ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών

ΝΟΜΙΚΗ ΣΧΟΛΗ
ΕΝΙΑΙΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΑΤΕΥΘΥΝΣΗ: ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΠΟΙΝΙΚΗ ΔΙΚΟΝΟΜΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2016-2017

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
του ΠΑΝΑΓΙΩΤΑΚΟΠΟΥΛΟΥ ΠΑΝΑΓΙΩΤΗ
Α.Μ.: 7340010916019

ΕΓΚΛΗΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ: ΟΙ ΝΟΜΟΘΕΤΙΚΕΣ ΜΕΤΑΒΟΛΕΣ ΤΟΥ ΝΟΜΟΥ 4411/2016

Επιβλέποντες:
Δ. Κιούπης, Αναπληρωτής Καθηγητής
Χ. Μυλωνόπουλος, Καθηγητής
Γ. Τριανταφύλλου, Επίκουρος Καθηγητής

Αθήνα, Δεκέμβριος 2017

Περίληψη

Με το Ν. 4411/2016 η Ελλάδα κύρωσε την υπ’ αριθμ. 185 Σύβαση του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο», η οποία υπεγράφη στη Βουδαπέστη στις

23.11.2001 (στο εξής «Σύμβαση»), το Πρόσθετο Πρωτόκολλο αυτής καθώς και την Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών (στο εξής «Οδηγία»). Από άποψη ουσιαστικού ποινικού δικαίου ο ως άνω νόμος θεσπίζει και τροποποιεί διατάξεις του Π.Κ. με τις οποίες ποινικοποιούνται συμπεριφορές που στρέφονται κατά των συστημάτων πληροφοριών και των δεδομένων τους, οι οποίες είναι δυνατό να τελούνται με ή χωρίς τη βοήθεια του διαδικτύου.

Η παρούσα διπλωματική εργασία χωρίζεται σε οκτώ Κεφάλαια. Το πρώτο Κεφάλαιο περιλαμβάνει μια συνοπτική εισαγωγή στην οποία περιγράφονται οι δυνατότητες που προσφέρει στους ανθρώπους η χρήση των πληροφοριακών συστημάτων και του διαδικτύου, οι οποίες ωστόσο μπορούν να χρησιμοποιηθούν για την διάπραξη εγκλημάτων και για αυτόν ακριβώς το λόγο θα πρέπει να υπάρχει το απαραίτητο νομικό πλαίσιο. Στο δεύτερο Κεφάλαιο, γίνεται μια προσπάθεια προσδιορισμού της έννοιας του πληροφοριακού εγκλήματος και οριοθέτησή της, σε σχέση με παρεμφερείς έννοιες, με σκοπό να γίνει αντιληπτό ποια κατηγορία πληροφοριακών εγκλημάτων θίγονται στην παρούσα εργασία.

Στο τρίτο Κεφάλαιο, παρατίθενται οι επιμέρους διατάξεις ουσιαστικού ποινικού δικαίου της ως άνω Σύμβασης του Συμβουλίου της Ευρώπης, επί των οποίων γίνεται μια συνοπτική ανάλυση προς τον σκοπό της κατανόησης του περιεχομένου τους. Κατόπιν, στο τέταρτο Κεφάλαιο, παρουσιάζονται τα σχετικά άρθρα της Οδηγίας που ποινικοποιούν τις επιθέσεις κατά συστημάτων πληροφοριών και των δεδομένων τους και αντιπαραβάλλεται το περιεχόμενο των ρυθμίσεών τους με το περιεχόμενο των ρυθμίσεων των αντίστοιχων άρθρων της Σύμβασης.

Στο πέμπτο κεφάλαιο παρουσιάζονται οι διατάξεις ουσιαστικού ποινικού δικαίου που θεσπίστηκαν ή τροποποιήθηκαν με τον Ν. 4411/2016 και οι οποίες προστατεύουν την ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων τους, και ειδικότερα η σχέση τους με τις αντίστοιχες διατάξεις της Σύμβασης και της Οδηγία, οι τρόποι τέλεσής τους καθώς και οι σχέση τους με άλλες σχετικές εθνικές διατάξεις οι οποίες είτε προϋπήρχαν είτε θεσπίστηκαν ή τροποποιήθηκαν επίσης με το Ν. 4411/2016.

Με την παρούσα εργασία δίνεται ιδιαίτερη έμφαση στην πλήρη ανάλυση των ζητημάτων που ανακύπτουν αναφορικά με τη διάταξη του άρθρου 381Α Π.Κ. που ποινικοποιεί την φθορά ηλεκτρονικών δεδομένων, καθώς και στην ανάλυση και τον σχολιασμό των διατάξεων που ποινικοποιούν τις προπαρασκευαστικές πράξεις της παραγωγής, της πώλησης, της προμήθειας, της εισαγωγής, της κατοχής, της διανομή ή της με κάθε άλλο

τρόπο διακίνησης τεχνικών μέσων ή κωδικών με σκοπό την τέλεση την τέλεση εγκλημάτων που στρέφονται κατά των πληροφοριακών συστημάτων και των δεδομένων τους. Οι διατάξεις αυτές οι οποίες θεσπίστηκαν με τον Ν. 4411/2016 αναλύονται στο έκτο και το έβδομο Κεφάλαιο αντίστοιχα.

Τέλος, στο όγδοο Κεφάλαιο της εργασίας κρίθηκε σκόπιμο, αντί επιλόγου, να γίνει ένα συνοπτικό σχόλιο αναφορικά με ζητήματα τα οποία δεν ρυθμίστηκαν ούτε από τη Σύμβασης ούτε από την Οδηγία αλλά ούτε και από το Ν. 4411/2016, καθώς και με τις σχετικές ρυθμίσεις του Γενικού Κανονισμού 2016/679 της Ε.Ε για την Προστασία Δεδομένων και την Οδηγία 2016/1148 της Ε.Ε. για την ασφάλεια των πληροφοριακών συστημάτων.

Abstract

With Law No. 4411/2016 Greece ratified the Council of Europe Convention No. 185 on Cybercrime, signed in Budapest on 23.11.2001 (hereinafter referred to as "the Convention"), its Additional Protocol and Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems (hereinafter referred to as "the Directive"). Regarding substantive criminal law, this Law establishes and amends provisions of the Penal Code that criminalize behaviours that are directed against information systems and their data, which can be carried out with or without the help of the internet.

This diploma thesis is divided into eight Chapters. The first Chapter contains a brief introduction that describes the new abilities that people have with the use of information systems and the internet, which can, however, be used for committing crimes, and exactly that is the reason why there should be the necessary legal framework. In the second Chapter, there is an attempt to define the concept of “information crime” and its relation to similar concepts in order to understand the kind of information crimes that are analysed in this thesis.

The third Chapter sets out the substantive criminal law provisions of the above-mentioned Council of Europe Convention, on which a concise analysis is made for the purpose of understanding their content. Then in Chapter Four, the relevant Articles of the Directive that criminalize attacks against information systems and their data and compare them with the relevant articles of the Convention.

The fifth Chapter presents the provisions of substantive criminal law, that were introduced or amended by Law No. 4411/2016, and which protect the security of information systems and their data, and also discusses their relationship with the corresponding provisions of the Convention and the Directive, how the criminal acts can be committed, and their relationship with other relevant national provisions which either pre-existed or were introduced or amended by Law No. 4411/2016.

This paper focuses on the full analysis of the issues raised in relation to the provision of article 381A of the Penal Code, which criminalizes the act of data interference, and also the analysis of the provisions criminalizing the preparatory acts of possession, production, sale, procurement for use, import, distribution or otherwise making available production of technical means or code in order to committing crimes against information systems and their data. These provisions, which were introduced by Law 4411/2016, are analysed in the sixth and seventh Chapters respectively.

Finally, in the eighth Chapter of this thesis, there is a concise comment on issues that were not regulated neither by the Convention neither by the Directive nor by Law 4411/2016,

and also a comment on the relevant regulations of the General Data Protection Regulation 2016/679 (EU) and the Directive 2016/1148 (EU), for the security of information systems (also known as NIS directive).

Περιεχόμενα

1. Εισαγωγή

Στην εποχή μας, οι ηλεκτρονικοί υπολογιστές διαδραματίζουν ραγδαία όλο και μεγαλύτερο και σπουδαιότερο ρόλο στην καθημερινότητα των ανθρώπων. Το γεγονός αυτό, αρχικώς, οφειλόταν στις διαρκώς αυξανόμενες δυνατότητες των ηλεκτρονικών υπολογιστών αφενός υπολογισμού μαθηματικών λύσεων και αφετέρου επεξεργασίας και αποθήκευσης αρχείων διαφόρων τύπων (λ.χ. εικόνων, εγγράφων κ.λπ.). Οι ως άνω δυνατότητες των ηλεκτρονικών υπολογιστών έχουν ως αποτέλεσμα τον μετριασμό σημαντικών περιορισμών του ανθρώπου (είτε αυτές οφείλονται αποκλειστικά σε αυτόν όπως π.χ. η δυνατότητα υπολογισμού, είτε αυτές οφείλονται στην δυνατότητα επίδρασης του στο περιβάλλον) με αποτέλεσμα την εξοικονόμηση χρόνου και χώρου, ή ακόμα και την άρση ορισμένων περιορισμών που ο άνθρωπος δεν θα ήταν ποτέ σε θέση να επιτύχει βασιζόμενος αποκλειστικά στις δικές του φυσικές ικανότητες ή τις ιδιότητες του φυσικού κόσμου.

Ο ψηφιακός κόσμος, με άλλα λόγια, θα μπορούσε να θεωρηθεί ότι παρέχει στον άνθρωπο υπερδυνάμεις, η δε ραγδαία εξέλιξη της τεχνολογίας σύμφωνα, μάλιστα, τουλάχιστον μέχρι πρότινος, με τον λεγόμενο «νόμο» του Moore[1], έχει ως αποτέλεσμα την σμίκρυνση των υπολογιστών (miniaturization) με παράλληλη αύξηση των δυνατοτήτων τους και τη μείωση του κόστους τους, γεγονότα που συνέβαλαν αποφασιστικά στην μαζικότητα της χρήσης τους.

Το γεγονός, όμως, που αποτέλεσε τομή στην διεύρυνση των δυνατοτήτων των ηλεκτρονικών υπολογιστών και στην μαζική υιοθέτηση της χρήσης τους ήταν η εφεύρεση του κυβερνοχώρου, ο οποίος ουσιαστικά είναι ένα παγκόσμιο δίκτυο ηλεκτρονικών υπολογιστών που τους επιτρέπει να επικοινωνούν μεταξύ τους και να ανταλλάσσουν πληροφορίες σε «πραγματικό χρόνο».

Ωστόσο, όπως παρατηρείται η ραγδαία ανάπτυξη της χρήσης του Διαδικτύου, η ψηφιοποίηση, η σύγκλιση και η εκτεταμένη διασύνδεση των συστημάτων πληροφοριών, παρέχουν σημαντική διευκόλυνση στη διάπραξη ποινικών αδικημάτων διασυνοριακού χαρακτήρα.[2]

---

[1] Ο αριθμός των τρανζίστορ που μπορούν να τοποθετηθούν χωρίς υπερβολικό κόστος σε ένα ολοκληρωμένο κύκλωμα (integrated circuit) διπλασιάζεται περίπου κάθε 18 μήνες

[2] Αιτιολογική Έκθεση στο σχέδιο νόθου «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά

Μάλιστα, η «κυβερνοεγκληματικότητα» («cybercriminality»), δηλαδή η διάπραξη ποινικών αδικημάτων μέσω του Διαδικτύου, συνιστά μια εξαιρετικά σοβαρή απειλή, η οποία στρέφεται όχι μόνο κατά φυσικών ή νομικών προσώπων ιδιωτικού και δημοσίου δικαίου που χρησιμοποιούν το διαδίκτυο, αλλά και κατά της εύρυθμης λειτουργίας των Κρατών (κυβερνοπόλεμος).

συστημάτων πληροφοριών και την αντικατάσταση της απόφασης πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις», σελ.1

2. Εννοιολογικός προσδιορισμός του όρου «πληροφοριακό έγκλημα»

Όπως έχει επισημανθεί, οι έννοιες ηλεκτρονικό έγκλημα, πληροφοριακό έγκλημα, έγκλημα με υπολογιστή, διαδικτυακό έγκλημα χρησιμοποιούνται συχνά αδιάκριτα και περιέχονται σε διεθνή ή εθνικά κείμενα χωρίς να αποσαφηνίζονται επαρκώς.[3]

Γίνεται γενικά δεκτό ότι πληροφοριακό έγκλημα είναι το έγκλημα που τελείται με την αξιοποίηση των δυνατότητων πληροφοριακών συστημάτων όπως λ.χ. ηλεκτρονικών υπολογιστών. Αν και ο ορισμός αυτός έχει επικριθεί ως εξαιρετικά ευρύς, στην πράξη περιέχει αρκετά στοιχεία για την κατανόηση της εν λόγω έννοιας.

Περαιτέρω, ορθά επισημαίνεται ότι οι τρόποι με τους οποίους είναι δυνατό να τελεστεί ένα πληροφοριακό έγκλημα μπορούν να ενταχθούν σε τρείς κατηγορίες.[4] Στην πρώτη κατηγορία, αυτή των λεγόμενων μη γνησίων πληροφοριακών εγκλημάτων, περιλαμβάνονται τα «παραδοσιακά» εγκλήματα τα οποία τελούνται με την βοήθεια πληροφοριακών συστημάτων (λ.χ. συκοφαντική δυσφήμιση μέσω του διαδικτύου). Στην δεύτερη κατηγορία, αυτή των λεγόμενων «γνήσιων» πληροφοριακών εγκλημάτων εντάσσονται τα εγκλήματα τα οποία στρέφονται κατά πληροφοριακών συστημάτων και δεν ανταποκρίνονται ακριβώς σε κανένα «παραδοσιακού» τύπου έγκλημα. Τέλος, η τρίτη κατηγορία είναι αυτή των εγκλημάτων του Κυβερνοχώρου ή κυβερνοεγκλημάτων τα οποία διαπράττονται σε περιβάλλον διαδικτύου.[5]

Η υπ' αριθ. 185 Σύμβαση του Συμβουλίου της Ευρώπης «για το έγκλημά στον Κυβερνοχώρο» διακρίνει την τελευταία αυτή κατηγορία δηλαδή των κυβερνοεγκλημάτων σε τέσσερις επιμέρους υποκατηγορίες. Η πρώτη αφορά τα εγκλήματα τα οποία στρέφονται κατά της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους, η οποία περιλαμβάνει ειδικότερα την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητας

---

[3] Δ. Κιούπη, Οι διατάξεις του Ποινικού Κώδικα για το διαδικτυακό έγκλημα, 3ο Πανελλήνιο Συνέδριο της Ένωσης Ελλήνων Νομικών, e-ΘΕΜΙΣ, Το Δίκαιο στην ψηφιακή εποχή, σελ. 151

[4] Δ. Κιούπη, Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ευρωπαϊκή Ένωση, Δικηγορικός Σύλλογος Πειραιά – Ένωση Ελλήνων Ποινικολόγων – Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, 2010, σελ. 192

[5] Ωστόσο, κατά το γράφοντα τα κυβερνοεγκλήματα είναι δυνατό να θεωρηθούν ως υποκατηγορία των άλλων δύο κατηγοριών πληροφοριακών εγκλημάτων, δηλαδή τα γνήσια και τα μη γνήσια πληροφοριακά εγκλήματα να διακρίνονται σε περιπτώσεις που διαπράχθηκαν με τη βοήθεια του διαδικτύου και περιπτώσεις που δεν διαπράχθηκαν συμπεριλαμβανομένων στην τελευταία περίπτωση και των περιπτώσεων (αν υπάρχουν) που η τέλεση με τη χρήση του διαδικτύου είναι εξ' ορισμού αδύνατη . Η διάκριση αυτή, μάλιστα, είναι σύμφωνη και με την γενική παραδοχή ότι το έγκλημα στον Κυβερνοχώρο είναι μια ειδικότερη μορφή του πληροφοριακού εγκλήματος, βλ. σχετικά και Ι. Αγγελή, Διαδίκτυο (Internet) και Ποινικό Δίκαιο, ΠοινΧρ 2000, σελ. 675 επ.

τους. Η δεύτερη υποκατηγορία αφορά τα σχετικά με υπολογιστές εγκλήματα, τα εγκλήματα δηλαδή που τελούνται με την βοήθεια των υπολογιστών και στρέφονται κατά «παραδοσιακών» έννομων αγαθών. Η τρίτη υποκατηγορία αφορά συμπεριφορές που η τέλεση του διευκολύνεται μέσω διαδικτύου και ποινικοποιούνται λόγω του περιεχόμενο τους όπως λ.χ. το έγκλημα της διακίνησης παιδικής πορνογραφίας. Τέλος, μια ακόμα διάκριση που γίνεται από τη Σύμβαση είναι αναφορικά με εγκλήματα σχετικά με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων.

Αντίθετα, η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών κάνει λόγο, όπως φαίνεται και από τον τίτλο της, μόνο για επιθέσεις κατά συστημάτων πληροφοριών. Στην κατηγορία αυτή η Οδηγία εντάσσει αποκλειστικά περιπτώσεις εγκλημάτων που στρέφονται μόνο κατά των συστημάτων πληροφοριών (λ.χ. το έγκλημα της παράνομης πρόσβασης σε πληροφοριακά συστήματα). Τα εγκλήματα αυτά μπορούν να τελεστούν είτε με είτε χωρίς τη χρήση του διαδικτύου.

Στην παρούσα εργασία εξετάζονται τα ζητήματα που αφορούν γνήσια πληροφοριακά εγκλήματα δηλαδή εγκλήματα που στρέφονται είτε μόνο κατά της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους (λ.χ. το έγκλημα της παράνομης πρόσβασης σε πληροφοριακά συστήματα), είτε από κοινού και κατά άλλων «παραδοσιακών» εννόμων αγαθών (λ.χ. απάτη με υπολογιστή), τα οποία είναι δυνατό να τελεστούν και χωρίς την χρήση του διαδικτύου, πλην όμως, συνήθως, τελούνται μέσω αυτού.

3. Διεθνές νομικό πλαίσιο - Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο

3.1. Εισαγωγή

Το Συμβούλιο της Ευρώπης, ήδη από το 1997, άρχισε να ασχολείται με το ζήτημα της αντιμετώπισης της εγκληματικότητας στον Κυβερνοχώρο. Το Συμβούλιο παρά το γεγονός ότι η ανάπτυξη τόσο του ίδιου του Κυβερνοχώρου, όσο και συνακόλουθα της εγκληματικότητας στο πλαίσιό του, βρισκόταν ακόμα σε πολύ πρώιμο στάδιο αντελήφθη τη σοβαρότητα του ζητήματος και την ανάγκη θέσπισης κανόνων δικαίου, με σκοπό την αντιμετώπιση της εγκληματικότητας στο Διαδίκτυο.

Για το σκοπό αυτό ανέλαβε την πρωτοβουλία για τη συγκρότηση μιας ειδικής επιτροπής εμπειρογνωμόνων. Αποτέλεσμα όλης αυτής της προσπάθειας ήταν η κατάρτιση της υπ' αριθμ. 185 Σύβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο», η οποία υπεγράφη στη Βουδαπέστη στις 23.11.2001.[6]

Ο γενικός σκοπός της Σύμβασης για την αποτελεσματική αντιμετώπιση των εγκλημάτων στον Κυβερνοχώρο δύναται να αναλυθεί σε τρείς επιμέρους στόχους – τρόπους επίτευξής του:

i. Στην εναρμόνιση των εθνικών νομοθεσιών σε ό,τι αφορά στην ποινικοποίηση συγκεκριμένων συμπεριφορών και στην υποχρέωση επιβολής των κατάλληλων ποινικών κυρώσεων για τον κολασμό τους.

ii. Στη συμπλήρωση των δικονομικών διατάξεων, που ισχύουν στα Συμβαλλόμενα Μέρη, προκειμένου να βελτιωθεί η δυνατότητα των Δικαστικών και Αστυνομικών Αρχών να διεξάγουν τις έρευνές τους «σε πραγματικό χρόνο» («in real time»), ώστε να συλλέγουν τα απαραίτητα αποδεικτικά στοιχεία, στα γεωγραφικά όρια της εκάστοτε εθνικής επικράτειας, πριν τα στοιχεία αυτά χαθούν, και

---

[6] Η Σύμβαση υπεγράφη από 30 χώρες τότε, 26 μέλη του Ευρωπαϊκού Συμβουλίου (Αλβανία, Αρμενία, Αυστρία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρος, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιταλία, Μολδαβία, Ολλανδία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Ισπανία, Σουηδία, Ελβετία, Π.Γ.Δ.Μ., Ουκρανία και Ηνωμένο Βασίλειο) και 4 χώρες μη μέλη (Καναδάς, Ιαπωνία, Ν. Αφρική και ΗΠΑ) που συμμετείχαν, όμως, στο σχεδιασμό της. Αξίζει να σημειωθεί ότι μέχρι σήμερα όλα τα μέλη του Συμβουλίου της Ευρώπης έχουν υπογράψει τη Σύμβαση, ενώ δεν την έχουν κυρώσει μόνο η Ιρλανδία, το Σαν Μαρίνο και η Σουηδία. Αναφορικά με χώρες μη μέλη του Συμβουλίου της Ευρώπης η Σύμβαση κυρώθηκε από την Αυστραλία, τον Καναδά, τη Χιλή, την Κόστα Ρίκα, τη Δομινικανή Δημοκρατία, το Ισραήλ, την Ιαπωνία, τον Μαυρίκιο, τον Παναμά, την Σενεγάλη, την Σρι Λάνκα, την Τόνγκα και τις ΗΠΑ, ενώ μόνο η Ν. Αφρική ενώ έχει υπογράψει τη Σύμβαση δεν την έχει κυρώσει μέχρι στιγμής.
Επίσημη πηγή: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

iii. Στην προσαρμογή των κανόνων που περιέχονται στη Σύμβασης του Συμβουλίου της Ευρώπης, σχετικά με την έκδοση και τη δικαστική συνδρομή. Αξίζει να σημειωθεί ότι πέραν των παραδοσιακών τρόπων επικοινωνίας, η Σύμβαση προβλέπει τη δημιουργία ενός δικτύου σημείων επαφής τα οποία θα λειτουργούν, σε εικοσιτετράωρη βάση, όλες τις ημέρες της εβδομάδας.

Τέλος, αξίζει να τονισθεί, ότι, όπως επισημαίνεται και στην Αιτιολογική Έκθεση του σχεδίου νόμου για την κύρωση της Σύμβασης, η τελευταία *«δεν έχει ως μόνο αντικείμενο την αντιμετώπιση της εγκληματικότητας στον Κυβερνοχώρο υπό στενή έννοια (γνήσια εγκλήματα του διαδικτύου), αφού εφαρμόζεται και σε ποινικά αδικήματα η καταστολή των οποίων προϋποθέτει τη συλλογή αποδείξεων ηλεκτρονικής φύσης (εγκλήματα δια του διαδικτύου)»*.[7] Με άλλα λόγια η Σύμβαση επιβάλει την ποινικοποίηση τόσο συμπεριφορών που στρέφονται κατά των συστημάτων πληροφοριών και των δεδομένων τους (γνήσια πληροφοριακά εγκλήματα) όσο και συμπεριφορές που προσβάλλουν διάφορα άλλα έννομα αγαθά και τελούνται μέσω ηλεκτρονικών υπολογιστών ή συμπεριφορές που μπορούν να αναχθούν σε εγκλήματα λόγω του περιεχομένου που διακινείται από τα συστήματα πληροφοριών (content related crimes όπως λ.χ. η διακίνηση πορνογραφίας ανηλίκων).

3.2. Τα επιμέρους άρθρα της Σύμβασης

3.2.1. Κεφάλαιο Ι – Ορολογία

Η Σύμβαση, στο πρώτο άρθρο του πρώτου Κεφαλαίου της, περιλαμβάνει συγκεκριμένους ορισμούς για τον προσδιορισμό ορισμένων εννοιών, τεχνικής φύσης, από τις οποίες όμως συναρτάται η εφαρμογή της. Ειδικότερα στο άρθρο αυτό δίνονται οι εξής ορισμοί:

i. «Σύστημα υπολογιστή»: ο όρος αυτός υποδηλώνει μια συσκευή ή ένα σύνολο διασυνδεδεμένων ή σχετιζόμενων συσκευών, μια η περισσότερες από τις οποίες πραγματοποιεί αυτόματη επεξεργασία δεδομένων βάσει ενός προγράμματος.

Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης «*ένα σύστημα υπολογιστή κατά την Σύμβαση είναι μια συσκευή που αποτελείται από υλισμικό (hardware) και λογισμικό (software)*

[7] Αιτιολογική Έκθεση στο σχέδιο νόμου «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημά στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις», σελ.2.

που αναπτύχθηκε για αυτόματη επεξεργασία των ψηφιακών δεδομένων το οποίο μπορεί να περιλαμβάνει μέσα εισαγωγής, εξαγωγής, και αποθήκευσης και το οποίο μπορεί να είναι αυτοτελές ή συνδεδεμένο σε ένα δίκτυο με άλλες παρόμοιες συσκευές». Περαιτέρω δίνονται οι εξής συμπληρωματικοί ορισμοί: α) «Αυτόματη» σημαίνει χωρίς άμεση ανθρώπινη παρέμβαση, β) «Επεξεργασία δεδομένων» σημαίνει ότι τα δεδομένα στο σύστημα υπολογιστή υφίστανται επεξεργασία εκτελώντας ένα πρόγραμμα υπολογιστή, γ) «Πρόγραμμα υπολογιστή» είναι ένα σύνολο από οδηγίες που μπορεί να εκτελεστούν από τον υπολογιστή για να επιτύχει το επιθυμητό αποτέλεσμα. Ένας υπολογιστής μπορεί να τρέξει διαφορετικά προγράμματα. Ένα σύστημα υπολογιστή συνήθως αποτελείται από διαφορετικές συσκευές, που να διαχωρίζονται ανάμεσα στον επεξεργαστή ή την κεντρική μονάδα επεξεργασίας, και στα περιφερειακά. «Περιφερειακή» ονομάζουμε την συσκευή που πραγματοποιεί συγκεκριμένες και ορισμένες λειτουργίες σε αλληλεπίδραση με την μονάδα επεξεργασίας, όπως ο εκτυπωτής, η οθόνη, η μονάδα ανάγνωσης/εγγραφής CD ή άλλη μονάδα αποθήκευσης, δ) «Δίκτυο» είναι μια διασύνδεση ανάμεσα σε δύο ή περισσότερα συστήματα υπολογιστή. Οι συνδέσεις μπορεί να είναι ενσύρματες (π.χ. σύρμα ή καλώδιο), ασύρματες (π.χ. ραδιοκύματα, υπέρυθρες ή δορυφορικές) ή και τα δύο. Ένα δίκτυο μπορεί να είναι γεωγραφικά περιορισμένο σε μια μικρή περιοχή (τοπικά δίκτυα) ή μπορεί να εξαπλώνεται σε μια μεγάλη περιοχή (δίκτυα ευρείας περιοχής), και τα οποία δίκτυα μπορεί να είναι με τη σειρά τους διασυνδεδεμένα. Το Διαδίκτυο είναι ένα παγκόσμιο δίκτυο αποτελούμενο από πολλά διασυνδεδεμένα δίκτυα, τα οποία χρησιμοποιούν κοινά πρωτόκολλα επικοινωνίας. Υπάρχουν και άλλοι τύποι δικτυών, συνδεδεμένων ή όχι με το Διαδίκτυο, που είναι δυνατόν να μεταδίδουν δεδομένα υπολογιστή μεταξύ υπολογιστικών συστημάτων. Τα συστήματα υπολογιστών μπορεί να είναι συνδεδεμένα στο δίκτυο ως τερματικοί σταθμοί ή ως μέσα υποβοήθησης της επικοινωνίας σε ένα δίκτυο. Αυτό που είναι ουσιώδες είναι ότι τα δεδομένα ανταλλάσσονται μέσω του δικτύου.[8]

ii. «Δεδομένα υπολογιστών»: με τον όρο αυτό εννοείται η αναπαράσταση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη για να υποστούν επεξεργασία σε ένα σύστημα υπολογιστή, περιλαμβανομένου και ενός προγράμματος κατάλληλου για να προκαλέσει την εκτέλεση μιας λειτουργίας από ένα σύστημα υπολογιστή.

[8] Σκέψεις 23 – 24 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

Ο ορισμός των δεδομένων υπολογιστή βασίζεται στον ορισμό ISO[9] των δεδομένων, ο οποίος περιλαμβάνει τον όρο «κατάλληλα για επεξεργασία». Αυτό σημαίνει πως τα δεδομένα αποθηκεύονται με τέτοιο τρόπο, ώστε να είναι δυνατόν να υποστούν άμεση επεξεργασία από το σύστημα πληροφοριών.[10]

iii. «Πάροχος υπηρεσιών» σημαίνει:

α) κάθε δημόσιος ή ιδιωτικός φορέας που παρέχει στους χρήστες των υπηρεσιών του τη δυνατότητα να επικοινωνούν μέσω ενός συστήματος υπολογιστή, και

β) κάθε άλλος φορέας που επεξεργάζεται ή αποθηκεύει δεδομένα υπολογιστών είτε για λογαριασμό αυτής της υπηρεσίας επικοινωνίας είτε των χρηστών αυτής της υπηρεσίας.

iv. «Δεδομένα κίνησης»: είναι τα δεδομένα υπολογιστών που σχετίζονται με μια επικοινωνία μέσω ενός συστήματος υπολογιστή, δημιουργούμενα από ένα σύστημα υπολογιστή που αποτελούσε τμήμα της αλυσίδας επικοινωνίας, τα οποία καταδεικνύουν την προέλευση, τον προορισμό, το δρομολόγιο, το χρόνο, την ημερομηνία, το μέγεθος, την διάρκεια ή τον τύπο της υφιστάμενης υπηρεσίας επικοινωνίας.

3.2.2. Κεφάλαιο ΙΙ Τμήμα 1 – Μέτρα ουσιαστικού ποινικού δικαίου που πρέπει να ληφθούν σε εθνικό επίπεδό

Στο πρώτο τμήμα του δεύτερου Κεφαλαίου της Σύμβασης, οριοθετείται η έννοια της «κυβερνοεγκληματικότητας» και προσδιορίζονται τα συγκεκριμένα αδικήματα, κατά τρόπο που να διασφαλίζεται η ιδιαιτερότητα κάθε εσωτερικής έννομης τάξης, με την υιοθέτηση, δηλαδή, όπως χαρακτηριστικά αναφέρεται στην Αιτιολογική Έκθεση της Σύμβασης, «εύκαμπτων» εννοιών και την παροχή στα Συμβαλλόμενα Μέρη δυνατότητας διατύπωσης επιφυλάξεων στην εφαρμογή ορισμένων διατάξεων.

Περαιτέρω, όπως ήδη εκτέθηκε, η Σύμβαση προβαίνει σε κατηγοριοποίηση των εγκλημάτων στον Κυβερνοχώρο, τοποθετώντας τα στις εξής ομάδες: i. εγκλήματα που στρέφονται κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων υπολογιστών, ii. εγκλήματα σχετικά με υπολογιστές, iii. εγκλήματα σχετικά με το περιεχόμενο, iv. εγκλήματα σχετικά με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων, και v. εξαρτημένη ευθύνη και κυρώσεις.

---

[9] ISO είναι συντομογραφία για το Διεθνή Οργανισμό Πιστοποίηση (International Organization for Standardization).

[10] Σκέψη 25 της Αιτιολογικής Έκθεσης τη Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο»

Επισημαίνεται ότι, σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης, όλες οι συμπεριφορές που περιγράφονται στην Σύμβαση πρέπει να ποινικοποιούνται όταν τελούνται «χωρίς δικαίωμα». Οι περιγραφόμενες συμπεριφορές δεν είναι, δηλαδή, εκ προοιμίου απαγορευμένες, αλλά μπορούν να είναι νόμιμές ή δικαιολογημένες με βάση τα συγκεκριμένα πραγματικά περιστατικά. Περαιτέρω δε, αφήνεται στην αρμοδιότητα των Συμβαλλομένων Μερών να προσδιορίσουν πότε δύναται να υπάρχει δικαίωμα τέλεσης των πράξεων αυτών. Ωστόσο κατά την Συντακτική Επιτροπή της Σύμβασης νόμιμες και συνήθεις ενέργειες απαραίτητες για τον σχεδιασμό δικτύων, ή νόμιμες και συνήθεις εργασίες ή εμπορικές πρακτικές, δεν θα πρέπει να ποινικοποιούνται.[11]

Ειδικότερα, οι ως άνω ομάδες περιλαμβάνουν τα εξής:

i. Εγκλήματα που στρέφονται κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων υπολογιστών

Η ασφάλεια (security), δηλαδή, η προστασία ενός συστήματος υπολογιστών και των δεδομένων του από απώλεια ή ζημιά, πρέπει να ικανοποιεί την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων. Εμπιστευτικότητα (confidentiality) των δεδομένων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος. Ακεραιότητα (integrity) των δεδομένων είναι η ιδιότητα των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή των να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας. Τέλος, διαθεσιμότητα (availability) των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος.[12]

Κάτω από το γενικό αυτό τίτλο των εγκλημάτων που στρέφονται κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων υπολογιστών περιλαμβάνονται τα άρθρα 2 έως και 6 της Σύμβασης. Με τα άρθρα αυτά επιβάλλεται ειδικότερα στα Συμβαλλόμενα Μέρη η υποχρέωση να χαρακτηρίσουν ως αξιόποινες, την παράνομη πρόσβαση (άρθρο 2), την υποκλοπή (άρθρο 3), την παρεμβολή σε δεδομένα (άρθρο 4) και τις παρεμβολές σε συστήματα (άρθρο 5). Τέλος ποινικοποιούνται αυτοτελώς οι προπαρασκευαστικές πράξεις της δημιουργίας και της διακίνησης μέσων για την τέλεση των προαναφερθέντων εγκλημάτων (άρθρο 6).

[11] Σκέψη 38 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[12] Ι. Αγγελής, Διαδίκτυο και Ποινικό Δίκαιο-Έγκλημα στον Κυβερνοχώρο, Ποινικά Χρονικά, τόμος 2000 σελ. 675 επ.

Συγκεκριμένα τα ως άνω άρθρα ποινικοποιούν τις ως άνω εγκληματικές συμπεριφορές ως εξής:

Α. Παράνομη πρόσβαση (Illegal Access)

«Άρθρο 2 – Παράνομη Πρόσβαση

Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η άνευ δικαιώματος πρόσβαση στο σύνολο ή σε μέρος ενός συστήματος υπολογιστή, όταν αυτή διαπράττεται από πρόθεση. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση διάπραξης του εγκλήματος την παραβίαση μέτρων ασφαλείας, με την πρόθεση να αποκτηθούν δεδομένα υπολογιστή ή με άλλη αθέμιτη πρόθεση ή σε σχέση με ένα σύστημα υπολογιστή που είναι συνδεδεμένο με άλλο σύστημα υπολογιστή.»

Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης προστατευόμενο έννομο αγαθό του εν λόγω εγκλήματος είναι η ασφάλεια του ηλεκτρονικού συστήματος, δηλαδή η πρόληψη της πρόσβασης από μη εξουσιοδοτημένα άτομα. Αποτελεί, με άλλα λόγια, το άρθρο αυτό, το «ηλεκτρονικό αντίστοιχο στον Κυβερνοχώρο» της διατάραξης οικιακής ειρήνης (άρθρο 334 Π.Κ.).[13] Όπως, δηλαδή, ο δικαιούχος της κατοικίας έχει το δικαίωμα να ορίζει ποιος μπορεί να εισέρχεται και να παραμένει σ' αυτήν, έτσι και ο «δικαιούχος» του ηλεκτρονικού υπολογιστή δικαιούται να ορίζει ποιος θα τον χρησιμοποιεί και ποιος θα έχει πρόσβαση σ' αυτόν.[14]

Περαιτέρω, επίσης, σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης, το έγκλημα της παράνομης πρόσβασης αποτελεί το βασικό έγκλημα που στρέφεται κατά της ασφάλειας των συστημάτων υπολογιστών και των δεδομένων τους (δηλαδή της εμπιστευτικότητας της ακεραιότητας και της διαθεσιμότητας τους) και καταλαμβάνει συμπεριφορές όπως το «hacking»[15] και το «cracking»[16]. Τέτοιου είδους εισβολές είναι δυνατό είτε να επιτρέψουν την πρόσβαση σε απόρρητα δεδομένα (συμπεριλαμβανομένων κωδικών και πληροφοριών του συστήματος) και μυστικά ή στη χρήση του συστήματος χωρίς πληρωμή, είτε ακόμα και

[13] Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999, σελ. 125

[14] Δ.Π. Αγγελόπουλος, Κυβερνοχώρος - Το διεθνές «γίγνεσθαι» στο ελληνικό «είναι», ΕΛ.Ε.Σ.ΜΕ.

[15] Ο όρος «hacking» συχνά αποδίδεται στα Ελληνικά ως «εισβολή».

[16] Ο όρος «cracking» αποτελεί ειδικότερη έκφανση του «hacking» όταν το τελευταίο τελείται με σκοπό την τέλεση κάποιου άλλου εγκλήματος που είτε στρέφεται κατά της ασφάλειας (δηλ. της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας) των πληροφοριακών συστημάτων και των δεδομένων τους, είτε τελείται μέσω υπολογιστή ήτοι η απάτη και η πλαστογραφία με υπολογιστή.

να ενθαρρύνουν τους δράστες να τελέσουν πιο επικίνδυνες μορφές εγκλημάτων σχετικών με του υπολογιστές όπως η πλαστογραφία ή η απάτη μέσω υπολογιστή.[17]

Η έννοια της «πρόσβασης» περιλαμβάνει την είσοδο σε ένα άλλο σύστημα υπολογιστή το οποίο είναι συνδεδεμένο μέσω δημοσίου δικτύου τηλεπικοινωνιών, ή σε ένα σύστημα υπολογιστή που βρίσκεται στο ίδιο δίκτυο λ.χ. σε ένα τοπικό δίκτυο (LAN)[18] ή σε ένα ενδοδίκτυο (intranet)[19] ενός οργανισμού. Η μέθοδος επικοινωνίας (λ.χ. ασύρματα, εξ αποστάσεως ή μέσω καλωδίων) είναι άνευ σημασίας.

Ο δικαιολογητικός λόγος της ποινικοποιήσεως της παράνομης πρόσβασης συνίσταται στο γεγονός ότι, ο κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος, τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσεως του υπολογιστή ή του συστήματος υπολογιστή. Ο αποτελεσματικότερος τρόπος προστασίας από τη χωρίς δικαίωμα πρόσβαση είναι η εφαρμογή μέτρων ασφαλείς όπως η χρήση συνθηματικού ή βιομετρικής ταυτοποίησης του χρήστη (λ.χ. με τη χρήση δακτυλικού αποτυπώματος). Ωστόσο κρίθηκε ότι μια αποτελεσματική αντιμετώπιση τέτοιων συμπεριφορών οφείλει να περιλαμβάνει και ποινικές κυρώσεις με σκοπό την αποτροπή τέτοιων φαινομένων.

Β. Αθέμιτη παγίδευση-Υποκλοπή (Illegal interception)

«Άρθρο 3 – Υποκλοπή

Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η υποκλοπή δια τεχνικών μέσων μη δημόσιων διαβιβάσεων δεδομένων υπολογιστή από και προς ή εντός ενός συστήματος υπολογιστή,

[17] Σκέψη 44 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[18] Local Area Network (LAN) ή στα ελληνικά Τοπικό δίκτυο, είναι ένα σύνολο ενσύρματα (με προδιαγραφές του φυσικού επιπέδου Ethernet) ή ασύρματα (WLAN) συνδεδεμένων πληροφοριακών συστημάτων. Η πιο συχνή χρήση τοπικών δικτύων είναι σε εγκαταστάσεις γραφείων ή επιχειρήσεων, με σκοπό την κοινή χρήση των περιφερειακών μέσων και την άμεση ανταλλαγή δεδομένων, συνήθως, μέσω ενός κοινού κεντρικού server (διακομιστή), στον οποίο όλοι οι υπολογιστές είναι συνδεδεμένοι, αλλά δεν αποκαλείται να συνδέονται και όλοι οι υπολογιστές μεταξύ τους άμεσα.

[19] Intranet ή στα ελληνικά ενδοδίκτυο είναι ένα ιδιωτικό δίκτυο πληροφοριακών συστημάτων το οποίο χρησιμοποιεί τις τεχνολογίες του διαδικτύου. Είναι με άλλα λόγια ένα διαδίκτυο ή ορθότερα μια μικρογραφία του, η πρόσβαση στο οποίο δεν είναι ελεύθερη σε όλους άλλα μόνο σε συγκεκριμένους χρήστες.

περιλαμβανομένων και των ηλεκτρομαγνητικών εκπομπών[20] *από ένα σύστημα υπολογιστή στο οποίο ευρίσκονται αυτά τα δεδομένα υπολογιστών, όταν αυτή διαπράττεται από πρόθεση. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση της διάπραξης του εγκλήματος την αθέμιτη πρόθεση, ή την επίτευξη σύνδεσης ενός συστήματος υπολογιστή με ένα άλλο σύστημα υπολογιστή».*

Η διάταξη αυτή, ουσιαστικά, επιβάλει στα συμβαλλόμενα μέρη τη διεύρυνση της «παραδοσιακής» έννοιας της υποκλοπής που αφορά την παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας ώστε να καταλαμβάνει κάθε μορφή διακίνησης ηλεκτρονικών δεδομένων, είτε αυτή γίνεται τηλεφωνικώς, είτε μεσώ fax ή e-mail, είτε με μεταφορά αρχείων. Κατά συνέπεια προστατευόμενο έννομο αγαθό είναι «το δικαίωμα στην ιδιωτική ζωή και της ασφάλειας των τηλεπικοινωνιών στον Κυβερνοχώρο».

Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης[21] η έννοια της υποκλοπής περιλαμβάνει συμπεριφορές όπως η ακρόαση (listening), η παρακολούθηση (monitoring), η επιτήρηση (surveillence) και η καταγραφή (recording). Επιπρόσθετα τονίζεται ότι το έγκλημα της υποκλοπής αφορά σε «μη δημόσιες»[22] εκπομπές ηλεκτρονικών δεδομένων. Τέλος επισημαίνεται ότι η επικοινωνία υπό τη μορφή εκπομπών ηλεκτρονικών δεδομένων είναι δυνατό να λάβει χώρα α) εντός ενός μίας μονάδας ηλεκτρονικού υπολογιστή λ.χ. από την κεντρική μονάδα επεξεργασίας (CPU) προς την οθόνη ή τον εκτυπωτή, β) μεταξύ δύο συστημάτων υπολογιστών τα οποία ανήκουν στο ίδιο άτομο, γ) μεταξύ δύο υπολογιστών που επικοινωνούν μεταξύ τους ή δ) μεταξύ ενός υπολογιστή και ενός προσώπου λ.χ. μέσω του πληκτρολογίου.

Γ. Επέμβαση σε δεδομένα (Data interference)

«Άρθρο 4 – Παρεμβολές σε δεδομένα

1. Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η άνευ δικαιώματος βλάβη, διαγραφή, φθορά, αλλοίωση ή καταστολή δεδομένων υπολογιστών όταν αυτή διαπράττεται από πρόθεση.

---

[20] Στην Αιτιολογική Έκθεση της Σύμβασης ορίζεται ότι οι ηλεκτρομαγνητικές εκπομπές που πιθανό να εκπέμπονται κατά τη λειτουργία του υπολογιστή δεν μπορούν να θεωρηθούν ως «δεδομένα» σύμφωνα με τον ορισμό του άρθρου 1 της Σύμβασης αλλά είναι δυνατό από τέτοιες εκπομπές να επανασυνθεθούν δεδομένα.

[21] Σκέψη 53 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[22] Ο όρος «μη δημόσιες» αφορά τη φύση των εκπομπών και όχι τη φύση των δεδομένων. Τα δεδομένα δύναται να είναι ελεύθερα διαθέσιμα αλλά τα μέρη να επιθυμούν να επικοινωνούν μεταξύ τους εμπιστευτικά.

2. Ένα Συμβαλλόμενο Μέρος μπορεί να διατηρεί το δικαίωμα να θέσει ως προϋπόθεση ύπαρξης εγκλήματος για την συμπεριφορά που περιγράφεται στην παρ. 1 την πρόκληση σοβαρής ζημίας».

Σκοπός του άρθρου αυτού είναι να προστατεύσει τα δεδομένα (data) και τα προγράμματα των ηλεκτρονικών υπολογιστών ως «υλικές υποστάσεις» από οποιαδήποτε επέμβαση (παρεμβολή), που γίνεται με πρόθεση πρόκλησης ζημιάς σ' αυτά. Προστατευόμενο έννομο αγαθό είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

Περαιτέρω στην Αιτιολογική Έκθεση της Σύμβασης[23] δίνεται μια επιγραμματική επεξήγηση των εννοιών που περιγράφονται στην πρώτη παράγραφο του άρθρου ως συμπεριφορές που πρέπει να ποινικοποιηθούν. Συγκεκριμένα, α) οι έννοιες «βλάβη» και «φθορά» είναι αλληλοκαλυπτόμενες και αφορούν αρνητική αλλοίωση της ακεραιότητας ή του πληροφοριακού περιεχομένου των δεδομένων και των προγραμμάτων, β) η έννοια της «διαγραφής» των δεδομένων είναι αντίστοιχη με την καταστροφή ενός αντικειμένου υπό την νομική του έννοια δηλαδή που έχει υλική υπόσταση, γ) η έννοια της «καταστολής» δεδομένων καταλαμβάνει κάθε συμπεριφορά που αποκλείει ή σταματά την διαθεσιμότητα των δεδομένων στο πρόσωπο που έχει πρόσβαση στον υπολογιστή ή τον φορέα δεδομένων στον οποίο ήταν αποθηκευμένα και τέλος δ) η έννοια της «αλλοίωσης» αφορά την τροποποίηση δεδομένων που προϋπήρχαν και συνεπώς καταλαμβάνει περιπτώσεις εισαγωγής κακόβουλου κώδικα «όπως είναι οι «ιοί» («viruses»)[24], τα «σκουλήκια» («warms»)[25] και οι «Δούρειοι Ίπποι» («Trojan Horses»).»[26] Θα πρέπει να γίνει δεκτό ότι τα

[23] Σκέψη 61 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[24] Οι ιοί είναι ένα είδος κακόβουλου προγράμματος, το οποίο όταν αναπαράγεται εισάγοντας τον κώδικά του σε άλλα προγράμματα ή δεδομένα που είναι ήδη εγκατεστημένα στο πληροφοριακό σύστημα το οποίο έχει προσβάλει. Εισάγοντας τον κώδικά του αλλοιώνει τα δεδομένα αυτά ή ακόμα και τα καταστρέφει.

[25] Τα «σκουλήκια» εν αντιθέσει με τους ιούς αυτοαναπαράγονται εντός ενός πληροφοριακού συστήματος χωρίς να προσβάλουν άλλα προγράμματα. Για αυτό το λόγο μπορούν και από μόνα τους να υπερφορτώσουν ένα πληροφοριακό σύστημα ή συνηθέστερα ένα τηλεπικοινωνιακό δίκτυο. Επίσης πολύ συχνά χρησιμοποιούνται για την τέλεση κατανεμημένων επιθέσεων άρνησης παροχής υπηρεσιών κατά άλλων πληροφοριακών συστημάτων δημιουργώντας botnets.

[26] προγράμματα αυτά παρουσιάζονται στον χρήστη (λ.χ. σε μία ιστοσελίδα ή σε μια ηλεκτρονική επιστολή) ότι επιτελούν ένα συγκεκριμένο σκοπό ή ότι έχουν ένα συγκεκριμένο περιεχόμενο, με αποτέλεσμα ο χρήστης να επιθυμεί την εγκατάστασή του και να τα εγκαθιστά το πληροφοριακό σύστημα. Πλην όμως, δεν επιτελούν (μόνο) αυτό το σκοπό του χρήστη για τον οποίο τα εγκατέστησε αλλά περιέχουν (και) κακόβουλο κώδικα. Ο

παραδείγματα αυτά πλην αυτού του ιού είναι άστοχα καθώς οι δύο άλλες περιπτώσεις που αναφέρονται δεν αλλοιώνουν υπάρχοντα δεδομένα του πληροφοριακού συστήματος αλλά εισάγουν νέα δεδομένα. Η εισαγωγή δεδομένων δεν τυποποιείται ως τρόπος τέλεσης του συγκεκριμένου εγκλήματος όμως το γεγονός ότι τυποποποείται ως τρόπος τέλεσης άλλων εγκλημάτων όπως της πρόσβασης ή της παρεμβολής σε σύστημα προδίδει ότι τα δεδομένα ενός πληροφοριακού συστήματος νοούνται αυτοτελώς και όχι ως σύνολο και επομένως για να τελείται το έγκλημα της επέμβασης σε δεδομένα με αλλοίωση τους θα πρέπει να αλλοιώνονται συγκεκριμένα δεδομένα και όχι το σύνολο των δεδομένων ως σύνολο καθώς σε αυτή την περίπτωση έχουν απλή εισαγωγή δεδομένων μπορεί να τιμωρηθεί με άλλες διατάξεις.

Περαιτέρω, με βάση την Αιτιολογική Έκθεση της Σύμβασης[27], οι ως άνω συμπεριφορές είναι ποινικά κολάσιμες μόνο όταν τελούνται «χωρίς δικαίωμα».). Ειδικότερα, «με δικαίωμα» και ως εκ τούτου δεν ποινικοποιούνται από το ως άνω άρθρο τελούνται *«[σ]υνήθεις συμπεριφορές αναγκαίες για τον σχεδιασμό δικτύων ή συνήθεις διαδικαστικές ή εμπορικές πρακτικές, όπως για παράδειγμα για την δοκιμή ή την προστασία της ασφάλειας ενός υπολογιστικού συστήματος οι οποίες γίνονται με την άδεια του ιδιοκτήτη ή του χρήστη, ή ο επαναπρογραμματισμός του λειτουργικού συστήματος (operating system) ενός υπολογιστή που λαμβάνει χώρα όταν ο χρήστης ενός συστήματος απόκτα νέο λογισμικό (λ.χ. λογισμικό που περιέχει πρόγραμμα που επιτρέπει την πρόσβαση στο διαδίκτυο απενεργοποιώντας παρόμοια προγράμματα που είχαν εγκατασταθεί προηγουμένως […] [η] τροποποίηση δεδομένων κίνησης για το σκοπό της διενέργειας ανώνυμων επικοινωνιών (λ.χ. συστημάτων anonymous remailer[28]) ή η τροποποίηση δεδομένων για το σκοπό της διασφάλισης των επικοινωνιών (λ.χ. κρυπτογράφηση), θα πρέπει κατ' αρχήν να θεωρείται νόμιμη προστασία του απορρήτου και ως εκ τούτου θα πρέπει να εκλαμβάνεται ότι γίνεται «με δικαίωμα»».* Ωστόσο, αφήνεται η διακριτική ευχέρεια στα Συμβαλλόμενα Μέλη να ποινικοποιούν ορισμένες καταχρηστικές συμπεριφορές αναφορικά με ανώνυμες επικοινωνίες όπως φέρ' ειπείν η αλλοίωση των

κακόβουλος αυτός κώδικας μπορεί να είναι ένας «ιός» («virus») ο οποίος επεμβαίνει στα ήδη υπάρχοντα δεδομένα του πληροφοριακού συστήματος ή ένα «σκουλήκι» («warm») το οποίο δεν επεμβαίνει στα ήδη υπάρχοντα δεδομένα του πληροφοριακού συστήματος αλλά δημιουργεί νέα.

[27] Σκέψη 62 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[28] Anonymous remailer είναι ένας διακομιστής (Server) ο οποίος λαμβάνει μηνύματα με ενσωματωμένες οδηγίες αναφορικά με το που να τα στείλει στη συνέχεια, και τα προωθεί χωρίς να αποκαλύπτει από που προήλθαν αρχικώς.

πληροφοριών του packet header δηλαδή των στοιχείων της διεύθυνσης IP[29] με σκοπό την απόκρυψη της ταυτότητας του δράστη για την τέλεση εγκλήματος.[30]

Τέλος, αξίζει να επισημανθεί, ότι η Οδηγία με την δεύτερη παράγραφο του άρθρου 4 δίνει την δυνατότητα στα Συμβαλλόμενα Μέρη να μην ποινικοποιήσουν συμπεριφορές που συνιστούν φθορά ηλεκτρονικών δεδομένων μόνο αν αυτές δεν έχουν ως αποτέλεσμα την πρόκληση σοβαρής ζημίας. Ωστόσο, εναπόκειται στους εθνικούς νομοθέτες να ορίζουν τι συνιστά σοβαρή ζημία.

Δ. Επέμβαση σε σύστημα (System Interference)

«Άρθρο 5 – Παρεμβολές σε συστήματα

Κάθε Συμβαλλόμενο Μέρος λαμβάνει 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 καταστολή δεδομένων υπολογιστή όταν αυτή διαπράττεται από πρόθεση».

Η ως άνω διάταξη, η οποία συχνά αναφέρεται ως δολιοφθορά ηλεκτρονικού υπολογιστή («computer sabotage»), έχει ως σκοπό την ποινικοποίηση της εσκεμμένης παρακώλυσης της νόμιμης λειτουργίας συστημάτων υπολογιστών, συμπεριλαμβανομένων και των υπηρεσιών τηλεπικοινωνιών, που γίνεται με τη χρήση ή των επηρεασμό ηλεκτρονικών δεδομένων.[31].

Η παρακώλυση, κατά το άρθρο αυτό, θα πρέπει να είναι «σοβαρή» για να είναι ποινικά κολάσιμη. Η Σύμβαση αφήνει στα συμβαλλόμενα μέρη το περιθώριο να καθορίσουν τα ίδια στην εσωτερική έννομη τάξη τους κριτήρια για το πότε πληρούται αυτή η προϋπόθεση. Ωστόσο οι συντάκτες της Σύμβασης εκλάμβαναν, σύμφωνα με την Αιτιολογική Έκθεση, ως «σοβαρή» παρακώλυση της λειτουργίας ενός συστήματος υπολογιστή, την αποστολή δεδομένων σε ένα συγκεκριμένο σύστημα, υπό τέτοια μορφή, μέγεθος ή συχνότητας που να επηρεάζει σημαντικά και καθοριστικά την δυνατότητα του ιδιοκτήτη ή του χρήστη να χρησιμοποιεί το σύστημα ή να επικοινωνεί με άλλα συστήματα (λ.χ. μέσω προγραμμάτων που δημιουργούν επιθέσεις άρνησης υπηρεσιών (DoS attacks), κακόβουλους κώδικες, όπως ιούς που αποτρέπουν οι επιβραδύνουν σημαντικά τη λειτουργία ενός συστήματος, ή

[29] Η διεύθυνση IP είναι η «προσωπική» διεύθυνση που έχει κάθε πληροφοριακό σύστημα που είναι συνδεδεμένο στο διαδίκτυο και με την οποία αναγνωρίζεται κατά την αποστολή και τη λήψη δεδομένων.

[30] Σκέψη 62 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[31] Σκέψη 65 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

προγράμματα που στέλνουν τεράστιες ποσότητες e-mail σε ένα λήπτη με σκοπό να εμποδίσουν την δυνατότητα επικοινωνίας του συστήματος).

Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης, περιπτώσεις που οι πράξεις παρεμπόδισης τελούνται για το σκοπό του ελέγχου της ασφάλειας ενός συστήματος υπολογιστή ή για την προστασία του, με την άδεια του ιδιοκτήτη ή του νόμιμου χρήστη, ή η αναβάθμιση ενός λειτουργικού συστήματος όταν ο χρήστης ή ο διαχειριστής ενός συστήματος εγκαθιστά καινούριο λογισμικό που περιλαμβάνει νέα προγράμματα, απενεργοποιεί όμως παρόμοια προγράμματα που ήταν ήδη εγκατεστημένα.[32]

Τέλος, το προστατευόμενο έννομο αγαθό στο άρθρο αυτό είναι, σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης,[33] το δικαίωμα του χρήστη να έχει μια «κανονική» λειτουργία του υπολογιστή του. Μια τέτοια συμπεριφορά στο παρελθόν μπορούσε να τιμωρηθεί μόνο ως φθορά υλικών μερών υπολογιστή κάτι που δεν επέδιδε κατά κανένα τρόπο την απαξία της επίδρασης στην επεξεργασία των δεδομένων.[34]

Ε. Κακή χρήση συσκευών (Misuse of devises)

«Άρθρο 6 – Κακή χρήση συσκευών

1. Κάθε Συμβαλλόμενο Μέρος λαμβάνει 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. Παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή άλλως διάθεση:

i. μια συσκευής, περιλαμβανομένου του προγράμματος υπολογιστή, σχεδιασμένης ή προσαρμοσμένης πρωτίστως 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,

ii. ενός συνθηματικού ή κωδικού πρόσβασης, ή άλλου παρεμφερούς δεδομένου, με την χρήση του οποίου είναι δυνατό να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός συστήματος υπολογιστή,

με πρόθεση να χρησιμοποιηθεί για τον σκοπό της διάπραξης κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5, και

[32] Σκέψη 68 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[33] Σκέψη 67 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

[34] Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1075.

β. Κατοχή ενός αντικειμένου από τα αναφερόμενα στις παραγράφους α.i και α.ii 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.

2. Το παρόν άρθρο δεν πρέπει να ερμηνευθεί ότι δημιουργεί ποινική ευθύνη σε περίπτωση που η παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή άλλως διάθεση ή κατοχή όπως περιγράφεται στην παράγραφο 1 του παρόντος άρθρου δεν γίνεται με σκοπό την διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα Άρθρα 2 έως 5 της παρούσης Σύμβασης, όπως π.χ. για την πραγματοποίηση επιτρεπτών δοκιμών ή για την προστασία ενός συστήματος υπολογιστή.

3. Κάθε Συμβαλλόμενο Μέρος μπορεί να διατηρήσει το δικαίωμα να μην εφαρμόσει την παράγραφο 1 του παρόντος άρθρου υπό τον όρο ότι η επιφύλαξη αυτή δεν αφορά στην πώληση, στην διανομή ή άλλως στην διάθεση των αντικειμένων που περιγράφονται στην παράγραφο 1 α.ii του παρόντος.»

Η διάταξη αυτή ποινικοποιεί αυτοτελώς τις προπαρασκευαστικές ενέργειες παραγωγής και διακίνησης συσκευών ή δεδομένων πρόσβασης που έχουν ως σκοπό την τέλεση των εγκλημάτων που στρέφονται κατά της της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων υπολογιστών.

Συγκεκριμένα, το άρθρο αυτό απαγορεύει τις πράξεις α) τόσο της κατασκευής, της κατοχής όσο και της διανομής ή της διάθεσης προγραμμάτων υπολογιστών και άλλα παρεμφερούς φύσης μέσα, που καθιστούν δυνατή τη διάπραξη ποινικών αδικημάτων, β) όσο και της διακίνησης συνθηματικών λέξεων («passwords») ή κωδικών πρόσβασης. Σημειωτέον δε ότι, με το άρθρο αυτό, δεν επιβάλλεται στα Συμβαλλόμενα Μέρη οποιαδήποτε απαγόρευση νόμιμων ενεργειών, όπως είναι η δημιουργία μέσων για την καταπολέμηση των ιών ή προγραμμάτων ασφάλειας των συστημάτων πληροφορικής.

Ωστόσο, αξίζει να επισημανθεί ότι, σύμφωνα με την παρ. 3 του άρθρου αυτού επιβάλλεται στα Κράτη Μέλη η ποινικοποίηση μόνο συμπεριφορών πώλησης ή με κάθε τρόπος διάθεσης συνθηματικών ή κωδικών πρόσβασης σε πληροφοριακά συστήματα ή παρεμφερών στοιχείων και όχι όλων των προβλεπόμενων στο άρθρο συμπεριφορών. Οι λοιπές αυτές συμπεριφορές δεν επιβάλλεται να ποινικοποιηθούν αλλά εναπόκειται στην διακριτική ευχέρεια των εθνικών νομοθετών αν θα τις ποινικοποιήσουν.[35]

[35] Όπως χαρακτηριστικά παρατηρεί η Γκμπάντι, *«εδώ αναγνωρίζει κανείς μια ζυγισμένη στάση του Συμβουλίου η οποία αξιολογώντας την εξαιρετική ευρύτητα του αξιοποίνου στο πεδίο των προπαρασκευαστικών πράξεων*

Περαιτέρω, αναφορικά με το δικαιολογητικό λόγο της θέσπισης του εν λόγω άρθρου, αυτός συνίσταται στο γεγονός ότι η τέλεση των βασικών εγκλημάτων των προπαρασκευαστικών πράξεων η οποία συχνά απαιτεί την κατοχή τεχνικών μέσων, συνιστά σημαντικό κίνητρο για την απόκτηση τους σε βαθμό που δημιουργείται ένα είδος μαύρης αγοράς για την παραγωγής και τη διακίνησή τους.

Τέλος, σημαντικό ζήτημα που απασχόλησε τη συντακτική επιτροπή της Σύμβασης[36] ήταν το κατά πόσο η συσκευή (ή το πρόγραμμα υπολογιστή) θα πρέπει να είναι σχεδιασμένη αποκλειστικά ή συγκεκριμένα για την διάπραξη εγκλημάτων, και ως εκ τούτου αν αποκλείονται από το πεδίο εφαρμογής του νόμου συσκευές διπλής χρήσης (dual use). Η άποψη αυτή κρίθηκε ως εξαιρετικά στενή και η υιοθέτηση της θα μπορούσε να έχει ως συνέπεια ανυπέρβλητα αποδεικτικά εμπόδια τα οποία ουσιαστικά θα καθιστούσαν την διάταξη αδρανή και μη εφαρμόσιμη πλην ελαχίστων περιπτώσεων. Η αντίθετη άποψη, κατά την οποία η διάταξη θα έπρεπε να καταλαμβάνει συμπεριφορές που αφορούν όλες τις συσκευές, ακόμα και αν παράγονται ή διανέμονται νόμιμα, απορρίφθηκε επίσης, λόγω του υπερβολικού εύρους της. Στην τελευταία αυτή περίπτωση, μόνο το υποκειμενικό στοιχείο του δόλου της τέλεσης εγκλήματος με υπολογιστή θα ήταν καθοριστικό για την επιβολή ποινής, κάτι το οποίο δεν υιοθετήθηκε, όπως επισημαίνεται, ούτε αναφορικά με την παραχάραξη νομισμάτων. Ως εκ τούτων, ως μέση λύση προκρίθηκε οι συσκευές να είναι αντικειμενικά σχεδιασμένες ή προσαρμοσμένες πρωτίστως με σκοπό την τέλεση εγκλημάτων, ρύθμιση η οποία συνήθως δεν θα καταλαμβάνει περιπτώσεις συσκευών διπλής χρήσης.

ii. Εγκλήματα σχετικά με υπολογιστές

Με το άρθρο 7 και το άρθρο 8 προβλέπεται η υποχρέωση των Συμβαλλόμενων Μερών να καταστήσουν αξιόποινες την πλαστογραφία και την απάτη μέσω υπολογιστή, αντιστοίχως.

Συγκεκριμένα τα ως άνω άρθρα ορίζουν τα εξής:

επιλέγει την δυνατότητα περιορισμού του μόνο σε πράξεις διακίνησης των αναμφισβήτητα επικίνδυνων μέσων τέλεσης δηλ. μέσων που μπορούν πραγματικά από τη φύση τους, από τον εκ κατασκευής λειτουργικό προορισμό τους, να εξασφαλίζουν πρόσβαση στα συστήματα πληροφοριών ή σε μέρος αυτών», βλ. Μ. Καϊάφα – Γκμπάντι, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 489 επ.

[36] Σκέψη 73 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

Α. Πλαστογραφία με υπολογιστή

«Άρθρο 7 – Πλαστογραφία σχετική με υπολογιστές

Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η από πρόθεση και άνευ δικαιώματος εισαγωγή, αλλοίωση, διαγραφή ή καταστολή δεδομένων υπολογιστή, που έχει ως αποτέλεσμα την παραγωγή μη αυθεντικών δεδομένων με σκοπό να θεωρηθούν αυτά αυθεντικά ή να γίνουν ενέργειες με βάση αυτά ωσάν να είναι αυθεντικά για νόμιμους σκοπούς, ασχέτως του εάν αυτά τα δεδομένα είναι ή όχι άμεσα αναγνώσιμα ή αντιληπτά. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεσή θεμελίωσης ποινικής ευθύνης την ύπαρξης πρόθεσης εξαπάτησης ή παρόμοια αθέμιτης πρόθεσης».

Σκοπός του άρθρου αυτού είναι να διευρύνει την έννοια της «παραδοσιακής» πλαστογραφίας, ώστε να καταλαμβάνει και περιπτώσεις που διαπράττεται με ηλεκτρονικά μέσα. Το προστατευόμενο έννομο αγαθό είναι το ίδιο με αυτό του άρθρου 216 Π.Κ. (σε συνδ. με το άρθρο 13 περ. γ', όπως αυτό προστέθηκε με το άρθρο 2 Ν 1805/88), δηλαδή η ασφάλεια, αξιοπιστία, πίστη και εγκυρότητα των ηλεκτρονικών δεδομένων, των οποίων η χρήση έχει έννομες συνέπειες. Η ελληνική έννομη τάξη, συνεπώς, είναι συμμορφωμένη με την υποχρέωση αυτή που επιβάλλεται με το εν λόγω άρθρο της Σύμβασης.

Β. Απάτη με υπολογιστή

«Άρθρο 8 – Απάτη σχετική με υπολογιστές

Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας δια της

α. εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή,

β. παρέμβασης στην λειτουργία ενός συστήματος υπολογιστή

με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο».

Η Ελλάδα είναι επίσης συμμορφωμένη και με την απαίτηση του εν λόγω άρθρου της Σύμβασης καθώς ήδη με το Ν. 1805/1988 εισήχθη στον Π.Κ. η διάταξη του άρθρου 386Α που ποινικοποιεί την απάτη με υπολογιστή, στο μέτρο ωστόσο που αυτή δεν τελείται με τη χρήση «χωρίς δικαίωμα» ορθών στοιχείων.

iii. Εγκλήματα σχετικά με το περιεχόμενο – παιδική πορνογραφία

Με το άρθρο 9 επιβάλλεται στα Συμβαλλόμενα Μέρη η υποχρέωση να καταστήσουν αξιόποινες συμπεριφορές που σχετίζονται με την παιδική πορνογραφία. Το πεδίο εφαρμογής της τελευταίας αυτής διάταξης είναι ιδιαιτέρως ευρύ, δεδομένου ότι με αυτή καλύπτεται η

απαγόρευση της παραγωγής, διάδοσης και της απλής κατοχής υλικού παιδικής πορνογραφίας.

Στην ελληνική έννομη τάξη το έγκλημα της παραγωγής, κατοχής και με κάθε τρόπο διάδοσης πορνογραφικού υλικού με ανηλίκους τυποποιείται στο άρθρο 348Α Π.Κ όπως αυτό τροποποιήθηκε με το άρθρο 8 του Ν. 4267/2014.

Συγκεκριμένα το ως άνω άρθρο έχει ως ακολούθως:

«Άρθρο 9 – Εγκλήματα σχετικά με την παιδική πορνογραφία

1. Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο οι ακόλουθες συμπεριφορές όταν διαπράττονται από πρόθεση και άνευ δικαιώματος:

α. παραγωγή παιδικής πορνογραφίας με σκοπό τη διανομή της μέσω ενός συστήματος υπολογιστή,

β. προσφορά ή διάθεση παιδικής πορνογραφίας μέσω ενός συστήματος ηλεκτρονικού υπολογιστή,

γ. διανομή ή μετάδοση παιδικής πορνογραφίας μέσω ενός συστήματος ηλεκτρονικού υπολογιστή,

δ. προμήθεια παιδικής πορνογραφίας μέσω ενός συστήματος υπολογιστή για ιδία χρήση ή για άλλο πρόσωπο.

ε. Κατοχή παιδικής πορνογραφία σε ένα σύστημα υπολογιστή ή σε ένα μέσο αποθήκευσης δεδομένων υπολογιστή.

2. Για τους σκοπούς της παραγράφου 1 ανωτέρω, ο όρος «παιδική πορνογραφία» περιλαμβάνει πορνογραφικό υλικό που απεικονίζει οπτικά:

α. ένα ανήλικο να εμπλέκεται σε σαφώς σεξουαλική συμπεριφορά,

β. ένα πρόσωπο που φαίνεται ότι είναι ανήλικο να συμμετέχει σε σαφώς σεξουαλική συμπεριφορά,

γ. ρεαλιστικές εικόνες που απεικονίζουν ένα ανήλικο να εμπλέκεται σε σαφώς σεξουαλική συμπεριφορά.

3. Για τους σκοπούς της παραγράφου 2 ανωτέρω, ο όρος «ανήλικος» περιλαμβάνει όλα τα πρόσωπα κάτω των 18 ετών. Ένα Συμβαλλόμενο Μέρος μπορεί, παρά ταύτα να ορίσει χαμηλότερο όριο ηλικίας το οποίο δεν μπορεί να είναι κάτω των 16 ετών.

4. Κάθε Συμβαλλόμενο Μέρος μπορεί να διατηρεί το δικαίωμα να μην εφαρμόσει εν όλω ή εν μέρει τις παραγράφους 1, υποπαράγραφος δ και ε και 2 και τις υποπαραγράφους β και γ.»

iv. Εγκλήματα σχετικά με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων

Με τη διάταξη του άρθρου 10 αντιμετωπίζονται εγκλήματα σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας, εφόσον αυτά διαπράττονται για εμπορικούς σκοπούς, αποβλέπουν δηλαδή στην επίτευξη κέρδους

Συγκεκριμένα το ως άνω άρθρο έχει προβλέπει τα εξής:

«Άρθρο 10 – Εγκλήματα σχετικά με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησία και συγγενικών δικαιωμάτων

1.Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που απαιτούνται για να ποινικοποιηθεί στο εσωτερικό δίκαιο του η παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας (copyright) όπως αυτά ορίζονται στο δίκαιο του Συμβαλλομένου Μέρους, σε εκτέλεση των υποχρεώσεων που έχει αναλάβει από την Πράξη του Παρισίου της 24 Ιουλίου 1971 που αναθεώρησε την Σύμβαση της Βέρνης για την Προστασία των Λογοτεχνικών και Καλλιτεχνικών Έργων (Bren Convention for the Protection of Literary and Artistic Works), την Συμφωνία για τις Εμπορικές πτυχές των Δικαιωμάτων Διανοητικής Ιδιοκτησίας (the Agreement on Trade-Related Aspects of Intellectual Property Rights) και τη Συνθήκη του Παγκόσμιου Οργανισμού Διανοητικής Ιδιοκτησίας WIPO για την πνευματική ιδιοκτησία (the WIPO Copyright Treaty), με εξαίρεση τα ηθικά δικαιώματα πνευματικής ιδιοκτησίας που παρέχονται από αυτές τις συμβάσεις, στην περίπτωση που αυτές οι πράξεις διαπράττονται από πρόθεση, σε εμπορική κλίμακα και με την χρήση ενός συστήματος υπολογιστή.

2. Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που απαιτούνται για να ποινικοποιηθεί στο εσωτερικό δίκαιο του η παραβίαση των συγγενικών δικαιωμάτων, όπως αυτά ορίζονται στο δίκαιο αυτού του Συμβαλλομένου Μέρους, σε εκτέλεση των υποχρεώσεων που έχει αναλάβει από τη Σύμβαση για την Προστασία των Ερμηνευτών ή Εκτελεστών Καλλιτεχνών, των Παραγωγών Φωτογραφικών και Ραδιοτηλεοπτικών Οργανισμών (Σύμβαση Ρώμης) (the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations – Rome Convention), την Συμφωνία για τις Εμπορικές Πτυχές των Δικαιωμάτων Διανοητικής Ιδιοκτησίας (The Agreement on Trade-Related Aspects of Intellectual Property Rights) και την Σύμβαση για τις Ερμηνείες / Εκτελέσεις και τα Φωνογραφήματα (the WIPO Performance and Phonograms Treaty), με εξαίρεση τα ηθικά δικαιώματα που παρέχονται από αυτές τις συμβάσεις, όταν αυτές οι πράξεις διαπράττονται από πρόθεση, σε εμπορικής κλίμακα και με την χρήση ενός συστήματος υπολογιστή.

3. Ένα Συμβαλλόμενο Μέρος μπορεί να διατηρεί το δικαίωμα να μην προβεί σε ποινικοποίηση σύμφωνα με τις παραγράφους 1 και 2 του παρόντος άρθρου σε περιορισμένες περιπτώσεις υπό τον όρο ότι διαθέτει άλλα αποτελεσματικά, προς τούτο, ένδικα βοηθήματα και ότι αυτή η επιφύλαξη δεν μειώνει τις διεθνείς υποχρεώσεις του Συμβαλλομένου Μέρους, όπως αυτές αναφέρονται στα διεθνή νομικά κείμενα που αναφέρονται στις παραγράφους 1 και 2 του παρόντος άρθρου.»

v. Εξαρτημένη ευθύνη και κυρώσεις

Οι διατάξεις των άρθρων 11, 12 και 13 της Σύβασης ρυθμίζουν ζητήματα ευθύνης και ποινικών κυρώσεων, με τη θέσπιση ορισμένων γενικής φύσης αρχών που επαναλαμβάνουν, κατά βάση, τις κλασσικές ρήτρες που περιέχουν οι Ευρωπαϊκές Συμβάσεις, που αφορούν σε θέματα ποινικού δικαίου. Πέραν της ποινικής ευθύνης των φυσικών προσώπων, προβλέπεται ακόμη η επιβολή κυρώσεων και σε βάρος νομικών προσώπων, οι οποίες μμπορεί να είναι ποινικής, διοικητικής ή αστικής φύσης.

Η Σύμβαση δεν περιέχει ειδικές ρυθμίσεις για την ποινική ευθύνη των παρόχων υπηρεσιών Διαδικτύου, σχετικά με το περιεχόμενο των μηνυμάτων που στέλνονται από τους χρήστες του Διαδικτύου ή τους συνδρομητές τους. Οι πάροχοι υπηρεσιών Διαδικτύου διέπονται σε ό,τι αφορά τις αξιόποινες πράξεις που τελούνται από τους υπαλλήλους τους για λογαριασμό τους, από τις κείμενες διατάξεις. Ειδικότερα, σε ό,τι αφορά στα Συμβαλλόμενα Μέρη που είναι ταυτόχρονα Κράτη-Μέλη (ΚΜ) της Ευρωπαϊκής Ένωσης (ΕΕ), διέπονται από τις διατάξεις της Οδηγίας 2000/31/ΕΚ σχετικά με το ηλεκτρονικό εμπόριο και από τις θεμελιώδεις αρχές της ποινικής ευθύνης που θεσπίζονται από την ποινική νομοθεσία εκάστου Κράτους.

Συγκεκριμένα τα ως άνω άρθρα προβλέπουν τα εξής:

«Άρθρο 11 – Απόπειρα και συμμετοχή

1. Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό δίκαιο του η συνδρομή ή εξώθηση στην διάπραξη οποιουδήποτε εκ των εγκλημάτων που ποινικοποιούνται σύμφωνα με τα άρθρα 2 έως 10 της παρούσας σύμβασης , όταν αυτά διαπράττονται από πρόθεση

2. Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό δίκαιο του η απόπειρα διάπραξης οιουδήποτε εκ των εγκλημάτων που ποινικοποιούνται σύμφωνα με τα άρθρα 3 έως 5, 7, 8 και 9.1α και γ της παρούσης Σύμβασης όταν η απόπειρα αυτή γίνεται με πρόθεση.

3. Κάθε Συμβαλλόμενο Μέρος μπορεί να διατηρεί το δικαίωμα να μην εφαρμόσει εν όλω ή εν μέρει την παράγραφο 2 του παρόντος άρθρου.»

*«**Άρθρο 12 – Ευθύνη Νομικών Προσώπων***

1. 1.Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να εξασφαλίσει ότι θα θεμελιούται ποινική ευθύνη των νομικών προσώπων για ποινικά εγκλήματα που ποινικοποιούνται σύμφωνα με την παρούσα Σύμβαση όταν αυτά διαπράττονται προς όφελος των νομικών προσώπων από ένα φυσικό πρόσωπο που ενεργεί είτε ατομικώς ή ως μέλος ενός οργάνου του νομικού προσώπου και έχει ιθύνουσα θέση εντός αυτού του νομικού προσώπου, δυνάμει:

- *εξουσιοδότησης να εκπροσωπεί το νομικό πρόσωπο ή*
- *εξουσίας να λαμβάνει αποφάσεις για λογαριασμό του νομικού προσώπου, ή*
- *εξουσίας να ασκεί έλεγχο εντός του νομικού προσώπου*

2. Πέραν των περιπτώσεων που έχουν ήδη προβλεφθεί στην παράγραφο 1 του παρόντος άρθρου, κάθε Συμβαλλόμενο Μέρος λαμβάνει τα αναγκαία μέτρα για να θεμελιώνεται ευθύνη ενός νομικού προσώπου, όταν η έλλειψη επίβλεψης ή ελέγχου από ένα φυσικό πρόσωπο όπως αναφέρεται στην παράγραφο 1, κατέστησε δυνατή τη διάπραξη ενός ποινικού αδικήματος που ποινικοποιείται από την παρούσα Σύμβαση, προς όφελος του νομικού προσώπου από ένα φυσικό πρόσωπο που ενεργεί υπό τον έλεγχό του.

3. Τηρουμένων των νομικών αρχών των Συμβαλλομένων Μερών, η ευθύνη ενός νομικού προσώπου μπορεί να είναι ποινική, αστική ή διοικητική.

4. Η εν λόγω ευθύνη δεν αποκλείει την θεμελίωση ποινικής ευθύνης των φυσικών προσώπων που διέπραξαν το αδίκημα.»

*«**Άρθρο 13 – Κυρώσεις και μέτρα***

Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που απαιτούνται για να εξασφαλίσει ότι τα ποινικά αδικήματα που καθιερώνονται σύμφωνα με τα άρθρα 2 έως 11 τιμωρούνται με αποτελεσματικές, αναλογικές, αποτρεπτικές ποινικές ή μη κυρώσεις ή μέτρα, περιλαμβανομένων των χρηματικών κυρώσεων.»

4. Ευρωπαϊκό νομικό πλαίσιο - Η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση[37] της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου

4.1. Εισαγωγή

Όπως παρατηρείται στο προοίμιο της ίδιας της Οδηγίας, *«[η] κοινωνία εξαρτάται σε υψηλό και συνεχώς αυξανόμενο βαθμό από αυτά [δηλ. τα πληροφοριακά συστήματα] […] [η] ομαλή λειτουργία και η ασφάλειά τους είναι ζωτικής σημασίας για την ανάπτυξη της εσωτερικής αγοράς και μιας ανταγωνιστικής και καινοτόμου οικονομίας εντός της Ευρωπαϊκής Ένωσης […] [ο]ι επιθέσεις κατά των συστημάτων πληροφοριών, συνδεόμενες ή μη με τη δράση του οργανωμένου εγκλήματος ή τρομοκρατικών οργανώσεων, συνιστούν συνεχώς αυξανόμενη απειλή, τόσο εντός της Ευρωπαϊκής Ένωσης όσο και παγκοσμίως […] [ο]ι ανησυχίες εντείνονται για το ενδεχόμενο τρομοκρατικών επιθέσεων ή επιθέσεων με πολιτικά κίνητρα κατά των συστημάτων πληροφοριών, που αποτελούν μέρος των υποδομών ζωτικής σημασίας των κρατών μελών της Ένωσης […] [ο]λα αυτά συνιστούν απειλή για την ασφάλεια της κοινωνίας της πληροφορίας, αλλά και για την εγκαθίδρυση στην Ευρωπαϊκή Ένωση ενός ενιαίου χώρου ελευθερίας, ασφάλειας και δικαιοσύνης.»*[38]

Δεδομένου ότι, η ίδια η Ευρωπαϊκή Ένωση δεν αποτελεί συμβαλλόμενο μέρος της Σύμβασης του Συμβουλίου για το Κυβερνοέγκλημα, καθώς και του ότι, παρά το γεγονός, ότι όλα μεν τα Κράτη Μέλη της την είχαν υπογράψει, δεν την είχαν, όμως, κυρώσει όλα, η αναγκαία αντιμετώπιση των ως άνω ζητημάτων σε ενωσιακό επίπεδο έγινε την 12η Αυγούστου 2013, όποτε και εξεδόθη η υπ' αριθ. 2013/40/ΕΕ Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της μη δεσμευτικής και ανεπαρκούς απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.[39] Ωστόσο, η Σύμβαση του Συμβουλίου της Ευρώπης για το «έγκλημα στο

---

[37] Σύμφωνα με την παρ. (34) του προοιμίου της Οδηγίας *«σκοπός της παρούσας οδηγίας είναι η τροποποίηση και επέκταση των διατάξεων της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, της 24ης Φεβρουάριου 2005, για τις επιθέσεις κατά των συστημάτων πληροφοριών ... [ε]πειδή οι τροποποιήσεις που πρέπει να επέλθουν είναι ουσιαστικές ως προς τον αριθμό και τη φύση τους, η απόφασης-πλαισίου 2005/222/ΔΕΥ θα πρέπει, για λογούς σαφήνειας, να αντικατασταθεί στο σύνολό της σε σχέση με τα Κράτη Μέλη που συμμετέχουν στην έκδοση της παρούσας Οδηγίας.»* (σελ. 218/11).

[38] Σκέψεις 2-3 του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

[39] Με την απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου δεν ποινικοποιούνταν ούτε η παράνομη υποκλοπή δεδομένων ούτε η παραγωγή και διάθεση εργαλείων για την διάπραξη ηλεκτρονικών εγκλημάτων. Επίσης η

κυβερνοχώρο» αποτελεί το νομικό πλαίσιο αναφοράς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών, πάνω στο οποίο βασίστηκε η Οδηγία.[40]

Στόχος της Οδηγίας αυτής είναι η εναρμόνιση της ποινικής νομοθεσίας των Κρατών Μελών της Ευρωπαϊκής Ένωσης σε θέματα επιθέσεών κατά συστημάτων πληροφοριών, με τη θέσπιση ελαχίστων κανόνων για τον ορισμό των ποινικών αδικημάτων και των σχετικά́ προβλεπόμενων κυρώσεων, τη βελτίωση της συνεργασίας των αρμοδίων αρχών των Κρατών Μελών, συμπεριλαμβανομένων των αστυνομικών ή άλλων υπηρεσιών επιφορτισμένων με την επιβολή του νομού, καθώς και των αρμοδίων ειδικευμένων οργανισμών και φορέων της Ευρωπαϊκής Ένωσης όπως η Eurojust, η Europol και το Ευρωπαϊκό Κέντρο Ηλεκτρονικού́ Εγκλήματος, καθώς και ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια δίκτυών και Πληροφοριών (ENISA).[41]

4.2. Τα επιμέρους άρθρα της Οδηγίας

4.2.1. Άρθρο 1 – Αντικείμενο

Το άρθρο 1 της Οδηγίας ρυθμίζει το αντικείμενό της, το οποίο, ειδικότερα, προσδιορίζεται ως η θέσπιση των απαραίτητων κανόνων σχετικά με τα ποινικά αδικήματα και τις αντίστοιχες κυρώσεις στον τομέα των επιθέσεων κατά των συστημάτων πληροφοριών. Επιπλέον αναφέρονται ρητά, ως σκοποί της Οδηγίας αναφέρονται, η διευκόλυνση της πρόληψης των αδικημάτων αυτών και η βελτίωση της συνεργασίας μεταξύ δικαστικών και άλλων αρμόδιων αρχών.

