητας, καθώς δεν συνιστά «συμπεριφορά προς έτερον» και συνεπώς δεν παρουσιάζει βλαπτικότητα, ούτε καν υπό μορφήν αφηρημένου κινδύνου. [347] Υποστηρίζεται [348] ότι αυτή δεν θα πρέπει να

---

[343] Kindhäuser/Neumann/Paeffgen/Saliger, Strafgesetzbuch, StGB vor § 13 Rn. 58, beck-online

[344] Άρθρο 7 της Οδηγίας

[345] «1. Κάθε συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος και από πρόθεση διάπραξη των κάτωθι:

α. ….

β. Κατοχή ενός αντικειμένου από τα αναφερόμενα στις παραγράφους α.ι και α.ιι ανωτέρω, με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση να υπάρχει κατοχή ενός αριθμού τέτοιων αντικειμένων πριν θεμελιωθεί ποινική ευθύνη.»

[346] Γ. Μπουρμά, Προσπάθειες εννοιολογικού προσδιορισμού της κατοχής ηλεκτρονικών δεδομένων με χαρακτήρα παιδικής πορνογραφίας, ΠοινΔ 2009, σελ. 324.

[347] Π. Τουργέλης, ο.π., σελ. 345, βλ. επίσης: Δ. Κιούπης, Πορνογραφία ανηλίκων σε: Προσφορά τιμής στην Α. Μπενάκη, σελ.: 245 επ.

[348] Ε. Καμπέρου, ό.π., σελ. 2103

τιμωρείται, εάν αφορά μικρό αριθμό τέτοιων «εργαλείων», καθώς, εάν δεν συνοδεύεται από άλλη εξωτερικευμένη ενέργεια του δράστη, δεν μπορεί να αποδείξει από μόνη της τον σκοπό τελέσεως εγκλήματος του α. 292Β ΠΚ. και πως, αντίθετα, η τιμώρηση αυτοτελώς της κατοχής προϋποθέτει σημαντικό αριθμό τέτοιου είδους εργαλείων, σε σημείο που να τεκμαίρεται, ή έστω να ενδεικνύεται, ο σκοπός της αξιόποινης χρήσης τους. [349]

Η *διανομή* συνιστά ενεργητική συμπεριφορά του δράστη με την οποία προωθεί τέτοια εργαλεία σε άλλους για την παρακώλυση λειτουργίας πληροφοριακών συστημάτων. [350]

Τέλος, η «*με άλλο τρόπο διακίνηση*» αναφέρεται σε λοιπές μορφές τέλεσης της πράξης του άρθρου 292Γ, οι οποίες δεν μπορούν να υπαχθούν στις ρητά τυποποιημένες συμπεριφορές και πάντως καθιστούν προσιτά για χρήση από αόριστο αριθμό προσώπων τα εργαλεία, τοποθετώντας τα "on line" στο διαδίκτυο προς χρήση άλλων.

9.2.4. Συσκευές, προγράμματα ηλεκτρονικών υπολογιστών, συνθηματικά, κωδικοί.

Στην πρώτη κατηγορία εντάσσονται οι συσκευές [351]και τα μολυσματικά προγράμματα, τα οποία έχουν ως λειτουργικό προορισμό την τέλεση επιθέσεων που αντιμετωπίζονται ποινικά από το άρθρο 292Β ΠΚ. Οι συσκευές δεν απαιτείται να είναι σχεδιασμένες ή προσαρμοσμένες αποκλειστικά και μόνο για να αξιοποιηθούν ως μέσα τέλεσης των εγκλημάτων του άρθρου 292Β ΠΚ, αλλά αρκεί να είναι σχεδιασμένες ή προσαρμοσμένες κυρίως για τον σκοπό τέλεσης κάποιου εγκλήματος από τα προαναφερόμενα, χωρίς δηλαδή να αποκλείεται να επιτελούν και νόμιμες λειτουργίες, συνιστώντας συσκευές «διπλής χρήσης» (dual-use devices). Τούτου δοθέντος, δεν συμπεριλαμβάνονται στις παραπάνω συσκευές τα απαραίτητα εργαλεία για την προστασία των ηλεκτρονικών υπολογιστών, όπως είναι ενδεικτικά τα προγράμματα «antivirus» και «firewall», τα οποία είναι εξαρχής σχεδιασμένα για να προστατεύουν τους υπολογιστές από επιθέσεις κακόβουλου λογισμικού. [352]

Σε μία δεύτερη κατηγορία τοποθετούνται συνθηματικά, κωδικοί πρόσβασης (passwords) και άλλα «παρεμφερή δεδομένα» πρόσβασης, όπως ψηφιοποιημένα βιομετρικά χαρακτηριστικά του δικαιούχου πρόσβασης, στα οποία συγκαταλέγονται τα χαρακτηριστικά ίριδας ματιού και τα δαχτυλικά αποτυπώματα, τα οποία διατίθενται στην αναπτυσσόμενη «μαύρη αγορά» [353] του «σκοτεινού διαδικτύου» (dark web) για την αθέμιτη πρόσβαση σε σύστημα πληροφοριών.

---

[349] βλ. σχετικώς και α. 74 Επεξηγηματικής Έκθεσης Σύμβασης της Βουδαπέστης

[350] Ε. Καμπέρου, ό.π., σελ. 2103 και Γ. Μπαμπινιώτη για τη γλωσσική ερμηνεία του όρου «διανομή», σελ. 495.

[351] Ο Έλληνας νομοθέτης επέλεξε να εντάξει σε αυτήν την ακτηγορία «εργαλείων» και την αξιοποίηση συσκευών (devices), δηλαδή μηχανημάτων κατηγορία (hardware), εναρμονιζόμενος έτσι με το άρθρο 6 της Σύμβασης, εν αντιθέσει με το αντίστοιχο άρθρο 7 της Οδηγίας, όπου δεν συμπεριλαμβάνονται οι συσκευές μεταξύ των «εργαλείων» για την τέλεση επιθέσεων κατά πληροφοριακών συστημάτων και δεδομένων. Στην παρ.3 του ως άνω άρθρου της Οδηγίας, παρέχεται η διακριτική ευχέρεια μη ποινικοποίησης της κατοχής, διάθεσης και διακίνησης τέτοιων συσκευών. Αξιοσημείωτο κρίνεται ότι χρήση αυτής της διακριτικής ευχέρειας έγινε από το Γερμανό Νομοθέτη κατά τη νομοτυπική διάπλαση της αντίστοιχης παρ. 202c γερμΠΚ, όπου δεν συγκαταλέγονται μεταξύ των εργαλείων τέλεσης επιθέσεων και οι συσκευές (devices).

[352] Ε. Καμπέρου, ό.π., σελ. 2103

[353] Explanatory Report, Nr.71. "…As the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. .."

Ενδιαφέρον παρουσιάζει εν προκειμένω η διάκριση ανάμεσα στη διακίνηση των κωδικών, που έχουν «γραφτεί» για την εκμετάλλευση των ευπαθειών «μηδέν (0) ημερών» (zero days exploits)[354] και στην «εμπορία» μόνο της γνώσης σχετικά με την ύπαρξη μίας πληροφορικής ευπάθειας. Αναφορικά με την πρώτη περίπτωση εντάσσεται στην έννοια των «μολυσματικών προγραμμάτων » Από την άλλη πλευρά, δυσχέρειες παρουσιάζει η εξέταση της δεύτερης περίπτωσης, καθώς δύσκολα μπορεί να υπαχθεί η παροχή γνώσης καθ' εαυτής, σχετικά με την ύπαρξη τρωτών σημείων πληροφορικής ασφάλειας (knowledge of vulnerability), στην έννοια των «παρεμφερών δεδομένων πρόσβασης».

9.2.5. Χωρίς δικαίωμα

Συγκριτικά με τις διατάξεις των άρθρων 292Β, 370Β και 370Ε εντοπίζεται η διαφορά στη δυνατότητα συγκατάθεσης του δικαιούχου, η οποία δεν μπορεί να νοηθεί σε ένα έγκλημα αφηρημένης διακινδύνευσης, ελλείψει συγκεκριμένου κινδύνου για το έννομο αγαθό. Κατά συνέπεια ο όρος «χωρίς δικαίωμα» συνιστά γενικό στοιχείο του αδίκου.

Όταν οι προβλεπόμενες πράξεις γίνονται κατόπιν εξουσιοδότησης του νόμιμου κατόχου του πληροφοριακού συστήματος για τη δοκιμή ή τη προστασία του πληροφοριακού συστήματος τελούνται με δικαίωμα του ενεργούντος και δεν εμπίπτουν καν στην αντικειμενική υπόσταση του εγκλήματος.[355] Ελλείψει κάποιας ειδικής ρύθμισης από τον Έλληνα νομοθέτη, εξετάζεται αποκλειστικά η συνδρομή γενικών λόγων άρσης του αδίκου, όπως είναι η ενάσκηση δικαιώματος για την παραγωγή λογισμικών διπλής χρήσης (dual-use-software) στο πλαίσιο ανάπτυξης της έρευνας για τη βελτίωση της ασφάλειας των πληροφοριακών συστημάτων.

Η πλάνη του δράστη ως προς την ύπαρξη δικαιώματος αποτελεί νομιζόμενο λόγο άρσης του αδίκου και εφόσον αφορά στις πραγματικές προϋποθέσεις συνδρομής του αξιολογείται ως ανάλογης μορφής πραγματική πλάνη που αποκλείει το δόλο άρθρο 30 παρ.1 εδ.ά) και επομένως την ποινική του ευθύνη.[356]

9.3. Υποκειμενική υπόσταση

Για τον καταλογισμό της πράξης στην ενοχή του δράστη απαιτείται πρόθεση, ήτοι τουλάχιστον ενδεχόμενος δόλος (όπως προκύπτει από το συνδυασμό των διατάξεων των άρθρων 18 και 26 ΠΚ), που πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης. Επιπροσθέτως, απαιτείται σκοπός τέλεσης των εγκλημάτων του άρθρου 292Β ΠΚ. Έτσι, ο δράστης πρέπει κατά τον χρόνο τέλεσης του εγκλήματος της παραγωγής, πώλησης, προμήθειας, διακίνησης κλπ. των συσκευών (ή προγραμμάτων ηλεκτρονικού

---

[354] A. C. Emery, Zero-day responsibility: the benefits of a safe harbor for cybersecurity research , HeinOnline, σελ. 247, όπου δίδεται ο ακόλουθος ορισμός: μια ευπάθεια «μηδέν (0) ημερών» είναι μια ευπάθεια που εντοπίζεται προτού την ανακαλύψει ο κατασκευαστής λογισμικού ή, αν την έχει ανακαλύψει ο κατασκευαστής, προτού ο κατασκευαστής μπορέσει να λάβει μέτρα για τη διόρθωσή της, καθώς και M. Fidler, Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis [article], HeinOnline, σελ. 409….. Ο όρος "ευπάθεια" μηδενικής ημέρας περιγράφει το ίδιο το ελάττωμα του λογισμικού. Όταν πωλείται μια ευπάθεια μηδενικής ημέρας, πωλείται η γνώση του ελαττώματος. Οι εκμεταλλεύσεις μηδενικής ημέρας ποικίλλουν σε πολυπλοκότητα και λειτουργικότητα, από το να επιτρέπουν την πρόσβαση σε ένα πρόγραμμα λογισμικού, την παρακολούθηση, την εξαγωγή πληροφοριών από αυτό ή την καταστροφή του. Για παράδειγμα, το πρόγραμμα Stuxnet που φέρεται να χρησιμοποιήθηκε από τις Ηνωμένες Πολιτείες για να καταστρέψει τις ιρανικές φυγόκεντρες εμπλουτισμού ουρανίου έκανε χρήση τεσσάρων ευπαθειών μηδενικής ημέρας.

[355] Ε. Καμπέρου, ό.π. σελ. 2104

[356] Π. Τουργέλης, ό.π., σελ. 2104

υπολογιστή ή συνθηματικών κ.λπ.) να έχει σκοπό να χρησιμοποιηθούν για την τέλεση κάποιου από τα προαναφερόμενα εγκλήματα. Διαπλάσσει συνεπώς ένα έγκλημα υπερχειλούς υποκειμενικής υπόστασης και αξιώνεται η συνδρομή ενός επιπλέον υποκειμενικού στοιχείου. Ακόμη, απαιτείται οι συσκευές κτλ που προμηθεύεται ή διακινεί να είναι πρόσφορες αντικειμενικά να επιφέρουν την τέλεση ενός από τα αναφερόμενα εγκλήματα. Επί παραδείγματι, δεν καταφάσκεται η συνδρομή της ως άνω προϋπόθεσης, όταν ο επιστήμονας ή ο "white hacker" που ελέγχει την ισχύ ενός συστήματος ασφάλειας πληροφοριών με δοκιμές διείσδυσης (penetration testing) είτε για το σκοπό προόδου της επιστήμης.[357]

Σε εναρμόνιση με το αντίστοιχο υπερεθνικό πλαίσιο, τελεί η διάταξη καθόσον αξιώνεται, όχι απλά πρόθεση, αλλά σκοπός διάπραξης επιθέσεων κατά πληροφοριακών συστημάτων και δεδομένων.[358] Δια μέσου αυτής της επιλογής αποφεύγεται ο κίνδυνος υπέρμετρης ποινικοποίησης (over-criminalisation) όταν απουσιάζει η επιδίωξη για αξιόποινη προπαρασκευαστική πράξη διακίνησης συνθηματικών πρόσβασης από «εισβολείς γκρι καπέλου» (gray hat hackers), οι οποίοι επιδιώκουν την ενημέρωση του κοινωνικού συνόλου, αποδεχόμενοι απλώς το ενδεχόμενο αξιοποίησης από «εισβολείς μαύρου καπέλου» (black hat hackers) για τις προσβολές συστημάτων πληροφοριών.[359]

9.4. Ειδικές μορφές εμφάνισης του εγκλήματος

9.4.1. Απόπειρα

Με δεδομένο ότι πρόκειται για έγκλημα επιχειρήσεως σύσσωμη η θεωρία δέχεται ότι πρέπει να αποκλειστεί η τιμωρία της απόπειρας, διότι με την αναγωγή αυτών των προπαρασκευαστικών πράξεων σε τυπικά ολοκληρωμένο και αυτοτελές έγκλημα εξαντλείται η δυνατότητα επέκτασης του αξιοποίνου στο στάδιο της απόπειρας. [360]

9.4.2. Συμμετοχή

Καταρχήν είναι νοητή κάθε μορφή συμμετοχής από τις προβλεπόμενες στα άρθρα 45 επ. του ΠΚ στο υπό εξέταση έγκλημα. Ενδεικτικά ποινική ευθύνη για συνέργεια δύναται να στοιχειοθετήσει για τον πάροχο φιλοξενίας, ο οποίος διαθέτει τη ψηφιακή πλατφόρμα, για τη διακίνηση ενός τεχνικού εργαλείου "hacking" από τρίτο πρόσωπο. Σαφώς, θα πρέπει να πληρούται η προϋπόθεση του διπλού συμμετοχικού δόλου, ήτοι αφενός άμεσος δόλος συνδρομής στην τέλεση της αξιόποινης πράξης και αφετέρου δόλος που αντιστοιχεί στο δόλο του φυσικού αυτουργού, δηλαδή ενδεχόμενος δόλος για όλα τα στοιχεία της αντικειμενικής υπόστασης.

9.4.3. Συρροή

Σε περίπτωση που ο αυτουργός του εγκλήματος του άρθρου 292Γ ΠΚ, της αξιόποινης προσπαρασκευαστικής πράξης (Vorfeldtäter) ήγουν, καταστεί και αυτουργός ή συμμέτοχος σε μια κύρια άδικη συμπεριφορά κατά της ακεραιότητας και διαθεσιμότητας ενός πληροφοριακού συστήματος, ενόψει του γεγονότος ότι με τη δεύτερη πράξη αποπερατώνει ουσιαστικά το πρώτο έγκλημα, τα δύο αδικήματα τελούν σε σχέση πραγματικής

[357] Ε. Καμπέρου, ό.π. σελ. 2104

[358] Επεξηγηματική έκθεση, σκέψη 75 "πρέπει να υπάρχει ο συγκεκριμένος (δηλαδή άμεσος) σκοπός ότι η συσκευή χρησιμοποιείται για τη διάπραξη οποιουδήποτε από τα αδικήματα που προβλέπονται στα άρθρα 2-5 της Σύμβασης".

[359] Π. Τουργέλης, ό.π., σελ. 350

[360] πρβλ. Μανωλεδάκης, Επιτομή, Ε΄ έκδοση, 373

φαινομενικής συρροής και θα επικρατήσει η διάταξη του άρθρου 292Β, κατά την αρχή της επικουρικότητας (Subsidiaritätsgrundsatz).[361]

Αντίστοιχα, το ίδιο πρέπει να γίνει δεκτό και για τη συρροή με τα εγκλήματα των άρθρων 370Β και 370Ε λόγω ταυτότητας του προσβαλλόμενου εννόμου αγαθού, ήτοι της ασφάλειας των πληροφοριακών συστημάτων και ψηφιακών δεδομένων.

9.5. Ποινικές κυρώσεις

Η επαπειλούμενη ποινική κύρωση των προπαρασκευαστικών πράξεων κατοχής και εν γένει διάθεσης εργαλείων χάκινγκ, επέλεξε ο Έλληνας νομοθέτης να συνίσταται είτε φυλάκιση έως δύο έτη ή χρηματική ποινή. [362] Η κυρωτική μεταχείριση των αξιόποινων προπαρασκευαστικών πράξεων είναι όμοια με εκείνη της διάταξης του άρθρου 370Β ΠΚ, γεγονός που δημιουργεί μια αξιολογική αντινομία, [363] καθόσον η αθέμιτη πρόσβαση στο σύστημα ή στα δεδομένα του δικαιούχου συνιστά εγκληματική συμπεριφορά που ενέχει βαρύτερο ποινικό άδικο. [364]

Τέλος, καθιερώνεται ένας λόγος δικαστικής άφεσης της ποινής και επομένως η δυνητική απαλλαγή του δράστη, κατά την ανέλεγκτη κρίση του δικαστηρίου της ουσίας, στην περίπτωση της καταστροφής των τεχνικών εργαλείων, προτού καταστούν διαθέσιμα σε αόριστο αριθμό προσώπων μέσω του διαδικτύου.

10. Προσβολές του απορρήτου των τηλεπικοινωνιών 292Δ ΠΚ

Στο άρθρο 292Δ, το οποίο εισήχθη το πρώτον στο νέο ΠΚ, τυποποιείται ως κοινώς επικίνδυνο έγκλημα η προσβολή του απορρήτου των τηλεπικοινωνιών του κοινού με την απόκτηση πρόσβασης σε σύνδεση ή σε δίκτυο παροχής στο κοινό υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας ή σε σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών. [365]

Στη διάταξη αυτή ενσωματώνεται σε μία εγκληματική μονάδα η διακινδύνευση αόριστου αριθμού ατόμων, γεγονός που δικαιολογεί την ιδιαίτερη επικινδυνότητα του εγκλήματος και τον χαρακτηρισμό του ως εγκλήματος γενικής διακινδύνευσης.[366] Ποινικοποιείται η χωρίς δικαίωμα πρόσβαση σε σύνδεση ή σε δίκτυο παροχής στο κοινό υπηρεσιών τηλεφωνίας, εφόσον, in concreto, θα μπορούσε να προκύψει κοινός κίνδυνος για το απόρρητο του περιεχομένου τηλεφωνικών ή ηλεκτρονικών επικοινωνιών ή των στοιχείων της θέσης ή κίνησης αυτών.

---

[361] Ε. Καμπέρου, ό.π. σελ. 2104

[362] Στο ίδιο ποινικό πλαίσιο κυμαίνεται και η αντίστοιχη διάταξη 202c γερμ.ΠΚ

[363] παρόμοια κριτική ασκείται και στη γερμανική θεωρία κατά το συσχετισμό των διατάξεων μεταξύ του 202c και. 202ª, 202b, 303ª και 303b γερμ.ΠΚ, σε M.Schreibauer/T.Hessel, Das 41.Strafrechtsänderungsgesetz, K&R 2007, σελ. 648.

[364] Όπως ισχύει για ένα έγκλημα βλάβης σε σχέση με ένα αντίστοιχο έγκλημα αφηρημένης διακινδύνευσης του ίδιου έννομου αγαθού, σύμφωνα με τη γενική θεωρία ποινικού δικαίου

[365] Αιτιολογική Έκθεση Νέου Π.Κ., σελ. 59, (https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/k-poinkod-eis-NEO.pdf)

[366] Καμπέρου σε «Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν 4619/2019», επιμ. Α. Χαραλαμπάκης, τόμος Β΄, 2020, άρθρο 292Δ ΠΚ, σελ. 2105, με περαιτέρω παραπομπή για τα κοινώς επικίνδυνα εγκλήματα σε Καΐάφα-Γκμπάντι, Κοινώς επικίνδυνα εγκλήματα

10.1. Προστατευόμενο έννομο αγαθό

Προστατευόμενο έννομο αγαθό συνιστά το απόρρητο των τηλεφωνικών επικοινωνιών, όπως προκύπτει και από την γραμματική διατύπωση της διάταξης,[367] ιδίως ως προς το στοιχείο της εμπιστευτικότητάς τους, το οποίο ως ατομικό δικαίωμα απολαύει προστασίας από το άρθρο 19 του Συντάγματος καθώς και από τα άρθρα 370 ΠΚ επ..

Προστατεύεται το κοινωνικό έννομο αγαθό του απορρήτου των τηλεπικοινωνιών, τόσο των τηλεφωνικών όσο και των ηλεκτρονικών επικοινωνιών του κοινού, δηλαδή αόριστου αριθμού ανθρώπων μη προσδιορισμένων εκ των προτέρων, οι οποίοι χρησιμοποιούν τις υπηρεσίες που προσφέρουν οι πάροχοι υπηρεσιών τηλεφωνίας και ηλεκτρονικής επικοινωνίας, προκειμένου να επικοινωνήσουν (φωνητικά ή γραπτά ή μέσω εικόνας) με τους συνανθρώπους τους.[368] Με την υπό εξέταση διάταξη διασφαλίζεται ότι το περιεχόμενο των τηλεφωνικών και ηλεκτρονικών επικοινωνιών και τα στοιχεία της θέσης και κίνησης αυτών, γίνονται γνωστά μόνο σε άτομα που επικοινωνούν μεταξύ τους και σε όποιους άλλους εκείνοι επιθυμούν και όχι σε τρίτα πρόσωπα άσχετα.

10.2. Χαρακτηρολογικά γνωρίσματα του εγκλήματος

Πρόκειται για πλημμέλημα, αδίκημα κοινό (δράστης του εγκλήματος μπορεί να είναι οιοσδήποτε στην παρ. 1), αλλά ιδιαίτερο στην πρώτη περίπτωση της παρ. 2 (ο δράστης πρέπει να φέρει τη συγκεκριμένη ιδιότητα), έγκλημα ενέργειας, κοινώς επικίνδυνο και δυνητικής διακινδύνευσης (καθώς δεν απαιτείται να κινδύνευσε πράγματι το απόρρητο των επικοινωνιών, αλλά αρκεί να μπορούσε να κινδυνεύσει) και στην περίπτωση της παρ. 2 και υπερχειλούς υποκειμενικής υπόστασης – έγκλημα σκοπού. [369]

Το αδίκημα τιμωρείται στη βασική του μορφή με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή, ενώ στην παράγραφο 2 του ως άνω άρθρου διαπλάσσονται δύο διακεκριμένες παραλλαγές με απειλούμενο πλαίσιο ποινής φυλάκιση τουλάχιστον 3 ετών και χρηματική ποινή.

10.3. Το βασικό έγκλημα της παρ. 1 του άρθρου 292Δ ΠΚ

10.3.1. Αντικειμενική υπόσταση

Δράστης του αδικήματος όπως προαναφέρθηκε μπορεί να είναι ο οποιοσδήποτε, εάν όμως ο δράστης φέρει μια από τις ιδιότητες που περιοριστικά απαριθμούνται στο εδ. β΄ της παραγράφου 2 του άρθρου, θα τιμωρηθεί επαχθέστερα λόγω ακριβώς της ιδιότητάς του ως προσώπου που έχει τη δυνατότητα πρόσβασης στα συστήματα του παρόχου και ως εκ τούτου αυξημένη υποχρέωση τήρησης του απορρήτου των τηλεφωνικών ή ηλεκτρονικών επικοινωνιών.

10.3.2. Εγκληματική συμπεριφορά

Η ποινικά απαξιολογούμενη συμπεριφορά, εν είδει εγκλήματος γενικής διακινδύνευσης, έγκειται στη χωρίς δικαίωμα απόκτηση πρόσβασης σε σύνδεση ή σε δίκτυο παροχής υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας ή σε σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, η οποία θα πρέπει να μπορούσε να προκαλέσει κοινό κίνδυνο για το απόρρητο των τηλεπικοινωνιών του κοινού.

---

[367] Αιτιολογική Έκθεση Νέου Π.Κ., σελ.: 59
[368] Ε. Καμπέρου, ό.π., σελ. 2106
[369] Ε. Καμπέρου, ό.π., σελ. 2107

Προκειμένου να πληρούται η αντικειμενική υπόσταση θα πρέπει ο δράστης να εκμεταλλεύεται τις αδυναμίες και τα κενά ασφαλείας στο δίκτυο ή στο σύστημα του παρόχου και κατ' αυτό το τρόπο να αποκτά πρόσβαση σε αυτό, παραβιάζοντας σταδιακά τα επίπεδα ασφαλείας του μέχρι να πετύχει να αποκτήσει την πρόσβαση σε απόρρητα δεδομένα των τηλεφωνικών και ηλεκτρονικών επικοινωνιών του κοινού, χωρίς να απαιτείται να επιτευχθεί αυτή η τελευταία.

Κρίσιμο κρίνεται να διευκρινιστεί για λόγους πληρέστερης αντίληψης της νομοτυπικής υπόστασης του αδικήματος, ότι στα δίκτυα των παρόχων κοινοποιούνται «πακέτα» που αποτελούνται από προσωπικές πληροφορίες των χρηστών της, τα ονόματα αυτών, οι κωδικοί εισόδου, οι λογαριασμοί ηλεκτρονικού ταχυδρομείου κ.λπ., μέσω κυρίως του πρωτοκόλλου μετάδοσης "Ethernet". Ο δράστης χρησιμοποιώντας τα κατάλληλα λογισμικά, συσκευές και μηχανήματα, μπορεί να αποκτήσει πρόσβαση σε αυτές της πληροφορίες και στη συνέχεια να υποκλέψει όχι μόνο τα στοιχεία θέσης και κίνησης αυτών αλλά και το περιεχόμενο των επικοινωνιών.[370]

Ο δράστης απαιτείται εκτός από τη διείσδυσή του στο σύστημα να έχει πραγματώσει και άλλους αιτιακούς όρους, οι οποίοι in concreto καθιστούν δυνατή τη διασάλευση της ειρηνευμένης κατάστασης του εννόμου αγαθού, ήγουν απαιτούνται περαιτέρω ενέργειες του δράστη, που συνιστούν παραβιάσεις εκείνων των συγκεκριμένων επιπέδων ασφαλείας που έχει θέσει ο πάροχος ώστε να προασπιστεί το απόρρητο των επικοινωνιών.

Οι έννοιες της σύνδεσης, του δικτύου και του συστήματος υλικού και λογισμικού, που χρησιμοποιούνται για την παροχή στο κοινό υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας, ως στοιχεία της αντικειμενικής υπόστασης του εγκλήματος του άρθρου 292Δ ΠΚ ερμηνεύονται κατά παραπομπή στην ειδική νομοθεσία για της ηλεκτρονικές επικοινωνίες, δηλαδή της διατάξεις νόμων και κοινοτικών οδηγιών. [371]

Ως *πρόσβαση* σε μια σύνδεση ή σε δίκτυο υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας ή σε σύστημα υλικού ή λογισμικού νοείται η φυσική ή και λογική είσοδος σε αυτό, που συνεπάγεται τη δυνατότητα αξιοποίησης των λειτουργιών του.[372]

10.4. Υποκειμενική υπόσταση.

Ελλείψει ειδικής αναφοράς, για την τέλεση του εγκλήματος απαιτείται οποιοδήποτε είδος δόλου, συμπεριλαμβανομένου του ενδεχόμενου, ο οποίος πρέπει να επικαλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος, συμπεριλαμβανομένης της δυνατότητας της πράξης να προκαλέσει κοινό κίνδυνο για το απόρρητο των τηλεπικοινωνιών αόριστου αριθμού ανθρώπων. Η πράξη είναι ανέγκλητη όταν το έγκλημα τελείται από αμέλεια, π.χ. είσοδος στα ηλεκτρονικά συστήματα του παρόχου «κατά λάθος», μολονότι πρόκειται για κοινώς επικίνδυνο έγκλημα, καθόσον σύμφωνα με την Αιτιολογική έκθεση δεν δικαιολογείται η ποινική καταστολή της.[373]

Δεν πληρούται η υποκειμενική υπόσταση του εγκλήματος, όταν λαμβάνει χώρα επιτρεπόμενη δοκιμή ή προστασία του δικτύου της τηλεφωνικής ή ηλεκτρονικής επικοινωνίας.

---

[370] Ε. Καμπέρου, ό.π., σελ. 2107

[371] Αναλυτικά για τις έννοιες αυτές Τσόλιας, για την ερμηνεία του άρθρου 292Α ΠΚ

[372] Σχετικώς η ΣυμβΠλημΑθ 4997/2012 ΠοινΔικ 2013, σελ. 504

[373] Π. Παπανδρέου, ό.π., σελ. 239

10.5. Οι διακεκριμένες παραλλαγές του εγκλήματος (άρθρο 292Δ παρ. 2 ΠΚ)

Η παράγραφος 2 του άρθρου 292Δ εισάγει δύο διακεκριμένες παραλλαγές του εγκλήματος, οι οποίες τιμωρούνται βαρύτερα, και συγκεκριμένα:

(α) την περίπτωση του νομικού εκπροσώπου κ.λπ. της εταιρείας παροχής υπηρεσιών επικοινωνιών,[374] η οποία συνεφέλκεται βαρύτερη ποινή, λόγω της θέσης του δράστη, η οποία αφ' ενός του προσφέρει πολύ μεγαλύτερη ευχέρεια στην διάπραξη του αδικήματος και αφ' ετέρου του επιβάλλει να μεριμνά για την ασφάλεια των επικοινωνιών, και

(β) την περίπτωση που ο δράστης ενεργεί με σκοπό προσπορισμού παράνομου περιουσιακού οφέλους, που ευλόγως τιμωρείται βαρύτερα, υπό την προϋπόθεση ότι η πράξη είναι αντικειμενικά πρόσφορη να επιφέρει στον δράστη το παραπάνω όφελος χωρίς να απαιτείται για την ολοκλήρωση του εγκλήματος να επιτεύχθηκε ο παραπάνω σκοπός. Επί παραδείγματι, εκείνος που σκοπεύει λόγου χάρη να πωλήσει σε άλλον τα απόρρητα ηλεκτρονικά δεδομένα αόριστου αριθμού χρηστών, στην απόκτηση των οποίων στόχευε όταν τέλεσε την πράξη, θα τιμωρηθεί με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή.

10.6. Ειδικές μορφές εμφάνισης του εγκλήματος

10.6.1. Απόπειρα

Δεν συνιστά ούτε αρχή εκτέλεσης του αδικήματος η απλή έρευνα αδυναμιών ή ευάλωτων σημείων των συστημάτων του παρόχου, με σκοπό σε μεταγενέστερο στάδιο ο δράστης να αποκτήσει πρόσβαση στο δίκτυο του παρόχου ούτε η προσπάθεια διείσδυσης στην περίμετρο του δικτύου του παρόχου που στέφθηκε ανεπιτυχής, καθώς οι συγκεκριμένες ενέργειες εντάσσονται στο στάδιο προπαρασκευής του αδικήματος. [375] Όταν ο δράστης επιτύχει να αποκτήσει πρόσβαση στα συστήματα του παρόχου που χρησιμοποιούνται για την παροχή τηλεπικοινωνιακών υπηρεσιών, αλλά δεν κατάφερε να παραβιάσει την ασφάλεια του δικτύου, τελεί το έγκλημα σε απόπειρα.

10.6.2. Συμμετοχή

Στο αδίκημα του άρθρου 292Δ ΠΚ είναι νοητή κάθε μορφή συμμετοχής (άρθρα 45-47 ΠΚ). Ιδιαίτερη μνεία χρειάζεται στην περίπτωση που ο συμμέτοχος έχει κάποια από τις περιοριστικά αναφερόμενες ιδιότητες στην παρ. 2 του ως άνω άρθρου, τότε εφαρμόζεται ως προς αυτόν το άρθρο 49 παρ. 2 ΠΚ και θα του επιβληθεί φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή (άρθρο 292Δ παρ. 2 ΠΚ), ενώ ο φυσικός αυτουργός, που δεν φέρει τέτοια ιδιότητα, θα τιμωρηθεί με ποινή φυλάκισης τουλάχιστον δύο ετών και χρηματική ποινή (άρθρο 292Δ παρ. 1 ΠΚ).

10.6.3. Συρροή

<u>Σχέση με το άρθρο 292Α ΠΚ</u>

Αναφορικά με τις υπηρεσίες της σταθερής και κινητής τηλεφωνίας, λεκτέα είναι τα ακόλουθα. Αρχικά, τα έννομα αγαθά που προστατεύουν οι δύο διατάξεις εν μέρει αλληλοεπικαλύπτονται. Όπως προκύπτει από την ιστορική-βουλητική ερμηνεία της διάταξης του άρθρου 292Α παρ. 1 ΠΚ, ο νομοθέτης έμελλε να προστατέψει ποινικά την ασφάλεια του

[374] Για της έννοιες του παρόχου, του εργαζόμενου στον πάροχο, του συνεργάτη, του υπεύθυνου διασφάλισης του απορρήτου βλ. Τσόλιας υπό άρθρο 292Α ΠΚ πλαγ. 23, 30-36, 59.
[375] Ε. Καμπέρου, ό.π., σελ. 2108

απορρήτου των τηλεφωνικών επικοινωνιών και στα τρία της συστατικά της στοιχεία, που είναι η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικοποίηση της τηλεφωνικής επικοινωνίας. [376] Συνεπώς, το απόρρητο των τηλεφωνικών επικοινωνιών (τόσο του περιεχομένου και όσο και των στοιχείων θέσης και κίνησης), που προβάλει ως αυτοτελές έννομο αγαθό του άρθρου 292Δ ΠΚ, αναφέρεται στο συστατικό στοιχείο της εμπιστευτικότητας της επικοινωνίας, με την οποία και ταυτίζεται, αποτελώντας, μ' άλλα λόγια, μια από της τρεις όψεις του εννόμου αγαθού της ασφάλειας του απορρήτου των τηλεφωνικών επικοινωνιών, που προστατεύεται συνολικά στο άρθρο 292Α ΠΚ.

Επίσης ο νομοθέτης έκρινε σκόπιμο να τιμωρήσει με βαρύτερη ποινή στο άρθρο 292Δ μόνο τη μερικότερη όψη της εμπιστευτικότητας, ήτοι του απορρήτου, των τηλεφωνικών επικοινωνιών του κοινού, καθώς έκρινε επί λέξει «συγκεχυμένο και σε πολλά σημεία αόριστο το περιεχόμενο του άρθρου 292Α ΠΚ». [377]

Τέλος, εξαιτίας της προκύπτουσας εν μέρει ταύτισης των εννόμων αγαθών που προστατεύουν οι δύο διατάξεις και με δεδομένο ότι τυποποιείται και στις δύο η ίδια εγκληματική συμπεριφορά, οι δύο διατάξεις συρρέουν μεταξύ τους κατ' ιδέαν φαινομενικά και εφαρμοστέα είναι εκείνη του άρθρου 290Δ ΠΚ που προβλέπει τη βαρύτερη ποινή, βάσει της αρχής της απορρόφησης. [378]

Σχέση με το άρθρο 292Ε ΠΚ

Όσον αφορά στις ηλεκτρονικές επικοινωνίες ιδίως μέσω του διαδικτύου, προστατεύονται αυτοτελώς στον νέο ΠΚ ως κοινωνικό έννομο αγαθό τόσο από πράξεις που προσβάλλουν την εμπιστευτικότητα (το απόρρητο) του περιεχομένου τους και των στοιχείων θέσης και κίνησης αυτών στη σχολιαζόμενη διάταξη, όσο και από πράξεις που παρακωλύουν τη λειτουργία της εγκατάστασης παροχής τους (εγκατάσταση κοινής ωφέλειας) (άρθρο 292Ε ΠΚ), αλλά και γενικότερα και από πράξεις που παρακωλύουν τη λειτουργία των πληροφοριακών συστημάτων που χρησιμοποιούνται για την παροχή ηλεκτρονικών υπηρεσιών, εκτός των παραπάνω κοινωφελών εγκαταστάσεων (άρθρο 292Β ΠΚ)

Σχέση με τις διατάξεις 370 επ ΠΚ

Το άρθρο 292Δ τυποποιεί αδίκημα γενικής διακινδύνευσης κατά των τηλεπικοινωνιών και δεν καταλαμβάνει τις ατομικές προσβολές του τηλεπικοινωνιακού απορρήτου (τηλεφωνικού ή ηλεκτρονικού), οι οποίες αποτελούν εγκλήματα βλάβης του απορρήτου συγκεκριμένων προσώπων και τιμωρούνται αυτοτελώς στις διατάξεις των άρθρων 370Α -370Ε και κατ΄

[376] Για της έννοιες της εμπιστευτικότητας, ακεραιότητας και αυθεντικοποίησης βλ. Τσόλιας, ό.π., πλαγ. 44 επ.