4.2.2. Άρθρο 2 – Ορισμοί

Στο άρθρο 2 περιέχονται οι βασικοί ορισμοί για τους όρους: α) «σύστημα πληροφοριών», β) «ηλεκτρονικά δεδομένα», γ) «νομικό πρόσωπο» και δ) «χωρίς δικαίωμα».

Αναλυτικά, οι ως άνω ορισμοί έχουν ως εξής*:*

*«α) **«σύστημα πληροφοριών»**: η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν*

απόφαση-πλαίσιο δεν λάμβανε υπόψη νέες μεθόδους διάπραξης των εγκλημάτων στον Κυβερνοχώρο και ιδίως την ολοένα και αυξανόμενη χρήση δικτύων προγραμμάτων ρομπότ (botnets).

[40] Σκέψη 15 του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

[41] Σκέψη 1του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή του·»

Όπως παρατηρείται ο όρος «σύστημα πληροφοριών» αντικατέστησε τον όρο «σύστημα υπολογιστή» που υπήρχε στη Σύμβαση και μάλιστα ήδη με την απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου σύμφωνα με την Αιτιολογική Έκθεση της οποίας *«[η] φράση «σύστημα πληροφοριών» χρησιμοποιείται σκοπίμως στο προκείμενο με την πλέον ευρεία έννοιά της αναγνωρίζοντας τη σύγκλιση μεταξύ των δικτύων ηλεκτρονικής επικοινωνίας και των διαφόρων συνδεδεμένων συστημάτων ... [γ]ια τους σκοπούς της παρούσας πρότασης, τα συστήματα πληροφοριών καλύπτουν συνεπώς τους αυτόνομους προσωπικούς υπολογιστές, τις προσωπικές ηλεκτρονικές ατζέντες, τα κινητά τηλέφωνα, τα εσωτερικά δίκτυα (intranets), τα εξωτερικά δίκτυα (extranets), και, φυσικά, τα δίκτυα, τους εξυπηρετητές και άλλες υποδομές του διαδικτύου»*. Περαιτέρω πέραν της διευκρίνησης αυτής, καθώς ουσιαστικά περί διευκρινήσεως πρόκειται, το περιεχόμενο του όρου διευρύνθηκε με την προσθήκη σε αυτόν, πέραν των συσκευών, και των ηλεκτρονικών δεδομένων, παραπέμποντας με αυτό τον τρόπο στον επόμενο ορισμό.

«β) ***«ηλεκτρονικά δεδομένα»****: η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία·»*[42]

«γ) ***«νομικό πρόσωπο»****: κάθε οντότητα που έχει το καθεστώς του νομικού προσώπου βάσει του εφαρμοστέου δικαίου, αλλά δεν περιλαμβάνει κράτη, ή δημόσιους φορείς κατά την άσκηση της εξουσίας τους ή δημόσιους διεθνείς οργανισμούς·»*

*«δ)****«χωρίς δικαίωμα»****: η αναφερόμενη στην παρούσα οδηγία συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δικαίου.»*[43]

[42] Το περιεχόμενο του όρου αυτού βασίζεται στον σχετικό ορισμό του ISO και είναι ταυτόσημο με αυτό του όρου «δεδομένα υπολογιστών» που υπάρχει στη Σύμβαση.

[43] Επισημαίνεται ότι σχετική ρύθμιση δεν υπήρχε ρητά στο σώμα της Σύμβασης ούτε ως σε γενική διάταξή ούτε στα επιμέρους άρθρα που ποινικοποιούν τις συγκεκριμένες συμπεριφορές, πλην όμως αναφερόταν στην Αιτιολογική της Έκθεση (σκέψη 38) ως γενική προϋπόθεση για την ποινικοποίηση όλων αυτών των εγκλημάτων.

4.2.3. Διατάξεις Ουσιαστικού Ποινικού Δικαίου

4.2.3.1. Άρθρο 3 – Παράνομη πρόσβαση σε σύστημα πληροφοριών

Το άρθρο 3 (το οποίο αντιστοιχεί στο άρθρο 2 της Σύμβασης του Συμβουλίου της Ευρώπης) αναφέρεται στο έγκλημα της παράνομής πρόσβασης σε συστήματα πληροφοριών.

Συγκεκριμένα το ως άνω άρθρο έχει ως ακολούθως:

«Άρθρο 3 – Παράνομη πρόσβαση σε συστήματα πληροφοριών

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.»

Η βασική διαφορά της διάταξης αυτής από της διάταξη του άρθρου 2 της Σύμβασης έγκειται στο γεγονός ότι η ως άνω διάταξη της Οδηγία θέτει ως προϋπόθεση της τέλεσης του εγκλήματος την παραβίαση μέτρου ασφαλείας σε αντίθεση με την διάταξη της Σύμβαση που απλώς αφήνει τη διακριτική ευχέρεια στα Συμβαλλόμενα Κράτη να εξαρτήσουν την στοιχειοθέτηση της αντικειμενικής υπόστασης του συγκεκριμένου εγκλήματός από τη ενός τέτοιου μέτρου. Η διαφοροποίηση αυτή στη ρύθμιση της Οδηγία, που επιβάλει για την τέλεση του εγκλήματος της παράνομης πρόσβασης σε σύστημα πληροφοριών την παραβίαση μέτρου ασφαλείας (όπως λ.χ. κωδικού ή βιομετρικής ταυτοποίησης) κρίνεται ως ορθή καθώς συμβαδίζει με το πνεύμα του ποινικού δικαίου που αντιμετωπίζει τον ποινικό κολασμό των πράξεων ως το έσχατο μέτρο (ultimum refugium) το οποίο θα πρέπει να λαμβάνεται για την επιβολή του δικαίου.[44] Ωστόσο, σε κάθε περίπτωση τα Κράτη Μέλη έχουν τον τελευταίο λόγο και δεν δεσμεύονται να μην ποινικοποιήσουν συμπεριφορές που συνιστούν παράνομη πρόσβαση σε πληροφοριακά συστήματα αν δεν υπάρχει παραβίαση μέτρου ασφαλείας. Επομένως, η διαφοροποίηση αυτή αν και θεμελιώδης, δεν έχει ουσιαστικές συνέπειες.

Μια δεύτερη διαφορά είναι ότι, σε αντίθεση με το άρθρο 2 της Σύμβασης, στο άρθρο 3 της Οδηγίας, η ποινικοποίηση του εγκλήματος της παράνομης πρόσβασης σε σύστημα πληροφοριών επιβάλλεται μόνο σε περιπτώσεις που δεν είναι ήσσονος σημασίας. Σύμφωνα, δε, με το προοίμιο της Οδηγίας *«[τ]α κράτη μέλη θα πρέπει να μπορούν να καθορίζουν τι συνιστά περίπτωση ήσσονος σημασίας σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές. Μια περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν, παραδείγματος χάριν, οι ζημίες που προκαλεί το αδίκημα και/ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον,*

[44] Μ. Καϊάφα – Γκμπάντι, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 489 επ.

όπως η ακεραιότητα ενός συστήματος υπολογιστών ή ηλεκτρονικών δεδομένων, ή η σωματική ακεραιότητα, τα δικαιώματά ή άλλα συμφέροντα ενός προσώπου, είναι αμελητέα ή τέτοιας φύσης ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης.»[45] Ωστόσο παρά την διευκρίνηση αυτή, ο όρος «ήσσονος σημασίας», παρότι τίθεται προς όφελος του δράστη, επικρίνεται ως υπερβολικά ευρύς σε βαθμό που να καθιστά όλη τη διάταξη μη συμβατή με την αρχή της νομιμότητας λόγω αοριστίας. Επομένως, ο όρος αυτός χρήζει εξειδίκευσης από τον εκάστοτε εθνικό νομοθέτη.

4.2.3.2. Άρθρο 4 – Παράνομη παρεμβολή σε σύστημα

Το άρθρο 4 (το οποίο αντιστοιχεί στο άρθρο 5 της Σύμβασης του Συμβουλίου της Ευρώπης) ρυθμίζει τις παράνομες παρεμβολές σε συστήματα πληροφοριών.

Συγκεκριμένα το ως άνω άρθρο 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».

Δύο είναι ουσιαστικά οι διαφορές από την διάταξη του άρθρου 5 της Σύμβασης. Η πρώτη συνίσταται στο ότι αναφέρεται πλέον ρητά[46] ως προϋπόθεση ποινικοποίησης της πράξης να έχει τελεστεί αυτή από το δράστη, χωρίς αυτός να έχει δικαίωμα προς τούτη. Εν προκειμένω, στην πράξη, συνήθως «με δικαίωμα» θα είναι περιπτώσεις ελέγχου, ενημέρωσης και αναβάθμισης της λειτουργίας του πληροφοριακού συστήματος, για το σκοπό τον οποίο η πρόσβαση ή η λειτουργία του θα πρέπει ή θα διακόπτεται για (περι)ορισμένο χρονικό διάστημα.

Η δεύτερη διαφορά είναι ότι σύμφωνα με τη διάταξη του άρθρου 6 της Οδηγίας δίνεται ρητά η δυνατότητα στα Κράτη Μέλη, μη ποινικοποίησης των συμπεριφορών που συνιστούν παρεμβολή σε πληροφοριακό σύστημα όταν αυτή είναι «ήσσονος σημασίας» όπως λ.χ. θα μπορούσαμε να πούμε ότι είναι όταν η παρεμπόδιση ή η διακοπή της λειτουργίας έχει μικρή χρονική διάρκεια. Ωστόσο η δυνατότητα αυτή, η οποία σημειωτέον προβλέπεται από τη

[45] Σκέψη 11 του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

[46] Η προϋπόθεση αυτή, όπως εκτέθηκε στο σχετικό χωρίο, δεν υπήρχε στο κείμενο της Σύμβασης παρά μόνο στην Αιτιολογική της Έκθεση (σκέψη 62).

Οδηγία σε όλα τα επιμέρους άρθρα στα οποία τυποποιούνται εγκλήματα που συνιστούν επιθέσεις κατά πληροφοριακών συστημάτων, στο συγκεκριμένο άρθρο είναι περιττή, καθώς υπερκαλύπτεται από την προϋπόθεση η παρεμπόδιση ή η διακοπή της λειτουργίας του πληροφοριακού συστήματος να είναι «σοβαρή». Όπως εκτέθηκε στο σχετικό με το άρθρο 5 της Σύμβασης χωρίο της παρούσας εργασίας «σοβαρή» θεωρείται η παρακώλυση της λειτουργίας ενός συστήματος με την αποστολή δεδομένων σε αυτό υπό τέτοια μορφή, μέγεθος ή συχνότητα που να επηρεάζει σημαντικά ή καθοριστικά την δυνατότητα του ιδιοκτήτη ή του χρήστη να χρησιμοποιεί το σύστημα ή να επικοινωνεί με άλλα συστήματα. Δεδομένου, ωστόσο, ότι παρεμπόδιση ή διακοπή της λειτουργίας ενός συστήματος δύναται να τελεστεί και με άλλους τρόπους εκτός από την υπερφόρτωση του συστήματος, θα πρέπει να εκλάβουμε την ως άνω ερμηνεία ως ενδεικτική και να μην αποκλείσουμε να αξιολογείται για το κατά πόσο η παρεμβολή σε ένα σύστημα είναι σοβαρή και η διάρκεια της παρεμπόδισης ή της διακοπής της λειτουργίας.

4.2.3.3. Άρθρο 5 – Παράνομη παρεμβολή σε δεδομένα

Το άρθρο 5 (το οποίο αντιστοιχεί στο άρθρο 4 της Σύμβασης του Συμβουλίου της Ευρώπης) ποινικοποιεί τις παράνομες παρεμβολές σε δεδομένα.

Συγκεκριμένα το ως άνω άρθρο έχει ως ακολούθως:

«Άρθρο 5 – Παράνομη παρεμβολή σε δεδομένα

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις».

Συγκριτικά με την σχετική διάταξη του 4 της Σύμβασης, παρατηρείται ότι η διαφοροποίηση των τρόπων τέλεσης με την προσθήκη της περίπτωσης της εξάλειψης ηλεκτρονικών δεδομένων είναι άνευ ουσιαστικής σημασίας καθώς μπορούσε ήδη να ενταχθεί νοηματικά στο περιεχόμενο των άλλων περιπτώσεων. Επίσης, στο άρθρο της Οδηγίας προβλέπεται πλέον ρητά ότι η παρεμβολή σε δεδομένα ποινικοποιείται μόνο όταν τελείται χωρίς δικαίωμα.[47]

Αντίθετα προς τα ανωτέρω, ουσιαστικές είναι οι συνέπειες που έχει η διαφορά ότι στο άρθρο της Σύμβασης επιτρέπεται στα Συμβαλλόμενα Μέρη να θέσουν ως προϋπόθεση της ποινικοποίησης της παρεμβολής σε δεδομένα αυτή να έχει ως συνέπεια την πρόκληση

[47] Η προϋπόθεση αυτή, όπως εκτέθηκε στο σχετικό χωρίο, δεν υπήρχε στο κείμενο της Σύμβασης παρά μόνο στην Αιτιολογική της Έκθεση (σκέψη 62).

«σοβαρής ζημίας», ενώ στο άρθρο της Οδηγία επιβάλλεται η μη ποινικοποίηση περιπτώσεων «ήσσονος σημασίας». Θα πρέπει να γίνει δεκτό ότι η έννοια της «σημασίας» του αδικήματος είναι ταυτόσημη με την έννοια της ζημίας δηλαδή της βλάβης του εννόμου αγαθού εν προκειμένω της ακεραιότητας και της κανονικής λειτουργίας ή χρήσης των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών κατά την Σύμβαση ή των πληροφοριακών συστημάτων καθ' αυτών κατά την Οδηγία. Η Οδηγία φαίνεται, λοιπόν, ως εκ τούτου, να είναι αυστηρότερη, καθώς, εν αντιθέσει με την Σύμβαση, ποινικοποιεί και περιπτώσεις μέτριας σημασίας.

4.2.3.4. Άρθρο 6 – Παράνομη υποκλοπή

Το άρθρο 6 (το οποίο αντιστοιχεί στο άρθρο 3 της Σύμβασης του Συμβουλίου της Ευρώπης) προσδιορίζει την αξιόποινη πράξη της παράνομής υποκλοπής.

Συγκεκριμένα το ως άνω άρθρο έχει ως ακολούθως:

«Άρθρο 6 – Παράνομη υποκλοπή

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις».

Σύμφωνα με το προοίμιο της Οδηγίας, η υποκλοπή περιλαμβάνει, ενδεικτικά, την ακρόαση, έλεγχο ή επιτήρηση του περιεχομένου των επικοινωνιών και την παροχή του περιεχομένου των δεδομένων είτε άμεσα, μέσω της πρόσβασης και χρήσης των συστημάτων πληροφοριών, είτε έμμεσα μέσω της χρήσης ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα.[48]

Το άρθρο αυτό ταυτίζεται, κατά διατύπωση και περιεχόμενο, με το άρθρο 3 της Σύμβασης, οπότε ισχύουν και εδώ όσα εκτέθηκαν στο σχετικό χωρίο της παρούσας, πλην όμως με ορισμένες μικρές διαφοροποιήσεις. Αρχικά σε αντίθεση με την ως άνω διάταξη της Σύμβασης, το άρθρο 6 της Οδηγίας απαιτεί πλέον ρητά[49] ως προϋπόθεση ποινικοποίησής της η συμπεριφορά που συνιστά υποκλοπή να τελέστηκε από το δράστη χωρίς αυτός να έχει

[48] Σκέψη 9 του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

[49] Η προϋπόθεση αυτή, όπως εκτέθηκε στο σχετικό χωρίο, δεν υπήρχε στο κείμενο της Σύμβασης παρά μόνο στην Αιτιολογική της Έκθεση (σκέψη 62).

κάποιο δικαίωμα.[50] Μία δεύτερη διαφορά είναι η Οδηγία επιτρέπει την μη ποινικοποίηση της πράξης υποκλοπής όταν αυτή συνιστά περίπτωση «ήσσονος σημασίας».[51] Πέρα από τη γενική προβληματική που υπάρχει αναφορικά με τον όρο αυτό, ειδικότερο ζήτημα αναφύεται στην συγκεκριμένη περίπτωση της υποκλοπής, δεδομένης της Συνταγματικά κατοχυρωμένης απόλυτης προστασίας του απορρήτου της με οποιοδήποτε τρόπο επικοινωνίας. Ωστόσο, ερμηνευτικά θα πρέπει να γίνει δεκτό ότι η Συνταγματική ρύθμιση αφορά μόνο περιπτώσεις επικοινωνίας μεταξύ δύο προσώπων ή έστω μεταξύ δύο πληροφοριακών συστημάτων και όχι εντός ενός και του αυτού πληροφοριακού συστήματος και επομένως η εν λόγω διάταξη του άρθρου 6 της Οδηγίας είναι ευρύτερη και προστατεύει και το δικαίωμα στην προσωπική ζωή και την ιδιωτικότητα. Τέλος, εν αντιθέσει με την σχετική διάταξη της Σύμβασης, στο άρθρο 6 της Οδηγίας δεν δίνεται η δυνατότητα στα Κράτη Μέλη να θέσουν ως προϋπόθεση τέλεσης του εγκλήματος την επίτευξη σύνδεσης ενός πληροφοριακού συστήματος με ένα άλλο. Αυτή η τελευταία διαφορά είναι λογική αν αναλογιστούμε ότι η Σύμβαση ποινικοποιεί μόνο εγκλήματα που τελούνται μέσω διαδικτύου ενώ η Οδηγία εγκλήματα που στρέφονται κατά πληροφοριακών συστημάτων καθ' αυτών ανεξάρτητα από το αν αυτά τελούνται με τη χρήση του διαδικτύου ή όχι.

4.2.3.5. Άρθρο 7 – Εργαλεία που χρησιμοποιούνται για την διάπραξη των αδικημάτων

Το άρθρο 7 (αντίστοιχο του άρθρου 6 της Σύμβασης του Συμβουλίου της Ευρώπης) αναφέρεται στα εργαλεία που χρησιμοποιούνται για τη διάπραξη των παραπάνω αναφερόμενων εγκλημάτων.

Συγκεκριμένα το ως άνω άρθρο έχει ως ακολούθως:

---

[50] πρβλ., ενδεικτικά, σχετικά με την δυνατότητα των Κρατών Μελών να επιτρέπουν στους εργοδότες να ελέγχουν την ηλεκτρονική αλληλογραφία των υπαλλήλων τους, την απόφαση της 05.09.2017 της Ολομέλειας (Grand Chamber) του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου στην υπόθεση BĂRBULESCU κατά Ρουμανίας (Application no. 61496/08)

[51] Όπως εκτέθηκε ανωτέρω, σύμφωνα με την σκέψη 11 του Προοίμιού της Οδηγίας «[τ]α κράτη μέλη θα πρέπει να μπορούν να καθορίζουν τι συνιστά περίπτωση ήσσονος σημασίας σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές. Η περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν, παραδείγματος χάριν, οι ζημίες που προκαλεί το αδίκημα και/ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον, όπως η ακεραιότητα ενός συστήματος υπολογιστών ή ηλεκτρονικών δεδομένων, ή η σωματική ακεραιότητα, τα δικαιώματά ή άλλα συμφέροντα ενός προσώπου, είναι αμελητέα ή τέτοιας φύσης ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου ή η απόδοση ποινικής ευθύνης.» Ωστόσο παρά την διευκρίνηση αυτή, ο όρος «ήσσονος σημασίας» παρότι τίθεται προς όφελος του δράστη έχει επικριθεί ως υπερβολικά ευρύς σε βαθμό που να καθιστά όλη τη διάταξη μη συμβατή με την αρχή της νομιμότητας λόγω αοριστίας.

«Άρθρο 7 – Εργαλεία που χρησιμοποιούνται για τη διάπραξη των αδικημάτων

Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλουθων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

α) πρόγραμμα υπολογιστή, που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6·

β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών».

Σύμφωνα με το προοίμιο της Οδηγίας *«[λ]αμβανομένων υπόψη των διαφορετικών τροπών με τους οποίους μπορούν να πραγματοποιηθούν οι επιθέσεις και της ταχείας εξέλιξης του υλισμικού και του λογισμικού, η παρούσα οδηγία αναφέρεται σε εργαλεία που μπορούν να χρησιμοποιηθούν για τη διάπραξη των αδικημάτων που απαριθμούνται στην παρούσα οδηγία […] [τ]έτοια εργαλεία μπορούν να περιλαμβάνουν το κακόβουλο λογισμικό — συμπεριλαμβανομένων των εργαλείων που μπορούν να δημιουργούν «botnet»*[52]*— το οποίο χρησιμοποιείται για τη διάπραξη επιθέσεων στον κυβερνοχώρο […] [α]κόμη και όταν ένα τέτοιο εργαλείο είναι κατάλληλο ή ιδιαιτέρως κατάλληλο για τη διάπραξη ενός εκ των αδικημάτων που ορίζονται στην παρούσα οδηγία, είναι πιθανό το εργαλείο να έχει παραχθεί για νόμιμο σκοπό […] [μ]ε αιτιολογία την ανάγκη να αποφευχθεί η ποινικοποίηση οσάκις τα εν λόγω εργαλεία παράγονται και διατίθενται στην αγορά για νόμιμους σκοπούς, όπως για τον έλεγχο της αξιοπιστίας των προϊόντων της τεχνολογίας πληροφοριών ή της ασφάλειας των συστημάτων πληροφοριών, εκτός από τη γενική απαίτηση της πρόθεσης, μια απαίτηση άμεσης πρόθεσης να χρησιμοποιήσει τα εργαλεία αυτά για να διαπράξει ένα ή περισσότερα εκ των αδικημάτων που ορίζονται στην παρούσα Οδηγία, πρέπει επίσης να πληρούται.»*[53]

[52] Δημιουργία botnet (δικτύων προγραμμάτων ρομπότ), όπως αναφέρεται στην παρούσα οδηγία, είναι η πράξη της απόκτησης εξ αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών διά της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο. Μόλις δημιουργηθεί, το προσβεβλημένο δίκτυο υπολογιστών, που συνιστά το «botnet», μπορεί να ενεργοποιείται εν αγνοία των χρηστών των εν λόγω υπολογιστών, με σκοπό την εξαπόλυση επιθέσεων στον κυβερνοχώρο μεγάλης κλίμακας, η οποία συνήθως μπορεί να προκαλέσει σοβαρές ζημίες,

[53] Σκέψη 27 του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών

Σε αυτό το σημείο, θα πρέπει να παρατηρήσουμε, ότι οι διαφορές του άρθρου αυτού με το άρθρο 6 της Σύμβασης («Κακή χρήση συσκευών) δεν περιορίζονται μόνο στον τίτλο και στον τρόπο διατύπωσης του άρθρου. Κατ' αρχήν, από την πρώτη προβλεπόμενη περίπτωση λείπει η αναφορά σε συσκευές[54] και παραμένει μόνο η αναφορά σε προγράμματα υπολογιστή. Ωστόσο, ορθή κρίνεται αυτή η διαφοροποίηση, καθώς πράγματι η αναφορά σε προγράμματα υπολογιστών καλύπτει όλες τις περιπτώσεις που είχε στο μυαλό του ο νομοθέτης, ακόμα και αν γίνονται με τη βοήθεια κάποιας συσκευής, καθώς η τελευταία θα πρέπει να περιέχει ένα πρόγραμμα που να μπορεί να χρησιμοποιηθεί για τη διάπραξη κάποιου γνήσιου πληροφοριακού εγκλήματος. Παράλληλα, εκτός αυτού, όπως ήδη επισημάνθηκε η διατύπωση του άρθρου 6 της Σύμβασης, σύμφωνα με την οποία η έννοια του προγράμματος υπολογιστή περιλαμβάνεται στην έννοια της συσκευής ήταν εντελώς άστοχη, χωρίς, ωστόσο, αυτή να είχε πρακτικές συνέπειες.

Μια δεύτερη διαφοροποίηση από το άρθρο 6 της Σύμβαση είναι ότι δεν ποινικοποιείται η κατοχή (προγραμμάτων ή κωδικών πρόσβασης). Και η διαφοροποίηση αυτή θα πρέπει να θεωρηθεί εν μέρει ως ορθή, λαμβανομένης υπόψη της δριμείας κριτικής κατά της ποινικοποίησης προπαρασκευαστικών πράξεων λόγω της εξαιρετικής δυσχέρειας στην απόδειξη του δόλου, δεδομένης, μάλιστα, της φύσης των προγραμμάτων ως διπλή χρήσης (dual use) δηλαδή όχι αποκλειστικά για το σκοπό τέλεσης εγκληματικών πράξεων. Αναφορικά, ωστόσο, με την κατοχή συνθηματικών ή κωδικών, θα ήταν ορθότερο να παραμείνει η πρόβλεψη για την ποινικοποίηση της κατοχής τους υπό την προϋπόθεση της κατοχής ενός ελάχιστου αριθμού τέτοιων όπως δινόταν η δυνατότητα στο εδ. β' της περ. β' του άρθρου 6 της Σύμβασης. Ο λόγος για τον οποίο θα έπρεπε να συμβαίνει αυτό είναι κατά το γράφοντα το γεγονός ότι οι κωδικοί πρόσβασης είναι προσωπικοί και δεν δύνανται να χρησιμεύουν εν αντιθέσει με τα ως άνω προγράμματα στην πραγματοποίηση επιτρεπτών δοκιμών ή για την προστασία ενός συστήματος υπολογιστή.

Επιπλέον, στο άρθρο 6 της Σύμβαση προβλεπόταν η δυνατότητα μη ποινικοποίησης των ως αν συμπεριφορών όταν γίνονται για την πραγματοποίηση επιτρεπτών δοκιμών (παρ. 2) καθώς και η δυνατότητα μη εφαρμογής του άρθρου αυτού πλην των περιπτώσεων παραγωγής, πώλησης, διανομής ή άλλως διάθεσης συνθηματικών κωδικών υπολογιστή, κωδικών πρόσβασης ή παρόμοιων στοιχείων (παρ. 3). Αντίθετα, στην εν λόγω διάταξη του άρθρου 7 της Οδηγίας, δεν υπάρχει σχετική πρόβλεψη γεγονός που εκ πρώτης όψεως φαίνεται να καθιστά τη διάταξη αυτή παράλογα αυστηρότερη καθώς ποινικοποιεί άκριτα όλα

[54] Για αυτό και η διαφοροποίηση στον τίτλο.

τα τεχνικά μέσα που εξυπηρετούν την τέλεση επιθέσεων κατά πληροφοριακών συστημάτων αδιαφορώντας για τον διπλής χρήσης (dual use) χαρακτήρα τους δηλαδή για το γεγονός ότι πολλές φορές αυτά εξυπηρετούν τον έλεγχο και την βελτίωση των λειτουργειών ασφαλείας των πληροφοριακών συστημάτων, όπως λ.χ. συμβαίνει κατεξοχήν με τα hacking tools, δηλαδή τα προγράμματα που συνιστούν τεχνικά μέσα για την πρόσβαση σε πληροφορικά συστήματα. Ωστόσο, η διατήρηση της ασφαλιστικής δικλείδας της προϋπόθεσης η τυποποιημένη συμπεριφορά να τελείται «χωρίς δικαίωμα», η οποία πλέον προβλέπεται ρητά[55], στην πράξη εξουδετερώνει τις δυσμενείς συνέπειες της παράλειψης αυτής. Επίσης έχει υποστηριχθεί ότι η ρητή αυτή εξαίρεση αυτή δεν είναι απαραίτητη στο μέτρο που η αναφορά στο σκοπό τέλεσης των πιο προβλεπόμενων αδικημάτων είναι ικανή να αποκλείσει το σκοπό της χρήσης τους για λόγους δοκιμής ή προστασίας ενός πληροφοριακού συστήματος, πλην όμως λόγω του γεγονότος ότι οι προβλεπόμενες πράξεις είναι ιδιαίτερα απομακρυσμένες από οποιαδήποτε πραγματική προσβολή των πληροφοριακών συστημάτων ή των δεδομένων τους, κάθε αποσαφήνιση των περιπτώσεων αποκλεισμού του αξιοποίνου μόνο θετικά μπορεί να κριθεί.[56]

Μια ακόμα ουσιαστική διαφορά που παρατηρείται είναι ότι, ενώ στην Σύμβαση επιβάλλεται η ποινικοποίηση μόνο για την πώληση, διανομή, ή άλλως διάθεση συνθηματικών κωδικών υπολογιστών, κωδικών πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος ενός πληροφοριακού συστήματος, στην Οδηγία δεν προβλέπεται για τα Κράτη Μέλη σχετική δυνατότητα, δηλαδή μη ποινικοποίησης των λοιπών περιπτώσεων.

Τέλος, εν αντιθέσει με την διάταξη του άρθρου 6 της Σύμβασης, το άρθρο 7 της Οδηγίας προβλέπει την δυνατότητα μη ποινικοποίησης «ήσσονος σημασίας» περιπτώσεων. Το δε περιεχόμενο του όρου αυτού στην συγκεκριμένη περίπτωση χρήζει ειδικής εξειδίκευσης, η οποία δεν παρέχεται από την Οδηγία και εναπόκειται αποκλειστικά στην βούληση του εθνικού νομοθέτη. Πάντως, ένα κριτήριο το οποίο θα μπορούσε πιθανόν να εφαρμοσθεί από τα Κράτη Μέλη αναφορικά με την αξιολόγηση της σημασίας των προπαρασκευαστικών συμπεριφορών των εγκλημάτων που συνιστούν επιθέσεις κατά πληροφοριακών συστημάτων είναι ο αριθμός των τεχνικών μέσων ή των κωδικών.

---

[55] Η προϋπόθεση αυτή, όπως εκτέθηκε στο σχετικό χωρίο, δεν υπήρχε στο κείμενο της Σύμβασης παρά μόνο στην Αιτιολογική της Έκθεση.

[56] Μ. Καϊάφα – Γκμπάντι, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 489 επ.

Συνεπώς, όπως έχει χαρακτηρίσθηκα επισημανθεί, δεν υιοθετήθηκε από την Οδηγία καμία πρόβλεψη που θα μπορούσε να εκλογικεύσει το αξιόποινο και να περιορίσει την ανασφάλεια δικαίου που δημιουργεί η ποινικοποίηση πράξεων παραγωγής, κατοχής κ.λπ. εργαλείων που μπορούν να χρησιμοποιηθούν για νόμιμους σκοπούς με αποτέλεσμα *«το αξιόποινο που ζητά από τα Κράτη Μέλη να δημιουργήσουν σε αυτό το πολύ προωθημένο στάδιο των προπαρασκευαστικών πράξεων [να] στηρίζεται κατεξοχήν σε δύσκολα διαγνώσιμα υποκειμενικά στοιχεία»*.[57]

4.2.3.6. Άρθρο 8 – Ηθική αυτουργία, υποβοήθηση και συνέργεια και απόπειρα

Το άρθρο 8 (αντίστοιχο του άρθρου 12 της Σύμβασης) προβλέπει την ποινικοποίηση της συμμετοχικής δράσης και της απόπειρας.

Συγκεκριμένα το ως άνω άρθρο έχει ως ακολούθως:

«Άρθρο 8 – Ηθική αυτουργία, υποβοήθηση και συνέργεια και απόπειρα

1. Τα κράτη μέλη εξασφαλίζουν ότι η ηθική αυτουργία, ή η υποβοήθηση και η συνέργεια, προς διάπραξη αδικήματος που αναφέρεται στα άρθρα 3 έως 7 τιμωρείται ως ποινικό αδίκημα.

2. Τα κράτη μέλη εξασφαλίζουν ότι η απόπειρα διάπραξης αδικήματος που αναφέρεται στα άρθρα 4 και 5 να τιμωρείται ως ποινικό αδίκημα.»

Αναφορικά με την ηθική αυτουργία, την υποβοήθηση και τη συνέργεια δεν παρατηρείται ουσιαστική διαφοροποίηση σε σχέση με την παρ. 1 του άρθρου 12 της Σύμβασης καθώς προβλέπεται η ποινικοποίησή τους για όλα τα προβλεπόμενα εγκλήματα συμπεριλαμβανομένης και της διάταξης του άρθρου 7 που αφορά την παραγωγή και τη διάθεση εργαλείων για την διάπραξη των λοιπών εγκλημάτων. Αντίθετα παρατηρείται διαφοροποίηση σε σχέση με την πρόβλεψη για την ποινικοποίηση της ηθικής αυτουργίας καθώς με βάση την Οδηγία τα Κράτη Μέλη οφείλουν να ποινικοποιούν μόνο την απόπειρα τέλεσης των εγκλημάτων της παράνομης παρεμβολής σε σύστημα (άρθρο 4) και της παράνομης παρεμβολής σε δεδομένα (άρθρο 5). Η πρόβλεψη αυτή είναι εν μέρη αυστηρότερη και εν μέρει ηπιότερη από αυτή της Σύμβασης καθώς στην τελευταία προβλεπόταν αφενός η ποινικοποίηση της απόπειρας όλων τυποποιούμενων σε αυτή εγκλημάτων με εξαίρεση αυτό της κακής χρήσης συσκευών του άρθρο 6 (παρ. 2), πλην όμως τα Συμβαλλόμενα μέρη διατηρούσαν το δικαίωμα να μην ποινικοποιήσουν την απόπειρα των εγκλημάτων αυτών (παρ. 3).

[57] Μ. Καϊάφα – Γκμπάντι, ο.π.

4.2.3.7. Άρθρο 9 – Κυρώσεις

Το άρθρο 9 αναφέρεται στο είδος των κυρώσεων που πρέπει να επιβάλλονται στις επιμέρους αξιόποινες πράξεις. Σύμφωνα με το προοίμιο της ίδιας της Οδηγίας τα Κράτη Μέλη θα πρέπει να προβλέπουν κυρώσεις για τις επιθέσεις κατά συστημάτων πληροφοριών. οι οποίες θα πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές και να περιλαμβάνουν φυλάκιση και/ή χρηματικές ποινές.[58] Η διάταξη αυτή διαφοροποιείται από τη διάταξή του άρθρου 13 της Σύμβασης καθώς καθορίζει με βάση την αρχή της επικουρικότητας στο πλαίσιο της Ένωσης τα κατώτατα ανώτερα όρια στα πλαίσια ποινών για τα τυποποιημένα εγκλήματα.

Συγκεκριμένα το ως άνω άρθρο έχει ως ακολούθως:

«Άρθρο 9 – Κυρώσεις

1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8 τιμωρούνται με αποτελεσματικές, αναλογικές και αποτρεπτικές ποινικές κυρώσεις.

2. Τα κράτη μέλη λαμβάνουν τα αναγκαίά μετρά για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 3 έως 7 τιμωρούνται με στερητική της ελευθερίας ποινή́, το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον δύο έτη, τουλάχιστον για περιπτώσεις που δεν είναι ήσσονος σημασίας.

3. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, οσάκις τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται εκ προθέσεως, και εφόσον έχει πληγεί́ σημαντικός αριθμός συστημάτων πληροφοριών μέσω της χρήσης εργαλείου αναφερομένου στο άρθρο 7, το οποίο έχει σχεδιασθεί ή προσαρμοσθεί πρωτίστως για τον σκοπό́ αυτό, τιμωρούνται με στερητική της ελευθερίας ποινή́ το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον τρία έτη.

4. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 τιμωρούνται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον πέντε έτη, εφόσον:

α) διαπράττονται στο πλαίσιο εγκληματικής οργάνωσης κατά την έννοια της απόφασης-πλαισίου 2008/841/ΔΕΥ, ανεξαρτήτως της κύρωσης που ορίζεται σε αυτή́.[59]

---

[58] Σκέψη 10 του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

[59] Σύμφωνα με την σκέψη 13 του Προοιμίου της Οδηγία *«[ε]ίναι σκόπιμο να προβλεφθούν αυστηρότερες κυρώσεις όταν μια επίθεση κατά συστήματος πληροφοριών διαπράττεται από εγκληματική οργάνωση, όπως ορίζεται στην απόφαση- πλαίσιο 2008/841/ΔΕΥ του Συμβουλίου, της 24ης Οκτωβρίου 2008, για την*

β) προκαλούν σημαντικές ζημίες[60] *ή*

γ) διαπράττονται κατά συστήματος πληροφοριών που αποτελεί μέρος ζωτικής σημασίας υποδομής[61].

5. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να διασφαλίσουν ότι εφόσον τα αδικήματα που αναφέρονται στα άρθρα 4 και 5 διαπράττονται με υφαρπαγή δεδομένων προσωπικού χαρακτήρα άλλου προσώπου, προκειμένου να αποκτηθεί η εμπιστοσύνη τρίτων, και, ως εκ τούτου, προκαλούν ζημία στον νόμιμο δικαιούχο της ταυτότητας, το γεγονός αυτό μπορεί, σύμφωνα με το εθνικό δίκαιο, να εκλαμβάνεται ως επιβαρυντική περίσταση, εκτός εάν οι εν λόγω περιστάσεις καλύπτονται ήδη από άλλο αδίκημα που τιμωρείται σύμφωνα με το εθνικό δίκαιο.[62]*»*

4.2.3.8. Άρθρο 10 – Ευθύνη νομικών προσώπων και Άρθρο 11 – Κυρώσεις κατά νομικών προσώπων

Το άρθρο 10 ρυθμίζει την ευθύνη των νομικών προσώπων (ταυτίζεται κατά περιεχόμενο με το άρθρο 12 της Σύμβασης), ενώ το άρθρο 11 προβλέπει τις κυρώσεις που πρέπει να επιβάλλονται εναντίον τους με βάση την αρχή της επικουρικότητας (και δεν ανταποκρίνεται σε κάποια διάταξη της Σύμβασης).

Συγκεκριμένα τα ως άνω άρθρα έχουν ως ακολούθως:

«Άρθρο 10 – Ευθύνη νομικών προσώπων

καταπολέμηση του οργανωμένου εγκλήματος, 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». Είναι επίσης σκόπιμο να προβλεφθούν αυστηρότερες κυρώσεις, όταν η επίθεση διεξάγεται κατά υποδομής ζωτικής σημασίας των κρατών μελών ή της Ένωσης.»

[60] βλ. αμέσως ανωτέρω υποσημείωση 41.

[61] Σύμφωνα με την παρ. 4 του προοιμίου της Οδηγίας *«[…] [υ]ποδομές ζωτικής σημασίας μπορούν να νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που ευρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των ζωτικών κοινωνιακών λειτουργιών, της υγείας, της ασφάλειας, της προστασίας της οικονομικής ή κοινωνικής ευημερίας, όπως εγκαταστάσεις παραγωγής ενεργείας, μεταφορικά δίκτυα ή κυβερνητικά δίκτυα, και η διακοπή ή η καταστροφή των οποίων θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών.»* (σελ 218/8).

[62] Σύμφωνα με την σκέψη 14 του Προοιμίου της Οδηγίας *«[η] θέσπιση αποτελεσματικών μέτρων κατά της κλοπής ταυτότητας και άλλων αδικημάτων σχετικών με την ταυτότητα αποτελεί ένα άλλο σημαντικό στοιχείο μιας ολοκληρωμένης προσέγγισης του εγκλήματος στον κυβερνοχώρο […] [η] τυχόν ανάγκη για δράση της Ένωσης σχετικά με αυτό το είδος εγκληματικής συμπεριφοράς θα μπορούσε επίσης να εξετάζεται στο πλαίσιο της αξιολόγησης της ανάγκης για μια συνολική οριζόντια πράξη της Ένωσης.»*

1. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι νομικά πρόσωπα είναι δυνατόν να υπέχουν ευθύνη για τα αδικήματα που αναφέρονται στα άρθρα 3 έως 8 τα οποία έχουν τελεσθεί προς όφελός τους από οιοδήποτε πρόσωπο, ενεργώντας είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου και το οποίο κατέχει ιθύνουσα θέση εντός του νομικού αυτού προσώπου, βάσει μιας από τις ακόλουθες εξουσίες:

α) εξουσία εκπροσώπησης του νομικού προσώπου·

β) εξουσία λήψης αποφάσεων για λογαριασμό του νομικού προσώπου·

γ) εξουσία άσκησης ελέγχου εντός του νομικού προσώπου.

2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα προκειμένου να εξασφαλίσουν ότι νομικά πρόσωπα μπορούν να θεωρούνται υπεύθυνα οσάκις η έλλειψη εποπτείας ή ελέγχου εκ μέρους ενός από τα πρόσωπα που αναφέρονται στην παράγραφο 1 έχει επιτρέψει τη διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 8 προς όφελος του εν λόγω νομικού προσώπου από πρόσωπο που τελεί υπό την εξουσία του.

3. Η ευθύνη των νομικών προσώπων δυνάμει των παραγράφων 1 και 2 δεν αποκλείει την ποινική δίωξη φυσικών προσώπων που είναι αυτουργοί ή ηθικοί αυτουργοί ή συνεργοί στη διάπραξη αδικημάτων που αναφέρονται στα άρθρα 3 έως 8.»

«Άρθρο 11 – Κυρώσεις κατά νομικών προσώπων

1. Τα κράτη μέλη λαμβάνουν τα αναγκαίά μετρά προκειμένου να εξασφαλίσουν ότι το νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 10 παράγραφος 1 τιμωρείται με αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις, στις οποίες περιλαμβάνονται χρηματικές ποινές ή πρόστιμα και οι οποίες μπορούν να περιλαμβάνουν και άλλες κυρώσεις, όπως:

α) αποκλεισμό από δημοσιές παροχές ή ενισχύσεις·

β) προσωρινή ή οριστική απαγόρευση της άσκησης εμπορικών δραστηριοτήτων·

γ) θέση υπό δικαστική εποπτεία·

δ) δικαστική εκκαθάριση·

ε) προσωρινό ή οριστικό κλείσιμο των εγκαταστάσεων που χρησιμοποιηθήκαν για τη διάπραξη του αδικήματος.