[377] ΑιτΕκθΣχΠΚ 2019, σελ. 57

[378] Ε. Καμπέρου, ό.π., σελ. 2112 με περαιτέρω παραπομπή σε Καϊάφα-Γκμπάντι, Κοινώς επικίνδυνα εγκλήματα, 1990, σελ. 479-480 για το πρόβλημα της συρροής του άρθρου 286 προϊσχύσαντος ΠΚ με εκείνες των άρθρων 264 και 270 προϊσχύσαντος ΠΚ, που τυγχάνουν χρήσιμες και στο υπό εξέταση ζήτημα και Παύλου, Οι αρχές της φαινομενικής συρροής, Ι, 2003, ιδίως 209 υποσ. 166, όπου στο ζήτημα της επίλυσης της συρροής μεταξύ των διατάξεων των άρθρων 286, 264 ή 270 προϊσχύσαντος ΠΚ θεωρεί ως πιο «ορθόδοξη» λύση την αρχή της απορρόφησης έναντι της αρχής της σιωπηρής επικουρικότητας· τέλος, και τον προβληματισμό Τσόλια, υπό άρθρο 292Α ΠΚ πλαγ. 90

αποτέλεσμα η διάταξη του άρθρου 292Δ να συρρέει πάντοτε αληθινά με τις ως άνω διατάξεις. [379]

Σχέση με το άρθρο 292Β ΠΚ

Στην περίπτωση που η χωρίς δικαίωμα πρόσβαση έγινε σε πληροφοριακό σύστημα, που χρησιμοποιείται για την παροχή υπηρεσιών τηλεφωνικής ή ηλεκτρονικής επικοινωνίας, με τους τρόπους που αναφέρονται στο άρθρο 292Β παρ. 1 ΠΚ (εισαγωγή, διαβίβαση ψηφιακών δεδομένων κ.λπ.) και από την πράξη αυτή αφενός παρεμποδίστηκε σοβαρά ή διακόπηκε η λειτουργία του πληροφοριακού συστήματος, αφετέρου θα μπορούσε να διακινδυνεύσει το απόρρητο των τηλεφωνικών ή ηλεκτρονικών υπηρεσιών του κοινού, η διάταξη του άρθρου 292Δ παρ. 1 ΠΚ συρρέει αληθινά με εκείνη του άρθρου 292Β ΠΚ, λόγω στης προσβολής διαφορετικών μερικότερων όψεων του εννόμου αγαθού της ασφάλειας των πληροφοριακών συστημάτων.[380]

Κατά τη διάταξη του άρθρου 298 παρ. 1 και 2 ΠΚ, περί έμπρακτης μετάνοιας, ορίζεται ότι η διάταξη του άρθρου 289 παρ. 1 ΠΚ, περί εξάλειψης αξιοποίνου, έχει ανάλογη εφαρμογή και στις περιπτώσεις των εγκλημάτων της παρ. 2 των άρθρων 290, 290Α, 291 και 292 του ΠΚ και η διάταξη του άρθρου 289 παρ. 2 ΠΚ, περί δικαστικής άφεσης ποινής, έχει ανάλογη στα εγκλήματα αυτού του 14ου κεφαλαίου, ήτοι το δικαστήριο μπορεί να κρίνει και την παραπάνω πράξη του άρθρου 292Δ ΠΚ ατιμώρητη, αν ο υπαίτιος με τη θέλησή του αποτρέψει την εξέλιξη του κινδύνου ή με τη γρήγορη αναγγελία του προς τις αρχές δώσει αφορμή για την αποτροπή της παρεμπόδισης της λειτουργίας της εγκατάστασης ή της πλήρους ανακοπής-ματαίωσης της λειτουργίας της εγκατάστασης τηλεπικοινωνιών. [381]

10.7. Δικονομικά

Δεδομένου του ότι το έγκλημα προσβάλλει ένα κοινωνικό/υπερατομικό έννομο αγαθό, που ανήκει σε αόριστο αριθμό ατόμων, παράσταση προς υποστήριξη της κατηγορίας δεν είναι κατ' αρχήν νοητή, ωστόσο, κατά μία άποψη, εάν τα άτομα των οποίων το απόρρητο της επικοινωνίας κινδύνεψε μπορούν να συγκεκριμενοποιηθούν, θα έπρεπε να γίνεται δεκτή η εκ μέρους τους παράσταση προς υποστήριξη της κατηγορίας.[382]

[379] Η ταυτότητα του εγκλήματος ως κοινώς επικίνδυνου οδηγεί ήγουν, σε περίπτωση που μέσα από τη συγκεκριμένη πράξη βλαφτεί το απόρρητο της επικοινωνίας συγκεκριμένων προσώπων, σε αληθινή συρροή εγκλημάτων, αφού το συγκεκριμένο κοινώς επικίνδυνο έγκλημα δεν μπορεί να απορροφήσει τη βλάβη του απορρήτου, αλλά ούτε και το αντίστροφο μπορεί να συμβεί. Και τούτο διότι η βλάβη αφορά το απόρρητο της επικοινωνίας συγκεκριμένων προσώπων, ενώ η προσβολή του απορρήτου των τηλεπικοινωνιών του κοινού αναφέρεται στη διακινδύνευση του απορρήτου αόριστου αριθμού ανθρώπων. Κ. Φράγκος, Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 292Δ, αρ. 3, Ενημέρωση:10/12/2019, sakkoulas-online

[380] Ε. Καμπέρου, ό.π., σελ. 2113

[381] Κ. Φράγκος, Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 292Δ, αρ. 4, Ενημέρωση:10/12/2019, sakkoulas-online

[382] Ε. Καμπέρου, ό.π., σελ. 2114

11. Παρακώλυση των τηλεπικοινωνιών (Άρθρο 292Ε ΠΚ)

Στο άρθρο αυτό τυποποιείται η παρακώλυση των τηλεπικοινωνιών ως έγκλημα βλάβης του κοινωνικού αγαθού των εγκαταστάσεων τηλεπικοινωνιών με τις οποίες παρέχονται στο κοινό υπηρεσίες τηλεφωνίας ή ηλεκτρονικής επικοινωνίας και ιδίως όταν αυτό συμβαίνει μέσω του διαδικτύου.[383]

Η διάταξη αυτή είναι ειδικότερη εκείνης του άρθρου 292Β ΠΚ, καθώς αφορά μία περίπτωση αυθαίρετης παρέμβασης σε συγκεκριμένου τύπου πληροφοριακό σύστημα ή ηλεκτρονικά δεδομένα, που, λόγω της θεώρησής τους ως κοινωφελών εγκαταστάσεων, καθιστούν το έγκλημα βαρύτερο. Συνεπώς, προστατεύονται μόνον εκείνα από το σύνολο των πληροφοριακών συστημάτων και ηλεκτρονικών (ψηφιακών) δεδομένων, που χρησιμοποιούνται για τη λειτουργία των εγκαταστάσεων τηλεπικοινωνιών παροχής στο κοινό υπηρεσιών τηλεφωνίας και ηλεκτρονικών επικοινωνιών. Εξαιτίας της θεώρησης των εγκαταστάσεων των παρόχων που εξυπηρετούν τις τηλεφωνικές και ηλεκτρονικές επικοινωνίες του κοινού ως κοινωφελών εγκαταστάσεων, το έγκλημα του άρθρου 292Ε παρ. 1 ΠΚ επισύρει ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή, ενώ εκείνο του άρθρου 2928 παρ. 1 ΠΚ τιμωρείται με φυλάκιση (δηλαδή με κατώτατο όριο ποινής τις δέκα μέρες, άρθρο 53 ΠΚ) και χρηματική ποινή.[384]

11.1. Προστατευόμενο έννομο αγαθό

Προστατευόμενο έννομο αγαθό συνιστά η προστασία των τηλεπικοινωνιών και δη η εύρυθμη λειτουργία των εγκαταστάσεων παροχής στο κοινωνικό σύνολο τηλεφωνικών και ηλεκτρονικών υπηρεσιών και ιδίως του διαδικτύου.[385] Το έννομο αγαθό χαρακτηρίζεται αφενός ατομικό, λόγω της ιδιότητας των υλικών αντικειμένων (κινητών ή ακίνητων) να συνιστούν ιδιοκτησία συγκεκριμένων φυσικών ή νομικών προσώπων και να εξυπηρετούν άμεσα συγκεκριμένες βιοτικές ανάγκες αορίστου αριθμού προσώπων, όπως φέρ' ειπείν την ανάγκη επικοινωνίας,[386] αλληλεπίδρασης με άλλους, μόρφωσης, εργασίας, ψυχαγωγίας κ.λπ..[387] Αφετέρου, το έννομο αγαθό χαρακτηρίζεται και ως υπερατομικό, καθότι οι εν λόγω εγκαταστάσεις, που εξυπηρετούν τις τηλεπικοινωνίες, συνεισφέρουν σε κοινωνικό όφελος, καθώς είναι σημαντικής αξίας για το σύνολο των εγκαταστάσεων κοινής ωφέλεια, μαζί με εκείνες που εξυπηρετούν την παροχή στο κοινό ταχυδρομικών υπηρεσιών, ύδρευσης, ηλεκτρισμού και ενέργειας. [388]

---

[383] Αιτιολογική Έκθεση Νέου Π.Κ., σελ. 60

[384] Ε. Μεταξάκης, ό.π., σελ. 501

[385] Καμπέρου σε «Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν 4619/2019», επιμ. Α. Χαραλαμπάκης, τόμος Β΄, 2020, άρθρο 292Ε ΠΚ, σελ. 2115

[386] Μανωλεδάκης, Το έννομο αγαθό ως βασική έννοια του ποινικού δικαίου, 1998, σελ. 269 επ, για την αναγωγή της «ανθρώπινης επικοινωνίας» σε αυτοτελές έννομο αγαθό, ως ουσιώδους όρου της κοινωνικής ζωής.

[387] βλ. Μανωλεδάκης, για τα πράγματα κοινής ωφέλειας, σε Εγκλήματα κατά της ιδιοκτησίας, 1994, σελ. 250- 251

[388] Ε. Καμπέρου, ό.π., σελ. 2115

11.2. Χαρακτηρολογικά γνωρίσματα

Στο άρθρο 292Ε παρ. 1 ΠΚ καταστρώνεται αδίκημα πλημμελληματικού βαθμού, κοινό στην παρ. 1 και ιδιαίτερο στην παρ. 2 (σε συνδυασμό με α. 292Δ παρ. 2),αποτελέσματος,[389] βλάβης,[390] ενέργειας,[391] στιγμιαίο καταρχήν, άλλοτε δε διαρκές, απλό και υπαλλακτικώς μικτό.[392]

11.3. Τυποποίηση των αδικημάτων

Στο άρθρο 292Ε ΠΚ, τυποποιείται το έγκλημα της παρακώλυσης των τηλεπικοινωνιών στη βασική του μορφή στην παράγραφο 1, που επισύρει ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή, ενώ στην παράγραφο 2 διαπλάσσονται δύο διακεκριμένες παραλλαγές όταν αφενός το ως άνω αδίκημα τελείται από κάποιο από τα περιοριστικά αναφερόμενα πρόσωπα της παραγράφου 2 του άρθρου 292Δ και αφετέρου όταν τελείται, με σκοπό προσπορισμού παράνομου περιουσιακού οφέλους, οπότε και απειλείται πλαίσιο φυλάκισης τουλάχιστον 3 ετών και χρηματική ποινή. Τέλος, στην τρίτη παράγραφο ορίζεται ότι η παρακώλυση των τηλεπικοινωνιών από αμέλεια, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.

11.4. Το έγκλημα της παρακώλυσης των τηλεπικοινωνιών στη βασική του μορφή (292Ε παρ. 1 ΠΚ)

11.4.1. Αντικειμενική υπόσταση

Η συμπεριφορά που κρίνεται αξιόποινη συνίσταται στη παρεμπόδιση ή διατάραξη σε μεγάλη έκταση ή για μεγάλο χρονικό διάστημα της λειτουργίας εγκατάστασης παροχής στο κοινό υπηρεσιών τηλεφωνίας ή ηλεκτρονικών επικοινωνιών και δη του διαδικτύου, με αθέμιτη πρόσβαση σε πράγμα ή σύστημα πληροφοριών ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία αυτής της εγκατάστασης.

Δράστης του υπό εξέταση εγκλήματος μπορεί να καταστεί ο οιοσδήποτε. Στην περίπτωση όμως που ο δράστης φέρει κάποια από τις περιοριστικά αναφερόμενες στο άρθρο 292Δ παρ. 2 ΠΚ ιδιότητες, στοιχειοθετείται ποινική του ευθύνη επί τη βάσει της παραγράφου 2 του άρθρου 292Ε ΠΚ.

11.4.2. Υλικό αντικείμενο

Αντικείμενο του αδικήματος συνιστά μια εγκατάσταση παροχής υπηρεσιών τηλεφωνίας ή ηλεκτρονικών επικοινωνιών στο κοινό. Η εγκατάσταση αποτελείται από τα κτίρια, τα μηχανήματα, τον εξοπλισμό και γενικότερα τα κινητά και ακίνητα στοιχεία που συνθέτουν το πάγιο ενεργητικό μιας επιχείρησης και που εξυπηρετούν τον λειτουργικό σκοπό της

[389] Οπότε απαιτείται να προκλήθηκε αιτιωδώς από την εγκληματική συμπεριφορά το αποτέλεσμα, σύμφωνα με τη θεωρία του ισοδυνάμου των όρων, conditio sine qua non.

[390] Περί αδικήματος βλάβης κάνει λόγο και η αιτιολογική έκθεση του Ν. 4619/2019, καθώς θα πρέπει να ματαιωθεί ή να διαταραχθεί σοβαρά η λειτουργία των εγκαταστάσεων τηλεπικοινωνιών για να είναι τετελεσμένο το έγκλημα, χωρίς να αρκεί ο κίνδυνος ή η απόπειρα πρόκλησης του κινδύνου.

[391] Και μη γνήσιας παράλειψης, όπου για να μπορεί να τελεσθεί με παράλειψη θα πρέπει ο δράστης να έχει ιδιαίτερη νομική υποχρέωση αποτροπής του αποτελέσματος βάσει του άρθρου 15 ΠΚ.

[392] Μπορεί συνεπώς να τελεστεί είτε με παρεμπόδιση είτε με σοβαρή διατάραξη της λειτουργίας της εγκατάστασης, οπότε αν ο δράστης προκαλέσει με την ενέργειά του, διαδοχικά πρώτα τη διατάραξη και μετά τη ματαίωση της λειτουργίας της, ένα μόνο έγκλημα τελεί, αφού προσβάλλει την ίδια μονάδα του εννόμου αγαθού. Ε. Μεταξάκης, ό.π., σελ. 501

εγκατάστασης να παρέχει στο κοινό τις τηλεπικοινωνιακές υπηρεσίες. [393] Στην εγκατάσταση παροχής τηλεπικοινωνιακών υπηρεσιών εμπίπτουν αναμφισβήτητα και οι συσκευές που απαρτίζουν το πληροφοριακό σύστημα, όπως και τα ηλεκτρονικά (ψηφιακά) δεδομένα του, αλλά και το λογισμικό που χρησιμοποιείται για την παροχή των τηλεπικοινωνιακών υπηρεσιών.

Γίνεται διάκριση ανάμεσα σε πράγματα της εγκατάστασης και στο πληροφοριακό σύστημα και τα δεδομένα του, που χρησιμοποιούνται για τη λειτουργία της εγκατάστασης. Ως πράγματα της εγκατάστασης νοούνται εκείνα τα μηχανήματα, όπως ιδίως οι ηλεκτρονικοί υπολογιστές ή άλλες συσκευές, κεραίες, ειδικές κατασκευές, καλώδια κ.λπ., τα οποία εξυπηρετούν τη λειτουργία της εγκατάστασης, οπότε αν ο δράστης παρέμβει στη λειτουργία τους, προκαλεί αιτιωδώς τη ματαίωση της λειτουργίας της εγκατάστασης ή την ουσιώδη και σοβαρή διατάραξη της λειτουργίας της. Το σύστημα πληροφοριών είναι το πληροφοριακό σύστημα που χρησιμοποιεί η εγκατάσταση προκειμένου να παρέχει τις τηλεπικοινωνιακές υπηρεσίες και τα ηλεκτρονικά δεδομένα είναι τα ψηφιακά δεδομένα που ανήκουν στο παραπάνω πληροφοριακό σύστημα. [394]

11.4.3. Εγκληματική συμπεριφορά

Προκειμένου να πληρούται η αντικειμενική υπόσταση του αδικήματος ο δράστης απαιτείται να παρέμβει αθέμιτα σε πράγμα ή σε σύστημα πληροφοριών ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία της εγκατάστασης. Αποτέλεσμα δε της ενέργειάς του είναι η παρεμπόδιση ή η ουσιώδης - σε μεγάλη έκταση ή για μεγάλο χρονικό διάστημα - διατάραξη της εγκατάστασης.

Παρεμπόδιση ή σοβαρή διατάραξη της λειτουργίας της εγκατάστασης μπορεί λόγου χάρη να προκληθεί με επιθέσεις, δηλαδή παρεμβολές, στο πληροφοριακό σύστημα που χρησιμοποιεί η εγκατάσταση, οι οποίες δημιουργούν τη λεγόμενη άρνηση υπηρεσιών (denial of service) ή που εμποδίζουν ή καθυστερούν σημαντικά τη λειτουργία της εγκατάστασης, με αποτέλεσμα να στερείται το κοινό της υπηρεσίες τηλεφωνίας ή ηλεκτρονικής επικοινωνίας είτε για μεγάλο χρονικό διάστημα είτε σε μεγάλη έκταση.

Ο δράστης παρεμβαίνει αθέμιτα στα πράγματα ή στο πληροφοριακό σύστημα ή στα ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία της εγκατάστασης, όταν δεν έχει σχετικό δικαίωμα από το νόμο ή όταν δεν έχει εξουσιοδοτηθεί αρμοδίως προς τούτο ή όταν υπερβαίνει τα όρια της εξουσιοδότησης που του έχει παρασχεθεί. [395] Εξ αντιδιαστολής, αν ο δράστης είχε το δικαίωμα να παρέμβει σε πράγμα ή σε πληροφοριακό σύστημα ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία της εγκατάστασης και έδρασε μέσα στα πλαίσια των αρμοδιοτήτων του, αλλά εξαιτίας της παρέμβασης του παρεμποδίστηκε ή διαταράχθηκε ουσιωδώς η λειτουργία της εγκατάστασης, δεν πληρούται στοιχείο της αντικειμενικής υπόστασης του εγκλήματος και η πράξη του δεν είναι ούτε αρχικά άδικη. Στο ίδιο παράδειγμα, δεν μπορεί να στοιχειοθετηθεί ούτε ευθύνη του από αμέλεια (άρθρο 292Ε παρ. 3 ΠΚ), διότι και εκείνη προϋποθέτει το αθέμιτο της δράσης του.

[393] Ε. Καμπέρου με περαιτέρω παραπομπή σε Μανωλεδάκη, Ερμηνεία κατ' άρθρο,σελ. 85 και Μπαμπινιώτη, Λεξικό της νέας ελληνικής γλώσσας, Β΄ έκδοση

[394] Για την έννοια του πληροφοριακού συστήματος και των δεδομένων του βλ. υπό άρθρο 13 εδ. στ΄ ΠΚ.

[395] βλ. αναλυτικότερα Τσόλια, υπό άρθρο 292Α ΠΚ

11.4.4. Το τυποποιημένο αποτέλεσμα

Δοθέντος ότι πρόκειται για αδίκημα αποτελέσματος, οπότε απαιτείται για να θεωρηθεί το έγκλημα τετελεσμένο να επήλθε πράγματι η παρεμπόδιση ή διατάραξη της λειτουργίας της παραπάνω εγκατάστασης, με την έννοια ότι στερήθηκε το κοινό (δηλαδή αόριστος) τις υπηρεσίες τηλεφωνίας ή ηλεκτρονικών επικοινωνιών που παρέχει η προσβληθείσα εγκατάσταση είτε για μεγάλο χρονικό διάστημα είτε σε μεγάλη έκταση. Επί τη βάσει της θεωρίας του ισοδυνάμου των όρων, θα πρέπει να καταφαθεί η αιτιώδης συνάφεια μεταξύ της εγκληματικής συμπεριφοράς του δράστη και του επελθόντος αποτελέσματος.

Ως *παρεμπόδιση* νοείται η πλήρης ανακοπή, δηλαδή η ματαίωση της λειτουργίας της εγκατάστασης παροχής τηλεπικοινωνιακών υπηρεσιών, ενώ η *διατάραξη* της λειτουργίας της καθίσταται αξιόποινη μόνο αν γίνεται σε μεγάλη έκταση ή για μεγάλο χρονικό διάστημα,[396] οπότε πρέπει να κρίνεται από το δικαστήριο, με βάση ενδείκτες και σοβαρή και όχι θεμελιωμένους στα πραγματικά περιστατικά της υπόθεσης, ως ουσιώδης ως μικρής έκτασης ή μικρής διάρκειας.

11.5. Υποκειμενική υπόσταση

Ελλείψει ειδικότερης μνείας του άρθρου, απαιτείται δόλος οποιουδήποτε βαθμού, αρκούντος του ενδεχόμενου, που να επικαλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος, συμπεριλαμβανομένου και του τυποποιημένου στο νόμο αποτελέσματος της παρεμπόδισης ή ουσιώδους διατάραξης της λειτουργίας της εγκατάστασης παροχής στο κοινό τηλεπικοινωνιακών υπηρεσιών. Επομένως, ο δράστης πρέπει όχι μόνον να γνωρίζει ότι παρεμβαίνει χωρίς να έχει δικαίωμα (αθέμιτα) σε πράγμα ή σε πληροφοριακό σύστημα ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία της παραπάνω εγκατάστασης, αλλά και ότι παρακωλύει με αυτόν τον τρόπο τη λειτουργία της εγκατάστασης και να θέλει να την παρακωλύσει ή έστω να αποδέχεται την επέλευση του αποτελέσματος της παρακώλυσής της.

11.6. Οι διακεκριμένες παραλλαγές της παρ. 2 του άρθρου 292Ε ΠΚ

Όπως προαναφέρθηκε, στην δεύτερη παράγραφο του εν λόγω άρθρου τυποποιούνται δύο διακεκριμένες παραλλαγές του βασικού αδικήματος της παρ. 1, που τιμωρούνται επαχθέστερα, ήγουν με ποινή φυλάκισης τουλάχιστον τριών ετών και αθροιστικά χρηματική ποινή.

Ως προς την πρώτη διακεκριμένη παραλλαγή (άρθρο 292Ε παρ. 2 σε συνδυασμό με το 292Δ παρ. 2 εδ. α΄ ΠΚ), η αυξημένη ποινική απαξία της πράξης του παρόχου ή του νόμιμου εκπροσώπου του ή του μέλους της διοίκησής του ή του εργαζόμενου ή συνεργάτη του ή του υπευθύνου διασφάλισης του απορρήτου, δικαιολογείται καθώς τα πρόσωπα αυτά έχουν ευχερέστερη πρόσβαση στην εγκατάσταση παροχής των τηλεπικοινωνιακών υπηρεσιών στο κοινό και λόγω των ιδιοτήτων τους οφείλουν να διασφαλίζουν την απρόσκοπτη λειτουργία της και όχι να τη βλάπτουν, με αθέμιτες παρεμβάσεις στα πράγματα ή στα πληροφοριακά συστήματα που την εξυπηρετούν.

Ως προς τη δεύτερη διακεκριμένη παραλλαγή του εγκλήματος (άρθρο 292Ε παρ. 2 σε συνδυασμό με άρθρο 292Δ παρ. 2 εδ. β΄ ΠΚ), η βαρύτερη τιμωρία οποιουδήποτε κρίνεται επιβεβλημένη για όποιον παρεμποδίζει ή διαταράσσει ουσιωδώς τη λειτουργία της εγκατάστασης παροχής τηλεπικοινωνιακών υπηρεσιών, έχοντας ως σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος (έγκλημα υπερχειλούς

[396] ΑιτΕκθΣΧΠΚ 2019, υπό άρθρο 292Ε ΠΚ, 59

υποκειμενικής υπόστασης ή σκοπού). Η πράξη πρέπει να είναι πρόσφορη να επιφέρει στον δράστη το παραπάνω όφελος και δεν απαιτείται για την ολοκλήρωση του εγκλήματος να επιτεύχθηκε ο παραπάνω σκοπός. [397]

11.7. Η παρακώλυση των τηλεπικοινωνιών από αμέλεια (άρθρο 292Ε παρ. 3 ΠΚ)

Σύμφωνα με τη διάταξη της παρ. 3 του άρθρου 292Ε ΠΚ, αν η πράξη της πρώτης παραγράφου τελέστηκε από αμέλεια, επιβάλλεται χρηματική ποινή ή παροχή κοινωφελούς εργασίας. Συνεπώς, ο δράστης πρέπει, άνευ δικαιώματος -αθέμιτα- να παρεμβαίνει σε πράγμα ή σε σύστημα πληροφοριών ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία εγκατάστασης παροχής τηλεπικοινωνιακών υπηρεσιών στο κοινό, χωρίς όμως να σκοπεύει να παρεμποδίσει ή να διαταράξει τη λειτουργία της τελευταίας, αλλά λόγω έλλειψης της προσοχής που όφειλε κατά τις περιστάσεις και μπορούσε να καταβάλλει είτε δεν προέβλεψε καθόλου το αποτέλεσμα της παρακώλυσης της λειτουργίας της εγκατάστασης, το οποίο επέφερε αιτιωδώς η πράξη του (αμέλεια χωρίς συνείδηση) είτε το προέβλεψε μεν ως δυνατό, αλλά πίστεψε ότι δεν επερχόταν (ενσυνείδητη αμέλεια) (άρθρο 28 ΠΚ).

11.8. Έμπρακτη μετάνοια

Κατά τη διάταξη του άρθρου 298 παρ. 1 και 2 ΠΚ, περί έμπρακτης μετάνοιας, ορίζεται ότι η διάταξη του άρθρου 289 παρ. 1 ΠΚ, περί εξάλειψης αξιόποινου, έχει ανάλογη εφαρμογή και στις περιπτώσεις των εγκλημάτων της παρ. 2 των άρθρων 290, 290Α, 291 και 292 του ΠΚ και η διάταξη του άρθρου 289 παρ. 2 ΠΚ, περί δικαστικής άφεσης ποινής έχει ανάλογη εφαρμογή στα εγκλήματα αυτού του 14ου κεφαλαίου, ήτοι το δικαστήριο μπορεί να κρίνει και την παραπάνω πράξη του άρθρου 292Ε ΠΚ ατιμώρητη αν ο υπαίτιος με τη θέλησή του αποτρέψει την εξέλιξη του κινδύνου ή με τη γρήγορη αναγγελία του προς τις αρχές δώσει αφορμή για την αποτροπή της.[398]

11.9. Ειδικές μορφές εμφάνισης του εγκλήματος

11.9.1 Απόπειρα

Απόπειρα του εγκλήματος του άρθρου 292Ε παρ. 1 ΠΚ (και των διακεκριμένων παραλλαγών του) διαγιγνώσκεται καταρχήν όταν ο δράστης αθέμιτα παρενέβη σε πράγμα ή σε σύστημα πληροφοριών ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία της εγκατάστασης παροχής στο κοινό τηλεπικοινωνιακών υπηρεσιών, αλλά για λόγους ανεξάρτητους από τη θέλησή του, δεν επήλθε το αποτέλεσμα της παρεμπόδισης ή σοβαρής κατ' έκταση ή χρόνο διατάραξης της λειτουργίας της εγκατάστασης. Εν αποπείρα βρίσκεται το αδίκημα και όταν ως συνέπεια της εγκληματικής συμπεριφοράς του δράστη διαταράχθηκε η λειτουργία της εγκατάστασης μεν , αλλά αυτή η διατάραξη ήταν σε μικρή έκταση ή έλαβε χώρα για σύντομο χρονικό διάστημα, διότι λ.χ. ο δράστης έγινε αντιληπτός και αποκαταστάθηκε η λειτουργία της εγκατάστασης. Σημειώνεται, ως εκ περισσού, ότι απόπειρα στο έγκλημα της παρακώλυσης των τηλεπικοινωνιών από αμέλεια (άρθρο 292Ε παρ. 3 ΠΚ) δεν είναι νοητή, διότι η απόπειρα προϋποθέτει δόλο (άρθρο 42 παρ. 1 ΠΚ).

---

[397] Για της έννοιες του παρόχου, του εργαζόμενου στον πάροχο, του συνεργάτη και του υπεύθυνου διασφάλισης του απορρήτου βλ. αναλυτικότερα Τσόλια, υπό άρθρο 292Α ΠΚ πλαγ. 23, 30-36, 59.

[398] Κ. Φράγκος, Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 292Ε, αρ. 3, Ενημέρωση:10/12/2019, sakkoulas-online

11.9.2 Συμμετοχή

Είναι δυνατή η συμμετοχή σε όλες της τις μορφές στο έγκλημα της παρακώλυσης των τηλεπικοινωνιών, που τελείται με δόλο (άρθρο 292Ε παρ. 1 ΠΚ). Όσον αφορά στο έγκλημα της παρακώλυσης των τηλεπικοινωνιών που τελείται από αμέλεια (άρθρο 2928 παρ. 3 ΠΚ), αποκλείεται η τέλεσή του κατά συναυτουργία, διότι η από κοινού δράση των συναυτουργών απαιτεί δόλο,[399] οπότε ο κάθε δράστης κρίνεται αυτοτελώς ως παραυτουργός, χωρίς να αποκλείεται η τέλεση του εγκλήματος από συγκλίνουσα αμέλεια περισσοτέρων.

Η διάταξη του άρθρου 292Ε ΠΚ θα συρρέει κατ' ιδέαν φαινομενικά με εκείνη του άρθρου 292Β ΠΚ σε περίπτωση που παρεμποδίζεται σοβαρά ή διακόπτεται η λειτουργία πληροφοριακού συστήματος, το οποίο όμως αποτελεί μέρος εγκατάστασης παροχής στο κοινό τηλεφωνικών ή ηλεκτρονικών επικοινωνιών και ιδίως του διαδικτύου. Τότε, θα εφαρμόζεται η διάταξη του άρθρου 292Ε ΠΚ, η οποία αποτελεί ειδική διάταξη σε σχέση με εκείνη του άρθρου 292Β ΠΚ, διότι αναφέρεται σε συγκεκριμένο είδος πληροφοριακών συστημάτων και δη εκείνων που εξυπηρετούν τις τηλεφωνικές και ηλεκτρονικές επικοινωνίες του κοινού, τιμωρεί δε την πράξη με βαρύτερη ποινή.

Παράσταση προς υποστήριξη της κατηγορίας. Δεν νοείται παράσταση προς υποστήριξη της κατηγορίας στα εγκλήματα του άρθρου 292Ε ΠΚ, διότι η διάταξη προστατεύει το κοινωνικό-υπερατομικό έννομο αγαθό των εγκαταστάσεων παροχής τηλεπικοινωνιακών υπηρεσιών, [400] του οποίου φορέας είναι το κοινό, δηλαδή αόριστος αριθμός ανθρώπων.

12. Φθορά ψηφιακών δεδομένων (379 ΠΚ)

Σφοδρή κριτική είχε δεχθεί η επιλογή του νομοθέτη του νέου Ποινικού Κώδικα να θεωρήσει άξια αυτοτελούς ποινικής προστασίας την εμπιστευτικότητα των ψηφιακών δεδομένων, διευρύνοντας την αντικειμενική υπόσταση του εγκλήματος της αθέμιτης πρόσβασης του άρθρου 370Β ΠΚ (illegal access), χωρίς ωστόσο να θεωρήσει αναγκαία και την αυτοτελή ποινική προστασία της ακεραιότητας και διαθεσιμότητά τους, [401] δηλαδή την προστασία τους έναντι πράξεων διαγραφής, καταστροφής ή αλλοίωσής τους, δημιουργώντας κατά αποτέλεσμα κενό προστασίας για το δικαιούχο της διαχείρισής τους.

Με το Νόμο 4947/2022 προσετέθη η διάταξη 379 ΠΚ,[402] η οποία επανεισάγει τη διάταξη 381Α του καταργηθέντος παλαιού ΠΚ που είχε θεσπιστεί τότε με το Νόμο 4411/2016 και δεν είχε συμπεριληφθεί αρχικά με το Νόμο 4619/2019.

[399] Μυλωνόπουλος, ό.π., ΓενΜ ΙΙ, σελ. 194

[400] ΑιτΕκθΣΧΠΚ 2019, υπό άρθρο 292Ε ΠΚ, 59

[401] *Μπιτζιλέκης Νικόλαος*, Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 325, Μυλωνόπουλος Χ., Εισήγηση στο Ινστιτούτο Ευρωπαϊκού και Διεθνούς Ποινικού Δικαίου, ΔΣΑ 27.3.2019, του ίδιου, Μεταξύ αναγκαιότητος και συγκυρίας, «Καθημερινή» 18.3.2019, του ίδιου, Ιδιοτελείς επικρίσεις και ανιδιοτελείς παραλείψεις, «Καθημερινή» 28.3.2019.

[402] Άρθρο 13. Φθορά ψηφιακών δεδομένων – σε συμμόρφωση με τα άρθρα 5 και 6 της Οδηγίας (ΕΕ) 2019/713 και άρθρα 5 και 7 της Οδηγίας (ΕΕ) 2013/40).

12.1. Προστατευόμενο έννομο αγαθό

Προστατευόμενο έννομο αγαθό της υπό εξέταση διάταξης συνιστά αφενός η ακεραιότητα και αφετέρου η διαθεσιμότητα των ψηφιακών δεδομένων. Η εμπιστευτικότητα δεν καθίσταται εν προκειμένω προστατευτέα, καθώς συνεφέλκεται με το ηλεκτρονικό εμπόριο.[403]

Τα ψηφιακά δεδομένα λόγω της εγγενούς φύσεώς τους ως μη ενσώματων αντικειμένων, δεν έχουν ιδιοκτήτη με την έννοια του δικαιώματος κυριότητας του εμπραγμάτου δικαίου. Όμως, έχουν περισσότερους δικαιούχους, πρόσωπα δηλαδή που κατά νόμο έχουν δικαίωμα να τα διαθέτουν ελεύθερα (να τα μεταβιβάζουν, αλλοιώνουν ή να τα καταστρέφουν), εξουσίες ήτοι προσιδιάζουσες σε εκείνες ενός κυρίου πράγματος. Προστατεύεται κατ' επέκταση κάθε δικαίωμα στα ηλεκτρονικά δεδομένα, όπως συμβαίνει με τα δεδομένα που κάποιος δημιουργεί (όπως ένα κείμενο, έναν πίνακα ή αρχείο), αλλά και σε όσα προγράμματα κάποιος ασκεί ένα είδος απόλυτου δικαιώματος χρήσης (αρχεία επιστημονικών δεδομένων σε εργαστήρια ή ερευνητικά κέντρα). [404]

Φορέας του εννόμου αγαθού είναι συνεπώς ο δικαιούχος των δεδομένων, που κάλλιστα μπορεί να είναι πρόσωπο διάφορο από τον ιδιοκτήτη των υλικών φορέων. Αυτό συμβαίνει κατεξοχήν με το υπολογιστικό νέφος (cloud computing)[405], αλλά και ειδικώς με την εικονοποίηση των εξυπηρετητών (Virtualization), όπου πρόκειται περί ενός ιδεατού μηχανήματος που αποτελείται εξ ολοκλήρου από software και δεν περιέχει υλικά μέρη, όπως αντιθέτως συμβαίνει με το φυσικό μηχάνημα.