2. Τα κράτη μέλη λαμβάνουν τα αναγκαία μετρά προκειμένου να εξασφαλίσουν ούτι το νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 10 παράγραφος 2 τιμωρείται με αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις ή άλλα μετρά.»

5. Εθνικό νομικό πλαίσιο

5.1. Οι προϋπάρχουσες διατάξεις του Π.Κ. για την προστασία από επιθέσεις σε βάρος πληροφοριακών συστημάτων

Πριν γίνει ανάλυση των νομοθετικών μεταβολών που επήλθαν με την θέση σε εφαρμογή του Ν. 4411/2016 κρίνεται σκόπιμο να γίνει μια συνοπτική επισκόπηση του προϋπάρχοντος νομοθετικού καθεστώτος είτε αυτό παραμένει ως είχε είτε τροποποιήθηκε, ούτως ώστε να δοθεί μια ολοκληρωμένη εικόνα της ποινικής αντιμετώπισης των επιθέσεων κατά συστημάτων πληροφοριών.

Η Ελλάδα, αν και μη τεχνολογικά προηγμένη, ήταν από τις πρώτες που αντιμετώπισε νομοθετικά με τη θέσπιση ποινικών κυρώσεων την τέλεση εγκλημάτων με υπολογιστές ήδη από το 1988. Οι σχετικές με την προστασία από επιθέσεις κατά πληροφοριακών συστημάτων διατάξεις που προστέθηκαν στον Π.Κ. με το νόμο 1805/1988 είναι οι εξής: α) τρίτο εδάφιο στο άρθρο 13 στοιχ. γ΄ Π.Κ.[63], με το οποίο διευρύνθηκε η νομική έννοια του εγγράφου ώστε να καταλαμβάνει και τα ηλεκτρονικά έγγραφα, γεγονός που επέτρεπε, πλην όμως πολύ περιορισμένα λόγω των λοιπών προϋποθέσεων της έννοιας του εγγράφου, την υπαγωγή ορισμένων συμπεριφορών με τις οποίες εκδηλώνονται επιθέσεις κατά πληροφοριακών συστημάτων στις διατάξεις του Π.Κ. για την προστασία των υπομνημάτων (άρθρα 216 Π.Κ. - πλαστογραφία και νόθευση και 222 Π.Κ. - υπεξαγωγή εγγράφου), β) το άρθρο 370Β[64] σύμφωνα με την παρ. 1 του οποίου ποινικοποιήθηκε η παράνομη πρόσβαση σε στοιχεία υπολογιστή που συνιστούν κρατικά, επαγγελματικά, επιστημονικά, επιχειρησιακά και άλλα

---

[63] «γ) έγγραφο είναι κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος αυτοτελώς ή σε συνδυασμό», ενώ σε ό,τι αφορά συγκεκριμένα τους Η/Υ, η έννοια του εγγράφου επεκτάθηκε και σε «κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων που δεν μπορούν να διαβαστούν άμεσα»

[64] *«Άρθρο 370Β*

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. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση».

απόρρητα[65], γ) το άρθρο 370Γ παρ. 2[66], σύμφωνα με το οποίο ποινικοποιήθηκε η παράνομη πρόσβαση σε στοιχεία υπολογιστή[67] και δ) το άρθρο 386Α σύμφωνα με το οποίο ποινικοποιήθηκε ο επηρεασμός της διαδικασίας ψηφιακών δεδομένων με σκοπό τον προσπορισμό παράνομου περιουσιακού οφέλους που βλάπτει ξένη περιουσία.

Σε συνδυασμό με τα ανωτέρω για την κάλυψη του νομοθετικού κενού σε περιπτώσεις φθοράς ηλεκτρονικών δεδομένων και παρακώλυση της λειτουργίας πληροφοριακών συστημάτων προτάθηκε από μέρος της Θεωρίας η εφαρμογή της διάταξης του άρθρου 381 Π.Κ..

Τέλος, παράλληλα με τις ως άνω διατάξεις, προστασία από επιθέσεις σε πληροφοριακά συστήματα παρεχόταν και εξακολουθεί να παρέχεται με τις ποινικές διατάξεις για την προστασία δεδομένων προσωπικού χαρακτήρα που προβλέπονται στο άρθρο 15 του Ν. 3471/2006[68] και στις παραγράφους 4 έως 8 του άρθρου 22 του Ν. 2472/1997[69].

---

[65] Αυτό που ενδιαφέρει στην συγκεκριμένη διάταξη είναι κυρίως όχι η προστασία των στοιχείων και των προγραμμάτων υπολογιστών αλλά η ταυτότητα των δεδομένων, πρβλ. σχετικά Δ. Κιούπη, Οι διατάξεις του Ποινικού Κώδικα για το διαδικτυακό έγκλημα, 3ο Πανελλήνιο Συνέδριο της Ένωσης Ελλήνων Νομικών, e-ΘΕΜΙΣ, Το Δίκαιο στην ψηφιακή εποχή, σελ. 157 και Χ. Μυλωνόπουλου, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ 71-85, για την ανάλυση του άρθρου.

[66] *«Άρθρο 370Γ […]*

2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα (29,00) ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

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

4. Οι πράξεις, των παραγράφων 1 έως 3 διώκονται ύστερα έγκληση».

[67] Πρόκειται για διάταξη που ποινικοποιεί την παραβίαση τυπικού απορρήτου και είναι αδιάφορη η ταυτότητα των δεδομένων, πρβλ. σχετικά Δ. Κιούπη, Οι διατάξεις του Ποινικού Κώδικα για το διαδικτυακό έγκλημα, 3ο Πανελλήνιο Συνέδριο της Ένωσης Ελλήνων Νομικών, e-ΘΕΜΙΣ, Το Δίκαιο στην ψηφιακή εποχή, σελ.158 και Χ. Μυλωνόπουλου, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991 σελ. 86-98, για τη ανάλυση του άρθρου.

[68] *«Άρθρο 15*

Ποινικές κυρώσεις

1. Όποιος, κατά παράβαση του παρόντος νόμου, χρησιμοποιεί, συλλέγει, αποθηκεύει, λαμβάνει γνώση, αφαιρεί, αλλοιώνει, καταστρέφει, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, ή τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των

εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον δέκα χιλιάδων ευρώ (10.000) μέχρι και εκατό χιλιάδων ευρώ (100.000), αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

2. Υπεύθυνος επεξεργασίας και τυχόν εκπρόσωπος του που δεν συμμορφώνεται με τις πράξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που επιβάλλουν τις διοικητικές κυρώσεις της προσωρινής ανάκλησης αδείας, της οριστικής ανάκλησης αδείας και της καταστροφής αρχείου ή διακοπής επεξεργασίας και καταστροφής των σχετικών δεδομένων, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον δώδεκα χιλιάδων ευρώ (12.000) μέχρι και εκατόν είκοσι χιλιάδων ευρώ (120.000).

3. Εφόσον ο δράστης των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να βλάψει τρίτο, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή τουλάχιστον δεκαπέντε χιλιάδων ευρώ (15.000) μέχρι και εκατόν πενήντα *χιλιάδων ευρώ (150.000). Αν προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή πενήντα χιλιάδων ευρώ (50.000) μέχρι και τριακοσίων πενήντα χιλιάδων ευρώ (350.000).*

4. Εφόσον οι πράξεις των παραγράφων 1 και 2 του παρόντος άρθρου τελεστούν από αμέλεια, επιβάλλεται φυλάκιση μέχρι δεκαοκτώ (18) μηνών και χρηματική ποινή μέχρι και δέκα χιλιάδων ευρώ (10.000).»

[69] *«4. Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) έως δέκα εκατομμυρίων (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.*

5. Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις αποφάσεις της Αρχής που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης, σύμφωνα με την παρ. 4 του άρθρου 12, για την ικανοποίηση του δικαιώματος αντίρρησης, σύμφωνα με την παρ. 2 του άρθρου 13, καθώς και με πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ', δ' και ε' της παρ. 1 του άρθρου 21 τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και με χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών. Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9 καθώς και εκείνος που δεν συμμορφώνεται προς την δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

6. Αν ο υπαίτιος των πράξεων των παρ. 1 έως 5 του παρόντος άρθρου είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, ή να βλάψει τρίτον, επιβάλλεται κάθειρξη έως δέκα (10) ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

7. Αν από τις πράξεις των παρ. 1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή τουλάχιστον πέντε εκατομμυρίων (5.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

8. Αν οι πράξεις των παρ. 1 έως 5 του παρόντος άρθρου τελέσθηκαν από αμέλεια, επιβάλλεται φυλάκιση έως τριών (3) ετών και χρηματική ποινή.»

Επισημαίνεται δε, ότι η πρώτη διάταξη που αφορά την επεξεργασία προσωπικών δεδομένων συγκεκριμένα στο πεδίο των υπηρεσιών ηλεκτρονικών επικοινωνιών υπερισχύει της δεύτερης ως ειδικότερη σε αυτές τις περιπτώσεις.[70]

Στην ίδια λογική σε περιπτώσεις που τα δεδομένα πληρούν τις προϋποθέσεις που απαιτεί ο νόμος για να χαρακτηρισθούν ως έργα, έχει εφαρμογή το άρθρο 66 παρ. Ν 2121/1993 για την πνευματική ιδιοκτησία.

Τέλος, ελλείψει διάταξης στον Π.Κ. για την προστασία της ακεραιότητας των ηλεκτρονικών δεδομένων και των συστημάτων πληροφοριών υποστηρίχθηκε η εφαρμογή της διάταξης του άρθρου 381 Π.Κ. για την φθορά ξένης ιδιοκτησίας όπως θα αναλυθεί εκτενέστερα στο σχετικό χωρίο της παρούσας.

5.2. Οι διατάξεις ουσιαστικού ποινικού δικαίου του Ν. 4411/2016

Με τον νόμο 4411/2016 κυρώθηκε η Σύμβαση για το έγκλημα στον κυβερνοχώρο και το Πρόσθετο Πρωτόκολλο αυτής καθώς επίσης μεταφέρθηκε στην ελληνική έννομη τάξη η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

5.2.1. Οι επιμέρους τροποποιήσεις του Ποινικού Κώδικα

Στο άρθρο δεύτερο του δευτέρου μέρους του Ν. 4411/2016 παρατίθενται οι διατάξεις ουσιαστικού ποινικού δικαίου, οι οποίες είναι απαραίτητες για την προσαρμογή της ελληνικής νομοθεσίας στη Σύμβαση και την εναρμόνιση της ελληνικής νομοθεσίας με την Οδηγία (άρθρα 2, 3, 4, 5, 6, 7, 9 παράγραφοι 2, 3, 4 αυτής).

Επισημαίνεται ότι, στην παρούσα μελέτη, κρίθηκε σκόπιμο η παράθεση των ως άνω διατάξεων να γίνει με βάση την σειρά, η οποία ακολουθείται στην Σύμβαση του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα[71] καθώς η σειρά, με την οποία παρατίθενται οι τροποποιήσεις στον Ν. 4411/2016, η οποία είναι σύμφωνα με τον αύξοντα αριθμό των άρθρων του Π.Κ. τα οποία προστίθενται ή τροποποιούνται, είναι νοηματικά αυθαίρετη και δεν ανταποκρίνεται στην ανάγκη κατάδειξης της νοηματικής σχέσης μεταξύ των εγκλημάτων που στρέφονται κατά πληροφοριακών συστημάτων.

---

[70] πρβλ. Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1069

[71] Με εξαίρεση τις διατάξεις που ποινικοποιούν τις προπαρασκευαστικές πράξεις της παραγωγής και της διάθεσης με βάση το άρθρο 6 της Σύμβασης και το άρθρο 7 της Οδηγίας, η οποίες παρατίθενται μετά το έγκλημα στο οποίο αναφέρονται καθώς ο Έλληνας νομοθέτης επέλεξε να μην θέσπιση ένα γενικό έγκλημα που να περιλαμβάνει συλλήβδην τις ως άνω προπαρασκευαστικές πράξεις αλλά αποφάσισε να θεσπίσει ειδικά εγκλήματα για κάθε μία από τις ξεχωριστές εγκληματικές πράξεις. Οι διατάξεις αυτές, ωστόσο, αναλύονται συλλήβδην στο τελευταίο κεφάλαιο της παρούσας.

5.2.1.1. Ορισμός των όρων «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα»

Η πρώτη παράγραφος του άρθρου δεύτερου του Ν. 4411/2016 ορίζει ότι το άρθρο 13 του Π.Κ., με στοιχεία η΄ και θ΄, εισάγονται, δύο πρόσθετοι ορισμοί, του πληροφοριακού συστήματος και των ψηφιακών δεδομένων, οι οποίοι περιέχονται στη Σύμβαση και την Οδηγία και είναι απαραίτητοι για την ερμηνεία τόσο των νέων διατάξεων που εισάγονται στον Ποινικό Κώδικα, όσο και εκείνων που τροποποιούνται με τον παρόντα νόμο.

Συγκεκριμένα η πρώτη παράγραφος του άρθρου δεύτερου του Ν. 4411/2016 προβλέπει ότι:

«1. Στο άρθρο 13 του Ποινικού Κώδικα προστίθενται περιπτώσεις η΄ και θ΄ ως εξής:

«η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».»

5.2.1.2. Αντικατάσταση του άρθρου 370Γ Π.Κ. – Παράνομη πρόσβαση σε πληροφοριακό σύστημα

i. Η διάταξη

Με την έκτη παράγραφο του άρθρου δεύτερου του νόμου 4411/2016 ουσιαστικά τροποποιείται το ήδη ισχύον άρθρο 370Γ Π.Κ. εναρμονιζόμενο με τις απαιτήσεις των διατάξεων του άρθρου 2 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στο κυβερνοχώρο και του άρθρου 3 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

Συγκεκριμένα η διάταξη του ως άνω άρθρου έχει πλέον ως εξής:

«Άρθρο 370Γ – Παράνομη πρόσβαση σε πληροφοριακό σύστημα

1. Οποίος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

2. Οποίος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχειά που μεταδίδονται με συστήματα τηλεπικοινωνίων, παραβιάζοντας

απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κάτοχου του πληροφοριακού συστήματος ή των στοιχειών, η πράξη της προηγούμενης παραγράφου τιμωρείται μονό αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από εγγραφή απόφαση του κάτοχου ή αρμοδίου υπάλληλου του.

4. Οι πράξεις των παραγραφών 1 έως 3 διώκονται υστέρα από έγκληση».

ii. Σύγκριση με το προγενέστερο νομοθετικό καθεστώς

Αρχικά, θα πρέπει να επισημανθεί ότι, παρά το γεγονός ότι το άρθρο υπό την καινούρια του διατύπωση αποκτά τον τίτλο «Παράνομη πρόσβαση σε πληροφοριακό σύστημα», ωστόσο, το άρθρο αυτό στην πρώτη του παράγραφο διατηρεί αυτούσια την προγενέστερη διάταξη που προστέθηκε με το άρθρο 4 του Ν 1805/1988 και απαγορεύει την χωρίς δικαίωμα αντιγραφή και χρησιμοποίηση προγραμμάτων υπολογιστών (γνωστή και ως «πειρατεία»)[72], η οποία σε καμία περίπτωση δεν δύναται να υπαχθεί στην έννοια του τίτλου αυτού[73]. Πρόκειται, συνεπώς, εν προκειμένω, για μια νομοθετική αστοχία η οποία ωστόσο δεν έχει ουσιαστικές συνέπειες αλλά αξίζει να επισημανθεί[74].

Ειδικότερα, οι αλλαγές που επήλθαν στο άρθρο 370Γ Π.Κ. εντοπίζονται αποκλειστικά στην δεύτερη παράγραφο αυτού. Συγκεκριμένα, με βάση την προγενέστερη διατύπωση της ως άνω διάταξης[75] τιμωρούταν αποκλειστικά η χωρίς δικαίωμα πρόσβαση σε στοιχεία που

[72] Η διάταξη αυτή ταυτίζεται κατά περιεχόμενο με τη διάταξη του άρθρου 370Β Π.Κ. στο μέτρο που αφορά περιπτώσεις πειρατείας με μόνη εξαίρεση ότι η τελευταία απαιτεί επιπλέον τα προγράμματα υπολογιστών να συνιστούν κρατικά επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, αυτό που ενδιαφέρει δηλαδή είναι η ταυτότητα των προγραμμάτων, πρβλ. σχετικά Δ. Κιούπη, Οι διατάξεις του Ποινικού Κώδικα για το διαδικτυακό έγκλημα, 3ο Πανελλήνιο Συνέδριο της Ένωσης Ελλήνων Νομικών, e-ΘΕΜΙΣ, Το Δίκαιο στην ψηφιακή εποχή, σελ. 157-158 για το κατά πόσο η περιπτώσεις που υπάγονται στη συγκεκριμένη διάταξη καλύπτονται ήδη από άρθρα 2 παρ. 3 και 66 Ν. 2121/1993 περί προστασίας της πνευματικής ιδιοκτησίας και των εκεί προβληματισμό για υπερβολική διεύρυνση των αξιόποινων περιπτώσεων.

[73] πρβλ. Χ. Μυλωνόπουλου, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ 87-89 για την περαιτέρω ανάλυση της διάταξης.

[74] Η διάταξη αυτή δεδομένου ότι δεν συνιστά επίθεση κατά πληροφοριακού συστήματος δεν θα μας απασχολήσει στην παρούσα εργασία. Για εκτενή ανάλυση βλ. Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1071-1075.

[75] *«2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα,*

μεταδίδονται με συστήματα τηλεπικοινωνιών. Η πρόβλεψη αυτή διατηρείται[76], επιπλέον όμως προστίθεται στην αντικειμενική υπόσταση του εγκλήματος και η χωρίς δικαίωμα πρόσβαση στο σύνολο ή σε τμήμα ενός πληροφοριακού συστήματος. Η νέα αυτή πρόβλεψη επιβάλλεται ευθέως από τα άρθρα 2 της Σύμβασης και 3 της Οδηγίας. Αντίθετα, η διατηρηθείσα πρόβλεψη που απαγορεύει την πρόσβαση σε στοιχεία που μεταδίδονται μέσω συστημάτων τηλεπικοινωνιών όπως είναι διατυπωμένη δεν ανταποκρίνεται σε κάποια υποχρέωση που να ανέλαβε η χώρα μας με βάση είτε την Σύμβαση είτε την Οδηγία. Πράγματι το περιεχόμενο του όρου «στοιχεία» δεν διευκρινίζεται, αν και θα πρέπει να γίνει δεκτό ότι αναφέρεται σε δεδομένα. Αν, περαιτέρω, όπως ισχύει πιθανότατα, με τον όρο αυτό νοούνται τα δεδομένα ως «ψηφιακά[77]» - «ηλεκτρονικά[78]» υπό την ιδιότητα τους δηλαδή να προστατεύονται καθ' αυτά ανεξαρτήτως του περιεχομένου τους τότε η συγκεκριμένη διάταξη είναι πλέον περιττή καθώς καλύπτεται νοηματικά από την νέα διάταξη που ποινικοποιεί την πρόσβαση σε πληροφοριακά συστήματα (στα οποία αυτονοήτως συγκαταλέγονται και τα συστήματα τηλεπικοινωνιών[79] και), τα οποία περιλαμβάνουν, σύμφωνα με τον ορισμό που δίνεται στην περίπτωση η' του άρθρου 13 Π.Κ. όπως εκτέθηκε ανωτέρω, και τα ψηφιακά δεδομένα. Αν, από την άλλη, παρ' ελπίδα, ήθελε κριθεί ότι με τον ορό στοιχεία νοούνται τα απόρρητα – προσωπικά δεδομένα, τότε, και σε αυτή την περίπτωση, η εν λόγω διάταξη είναι περιττή καθώς καλύπτεται νοηματικά, αν όχι από τις διατάξεις των ειδικών νόμων για τα προσωπικά δεδομένα[80], από την διάταξη του αμέσως επόμενου άρθρου υπ' αριθμ. 370Δ όπως αυτό εισήχθη στον Π.Κ. με τον παρόντα νόμο.[81]

ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα (29,00) ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.»

[76] πρβλ. Χ. Μυλωνόπουλου, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991, σελ 90-98, σχετικά με την ανάλυση της εν λόγω διάταξης.

[77] όπως αναφέρονται στην περίπτωση θ' του άρθρου 13 ΠΚ.

[78] όπως αναφέρονται στο άρθρο 381Α Π.Κ. όπως αυτό εισήχθη με τον υπό κρίση νόμο 4411/2016.

[79] πρβλ. σχετικά Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999 σελ. 128-129 και επ. έως σελ. 124 όπου επισημαίνεται η κάλυψη του περιεχομένου του άρθρου 370Α αναφορικά με το απόρρητο των τηλεφωνικών επικοινωνιών από το άρθρο 370Γ παρ. 2 ήδη όπως ίσχυε πριν από την τροποποίησή του με το Ν. 4411/2016. Ωστόσο το άρθρο 370Α υπερισχύει ως ειδικότερο αν και παραδόξως απειλεί με ηπιότερο πλαίσιο ποινής.

[80] βλ. ανωτέρω σελ. 50 υποσημ. 68 και 69 για το κείμενο των διατάξεων.

[81] βλ. κατωτέρω τη σύγκριση με το άρθρο 370Γ παρ. 2 Π.Κ.

iii. Σύγκριση με τις διατάξεις του άρθρου 2 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στο κυβερνοχώρο και του άρθρου 3 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών

Αναφορικά με τον τρόπο τυποποίησης του εγκλήματος της παράνομης πρόσβασης σε πληροφοριακό σύστημα, σε σχέση με τις υποχρεώσεις που ανέλαβε από την Σύμβαση και από την Οδηγία, αξίζει να γίνουν δύο παρατηρήσεις. Πρώτον, ο Έλληνας νομοθέτης επέλεξε να θέσει ως στοιχείο της αντικειμενικής υπόστασης του την παραβίαση κάποιου μέτρου ασφαλείας (λ.χ. κωδικού πρόσβασης ή βιομετρικής ταυτοποίησης), επιλογή που κρίνεται ως εξαιρετικά ορθή καθώς συμβαδίζει με το πνεύμα του ποινικού δικαίου σύμφωνα με το οποίο η ποινή θα πρέπει να είναι το έσχατο μέτρο (ultimum refugium). Στο άρθρο 2 της Σύμβασης η προϋπόθεση αυτή για την τέλεση του εγκλήματος του Συμβουλίου αφήνεται στην διακριτική ευχέρεια του εθνικού νομοθέτη. Περαιτέρω, στην ίδια λογική, το άρθρο 3 της Οδηγίας δεν επιβάλει την μη ποινικοποίηση όταν δεν παραβιάζεται μέτρο ασφαλείας, αν και το ζήτημα είχε απασχολήσει τη συντακτική επιτροπή και τις συζητήσεις στο Ευρωπαϊκό Κοινοβούλιο, αλλά επιβάλει την ποινικοποίηση τουλάχιστον σε αυτές τις περιπτώσεις που έχει υπάρξει παραβίαση μέτρου ασφαλείας. Τέλος, σε αντίθεση με την διάταξη του άρθρου 3 της Οδηγίας το οποίο απαιτεί η παράνομη πρόσβαση να ποινικοποιείται όταν δεν πρόκειται για περιπτώσεις ήσσονος σημασίας, στο άρθρο 370Γ παρ. 2 Π.Κ. δεν περιέχει αυτή την εξαίρεση, κάτι που φαίνεται καθιστά τη διάταξη αυτή κάπως ανελαστική. Ωστόσο, ο όρος «ήσσονος σημασίας» έχει επικριθεί ως υπερβολικά αόριστος σε τέτοιο βαθμό που να μην συμβαδίζει με την αρχή της νομιμότητας που διέπει το ποινικό δίκαιο και επομένως θα μπορούσε να ενσωματωθεί στην εθνική διάταξη μόνο αν εξειδικευόταν επαρκώς.

iv. Τρόπος τέλεσης του εγκλήματος και συρροή του τρόπου τέλεσης με άλλα εγκλήματα

Η συμπεριφορά αυτή τελείται συνηθέστερα όταν παραβιάζεται ή παρακάμπτεται ο κωδικός πρόσβασης (password), όπως ορίζει το άρθρο, είτε στο σύνολο ή τμήμα πληροφοριακού συστήματος, είτε σε στοιχεία που μεταδίδονται μέσω συστημάτων τηλεπικοινωνιών. Ωστόσο, είναι δυνατό να τελεστεί και με άλλους τρόπους όπως η παράκαμψη βιομετρικής ταυτοποίησης (λ.χ. προσώπου ή δακτυλικού αποτυπώματος) ή η παραβίαση ή η παράκαμψη του συστήματος ελέγχου ταυτότητας δύο παραγόντων (two factor verirification system).

Ο όρος παράνομη πρόσβαση σε πληροφοριακό σύστημα δεν θα πρέπει να ταυτίζεται με τον όρο «hacking». Το hacking είναι η διαδικασία κατά την οποία ο δράστης εντοπίζει τα

κενά ασφαλείας ενός συστήματος και στην συνέχεια αποκτά πρόσβαση σε αυτό. Η πρόσβαση αυτή μπορεί να γίνει με δύο τρόπους: α) είτε απλώς με την εύρεση και την εισαγωγή ορθών στοιχείων σε ένα πληροφοριακό σύστημα, β) είτε με συνδυασμό εισαγωγής ορθών στοιχείων και αλλοίωσης δεδομένων παρακωλύοντας όχι τη λειτουργία του συστήματος συνολικά (αν και δεν αποκλείεται) αλλά μόνο τη λειτουργία ελέγχου πρόσβασης λ.χ. με τη χρήση Δούρειων Ίππων οι οποίοι εγκαθιστούν σχετικά προγράμματα στο σύστημα[82], ή με επιθέσεις άρνησης υπηρεσιών[83] και αντίστοιχες τεχνικές με τις οποίες ο δράστης αποκτά άμεσα πρόσβαση στο σύστημα.

Η πρώτη περίπτωση, θα λέγαμε ότι, αποτελεί την απλή μορφή hacking και ομοιάζει με ένα συνδυασμό των δύο τελευταίων περιπτώσεων του εγκλήματος της απάτης με υπολογιστή του άρθρου 386Α Π.Κ., όπως αυτό διαμορφώθηκε με τον υπό κρίση νόμο 4411/2016, ήτοι με τη χωρίς δικαίωμα χρήση δεδομένων και τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, χωρίς ωστόσο να έχει το σκοπό παράνομου περιουσιακού οφέλους.

Η δεύτερη περίπτωση, όπου ο δράστης επιπλέον αλλοιώνει τα δεδομένα του υπολογιστή συνιστά και φθορά ηλεκτρονικών δεδομένων όπως αυτή τυποποιήθηκε στο άρθρο 381Α Π.Κ. με τον παρόντα νόμο. Δεδομένου δε, ότι με το τελευταίο αυτό άρθρο, προστατεύεται το έννομο αγαθό της ακεραιότητας των ψηφιακών δεδομένων και με το έγκλημα της παράνομης πρόσβασης προστατεύεται το έννομο αγαθό της ασφάλειας (συμπεριλαμβανομένης της ακεραιότητας) των πληροφοριακών συστημάτων (συμπεριλαμβανομένων των δεδομένων τους) ή σε κάθε περίπτωση με βάση την Οδηγία το έννομο αγαθό των συστημάτων πληροφοριών καθ' αυτών[84], θα πρέπει να γίνει δεκτό ότι η πράξη της αλλοίωσης του άρθρου 381Α Π.Κ. συρρέει με την πράξη της πρόσβασης του άρθρου 370Γ παρ. 2 Π.Κ. φαινομενικά.

---

[82] Πρόκειται για προγράμματα που παραπλανούν το χρήστη να τα εγκαταστήσει και μέσω αυτών ο δράστης μπορεί να αποκτήσει πρόσβαση στο σύστημα, ή (και) να μεταδώσει κάποιον ιό αλλά και οτιδήποτε άλλο ανάλογα με το σκοπό του λ.χ. χρησιμοποίηση της επεξεργαστικής ισχύος του υπολογιστή του θύματος για την εξόρυξη - mining κρυπτονομισμάτων ή την κατανεμημένη επίθεση άρνησης υπηρεσιών (βλ. αμέσως κατωτέρω υπο. 16).

[83] Επιθέσεις άρνησης υπηρεσιών (DoS attacks) κατά πληροφοριακών συστημάτων συμπεριλαμβανομένων και των δικτύων τηλεπικοινωνιών τελούνται με την αποστολή τεράστιου όγκου αιτημάτων προς αυτά με αποτέλεσμα αυτά να υπερφορτώνονται και είτε να καταρρέουν (δηλαδή να βγαίνουν εκτός λειτουργίας) είτε να μη μπορούν να εξυπηρετήσουν πραγματικά αιτήματα. Η κυριότερη μορφή των επιθέσεων αυτών χρησιμοποιεί πολλαπλές επιθέσεις μέσω άλλων θυμάτων ή και συνεργών και είναι γνωστή ως κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS attacks).

[84] βλ. αναλυτικότερα. κατωτέρω, κεφ. v. «Το προστατευόμενο έννομο αγαθό».

Θα συρρέει δε και πραγματικά διότι με άλλη πράξη καθίσταται ανενεργή ή δυσλειτουργική η λειτουργία ελέγχου πρόσβασης στο πληροφοριακό σύστημα και με άλλη πράξη εισαγωγής τυπικά ορθών δεδομένων γίνεται η είσοδος στο πληροφοριακό σύστημα και αποκτάται πρόσβαση σε αυτό και τα δεδομένα του. Επομένως δεδομένου ότι η πράξη της αλλοίωσης των ηλεκτρονικών δεδομένων γίνεται με σκοπό την τέλεση της πράξης της παράνομης πρόσβαση στο πληροφοριακό σύστημα, η δεύτερη απορρόφα την πρώτη, της οποίας η απαξία συνεκτιμάται κατά την επιμέτρηση της ποινής.

Ωστόσο, το hacking, είτε τελείται ως αυτοσκοπός, είτε, συνηθέστερα, με σκοπό την τέλεση κάποιου άλλου εγκλήματος (cracking), δεν είναι ο μόνος τρόπος να αποκτήσει κανείς χωρίς δικαίωμα πρόσβαση σε ένα πληροφοριακό σύστημα. Το hacking εντάσσεται σε μια ευρύτερη κατηγορία μεθόδων απόκτησης πρόσβασης, οι οποίες γίνονται με τη χρήση πληροφοριακών προγραμμάτων. Στην κατηγορία αυτή εντάσσονται επίσης τεχνικές όπως αυτή του pharming[85], όπου ο δράστης δεν αποκτά άμεσα πρόσβαση στο σύστημα αλλά έμμεσα μαθαίνοντας τους κωδικούς πρόσβασης. Η δεύτερη μεγάλη κατηγορία μεθόδων απόκτησης πρόσβασης αφορά επίσης περιπτώσεις που ο δράστης αποκτά πρόσβαση με έμμεσο τρόπο μαθαίνοντας τους κωδικούς του θύματος χωρίς τη χρήση κάποιου προγράμματος. Αυτές οι μέθοδοι είναι οι λεγόμενες εξωπρογραμματιστικές[86] (που δεν γίνονται δηλαδή με τη χρήση προγραμμάτων[87]) ή, κατ' άλλη ορολογία, τεχνικές «συλλογής πληροφοριών» (information gathering), στις οποίες περιλαμβάνονται τακτικές όπως το phishing[88] και η «παραδοσιακή» υποκλοπή[89] και η λεγόμενη «κοινωνική μηχανική» («social

[85] Ο δράστης χρησιμοποιεί πρόγραμμα που αναδρομολογεί τους χρήστες συγκεκριμένης ιστοσελίδας σε άλλη όμοια ή πανομοιότυπη ιστοσελίδα από αυτή που έχουν εισάγει στο πρόγραμμα περιήγησης του διαδικτύου. Όταν οι χρήστες θεωρώντας ότι βρίσκονται την γνήσια σελίδα εισάγουν τα στοιχεία τους και τον κωδικό εισόδου, ο δράστης λαμβάνει γνώση των στοιχείων αυτών και αποκτά πρόσβαση στο λογαριασμό. Επισημαίνεται ότι με την τεχνική αυτή του pharming τελείται πλαστογραφία με υπολογιστή, βλ. σχετικά Δ. Κιούπη, Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ευρωπαϊκή Ένωση, Δικηγορικός Σύλλογος Πειραιά – Ένωση Ελλήνων Ποινικολόγων – Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, 2010, σελ. 205-206 με εκεί παραπομπή αναφορικά με την ιστοσελίδα ως έγγραφο.

[86] βλ. αναλυτικότερα Φ. Σπυρόπουλου, Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking) σελ 93-101.

[87] Ωστόσο, είναι δυνατή η δημιουργία προγραμμάτων που να εξυπηρετούν τις μεθόδους αλλά το θύμα δεν χρησιμοποιεί το πρόγραμμα αλλά το προϊόν του, λ.χ. την επιστολή ηλεκτρονικού ταχυδρομείου με την οποία γίνεται «επίθεση» phishing, (για το τι είναι phishing βλ. αμέσως κατωτέρω την επόμενη υπ. 90).

[88] Το θύμα λαμβάνει ηλεκτρονική επιστολή που υποτίθεται ότι προέρχεται από κάποια εταιρία στην οποία το θύμα έχει λογαριασμό όπως λ.χ. από μια τράπεζα, στην οποία καλείται να απαντήσει στέλνοντας προσωπικά

engineering»)[90]. Όπως είναι αυτονόητο οι συμπεριφορές, αυτές με τις οποίες ο δράστης δεν αποκτά άμεσα πρόσβαση αλλά με κάποιο τρόπο μαθαίνει τον κωδικό που είναι απαραίτητος για να αποκτήσει πρόσβαση, δεν τιμωρούνται με το άρθρο 370Γ παρ. 2 το οποίο ποινικοποιεί αποκλειστικά την πράξη της μη εξουσιοδοτημένης πρόσβασης[91] αλλά πιθανόν να ποινικοποιούνται με άλλες διατάξεις οι οποίες συρρέουν με αυτό πραγματικά όταν τελικά ο δράστης αποκτά πρόσβαση.

Τέλος, υποστηρίζεται ότι και η εγκατάσταση κακόβουλου λογισμικού σε ένα πληροφοριακό σύστημα συνιστά «απόκτηση πρόσβασης» σε αυτό.[92] Αυτή η άποψη διευρύνει την παραδοσιακή έννοια του όρου «πρόσβαση» που όλοι έχουμε κατά νου και η οποία μπορεί να νοηθεί ότι υπάρχει μόνο στις περιπτώσεις που ένα κακόβουλο πρόγραμμα παρέχει στο δράστη τη δυνατότητα ελέγχου του συστήματος (το λεγόμενο «rootkit»). Τα

του στοιχεία ή στοιχεία του λογαριασμού του. Ο δράστης έτσι παραπλανά το θύμα του και αποκτά τα στοιχεία που χρειάζεται, δεν παρεμβαίνει δηλαδή στα στοιχεία του υπολογιστή αλλά επιχειρεί να δημιουργήσει πλάνη στο νοητικό του θύματος, πρβλ. Δ. Κιούπη, Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ευρωπαϊκή Ένωση, Δικηγορικός Σύλλογος Πειραιά – Ένωση Ελλήνων Ποινικολόγων – Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, 2010, σελ. 200-202.

[89]Αναφέρεται στο σημείο αυτό μόνο η «παραδοσιακή» υποκλοπή διότι τεχνικές υποκλοπής που τελούνται με την βοήθεια προγραμμάτων όπως η «καταγραφή πλήκτρων» («key logger») εντάσσονται στην έννοια του hacking και συνήθως τα προγράμματα αυτά εγκαθίστανται στον υπολογιστή του θύματος ως Δούρειοι Ίπποι. Ωστόσο και η χρήση προγραμμάτων υποκλοπής μπορεί να ενταχθεί σε αυτές τις περιπτώσεις όταν ο δράστης έχει αποκτήσει πρόσβαση σε υπολογιστή και θέλει περαιτέρω να αποκτήσει πρόσβαση και σε άλλο πληροφοριακό σύστημα λ.χ. που φιλοξενεί κάποιο διαδικτυακό λογαριασμό του θύματος.

[90] Μια πολύ συχνή στην πράξη περίπτωση συλλογής πληροφοριών με «κοινωνική μηχανική» (όπου ο δράστης ξεγελά το θύμα να του παραδώσει τα στοιχεία πρόσβασης ή στοιχεία από τα οποία προκύπτουν τα στοιχεία πρόσβασης) είναι αυτή κατά την οποία ο δράστης πληροφορείται τηλεφωνικώς τα απαραίτητα απόρρητα στοιχεία για την πρόσβαση σε ένα πληροφοριακό σύστημα (λ.χ. όνομα χρήστη και κωδικό) από έναν υπάλληλο μιας εταιρίας προσποιούμενος ότι καλεί από το τμήμα τεχνικής υποστήριξης (I.T. Department) δήθεν για τον έλεγχο ή την επίλυση κάποιου προβλήματος («pretexting»).

[91] πρβλ. Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1066

[92] βλ. Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999 σελ. 141, καθώς και Μ. Καϊάφα – Γκμπάντι, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 489 επ., η οποία συμφωνεί με την άποψη αυτή βασιζόμενη επίσης στο γεγονός ότι το έγκλημα της παράνομης πρόσβασης δεν απαιτεί και λήψη γνώσης των δεδομένων του πληροφοριακού συστήματος αλλά απλώς θεμελιώνεται με την διάσπαση των μέτρων ασφαλείας.

υπόλοιπα προγράμματα που επεμβαίνουν στο σύστημα[93] δεν παρέχουν πρόσβαση στο δράστη στο πληροφοριακό σύστημα παρά μόνο στο μέτρο που είναι προγραμματισμένα να εκτελέσουν μια συγκεκριμένη λειτουργία. Πρόκειται, συνεπώς για μια μορφή έμμεσης αυτουργίας πρόσβασης σε πληροφοριακό σύστημα καθώς το θύμα παραπλανάται και εγκαθιστά το πρόγραμμα το οποίο για λογαριασμό του δράστη επεμβαίνει στο σύστημα χωρίς ο τελευταίος να αποκτά πρόσβαση σε αυτό υπό την stricto sensu έννοιας της. Επομένως, η εγκατάσταση κακόβουλου λογισμικού σε πληροφοριακό σύστημα, η οποία γίνεται όχι με συναίνεση αλλά με παραπλάνηση του θύματος, θα πρέπει να γίνει δεκτό με βάση ιστορική ερμηνεία ότι πράγματι συνιστά το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα. Μάλιστα, υπό αυτή την άποψη, το πρόγραμμα δεν χρειάζεται να είναι καν κακόβουλο υπό την έννοια του νόμου, δηλαδή δεν απαιτείται η λειτουργεία του να πληροί την αντικειμενική υπόσταση κάποιου άλλου εγκλήματος, πληροφοριακού ή μη. Η παραδοχή αυτή είναι πολύ σημαντική διότι έτσι ποινικοποιούνται συμπεριφορές όπως η εγκατάσταση λογισμικού ανεπιθύμητων διαφημίσεων («adware») ή λογισμικού που εν αγνοία του χρήστη εντάσσει το πληροφοριακό σύστημα σε ένα οργανωμένο δίκτυο (botnet) είτε για την ομαδική «εξόρυξη» κρυπτονομισμάτων («pool mining») είτε για την τέλεση κατανεμημένων επιθέσεων άρνησης υπηρεσιών άλλων πληροφοριακών συστημάτων. Επισημαίνεται δε, ότι τέτοιου είδους προγράμματα ακόμα και αν αποβλέπουν στην αποκόμιση παράνομου περιουσιακού οφέλους σπάνια θα μπορούσαν να θεωρηθούν ότι υπάγονται στο πεδίο εφαρμογής του εγκλήματος της απάτης με υπολογιστή καθώς η περιουσιακή βλάβη του θύματος, αν υπάρχει, είτε συνήθως θα είναι μηδαμινή είτε σχεδόν πάντα δεν θα βρίσκεται σε υλική αντιστοιχία με το περιουσιακό όφελος του δράστη.

v. Το προστατευόμενο έννομο αγαθό

Ο δικαιολογητικός λόγος της ποινικοποιήσεως της παράνομης πρόσβασης συνίσταται στο γεγονός ότι, ο κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος, τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσεως του υπολογιστή ή του συστήματος υπολογιστή. Αποτελεί δηλαδή το άρθρο αυτό, το «ηλεκτρονικό αντίστοιχο» της διατάραξης οικιακής ειρήνης (άρθρο 334 Π.Κ.). Όπως δηλαδή ο δικαιούχος της κατοικίας έχει το δικαίωμα να ορίζει ποιος μπορεί να εισέρχεται και να παραμένει σ' αυτήν, έτσι και ο «δικαιούχος» του ηλεκτρονικού υπολογιστή δικαιούται να ορίζει ποιος θα τον χρησιμοποιεί και ποιος θα έχει πρόσβαση σ' αυτόν.

[93] Σημειωτέον ότι στα άρθρα της Σύμβασης αλλά και της Οδηγίας στα οποία βασίζεται η υπό κρίση διάταξη δεν γίνεται αναφορά σε πρόσβαση σε σύστημα αλλά σε επέμβαση και παρεμβολή αντίστοιχα.

Σύμφωνα, δε, με την Αιτιολογική Έκθεση της Σύμβασης, όπως αναφέρθηκε, το προστατευόμενο έννομο αγαθό της αντίστοιχης διάταξης είναι η ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων τους, δηλαδή η πρόληψη της πρόσβασης από μη εξουσιοδοτημένα άτομα περαιτέρω. Η ασφάλεια, δε, των πληροφοριακών συστημάτων και των δεδομένων τους περιλαμβάνει ειδικότερα την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητά τους. Θα πρέπει, λοιπόν, να γίνει δεκτό, ότι πρόκειται για ένα έγκλημα που προστατεύει αφηρημένα τα συστήματα και τα ηλεκτρονικά δεδομένα σε πρώτο επίπεδο πριν από την τέλεση κάποιου άλλου πληροφοριακού εγκλήματος το οποίο να στρέφεται κατά κάποια συγκεκριμένης πτυχής του εννόμου αυτού αγαθού. Σε κάθε περίπτωση, πάντως, η Οδηγία ανάγει τα πληροφοριακά συστήματα και τα δεδομένα τους σε αυτοτελές έννομο αγαθό, το οποίο μάλιστα θα πρέπει γίνει δεκτό ότι εξειδικεύεται κατά περίπτωση σύμφωνα με τα όσα αναφέρονται στο Προοίμιό της, στην ίδια τη Σύμβαση αλλά και την Αιτιολογική της Έκθεση.

Ωστόσο, ο Έλληνας νομοθέτης επέλεξε να εντάξει την διάταξη που ποινικοποιεί την παράνομη πρόσβαση σε πληροφοριακό σύστημα (άρθρο 370Γ παρ. 2) στο εικοστό δεύτερο κεφάλαιο του Π.Κ. στο οποίο περιλαμβάνονται οι διατάξεις που προστατεύουν το έννομο αγαθό του απορρήτου της επικοινωνίας. Η επιλογή αυτή θα πρέπει, πλέον με βάση τα ερμηνευτικά εργαλεία που παρέχουν τα διεθνή κείμενα, να κριθεί, μάλλον, ως άστοχη, δεδομένου ότι, η εν λόγω διάταξη ποινικοποιεί, απλώς, την πρόσβαση, χωρίς, δηλαδή, να χρειάζεται ο δράστης να λάβει και γνώση του περιεχομένου[94]. Ορθότερο θα ήταν η διάταξη να είχε ενταχθεί στο δέκατο τέταρτο κεφάλαιο του Π.Κ. στο οποίο προστατεύεται μεταξύ άλλων και η ασφάλεια των τηλεπικοινωνιών και στο οποίο εντάχθηκε και το έγκλημα της παρακώλυσης της λειτουργίας πληροφοριακών συστημάτων (άρθρο 292Β Π.Κ.) το οποίο αναλύεται κατωτέρω σε σχετικό χωρίο της παρούσας.

vi. Συρροή της διάταξης του άρθρου 370Γ παρ. 2 (παράνομη πρόσβαση) με άλλα εγκλήματα που συνιστούν επίθεση κατά συστημάτων υπολογιστών

Σύμφωνα και με την Αιτιολογική Έκθεση της Σύμβασης το έγκλημα της παράνομης πρόσβασης αποτελεί την βασικό έγκλημα δηλαδή την πιο απλή μορφή εγκλήματος που στρέφεται κατά της ασφάλειας των συστημάτων υπολογιστών και των δεδομένων τους (δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας τους). Τα λοιπά εγκλήματα τα οποία είτε προστατεύουν την ασφάλεια των συστημάτων υπολογιστών εν γένει είτε συγκεκριμένα λ.χ. την εμπιστευτικότητα τους ή κάποια άλλη πτυχή της ασφάλειας τους,

[94] πρβλ. Μ. Καϊάφα – Γκμπάντι, ο.π.

είτε πρόκειται για εγκλήματα σχετικά με τους υπολογιστές, συνηθέστατα τελούνται αφού ο δράστης αποκτήσει πρόσβαση στο σύστημα ή στα δεδομένα του.

Αν και δεν αποκλείεται στην πράξη τα ως άνω λοιπά εγκλήματα να τελούνται χωρίς ο δράστης να αποκτήσει πρόσβαση στο σύστημα ή τα δεδομένα του είτε πραγματικά είτε έμμεσα (λ.χ. με εξαπάτηση του θύματος και εγκατάσταση κάποιου ιού), όπως συμβαίνει για παράδειγμα σε περιπτώσεις επιθέσεων άρνησης υπηρεσιών που συνιστούν το έγκλημα της παρακώλυσης της λειτουργίας πληροφοριακών συστημάτων, εξαιρετικά σπάνια θα τελείται η πράξη της παράνομης πρόσβασης ως αυτοσκοπός και όχι προς το σκοπό τέλεσης κάποιου άλλου εγκλήματος, συνήθως πληροφοριακού, όπως λ.χ. του εγκλήματος του άρθρου 370Β Π.Κ. το οποίο συνιστά το κάτι παραπάνω σε σχέση με το άρθρο 370Γ παρ. 2 Π.Κ. δηλαδή τη λήψη γνώσης του περιεχομένου των δεδομένων.[95]

Περαιτέρω, θα πρέπει να γίνει δεκτό ότι, όταν ο δράστης αποκτά πρόσβαση στο σύστημα με σκοπό την τέλεση άλλων πληροφοριακών εγκλημάτων συμπεριλαμβανομένων και των σχετικών με του υπολογιστές εγκλημάτων καθώς το έγκλημα της παράνομης πρόσβασης του άρθρου 370Γ παρ. 2 Π.Κ. θα συρρέει με αυτά φαινομενικά πραγματικά καθώς το ευρύ έννομο αγαθό της ασφάλειας των πληροφοριακών συστημάτων δεν αποτελεί απλώς προστάδιο αλλά θα πρέπει μάλιστα να γίνει δεκτό ότι εξειδικεύεται με την τέλεση του εγκλήματος – σκοπού και καλύπτεται από αυτό. Ωστόσο, ο Έλληνας νομοθέτης δεν έλαβε υπόψη το γεγονός ότι τις περισσότερες φορές το έγκλημα της παράνομης πρόσβασης είναι το μέσο για την τέλεση άλλων εγκλημάτων σχετικών με τα πληροφοριακά συστήματα, ούτε ότι προφανώς η συμπεριφορά αυτή σε κάθε περίπτωση έχει λιγότερη απαξία από τα εγκλήματα αυτά. Παραδόξως, λοιπόν, το απειλούμενο πλαίσιο ποινής του άρθρου 370Γ παρ. 2 (ποινή φυλάκισης, δηλαδή φυλάκιση από 10 μέρες έως 5 έτη κατά το άρθρο 53 Π.Κ.) είναι αυστηρότερο από αυτό των πλημμελληματικών μορφών των εγκλημάτων λ.χ. των άρθρων 292Β Π.Κ. (παρακώλυση λειτουργίας πληροφοριακού συστήματος), 381Α Π.Κ. (φθορά ηλεκτρονικών δεδομένων) και 386Α (απάτη με υπολογιστή). Επομένως, τα άρθρα αυτά δεν μπορούν να απορροφήσουν το άρθρο 370Γ παρ. 2 όταν αυτό τελείται προς τον σκοπό τέλεσης τους, και να επιβληθεί ποινή μόνο με βάση το δικό τους πλαίσιο συνυπολογιζόμενης της απαξίας της πράξης της παράνομης πρόσβασης. Η νομοθετική αυτή κακοτεχνία είναι βέβαιο ότι οφείλεται σε απερισκεψία και χρήζει άμεσης τροποποίησης, ώστε να είναι

[95] Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999 σελ. 128-129 και επ. έως σελ. 134 για τη δυνατότητα εφαρμογής του άρθρου 370Β Π.Κ. σε περιπτώσεις απλού hacking και τα προβλήματα που ανακύπτουν.

δικαιοπολιτικά ορθή στο πλαίσιο του συστήματος του ελληνικού ποινικού δικαίου. Αξίζει, δε, μάλιστα, να επισημανθεί ότι η απειλουμένη αυτή ποινή με το άρθρο 370Γ παρ. 2 είναι υπερβολικά αυστηρότερη από τη ρύθμιση του άρθρο 9 της Οδηγίας προβλέπει ότι οι στερητικές τις ελευθερίας ποινές που πρέπει να θεσπίσουν τα Κράτη Μέλη για τα εγκλήματα που προβλέπονται στην Οδηγία πρέπει να έχει ανώτατο όριο τουλάχιστον 2 έτη.

vii. Συρροή με άλλα εγκλήματα

Το περιεχόμενο της διάταξη του άρθρου 370Γ παρ. 2 Π.Κ. καλύπτει την προστασία του απορρήτου των τηλεφωνικών συνομιλιών του άρθρου 370Α Π.Κ.[96], το οποίο ωστόσο όπως εκτέθηκε[97] υπερισχύει ως ειδικότερο. Παράλληλα, επίσης καλύπτεται εννοιολογικά και η περίπτωση παραβίασης επιστολών ηλεκτρονικού ταχυδρομείου, η οποία δεδομένης της διευρυμένης έννοιας του εγγράφου δύναται να υπαχθεί και στο άρθρο 370 Π.Κ[98]. Ωστόσο σε αυτή την περίπτωση θα πρέπει να γίνει δεκτό ότι υπερισχύει η διάταξη του άρθρου 370Γ παρ. 2 Π.Κ. ως ειδικότερη δεδομένου μάλιστα ότι το άρθρο 370Γ Π.Κ. δεν απαιτεί και λήψη γνώσης του περιεχομένου της επιστολής αλλά μόνο σκοπό προς τη λήψη της γνώσης αυτής[99].

Τέλος, ειδικές διατάξεις για την παράνομη πρόσβαση σε δεδομένα αποτελούν το άρθρο 15 του Ν. 3471/2006 και το άρθρο 22 παρ. 4 έως 8 του Ν. 2472/1997 που ποινικοποιούν την παράνομη πρόσβαση σε δεδομένα.[100] Όπως έχει επισημανθεί[101], με βάση το γράμμα του νόμου, οι διατάξεις αυτές που επίσης δεν προϋποθέτουν λήψη γνώσης του περιεχομένου των δεδομένων αυτών και ως εκ τούτου συρρέουν κατ' ιδέαν φαινομενικά και εφαρμόζονται ως ειδικότερες. Σημειώνεται δε ότι δεν υπάρχει αξιολογική αντινομία αφού οι διατάξεις αυτές επαπειλούν βαρύτερη ποινή συγκριτικά με τη διάταξη του άρθρου 370Γ παρ. 2.[102]

---

[96] Για το κείμενο του άρθρου βλ. κατωτέρω υποσημ. 105.

[97] βλ. ανωτέρω σελ. 54 με την εκεί παραπομπή στην υποσημ. 79 σε Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999 σελ. 128-129 και επ. έως σελ. 124.

[98] Δ. Κιούπη, ο.π.

[99] πρβλ. Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1066-1067 όπου γίνεται αναφορά στο παράδοξο με βάση το προγενέστερο νομοθετικό καθεστώς όπου το άρθρο 370Γ παρ. 2 Π.Κ. απειλούσε μικρότερης βαρύτητας ποινές συγκριτικά με το άρθρο 370 Π.Κ.

[100] βλ. ανωτέρω σελ. 50 υποσημ. 68 και 69 για το κείμενο των διατάξεων.

[101] βλ. Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999, σελ.134 -136 όπου γίνεται αναφορά μόνο στο άρθρο 22 του Ν. 2472/1997 δεδομένου ότι ο Ν. 3471/2006 είναι πολύ μεταγενέστερος της έκδοσης του βιβλίου, και. Μ. Καϊάφα – Γκμπάντι, ο.π. σελ 1068 και γενικά έως 1071.

[102] Συγκεκριμένα απειλούν ποινή φυλάκισης τουλάχιστον ενός έτους μέχρι 5 έτη εν αντιθέσει με το άρθρο 370Γ που απειλή ποινή φυλάκισης γενικά δηλ. από 10 μέρες έως 5 έτη.

5.2.1.3. Προσθήκη άρθρου 370Δ Π.Κ. – Παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων

i. Η διάταξη

Με τη έβδομη παράγραφο του άρθρου δεύτερου του νόμου 4411/2016 προστίθεται στον Π.Κ νέα διάταξη του άρθρου 370Δ με την οποία τιμωρείται αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων και η χρήση των πληροφοριών με ποινές αντίστοιχες της παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών που προβλέπονται στη διάταξη του άρθρου 370Α Π.Κ. (κάθειρξη μέχρι δέκα ετών). Αν οι πράξεις αυτές συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146 Π.Κ.. Η διάταξη αυτή βασίζεται στα άρθρα 3 της Σύμβασης (αθέμιτη παγίδευση – υποκλοπή) και 6 της Οδηγίας (παράνομη υποκλοπή) και έχει ως σκοπό σύμφωνα την Αιτιολογική Έκθεση της Σύμβαση την προστασία του εννόμου αγαθού του δικαιώματος στην ιδιωτική ζωή και της ασφάλειας των τηλεπικοινωνιών στον κυβερνοχώρο.

Συγκεκριμένα, η έβδομη παράγραφος του άρθρου δεύτερου του νόμου 4411/2016 ορίζει ότι:

«7. Μετά το άρθρο 370Γ του Ποινικού Κώδικα προστίθεται άρθρο 370Δ ως εξής:

Άρθρο 370Δ

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 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146».

ii. Σύγκριση με τις διατάξεις του άρθρου 3 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στο κυβερνοχώρο και του άρθρου 6 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

Αρχικά αξίζει να επισημανθεί ότι ο Έλληνας νομοθέτης, αντί να διευρύνει το έγκλημα της υποκλοπής του άρθρου 370Α[103] ώστε αυτό να περιλαμβάνει εκτός από περιπτώσεις υποκλοπής τηλεφωνικών συνομιλιών (παρ. 1) και περιπτώσεις υποκλοπής μη δημόσιων διαβιβάσεων δεδομένων και ηλεκτρομαγνητικών εκπομπών, όπως μάλιστα ήταν το σκεπτικό πίσω από τις σχετικές διατάξεις τόσο της Σύμβασης όσο και της Οδηγίας, επέλεξε την δημιουργία ενός νέου αυτοτελούς άρθρου. Η επιλογή αυτή ωστόσο έχει ως συνέπεια το περιεχόμενο του άρθρου 370Α παρ. 1 Π.Κ. να καλύπτεται πλήρως από την νέα διάταξη του άρθρου 370Δ Π.Κ. καθώς η έννοια των μη δημόσιων διαβιβάσεων δεδομένων και ηλεκτρομαγνητικών εκπομπών περιλαμβάνει εννοιολογικά και περιπτώσεις τηλεφωνικών επικοινωνιών, δεδομένου ότι οι τελευταίες δεν αποτελούν τίποτα περισσότερο από των

---

[103] *«Άρθρο 370Α*

Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή τα στοιχεία της θέσης και κίνησης της εν λόγω επικοινωνίας, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου. 2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου. 3. Με κάθειρξη μέχρι δέκα ετών τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου. 4. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι δέκα ετών και χρηματική ποινή από πενήντα πέντε χιλιάδες (55.000) μέχρι διακόσιες χιλιάδες (200.000) ευρώ. 5. Αν οι πράξεις των παραγράφων 1 και 3 αυτού του άρθρου συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, τιμωρούνται κατά τα άρθρα 146 και 147 του Ποινικού Κώδικα.»

συνδυασμό αυτών των δύο στοιχείων (δηλαδή των ηλεκτρονικών δεδομένων και των ηλεκτρομαγνητικών εκπομπών, στις οποίες εντάσσονται και τα ραδιοκύματα).

Επιπλέον, σε αντίθεση με την σχετική διάταξη της Οδηγίας, η οποία δεν επιβάλει την ποινικοποίηση περιπτώσεων ήσσονος σημασίας, η διάταξη του άρθρου 370Δ δεν περιέχει σχετική πρόβλεψη. Ωστόσο, αν και αυτό φαίνεται να καθιστά τη διάταξη αυτή ανελαστική, ο όρος «ήσσονος σημασίας» έχει επικριθεί ως υπερβολικά αόριστος σε τέτοιο βαθμό που να μην συμβαδίζει με την αρχή της νομιμότητας που διέπει το ποινικό δίκαιο. Επομένως, αν η πρόβλεψη αυτή εντασσόταν στο κείμενο της διάταξης θα έπρεπε να προσδιοριζόταν επαρκώς το περιεχόμενο της.

Τέλος, αξίζει να επισημανθεί το πολύ αυστηρότερο πλαίσιο ποινής, που απειλείται, συγκριτικά με το επιβαλλόμενο από την Οδηγία κατώτερο επιτρεπτό ανώτατο όριο του πλαισίου ποινής. Συγκεκριμένα με τη διάταξη του άρθρου 370Δ Π.Κ. επαπειλείται ποινή κάθειρξης έως 10 χρόνια ενώ η Οδηγία στο άρθρο 9 επιβάλει υποχρέωση στα Κράτη Μέλη να θεσπίσουν ως ανώτερο πλαίσιο ποινής τουλάχιστον τα 2 χρόνια στερητικής τη ελευθερίας ποινής. Η αυστηρότατη αυτή πρόβλεψη βασίζεται στο πλαίσιο ποινής της διάταξης του άρθρου 370Α Π.Κ., που προστατεύει το απόρρητο των τηλεφωνικών επικοινωνιών και των μη δημόσιων προφορικών συνομιλιών εν γένει. Ωστόσο η επιλογή αυτή απειλής τόσο αυστηρών ποινών δεν μπορεί να θεωρηθεί δικαιοπολιτικά ορθή καθώς δεν υπακούει σε καμία αναλογία στο πλαίσιο του ελληνικού συστήματος απονομής ποινικής δικαιοσύνης αλλά έγινε προς εξυπηρέτηση πολιτικών σκοπιμοτήτων με άστοχο, μάλιστα, τρόπο.

iii. Τρόπος τέλεσης

Από το συνδυασμό των σκέψεων της Αιτιολογικής Έκθεσης της Σύμβαση και του προοιμίου της Οδηγίας[104] προκύπτει ότι η έννοια της υποκλοπής περιλαμβάνει συμπεριφορές όπως η ακρόαση, η παρακολούθηση, η επιτήρηση, η καταγραφή και η παροχή του περιεχομένου των δεδομένων είτε άμεσα, μέσω της πρόσβασης και χρήσης των συστημάτων πληροφοριών, είτε έμμεσα μέσω της χρήσης ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα.[105]

Περαιτέρω το έγκλημα της υποκλοπής αφορά σε «μη δημόσιες» εκπομπές ηλεκτρονικών δεδομένων. Ο όρος «μη δημόσιες» αφορά τη φύση των εκπομπών και όχι τη φύση των

[104] Βλ. ανωτέρω τα σχετικά χωρία με τις σχετικές παραπομπές.

[105] Σκέψη 9 του Προοιμίου της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

δεδομένων. Τα δεδομένα δύναται να είναι ελεύθερα διαθέσιμα αλλά τα μέρη να επιθυμούν να επικοινωνούν μεταξύ τους εμπιστευτικά.

Αναφορικά με την έννοια των ηλεκτρομαγνητικών εκπομπών σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης, αυτές εκπέμπονται κατά την λειτουργία ενός πληροφοριακού συστήματος. Οι εκπομπές αυτές δεν νοούνται ως δεδομένα με βάση τη περ. θ' του άρθρου 13 Π.Κ., πλην όμως δεδομένα μπορούν να ξανακατασκευαστούν από τις εκπομπές αυτές.

Επίσης, θα πρέπει να επισημανθεί ότι τόσο με βάση τη Σύμβαση όσο και με βάση την Οδηγία η επικοινωνία υπό τη μορφή εκπομπών ηλεκτρονικών δεδομένων είναι δυνατό να λάβει χώρα α) εντός μίας μονάδας ηλεκτρονικού υπολογιστή λ.χ. από την κεντρική μονάδα επεξεργασίας (CPU) προς την οθόνη ή τον εκτυπωτή, β) μεταξύ δύο συστημάτων υπολογιστών τα οποία ανήκουν στο ίδιο άτομο, γ) μεταξύ δύο υπολογιστών που επικοινωνούν μεταξύ τους ή δ) μεταξύ ενός υπολογιστή και ενός προσώπου λ.χ. μέσω του πληκτρολογίου. Το γεγονός ότι αυτού του είδους η επικοινωνία υπάρχει με βάση τα ανωτέρω ακόμα και με την απλή λειτουργία ενός πληροφοριακού συστήματος διευρύνει την «παραδοσιακή» έννοια της επικοινωνίας, η οποία απαιτεί επικοινωνία τουλάχιστον δύο μερών αν όχι ατόμων, ώστε αυτή να ομοιάζει περισσότερο με την έννοια τον δεδομένων, τα οποία ουσιαστικά διαβιβάζονται εντός ενός συστήματος για να επεξεργασθούν (λ.χ. από την μονάδα αποθήκευσης στην RAM και από εκεί στον επεξεργαστή). Καθώς λοιπόν το άρθρο 370Δ αναφέρεται και σε διαβιβάσεις δεδομένων και ηλεκτρομαγνητικών εκπομπών και εντός πληροφοριακών συστημάτων, θα πρέπει να γίνει δεκτό ότι αναφέρεται σε κάθε αρχείο που είναι αποθηκευμένο σε ένα πληροφοριακό σύστημα, δεδομένου ότι και η ίδια η αποθήκευση αρχείων αποτελεί διαβίβαση των δεδομένων αυτών αν μη τι άλλο στην προσωρινή μνήμη του πληροφοριακού αυτού συστήματος.[106]

iv. Το προστατευόμενο έννομο αγαθό

Η διάταξη αυτή αντιμετωπίζει τα δεδομένα όχι ως «ψηφιακά δεδομένα» υπό την υλική τους υπόσταση αλλά ως απόρρητα στοιχεία επικοινωνίας. Αυτό που έχει σημασία δεν είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών αλλά η διασφάλιση του απορρήτου του περιεχομένου τους.

[106] Η προσωρινή μνήμη, γνωστή και ως RAM (Random Access Memory = Μνήμη τυχαίας προσπέλασης) είναι ένας τύπος προσωρινής μονάδας αποθήκευσης δεδομένων τα οποία βρίσκονται σε χρήση από τον επεξεργαστή.

Προστατευόμενο έννομο αγαθό είναι «το δικαίωμα στην ιδιωτική ζωή υπό την έκφανση του απόρρητο των επικοινωνιών και η ασφάλεια των τηλεπικοινωνιών στον κυβερνοχώρο». Σε κάθε περίπτωση δε αν θεωρήσουμε τα πληροφοριακά συστήματα ως αυτοτελές έννομο αγαθό όπως υπαγορεύει η Οδηγία, το άρθρο 370Δ Π.Κ. τείνει προς την προστασία του από επιθέσεις σε συνδυασμό με την προστασία του απορρήτου των επικοινωνιών.

ν. Συρροή με άλλες διατάξεις

Όπως εκτέθηκε σχετικά με τη διάταξη του άρθρου 370Γ παρ. 2 Π.Κ. (παράνομη πρόσβαση), όταν συρρέει με τη διάταξη του άρθρου 370Α Π.Κ. που προστατεύει το απόρρητο των τηλεφωνικών επικοινωνιών, η τελευταία υπερισχύει ως ειδικότερη. Κατά την ίδια λογική και η διάταξη του άρθρου 370Δ Π.Κ υπερισχύει ως ειδικότερη έναντι της διάταξης του άρθρου 370Γ παρ. 2 Π.Κ. καθώς αποτελεί στενότερη (της διάταξης του άρθρου 370Δ Π.Κ.) διεύρυνση της ειδική διάταξης του 370Α Π.Κ. ώστε η τελευταία να καταλαμβάνει όλες τις περιπτώσεις παραβίασης του απορρήτου των επικοινωνιών που γίνονται μέσω πληροφοριακών συστημάτων. Μάλιστα δεν υπάρχει αξιολογική αντινομία καθώς με την ειδικότερη αυτή διάταξη απειλείται αυστηρότερο πλαίσιο ποινής και συγκεκριμένα κάθειρξη έως 10 ετών.

Τέλος αναφορικά με τις διατάξεις περί προστασίας προσωπικών δεδομένων ήτοι τις διατάξεις του άρθρου 15 του Ν. 3471/2006 και των παραγράφων 4 έως 8 του άρθρου 22 του Ν. 2472/1997[107] επισημαίνεται ότι η εφαρμογή των διατάξεων αυτών δεν προϋποθέτει λήψη γνώσης[108] και ότι η πρώτη διάταξη που αφορά την επεξεργασία προσωπικών δεδομένων συγκεκριμένα στο πεδίο των υπηρεσιών ηλεκτρονικών επικοινωνιών υπερισχύει της δεύτερης ως ειδικότερη σε αυτές τις περιπτώσεις.[109] Σε σχέση με το άρθρο 370Δ θα πρέπει να γίνει δεκτό ότι στις περιπτώσεις που συρρέει με το άρθρο 15 του Ν. 3471/2006 (δηλαδή σε περιπτώσεις υποκλοπής) υπερισχύει έναντι αυτού ως ειδικότερο, δεδομένου μάλιστα ότι το άρθρο απειλεί με κάθειρξης μέχρι 10 έτη δηλαδή κατά πολύ αυστηρότερη του άρθρου 15 του Ν. 3471/2006.

[107] βλ. ανωτέρω σελ. 50 και υποσημ. 68 και 69.

[108] [108] βλ. Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999, σελ.134 -136 όπου γίνεται αναφορά μόνο στο άρθρο 22 του Ν. 2472/1997 δεδομένου ότι ο Ν. 3471/2006 είναι πολύ μεταγενέστερος της έκδοσης του βιβλίου, και. Μ. Καϊάφα – Γκμπάντι, ο.π. σελ 1068 και γενικά έως 1071.

[109] πρβλ. Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1069.

5.2.1.4. Προσθήκη άρθρου 370Ε Π.Κ. - Εισαγωγή, διανομή κατοχή και διάθεση προγραμμάτων, συσκευών ή τεχνικών μέσων, με τα οποία θα ήταν δυνατή η πρόσβαση σε πληροφοριακό σύστημα, προκειμένου να διαπραχθούν τα εγκλήματα που αναφέρονται στα άρθρα 370Α μέχρι 370Δ Π.Κ.

Με την όγδοη παράγραφο του δεύτερου άρθρου του Ν. 4411/2016 εισάγεται Π.Κ η νέα διάταξη του άρθρου 370Ε. τιμωρείται αυτοτελώς η εισαγωγή, διανομή κατοχή και διάθεση προγραμμάτων, συσκευών ή τεχνικών μέσων, με τα οποία θα ήταν δυνατή η πρόσβαση σε πληροφοριακό σύστημα, προκειμένου να διαπραχθούν τα εγκλήματα που αναφέρονται στα άρθρα 370Α μέχρι 370Δ Π.Κ.

Συγκεκριμένα η όγδοη παράγραφος του δεύτερου άρθρου του Ν. 4411/2016 ορίζει τα εξής:

«8. Μετά το άρθρο 370Δ του Ποινικού Κώδικα προστίθεται άρθρο 370Ε ως εξής:

Άρθρο 370Ε

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, β) 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».

Η διάταξη αυτή αναλύεται κατωτέρω σε ειδικό κεφάλαιο, μαζί με τις υπόλοιπες διατάξεις που ποινικοποιούν τις προπαρασκευαστικές πράξεις της παραγωγής και της διάθεσης τεχνικών μέσων και κωδικών με σκοπό την τέλεση εγκλημάτων που στρέφονται κατά πληροφοριακών συστημάτων, σύμφωνα με το άρθρο 6 της Σύμβασης και το άρθρο 7 της Οδηγίας.

5.2.1.5. Προσθήκη άρθρου 381Α Π.Κ. – Φθορά ηλεκτρονικών δεδομένων

Με την ένατη παράγραφο του άρθρου δεύτερου του Ν. 4411/2016 εισάγεται στον Π.Κ. η νέα του άρθρου 381Α με το οποίο εναρμονίζεται η ελληνική νομοθεσία με τα άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας. Με τη νέα διάταξη αυτή καλύπτεται ένα κενό της ελληνικής νομοθεσίας και προστατεύονται πλέον αυτοτελώς τα ψηφιακά δεδομένα από πράξεις καταστροφής, διαγραφής αλλοίωσής τους κ.λπ.. Έτσι αποφεύγεται το άτοπο τα ψηφιακά δεδομένα να προστατεύονται αντανακλαστικά μόνο στο βαθιό και την έκταση που πλήττεται ο υλικός τους φορέας (σκληρός δίσκος, φορητή μνήμη κ.λπ.). Στις παραγράφους 2 και 3 προβλέπονται διακεκριμένες παραλλαγές σύμφωνα με τις ρυθμίσεις της Οδηγίας, ενώ

στην παράγραφο 4 προβλέπεται ότι το βασικό έγκλημα της παραγράφου 1 διώκεται κατ' έγκληση.

Συγκεκριμένα η ένατη παράγραφος του άρθρου δεύτερου του Ν. 4411/2016 ορίζει ότι:

«9. Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται άρθρο 381Α ως εξής:

Άρθρο 381Α Φθορά ηλεκτρονικών δεδομένων

1. Όποιος χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, 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 ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, 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 ενός (1) έτους, 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.

3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

Τα ζητήματα που ανακύπτουν αναφορικά με την εν λόγω διάταξη αναλύονται εκτενώς στο επόμενο κεφάλαιο.

5.2.1.6. Προσθήκη άρθρου 381Β Π.Κ. – Παραγωγή, πώληση, προμήθεια, εισαγωγή, κατοχή διανομή ή με άλλο τρόπο διακίνηση προγραμμάτων ή κωδικών με σκοπό την τέλεση της πράξης της φθοράς ηλεκτρονικών δεδομένων.

Με την δέκατη παράγραφο του άρθρου δεύτερου του Ν. 4411/2016 προστίθεται στον Π.Κ. το νέο άρθρο 381Β με το οποίο η ελληνική νομοθεσία εναρμονίζεται με το άρθρο 7 της Οδηγίας, που προβλέπει την ποινική ευθύνη προσώπων για πράξεις αγοράς, πώλησης, προμήθειας, κατοχής κ.λπ. προγραμμάτων ή κωδικών που μπορούν να χρησιμοποιηθούν για την τέλεση διάφορων αξιόποινων πράξεων μεταξύ των οποίων και οι προβλεπόμενες πλέον στο άρθρο 381Α Π.Κ..

Συγκεκριμένα η δέκατη παράγραφος του άρθρου δεύτερου του Ν. 4411/2016 ορίζει ότι:

«10. Μετά το άρθρο 381Α του Ποινικού Κώδικα προστίθεται άρθρο 381Β ως εξής:

Άρθρο 381Β

Με φυλάκιση μέχρι δύο (2) ετών, τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα του άρθρου 381Α παράγραφοι 1, 2 και 3 παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α, β) 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».

Η διάταξη αυτή αναλύεται κατωτέρω σε ειδικό κεφάλαιο μαζί με τις υπόλοιπες διατάξεις που ποινικοποιούν τις προπαρασκευαστικές πράξεις της παραγωγής και της διάθεσης τεχνικών μέσων και κωδικών με σκοπό την τέλεση εγκλημάτων που στρέφονται κατά πληροφοριακών συστημάτων, σύμφωνα με το άρθρο 6 της Σύμβασης και το άρθρο 7 της Οδηγίας.

5.2.1.7. Προσθήκη του άρθρου 292Β Π.Κ. – Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

i. Η διάταξη

Η δεύτερη παράγραφος του άρθρου δεύτερου του νόμου 4411/2016 προβλέπει την προσθήκη του άρθρου 292Β στον Ποινικό Κώδικα, με την οποία η ελληνική νομοθεσία εναρμονίζεται με τις διατάξεις που περιέχονται στα άρθρα 5 της Σύβασης και 4 της Οδηγίας. Με το εισαγόμενο άρθρο προσαρμόζεται η ποινική προστασία στα πλαίσια των ποινών που η Οδηγία προβλέπει και με γνώμονα την τήρηση της αρχής της αναλογικότητας ανάλογα με το είδος και την ένταση της προσβολής που οι πράξεις αυτές επιφέρουν. Σύμφωνα με τα οριζόμενα στην Οδηγία προβλέπεται αυστηρότερο πλαίσιο ποινής στις περιπτώσεις, όπου η

αξιόποινη συμπεριφορά προκαλεί ζημία σε σημαντικό αριθμό πληροφοριακών συστημάτων μέσω της χρήσης εργαλείων που έχουν σχεδιαστεί κυρίως για το σκοπό αυτόν, τελείται στο πλαίσιο δράσης εγκληματικής οργάνωσης, σε αντιστοιχία με τον ορισμό αυτής στο άρθρο 187 Π.Κ., προκαλεί ιδιαίτερα μεγάλη ζημία ή πλήττει πληροφοριακά συστήματα τα οποία αποτελούν μμέρος υποδομής που παρέχει ζωτικής σημασίας αγαθά ή υπηρεσίες για την κοινωνία και το κράτος.

Συγκεκριμένα η δεύτερη παράγραφος του άρθρου δεύτερου του νόμου 4411/2016 ορίζει ότι:

«2. Μετά το άρθρο 292Α του Ποινικού Κώδικα προστίθεται άρθρο 292Β ως εξής:

« Άρθρο 292Β

Παρακώλυση λειτουργιάς πληροφοριακών συστημάτων

1. Οποίος 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 μέχρι τριών (3) ετών.

2. Η πράξη της πρώτης παραγράφου τιμωρείται:

α) με φυλάκιση από ένα (1) έως τρία (3) έτη, 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 ζημιές και ιδίως επιθέσεων που προκαλούν μεγάλής 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 ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλής έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαιτέρα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον εντός (1) έτους, 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.

3. Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσοτέρων προσώπων, που επιδιώκει την τέλεση περισσοτέρων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».»

ii. Σύγκριση με τις διατάξεων του άρθρου 5 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στο κυβερνοχώρο και του άρθρου 4 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών

Ο Έλληνας νομοθέτης στο άρθρο 292Β Π.Κ. ακολούθησε πιστά τα όσα προβλέπονται στο άρθρο 5 της Σύμβασης και το άρθρο 6 της Οδηγίας με μόνη εξαίρεση την πρόβλεψη για περιπτώσεις «ήσσονος σημασίας» η οποία όπως εκτέθηκε είναι και περιττή αφού υπερκαλύπτεται από την προϋπόθεση η παρεμπόδιση ή η διακοπή της λειτουργίας ενός πληροφοριακού συστήματος να είναι «σοβαρές» για να είναι ποινικά αξιόλογες. Όπως εκτέθηκε σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης «σοβαρή» θεωρείται η παρακώλυση της λειτουργίας ενός συστήματος με την αποστολή δεδομένων σε αυτό υπό τέτοια μορφή, μέγεθος ή συχνότητα που να επηρεάζει σημαντικά ή καθοριστικά την δυνατότητα του ιδιοκτήτη ή του χρήστη να χρησιμοποιεί το σύστημα ή να επικοινωνεί με άλλα συστήματα (λ.χ. μέσω προγραμμάτων που δημιουργούν επιθέσεις άρνησης υπηρεσιών – DoS attacks, κακόβουλους κώδικες, όπως ιούς που αποτρέπουν οι επιβραδύνουν σημαντικά τη λειτουργία ενός συστήματος, ή προγράμματα που στέλνουν τεράστιες ποσότητες e-mail σε ένα λήπτη με σκοπό να εμποδίσουν την δυνατότητα επικοινωνίας του συστήματος). Ωστόσο αυτή η απαρίθμηση, πρέπει να θεωρηθεί ενδεικτική δεδομένου ότι το υπό κρίση έγκλημα μπορεί να τελεστεί εκτός από τρόπο της εισαγωγής δεδομένων τον οποίο αφορούν τα ανωτέρω παραδείγματα υπερφόρτωσης του συστήματος και με όλους τους τρόπους με τους οποίους είναι δυνατό να τελεστεί το έγκλημα της φθοράς ηλεκτρονικών δεδομένων ήτοι με την διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα όπως αναλύεται αμέσως στη συνέχεια.

iii. Τρόπος τέλεσης

Σύμφωνα με τον ορισμό που δίνεται στην περ. η' του άρθρου 13 Π.Κ. *«[π]ληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια 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».* Παρατηρείται λοιπόν ότι στην έννοια του πληροφοριακού συστήματος περιλαμβάνει και τα δεδομένα που υπάρχουν σε αυτό.

Περαιτέρω, οι πράξεις με τις οποίες μπορεί να επέλθει παρακώλυση της λειτουργίας ενός πληροφοριακού συστήματος είναι οι ίδιες με αυτές που τυποποιούνται στο έγκλημα της

φθοράς ηλεκτρονικών δεδομένων πλέον της πράξης της εισαγωγής δεδομένων. Επομένως θα πρέπει να διακρίνουμε δύο περιπτώσεις.

Στην πρώτη περίπτωση η σοβαρή παρακώλυση της λειτουργίας ενός πληροφοριακού συστήματος είναι συνέπεια της φθοράς ηλεκτρονικών δεδομένων η οποία ποινικοποιείται στην διάταξη της πρώτης παραγράφου του άρθρου 381Α Π.Κ.. Σε αυτή την περίπτωση ισχύουν ως τρόποι τέλεσης όσα αναφέρονται στο σχετικό χωρίο για το έγκλημα της φθοράς ηλεκτρονικών δεδομένων καθώς η παρακώλυση της λειτουργίας του πληροφοριακού συστήματος συνιστά το κάτι επιπλέον σε σχέση με αυτό.

Ωστόσο αναφορικά με την περίπτωση αυτή θα πρέπει να γίνει μια παρατήρηση. Με την δεύτερη επιβαρυντική περίσταση της φθοράς ηλεκτρονικών δεδομένων που προβλέπεται στην δεύτερη παράγραφο του άρθρου 381Α Π.Κ. απειλείται αυστηρότερο πλαίσιο ποινής για συμπεριφορές που συνιστούν το έγκλημα της φθοράς ηλεκτρονικών δεδομένων όταν αυτές έχουν ως αποτέλεσμα την πρόκληση «σοβαρών ζημιών», έννοια η οποία εν συνεχεία διευκρινίζεται ότι περιλαμβάνει ενδεικτικά τη διατάραξη των υπηρεσιών συστημάτων υπηρεσιών, και μάλιστα όχι οποιαδήποτε διατάραξη αλλά διατάραξη μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα. Γεννάται λοιπόν το ερώτημα ποιες περιπτώσεις συνιστούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών πληροφοριακού συστήματος και ποιες σοβαρή παρακώλυση της λειτουργίας πληροφοριακού συστήματος, ώστε οι συμπεριφορές αυτές να υπάγονται στη διάταξη του άρθρου 381Α παρ. 2 περ. 2 Π.Κ. ή στη διάταξη του άρθρου 292 παρ. 1 Π.Κ. αντίστοιχα υπό το φως του περιεχομένου του όρου σοβαρή παρακώλυση όπως αυτό αποδίδεται στην Αιτιολογική Έκθεση της Σύμβασης όπως εκτέθηκε ακριβώς προηγουμένως[110] και δεδομένου ότι η πρώτη απειλεί ποινή φυλάκισης τουλάχιστον ενός έτους ενώ η δεύτερη ενός έως τριών ετών. Μάλιστα το εν λόγω ζήτημα αποκτά ακόμα περισσότερο ενδιαφέρον όταν κανείς αντιληφθεί ότι η επιβαρυντικής αυτή περίσταση του άρθρου 381Α παρ. 2 περ. 2 Π.Κ. επαναλαμβάνεται αυτούσια ως επιβαρυντική περίσταση στο άρθρο 281Β παρ. 2 περ. 2. Π.Κ. αναφορικά με την σοβαρή παρακώλυση της λειτουργίας πληροφοριακών συστημάτων. Αφού όμως η παρακώλυση ποινικοποιείται ήδη ως βασικό έγκλημα μόνο όταν είναι σοβαρή, ποια είναι η σκοπιμότητα της εν λόγω επιβαρυντικής πρόβλεψης αφού αυτή ήδη υπάγεται στο γράμμα του βασικού εγκλήματος. Συνεπώς, κατά το γράφοντα όταν η φθορά ηλεκτρονικών δεδομένων προκαλεί σοβαρή ζημία η οποία συνιστά μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα παρακώλυση των υπηρεσιών ενός πληροφοριακού συστήματος τότε εφαρμογή θα έχει η

[110] βλ. υποενότητα ii.

διάταξη της παρ. του άρθρου 281Β Π.Κ. και όχι η διάταξη της περ. 2 της παρ. 2 του άρθρου 381Α Π.Κ. καθώς η δεύτερη αποτελεί απλώς μια ενδεικτικώς απαριθμούμενη περίπτωση, η οποία δεν μπορεί να θεωρηθεί δεσμευτική από τη στιγμή που το ζήτημα ρυθμίζεται ειδικά από άλλη διάταξη. Τέλος αναφορικά με την επιβαρυντική περίσταση της πρόκλησης μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών ενός πληροφοριακού συστήματος, ως ενδεικτική περίπτωση πρόκλησης σοβαρής ζημίας, η οποία σχολιάζεται επ' ευκαιρία στο συγκεκριμένο σημείο καθώς δεν απαιτείται να έχει τελεστεί με πράξη φθοράς ηλεκτρονικών δεδομένων, δεδομένου ότι δεν βασίζεται σε καμία ρητή διάταξη διεθνούς κειμένου που να δεσμεύει τον Έλληνα νομοθέτη, θα πρέπει να θεωρηθεί ότι καλύπτεται από το βασικό έγκλημα και η έννοια της σοβαρής ζημίας να ερμηνευθεί συσταλτικά ως σοβαρή «οικονομική» ζημία.

Στην δεύτερη περίπτωση, η οποία μάλιστα είναι και η πιο συχνή, η παρακώλυση της λειτουργίας ενός πληροφοριακού συστήματος γίνεται με την εισαγωγή δεδομένων τα οποία υπερφορτώνουν το σύστημα μα αποτέλεσμα αυτό να καταρρέει δηλαδή να βγαίνει εκτός λειτουργίας μόνιμα ή προσωρινά. Ο τρόπος αυτός με τον οποίο τελείται παρακώλυση της λειτουργίας ενός πληροφοριακού συστήματος με εισαγωγή δεδομένων ονομάζεται επίθεση άρνησης υπηρεσιών (DoS attack). Οι επιθέσεις άρνησης υπηρεσιών (DoS attacks) κατά πληροφοριακών συστημάτων συμπεριλαμβανομένων και των δικτύων τηλεπικοινωνιών τελούνται με την αποστολή τεράστιου όγκου αιτημάτων προς αυτά με αποτέλεσμα αυτά να υπερφορτώνονται και είτε να καταρρέουν (δηλαδή να βγαίνουν εκτός λειτουργίας) είτε να μη μπορούν να εξυπηρετήσουν πραγματικά αιτήματα.