---

[403] *Μπιτζιλέκης Νικόλαος*, Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 325

[404] Ωστόσο θα πρέπει να επισημανθεί ότι δεν πρέπει απαραιτήτως να πρόκειται για αντικείμενο πνευματικής ιδιοκτησίας, προστατευόμενο από το Ν. 2121/1993, Βλ. Μπιτζιλέκη Ν., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 326

[405] Η τεχνολογία του «υπολογιστικού νέφους» περιορίζει σημαντικά τη σημασία και τη χρησιμότητα της φυσικής υποδομής, τόσο εκ μέρους των προμηθευτών των σχετικών υπηρεσιών όσο και των χρηστών τους. Αποκρυσταλλώνοντας τα τρία βασικά μοντέλα λειτουργίας των εφαρμογών «υπολογιστικού νέφους» καταρχάς θα αναφερθούμε στο μοντέλο "Infrastructure as a Service" ("IaaS"), το οποίο αφορά στην διαμόρφωση των κατάλληλων συνθηκών για την παροχή υπολογιστικών πόρων, καθώς και ευέλικτης υπολογιστικής δύναμης και σημαντικού αποθηκευτικού χώρου. Στο μοντέλο αυτό ο προμηθευτής των εφαρμογών «υπολογιστικού νέφους» φροντίζει, μέσω της τεχνολογίας εικονικοποίησης, να παράσχει στον εκάστοτε χρήστη τη βασική υποδομή για την εγκατάσταση και ανάπτυξη του υπολογιστικού του οικοσυστήματος. Υφίσταται και το μοντέλο "Platform as a Service" ("PaaS"), που αναφέρεται κυρίως στην εκ μέρους του προμηθευτή διαμόρφωση των κατάλληλων συνθηκών, έτσι ώστε ο εκάστοτε χρήστης να δύναται να αναπτύξει υπολογιστικές εφαρμογές.
Τέλος, αυτό που οι περισσότεροι χρήστες του διαδικτύου γνωρίζουν και χρησιμοποιούν συνιστά το μοντέλο "Software as a Service" ("SaaS") και αναφέρεται στην παροχή παραμετροποιημένων υπολογιστικών εφαρμογών προς άμεση χρήση, χωρίς να απαιτείται κάποια ιδιαίτερη τεχνική διαμόρφωσή τους εκ μέρους του εκάστοτε χρήστη τους. Χαρακτηριστικά παραδείγματα εμφάνισης του μοντέλου "Software as a Service" συνιστούν οι υπηρεσίες ηλεκτρονικού ταχυδρομείου, κειμενογράφου, κατάρτισης υπολογιστικών φύλλων και παρουσιάσεων που προσφέρονται από την εταιρία Google (Gmail, Google Docs, Google Sheets, Google Slides αντίστοιχα), οι αντίστοιχες υπηρεσίες της εταιρίας Microsoft (Outlook, Office 365), καθώς και οι υπηρεσίες δημιουργίας ψηφιακών αποθηκευτικών χώρων όπως λ.χ. αυτές που παρέχονται από την Dropbox, την Google (Google Drive) και την Microsoft (OneDrive). Βλ. *Ρεβολίδη Ιωάννη*, Διεθνής δικαιοδοσία και διαδίκτυο, Κεφάλαιο 6.3.2.3. Ο νομικός χαρακτηρισμός των συμβάσεων «υπολογιστικού νέφους» (cloud computing) 2020, σ. 233, αρ. 124 = sakkoulas-online

Ένα φυσικό σύστημα δύναται να διαχωρίζεται σε πολλαπλά εικονικά περιβάλλοντα, με συνήθη την απόκρυψη της ταυτότητας των φυσικών εξυπηρετών του υπολογιστή, των λειτουργικών συστημάτων και των επεξεργαστών από το χρήστη του εικονικού επεξεργαστή. Πρόκειται για ένα λειτουργικό ιδεατό μηχάνημα με το δικό του λειτουργικό σύστημα και εφαρμογές, όπως και ένας «πραγματικός» υπολογιστής. Ήγουν αυτή η διαφοροποίηση μεταξύ του φυσικού εξυπηρετητή (οικοδεσπότη - host) στον οποίο δύνανται να εγκατασταθούν και να φιλοξενηθούν πλείονα αυτοτελή και μεταξύ τους απομονωμένα λειτουργικά συστήματα (φιλοξενούμενοι εξυπηρετητές - guests), δημιουργεί την ανάγκη αυτοτελούς ποινικής προστασίας του δικαιώματος καθέκαστου.

Το προστατευόμενο έννομο αγαθό έχει χαρακτηριστεί ως κοινωνικό, καθώς το δικαίωμα ακώλυτης χρήσης των δεδομένων από τα δικαιούμενα προς τούτο πρόσωπα μπορεί να αφορά ένα εξαιρετικά μεγάλο αριθμό και απροσδιορίστου ταυτότητας κύκλο προσώπων. [406]

12.2. Χαρακτηρολογικά γνωρίσματα

Λόγω της συστηματικής ένταξης του υπό κρίσιν άρθρου στα εγκλήματα κατά της Ιδιοκτησίας, καθώς και εξαιτίας της διαβάθμισης της ποινικής απαξιολόγησης της εγκληματικής συμπεριφοράς (προνομιούχα και διακεκριμένη παραλλαγή) με γνώμονα -κυρίως- την επελθούσα ζημία, ευλόγως θα μπορούσε να χαρακτηριστεί ως αδίκημα με περιουσιακό χαρακτήρα. Ωστόσο η φθορά ψηφιακών δεδομένων δεν συνιστά αμιγώς περιουσιακό αδίκημα, καθόσον τα ψηφιακά δεδομένα δεν είναι μόνο περιουσιακά αντικείμενα αλλά και χώρος δημιουργίας και ελευθερίας, κομμάτι του ψηφιακού αυτοκαθορισμού του ατόμου, ο «ψηφιακός του κόσμος». [407] Η θέση αυτή επιρρωνύεται από το γεγονός ότι για το εν λόγω αδίκημα δεν προβλέπεται, σε αντίθεση με την κλασική φθορά του άρθρου 378 ΠΚ, ο θεσμός της έμπρακτης μετάνοιας, τον οποίο θα θεμελίωνε η αποκατάσταση της τυχόν προκληθείσης περιουσιακής ζημίας. [408]

Το αδίκημα χαρακτηρίζεται ως έγκλημα απλό, ενεργείας[409], γνήσιο πολύτροπο ή υπαλλακτικώς μικτό, αποτελέσματος (ουσιαστικό), στιγμιαίο και πλημμέλημα.

12.3. Στοιχεία της αντικειμενικής υπόστασης:

Όποιος, χωρίς δικαίωμα, διαγράφει, καταστρέφει, αλλοιώνει, αποκρύπτει, καθιστά ανέφικτη ή αποκλείει την πρόσβαση με οποιονδήποτε τρόπο (:βλαπτική ενέργεια εν στενή εννοία) σε ψηφιακά δεδομένα ενός συστήματος πληροφοριών.

Κοινό έγκλημα: Δράστης του αδικήματος του άρθρου 379 μπορεί να είναι ο οιοσδήποτε

---

[406] Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 237

[407] *Μπιτζιλέκης Ν.*, Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 326

[408] Άρθρο 381 παρ. 2 ΠΚ, όπου γίνεται αναφορά στα αδικήματα κατά της Ιδιοκτησίας πλην των άρθρων 379 και 379Α ΠΚ.

[409] Η φθορά κατ΄ άρθρο 379 ΠΚ μπορεί να διαπραχθεί και με παράλειψη από πρόσωπο που έχει ιδιαίτερη νομική υποχρέωση, βάσει του άρθρου 15 ΠΚ. Φέρ' ειπείν πληρούται η αντικειμενική υπόσταση του εγκλήματος όταν ο υπεύθυνος προγραμματιστής σε μια επιχείρηση δεν εμποδίζει έναν ιό που αντιλήφθηκε ότι εισήλθε στο σύστημα να διαγράψει ή να κλειδώσει τα ηλεκτρονικά αρχεία της επιχείρησης. (Το παράδειγμα από *Μπιτζιλέκη Ν.*, Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 328).

12.3.1. Ψηφιακά δεδομένα και πληροφοριακά συστήματα

Αντικείμενο της κατ' άρθρον 379 ΠΚ φθοράς αποτελούν τα ψηφιακά δεδομένα ενός συστήματος πληροφοριών. Η έννοια των ψηφιακών δεδομένων ορίζεται στο άρθρο 13 περ. ζ' ΠΚ, ενώ στο στοιχείο στ΄ ιδίου άρθρου απαντάται ο ορισμός του πληροφοριακού συστήματος, όπως έχει αναλυθεί εκτενώς ανωτέρω στην παρούσα εργασία. Εν συντομία, τα δεδομένα είναι ροές πρωτογενών στοιχείων πριν οργανωθούν (αναλυθούν και αθροιστούν), προκειμένου να επικοινωνούν κάποιο συγκεκριμένο νόημα. Οι πληροφορίες (για λήψη αποφάσεων, ελέγχων, ανάλυση προβλημάτων, καταγραφή και απεικόνιση θεμάτων) αποτελούν λοιπόν δεδομένα που αποδίδουν κάποιο νόημα και χρησιμότητα, έχοντας ευρύτερη έννοια σε σχέση με την πληροφορία. [410] Όσον αφορά το πληροφοριακό σύστημα (information system) ως τέτοιο νοείται η συσκευή ή ένα σύνολο αλληλοσχετιζόμενων συσκευών, με τα οποία γίνεται συλλογή, επεξεργασία, αποθήκευση και διανομή κάθε είδους ψηφιακών δεδομένων. Ένα πληροφοριακό σύστημα συναπαρτίζεται από το υλικό (hardware), το λογισμικό (software), τις βάσεις δεδομένων, τα δίκτυα και τις διαδικασίες. Οι υπολογιστές με το υλικό και το λογισμικό αποτελούν μέρος του υπολογιστικού συστήματος.[411]

12.3.2. Πράξη φθοράς ψηφιακών δεδομένων

Η περιγραφόμενη από το άρθρο 379ΠΚ πράξη φθοράς των ψηφιακών δεδομένων μπορεί να λάβει χώρα με τη διαγραφή, καταστροφή, αλλοίωση ή απόκρυψη των ψηφιακών δεδομένων ενός συστήματος πληροφοριών. Η ως άνω επέμβαση δύναται να επισυμβεί σε τρία στάδια επεξεργασίας. Συγκεκριμένα, μπορεί να γίνει κατά την είσοδο του πληροφοριακού συστήματος, το οποίο συλλέγει τα πρωτογενή δεδομένα (input), είτε κατά την επεξεργασία που ταξινομεί, διευθετεί και υπολογίζει, μετατρέποντας τα στοιχεία της εισόδου σε κατανοητή μορφή (process), είτε ακόμη και κατά την έξοδο που μεταφέρει τις ζητηθείσες πληροφορίες (output).[412]

Ως ***διαγραφή*** νοείται το σβήσιμο των δεδομένων, υπό την έννοια της άρσης της υλικής σύνδεσης των δεδομένων με τον υλικό φορέα, ήτοι της οριστικής μη ενύλωσης των δεδομένων αυτών. Η εν λόγω επέμβαση μπορεί να γίνει είτε άμεσα, με την επενέργεια επί του υλικού φορέα που περιέχει αυτά, αδιάφορα από το εάν η επενέργεια θα έπεται και φθορά του υλικού φορέα, όπως επί παραδείγματι με την εντελή καταστροφή του ή με την χρήση της εντολής «delete», είτε και έμμεσα, μέσω ενός ειδικού λογισμικού, ενός ιού ή δια μέσου εργαλείων που παρέχει η νεφοϋπολογιστική. [413] Διαγραφή δεν συνιστά η περίπτωση που τα δεδομένα μπορούν να επανακτηθούν άμεσα και χωρίς δυσκολία (με επαναφορά από το «Κάδο Ανακύκλωσης» φέρ' ειπείν), ενώ εάν επανακτηθούν επειδή βρίσκονται αποθηκευμένα και σε άλλους υλικούς φορείς η ποινική απαξία της συμπεριφοράς του δράστη μένει ακέραιη.[414]

Η διαγραφή των δεδομένων συνιστά επί της ουσίας μια μορφή *καταστροφής* και ο όρος αυτός κρίνεται αδόκιμος, καθώς προσιδιάζει σε υλικά αντικείμενα.[415] Ως ***καταστροφή***

---

[410] *Μπιτζιλέκης Ν*., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 327.
[411] *Μπιτζιλέκης Ν*., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 327.
[412] *Μπιτζιλέκης Ν*., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 327.
[413] *Μπιτζιλέκης Ν*., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 328.
[414] "Überwiegend wird angenommen, es müsse um das Löschen der **konkreten** Speicherung gehen: die Existenz zB v. Sicherungskopien ist unerheblich." Urs Kindhäuser, *Strafgesetzbuch. Band 3* (5. Auflage, Nomos 2017). Σελ. 1595
[415] *Χαραλαμπάκης Α*. σε συνεργασία με Μπουρμά Γ., ΟΙ ΑΛΛΑΓΕΣ ΤΟΥ ΝΕΟΥ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ

νοείται στην προκειμένη περίπτωση, εν στενή εννοία, η διαγραφή και εν ευρεία εννοία η απόκρυψη ηλεκτρονικών δεδομένων. [416] Ως μορφή καταστροφής νοείται και εκείνη που επέρχεται με την άμεση καταστροφή του υλικού φορέα των δεδομένων, οπού εκτός του άρθρου 378 πληρούται και η αντικειμενική υπόσταση του 379 ΠΚ, η οποία αφορά στην απώλεια των δεδομένων, πέραν του υλικού φορέα που επεξεργάζεται ή αποθηκεύει τα δεδομένα και το λογισμικό.

Αλλοίωση συνιστά η αλλαγή του περιεχομένου των δεδομένων με προσθήκη άλλων ή αφαίρεση κάποιων άλλων. Η ως άνω αλλοίωση θα πρέπει να λαμβάνει χώρα στον υλικό φορέα που ενυλώνει τα δεδομένα και δεν στοιχειοθετείται ποινική ευθύνη εάν κανείς τα μεταφέρει σε δικό του υλικό φορέα και εκεί στη συνέχεια επιφέρει τις όποιες αλλαγές. Επί παραδείγματι, οι εργαζόμενοι στο δημόσιο είθισται να έχουν δικαίωμα τροποποίησης των αρχείων του τμήματός τους, μπορούν όμως να προβάλουν και να αποθηκεύσουν αρχεία άλλων τμημάτων. Εάν το πράξουν αυτό και εν συνεχεία τροποποιήσουν το περιεχόμενο ενός αρχείου, δεν διαπράτουν το αδίκημα διότι στο φάκελο τον προσπελάσιμο από όλους το αρχείο έχει παραμείνει αλώβητο.

Με γνώμονα το γεγονός ότι το αδίκημα δεν συνιστά αμιγώς περιουσιακής φύσεως έγκλημα, άνευ σημασίας κρίνεται το γεγονός ότι η αλλαγή ενδέχεται να οδήγησε σε ποιοτική αναβάθμιση των δεδομένων αυτών, καθώς η αλλαγή αυτή δεν είναι απαραίτητο να μεταφράζεται σε περιουσιακή ζημία. [417]

Απόκρυψη σημαίνει στέρηση πρόσβασης στα δεδομένα του δικαιούχου, είτε αυτή έχει διαρκή ή πρόσκαιρο χαρακτήρα και δύναται να τελεσθεί τόσο με την απόκρυψη του ίδιου του υλικού φορέα που τα εμπεριέχει όσο και με την εισαγωγή ενός ιού ή προγράμματος, που κλειδώνει τα δεδομένα (κλείδωμα «αχρήστευση»). Εν προκειμένω, παραλληλίζεται με την άρση της λειτουργικής χρησιμότητας των δεδομένων, όπως απαντάται και στο άρθρο 378 στο αδίκημα της κλασικής φθοράς υλικών αντικειμένων. Δεν είναι απαραίτητο να διαπιστωθεί η συγκεκριμένη πρόθεση του εξουσιοδοτημένου ατόμου να χρησιμοποιήσει τα δεδομένα, αλλά ο αποφασιστικός παράγοντας είναι η παρεμπόδιση της πιθανής πρόσβασής του. [418]

Με τον όρο «***καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση***» νοείται κάθε άλλη- διαφορετική από τις προαναφερθείσες-μορφή βλαπτικής επέμβασης σε ηλεκτρονικά δεδομένα. Εν προκειμένω ειδοποιός διαφορά συνιστά το γεγονός ότι ο χρήστης έχει πρόσβαση, αλλά τα δεδομένα ή το ηλεκτρονικό σύστημα δεν είναι διαθέσιμα ή λειτουργικά. [419]

Η «αχρηστεύση» καταφάσκεται όταν η χρηστικότητα των δεδομένων είναι τόσο μειωμένη που δεν μπορούν πλέον να χρησιμοποιηθούν σωστά και επομένως δεν μπορούν πλέον να

Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 235.

[416] Παπανδρέου Πόπη (υπό την επιμέλεια Χαραλαμπάκη Α. και σε συνεργασία Συνεργασία: Γεωργιάδου Μ., Χατζηκωνσταντή Σ.) ΔΙΑΓΡΑΜΜΑΤΑ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ, Γενικό & Ειδικό Μέρος με σχόλια και παρατηρήσεις, Εκδοση 3η 2023, Νομική Βιβλιοθήκη, σελ. 327 υποσ.6.

[417] *Μπιτζιλέκης Ν*., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 328.

[418] Adolf Schönke and others, *Strafgesetzbuch: Kommentar* (30., neu bearbeitete Auflage, CH Beck 2019) Σελ. 2970.

[419] *Χαραλαμπάκης Α*. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ
Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 235.