Η κυριότερη μορφή των επιθέσεων αυτών χρησιμοποιεί πολλαπλές επιθέσεις μέσω υπολογιστών οι οποίοι έχουν προσβληθεί από κάποιον κακόβουλο λογισμικό και είναι γνωστή ως κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS attacks). Το κακόβουλο λογισμικό που χρησιμοποιείται συνηθέστερα για αυτό το σκοπό ονομάζεται «σκουλήκι» («worm»). Τα «σκουλήκια» εν αντιθέσει με τους ιούς αυτοαναπαράγονται εντός ενός πληροφοριακού συστήματος χωρίς να προσβάλουν άλλα προγράμματα. Για αυτό το λόγο μπορούν από μόνα τους να υπερφορτώσουν ένα πληροφοριακό σύστημα ή συνηθέστερα ένα τηλεπικοινωνιακό δίκτυο. Επίσης, όπως αναφέρθηκε τα «σκουλήκια» χρησιμοποιούνται πολύ συχνά για την τέλεση κατανεμημένων επιθέσεων άρνησης παροχής υπηρεσιών. Συγκεκριμένα συνήθως εγκαθιστούν μια «κερκόπορτα» («backdoor») στα πληροφοριακά συστήματα τα οποία προσβάλουν, η οποία επιτρέπει να ελέγχονται εξ' αποστάσεως. Τα πληροφοριακά αυτά συστήματα ονομάζονται ζόμπυ (« zombies») καθώς εν αγνοία του ιδιοκτήτη ή του χρήστη τους βρίσκονται υπό τον έλεγχο και επιτελούν του σκοπούς του

δράστη. Τα δίκτυα αυτών το υπολογιστών είναι γνωστά ως «botnets» και χρησιμοποιούνται για μαζικές ή αλλιώς κατανεμημένες επιθέσεις άρνησης υπηρεσιών.

iv. Το προστατευόμενο έννομο αγαθό

Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης, το έννομο αγαθό που προστατεύεται με την ποινικοποίηση συμπεριφορών παρακώλυσης της λειτουργίας πληροφορικών συστημάτων είναι το δικαίωμα του χρήστη να έχει μια «κανονική» λειτουργία του υπολογιστή του. Σύμφωνα, δε, με την Οδηγία το πληροφοριακά συστήματα ανάγονται σε αυτοτελές έννομο αγαθό, κάτι το οποίο ωστόσο θα πρέπει να εξειδικεύεται με βάση τα προβλεπόμενα στην Σύμβαση. Πράγματι, εκεί γίνεται αναφορά στην ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων τους η οποία αναλύεσαι στην ακεραιότητα την εμπιστευτικότητα και την διαθεσιμότητα τους, στοιχεία που αποτελούν και τον τίτλο του κεφαλαίου εντός του οποίου εντάσσεται και το έγκλημα την παρακώλυση της λειτουργίας πληροφοριακού συστήματος. Μάλιστα και ο Έλληνας νομοθέτης επέλεξε ορθώς να εντάξει το συγκεκριμένο έγκλημα στο δέκατο τέταρτο Κεφάλαιο του Π.Κ. το οποίο έχει τον γενικό τίτλο «εγκλήματα κατά της ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών και κατά των κοινωφελών εγκαταστάσεων» και το οποίο πλέον περιλαμβάνει, εκτός από εγκλήματα που στρέφονται κατά της ασφάλειας δημοσίων - υπερατομικών αγαθών και υπηρεσιών, και κατά ιδιωτικών – ατομικών αγαθών.

v. Συρροή με φθορά ξένης ιδιοκτησίας

Πριν την θεσμοθέτηση του άρθρου 292Β Π.Κ. μια συμπεριφορά παρακώλυσης της λειτουργίας πληροφοριακού συστήματος γνωστή και ως δολιοφθορά ηλεκτρονικού υπολογιστή μπορούσε να τιμωρηθεί μόνο ως φθορά υλικών μερών υπολογιστή κάτι που δεν επέδιδε κατά κανένα τρόπο την απαξία του της συμπεριφοράς δεδομένου ότι το σύστημα ή τα δεδομένα του είναι δυνατό να έχουν πολλαπλάσια αξία από τον υλικό φορά στα οποία είναι αποθηκευμένα.[111]

Πάντως, πλέον, με την θέσπιση του εγκλήματος αυτού θα πρέπει να γίνει δεκτό ότι τα δύο αυτά εγκλήματα συρρέουν μεταξύ τους σε περιπτώσεις που η παρακώλυση της λειτουργίας του πληροφοριακού συστήματος έχει ως συνέπεια και την υλική βλάβη του πληροφοριακού συστήματος ή και αντίστροφα όταν η υλική βλάβη του πληροφοριακού συστήματος έχει ως συνέπεια την παρακώλυση της λειτουργίας του. Τα δύο αυτά εγκλήματα θα συρρέουν κατ' ιδέαν και αληθινά καθώς προστατεύουν διαφορετικά έννομα αγαθά.

[111] Καϊάφα – Γκμπάντι, Ποινικό Δίκαιο και καταχρήσεις της πληροφορικής, Αρμ. 2007, σελ. 1075.

5.2.1.8. Προσθήκη του άρθρου 292Γ Π.Κ. - Παραγωγή, πώληση, διανομή, εισαγωγή, κατοχή, διανομή ή με κάθε άλλο τρόπο διακίνηση προγραμμάτων ή συσκευών σχεδιασμένων ή προσαρμοσμένων για την τέλεση της πράξης της παρακώλυσης της λειτουργίας πληροφοριακών συστημάτων

Η τρίτη παράγραφος του άρθρου δεύτερου του Ν. 4411/2016 προβλέπει την προσθήκη του άρθρου 292Γ του Ποινικού Κώδικα, με το οποίο η ελληνική έννομη τάξη εναρμονίζεται με το άρθρο 7 της Οδηγίας, καθώς με αυτό ποινικοποιούνται αυτοτελώς συμπεριφορές που κατατείνουν στην τέλεση των εγκλημάτων του άρθρου 292Β Π.Κ. και ειδικότερα παραγωγή, πώληση, διανομή, εισαγωγή, κατοχή κ.λπ. προγραμμάτων ή συσκευών σχεδιασμένων ή προσαρμοσμένων για την τέλεση των πράξεων του άρθρου αυτού.

Συγκεκριμένα τρίτη παράγραφος του άρθρου δεύτερου του Ν. 4411/2016 ορίζει ότι:

«3. Μετά το άρθρο 292Β του Ποινικού Κώδικα προστίθεται άρθρο 292Γ ως εξής:

« Άρθρο 292Γ

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκληματών του άρθρου 292Β, β) 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».»

Η διάταξη αυτή αναλύεται κατωτέρω σε ειδικό κεφάλαιο μαζί με τις υπόλοιπες διατάξεις που ποινικοποιούν τις προπαρασκευαστικές πράξεις της παραγωγής και της διάθεσης τεχνικών μέσων και κωδικών με σκοπό την τέλεση εγκλημάτων που στρέφονται κατά πληροφοριακών συστημάτων, σύμφωνα με το άρθρο 6 της Σύμβασης και το άρθρο 7 της Οδηγίας.

5.2.1.9. Αντικατάσταση του άρθρου 386Α – Απάτη με υπολογιστή

Με την εντέκατη παράγραφο του άρθρου δεύτερου του Ν. 4411/2016 τροποποιείται το άρθρο 386Α Π.Κ. (απάτη υπολογιστή) κατά τα οριζόμενα στο άρθρο 8 της Σύμβασης. Σύμφωνα με τη νέα διάταξη περιλαμβάνεται ρητά στις περιοριστικά πλέον αναφερόμενες περιπτώσεις απάτης με υπολογιστή και η χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα, όπως π.χ. στην περίπτωση του δράστη που έχει αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου.

Συγκεκριμένα με η εντέκατη παράγραφος του άρθρου δεύτερου του Ν. 4411/2016 ορίζει ότι:

«11. Το άρθρο 386Α του Ποινικού Κώδικα αντικαθίσταται ως εξής:

«Άρθρο 386Α Απατή με υπολογιστή

Οποίος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχειών είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγουμένου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα».

Η διάταξη του άρθρου 386Α Π.Κ. ουσιαστικά παρέμεινε ως είχε[112], με μόνη διαφορά ότι πλέον οι τρόποι με του οποίους μπορεί να τελεστεί το έγκλημα της απάτης με υπολογιστή απαριθμούνται περιοριστικώς και όχι ενδεικτικώς ενώ παράλληλα σε αυτούς προστέθηκαν δύο νέοι τρόποι τέλεσης, και συγκεκριμένα η χωρίς δικαίωμα χρήση δεδομένων και η χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα.

Πριν την τροποποίηση του άρθρου 386Α Π.Κ. με το Ν. 4411/2016, περιπτώσεις επηρεασμού με χρήση ορθών στοιχείων, η οποία όμως χρήση δεν ήταν σύννομη, υπάγονταν κατά μία άποψη, σε αυτό το άρθρο, λόγω της ενδεικτικής απαρίθμησης των τρόπων επηρεασμού που προέβλεπε («είτε με οποιονδήποτε άλλο τρόπο»). Στις περιπτώσεις αυτές περιλαμβάνονται η μεταβίβαση λογιστικών χρημάτων από μη δικαιούχο σε άλλο λογαριασμό και η ανάληψη χρημάτων από ΑΤΜ από μη δικαιούχο με τη χρήση κλεμμένης κάρτας και της. Έτσι με το νέο νόμο δίνεται ένα τέλος σε αυτό το για πάνω από δυόμισι δεκαετίες εριζόμενο ζήτημα.

Ωστόσο, με την νέα ρύθμιση δεν επιλύονται περιπτώσεις που ο δράστης έχει τυπικό δικαίωμα επί του λογαριασμού, δεν έχει όμως ουσιαστικό δικαίωμα επί των συγκεκριμένων

[112] Σκοπός της παρούσας εργασίας είναι ο εντοπισμός και ο σχολιασμός των ζητημάτων που ανακύπτουν αναφορικά με τις νομοθετικές μεταρρυθμίσεις που επήλθαν στον Π.Κ. για αυτό δεν γίνεται ανάλυση των ρυθμίσεων του άρθρου που παρέμειναν ίδιες. Για την ανάλυση των διατάξεων που διατηρήθηκαν καθώς και για τους σχετικούς προβληματισμούς αναφορικά με την προηγούμενη διατύπωση του άρθρου βλ. μεταξύ άλλων κυρίως. Χρ. Μυλωνόπουλου, Ποινικό Δίκαιο Ειδικό Μέρος Β' έκδοση, σελ 54-56 και 596 επ. αλλά και Δ. Κιούπη, Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ευρωπαϊκή Ένωση, Δικηγορικός Σύλλογος Πειραιά – Ένωση Ελλήνων Ποινικολόγων – Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, 2010, σελ. 198 -204, και Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1078-1082.

χρημάτων, είτε επειδή ανέλαβε τα χρήματα και τα χρησιμοποίησε κατά παράβαση των συμφωνηθέντων, είτε επειδή τα μεταβίβασε σε τραπεζικό λογαριασμό κατά παράβαση των συμφωνηθέντων. Η διάταξη του 386Α Π.Κ. δεν εισέρχεται στο επίπεδο της εσωτερικής σχέσης δράστη θύματος καθώς αυτό εκφεύγει όχι μόνο των λεκτικών αλλά και των λογικών ορίων της. Αντίθετα, περιορίζεται στο δικαίωμα χρήσης των δεδομένων ήτοι το τυπικό δικαίωμα χρήσης του τραπεζικού λογαριασμού.

Για το λόγο αυτό, της ύπαρξης δηλαδή των ως άνω μη ρυθμιζόμενων νομοθετικά περιπτώσεων, προκρίνεται από το γράφοντα η αντιμετώπιση των λογιστικών μονάδων ως πραγμάτων κατά πλάσμα δικαίου, η οποία εξυπηρετεί ταυτόχρονα και την ανάγκη ενδοσυστημικής συνέπειας ώστε να μην αντιμετωπίζονται ανόμοια όμοιες περιπτώσεις. Ήτοι, περιπτώσεις που εν γένει χρήματα αντιμετωπίζονται είτε με το πλαίσιο ποινής της απάτης αν πρόκειται για λογιστικά χρήματα, είτε με το πλαίσιο ποινής κατά περίπτωση της κλοπής της υπεξαίρεσης ή ακόμα και της υφαίρεσης αν πρόκειται για χρήματα που έχουν υλική υπόσταση. Μάλιστα, ήδη η ίδια η νομολογία καταφεύγει στην λύση αυτή, αντιμετωπίζοντας την πρώτη ως άνω περίπτωση σαν υπεξαίρεση και την δεύτερη σαν κλοπή.[113] Πλην όμως οι αναλογικές αυτές εφαρμογές δεν μπορούν να κριθούν επιτρεπτές με βάση την αρχή της νομιμότητας καθώς πράγματα κατά την έννοια του ποινικού δικαίου είναι μόνο ενσώματα αντικείμενα. Για το λόγο αυτό κρίνεται αναγκαίο να υπάρξει σχετική ρητή νομοθετική πρόβλεψη.

5.3. Η διάταξη για την ευθύνη νομικών προσώπων

Με το άρθρο τέταρτο ρυθμίζεται το ζήτημα της ευθύνης των νομικών προσώπων (άρθρο 12 της Σύμβασης και άρθρο 10 της Οδηγίας) και των διοικητικών κυρώσεων κατά αυτών (άρθρο 11 της Οδηγίας). Η υιοθέτηση του συστήματος διοικητικών κυρώσεων ακολουθεί το πρότυπο αντίστοιχων ρυθμίσεων κατά την εναρμόνιση της ελληνικής νομοθεσίας με άλλες οδηγίες καθώς στην ελληνική έννομη τάξη δεν προβλέπεται ποινική ευθύνη των ίδιων των νομικών προσώπων.

Συγκεκριμένα το άρθρο τέταρτο του Ν. 4411/2016 έχει ως ακολούθως

«Άρθρο τέταρτο – Ευθύνη νομικών προσώπων (Άρθρο 11 της Οδηγίας)

1. Αν κάποια από τις πράξεις των άρθρων 292Β, 370Γ, 370Δ, 370Ε, 381Α και 386Α του Ποινικού Κώδικα τελέστηκε, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, από φυσικό πρόσωπο που ενεργεί είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου ή της ένωσης προσώπων και έχει εξουσία εκπροσώπησής τους ή εξουσιοδότηση για

[113] Α.Π. 742/2012

τη λήψη αποφάσεων για λογαριασμό τους ή για την άσκηση ελέγχου εντός αυτών, επιβάλλονται στο νομικό πρόσωπο ή στην ένωση προσώπων με ειδικά αιτιολογημένη απόφαση της Αρχής Διασφάλισης του Απόρρητου των Επικοινωνιών, κατά περίπτωση, σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις,

α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,

β) διοικητικό πρόστιμο από 20.000 έως 1.000.000 ευρώ,

γ) ανάκληση ή αναστολή της άδειας λειτουργίας τους για χρονικό διάστημα από ένα (1) μήνα έως δύο (2) έτη ή απαγόρευση άσκησης της επιχειρηματικής τους δραστηριότητας για το ίδιο χρονικό διάστημα,

δ) αποκλεισμός από δημόσιες παροχές, ενισχύσεις, επιδοτήσεις, αναθέσεις έργων και υπηρεσιών, προμήθειες, διαφημίσεις και διαγωνισμούς του Δημοσίου ή των νομικών προσώπων του δημόσιου τομέα για το ίδιο διάστημα.

Σε περίπτωση υποτροπής οι κυρώσεις των περιπτώσεων γ΄ και δ΄ μπορεί να έχουν οριστικό χαρακτήρα και εφόσον πρόκειται περί σωματείων ή ενώσεων προσώπων, η υποτροπή μπορεί να έχει ως συνέπεια τη διάλυσή τους, σύμφωνα με τις εκάστοτε ισχύουσες διατάξεις.

2. Όταν η έλλειψη εποπτείας ή ελέγχου από φυσικό πρόσωπο που αναφέρεται στην παράγραφο 1, κατέστησε δυνατή την τέλεση από πρόσωπο που τελεί υπό την εξουσία του κάποιας από τις αξιόποινες πράξεις που αναφέρονται στην ίδια ως άνω παράγραφο, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, επιβάλλονται στο νομικό πρόσωπο, σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις:

α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,

β) διοικητικό πρόστιμο από 10.000 έως 1.000.000 ευρώ,

γ) οι προβλεπόμενες στις περιπτώσεις γ΄ και δ΄ της προηγούμενης παραγράφου κυρώσεις για χρονικό διάστημα από δέκα (10) ημέρες έως έξι (6) μήνες.

3. Για τη σωρευτική ή διαζευκτική επιβολή των κυρώσεων που προβλέπονται στις προηγούμενες παραγράφους και για την επιμέτρηση των κυρώσεων αυτών λαμβάνονται υπόψη ιδίως η βαρύτητα της παράβασης, ο βαθμός της υπαιτιότητας, η οικονομική επιφάνεια του νομικού προσώπου ή της ένωσης προσώπων και η τυχόν υποτροπή τους.

4. Η εφαρμογή των διατάξεων των προηγούμενων παραγράφων είναι ανεξάρτητη από την αστική, πειθαρχική ή ποινική ευθύνη των αναφερόμενων σε αυτές φυσικών προσώπων. Καμιά κύρωση δεν επιβάλλεται χωρίς προηγούμενη κλήτευση των νόμιμων εκπροσώπων του νομικού προσώπου ή της ένωσης προσώπων προς παροχή εξηγήσεων. Η κλήση κοινοποιείται

τουλάχιστον δέκα (10) ημέρες πριν από την ημέρα της ακρόασης. Κατά τα λοιπά, εφαρμόζονται οι διατάξεις των παραγράφων 1 και 2 του άρθρου 6 του Κώδικα Διοικητικής Διαδικασίας. Σε περίπτωση άσκησης ποινικής δίωξης για κάποια από τις προβλεπόμενες στην παράγραφο 1 αξιόποινες πράξεις που τελέστηκε από πρόσωπο αναφερόμενο στις παραγράφους 1 και 2 και προκειμένου να εφαρμοστεί η προβλεπόμενη στο άρθρο αυτό διαδικασία επιβολής διοικητικών κυρώσεων, οι εισαγγελικές αρχές ενημερώνουν αμέσως τον Υπουργό Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και αποστέλλουν σε αυτόν αντίγραφα της δικογραφίας.

5. Σε περίπτωση αμετάκλητης απαλλαγής του παραπεφθέντος οι κατά τα ανωτέρω αποφάσεις επιβολής διοικητικών κυρώσεων ανακαλούνται.

6. Οι διατάξεις των προηγουμένων παραγράφων δεν εφαρμόζονται στο κράτος, στους φορείς δημόσιας εξουσίας και στους διεθνείς οργανισμούς δημοσίου δικαίου, χωρίς αυτό να επηρεάζει την εφαρμογή των ισχυουσών κάθε φορά διατάξεων περί αστικής, πειθαρχικής ή ποινικής ευθύνης.»

6. Φθορά ηλεκτρονικών δεδομένων

6.1. Η διάταξη

Άρθρο 381Α Φθορά ηλεκτρονικών δεδομένων

1. Οποίος χωρίς δικαίωμα διαγραφεί, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαιτέρα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, 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 ζημία ιδιαιτέρα μεγάλής αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλής έκτασης ή για μεγάλο χρονικό́ διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαιτέρα μεγάλής αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, 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.

3. Αν οι πράξεις των προηγουμένων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσοτέρων προσώπων, που επιδιώκει την τέλεση περισσοτέρων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4. Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

6.2. Σύγκριση με τις διατάξεις του άρθρου 4 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στο κυβερνοχώρο και του άρθρου 5 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών

6.2.1. Αναφορικά με τις επιμέρους τυποποιούμενες συμπεριφορές

Αρχικά, παρατηρείται ότι το άρθρο 381Α Π.Κ, προβλέπει ως επιμέρους τρόπους τέλεσης φθοράς ηλεκτρονικών δεδομένων την διαγραφή, την καταστροφή, την αλλοίωση και την

απόκρυψη των δεδομένων ενός πληροφοριακού συστήματος, την κατάσταση ανέφικτης της χρήσης τους και τον με οποιοδήποτε τρόπο αποκλεισμό της πρόσβασης σε αυτά. Η μικρή διαφοροποίηση αναφορικά με τις προβλεπόμενες συμπεριφορές ή την διατύπωσή τους συγκριτικά με την Σύμβαση και την Οδηγία, δεν θα πρέπει να θεωρηθεί ότι έχει ουσιαστικές συνέπειες στο περιεχόμενο της διάταξης και το εύρος των περιπτώσεων τις οποίες καλύπτει, λαμβανομένων, μάλιστα, υπόψιν των επεξηγήσεων των όρων που δίνονται στην Αιτιολογική Έκθεσης της Σύμβασης[114]. Ωστόσο θε πρέπει να γίνει δεκτό ότι και μόνο ο όρος «αλλοίωση» περιλαμβάνει όλες τις λοιπές περιγραφόμενες συμπεριφορές οι οποίες ουσιαστικά την εξειδικεύουν. Πράγματι, ακόμα και οι έννοιες της «κατάστασης της χρήσης των ηλεκτρονικών δεδομένων ως ανέφικτης» και του «αποκλεισμού της πρόσβασης στα ηλεκτρονικά δεδομένα» δύναται να υπαχθούν στην έννοια της «αλλοίωσης» καθώς πρόκειται για συμπεριφορές που επιδρούν σε αυτά αλλοιώνοντας αν όχι και το περιεχόμενο τους (σε περίπτωση «κλειδώματος»), σε κάθε περίπτωση τα εξωτερικά στοιχεία των δεδομένων αυτών όπως λ.χ. τη θέση τους.

6.2.2. Αναφορικά με τον περιορισμό του αξιοποίνου

Μια δεύτερη διαφορά, πιο ουσιώδης αυτή τη φορά, είναι η πρόβλεψη δυνητικού λόγου δικαστικής άφεσης της ποινής με βάση τις περιστάσεις τέλεσης του εγκλήματος όταν πρόκειται για ιδιαίτερα ελαφρές περιπτώσεις. Όπως εκτέθηκε, η Σύμβαση παρέχει την δυνατότητα στα Συμβαλλόμενα Μέρη να μην ποινικοποιήσουν στην εσωτερική τους έννομη τάξη συμπεριφορές που συνιστούν επέμβαση σε δεδομένα όταν αυτές δεν έχουν ως συνέπεια την πρόκληση σοβαρής ζημίας. Αντίθετα η Οδηγία δίνει δυνατότητα στα Κράτη Μέλη μη ποινικοποίησης συμπεριφορών «ήσσονος σημασίας». Έχει επισημανθεί[115], ότι η ρύθμιση αυτή της Οδηγίας είναι στενότερη από αυτή της Σύμβασης αφού σε αντίθεση με την τελευταία δεν παρέχει δυνατότητα μη ποινικοποίησης μέτριας βαρύτητας περιπτώσεων. Ο Έλληνας νομοθέτης, ωστόσο, δεν ακολούθησε ούτε αυτή τη λιγότερο ευνοϊκή δυνατότητα

[114] Σύμφωνα με την παρ. 64 της Αιτιολογικής Έκθεσης της Σύμβασης α) οι έννοιες «βλάβη» και «φθορά» είναι αλληλοκαλυπτόμενες και αφορούν αρνητική αλλοίωση της ακεραιότητας ή του πληροφοριακού περιεχομένου των δεδομένων και των προγραμμάτων, β) η έννοια της «διαγραφής» των δεδομένων είναι αντίστοιχη με την καταστροφή ενός αντικειμένου υπό την νομική του έννοια δηλαδή που έχει υλική υπόσταση, γ) η έννοια της «καταστολής» δεδομένων καταλαμβάνει κάθε συμπεριφορά που αποκλείει ή σταματά την διαθεσιμότητα των δεδομένων στο πρόσωπο που έχει πρόσβαση στον υπολογιστή ή τον φορέα δεδομένων στον οποίο ήταν αποθηκευμένα και τέλος δ) η έννοια της «αλλοίωσης» αφορά την τροποποίηση δεδομένων που προϋπήρχαν

[115] Μ. Καϊάφα – Γκμπάντι, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 489 επ.

που παρέχει η Οδηγία, αλλά επέλεξε να εισάγει στο άρθρο 381Α Π.Κ. απλώς την δυνατότητα δικαστικής άφεσης της ποινής σε εξαιρετικά ελαφρές περιπτώσεις, λαμβανομένων υπόψιν των περιστάσεων τέλεσης του εγκλήματος. Αν και ο όρος «εξαιρετικά ελαφρές περιπτώσεις» δεν θα πρέπει να θεωρείται διάφορος από τον όρο «ήσσονος σημασίας» που χρησιμοποιείται από την σύμβαση[116], δεν θα πρέπει να υπάρχει καμία αμφιβολία ότι η δικαστική άφεση της ποινής και μάλιστα δυνητική είναι υπερβολικά αυστηρότερη από την μη ποινικοποίηση αφού είναι πραγματικά το τελευταίο στάδιο που είναι δυνατό να υπάρξει για να μην καταδικαστεί ο δράστης και μάλιστα στην εν λόγω περίπτωση υπό την αίρεση της αξιολόγησης των συγκεκριμένων περιστάσεων. Πάντως, εντύπωση δημιουργεί ότι ενώ η Οδηγία παρέχει τη δυνατότητα μη ποινικοποίηση περιπτώσεων ήσσονος σημασίας αναφορικά με όλα τα εγκλήματα που στρέφονται κατά πληροφοριακών συστημάτων και των δεδομένων τους, ο Έλληνας νομοθέτης επέλεξε των περιορισμό του αξιοποίνου στη συγκεκριμένη περίπτωση αν και όχι με ένα;Σ αρνητικά διατυπωμένο ειδικό στοιχείο του αδίκου αλλά με ένα δυνητικό λόγο δικαστικής άφεσης της ποινής. Δεδομένου ότι δεν υπάρχει σχετική σκέψη στην Αιτιολογική Έκθεση του νόμου, μπορούμε μόνο να εικάσουμε αναφορικά το τι οδήγησε τον Έλληνα νομοθέτη στην επιλογή αυτή. Κατά την άποψη του γράφοντος η συγκεκριμένη πρόβλεψη, μάλλον, ανταποκρίνεται στην ανάγκη μη τιμώρησης συμπεριφορών φθοράς των υλικών φορέων των δεδομένων εκτός για το έγκλημα της φθοράς ξένης ιδιοκτησίας και για το έγκλημα της φθοράς ηλεκτρονικών δεδομένων, όταν τα δεδομένα αυτά είναι τυποποιημένα και δεν έχουν υποστεί επεξεργασία που να τους προσδίδει μοναδικότητα, ή περιπτώσεις που τα δεδομένα δεν ταυτίζονται με τον υλικό φορέα αλλά μπορούν να ανακτηθούν.

6.3. Η έννοια των ηλεκτρονικών δεδομένων

Το άρθρο 381Α Π.Κ. ποινικοποιεί την φθορά ηλεκτρονικών δεδομένων. Ωστόσο, για να εξετάσουμε τι δύναται να συνιστά φθορά ηλεκτρονικών δεδομένων, πρέπει να κατανοήσουμε το τι συνιστά ηλεκτρονικά δεδομένα.

Όπως εκτέθηκε, σύμφωνα με το στοιχείο θ’ του άρθρου 13 Π.Κ. όπως αυτό προστέθηκε με την πρώτη παράγραφο του άρθρου δεύτερου του Ν. 4411/2016 *«[ψ]ηφιακά δεδομένα*

[116] Θα μπορούσε βέβαια να υποστηριχθεί ότι ο Έλληνα νομοθέτης δεν αρκείται σε ελαφρές περιπτώσεις δηλαδή «ήσσονος σημασίας» αλλά αναφέρεται ακόμα αυστηρότερα σε ιδιαίτερα ελαφρές περιπτώσεις. Ωστόσο οι όροι αυτοί δεν έχουν κάποιο συγκεκριμένο περιεχόμενο. Μάλιστα ο όρος «ήσσονος σημασίας» που χρησιμοποιείται από τη Οδηγία έχει επικριθεί σοβαρά ότι παραβιάζει τη αρχή της νομιμότητας, λόγω της αοριστίας που ενέχει η οποία είναι σε τέτοιο βαθμό που, παρά το γεγονός ότι τίθεται προς όφελος του δράστη, καθιστά όλη τη διάταξη αόριστη αφού δεν μπορεί ευχερώς να προσδιορισθεί ποιες περιπτώσεις υπάγονται σε αυτή και ποιες όχι .

είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».

Με άλλα λόγια, τα δεδομένα, απλουστευτικά, είναι στοιχεία αποθηκευμένα σε μια μονάδα αποθήκευσης η οποία μπορεί να αποτελεί μέρος ενός πληροφοριακού συστήματος όπως ενός ηλεκτρονικού υπολογιστή (λ.χ. σε ένα σκληρό δίσκο – Hard Drive ή σε μια μονάδα αποθήκευσης σταθερής κατάστασης – SSD) ή ένα συνδέεται εξωτερικά με αυτό (λ.χ. ένα CD, ή ένα «στικάκι USB»). Τα δεδομένα μεταφέρονται είτε τα ίδια είτε αντίγραφα τους από την μονάδα αποθήκευσης στην προσωρινή μνήμη του πληροφοριακού συστήματος όπου είναι προσβάσιμα στον επεξεργαστή (CPU) ο οποίος είτε απλώς τα προβάλει στην οθόνη του συστήματος είτε τα επεξεργάζεται σύμφωνα με της οδηγίες του χρήστη με σκοπό την δημιουργία νέων δεδομένων. Τα δεδομένα μπορεί να αντιπροσωπεύουν κάθε είδους αρχεία (λ.χ. εικόνας, ήχου κ.λπ.) ή και προγράμματα. Τα νέα δεδομένα που παράγονται αποθηκεύονται εκ νέου στην μονάδα αποθήκευση είτε αν πρόκειται για αντίγραφα αντικαθιστούν τα αποθηκευμένα στην μονάδα αποθήκευσης δεδομένα στα οποία βασίζονται.

6.4. Το προστατευόμενο έννομο αγαθό

Τα δεδομένα των πληροφοριακών συστημάτων έχουν δύο διακριτές υποστάσεις, μια υλική και μια ψηφιακή. Και οι δύο αυτές υποστάσεις προστατεύονται από το ποινικό δίκαιο αυτοτελώς. Αφενός, η υλική τους υπόσταση προστατεύεται με την διάταξη του άρθρου 381Α Π.Κ. αλλά και του άρθρου 292Β (στο βαθμό που αυτή προστατεύει και τα δεδομένων, τα οποία εμπεριέχονται στην έννοια των πληροφοριακών συστημάτων σύμφωνα με τον ορισμό των τελευταίων). Αφετέρου, η ψηφιακή τους υπόσταση, η οποία αφορά το περιεχόμενο τους, δηλαδή τις πληροφορίες τις οποίες εμπεριέχουν, και η οποία, όπως αναλυτικά εκτέθηκε στο προηγούμενο κεφάλαιο, προστατεύεται από διατάξεις που προστατεύουν και το απόρρητο ή άλλως την εμπιστευτικότητα (άρθρα 370Α, 370Γ παρ. 2 και 370Δ Π.Κ.), τα προσωπικά δεδομένα (άρθρο 15 του Ν. 3471/2006 και άρθρο 22 παρ. 4 έως 8 του Ν. 2472/1997)και τα πνευματικά δικαιώματα (άρθρα 2 παρ. 3 και 66 Ν. 2121/1993).

Ειδικότερα, αναφορικά με το έγκλημα της φθοράς ηλεκτρονικών δεδομένων, σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης του Συμβουλίου, το προστατευόμενο έννομο αγαθό της παρεμβολής σε δεδομένα είναι η ακεραιότητα και η ορθή λειτουργία ή χρήση αποθηκευμένων δεδομένων υπολογιστή και προγραμμάτων.[117] Από την άλλη σύμφωνα με

[117] Σκέψη 60 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

την Οδηγία τα ίδια τα πληροφοριακά συστήματα και τα δεδομένα τους ανάγονται, σε προστατευόμενο έννομο αγαθό όλων των προβλεπόμενων από αυτή ποινικών αδικημάτων. Οι δύο αυτές προβλέψεις δεν έρχονται σε σύγκρουση μεταξύ τους. Ουσιαστικά, ο ορισμός που δίδεται από την Σύμβαση εξειδικεύει κατά περίπτωση το έννομο αγαθό που περιγράφεται στην Οδηγία.

Ένα ενδιαφέρον ζήτημα, το οποίο δεν θα πρέπει να παραβλέψουμε, είναι το γεγονός ότι ο Έλληνας νομοθέτης δεν ενέταξε το υπό κρίση έγκλημα σε ένα νέο κεφάλαιο του ποινικού κώδικα το οποίο να περιλαμβάνει όλα τα εγκλήματα που στρέφονται κατά των πληροφοριακών συστημάτων και των δεδομένων τους, όπως είχε προταθεί και όπως ίσως να ήταν ορθότερο λαμβανομένων υπόψιν και των λοιπών εγκλημάτων που ποινικοποιούνται με τον Ν. 4411/2016 τα οποία είναι διασκορπισμένα στον ποινικό κώδικα κατά εντελώς, πολλές φορές, αυθαίρετο και άστοχο τρόπο όπως εκτίθεται στα οικεία κεφάλαια της παρούσας. Αντίθετα, επέλεξε να το εντάξει στο εικοστό τρίτο κεφάλαιο του ποινικού κώδικα στο οποίο περιλαμβάνονται τα εγκλήματα που στρέφονται κατά του εννόμου αγαθού της ιδιοκτησίας. Ο προφανής λόγος για τον οποίο έγινε αυτή η επιλογή είναι επειδή στα ελληνικά ο τίτλος του εγκλήματος αποδόθηκε με τη χρήση της λέξης «φθορά». Επιπρόσθετα αναμφίβολα επηρέασε την απόφαση αυτή, ή μάλλον ακόμα και την ίδια την ονομασία του εγκλήματος[118], το γεγονός, ότι, πριν την θεσμοθέτηση του υπό κρίση άρθρου, το κενό της προστασίας του ποινικού κώδικα καλυπτόταν με την εφαρμογή του άρθρου 381 Π.Κ. που προστατεύει τη φθορά ξένης ιδιοκτησίας.**[119]**

Ωστόσο, κατά τον γράφοντα, δεν θα πρέπει να γίνει δεκτό ότι με το άρθρο αυτό συμπροστατεύεται και το έννομο αγαθό της ιδιοκτησίας και ότι επομένως το άρθρο 381Α Π.Κ. είναι ειδικότερο του άρθρου 381 Π.Κ.. Παρά το γεγονός ότι το άρθρο 381Α Π.Κ. άπτεται της υλικής υπόστασης των ηλεκτρονικών δεδομένων θα ήταν καταχρηστικό να δεχτούμε ότι αυτά μπορούν να υπαχθούν στην έννοια του πράγματος καθώς θα επρόκειτο για απαγορευμένη αναλογία κατά παράβαση της αρχής την νομιμότητας. Για το λόγο αυτό ίσως θα πρέπει να αντιληφθούμε την έννοια της υλικής υπόστασης των ηλεκτρονικών δεδομένων αποκλειστικά σε αντιπαραβολή με την ψηφιακή τους υπόσταση. Θα πρέπει δηλαδή να την έχουμε στο νου μας ως την λειτουργικότητα τους ανεξαρτήτως περιεχομένου. Με τη άποψη αυτή είναι σύμφωνο και το γεγονός ότι κατά την Οδηγία τα ίδια τα ηλεκτρονικά δεδομένα

[118] Στο αγγλικό κείμενο τόσο της Σύμβασης όσο και της Οδηγίας χρησιμοποιείται ο όρος «interference» ο οποίος αποδόθηκε στις ελληνικές μεταφράσεις ως «επέμβαση» και «παρεμβολή» αντίστοιχα.

[119] Για την συρροή του άρθρου 381Α Π.Κ. με το άρθρο 381 Π.Κ. βλ. κατωτέρω υποενότητα 6.8.3.1.

ανάγονται σε έννομο αγαθό. Η λειτουργικότητα, όπως προκύπτει από τα ίδια τα έννομα αγαθά, υφίσταται σε σχέση πάντα με το υποκείμενο των δεδομένων (αυτόν στον οποίο ανήκουν τα ηλεκτρονικά δεδομένα και όχι αυτός, τον οποίο αφορούν, καθώς το περιεχόμενο είναι αδιάφορο για το εν λόγω έγκλημα) γεγονός το οποίο καθιστά τα έννομα αγαθά ατομικά. Αυτή είναι και η μοναδική κατ' ουσίαν ομοιότητα του εγκλήματος του άρθρου 381Α Π.Κ. με το έγκλημα της φθορά ξένης ιδιοκτησίας, όμως εδώ δεν πρόκειται για ιδιοκτήτη ή κάτοχο ηλεκτρονικών δεδομένων όπως θα λέγαμε στην καθομιλουμένη αλλά σύμφωνα με την νομική ορολογία για αυτόν ο οποίος έχει δικαίωμα στην ακεραιότητα και την ορθή λειτουργία και χρήση αποθηκευμένων δεδομένων υπολογιστή και προγραμμάτων.

6.5. Τρόποι τέλεσης

Είναι δυνατό να εντάξουμε τους τρόπους με τους οποίους μπορεί να επέλθει αλλοίωση των ηλεκτρονικών δεδομένων ενός υπολογιστή σε δύο μεγάλες κατηγορίες. Ο πρώτος τρόπος είναι με την φθορά του υλικού φορέα στον οποίο είναι αποθηκευμένα είτε μόνιμα είτε προσωρινά (λ.χ. το σπάσιμο του σκληρού δίσκου ή της προσωρινής μνήμης (RAM) ή του επεξεργαστή). Ο δεύτερος τρόπος είναι με την επέμβαση στα δεδομένα αυτά. Η επέμβαση αυτή μπορεί να γίνει είτε από τον ίδιο τον δράστη αφού αποκτήσει πρόσβαση στο πληροφοριακό σύστημα όπως εκτέθηκε στο σχετικό χωρίο είτε αυτοματοποιημένα με την χρήση κάποιου προγράμματος χωρίς ο δράστης να είχε ποτέ αποκτήσει πραγματικά πρόσβαση στα δεδομένα παρά μόνο έμμεσα. Στην δεύτερη αυτή γενική περίπτωση περιλαμβάνονται οι περιπτώσεις εισαγωγής κακόβουλου κώδικα (malware) που επεμβαίνει στα δεδομένα.[120]

Ειδικότερα, στην τελευταία αυτή περίπτωση συνήθως το ίδιο το θύμα εγκαθιστά εν αγνοία του το κακόβουλο λογισμικό. Αυτό γίνεται μέσω προγραμμάτων που αποκαλούνται «Δούρειοι Ίπποι» («Trojan Horses»). Τα προγράμματα αυτά παρουσιάζονται στον χρήστη (λ.χ. σε μία ιστοσελίδα ή σε μια ηλεκτρονική επιστολή) ότι επιτελούν ένα συγκεκριμένο σκοπό ή ότι έχουν ένα συγκεκριμένο περιεχόμενο, με αποτέλεσμα ο χρήστης να επιθυμεί την εγκατάστασή του και να τα εγκαθιστά το πληροφοριακό σύστημα. Πλην όμως, δεν επιτελούν (μόνο) αυτό το σκοπό του χρήστη για τον οποίο τα εγκατέστησε αλλά περιέχουν (και)

[120] όχι βέβαια ότι αποκλείεται ο δράστης να εγκαταστήσει τον κακόβουλο αυτό κώδικα ο ίδιο κατόπιν της με οποιοδήποτε τρόπο απόκτησης πρόσβασης στο πληροφοριακό σύστημα.

κακόβουλο κώδικα. Ο κακόβουλος αυτός κώδικας μπορεί να είναι ένας «ιός» («virus»)[121] ο οποίος επεμβαίνει στα ήδη υπάρχοντα δεδομένα του πληροφοριακού συστήματος.

6.6. «Χωρίς δικαίωμα» τέλεση

Πριν ακόμα από την παράθεση των επιμέρους τρόπων τέλεσης της πράξης της φθοράς ηλεκτρονικών δεδομένων, ο νομοθέτης επέλεξε να θέσει ένα στοιχείο το οποίο είναι κοινό για όλους τους ως άνω τρόπους και το οποίο μάλιστα είναι κοινό για όλα τα εγκλήματα που στρέφονται κατά συστημάτων πληροφοριών. Το στοιχείο αυτό δεν είναι άλλο από την έλλειψη δικαιώματος προς την οιαδήποτε σχετική συμπεριφορά.

Συγκεκριμένα σύμφωνα με το άρθρο 2 της Οδηγίας[122], «χωρίς δικαίωμα» σημαίνει ότι η αναφερομένη συμπεριφορά, συμπεριλαμβανομένης της πρόσβασης, παρεμβολής ή υποκλοπής, είναι μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δίκαιου. Περαιτέρω αν και δεν υπήρχε ρητή σχετική πρόβλεψη στο κείμενο της Σύμβασης, στην Αιτιολογική της Έκθεση οριζόταν ότι οι προβλεπόμενες συμπεριφορές, μεταξύ των οποίων και η επέμβαση σε δεδομένα, είναι ποινικά κολάσιμες μόνο όταν τελούνται «χωρίς δικαίωμα»[123]. Στην ίδια λογική, η Οδηγία στην παρ. 17 του προοιμίου της ορίζει ότι *«η παρούσα οδηγία δεν αποδίδει ποινική ευθύνη όταν πληρούνται τα αντικειμενικά κριτήρια των αδικημάτων που ορίζονται στην παρούσα Οδηγία, αλλά οι πράξεις διαπράττονται χωρίς εγκληματική πρόθεση, παραδείγματος χάριν όταν το πρόσωπο δεν γνωρίζει ότι απαγορεύεται η πρόσβαση ή στη περίπτωση εξουσιοδοτημένης δοκιμής ή προστασίας συστημάτων πληροφοριών, όπως όταν μια εταιρία ή ένας πωλητής αναθέτει σε ένα πρόσωπο να ελέγξει την ισχύ συστήματος ασφαλείας του».*

Από τα ανωτέρω προκύπτει αναμφίβολα ότι το «χωρίς δικαίωμα» είναι ειδικό στοιχείο του αδίκου δηλαδή στοιχείο της αντικειμενικής υπόστασης του εγκλήματος και όχι εξωτερικός όρος του αξιοποίνου καθώς αφορά την ίδια την πράξη του δράστη και για το λόγω αυτό πρέπει να καλύπτεται από την απαιτούμενη υπαιτιότητα του.

---

[121] Οι ιοί είναι ένα είδος κακόβουλου προγράμματος, το οποίο όταν αναπαράγεται εισάγοντας τον κώδικά του σε άλλα προγράμματα ή δεδομένα που είναι ήδη εγκατεστημένα στο πληροφοριακό σύστημα το οποίο έχει προσβάλει. Εισάγοντας τον κώδικά του αλλοιώνει τα δεδομένα αυτά ή ακόμα και τα καταστρέφει.

[122] Σκέψη 62 της Αιτιολογικής Έκθεσης της Σύμβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο».

Η μη ύπαρξη, λοιπόν, δικαιώματος δεν αίρει απλά τον άδικο χαρακτήρα της πράξης αλλά καθιστά την ίδια την πράξη ήδη κατ' αρχήν μη άδικη. Δεν ομοιάζει συνεπώς η ύπαρξη δικαιώματος με τη συναίνεση του παθόντος στο έγκλημα της απλής σωματικής βλάβης αλλά με την συγκατάθεση (μη δηλαδή εξαναγκασμό) στην πράξη της συνουσίας που την καθιστά εξ' ορισμού μη ποινικά αξιόλογη.

Σε αυτό το σημείο, αξίζει να επισημανθεί, επίσης, ότι στην Αιτιολογική Έκθεση της Σύμβασης αναφέρεται σχετικά με το ζήτημα ότι *«[σ]υνήθεις συμπεριφορές αναγκαίες για τον σχεδιασμό δικτύων ή συνήθεις διαδικαστικές ή εμπορικές πρακτικές, όπως για παράδειγμα για την δοκιμή ή την προστασία της ασφάλειας ενός υπολογιστικού συστήματος οι οποίες γίνονται με την άδεια του ιδιοκτήτη ή του χρήστη, ή ο επαναπρογραμματισμός του λειτουργικού συστήματος (operating system) ενός υπολογιστή που λαμβάνει χώρα όταν ο χρήστης ενός συστήματος απόκτα νέο λογισμικό (λ.χ. λογισμικό που περιέχει πρόγραμμα που επιτρέπει την πρόσβαση στο διαδίκτυο απενεργοποιώντας παρόμοια προγράμματα που είχαν εγκατασταθεί προηγουμένως), γίνονται «με δικαίωμα» και ως εκ τούτου δεν ποινικοποιούνται από το ως άνω άρθρο».*

Τέλος, τονίζεται ότι την ίδια λογική εξυπηρετεί και το γεγονός ότι στην ελληνική έννομη τάξη η βασική μορφή φθοράς ηλεκτρονικών δεδομένων δεν διώκεται αυτεπάγγελτα αλλά μόνο κατ' έγκληση.

6.7. Διακεκριμένες παραλλαγές

Σύμφωνα με την παρ. 13 του προοιμίου της Οδηγίας της Ε.Ε. για τις επιθέσεις κατά πληροφοριακών συστημάτων *«[ε]ίναι σκόπιμο να προβλεφθούν αυστηρότερες κυρώσεις όταν μια επίθεση κατά συστήματος πληροφοριών διαπράττεται από εγκληματική οργάνωση, όπως ορίζεται στην απόφαση- πλαίσιο 2008/841/ΔΕΥ του Συμβουλίου, της 24ης Οκτωβρίου 2008, για την καταπολέμηση του οργανωμένου εγκλήματος, 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» […] [ε]ίναι επίσης σκόπιμο να προβλεφθούν αυστηρότερες κυρώσεις, όταν η επίθεση διεξάγεται κατά υποδομής ζωτικής σημασίας των κρατών μελών ή της Ένωσης.»* Σχετικά στη παρ. 4 του προοιμίου της Οδηγίας προβλέπεται ότι *«[υ]πάρχουν ορισμένες υποδομές ζωτικής σημασίας στην Ένωση, η διακοπή ή η καταστροφή των οποίων θα μπορούσε να έχει σημαντικό διασυνοριακό αντίκτυπο.»* και ότι *«[έ]χει καταστεί προφανές, λόγω της ανάγκης να ενισχυθεί η προστασία των υποδομών ζωτικής σημασίας στην Ένωση, ότι τα μέτρα*

κατά των επιθέσεων στον κυβερνοχώρο θα πρέπει να συμπληρώνονται με αυστηρές ποινικές κυρώσεις που να αντανακλούν τη σοβαρότητα των επιθέσεων αυτών.»

Στην δεύτερη και την τρίτη λοιπόν παράγραφο του άρθρου 381Α προβλέπονται αυστηρότερες ποινές για τις συμπεριφορές που συνιστούν φθορά ηλεκτρονικών δεδομένων όταν συντρέχουν οι ως άνω επιβαρυντικές περιστάσεις. Τονίζεται δε εκ των προτέρων ότι όλες αυτές οι διακεκριμένες παραλλαγές του εγκλήματος της φθοράς ηλεκτρονικών δεδομένων, διώκονται αυτεπάγγελτα εν αντιθέσει με τη βασική μορφή.

6.7.1 Τέλεση με εργαλείο σχεδιασμένο κατά κύριο λόγο για την τέλεση επιθέσεων που επηρεάζουν μεγάλο αριθμό πληροφοριακών συστημάτων ή που προκαλούν σοβαρές ζημίες

Η πρώτη επιβαρυντική περίσταση είναι όταν η φθορά ηλεκτρονικών δεδομένων τελείται με τη χρήση τεχνικού μέσου – προγράμματος που έχει σχεδιαστεί κατά κύριο λόγο για την πραγματοποίηση α) επιθέσεων που επηρεάζουν μεγάλο αριθμό πληροφοριακών συστημάτων ή β) επιθέσεων που προκαλούν σοβαρές ζημίες. Με βάση τη ρύθμιση αυτή αρκεί απλώς το πρόγραμμα να είχε σχεδιαστεί για την πραγματοποίηση τέτοιου είδους επιθέσεων ανεξάρτητα από το αν μια τέτοια μαζική επίθεση συνέβη ή ανεξάρτητα από το αν επήλθε σοβαρή ζημία.

Πράγματι είναι αντικειμενικά διαγνώσιμο το αν ένα πρόγραμμα έχει τη δυνατότητα και έχει σχεδιαστεί κυρίως για να προκαλέσει τα ως άνω αποτελέσματα. Ωστόσο, η έννοια του όρου «σχεδιασμένο κατά κύριο λόγο» θα πρέπει να ερμηνεύεται στενά, δηλαδή να καταλαμβάνει περιπτώσεις όχι που απλά ο δημιουργός του σχεδίασε το πρόγραμμα για αυτό το σκοπό αλλά και το πρόγραμμα να είναι αντικειμενικά πρόσφορο ως μέσο να έχει δηλαδή αντικειμενικά τη δυνατότητα να επηρεάσει μεγάλο αριθμό πληροφοριακών συστημάτων ή να προκαλέσει σοβαρές ζημίες. Σε κάθε περίπτωση δε σε υποκειμενικό επίπεδο ο δράστης θα πρέπει να γνωρίζει τη δυνατότητα του προγράμματος να προκαλέσει τα περιγραφόμενα αποτελέσματα και μάλιστα την αντικειμενική δυνατότητα και όχι απλώς να γνωρίζε ότι το πρόγραμμα ήταν σχεδιασμένο για αυτό το σκοπό αλλά «γνώριζε» εσφαλμένως ότι ο σκοπός αυτός δεν μπορεί να επιτευχθεί.

Περαιτέρω, η ίδια η διάταξη απαριθμεί ορισμένες ενδεικτικές περιπτώσεις όπου συντρέχει η εν λόγω επιβαρυντική περίσταση και οι οποίες είναι, συγκεκριμένα το πρόγραμμα να έχει σχεδιαστεί με κύριο σκοπό την πρόκληση μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξης των υπηρεσιών πληροφοριακών συστημάτων, την πρόκληση ιδιαίτερα μεγάλης οικονομικής ζημίας και τη σημαντική απώλεια δεδομένων.

Αναφορικά με την πρώτη περίπτωση η οποία αφορά την δυνατότητα πρόκλησης μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξης των υπηρεσιών πληροφοριακών συστημάτων ο όρος αυτός δεν θα πρέπει να θεωρείται ότι διαφέρει από τη «σοβαρή παρακώλυση της λειτουργίας πληροφοριακού συστήματος» η οποία ποινικοποιείται στο άρθρο 281Β Π.Κ..[124] Στην συγκεκριμένη, βέβαια, περίπτωση προβλέπεται απλώς η «δυνατότητα» πρόκλησης των συνεπειών αυτών.

Τέλος, το απειλούμενο πλαίσιο ποινής με την συγκεκριμένη διακεκριμένη παραλλαγή του εγκλήματος της φθοράς ηλεκτρονικών δεδομένων είναι 1 έως 3 έτη. Δηλαδή σε σχέση με το βασικό έγκλημα αυξάνεται απλώς το κατώτατο όριο του πλαισίου ποινής από 10 ημέρες (δεδομένου ότι προβλέπεται ποινή φυλάκισης έως 3 έτη) σε ένα έτος.

6.7.2. Πρόκληση σοβαρών ζημιών

Η δεύτερη επιβαρυντική περίσταση που προβλέπεται στην δεύτερη παράγραφο του άρθρου 381Α Π.Κ. είναι η πρόκληση σοβαρών ζημιών από την πράξη της φθοράς ηλεκτρονικών δεδομένων. Ο όρο αυτός επεξηγείται στην συνέχεια με την ενδεικτική απαρίθμηση ορισμένων περιπτώσεων που κρίνεται από το νομοθέτη ότι συνιστούν σοβαρή ζημία. Η πρώτη από αυτές είναι η μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών συστημάτων πληροφοριών η οποία αναλύεται σε σχέση με το έγκλημα της σοβαρής παρακώλυσης της λειτουργίας πληροφοριακού συστήματος που ποινικοποιείται στο άρθρο 281Β Π.Κ. στο σχετικό χωρίο της παρούσας[125]. Η δεύτερη περίπτωση είναι η ιδιαίτερα μεγάλης αξίας οικονομική ζημία η οποία με βάση τη συστηματική ερμηνεία στο πλαίσιο του ελληνικού ποινικού δικαίου θα πρέπει να υπερβαίνει τις 120.000 ευρώ. Τέλος αναφέρεται ενδεικτικά ως σοβαρή ζημία, η σημαντική απώλεια δεδομένων η οποία ενέχει μία κάποια αοριστία και για αυτό θα πρέπει να γίνεται επίκληση σε αυτή με φειδώ.

Το πλαίσιο ποινής που απειλείται με την συγκεκριμένη διακεκριμένη παραλλαγή της φθοράς ηλεκτρονικών δεδομένων είναι από τουλάχιστον 1 έτος φυλάκισης δηλαδή έως 5 έτη. Αξίζει δε σχετικά να παρατηρηθεί ότι το απειλούμενο αυτό πλαίσιο ποινής είναι σε μεγάλο βαθμό επάλληλο με το πλαίσιο ποινής της βασικής μορφής του εγκλήματος δηλαδή όταν αυτό δεν είχε ως συνέπεια την πρόκληση σοβαρής ζημίας και ακόμα περισσότερο

[124] βλ. αναλυτικότερα για την σύγκριση των δύο όρων, ανωτέρω, σελ 72 επ., ενότητα 5.2.1.7. Προσθήκη του άρθρου 292Β Π.Κ. – Παρακώλυση λειτουργίας πληροφοριακών συστημάτων, iii. Τρόπος τέλεσης, περίπτωση πρώτη.

[125] βλ. ανωτέρω, σελ 72 επ., ενότητα 5.2.1.7. Προσθήκη του άρθρου 292Β Π.Κ. – Παρακώλυση λειτουργίας πληροφοριακών συστημάτων, iii. Τρόπος τέλεσης, περίπτωση πρώτη.

επάλληλο με το απειλούμενο πλαίσιο ποινής της προαναφερθείσας πρώτης επιβαρυντικής περίστασης η οποία αφορά περιπτώσεις που δεν επήλθε τελικά σοβαρή ζημία αν και θα μπορούσε.

6.7.3. Κατά συστημάτων πληροφοριών που συνιστούν μέρος υποδομής για την προμήθεια ζωτικής σημασίας αγαθών ή υπηρεσιών.

Η τρίτη επιβαρυντική περίσταση που προβλέπεται στην δεύτερη παράγραφο του άρθρου 381Α είναι να στρέφεται η πράξη της φθοράς ηλεκτρονικών δεδομένων κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Όπως η ίδια η διάταξη επεξηγεί στην συνέχεια ότι ως ζωτικής σημασίας αγαθά ή υπηρεσίες είναι ενδεικτικά η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

Σύμφωνα δε με το τρίτο εδάφιο της παρ. 4 του προοιμίου της Οδηγίας *«[ω]ς υποδομές ζωτικής σημασίας μπορούν να νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που ευρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των ζωτικών κοινωνιακών λειτουργιών, της υγείας, της ασφάλειας, της προστασίας της οικονομικής ή κοινωνικής ευημερίας, όπως εγκαταστάσεις παραγωγής ενεργείας, μεταφορικά δίκτυα ή κυβερνητικά δίκτυα, και η διακοπή ή η καταστροφή των οποίων θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών».* Η σκέψη αυτή της Οδηγίας είναι ευρύτερη από την ενδεικτική επεξήγηση που δίνεται στην σχετική εθνική διάταξη και δεν αφήνει καμία αμφιβολία ότι στις ζωτικής σημασίας υπηρεσίες περιλαμβάνονται και η αστυνομία και οι τράπεζες ή δυνητικά ακόμα και τα ανταλλακτήρια εικονικών νομισμάτων.

Το απειλούμενο πλαίσιο ποινής και σε αυτή την περίπτωση είναι από 1 έτος έως 5 έτη φυλάκισης.

6.7.4. Στο πλαίσιο εγκληματικής οργάνωσης

Στην τρίτη παράγραφο του άρθρου 381Α προβλέπεται η τέταρτη και αυστηρότερη διακεκριμένη παραλλαγή του εγκλήματος της φθοράς ηλεκτρονικών δεδομένων. Με βάση την διάταξη αυτής της παραγράφου όταν η πράξη της φθοράς ηλεκτρονικών δεδομένων τελείται στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών. Αξίζει να σημειωθεί ότι η ειδική αυτή ρύθμιση έχει πολύ ηπιότερο απειλούμενο πλαίσιο ποινής σε σχέση με το άρθρο 187 Π.Κ. το οποίο προβλέπει γενικά για ορισμένα εγκλήματα μεταξύ και η πλαστογραφία (με υπολογιστή) και η απάτη με υπολογιστή ποινή κάθειρξης έως δέκα έτη.

6.8. Συρροές

6.8.1. Συρροές μεταξύ των τρόπων τέλεσης

Όπως εκτέθηκε το άρθρο 381Α Π.Κ, προβλέπει, ως πράξεις τέλεσης φθοράς ηλεκτρονικών δεδομένων, την διαγραφή, την καταστροφή, την αλλοίωση και την απόκρυψη των δεδομένων ενός πληροφοριακού συστήματος, την κατάσταση ανέφικτης της χρήσης τους και τον με οποιοδήποτε τρόπο αποκλεισμό της πρόσβασης σε αυτά.

Το έγκλημα του άρθρου 381Α Π.Κ. είναι ένα γνήσιο πολύτροπο ή αλλιώς ένα υπαλλακτικώς μικτό έγκλημα. Αυτό σημαίνει ότι όταν οι περισσότερες από τις επιμέρους πράξεις οι οποίες περιγράφονται στην αντικειμενική του υπόσταση τελούνται κατά της ίδιας μονάδας εννόμου αγαθού ο δράστης τελεί ένα έγκλημα. Δεδομένου ότι το έννομο αγαθό που προστατεύεται με το άρθρο αυτό δεν είναι προσωποπαγές καθώς αφορά την υλική υπόσταση των ηλεκτρονικών δεδομένων, ενδιαφέρον παρουσιάζει το ζήτημα του πότε ειρηνεύει το έννομο αγαθό ώστε νέα προσβολή του να συνιστά άλλο έγκλημα.

Αρχικά η περίπτωση που ο δράστης έχει αποκτήσει πρόσβαση σε ένα πληροφοριακό σύστημα με σκοπό να «φθείρει» τα ηλεκτρονικά του δεδομένα και τα «φθείρει», ομοιάζει με την περίπτωση που ένας διαρρήκτης εισέρχεται παράνομα λ.χ. σε μια οικεία και σπάζει ή αφαιρεί τα αντικείμενα που βρίσκονται σε αυτή. Σε αυτή την περίπτωση θα πρέπει να γίνει δεκτό ότι το έγκλημα της φθοράς ηλεκτρονικών δεδομένων τελείται μόνο μια φορά. Το έννομο αγαθό θα ειρηνεύσει μόνο όταν ο δράστης παύσει να έχει πρόσβαση στο σύστημα. Ωστόσο στον ψηφιακό κόσμο το ζήτημα δε είναι τόσο απλό όσο στον υλικό κόσμο. Αν για παράδειγμα ο δράστης αποκτήσει πρόσβαση στο πληροφοριακό σύστημα «από κοντά» δηλαδή με υλική επαφή με αυτό, το έννομο αγαθό θα ειρηνεύσει όταν θα απομακρυνθεί από το πληροφοριακό σύστημα. Αν όμως ο δράστης απέκτησε πρόσβαση στο σύστημα μέσω του διαδικτύου, τότε το έννομο αγαθό θα ειρηνεύσει μόνο όταν αυτός αποσυνδεθεί από αυτό. Πλην όμως κάτι τέτοιο μπορεί να μην συμβεί ποτέ. Σε αυτή την περίπτωση δύο απόψεις μπορούν να υποστηριχθούν, είτε ότι το έννομο αγαθό δεν ειρηνεύει ποτέ, είτε ότι το έννομο αγαθό ειρηνεύει μετά από την πάροδο ενός μεγάλου χρονικού διαστήματος κατά το οποίο δεν εκδηλώθηκε κάποια συμπεριφορά, π.χ. αν ο δράστης διαγράψει τα αρχεία ενός πληροφοριακού συστήματος και μετά από 5 χρόνια που ο ιδιοκτήτης του πληροφοριακού συστήματος εσφαλμένως θεωρεί ότι έχει καλύψει το κενό ασφαλείας που εκμεταλλευτικέ ο δράστης, ο τελευταίος διαγράψει εκ νέου τα δεδομένα του πληροφοριακού αυτού συστήματος. Πρόκειται για ένα πολύ σοβαρό δογματικό ζήτημα.

Από την άλλη, είναι εντελώς διαφορετική η περίπτωση που ο δράστη δεν έχει αποκτήσει ποτέ «πραγματικά» πρόσβαση στο πληροφοριακό σύστημα αλλά έχει παραπλανήσει τον

χρήστη του να εγκαταστήσει έναν ιό ο οποίος και αλλοιώνει τα δεδομένα του πληροφοριακού συστήματος. Αρχικά, όπως έχει επισημανθεί, παρά το γεγονός ότι πρόκειται για μια αυτοματοποιημένη λειτουργία του προγράμματος αυτή εμπίπτει στην έννοια της πράξης του δράστη, όπως συμβαίνει λ.χ. και στην περίπτωση του ιδιοκτήτη ενός εκπαιδευμένου σκύλου τον οποίο προστάζει να επιτεθεί στο θύμα. Πρόκειται δηλαδή για μια περίπτωση έμμεσης αυτουργίας του εγκλήματος εξαπατά το θύμα και αποκτά πρόσβαση με τη χρήση ενός προγράμματος για το σκοπό της τέλεσης μιας εγκληματικής συμπεριφοράς. Σε αυτή την περίπτωση πρόσβαση στο σύστημα έχει αποκτήσει αυτό το αυτοματοποιημένο πρόγραμμα και όσο διαρκεί η επιρροή του επί των δεδομένων του πληροφοριακού συστήματος το έννομο αγαθό διαταράσσεται. Επομένως σε αυτή την περίπτωση τελείται ένα έγκλημα ανεξάρτητα από το αν κάποια αρχεία του πληροφοριακού συστήματος λ.χ. διαγράφονται και κάποια άλλα αποκρύπτονται, δεδομένου μάλιστα ότι το πληττόμενο έννομο αγαθό δεν είναι προσωποπαγές.

Τέλος, ενδιαφέρον παρουσιάζει και η πιο σύνθετη εκδοχή, κατά την οποία το αυτοματοποιημένο πρόγραμμα – ιός μεταδίδεται και σε άλλα πληροφοριακά συστήματα των οποίων τα δεδομένα «φθείρει». Και σε αυτή την περίπτωση θα πρέπει να γίνει δεκτό, δεδομένου ότι το έννομο αγαθό δεν είναι προσωποπαγές, ότι τελείται ένα μόνο έγκλημα. Στην άποψη αυτή συνηγορεί μάλιστα το γεγονός ότι προβλέπεται στην δεύτερη περίπτωση της δεύτερης παραγράφου του άρθρου 381Α Π.Κ. ως επιβαρυντική περίσταση η πρόκληση σοβαρών ζημιών και ενδεικτικά παρατίθεται η μεγάλη έκταση της διατάραξης των υπηρεσιών των πληροφοριακών συστημάτων. Αυτή η πρόβλεψη είναι προφανές ότι δεν αναφέρεται σε μεγάλη έκταση εντός ενός πληροφοριακού συστήματος, Μάλιστα η ίδια η εν λόγω αναφορά γίνεται στο πληθυντικό καθώς αναφέρεται στις υπηρεσίες πληροφοριακών συστημάτων και όχι πληροφοριακού συστήματος. Φαίνεται λοιπόν ότι ο νομοθέτης είχε υπόψη του την εν λόγω περίπτωση και την ενέταξε στην συγκεκριμένη επιβαρυντική περίσταση, διευκρινίζοντας το μάλιστα για να μην υπάρχει καμία αμφιβολία περί τούτου.

6.8.2. Συρροές με τα άλλα εγκλήματα του Ν. 4411/2016

6.8.2.1. Με το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα (άρθρο 370Γ παρ.2 Π.Κ.)

Όπως ήδη επισημάνθηκε, η σειρά με την οποία παρατίθενται τα εγκλήματα που προβλέπονται στην Σύμβαση, η οποία ακολουθείται και στην παρούσα εργασία, είναι από το πιο απλό προς τις πιο σύνθετες μορφές. Το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα είναι αυτό που παρατίθεται πρώτο, δηλαδή το πιο απλό. Στην ίδια λογική, σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης, το έγκλημα της παράνομη

πρόσβασης προστατεύει το έννομο αγαθό της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους (η οποία περαιτέρω αναλύεται στην ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των πληροφορικών συστημάτων και των δεδομένων τους). Από την άλλη, αναφέρεται επίσης ότι το έννομο αγαθό που προστατεύεται με το έγκλημα της φθοράς ηλεκτρονικών δεδομένων είναι η ακεραιότητα και η ορθή λειτουργία ή χρήση αποθηκευμένων δεδομένων, η οποία είναι ειδικότερη έκφανση του εννόμου αγαθού της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους. Σύμφωνα δε με την Οδηγία, τα πληροφοριακά συστήματα και τα δεδομένα τους ανάγονται σε αυτοτελές έννομο αγαθό το οποίο (συμ)προστετεύεται από όλα τα προβλεπόμενα σε αυτή εγκλήματα. Σε κάθε περίπτωση δηλαδή το έννομο αγαθό που προστατεύεται με το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα είναι ευρύτερο από αυτό των άλλων εγκλημάτων συμπεριλαμβανομένου και του εγκλήματος της φθοράς ηλεκτρονικών δεδομένων.

Συχνά ο δράστης για να μπορέσει να τελέσει μια πράξη που συνιστά φθορά ηλεκτρονικών δεδομένων αποκτά πρώτα χωρίς δικαίωμα πρόσβαση στο πληροφοριακό σύστημα στο οποίο είναι αποθηκευμένα τα ηλεκτρονικά δεδομένα. Με άλλα λόγια το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα είναι το μέσο προς την εξυπηρέτηση του σκοπού της φθοράς ηλεκτρονικών δεδομένων. Η πράξη λοιπόν της παράνομης πρόσβασης θα πρέπει να απορροφηθεί από την πράξη της φθοράς ηλεκτρονικών δεδομένων ως πρότερη συντιμωριτή λαμβανομένου και να συναξιολογηθεί κατά το στάδιο της επιμέτρησης της ποινής εντός του πλαισίου ποινής. Μάλιστα, αναφορικά με το γεγονός ότι η πρώτη πράξη (μέσο) ποινικοποιείται με μια διάταξη που παρέχει ευρύτερη προστασία από την δεύτερη (σκοπό), θα πρέπει να γίνει δεκτό ότι σε αυτή την περίπτωση το ευρύτερο έννομο αγαθό της πρώτης πράξης πλήττεται τελικώς υπό τη συγκεκριμένη πτυχή του που προστατεύεται και εξειδικεύεται από την ποινικοποίηση της δεύτερης πράξης, κάτι το οποίο ήταν και το εγκληματικό σχέδιο του δράστης. Συνεπώς υπάρχει φαινομενική συρροή.

Ωστόσο, η ανωτέρω θεωρία δεν μπορεί να εφαρμοσθεί στην πράξη καθώς το έγκλημα της παράνομης πρόσβασης σε πληροφοριακό σύστημα, όπως τυποποιείται στο άρθρο 370Γ παρ. 2 Π.Κ. προβλέπει αυστηρότερο πλαίσιο ποινής (ήτοι φυλάκιση από 10 μέρες έως 5 έτη) από το έγκλημα της φθοράς ηλεκτρονικών δεδομένων του άρθρου 381Α Π.Κ. (φυλάκιση έως 3 έτη) συμπεριλαμβανομένης μάλιστα και της πρώτης διακεκριμένης παραλλαγής του εγκλήματος αυτού (φυλάκιση από 1 έτους έως 3 έτη). Επομένως υπάρχει αξιολογική αντινομία καθώς το έγκλημα της φθοράς ηλεκτρονικών δεδομένων δεν συμπεριλαμβάνει όλη την απαξία της πράξης της παράνομης πρόσβασης. Η αξιολογική δε αυτή αντινομία δεν μπορεί να επιλυθεί με άλλο τρόπο παρά μόνο με διορθωτική νομοθετική παρέμβαση που θα

μειώνει το ανώτατο όριο του πλαισίου ποινή του εγκλήματος της παράνομης πρόσβασης σε πληροφοριακό σύστημα, ακόμα και στα 2 έτη που είναι και το κατώτατο δυνατό ανώτατο όριο πλαισίου ποινής που επιτρέπεται για τα προβλεπόμενά από την Οδηγία εγκλήματα στο άρθρο 9 αυτής[126].

Είναι επίσης δυνατή και η αντίστροφη περίπτωση στην οποία το έγκλημα του άρθρου 381Α Π.Κ τελείται με σκοπό την απόκτηση πρόσβασης ή με άλλα λόγια είναι ο τρόπος με τον οποίο αποκτάται πρόσβαση. Σε αυτή την περίπτωση βέβαια έχουμε μια πράξη φθοράς ηλεκτρονικών δεδομένων με την οποία επιτυγχάνεται και η πρόσβαση. Επομένως τα δύο εγκλήματα συρρέουν κατ' ιδέαν και φαινομενικά γιατί προσβάλλεται το ίδιο έννομο αγαθό και θα εφαρμοσθεί μόνο το άρθρο 370Γ παρ. 2 Π.Κ. με βάση την αρχή της ειδικότητας καθώς δεν πρόκειται για οποιαδήποτε φθορά δεδομένων αλλά ως τρόπος πρόσβασης σε πληροφοριακό σύστημα και επομένως το άρθρο 370Γ παρ. 2 Π.Κ περιγράφει ειδικότερα την πράξη.

6.8.2.2. Με το έγκλημα της παραβίασης του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων (άρθρο 370Δ Π.Κ.)

Όπως έχει ήδη αναφερθεί, τα δεδομένα των πληροφοριακών συστημάτων έχουν δύο υποστάσεις, μια υλική και μια ψηφιακή. Η διάταξη του άρθρου 370Δ Π.Κ. αντιμετωπίζει τα δεδομένα αυτά όχι υπό την υλική τους υπόσταση αλλά ως απόρρητα στοιχεία επικοινωνίας. Αυτό που έχει σημασία δηλαδή, σε αντίθεση με το άρθρο 381Α Π.Κ., δεν είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών αλλά «το δικαίωμα στην ιδιωτική ζωή υπό την έκφανση του απόρρητο των επικοινωνιών και η ασφάλεια των τηλεπικοινωνιών στον κυβερνοχώρο». Πρόκειται δηλαδή για την προστασία δύο διαφορετικών εκφάνσεων της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους. Από την μία με το άρθρο 381Α Π.Κ. προστατεύεται η ακεραιότητα των δεδομένων και από την άλλη με το άρθρο 370Δ Π.Κ. προστατεύεται η εμπιστευτικότητα τους.

Σύμφωνα, δε με την Οδηγία τα πληροφοριακά συστήματα και τα δεδομένα τους ανάγονται σε αυτοτελές έννομο αγαθό που προστατεύεται με τα προβλεπόμενα σε αυτή εγκλήματα μεταξύ των οποίων και το έγκλημα του άρθρου 370Δ Π.Κ.. Ωστόσο, θα πρέπει να γίνει δεκτό ότι το άρθρο αυτό δεν προστατεύει αποκλειστικά το έννομο αγαθό των

[126] Ωστόσο, σε αυτή την περίπτωση θα δημιουργείται πρόβλημα αναφορικά με τις προπαρασκευαστικές πράξεις της παράνομης πρόσβασης που ποινικοποιούνται αυτοτελώς στο άρθρο 370Ε καθώς για αυτές απειλείται ποινή φυλάκισης έως 2 ετών, και δεν είναι δυνατόν να απειλείται η ίδια ποινή τόσο για το βασικό έγκλημα όσο και για τις προπαρασκευαστικές του πράξεις.

πληροφοριακών συστημάτων και των δεδομένων τους αλλά από κοινού με το έννομο αγαθό απορρήτου του περιεχομένου τους στο πλαίσιο της επικοινωνίας.

Για όλους του ανωτέρω λόγους κρίνεται ορθή η άποψη ότι τα έννομα αγαθά που προστατεύονται με τις διατάξεις των ως άνω δύο εγκλημάτων δεν ταυτίζονται και επομένως τα εγκλήματα αυτά συρρέουν μεταξύ τους αληθινά.

6.8.2.3. Με το έγκλημα της παρακώλυσης λειτουργίας πληροφοριακών συστημάτων (άρθρο 292Β Π.Κ.)

Όπως ήδη εκτέθηκε στο σχετικό χωρίο, το στοιχείο η' του άρθρου 13 Π.Κ. όπως αυτό προστέθηκε με την πρώτη παράγραφο του άρθρου δεύτερου του Ν. 4411/2016 προβλέπει ότι «*[π]ληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια 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 λειτουργιά, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών».*

Το έγκλημα της φθοράς ηλεκτρονικών δεδομένων ποινικοποιεί τη διαγραφή, καταστροφή, αλλοίωση ή απόκρυψη ψηφιακών δεδομένων ενός συστήματος πληροφοριών, την κατάσταση της χρήσης τους ως ανέφικτης και τον με οποιοδήποτε τρόπο αποκλεισμό της πρόσβασης στα δεδομένα αυτά. Αντίστοιχα, το έγκλημα της παρακώλυσης λειτουργίας πληροφοριακών συστημάτων ποινικοποιεί την σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά. Και τα δύο εγκλήματα απαιτούν οι ως άνω συμπεριφορές να έγιναν χωρίς δικαίωμα και με δόλο.

Και τα δύο εγκλήματα, σύμφωνα με την Σύμβαση, εντάσσονται κάτω από το γενικό τίτλο αυτών που στρέφονται κατά της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους δηλαδή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων υπολογιστών. Ωστόσο, ειδικότερα σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης προστατευόμενο έννομο αγαθό στο έγκλημα της παρακώλυσης της λειτουργίας πληροφοριακών συστημάτων είναι το δικαίωμα του χρήστη να έχει μια «κανονική» λειτουργία του υπολογιστή του, ενώ προστατευόμενο έννομο αγαθό στο έγκλημα της φθοράς ηλεκτρονικών δεδομένων είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών. Σε αυτό το σημείο θα πρέπει δε να γίνει δεκτό ότι τα ανωτέρω προβλεπόμενα στην Σύμβαση και την Αιτιολογική της Έκθεση εξειδικεύουν και ερμηνεύουν την Οδηγία

που ανάγει τα πληροφοριακά συστήματα και τα δεδομένα τους σε αυτοτελές έννομο αγαθό εν γένει.

Όπως περαιτέρω παρατηρείται, η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών φαίνεται να υπονοείται και να προϋποτίθεται ως έννομο αγαθό που προστατεύεται με τη θέσπιση του εγκλήματος της παρακώλυσης της λειτουργίας πληροφοριακών συστημάτων. Η προστασία της «κανονικής» λειτουργίας του υπολογιστή προϋποθέτει τη διατήρηση της ακεραιότητας και της κανονικής λειτουργίας ή χρήσης των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

Επομένως, σύμφωνα με τα ανωτέρω, σε περιπτώσεις διαγραφής, καταστροφής, αλλοίωσης ή απόκρυψης ψηφιακών δεδομένων ενός συστήματος πληροφοριών, της κατάστασης της χρήσης τους ως ανέφικτης και του με οποιοδήποτε τρόπο αποκλεισμού της πρόσβασης στα δεδομένα αυτά, οι οποίες έχουν ως αποτέλεσμα την σοβαρή[127] παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, έχουμε φαινομενική κατ' ιδέαν συρροή μεταξύ του εγκλήματος της παρακώλυσης λειτουργίας πληροφοριακών συστημάτων (άρθρο 292Β Π.Κ.) και του εγκλήματος της φθορά ηλεκτρονικών δεδομένων (άρθρο 381Α Π.Κ.), οπότε και θα πρέπει να εφαρμοσθεί μόνο το πρώτο και μάλιστα με βάση την αρχή της ειδικότητας και όχι με βάση την αρχή της απορρόφησης καθώς το 292Β Π.Κ. περιλαμβάνει στα στοιχεία της αντικειμενικής του υπόστασης όλα τα στοιχεία της αντικειμενικής υπόστασης του άρθρου 381Α Π.Κ., με αποτέλεσμα να μην μπορεί να συνεκτιμηθεί από το δικαστήριο κατά την επιβολή της ποινής εντός του προβλεπόμενου πλαισίου και η τέλεση φθοράς ηλεκτρονικών δεδομένων σε αυτές τις περιπτώσεις. Ενδιαφέρον δε σχετικά παρουσιάζει το γεγονός ότι και τα δύο εγκλήματα απειλούν στην βασική του μορφή ποινή φυλάκισης από 10 ημέρες έως 3 έτη παρότι όπως εκτέθηκε η παρακώλυση της λειτουργία ενός πληροφοριακού συστήματος δύναται στις περισσότερες περιπτώσεις να αποτελεί το κάτι παραπάνω σε σχέση με την φθορά ηλεκτρονικών δεδομένων και παρότι, μάλιστα, αυτή ποινικοποιείται μόνο όταν είναι σοβαρή.

Υπάρχουν ωστόσο και περιπτώσεις που τελείται παρακώλυση πληροφοριακού συστήματος χωρίς να τελείται φθορά ηλεκτρονικών δεδομένων καθώς στο άρθρο 292Β Π.Κ. προβλέπονται ως τρόποι τέλεσης του εγκλήματος της παρακώλυσης της λειτουργίας πληροφοριακού συστήματος η εισαγωγή και η διαβίβαση ηλεκτρονικών δεδομένων, οι

[127] Αν η παρεμπόδιση δεν είναι σοβαρή τότε δεν πληρούται η αντικειμενική υπόσταση του άρθρου 292Β Π.Κ. και εφαρμόζεται το άρθρο 381Α Π.Κ..

οποίες δεν προβλέπονται στο άρθρο 381Α Π.Κ.. Επομένως είναι δυνατό να έχουμε παρακώλυση της λειτουργίας ενός πληροφοριακού συστήματος όταν γίνεται με αυτούς τους τρόπους χωρίς να έχουμε φθορά ηλεκτρονικών δεδομένων. Σε αυτή την περίπτωση θα πρέπει να γίνει δεκτό ότι τα δύο εγκλήματα συρρέουν μεταξύ τους αληθινά.

6.8.2.4. Με την απάτη με υπολογιστές (άρθρο 386Α Π.Κ.)

Με το Ν. 4411/2016 τροποποιήθηκε το άρθρο 386Α Π.Κ. και στην οποία περιλαμβάνεται πλέον ρητά στις περιπτώσεις απάτης με υπολογιστή και η χρήση (ορθών) δεδομένων που γίνεται χωρίς δικαίωμα, όπως π.χ. στην περίπτωση του δράστη που έχει αποκτήσει παράνομα το όνομα χρήστη και τον κωδικό χρήσης του δικαιούχου.

Το άρθρο αυτό κατά τα λοιπά παρέμεινε ως είχε καθώς κρίθηκε ότι είναι σύμφωνο με το άρθρο 8 της Σύμβασης το οποίο ορίζει «*[κ]άθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η από πρόθεση και άνευ δικαιώματος πρόκληση απώλειας ξένης περιουσίας δια της α) εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή, β) παρέμβασης στην λειτουργία ενός συστήματος υπολογιστή, με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο».*

Από την διατύπωση του άρθρου αυτού και συγκεκριμένα της πρώτης περίπτωσής του, γίνεται αντιληπτό ότι το έγκλημα της απάτης με υπολογιστή δύναται να τελείται με πράξεις που συνιστούν το έγκλημα της φθοράς ηλεκτρονικών δεδομένων.[128] Όταν λοιπόν τελείται μια πράξη που συνιστά φθορά ηλεκτρονικών δεδομένων και παράλληλα πληρούνται και τα λοιπά στοιχεία της αντικειμενικής υπόστασης του εγκλήματος της απάτης με υπολογιστή, τότε τα δύο αυτά εγκλήματα συρρέουν μεταξύ τους κατ' ιδέαν. Συρρέουν δε μεταξύ τους και φαινομενικά καθώς θα πρέπει να γίνει δεκτό ότι το έγκλημα του άρθρου 386Α Π.Κ. συμπροστατεύει μαζί με το έννομο αγαθό της περιουσίας και το έννομο αγαθό της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους, πτυχή της οποίας είναι και η ακεραιότητα των δεδομένων αυτών η οποία προστατεύεται με το άρθρο 381Α Π.Κ..

Επομένως, στη περίπτωση αυτή που τα δύο αυτά εγκλήματα συρρέουν μεταξύ τους κατ' ιδέαν φαινομενικά, δεδομένου ότι στο έγκλημα της απάτης με υπολογιστή τυποποιούνται

[128] Οι περιπτώσεις αυτές θα πρέπει να γίνει δεκτό ότι υπάγονται στην δεύτερη περίπτωση που προβλέπεται στο άρθρο 386Α Π.Κ. ήτοι τη μη ορθή διαμόρφωση προγράμματος υπολογιστή, δεδομένου ότι όπως εκτέθηκε σύμφωνα με στοιχ. θ' του άρθρου 13 Π.Κ., τα προγράμματα υπολογιστών εντάσσονται στην έννοια των ψηφιακών δεδομένων. Ωστόσο για αυτόν ακριβώς το λόγο, ότι τα προγράμματα δεν ταυτίζονται με τα δεδομένα αλλά περιλαμβάνονται σε αυτά, απορία γεννάται αναφορικά με το που υπάγονται οι περιπτώσεις που αφορούν δεδομένα που δεν είναι προγράμματα.

επιπλέον στοιχεία της αντικειμενικής υπόστασης σε σχέση με το έγκλημα της φθοράς, ο δράστης θα τιμωρηθεί μόνο για το έγκλημα της απάτης με υπολογιστή με βάση την αρχή της ειδικότητας.

6.8.3. Με άλλα εγκλήματα

6.8.3.1. Με το έγκλημα της φθοράς ξένης ιδιοκτησίας

Είχε υποστηριχθεί, ότι οι συμπεριφορές που συνιστούν τρόπους τέλεσης του εγκλήματος της φθοράς ηλεκτρονικών δεδομένων στοιχειοθετούν πάντα φθορά ξένης ιδιοκτησίας, όχι υπό την έννοια της προσβολής των πληροφοριών αλλά ως επέμβαση στον υλικό φορέα τους, όταν αυτά βέβαια είναι ενσωματωμένα σε ένα υλικό φορέα, με την λογική ότι αυτές οι επεμβάσεις στα δεδομένα αποτυπώνονται σε υλικό φορέα του πληροφοριακού συστήματος με την μεταβολή της κατεύθυνση και του φορτίου διπολικών στοιχείων, αλλά και επειδή υπάρχει μείωση της κατά προορισμό χρηστικότητας του πράγματος.[129] Ωστόσο, η άποψη αυτή είχε υποστηριχθεί ως μια λύση για την κάλυψη του νομοθετικού κενού που υπήρχε για την ποινικοποίηση των συμπεριφορών πριν την θεσμοθέτηση του άρθρου 381Α Π.Κ. με το Ν. 4411/2016, το οποίο πλέον καλύπτει όλη την απαξία της πληροφοριακής βλάβης[130].