εκπληρώσουν τον προορισμό τους. [420] Αυτό καθίσταται εφικτό όταν ο δράστης επενεργεί είτε στο πράγραμμα επεξεργασίας είτε στα ηλεκτρονικά δεδομένα καθεαυτά με τέτοιο τρόπο, ώστε αυτά, χωρίς να διαγράφονται ή να αποκρύπτονται, αντικειμενικά να μην μπορούν να αποτελέσουν σημείο αναφοράς για αυτόματη επεξεργασία είτε αυτοτελώς ή εντός συγκεκριμένου πληροφοριακού συστήματος, στο οποίο εντάσσονται, βάσει ορισμένου προγράμματος, οπότε συνακόλουθα διαταράσσονται σοβαρά οι υπηρεσίες των εκάστοτε προσβαλλομένων συστημάτων πληροφοριών. Κατ' επέκταση, δεν μπορούν τα ηλεκτρονικά δεδομένα, να ανακτηθούν ή διαβιβαστούν από τη συσκευή ή την ομάδα συσκευών, όπου είναι αποθηκευμένα, με σκοπό τη λειτουργία, την χρήση, την προστασία και την συντήρηση των συσκευών αυτών. Ο χρήστης δεν έχει πρόσβαση στα ηλεκτρονικά δεδομένα, τα οποία όμως εξακολουθούν να ανήκουν σε ένα λειτουργικό ακόμη σύστημα πληροφοριών. [421]

12.3.3. Χωρίς δικαίωμα

Όλες οι ανωτέρω πράξεις φθοράς των ψηφιακών δεδομένων καθίστανται αξιόποινες, όταν συντελούνται ***χωρίς δικαίωμα***. Παρανόμως πράττει όποιος αποκτά πρόσβαση σε δεδομένα που δεν προορίζονται για αυτόν. Τα δεδομένα προορίζονται για τον παραλήπτη, όταν του διαβιβάζονται για χρήση. Ο όρος της «χωρίς δικαίωμα» (παράνομης ή αυθαίρετης) βλαπτικής επενέργειας στα ηλεκτρονικά δεδομένα αποτελεί αδιαμφισβήτητα νομική αξιολογική έννοια και δη ειδικό στοιχείο του αδίκου,[422] βάσει του οποίου προσδιορίζεται και περιορίζεται το μέγεθος της αξιόποινης προσβολής, η αξιόποινη δηλαδή επέμβαση στα δεδομένα άλλου. Πλάνη ως προς τις πραγματικές προϋποθέσεις των στοιχείων αυτών είναι πραγματική, ενώ η πλάνη ως προς την αξιολόγηση που αυτά εκφράζουν είναι πλάνη περί το άδικο (31 παρ. 2 ΠΚ) και ωφελεί το δράστη, μόνο αν είναι συγγνωστή. Τέτοια πλάνη υπάρχει ακριβώς όταν ο δράστης δεν βρίσκεται σε θέση να αντιληφθεί το κοινωνικό νόημα της συμπεριφοράς του.[423]

---

[420] Schönke and others (n 18). Σελ΄. 2970 στα πλαίσια ερμηνείας του άρθρου 303a StGB "Datenveränderung"

[421] Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 236.

[422] Η σπουδαιότητα της επισήμανσης αυτής έγκειται στο ότι, ενώ τα στοιχεία της αντικειμενικής υπόστασης επικαλύπτονται από τη γνώση και θέληση του δράστη να τα πραγματώσει (από την υποκειμενική υπόσταση) και, κατά συνέπεια, η άγνοιά τους συνιστά πραγματική πλάνη, τα ειδικά στοιχεία του αδίκου επικαλύπτονται όχι από την υποκειμενική υπόσταση, αλλά από τη συνείδηση του αδίκου, ώστε η άγνοια –ή ορθότερα: η εσφαλμένη αντίληψή τους– να αποτελεί νομική πλάνη, η οποία, αίρει τον καταλογισμό, μόνον αν κριθεί «συγγνωστή» (συγχωρητή) όπως προκύπτει από Μανωλεδάκη Ι., Ποινικό Δίκαιο, 7η έκδ., 2005, σ. 604, αρ. 1030 = sakkoulas-online, καθώς και Χαραλαμπάκη Α., Σύνοψη Ποινικού Δικαίου, Γενικό Μέρος Ι, Το έγκλημα, Π.Ν. Σάκκουλας 2010, σελ. 433, Μυλωνόπουλο Χ., Ποινικό Δίκαιο, Γενικό Μέρος Ι, Δίκαιο και Οικονομία 2007, σελ. 289, και Ά. Ψαρούδα-Μπενάκη, Τα αξιολογικά στοιχεία της αντικειμενικής υποστάσεως του εγκλήματος, Αφοί Π. Σάκκουλα 1971, σελ. 139 επ.

[423] Όταν γίνεται αναφορά σε «γνώση» ή «άγνοια» των περιστατικών δεν σημαίνει ότι ο δράστης θα πρέπει απαραίτητα να είναι σε θέση να προβεί και στην ακριβή νομική αξιολόγησή τους, αλλά αρκεί να είναι σε θέση να αντιληφθεί το κοινωνικό νόημα της συμπεριφοράς του επί τη βάσει της λεγόμενης « παράλληλης εκτίμησης στην κοινή γνώμη», όπως προκύπτει από Χαραλαμπάκη Α., Σύνοψη Ποινικού Δικαίου, Γενικό Μέρος Ι, Το έγκλημα, Π.Ν. Σάκκουλας 2010, σελ.586. Κρίνεται εύλογη η μη απαίτηση ακριβούς γνώσης του παραβιαζόμενου κανόνα, διότι διαφορετικά, όπως είπε και ο Frank «μόνο οι νομικοί θα μπορούσαν να τελούν αδικήματα» από Μυλωνόπουλο Χ., Ποινικό Δίκαιο, Γενικό Μέρος Ι, Δίκαιο και Οικονομία 2007, σελ.632 (Frank, Das Strafgesetzbuch für das Deutsche Reich, 18. Aufl. 1931, § 59 αρ. II). Συνεπώς, δεν αρκεί μια ενγένει γνώση, ότι η περί ης πρόκειται συμπεριφορά αντιφάσκει σε μια οποιαδήποτε απαγόρευση ή επιταγή του δικαίου, αλλά απαιτείται μια «παράλληλη» έστω

Όσον αφορά το περιεχόμενο του νομοτυπικού όρου «χωρίς δικαίωμα» σκόπιμη κρίνεται η μνεία του άρθρου 2 στοιχεί δ΄ της Οδηγίας για το Κυβερνοέγκλημα, όπου η ως άνω έννοια στα πλαίσια της Οδηγίας νοείται ως συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, (παρεμβολής ή υποκλοπής), μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου. Ωστόσο με τον ορισμό αυτό δεν προσδιορίζεται η έννοια της «μη εξουσιοδοτημένης» πρόσβασης, ενώ για το «επιτρεπτό ή μη» επαφίεται στην κρίση του εκάστου κράτος.

Δικαίωμα υπάρχει πρωτίστως όταν ο δικαιούχος των ψηφιακών δεδομένων, συναινεί στην αλλοίωση, στη διαγραφή ή στο κλείδωμά τους. Χωρίς δικαίωμα επενεργεί κάποιος βλαπτικά σε ηλεκτρονικά δεδομένα αφενός όταν δεν είναι ο νόμιμος δικαιούχος ή κάτοχος/ χρήστης τους και αφετέρου όταν είναι μεν νόμιμος κάτοχός τους, αλλά περιορίζεται από το νόμο ή τη σύμβαση ως προς το τρόπο της χρήσης τους και παραβαίνει αυτούς τους περιορισμούς.[424]

Κάτοχος των ηλεκτρονικών δεδομένων καθίσταται εκείνος ο οποίος έχει την «ψηφιακή» εξουσία πάνω στα σχετικά δεδομένα και μπορεί να έχει πρόσβαση πάνω σ' αυτά, να τα επεξεργάζεται, αποθηκεύει, διακινεί και γενικότερα διαθέτει αυτά, όποτε και όπως επιθυμεί.[425] Η ως άνω ιδιότητα δεν συμπίπτει απαραιτήτως και για το λόγο αυτό δεν πρέπει να συγχέεται με την ιδιότητα του ιδιοκτήτη επί του υλικού φορέα, στον οποίο είναι αποθηκευμένα τα εκάστοτε ηλεκτρονικά δεδομένα, ή με εκείνη του δικαιούχου των εν λόγω άυλων στοιχείων. [426]

Δικαιούχος είναι το πρόσωπο, το οποίο αφορούν είτε α) τα δεδομένα αυτά καθεαυτά είτε β) το σύστημα πληροφοριών, στο οποίο εντάσσονται αυτά, είτε γ) τέλος το πρόγραμμα, σύμφωνα με το οποίο πραγματοποιείται η αυτόματη επεξεργασία των δεδομένων.

«εκτίμηση στη σφαίρα του μη ειδήμονος» γνώση του εκάστοτε συγκεκριμένου αδίκου, εκείνου που περιλαμβάνεται στην οικεία ειδική υπόσταση, όπως Ανδρουλάκης Ν., Ποινικό Δίκαιο, Γενικό Μέρος Ι, Θεωρίες για το έγκλημα, σελ. 518 – 520. Δίκαιο και Οικονομία 2006,Βλ. και Die Lehre von der Parallelwertung in der Laiensphäre bei den sog. normativen Tatbestandsmerkmalen, NK-StGB/Puppe, 6. Aufl. 2023, StGB § 16

[424] Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 236.

[425] Παπανδρέου Πόπη (υπό την επιμέλεια Χαραλαμπάκη Α. και σε συνεργασία Συνεργασία: Γεωργιάδου Μ., Χατζηκωνσταντή Σ.) ΔΙΑΓΡΑΜΜΑΤΑ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ, Γενικό & Ειδικό Μέρος με σχόλια και παρατηρήσεις, Έκδοση 3η 2023, Νομική Βιβλιοθήκη, σελ. 327 υποσ. 7.

[426] Νομολογιακά έχει τύχει επεξεργασίας η έννοια της κατοχής, κυρίως στα πλαίσια κατοχής πορνογραφικού υλικού, με υιοθετούμενο κριτήριο για τη στοιχειοθέτησή της αυτό της δυνατότητας πρόσβασης στο υλικό, ενδεικτικά βλ. Γεώργιος Νούσκαλης, Παρατηρήσεις στην ΑΠ (Συμβ) 465/2008, ΤΝΠ QUALEX ΠοινΔικ, 1/2009, σελ. 23 – 24, Απόφαση ΑΠ 1141 / 2008 (ΣΤ, ΠΟΙΝΙΚΕΣ) (προσπελάσιμη: https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=tGTmKhEZx6VgA29oxUej2zANdjdJC0&apof=1141_2008&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%D3%D4), Απόφαση ΑΠ 628 / 2006 (ΣΤ, ΠΟΙΝΙΚΕΣ) (προσπελάσιμη: https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=NFJVYQ3XV1CYP5D24X6IG8PS79Z30Y&apof=628_2006&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%D3%D4), Απόφαση ΑΠ 810 / 2007 (Ζ, ΠΟΙΝΙΚΕΣ) (προσπελάσιμη: https://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=UklGMfc9ZnLrxH4NcmP5bv4E25O3TR&apof=810_2007&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%C6), καθώς από θεωρία βλ. της Βασιλικής Χαλκιαδάκη, Παιδική πορνογραφία στο διαδίκτυο, Η κατοχή υλικού παιδικής πορνογραφίας μέσω ηλεκτρονικού συστήματος υπό το φως της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των παιδιών κατά της γενετήσιας κακοποίησης και εκμετάλλευσης, Τεύχος 19 - Ιούλιος 2011.

Υποστηρίζεται μάλιστα ότι μόνο τα πρόσωπα αυτά (ήγουν ο νόμιμος δικαιούχος ή κάτοχος – χρήστης των δεδομένων) μπορούν να θεωρηθούν ως φορείς του προστατευόμενου εννόμου αγαθού, παθόντες από το συγκεκριμένο έγκλημα και κατ' επέκταση νομιμοποιούμενοι προς παράσταση για την υποστήριξη της κατηγορίας κατά του δράστη του εγκλήματος αυτού. [427]

Συγκεφαλαιωτικά, εκείνος ο οποίος έχει την αποκλειστική εξουσία για ολόκληρο το σύστημα, δεν πράττει αξιόποινα αν τελέσει κάποια από τις περιγραφόμενες στο άρθρο 379 ΠΚ πράξεις. Ωστόσο, δράστης καθίσταται εκείνος ο οποίος είναι εξουσιοδοτημένος να χρησιμοποιήσει μέρος μόνο του συστήματος ή δεν έχει καθόλου τη σχετική εξουσιοδότηση.

12.4. Προνομιούχα παραλλαγή

Στην παράγραφο 1 in fine διαπλάσσεται προνομιούχα παραλλαγή του αδικήματος, όταν η ζημία που προκλήθηκε είναι ελαφρά και ο υπαίτιος τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.[428]

Ο όρος «ελαφρά ζημία» έχει κριθεί ως αόριστη νομική αξιολογική – διαβαθμίσιμη έννοια. Αξιολογικές είναι οι έννοιες, η συνδρομή των οποίων διαπιστώνεται με τη βοήθεια μιας νομικής ή κοινωνικοηθικής αξιολόγησης.[429] Δέον η έννοια αυτή να ελέγχεται αναιρετικά από τον Άρειο Πάγο. Επιπλέον, ως διαβαθμίσιμη έννοια, προσδιορίζεται με συγκριτική συσχέτιση με ένα σημείο αναφοράς, το οποίο διαφέρει ανάλογα με το πλαίσιο (Kontext), στο οποίο κάθε φορά αναφερόμαστε. Βάσει των ανωτέρω, η συγκεκριμένη έννοια δύναται να χαρακτηριστεί ως συγκριτική (comparative Begriffe) και η διαπίστωσή της μπορεί να γίνει με συλλογισμούς της μορφής: όσο περισσότερο η υπό κρίση αξία προσεγγίζει ένα ασφαλές σημείο αναφοράς, τόσο περισσότερο υποστηρίξιμη είναι η άποψη, ότι η έννοια συντρέχει.

12.5. Διακεκριμένες περιπτώσεις φθοράς κατά την παράγραφο 2 του άρθρου 379 ΠΚ

Α) Βάσει του μεγέθους της ψηφιακής επέμβασης.

Η φθορά ψηφιακών δεδομένων όταν θίγει ένα μεγάλο αριθμό πληροφοριακών συστημάτων με παράλληλη χρήση εργαλείου σχεδιασμένου κατά κύριο λόγο για το σκοπό αυτό, ανάγει την εν λόγω συμπεριφορά σε απλώς διακεκριμένη παραλλαγή, επισύροντας ποινή φυλακίσεως από 10 ημέρες έως 3 έτη και σωρευτικά χρηματική ποινή (379 παρ. 2 στοιχείο α΄). Η επέμβαση στο σύστημα μπορεί να λάβει χώρα με την αποστολή λόγου χάρη ενός ιού, που διαγράφει ή κλειδώνει δεδομένα, τα οποία ανήκουν σε πολλά πληροφοριακά συστήματα και καταρχήν θίγουν περισσότερους δικαιούχους, αφού τα πολλά πληροφοριακά συστήματα, ως διαφορετικά συστήματα διαχείρισης βάσης δεδομένων, είτε ανήκουν σε περισσότερα πρόσωπα είτε διαμορφώνουν διαφορετικές διαδικασίες λήψης αποφάσεων και δράσης. [430] Κρίσιμη παράμετρο για τη σταχυολόγηση των περιπτώσεων που αναβιβάζονται

[427] Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 237

[428] Για την παροχή κοινωφελούς εργασίας Βλ. ΚΥΑ 56169/2022 (ΦΕΚ Β' 6259/12.12.2022). Έναρξη ισχύος 3 μήνες από τη δημοσίευσή της στην Εφημερίδα της Κυβερνήσεως. (προσπελάσιμο: https://www.karagilanis.gr/files/kya_56169_2022.pdf)

[429] Βλ. Μυλωνόπουλο Χ., Ποινικό Δίκαιο, Γενικό Μέρος, Έκδοση 2η 2020, σελ. 164 επ. (Κεφάλαιο για τα αξιολογικά και περιγραφικά στοιχεία της αντικειμενικής υπόστασης).

[430] Μπιτζιλέκης Ν., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 332.

σε διακεκριμένη παραλλαγή υπό το στοιχείο α' της παρ. 2 του 379, θα αποτελέσει η αυτοτέλεια του κάθε επιμέρους συστήματος. Φέρ' ειπείν, σε μια επιχείρηση ή υπηρεσία μπορεί ένα σύστημα για τους εργαζομένους, άλλο για τα κτίρια και τις υποδομές, άλλο για τη διαχείριση πελατειακών σχέσεων και άλλο για τα κεφάλαια και έκαστο τέτοιο σύστημα κάλλιστα μπορεί να αναλύεται σε άλλα υποσυστήματα. [431]

Η φθορά εκτός από το μεγάλο αριθμό πληροφοριακών συστημάτων που πρέπει να θίγει, προσαπαιτείται να έχει προκληθεί με εργαλείο που έχει σχεδιαστεί κατά κύριο λόγο για έναν τέτοιο σκοπό. Στην συγκεκριμένη διάταξη ο όρος «εργαλείο» εννοιολογικά ταυτίζεται με τα «προηγμένης τεχνολογίας» εργαλεία για τη τέλεση κυβερνοεγκλημάτων, τα οποία περιγράφονται στην παράγραφο 3 του υπό εξέταση άρθρου. [432] Εν προκειμένω ως εργαλείο υπολαμβάνεται όχι μόνον το υλικό αντικείμενο, αλλά και μέσο. Τουτέστιν, στην ως άνω έννοια μπορεί να υπαχθεί και ένα κακόβουλο λογισμικό, το οποίο έχει δημιουργηθεί προκειμένου να πλήξει τα ψηφιακά δεδομένα.

Β) Βάσει του ύψους της ζημίας

Με βάση το ύψος της επελθούσης ζημίας από τη φθορά των ψηφιακών δεδομένων, συνδιαμορφώνεται ιδιαίτερα διακεκριμένη παραλλαγή του αδικήματος στην παράγραφο 2 στοιχείο β΄, με προβλεπόμενο πλαίσιο ποινής φυλάκιση από 1 έως 5 έτη και χρηματική ποινή. Το μέγεθος της ζημίας αποτελεί αξιολογική στάθμιση - διαβαθμίσιμη έννοια και ο προσδιορισμός της επαφίεται στο δικαστή, όπως αντίστοιχα συμβαίνει και με τη διαβάθμιση της αξίας του πράγματος.[433] Το μέγεθος της ζημίας επί τη βάσει τριών διαφορετικών κατευθύνσεων.

Αρχικά, ζημία μπορεί να συνιστά το αποτέλεσμα της *μη λειτουργίας ή μη ορθής λειτουργίας των πληροφοριακών συστημάτων*, με σημείο αναφοράς το βαθμό αδρανοποίησης της λειτουργίας των συστημάτων πληροφορικής. Ενδεικτικά, αναφέρεται η μεγάλη έκσταση ή σε χρόνο διατάραξη των υπηρεσιών των συστημάτων πληροφοριών.

Περαιτέρω, καταφάσκεται η «σοβαρή» ζημία, όταν επέρχεται *οικονομική ζημία ιδιαίτερα μεγάλης αξίας*, σε συστοιχία με την κλασική φθορά ιδιαίτερα μεγάλης αξίας. Εν προκειμένω καλύπτεται όχι μόνο η αξία των δεδομένων, με το κόστος επανάκτησής τους, αλλά και η έμμεση οικονομική ζημία και τα περιουσιακά δικαιώματα, τα οποία χάνονται από την απώλεια των ψηφιακών δεδομένων (λ.χ. μη έγκαιρη κατάθεση προσφοράς και μη συμμετοχή σε κάποιο διαγωνισμό).[434]

Τέλος, η σοβαρή ζημία προσδιορίζεται και επί τη βάσει του εύρους της απώλειας των δεδομένων. Εν προκειμένω, βαρύνουσας σημασίας είναι το πλήθος των δεδομένων που απωλέσθηκαν, ανεξάρτητα από το εάν η απώλεια αυτή επέφερε μεγάλη οικονομική ζημία ή αν το ύψος της ζημίας είναι δύσκολο ή αδύνατο να υπολογιστεί. Εδώ εντάσσονται

[431] *Μπιτζιλέκης Ν*., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 332.
[432] Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 240.
[433] Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 240
[434] *Μπιτζιλέκης Ν*., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 333.

περιπτώσεις επιστημονικών εργασιών, ερευνητικών μελετών ή άλλων αρχείων (ιστορικών, πολιτικών) τα οποία δεν έχουν άμεσα οικονομική – περιουσιακή αποτίμηση ή μια τέτοια αποτίμηση θα ήτο δύσκολη ή εν πάση περιπτώσει αδιάφορη. [435]

Γ) Βάσει του είδους των πληροφοριακών συστημάτων

Η επελθούσα περιουσιακή ζημία μπορεί να χαρακτηριστεί σοβαρή με γνώμονα το είδος των πληροφοριακών συστημάτων τα οποία προσβάλλονται. Συγκεκριμένα πρόκειται για συστήματα τα οποία αποτελούν μέρος υποδομής αναφορικά με την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Από την ίδια τη διάταξη (379 παρ. 2 in fine), ενδεικτικώς απαριθμούνται η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια, ως ζωτικής σημασίας αγαθά ή υπηρεσίες. Προς την ίδια κατεύθυνση μπορεί ο εν λόγω κατάλογος να συμπληρωθεί με άλλους ανάλογους τομείς, όπως η παιδεία, ο πολιτισμός, το περιβάλλον, η εθνική οικονομία, η δημόσια ασφάλεια και η δικαιοσύνη. Η ratio της συγκεκριμένης πρόβλεψης συνίσταται στην αυστηρότερη μεταχείριση επιθέσεων που πλήττουν μέρος των υπηρεσιών (δημοσίου ή ιδιωτικού τομέα) που παρέχουν αυτά τα ζωτικής για το πληθυσμό αγαθά, ήτοι δεν αρκεί μια απλή διατάραξη των πληροφοριακών συστημάτων, τα οποία εξυπηρετούν τη λειτουργία των πιο πάνω υπηρεσιών, αλλά απαιτείται μια διατάραξη από την οποία να θίγεται η ίδια η υποδομή των παροχών. [436]

Λόγω του ιδιαίτερου ειδοποιού γνωρίσματος του εγκλήματος της τελευταίας περίπτωσης, ήτοι της μεγάλης σημασίας του πληττόμενου εννόμου αγαθού (ζωτικής σημασίας), το οποίο δεν μόνον ατομικό αλλά και κοινωνικό, υποστηρίζεται ότι το συγκεκριμένο έγκλημα είναι ιδιώνυμο ως προς αυτό της παραγράφου 1 του άρθρου 379.[437]

12.6. Τιμώρηση των προπαρασκευαστικών πράξεων

Η διάταξη της παρ. 3 του άρθρου 379 ΠΚ καθιστά ποινικό αδίκημα τις προπαρασκευαστικές των προπ- γούμενων εγκλημάτων πράξεις, όπως η χρήση δικτύων botnets,

Το αδίκημα χαρακτηρίζεται ως ιδιώνυμο ως προς αυτά της παρ. 1.[438] Επίσης, συνιστά έγκλημα αφηρημένης διακινδύνευσης καθώς και έγκλημα σκοπού, ήγουν με υπερχειλή υποκειμενική υπόσταση. [439]

12.7. Υποκειμενική υπόσταση

Για την πλήρωση της υποκειμενικής υπόστασης τόσο του βασικού εγκλήματος όσο και των διακεκριμένων παραλλαγών αρκεί κάθε μορφή δόλου, όπως συνάγεται από τον συνδυασμό των άρθρων 18, 26 και 27 παρ. 1 ΠΚ, ο οποίος θα επικαλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης.

12.8. Ποινική κύρωση

Με ποινή φυλάκισης έως 2 έτη και χρηματική ποινή τιμωρείται η φθορά ψηφιακών δεδομένων στη βασική της μορφή (παρ. 1 εδ. α' ΠΚ). Στην περίπτωση που η προκληθείσα ζημία είναι ελαφρά, η ποινή είναι χρηματική ή συνιστάται σε παροχή κοινωφελούς

[435] *Μπιτζιλέκης Ν.*, Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 333.
[436] *Μπιτζιλέκης Ν.*, Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 334
[437] Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη, σελ. 240
[438] Χαραλαμπάκης, ό.π. σελ. 241
[439] Χαραλαμπάκης, Σύνοψη ΓενΜ Ι, σελ. 431, Μυλωνόπουλος, ΓενΜ Ι, σελ. 239

εργασίας.. Εφόσον πληρούνται οι όροι της παραγράφου 2 του άρθρου, η ποινή διαμορφώνεται στην α' περίπτωση σε φυλάκιση από 10 ημέρες έως 3 έτη και χρηματική ποινή, ενώ στη β΄ περίπτωση σε φυλάκιση από 1 έτος έως 5 έτη και χρηματική ποινή. Διακεκριμένη παραλλαγή στοιχειοθετείται στην περίπτωση που το αδίκημα έλαβε χώρα στο πλαίσιο εγκληματικής οργάνωσης, επαπειλώντας το άρθρο 379Α ΠΚ, ποινή φυλάκισης τουλάχιστον 1 έτους και χρηματική ποινή, όπως το άρθρο προστέθηκε με το άρθρο 14 του Νόμου 4947/2022).

12.9. Ειδικές μορφές εμφάνισης του εγκλήματος

12.9.1. Απόπειρα

Αναφορικά με τα αδικήματα τα προβλεπόμενα στις παραγράφους 1 και 2 δεν υπάρχουν αποκκλίσεις από τις οικείες προβλέψεις του γενικού μέρους. Αναφορικά με την παράγραφο 3 δεδομένου ότι ανάγονται σε αξιόποινη συμπεριφορά οι προπαρασκευαστικές πράξεις του βασικού αδικήματος, ορθότερο να γίνει δεκτό, ενόψει του ότι πρόκειται για έγκλημα επιχειρήσεως, ότι δεν τιμωρείται η απόπειρα αυτού.

12.9.2. Συμμετοχή

Ομοίως και για τη συμμετοχική ευθύνη δεν εντοπίζονται παρεκκλίσεις από τις οικείες διατάξεις του γενικού μέρους.

12.9.3. Συρροές

Η συρροή του αδικήματος του άρθρου 379 ΠΚ με τη φθορά του υλικού φορέα των δεδομένων (378 ΠΚ) ενός υπολογιστή, ενός εξωτερικού δίσκου ή USB, αλλά και ενός έξυπνου κινητού τηλεφώνου, ψηφιακής τηλεόρασης ή φωτογραφικής μηχανής που περιέχουν ψηφιακά δεδομένα, θα είναι φαινομενική εφόσον η φθορά του υλικού φορέα λειτουργεί ως αναγκαίο μέσο για τη φθορά των ψηφιακών δεδομένων τα οποία περιέχονται στον υλικό φορέα. Θα υπερισχύσει το βαρύτερο αδίκημα καθώς είναι δυνατόν η φθορά του υλικού φορέα να είναι μικρή ή κανονικής αξίας, ενώ αντιθέτως η φθορά των δεδομένων που προκαλείται από αυτή ιδιαίτερα μεγάλης αξίας. [440]

13. Αντί επιλόγου

Τα συστήματα πληροφοριών και τα ψηφιακά δεδομένα αναγνωρίζονται ως βασικό στοιχείο της πολιτικής, κοινωνικής και οικονομικής αλληλεπίδρασης. Η πληροφοριακή ασφάλεια αποτελεί, χωρίς αμφιβολία, παράμετρο ζωτικής σημασίας για τη νομοθεσία στον τομέα του ηλεκτρονικού εγκλήματος. Ειδικά όσον αφορά την πολιτική της ΕΕ, τα πληροφοριακά συστήματα και η ασφάλειά τους αποτελούν αγαθό που πρέπει να διασφαλίζεται και να προστατεύεται με πολλαπλό τρόπο. Η προστασία των πληροφοριακών συστημάτων και ψηφιακών δεδομένων επιτυγχάνεται όταν το ακόλουθο τρίπτυχο προασπίζεται. Συγκεκριμένα,

α) Εμπιστευτικότητα (confidentiality)

Η «εμπιστευτικότητα» επιτυγχάνεται όταν ένα μη εξουσιοδοτημένο τρίτο μέρος δεν μπορεί να αποκτήσει γνώση του περιεχομένου των μηνυμάτων ή των δεδομένων. Η εμπιστευτικότητα συνυφαίνεται με την ιδιωτικότητα, δηλαδή τα δεδομένα να μην διαβιβάζονται σε μη εξουσιοδοτημένα άτομα και τα εξουσιοδοτημένα άτομα να λαμβάνουν μόνο τα απολύτως απαραίτητα δεδομένα.

[440] *Μπιτζιλέκης Ν.*, Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα, σελ. 329.

β) Ακεραιότητα (integrity)

Η απαίτηση ακεραιότητας βασίζεται στο αμετάβλητο των δεδομένων από μη εξουσιοδοτημένα πρόσωπα.

γ) Διαθεσιμότητα (availability)

Η Διαθεσιμότητα που σχετίζεται με την εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι προσπελάσιμα χωρίς αδικαιολόγητη καθυστέρηση σε εξουσιοδοτημένους χρήστες. Μια τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης παροχής υπηρεσιών, DOS attack.

Το Ανώτατο Συνταγματικό Δικαστήριο της Γερμανίας ανήγαγε σε συνταγματικό δικαίωμα τη πληροφορική ασφάλεια (IT-Sicherheit) και αυθεντικά ορισμοδότησε στην απόφασή του το περιεχόμενο του δικαιώματος αυτού, το οποίο διέκρινε τόσο από το δικαίωμα πληροφοριακού αυτοκαθορισμού (Recht auf informationelle Selbstbestimmung), όσο και από το απόρρητο των τηλεπικοινωνιών (Telekommunikationsgeheimnis).

Παρ’ ημίν, οι ποινικώς κολάσιμες συμπεριφορές που βάλλουν κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών συστημάτων και ψηφιακών δεδομένων, απαντώνται στις διατάξεις 370Β έως 370ΣΤ, 292Β έως 292Ε και 379 του νέου Ποινικού Κώδικα, όπως ισχύει μετά τους Νόμους 4947/2022 και 5002/2022.

Οι τυποποιούμενες αξιόποινες προσβολές καταρχήν συμπλέουν με το διεθνές (Σύμβαση της Βουδαπέστης) και ενωσιακό νομοθετικό πλαίσιο (Οδηγία 2013/40/ΕΕ) για την ποινική αντιμετώπιση των επιθέσεων κατά της ασφάλειας των πληροφοριακών συστημάτων και δεδομένων. Αναντίρρητα ο Έλληνας νομοθέτης έχει επιδείξει μείζον ενδιαφέρον προς την κατεύθυνση καταστολής συμπεριφορών που πλήττουν την πληροφοριακή ασφάλεια, υπερακοντίζοντας τις επιταγές των ενωσιακών ή διεθνών νομικών νομοθετικών κειμένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Συγγράμματα

Ανδρουλάκης Ν., Ποινικό Δίκαιο- Γενικό Μέρος, ΙΙ Απόπειρα και Συμμετοχή, (Π.Ν. Σάκκουλας 2004

Ανδρουλάκης Ν., Ποινικό Δίκαιο, Γενικό Μέρος Ι, Θεωρίες για το έγκλημα

Αργυρόπουλος Α., Ηλεκτρονική εγκληματικότητα, Τα αδικήματα της χωρίς άδεια απόκτησης δεδομένων (202a StGB), της παραποίησης δεδομένων (303a StGB) και της δολιοφθοράς Η/Υ (303b StGB) σε σχέση με το hacking και τη μετάδοση των ηλεκτρονικών ιών στο Internet (ΑΝΤ. Ν. Σάκκουλα 2001).

Βασιλάκη Ε., Η ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ ΜΕΣΩ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ Η Αντιμετώπιση Του Προβλήματος Ιδιαίτερα Μετά Την Εισαγωγή Του Ν 1805/88 (ΑΝΤ Ν ΣΑΚΚΟΥΛΑ 1993). Σελ. 159-162

Δαλακούρα Θ., Ηλεκτρονικό Έγκλημα - Ουσιαστικές και δικονομικές όψεις, 2η έκδοση, (Νομική Βιβλιοθήκη 2023), σελ. 38

Ζέκος Γ., Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, 2022

Ζήσης Α., Από τον πολιτικώς ενάγοντα στον παριστάμενο για την υποστήριξη της κατηγορίας, 2023, σ. 213-216

Ιγγλεζάκης Ι., Δίκαιο Πληροφορικής, 4η έκδ., 2021

Καμπέρου Ε. σε Αριστοτέλη Χαραλαμπάκη (ed), *Ο Νέος Ποινικός Κώδικας, Ερμηνεία Κατ΄ Άρθρο, Άρθρα 235-469*, vol 2 (Νομική Βιβλιοθήκη 2021).

Κιούπης Δ., Ποινικό Δίκαιο και Internet (ΑΝΤ. Ν. Σάκκουλα 1999), Κονταξής Α., ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ – Συνδυασμός θεωρίας και πράξης, τόμος Β΄, 3η έκδοση, (Αντ. Ν. Σάκκουλας, 2000)

Κοτσίρης, Δίκαιο ανταγωνισμού

Κουμάντου, Πνευματική ιδιοκτησία

Κωνσταντινίδης, Καθήκον μαρτυρίας και επαγγελματικό απόρρητο στην ποινική δίκη, τεύχος β', ΑΝΤ. Ν. ΣΑΚΚΟΥΛΑΣ 1991

Κωστάρας Α., *ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ – ΕΠΙΤΟΜΗ ΕΙΔΙΚΟΥ ΜΕΡΟΥΣ (Άρθρα 134-410 ΠΚ)* (4η, Νομική Βιβλιοθήκη 2014). Σελ. 1153

Λαμπράκης Χ., σε Χαραλαμπάκη Α., Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο, τόμος Β', άρθρα 207-473, σελ. 1722, στα πλαίσια ερμηνεία του παλαιού 370Β ΠΚ

Μανωλεδάκη Ι., Ποινικό Δίκαιο, 7η έκδ., 2005

Μανωλεδάκης Ι., Επιτομή Γενικού Μέρους, ζ΄ έκδοση, Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2005

Μανωλεδάκης, Ερμηνεία κατ᾽ άρθρο των όρων του ειδικού μέρους του Ποινικού Κώδικα,(Σάκκουλα 1996)

Μαργαρίτης Μ. και Μαργαρίτη Α., *ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ Ερμηνεία – Εφαρμογές* (4η, Π Ν Σάκκουλας 2020). Σελ. 1084

Μαρίνου, Πνευματική ιδιοκτησία

Μαυρίδης Ι., Ασφάλεια πληροφοριών στο διαδίκτυο, σελ. 40 επ., Κεφάλαιο 2.6. «Το επίπεδο Εφαρμογής», Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα, www.kallipos.gr, ΣΕΑΒ, 2015.

Μεταξάκης Ε., ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ Βασικές έννοιες – Ερμηνεία διεθνούς, ενωσιακής και ημεδαπής νομοθεσίας – Τυπολογία, (Π. Ν. Σάκκουλας 2022)

Μπαμπινιώτη Γ., Λεξικό της νέας ελληνικής γλώσσας

Μπενάκη, Αξιολογικά στοιχεία της αντικειμενικής υποστάσεως του εγκλήματος, 1971, σελ. 193, επ)

Μπιτζιλέκης Ν., Εγκλήματα κατά της ιδιοκτησίας, 2η έκδοση 2023, Εκδόσεις Σάκκουλα

Μυλωνόπουλο Χ., Ποινικό Δίκαιο, Γενικό Μέρος Ι, Δίκαιο και Οικονομία 2007

του Ιδίου, Ποινικό Δίκαιο, Γενικό Μέρος, Έκδοση 2η 2020

του Ιδίου, «Ζητήματα Απόπειρας κατά τον νέο Ποινικό Κώδικα» Ποινική Δικαιοσύνη 2020, σελίδα 321

του Ιδίου, Διεθνές & Ευρωπαϊκό Ποινικό Δίκαιο, 2021

του Ιδίου, ΗΛΕΚΤΡΟΝΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ Συμβολή Στην Ερμηνεία Των Άρθρων 13γ, 370Β, 370Γ Και 386Α ΠΚ (Άρθρα 2-5 Ν. 1805/1988) (ΑΝΤ Ν ΣΑΚΚΟΥΛΑ 1991).Σελ. 92

του Ιδίου, Ιδιοτελείς επικρίσεις και ανιδιοτελείς παραλείψεις, «Καθημερινή» 28.3.2019

του Ιδίου, Μεταξύ αναγκαιότητος και συγκυρίας, «Καθημερινή» 18.3.2019

του Ιδίου., Εισήγηση στο Ινστιτούτο Ευρωπαϊκού και Διεθνούς Ποινικού Δικαίου, ΔΣΑ 27.3.2019

Παπαδαμάκης Α., Στρατιωτικό Ποινικό Δίκαιο, Θεωρητική θεμελίωση και συστηματική ερμηνεία του νέου στρατιωτικού ποινικού κώδικα: Εισαγωγή, θεμελιώδεις έννοιες, ουσιαστικό μέρος, δικονομικό μέρος, (Σάκκουλας 2008), σελ. 354 έως 355

Παπαδοπούλου Α., Το επιχειρηματικό απόρρητο, 2007

Παπανδρέου Πόπη (υπό την επιμέλεια Χαραλαμπάκη Α. και σε συνεργασία Συνεργασία: Γεωργιάδου Μ., Χατζηκωνσταντή Σ.) ΔΙΑΓΡΑΜΜΑΤΑ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ, Γενικό & Ειδικό Μέρος με σχόλια και παρατηρήσεις, Εκδοση 3η 2023, Νομική Βιβλιοθήκη

Ρεβολίδης Ιωάννης, Διεθνής δικαιοδοσία και διαδίκτυο, Κεφάλαιο 6.3.2.3. Ο νομικός χαρακτηρισμός των συμβάσεων «υπολογιστικού νέφους» (cloud computing) 2020

Ρόκας, Αθέμιτος ανταγωνισμός, σελ. 127

Σπυρόπουλος Φ., Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking), 2016, σελ. 180

Τουργέλης Π., Αξιόποινες προσβολές πληροφοριακών συστημάτων και ψηφιακών δεδομένων: συμβολή στην ερμηνεία των άρθρων 292Β, 292Γ, 370Β και 370Ε ΠΚ' (Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ), Σχολή Νομικής 2022

Τσέτουρα Α., Το θεσμικό πλαίσιο της κοινωνικής εργασίας, 2022

Φιλόπουλος Π., Ποινική Προστασία του Απορρήτου-Συστηματική Ερμηνεία Άρθρων 370-371 ΠΚ, 2015

Φράγκος Κ., Online κατ' άρθρο ερμηνεία Ποινικού Κώδικα, άρθ. 370Γ, αρ. 1, Ενημέρωση:10/12/2019, sakkoulas-online

Χαραλαμπάκης Α. σε συνεργασία με Μπουρμά Γ., Οι αλλαγές του νέου ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ Μετά τους Ν 4855/2021, 4871/2021, 4908/2022 και 4947/2022, Ερμηνεία κατ' άρθρο των διατάξεων του Ν 4619/2019 που τροποποιήθηκαν, Έκδοση 2022, Νομική Βιβλιοθήκη

Χαραλαμπάκης Α., "Η έμμεση αυτουργία – Σκέψεις σε βασικά προβλήματα της συμμετοχής στο ελληνικό ποινικό δίκαιο" (ΑΝΤ. Ν. Σάκκουλα Αθήνα- Κομοτηνή 1998)

Χαραλαμπάκης Α., Σύνοψη Ποινικού Δικαίου, Γενικό Μέρος Ι, Το έγκλημα, Π.Ν. Σάκκουλας 2010

Χατζηιωάννου Κ. , Η ποινική αντιμετώπιση των προσβολών ηλεκτρονικών δεδομένων και συστημάτων πληροφοριών: ευρωπαϊκή και εθνική διάσταση, διδακτορική διατριβή 2013, (https://freader.ekt.gr/eadd/index.php?doc=39060&lang=el#p=321),

Χατζηνικολάου Ν., Ποινικό Δίκαιο, Ειδικό Μέρος, Εγκλήματα κατά της ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών, των κοινωφελών εγκαταστέσεων, της λειτουργίας πληροφοριακών συστημάτων, άρθρα 290 – 298, 2017

Ψαρούδα-Μπενάκη Α., Τα αξιολογικά στοιχεία της αντικειμενικής υποστάσεως του εγκλήματος, Αφοί Π. Σάκκουλα 1971

Αρθρογραφία

Γανιάρης Ν., στο περιοδικό Art of Crime, Νοέμβριος 2021, στο σύνδεσμο: (https://theartofcrime.gr/%CF%80%CE%B1%CF%81%CE%AC%CE%BD%CE%BF%CE%BC%CE%B7-%CE%B1%CF%80%CF%8C%CE%BA%CF%84%CE%B7%CF%83%CE%B7-%CF%80%CF%81%CF%8C%CF%83%CE%B2%CE%B1%CF%83%CE%B7%CF%82-%CF%83%CE%B5-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC/#:~:text=%CE%A3%CF%84%CE%BF%20%CE%AC%CF%81%CE%B8%CF%81%CE%BF%20370%CE%92%20%CF%80%CE%B1%CF%81.,%CE%BA%CE%B1%CF%84%CF%8C%CF%87%CE%BF%CF%85%20%CE%AE%20%CE%B1%CF%81%CE%BC%CE%BF%CE%B4%CE%AF%CE%BF%CF%85%20%CF%85%CF%80%CE%B1%CE%BB%CE%BB%CE%AE%CE%BB%CE%BF%CF%85%20%CF%84%CE%BF%CF%85%C2%BB.)
Ιδ. ΝαυτΠειρ 530/2003, ΠοινΧρ 2014, σελ. 75 επ.

Καϊάφα – Γκμπάντι, Παρατηρήσεις στην ΕφΑθ 217/1997, Υπερ 1997, σελ. 850

Καϊάφα-Γκμπάντι, Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, Αρμ 7/2007, σελ. 1068

Κιούπης Δ., Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, Υπερ. 2000, σελ. 970

Κωνσταντινίδης, Η διακεκριμένη παραβίαση απορρήτων στοιχείων (άρθρο 370Β παρ. 2 περ. β' ΠΚ, ΠοινΧρον 1997, σελ. 1216 επ.

ΜονΠρωτΠειρ 4137/2019 (Ειδ.) σε ΤΝΠ QUALEX, και σε ΙΣΟΚΡΑΤΗ

Μπουρμά Γ., Προσπάθειες εννοιολογικού προσδιορισμού της κατοχής ηλεκτρονικών δεδομένων με χαρακτήρα παιδικής πορνογραφίας, ΠοινΔ 2009, σελ. 324.

Νούσκαλης Γεώργιος, Παρατηρήσεις στην ΑΠ (Συμβ) 465/2008, ΤΝΠ QUALEX ΠοινΔικ, 1/2009

Του Ιδίου, Υπερ. 1994, σελ. 1133 σχόλιο επί του Βουλεύματος του Συμβουλίου Πλημμελειοδικών Θεσσαλονίκης υπ' αριθμόν 3204/1993

Του Ιδίου, ΑΠ 121/2003 ΣΤ' Τμ. [Αντιγραφή και χρήση προγραμμάτων Η/Υ]

ΠοινΔικ, 6/2003, σελ. 619 – 620, ΤΝΠ QUALEX ΠλημΚαλαμ 127/2016 ΠΧρ 2016 σελ. 387

Σεφερίδης Η., Ηλεκτρονικά εγκλήματα, ΠραξΛογΠΔ 4/2021.1004 = sakkoulas-online

ΣυμβΑΠ 1294/2007 ΠραξΛογΠΔ 2007 σελ. 333

ΣυμβΕφΑθ 217/1997 Υπερ σελ. 846

ΣυμβΕφΑθ 2949/2003, ΠοινΔικ 2004, σελ. 1110

ΣυμβΠλημΑθ 4742/2004, ΠοινΔικ 2005, σελ. 407

ΣυμβΠλημΑθ 4997/2012 ΠοινΔικ 2013, σελ. 504

ΣυμβΠλημΘεσσ 3204/2003

ΤρΠλημΑθ 2484/2019 ΠοινΔικ, 5/2020, σελ. 461 – 462 (ΤΝΠ QUALEX)

Υπόθεση Van Buren v. United States, 141 S. Ct. 1648 (2021) 'Van Buren v. United States, 141 S. Ct. 1648 | Casetext Search + Citator' <https://casetext.com/case/van-buren-v-united-states-5 > accessed 21 September 2023.

Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών, ΠοινΔικ 2021

Χαλκιαδάκη Βασιλική, Παιδική πορνογραφία στο διαδίκτυο, Η κατοχή υλικού παιδικής πορνογραφίας μέσω ηλεκτρονικού συστήματος υπό το φως της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των παιδιών κατά της γενετήσιας κακοποίησης και εκμετάλλευσης, Τεύχος 19 - Ιούλιος 2011.

Νόμοι

Αιτιολογική Έκθεση Σύμβασης της Βουδαπέστης (Convention on Cybercrime (ETS No. 185) Explanatory Report), https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf

Αιτιολογική Έκθεση του Ν 1805/1988 για το αδίκημα της παράνομης πρόσβασης

Αιτιολογική Έκθεση του Ν. 4919/2019 (https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/k-poinkod-eis-NEO.pdf)

Αιτιολογική Έκθεση του Ν. 4411/2016 Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της

Αιτιολογική του 41ου Τροποποιητικού Νόμου με τον οποίο αναδιατυπώθηκε του 202a γερμΠΚ, Drucksache 16/3656 (https://dserver.bundestag.de/btd/16/036/1603656.pdf)

Ανακοίνωση προς μία Γενική Πολιτική σχετικά με την Καταπολέμηση του Εγκλήματος στον Κυβερνοχώρο, COM(2007) 267, § 1.1.

Άρθρο 16 του Νόμου περί Αθεμίτου Ανταγωνισμού

Άρθρο 2 παρ. 3 Ν. 2121/1993, όπως διαμορφώθηκε ως άνω με το άρθρο 53 παρ. 1 του Ν.4961/2022 (ΦΕΚ Α 146/27.07.2022.)

Άρθρο 22Α Ν 1733/1987 (σχετικά με την προστασία της τεχνογνωσίας και των επιχειρηματικών πληροφοριών που δεν έχουν αποκαλυφθεί -εμπορικό απόρρητο- από την παράνομη απόκτηση, χρήση και αποκάλυψη) μετά το 1 Ν.4605/2019, ΦΕΚ Α 52/1.4.2019 με το σκοπό εναρμόνιση με την Οδηγία (ΕΕ) 2016/943.

ΚΥΑ 56169/2022 (ΦΕΚ Β' 6259/12.12.2022)

Νόμος 5002/2022 "Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών"

Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

Σύμβαση της Βουδαπέστης προσπελάσιμη στον ακόλουθο σύνδεσμο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32013L0040

U.S. Code § 1030 (άρθρο 18 παρ. 2: Απάτη και συναφείς δραστηριότητες σε σχέση με υπολογιστές)

Ξενόγλωσση Βιβλιογραφία

Anmerkung zu LG Wuppertal ZUM 2011, 190, Von Frank Michael Höfinger*, Köln (ZUM 2011, 212, beck-online) Zur Straflosigkeit des sogenannten »Schwarz-Surfens«

Bachmann Michael, 'What Makes Them Click? Applying The Rational Choice Perspective To The Hacking Underground' (2008)

BeckOK StGB/Weidemann, 58. Ed. 1.8.2023, StGB § 202a Rn. 20 (B. Objektiver Tatbestand (Rn. 3-11)- V. Unbefugt (Rn. 11)

BeckOK StGB/Weidemann, 58th Ed. 1 Αυγούστου 2023, StGB § 202a Rn. 12-16.1

Benutzung „Trojanischer Pferde" und anderer Spionageprogramme (MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a)

BGH, 21ης Ιουλίου 2015 - 1 StR 16/15 - Δημιουργία Bitcoin [2015] BGH 1 StR 16/15, 2015 NJW 3463.

BGH, 13 Μαΐου 2020 - 5 StR 614/19 - Παράνομη πρόσβαση σε γραμματοκιβώτια από τον διαχειριστή του συστήματος [2020] BGH 5 StR 614/19, 2020 NStZ-RR 278.

BGH, 27 Ιουλίου 2017 − 1 StR 412/16 (LG Kempten) για την ποινική ευθύνη της παράνομης εξόρυξης Bitcoin με χρήση υπολογιστών τρίτων (*μετάφραση*) (NStZ 2018, 401, beck-online)

BVerfG, Urt. v.27/02/2008, BvR 370/07, 595/07)

Emery A. C., Zero-day responsibility: the benefits of a safe harbor for cybersecurity research , HeinOnline

Ernst S. (επιμέλεια), Hacker, Cracker & Computerviren, Κολωνία: O. Schmidt Verlag, 2004, περιθωριακός αριθμός 393.

Ernst Stefan, 'Το Νέο Ποινικό Δίκαιο Των Υπολογιστών, (*μετάφραση*) NJW 2007 , 2661

Gercke M., Understanding Cybercrime (https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf)

Hassemer Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht 3. Auflage 2019 Rn. 92-102

Hilgendorf E., Grundfalle zum Computerstrafrecht, JuS 1996

Hoffmann Christian, Google INC.., Die Verletzung der Vertraulichkeit informationstechnischer Systemedurch Google Street View (https://www.degruyter.com/document/doi/10.9785/ovs-cr-2010-514/html

Humied Ismail, Common Risks and Challenges in Cybercrime (May 2023) DOI:10.13140/RG.2.2.34392.67840 (file:///C:/Users/User/Downloads/9-21CommonRisksandChallengesinCybercrime.pdf)

Kargl Kindhäuser/Neumann/Paeffgen/Saliger, έκδοση 2023 7, 8

Kindhäuser Urs, *Strafgesetzbuch. Band 3* (5. Auflage, Nomos 2017)

Kindhäuser/Neumann/Paeffgen/Saliger, Strafgesetzbuch, 6. Auflage 2023

Klaas Arne, '"White Hat Hacking" – Αποκάλυψη Τρωτών Σημείων Ασφαλείας Σε Δομές Πληροφορικής Όρια Ποινικής Ευθύνης Για Ηθικές Επιθέσεις Hacking' (*μετάφραση*) [2022] Multimedia und Recht 187. (MMR 2022, 187, beck-online)

Kühne K., Die Entwicklung des Internetstrafrechts, unter besonderer Berücksichtigung der §§ 202a–202c StGB sowie § 303a und § 303b StGB, De Gruyter 2018

Kusnik: Abfangen von Daten - Straftatbestand des § 202b StGB auf dem Prüfstand MMR 2011, 720

Lackner/Kühl/Heger/Heger, 30η έκδοση 2023, StGB § 202a Rn. 1

LG Düsseldorf: DDoS-Attacken als Erpressung und Computersabotage, (MMR 2011, Seite 624, beck-online

MAH Strafverteidigung, § 50 Cybercrime und Datenkriminalität Rn. 44, beck-online

McLaurin, Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service,

MMR 2011, 720, beck-online (και συγκεκριμένα ενότητα 2. Με τίτλο Elektromagnetische Abstrahlung επόμενα

MüKoStGB/Graf, 4η έκδοση 2021, StGB § 202a Rn. 2

MüKoStGB/Wieck-Noodt, 4. Aufl. 2022, StGB § 303b Rn. 6

Müller Daniel, *Der strafrechtliche Schutz der Datenvertraulichkeit vor potentiellen Insiderangriffen* (file:///C:/Users/User/Downloads/s11623-017-0794-z.pdf) accessed

NK-StGB/Kargl, 6. Aufl. 2023, StGB § 202a Rn. 26

NK-StGB/Schild/Kretschmer, 6. Aufl. 2023, StGB § 25 Rn. 29

OLG Frankfurt/M.: Strafbarkeit einer „Online-Demo" (MMR 2006, 547, beck-online)

Pfister, Christa, Hacking. Die Schweizer Hacking-Strafnorm (Art. 143bis StGB) im Vergleich mit den Bestimmungen der Cybercrime Convention, des Rechts der Europaischen Union, des deutschen und des österreichischen Strafrechts, Dissertation der Rechtswissenschaftlichen Fakultat Universitat Zürich

Popp Andreas σε Hilgendorf/Kudlich/Valerius, Handbuch des Strafrechts Bd. 4 (C.F. Müller GmbH, Jan 1, 2019),

Roxin Claus, Täterschaft und Tatherrschaft, Schönke/Schröder, StGB vor § 25 Rn. 57, beck-online

Schönke Adolf and others, Strafgesetzbuch: Kommentar (30., neu bearbeitete Auflage, CH Beck 2019) Σελ. 2970

Schönke/Schröder/Stree/Hecker, 29. Aufl. 2014, StGB § 303b Rn. 1, beck-online

Schreibauer/T.Hessel M., Das 41.Strafrechtsänderungsgesetz, K&R 2007

Schwarzenegger C., Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001 am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Femmeldegeimnisses, σε: Festschrift für Stefan Trechsel zum 65. Geburtstag. Zürich, 2002, σελ. 316. (https://www.zora.uzh.ch/id/eprint/23961/8/Schwarzenegger_FS_Trechsel_2002.pdf)

Sieber Inf Tech 19/20, 53

Valerius, στο: Graf/Jäger/Wittig, WirtschaftsStrR, 2nd ed., § 202 a StGB Rn 26

Διάφορα

CASE OF BUTURUGĂ v. ROMANIA, Η διαδικτυακή βία ως μορφή ενδοοικογενειακής βίας με παραπομπή στην εξής έκθεση: https://en.unesco.org/sites/default/files/genderreport2015final.pdf

Raymond Andrè Hagen ' Tools for Achieving Anonymity on the Internet | LinkedIn'

Shoulder surfing: https://www.techtarget.com/searchsecurity/definition/shoulder-surfing

"Prosecuting Computer Crimes": https://www.justice.gov/criminal/file/442156/download
Smishing (https://www.ibm.com/topics/smishing)

"Botnet" (https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/) accessed 19 September 2023

(DDoS-as-a-service). Βλ. https://encyclopedia.kaspersky.com/glossary/ddos-as-a-service/ (accessed 19 September 2023)

ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92

Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στην οποία αξιολογείται κατά πόσον τα κράτη μέλη έχουν λάβει τα αναγκαία μέτρα προκειμένου να συμμορφωθούν με την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου «Good administration (europa.eu) »