Για το λόγο αυτό, πλέον γίνεται δεκτό ότι, για να κριθεί ότι μια πράξη που συνιστά τρόπο τέλεσης του εγκλήματος της φθοράς ηλεκτρονικών δεδομένων συνιστά και φθορά ξένης ιδιοκτησίας (άρθρο 381 Π.Κ.), πρέπει παράλληλα να υπάρχει και καταστροφή ή βλάβη του υλικού φορέα στον οποίο είναι εγγεγραμμένα τα δεδομένα.[131] Στην Θεωρία αναφέρεται ως παράδειγμα τέτοιας περίπτωσης το γέμισμα του σκληρού δίσκου που καθιστά αδύνατη τη χρήση του. Ωστόσο αυτή η περίπτωση δεν μπορεί να υπαχθεί στην νομοτυπική μορφή του εγκλήματος του άρθρου 381Α Π.Κ. για το λόγο ότι από τη στιγμή που η μονάδα αποθήκευσης είναι σταθερή, δηλαδή ενσωματωμένη με το πληροφοριακό σύστημα, όπως εδώ ο σκληρός δίσκος ενός υπολογιστή, αν καταστεί αδύνατη η χρήση του σκληρού δίσκου θα τελείται το έγκλημα της παρακώλυσης πληροφοριακού συστήματος. Μάλιστα, επιπλέον, στην συγκεκριμένη περίπτωση, το γέμισμα του σκληρού δίσκου είναι δυνατό να τελεστεί, όπως είναι αυτονόητο, μόνο με εισαγωγή δεδομένων, η οποία δεν περιλαμβάνεται στους τρόπους τέλεσης του εγκλήματος της φθορά ηλεκτρονικών δεδομένων αλλά μόνο στους τρόπους εγκλήματος της παρακώλυσης πληροφοριακού συστήματος.

---

[129] βλ. Χ. Μυλωνόπουλου, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991σελ 25-26.

[130] Για τη σχέση εννόμου του εννόμου αγαθού ιδιοκτησίας με το έννομο αγαθό που προστατεύεται με το άρθρο 381Α Π.Κ. βλ. ανωτέρω υποενότητα 6.4. Το προστατευόμενο έννομο αγαθό.

[131] Βλ. Δ. Κιούπη, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, Υπεράσπιση 2000 σελ. 956 επ., του ίδιου Ποινικό δίκαιο και Internet, Ποινικά 57, 1999 σελ. 139-140.

Το έγκλημα της φθοράς ηλεκτρονικών δεδομένων μπορεί να συρρέει με το έγκλημα της φθοράς ξένης ιδιοκτησίας μόνο όταν ο υλικός φορέας στον οποίο είναι αποθηκευμένα τα δεδομένα δεν εμπίπτει στην έννοια του πληροφοριακού συστήματος δηλαδή δεν αποτελεί μέρος ενός τέτοιου. Τέτοιες περιπτώσεις είναι οι εξωτερικοί σκληροί δίσκοι, τα «στικάκια» USB, τα CD κ.λπ. Σε αυτές της περιπτώσεις αν γίνει υπερφόρτωση με την εισαγωγή δεδομένων από ένα πληροφοριακό σύστημα σε βαθμό που να καθίσταται αδύνατη η χρήση του υλικού αυτού φορέα τότε τελείται φθορά ξένης ιδιοκτησίας και φθορά ηλεκτρονικών δεδομένων καθώς ο υλικός φορέας περιείχε ηλεκτρονικά δεδομένα τα οποία πλέον δεν είναι ακέραια ή διαθέσιμα. Το ίδιο ισχύει και στην περίπτωση που πλήττεται ο υλικός φορέας με υλική πράξη φθοράς και λόγω της αδυναμίας χρήσης του δεν είναι διαθέσιμα τα αποθηκευμένα δεδομένα. Επισημαίνεται δε ότι και στις δύο αυτές περιπτώσεις ουσιαστικά η φθορά του υλικού φορέα είναι αυτή που έχει ως συνέπεια την απώλεια των δεδομένων

6.8.3.2. Με τα εγκλήματα που προστατεύουν τα υπομνήματα (πλαστογραφία με υπολογιστή και υπεξαγωγή ηλεκτρονικού εγγράφου)

Με το άρθρο 7 της Σύμβασης προβλέπεται η υποχρέωση των Συμβαλλόμενων Μερών να καταστήσουν αξιόποινη την πλαστογραφία μέσω υπολογιστή.

Συγκεκριμένα ορίζεται το εξής:

«*«Άρθρο 7 – Πλαστογραφία σχετική με υπολογιστές*

Κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η από πρόθεση και άνευ δικαιώματος εισαγωγή, αλλοίωση, διαγραφή ή καταστολή δεδομένων υπολογιστή, που έχει ως αποτέλεσμα την παραγωγή μη αυθεντικών δεδομένων με σκοπό να θεωρηθούν αυτά αυθεντικά ή να γίνουν ενέργειες με βάση αυτά ωσάν να είναι αυθεντικά για νόμιμους σκοπούς, ασχέτως του εάν αυτά τα δεδομένα είναι ή όχι άμεσα αναγνώσιμα ή αντιληπτά. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεσή θεμελίωσης ποινικής ευθύνης την ύπαρξης πρόθεσης εξαπάτησης ή παρόμοια αθέμιτης πρόθεσης».

Σκοπός του άρθρου αυτού ήταν η εναρμόνιση της «παραδοσιακής» πλαστογραφία, με αυτή που διαπράττεται με ηλεκτρονικά μέσα. Προστατευόμενο έννομο αγαθό είναι η ασφάλεια, αξιοπιστία, πίστη και εγκυρότητα των ηλεκτρονικών δεδομένων, των οποίων η χρήση έχει έννομες συνέπειες.

Σχετικά σύμφωνα με την περ. γ’ του άρθρου 13, όπως αυτό προστέθηκε με το άρθρο 2 Ν 1805/1988 *«έγγραφο είναι κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός […] [ε]γγραφο είναι και κάθε μέσο στο οποίο χρησιμοποιείται από υπολογιστή*

ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία». Δεδομένης της πρόβλεψης αυτής ο Έλληνας νομοθέτης ορθώς έκρινε ότι τόσο ο σκοπός όσο και το περιεχόμενο του άρθρου 7 της Σύμβασης καλύπτεται από το άρθρο 216 Π.Κ. σε συνδυασμό με το άρθρο 13 περ. γ' Π.Κ. και ως εκ τούτου δεν ήταν απαραίτητη την τυποποίηση νέου, ειδικού εγκλήματος πλαστογραφίας μέσω υπολογιστή.

Σε σχέση με το έγκλημα της φθοράς ηλεκτρονικών δεδομένων, είχε παρατηρηθεί[132] ότι «εφόσον τα δεδομένα είναι σταθερά ενσωματωμένα σε υλικό φορέα και μπορούμε να κάνουμε λόγο για έγγραφο για το οποίο προκύπτει ο εκδότης, η αλλοίωση των δεδομένων αν επηρεάζει την αποδεικτική τους σημασία θα μπορούσε να αποτελεί πλαστογραφία (άρθρο 216 Π.Κ. [133]), στο μέτρο που συνοδεύεται από τον σκοπό παραπλάνησης άλλου με τη χρήση του εγγράφου που θα μπορούσε να έχει έννομες συνέπειες».[134] Μάλιστα από την ίδια την διατύπωση του άρθρου 7 της Σύμβασης προκύπτει ότι η πλαστογραφία με υπολογιστή τελείται κατ' ουσίαν με τους ίδιους τρόπους με τους οποίους τελείται και η φθορά ηλεκτρονικών δεδομένων, πλέον της εισαγωγής δεδομένων. Εφόσον λοιπόν υπάρχει «φθορά» δεδομένων δηλαδή επέμβαση στα δεδομένα με ένα από τους περιγραφόμενους στο άρθρο 381Α Π.Κ. τρόπους και επιπλέον πληρούνται οι προϋποθέσεις ώστε τα δεδομένα να

---

[132] Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1075 επ.

[133] *«Άρθρο 216 - Πλαστογραφία*

1. Όποιος καταρτίζει πλαστό ή νοθεύει έγγραφο με σκοπό να παραπλανήσει με τη χρήση του άλλον σχετικά με γεγονός που μπορεί να έχει έννομες συνέπειες τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Η χρήση του εγγράφου από αυτόν θεωρείται επιβαρυντική περίπτωση.

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

3. Αν ο υπαίτιος αυτών των πράξεων (παράγραφοι 1-2) σκόπευε να προσπορίσει στον εαυτό του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον τιμωρείται με κάθειρξη μέχρι δέκα ετών εάν το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των εβδομήντα εκατό είκοσι χιλιάδων (120.000) ευρώ. Με την ίδια ποινή τιμωρείται ο υπαίτιος που διαπράττει πλαστογραφίες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των τριάντα χιλιάδων (30.000) ευρώ.»

[134] Βλ. αναλυτικά για το έγκλημα της πλαστογραφίας με υπολογιστή, Χ. Μυλωνόπουλου, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991 σελ. 42-53.

μπορούν να υπαχθούν στην έννοια του εγγράφου και υπάρχει σκοπός παραπλάνησης σχετικά με γεγονός που μπορεί να έχει έννομες και γίνεται χρήση των δεδομένων αυτών, τότε σε αυτή την περίπτωση συρρέει το έγκλημα της φθοράς ηλεκτρονικών δεδομένων του άρθρου 381Α Π.Κ. με το έγκλημα της πλαστογραφίας με υπολογιστή του άρθρου 261 Π.Κ. σε συνδυασμό με το άρθρο 13 στ. γ' Π.Κ.. Σε αυτή την περίπτωση θα πρέπει αρχάς να γίνει δεκτό ότι το έγκλημα της πλαστογραφίας με υπολογιστής συμπροστατεύει από κοινού με το έννομο αγαθό του υπομνήματος και το έννομο αγαθό της ακεραιότητας των δεδομένων το οποίο προστατεύεται με το έγκλημα της φθοράς ηλεκτρονικών δεδομένων. Επομένως τα δύο εγκλήματα θα συρρέουν μεταξύ του κατ' ιδέαν φαινομενικά και θα εφαρμοσθεί μόνο το άρθρο 261 Π.Κ. σε συνδυασμό με το άρθρο 13 στ. γ' Π.Κ. με βάση την αρχή της ειδικότητας, καθώς το έγκλημα αυτό του δράστη περιγράφεται ακριβέστερα στα άρθρα αυτά και αποτελεί το κάτι παραπάνω από το έγκλημα της φθοράς ηλεκτρονικών δεδομένων.

Αντίστοιχα, σε περιπτώσεις που τα δεδομένα πληρούν τις προϋποθέσεις της έννοιας του εγγράφου, όπως αυτές περιγράφονται στο στοιχείο γ' του άρθρου 13 Π.Κ. και η «φθορά» των ηλεκτρονικών δεδομένων γίνεται με σκοπό απλώς βλάβης του θύματος, τότε η συμπεριφορά του δράστη έκτος από την αντικειμενική υπόσταση του εγκλήματος της φθοράς ηλεκτρονικών δεδομένων όπως αυτή περιγράφεται στο άρθρο 381Α Π.Κ. μπορεί να υπαχθεί και στο έγκλημα της υπεξαγωγής εγγράφου (άρθρο 222 Π.Κ.[135]). Το έγκλημα της υπεξαγωγής ηλεκτρονικού εγγράφου ποινικοποιεί το κάτι παραπάνω από αυτό της φθοράς ηλεκτρονικών δεδομένων καθώς θα πρέπει να συντρέχουν ειδικότερα οι προϋποθέσεις του εγγράφου. Επίσης όπως αναλύθηκε και στην περίπτωση του άρθρου 216 Π.Κ. το άρθρο αυτό δεδομένου ότι συνδυάζεται με το άρθρο 13 στ. γ' Π.Κ. συμπροστατεύει μαζί με το έννομο αγαθό του υπομνήματος και το έννομο αγαθό της ακεραιότητας των ηλεκτρονικών δεδομένων. Για τους λόγους αυτούς τα δύο εγκλήματα συρρέουν μεταξύ του κατ' ιδέαν φαινομενικά και θα εφαρμοσθεί μόνο η διάταξη του άρθρου 222 Π.Κ. σε συνδυασμό με το άρθρο 13 στ. γ' Π.Κ με βάση την αρχή της ειδικότητας. Ωστόσο στην περίπτωση αυτή συμβαίνει το εξής παράδοξο, ότι το έγκλημα της υπεξαγωγής ηλεκτρονικού εγγράφου προβλέπει ηπιότερο πλαίσιο ποινής (ήτοι 10 μέρες έως 2 έτη φυλάκιση) από το έγκλημα της

[135] *«Άρθρο 222 - Υπεξαγωγή εγγράφων*

Όποιος με σκοπό να βλάψει άλλον αποκρύπτει, βλάπτει ή καταστρέφει έγγραφο του οποίου δεν είναι κύριος ή δεν είναι αποκλειστικά κύριος ή που άλλος έχει δικαίωμα, κατά τις διατάξεις του αστικού δικαίου, να ζητήσει την παράδοση ή την επίδειξή του τιμωρείται με φυλάκιση μέχρι δύο ετών.»

φθοράς ηλεκτρονικών δεδομένων ακόμα και στη βασική του μορφή (ήτοι 10 μέρες έως 3 έτη)[136].

6.8.3.3. Με τις διατάξεις για την προστασία προσωπικών δεδομένων και πνευματικών δικαιωμάτων

Οι διατάξεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και την προστασία των πνευματικών δικαιωμάτων προστατεύουν τα ηλεκτρονικά δεδομένα και υπό την υλική τους υπόσταση όταν αυτά έχουν συγκεκριμένο περιεχόμενο. Αν η μερική αλλοίωση ή ολοσχερής εξάλειψη αφορά δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών δημοσίου δικτύου ηλεκτρονικών επικοινωνιών υπάγεται με τις διατάξεις των άρθρων 22 παρ. 4 Ν. 2472/1997 και 15 παρ. 1 Ν. 3471/2006. Αντίστοιχα, αν η αλλοίωση προγράμματος υπολογιστή μπορεί να υπαχθεί με το άρθρο 66 παρ. Ν. 2121/1993 για την πνευματική ιδιοκτησία, στο μέτρο που τέτοιες αλλοιώσεις αποτελούν μη επιτρεπόμενη διασκευή προσαρμογή ή μετατροπή προγράμματος και με την προϋπόθεση, βέβαια ότι τούτο έχει και τα χαρακτηριστικά του έργου που προστατεύεται από τον παραπάνω νόμο[137].

Οι διατάξεις αυτές θα συρρέουν κατά περίπτωση με την διάταξη του άρθρου 381Α Π.Κ., όταν τελείται μια συμπεριφορά που συνιστά τρόπο τέλεση φθορά ηλεκτρονικών δεδομένων. Η συρροή θα πρέπει να γίνει δεκτό ότι είναι κατ' ιδέαν φαινομενική, και δεδομένου ότι τα εγκλήματα αυτά στην αντικειμενική τους υπόσταση απαιτούν κάτι επιπλέον σε σχέση με το έγκλημα της φθοράς ηλεκτρονικών δεδομένων, θα πρέπει να εφαρμοσθούν αποκλειστικά οι διατάξεις των άρθρων που ποινικοποιούν τα εγκλήματα αυτά με βάση την αρχή της ειδικότητας.

[136] Ωστόσο η μείωση του ανώτατου ορίου του πλαισίου ποινής της φθοράς ηλεκτρονικών δεδομένων στα 2 έτη θα δημιουργούσε πρόβλημα λόγω του γεγονότος ότι στο άρθρο 381Β Π.Κ. που ποινικοποιούνται αυτοτελώς οι προπαρασκευαστικές πράξεις της φθοράς ηλεκτρονικών δεδομένων απειλείται πλαίσιο ποινής φυλάκισης με ανώτατο όριο τα 2 έτη όπως επιβάλλεται κατ' ελάχιστον από το άρθρο 9 της Οδηγίας ανεξαιρέτως για όλα τα προβλεπόμενα σε αυτή εγκλήματα.

[137] Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1075.

7. Προπαρασκευαστικές πράξεις

7.1. Η σχετικές διατάξεις της Σύμβασης και της Οδηγίας

Σ αυτό το σημείο κρίνεται σκόπιμο να γίνει συνοπτική παράθεση του περιεχομένου του άρθρου 6 της Σύμβασης και του άρθρου 7 της Οδηγίας στα οποία βασίστηκε ο Έλληνας νομοθέτης για την ποινικοποίηση των προπαρασκευαστικών πράξεων ορισμένων εκ των προβλεπόμενων στο Ν. 4411/2016 πράξεων.[138]

7.1.1. Το άρθρο 6 της Σύβασης του Συμβουλίου της Ευρώπης «για το έγκλημα στον Κυβερνοχώρο»

Με το άρθρο 6 της Σύμβαση προβλεπόταν τα Συμβαλλόμενα Μέρη να λάβουν μέτρα για την ποινικοποίηση εκ προθέσεως και άνευ δικαιώματος παραγωγή, πώληση, εισαγωγή, διανομή ή με κάθε τρόπο διάθεση αλλά και την κατοχή α) συσκευής ή προγράμματος σχεδιασμένων ή προσαρμοσμένων πρωτίστως για την τέλεση συμπεριφορών που συνιστούν τα εγκλήματα, της παράνομης πρόσβασης σε πληροφοριακό σύστημα, της παραβίασης του απορρήτου πληροφοριακών συστημάτων, της φθορά ηλεκτρονικών δεδομένων και της παρακώλυσης της λειτουργίας πληροφοριακού συστήματος, και β) κωδικών πρόσβασης ή παρεμφερών στοιχείων με τα οποία μπορεί να αποκτηθεί πρόσβαση σε πληροφοριακά συστήματα, όταν γίνονται με πρόθεση διάπραξης κάποιου εκ των προαναφερθέντων εγκλημάτων. Περαιτέρω εξαιρούσε ρητά περιπτώσεις τέλεσης των πράξεων με σκοπό την πραγματοποίηση επιτρεπτών δοκιμών ή για την προστασία ενός συστήματος υπολογιστή, ενώ παράλληλα έδινε την δυνατότητα στα Συμβαλλόμενα Μέρη εξαρτήσουν την ποινικοποίηση των ως άνω συμπεριφορών από την κατοχή ενός συγκεκριμένου αριθμού των αναφερόμενων αντικειμένων, καθώς και μη ποινικοποίησης των συμπεριφορών πλην αυτών που συνιστούν με κάθε τρόπο διάθεση συνθηματικών, κωδικών πρόσβασης σε πληροφοριακά συστήματα ή παρεμφερών στοιχείων.

7.1.2. Το άρθρο 7 της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

Με το άρθρο 7 της Οδηγίας τα Κράτη Μέλη ανέλαβαν την υποχρέωση να ποινικοποιήσουν την εκ προθέσεως χωρίς δικαίωμα στην εσωτερική έννομη τάξης τους την εκ προθέσεως και άνευ δικαιώματος πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή η με κάθε τρόπο διάθεση α) προγραμμάτων σχεδιασμένων ή προσαρμοσμένων πρωτίστως για

[138] Για το κείμενο των άρθρων καθώς και για εκτενέστερη ανάλυση του περιεχομένου του βλ. τα σχετικά χωριά της παρούσας, ανωτέρω υποενότητα 3.2.2 στοιχ. i. υποστοιχ, Ε σελ. 25 για το άρθρο 6 της Οδηγίας και υποενότητα. 4.2.3.5 σελ. 40 για το άρθρο 7 της Σύμβασης και τη σύγκριση του με το άρθρο 6 της Οδηγίας.

την τέλεση συμπεριφορών που συνιστούν τα εγκλήματα, της παράνομης πρόσβασης σε πληροφοριακό σύστημα, της παραβίασης του απορρήτου πληροφοριακών συστημάτων, της φθορά ηλεκτρονικών δεδομένων και της παρακώλυσης της λειτουργίας πληροφοριακού συστήματος β) κωδικών πρόσβασης ή παρεμφερών στοιχείων με τα οποία μπορεί να αποκτηθεί πρόσβαση σε πληροφοριακά συστήματα, όταν γίνονται με πρόθεση διάπραξης κάποιου εκ των προαναφερθέντων εγκλημάτων.

7.2. Η συμμόρφωση της ελληνικής έννομης τάξης με τις υποχρεώσεις που ανέλαβε με το άρθρο 6 της Σύμβασης και το άρθρο 7 της Οδηγίας.

7.2.1 Τα κείμενα των διατάξεων

«Άρθρο 370Ε

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται οποίος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, β) 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».

« Άρθρο 292Γ

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκλημάτων του άρθρου 292Β, β) 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».»

«Άρθρο 381Β

Με φυλάκιση μέχρι δύο (2) ετών, τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα του άρθρου 381Α παράγραφοι 1, 2 και 3 παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα του άρθρου 381Α, β) 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».

7.2.2 Ο λόγος θέσπισης τριών επιμέρους άρθρων

Με το Ν. 4411/2016 ο Έλληνας νομοθέτης επέλεξε να συμμορφωθεί με τις υποχρεώσεις που ανέλαβε με το άρθρο 6 της Σύμβασης της Βουδαπέστης και το άρθρο 7 της Οδηγίας για της επιθέσεις κατά συστημάτων πληροφοριών, θεσπίζοντας και εισάγοντας στον Π.Κ. όχι μία γενική διάταξη που να περιλαμβάνει της προπαρασκευαστικές πράξεις των προβλεπόμενων εγκλημάτων, αλλά τρείς ειδικές διατάξεις μετά από τα σχετικά άρθρα με τα οποία γίνεται ποινικοποίηση των βασικών εγκλημάτων. Η επιλογή αυτή οφείλεται στο γεγονός ότι παρά την σχετική πρόταση, τα εγκλήματα που στρέφονται κατά των πληροφοριακών συστημάτων και των δεδομένων τους δεν θα εντάχθηκαν όλα μαζί σε ένα νέο κεφάλαιο του Π.Κ. αλλά προστέθηκαν διάσπαρτα σε διάφορα κεφάλαια κοντά σε εγκλήματα με τα οποία κατά κάποιο τρόπο σχετίζονται. Αυτό είχε ως συνέπεια να μην μπορεί να εισαχθεί μια διάταξη που να τα περιλαμβάνει όλα καθώς εντός του συστήματος του Π.Κ. τα άρθρα αυτά τουλάχιστον χωροταξικά δεν σχετίζονται. Επομένως δεδομένων όλων των ανωτέρω ορθώς ο νομοθέτης επέλεξε της λύση της θέσπισης επιμέρους διατάξεων.

7.2.3. Οι προβλεπόμενοι τρόποι τέλεσης

Στις αντικειμενικές υποστάσεις και των τριών επιμέρους άρθρων τυποποιούνται ως τρόποι τέλεσης των εγκλημάτων η παραγωγή, η πώληση, η προμήθεια προς χρήση, η εισαγωγή, η κατοχή, η διανομή και η με κάθε άλλο τρόπο διακίνηση των εκάστοτε «αντικειμένων». Οι τρόποι αυτοί τέλεσης των εγκλημάτων αποτελούν ένα αμάλγαμα, ένα συνδυασμό των προβλεπόμενων από την Σύμβαση και την Οδηγία, καθώς πέραν των κοινών τρόπων τέλεσης που προβλέπονται σε αυτές, στην μεν πρώτη προβλέπεται επιπλέον η παραγωγή και η κατοχή, στη δε δεύτερη προβλέπεται η προμήθεια προς χρήση που δεν προβλέπεται στη Σύμβαση.

Με μια πρώτη ματιά λοιπόν, η επιλογή του Έλληνα νομοθέτη να συμπεριλάβει όλους του τρόπους τέλεσης φαίνεται ότι αποτελούσε μονόδρομο καθώς αυτός δεσμεύεται και από τα δύο διεθνή κείμενα. Ωστόσο, η πραγματικότητα δεν είναι έτσι. Η Οδηγία δεν επιβάλει στα Κράτη Μέλη να ποινικοποιήσουν όλες τις προβλεπόμενες σε αυτές συμπεριφορές καθώς ρητά αναφέρεται στην παρ. 3 του άρθρου 6 ότι τα κράτη υποχρεούνται να ποινικοποιήσουν μόνο την με κάθε τρόπο διάθεση συνθηματικών, κωδικών πρόσβασης σε πληροφοριακά συστήματα ή παρεμφερών στοιχείων. Επομένως ο Έλληνας νομοθέτης είχε την δυνατότητα να μην συμπεριλάβει στους τρόπους τέλεσης του εγκλήματος και τις πράξεις της παραγωγής και της κατοχής, δεδομένου ότι αυτές δεν συμπεριελήφθησαν καν στο σχετικό άρθρο της Οδηγίας. Μάλιστα σκόπιμα δεν συμπεριελήφθησαν οι πράξεις αυτές στο τελικό κείμενο της Οδηγίας εξαιτίας του γεγονότος ότι κρίθηκε ότι η ποινικοποίησή τους θα διεύρυνε

υπερβολικά το αξιόποινο σε μη επιτρεπτό επίπεδο καθώς δεν προκύπτει πως από τις πράξεις αυτές υπάρχει έστω και διακινδύνευση της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους[139], δεδομένου μάλιστα του γεγονότος ότι τα εργαλεία τέλεσης των πράξεων αυτών είναι σχεδόν πάντα διπλής χρήσης δηλαδή δεν εξυπηρετούν αποκλειστικά το σκοπό τέλεσης εγκλημάτων όπως θα αναλυθεί στην συνέχεια. Συνεπώς Έλληνας νομοθέτης δεν δεσμευόταν για την ποινικοποίηση των δύο αυτών προπαρασκευαστικών πράξεων, της παραγωγής και της κατοχής και θα ήταν ορθότερο να απέχει από την ποινικοποίησή τους[140].

Περαιτέρω, αναφορικά με τους λοιπούς τρόπους τέλεσης αξίζει να αναφερθούν ορισμένες διευκρινήσεις που δίνονται από την Αιτιολογική Έκθεση της Σύμβασης. Συγκεκριμένα στην σκέψη 72 αυτής ορίζεται ότι ως «διανομή» νοείται η άμεση ενέργεια προώθησης δεδομένων σε άλλους, ενώ ως «διάθεση» ορίζεται η δημοσίευση στο διαδίκτυο συσκευών για χρήση από άλλους, όρος ο οποίος επίσης αποσκοπεί στο να καλύψει την δημιουργία ή συσσώρευση υπερσυνδέσμων ώστε να διευκολυνθεί η πρόσβαση σε τέτοιες συσκευές ή προγράμματα.

Τέλος, αναφορικά με την πράξη της προμήθειας αξίζει να επισημανθεί ότι αυτή τιμωρείται μόνο σε περιπτώσεις που γίνεται προς χρήση και όχι όταν υπάρχει σκοπός περαιτέρω διάθεσης. Όπως αναφέρθηκε, αυτή η πρόβλεψη δεν υπάρχει στο κείμενο της Σύμβασης αλλά μόνο στην Οδηγία. Αν και η επιλογή αυτή προκαλεί εντύπωση, θα πρέπει να θεωρήσουμε έγινε με γνώμονα ότι η προμήθεια προς χρήση είναι εγγύτερα στην προσβολή των πληροφοριακών συστημάτων ή των δεδομένων τους και άρα ενέχει μεγαλύτερο και πιο απτό κίνδυνο για αυτά από την προμήθεια προς περαιτέρω διάθεση, παρά το γεγονός ότι η δεύτερη σαν πράξη μας παραπέμπει περισσότερο σε έναν κατ' επάγγελμα εγκληματία, η συμπεριφορά του οποίου ενέχει μεγαλύτερη απαξία από αυτή ενός περιστασιακού.

---

[139] βλ. Μ. Καϊάφα – Γκμπάντι, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 489 επ. υπ. 35 όπου *επισημαίνεται «ότι ο ευρωπαίος νομοθέτης οφείλει να προσδιορίζει λεπτομερώς τα προσβαλλόμενα συμφέροντα και τεκμηριώνει την μη επουσιώδη προσβολή τους από τις συμπεριφορές που θέλεις να ποινικοποιήσεις»,* και την εκεί παραπομπή σε ECPI, ΠοινΔικ 2010, σελ. 70

[140] Ωστόσο όπως εκτέθηκε και στο χωρίο της παρούσας όπου αναλύεται το άρθρο 7 της Οδηγίας, συγκεκριμένα η ποινικοποίηση της κατοχής κωδικών ή παρόμοιων στοιχείων πρόσβασης, τους οποίους από τη φύση τους θα πρέπει να γνωρίζει μόνο ο χρήστης του λογαριασμού ή του πληροφοριακού συστήματος, θα μπορούσε να διατηρηθεί υπό την προϋπόθεση ωστόσο της κατοχής τουλάχιστον συγκεκριμένου αριθμού τέτοιων στοιχείων και με δεδομένο πάντοτε το σκοπό τέλεσης του εγκλήματος της παράνομης πρόσβασης.

7.2.4. Οι συσκευές, τα προγράμματα και οι κωδικοί ως αντικείμενα των πράξεων

Στο άρθρο 6 της Σύμβαση ως αντικείμενα των προπαρασκευαστικών πράξεων προβλέπονται χαρακτηριστικά συσκευές, «συμπεριλαμβανομένων» των προγραμμάτων υπολογιστή σχεδιασμένων ή προσαρμοσμένων πρωτίστως για τον σκοπό της πραγματοποίησης εγκλημάτων που στρέφονται κατά της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους, καθώς και συνθηματικοί κωδικοί υπολογιστή, κωδικοί πρόσβασης, η παρόμοια δεδομένα με τα οποία μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε ένα μέρος συστήματος υπολογιστή (όπως τα στοιχεία βιομετρικής ταυτοποίησης λ.χ. το δακτυλικό αποτύπωμα, τα πρόσωπο κ.λπ.). Από την άλλη στο άρθρο 7 της Οδηγίας δεν γίνεται αναφορά σε συσκευές. Πράγματι η πρόβλεψη ως αντικειμένων των προπαρασκευαστικών πράξεων και των συσκευών είναι περιττή δεδομένου ότι τα βασικά εγκλήματα μπορούν να τελεστούν από συσκευές μόνο αν σε αυτές περιέχονται κακόβουλα προγράμματα. Επίσης η συμπερίληψη των προγραμμάτων στην έννοια των συσκευών είναι εντελώς άστοχη. Παρόλα αυτά ο Έλληνας νομοθέτης μη κατανοώντας το περιεχόμενο των όρων και θεωρώντας ότι δεσμεύεται και από τα δύο ως άνω άρθρα συμπεριέλαβε και τις συσκευές ως αντικείμενα των πράξεων, διορθώνοντας τουλάχιστον την διατύπωση, μη συμπεριλαμβάνοντας τα προγράμματα υπολογιστών στην έννοια αυτών (δηλ. των συσκευών) αλλά παραθέτοντάς τα ως ξεχωριστό είδος αντικειμένων του εγκλήματος.

7.2.5. Ο σκοπός τέλεσης των βασικών εγκλημάτων

Ένα σημείο που χρήζει σχολιασμού είναι ότι και στα τρία επιμέρους άρθρα που ποινικοποιούν τις προπαρασκευαστικές πράξεις απαιτείται για την πλήρωση της αντικειμενικής τους υπόστασης να υπάρχει σκοπός τέλεσης του αντίστοιχου βασικού εγκλήματος τους. Σχετική δε πρόβλεψη υπάρχει και στο άρθρο 6 της Σύμβασης και στο άρθρο 7 της Οδηγίας. Αναφορικά με την πρώτη προβλεπόμενη στα άρθρα αυτά περίπτωση, ήτοι όταν οι τυποποιούμενες πράξεις αφορούν συσκευές ή προγράμματα, δεν υπάρχει κάποιο πρόβλημα καθώς ο σκοπός του δράστη για την τέλεση των συγκεκριμένων κάθε φορά εγκλημάτων θα προκύπτει από την ίδια την φύση των προγραμμάτων τα οποία θα επιτελούν ένα συγκεκριμένο σκοπό. Μάλιστα ορθά θα μπορούσε να υποστηριχθεί ότι η απαίτηση του σκοπού τέλεσης των σχετικών βασικών εγκλημάτων είναι περιττή καθώς καλύπτεται από το γεγονός ότι τα αντικείμενα της πράξης είναι σχεδιασμένα ή προσαρμοσμένα κυρίως για την τέλεση των πράξεων αυτών.

Το ίδιο ισχύει εν μέρει, για άλλο λόγο ωστόσο, στην δεύτερη προβλεπόμενη στα άρθρα αυτά περίπτωση, η οποία είναι όταν οι προβλεπόμενες πράξεις αφορούν συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατό να

αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος ενός πληροφοριακού συστήματος. Στην περίπτωση αυτή, ο σκοπός του δράστη δεν προκύπτει αντικειμενικά από πουθενά και συνεπώς είναι ζήτημα απόδειξης αν υπάρχει και πιο συγκεκριμένο έγκλημα αφορά και άρα σε πια από τις τρείς διατάξεις θα υπαχθεί. Σε κάθε περίπτωση ο σκοπός του δράστη μιας τέτοιας προπαρασκευαστικής πράξης που αφορά κωδικούς και παρεμφερή στοιχεία πρόσβασης θα έχει σίγουρα ως σκοπό (τουλάχιστον) την τέλεση του εγκλήματος της παράνομης πρόσβασης. Δεδομένου μάλιστα ότι δεν χρειάζεται κάτι παραπάνω για την τέλεση του προπαρασκευαστικού εγκλήματος (δηλαδή αρκεί ο σκοπός της τέλεσης αυτού του εγκλήματος) και ότι και οι τρεις διατάξεις έχουν το ίδιο πλαίσιο ποινής, η πρόβλεψη της εν λόγω περίπτωσης και στα τρία επιμέρους άρθρα είναι περιττή.

Με βάση όλα τα ανωτέρω θα ήταν ορθότερο να μην απαιτούσε ο νομοθέτης ως στοιχείο της ειδικής υπόστασης τον σκοπό τέλεσης του αντίστοιχου κάθε διατάξεως βασικού εγκλήματος. Επίσης κατά τα ανωτέρω θα έπρεπε η δεύτερη περίπτωση των τριών αυτών άρθρων που αφορά κωδικούς πρόσβασης και αντίστοιχα στοιχεία να συμπεριληφθεί μόνο στο άρθρο 370Ε Π.Κ. (το οποίο έχει ως βασικό έγκλημα μεταξύ άλλων και αυτό της παράνομης πρόσβασης) και να προστεθεί στη διατύπωσή της ο σκοπός τέλεσης του εγκλήματος της παράνομης πρόσβασης.

7.2.6. «Χωρίς δικαίωμα» τέλεση

Όπως έχει εκτεθεί, στην Αιτιολογική Έκθεση της Σύμβασης ορίζεται ότι οι προβλεπόμενες από αυτή συμπεριφορές πρέπει να λογίζονται ότι τιμωρούνται μόνο όταν τελούνται «χωρίς δικαίωμα». Σχετικά στην σκέψη 77 της Αιτιολογικής Έκθεσης της Σύμβασης ορίζεται ότι εντός του περιεχομένου της έννοιας του όρου «χωρίς δικαίωμα» καλύπτεται και το σκεπτικό της παρ. 2 του άρθρου 6 της Σύμβασης, σύμφωνα με το οποίο, το άρθρο αυτό δεν θα πρέπει να ερμηνεύεται με τρόπο που να αναγνωρίζει ποινική ευθύνη όταν οι περιγραφόμενες πράξεις δεν αποσκοπούν στην διάπραξη των βασικών εγκλημάτων όπως «*για την εγκεκριμένη διενέργεια ελέγχων ή προστασία ενός συστήματος υπολογιστή*».[141]

Η προϋπόθεση αυτή, η πράξη να έχει τελεστεί «χωρίς δικαίωμα», υιοθετήθηκε και από την Οδηγία η οποία περιέλαβε ειδική πρόβλεψη σε κάθε άρθρο της με το οποίο επιβάλλεται η ποινικοποίηση μιας συμπεριφοράς, συμπεριλαμβανομένου και του άρθρου 7 που ποινικοποιεί τις προπαρασκευαστικές των λοιπών εγκλημάτων πράξεις. Περαιτέρω,

[141] Η εξαίρεση αυτή δεν προβλέπεται ρητά στα σχετικά επιμέρους άρθρα του ποινικού κώδικα, πλην όμως θα πρέπει να θεωρηθεί ότι προκύπτει εξ' αντιδιαστολής από τον απαιτούμενο σε αυτά σκοπό διάπραξης των βασικών εγκλημάτων.

σύμφωνα με τον ορισμό που δίνεται στο άρθρο 2 της Οδηγίας, «χωρίς δικαίωμα» σημαίνει ότι η αναφερομένη συμπεριφορά, είναι μη εξουσιοδοτημένη από τον ιδιοκτήτη ή από άλλο νόμιμο δικαιούχο του συστήματος ή μέρους του ή μη επιτρεπόμενη δυνάμει του εθνικού δίκαιου.

Αυτός ο ορισμός όμως δεν ανταποκρίνεται στο περιεχόμενο του άρθρου 7[142] της Οδηγίας και συνακόλουθα των επιμέρους άρθρων του Π.Κ. με τα οποία ποινικοποιούνται οι προπαρασκευαστικές πράξεις των βασικών εγκλημάτων στα οποία διατηρήθηκε η σχετική πρόβλεψη ως ειδικό στοιχείο του αδίκου. Ο λόγος είναι ότι οι συμπεριφορές αυτές είναι τόσο απομακρυσμένες από την βλάβη ενός συγκεκριμένου εννόμου αγαθού που είναι δύσκολο αν όχι ακατόρθωτο να ανατρέξουμε στην τυχόν βούληση του νόμιμου δικαιούχου του πληροφοριακού συστήματος ή των δεδομένων επί των οποίων θα τελεστούν οι συμπεριφορές των βασικών εγκλημάτων. Το «χωρίς δικαίωμα» επομένως στην περίπτωση των προπαρασκευαστικών πράξεων δεν μπορεί να αφορά το βασικό τους έγκλημα αλλά θα πρέπει να αφορά την ίδια την προπαρασκευαστική πράξη που κάθε φορά τελείται.

Με δεδομένη μάλλον αυτή την παραδοχή προτάθηκε από την Θεωρία[143] «*για να αποφευχθεί ο κίνδυνος ενός άμετρου αξιοποίνου για πράξεις ακόμα και απλής κατοχής συσκευών που δεν είναι εκ κατασκευής αποκλειστικά προσαρμοσμένες για προσβολές κατά συστημάτων πληροφοριών θα μπορούσε να εισαγάγει ο νομοθέτης ως αναγκαία προϋπόθεση της παραγωγής, πώλησης, διάθεσης, αλλά ακόμα και της προμήθειας για χρήση ή κατοχής προγραμμάτων υπολογιστών κατά κύριο λόγω σχεδιασμένων για επιθέσεις κατά συστημάτων πληροφοριών και κωδικών που αναφέρονται στην Οδηγία, την χορήγησης σχετικής άδειας*». Ωστόσο ο Έλληνας νομοθέτης δεν προέβη στην θέσπιση καμίας τέτοιας άδειας.

Μια τέτοια πρόβλεψη για την άμβλυνση του αξιοποίνου νομικά θα κρινόταν εξαιρετικά αποτελεσματική καθώς με αυτό τον τρόπο, όπως παρατηρείται, η δόμηση του αξιοποίνου γίνεται στη βάση της έλλειψης του στοιχείου της σχετικής άδειας. Με άλλα λόγια το αξιόποινο για όποιον κατέχει άδεια θα ξεκινούσε από το στάδιο της απόπειρας των βασικών εγκλημάτων.

Ωστόσο, η απαίτηση κατοχής σχετικής άδειας για την τέλεση συμπεριφορών που ποινικοποιούνται ως προπαρασκευαστικές αυτών που στρέφονται κατά πληροφορικών συστημάτων και των δεδομένων τους δεν θα πρέπει να κριθεί και ως δικαιοπολιτικά ορθή. Συγκεκριμένα οι συμπεριφορές αυτές αφορούν προγράμματα διπλής χρήσης, δηλαδή που δεν

[142] Αντίθετα, όπως εκτέθηκε, στην πεποίθηση των συντακτών της Σύμβασης

[143] βλ. Μ. Καϊάφα – Γκμπάντι, ο.π. σελ. 489 επ.

μπορούν να χρησιμοποιηθούν μόνο για την τέλεση εγκλημάτων, αλλά, μάλιστα, αντιθέτως, και για την αποφυγή της τέλεσης εγκλημάτων και την προστασία των πληροφοριακών συστημάτων μέσω του ελέγχου και της βελτίωσης των λειτουργιών ασφαλείας τους. Καθιστώντας απαραίτητη την κατοχή άδειας ουσιαστικά περιορίζεται ο αριθμός των ατόμων που δεν ανήκουν στο προσωπικό κάποιας εταιρίας αλλά ανακαλύπτουν ευπάθειες του λογισμικού τους επ' αμοιβή[144], καθώς η συμπεριφορά τους αυτή θα είναι άδικη και μόνο από την κατοχή των σχετικών προγραμμάτων[145]. Επίσης πρόβλημα δημιουργείται με το ποιες θα είναι οι προϋποθέσεις για να αποκτήσει κάποιος άδεια ακόμα και για την κατοχή και πως θα αποδεικνύεται ότι κάποιος που έχει άδεια δεν θα τελεί και παράνομες πράξεις εκμεταλλευόμενος την άδεια. Επομένως μια τέτοια πρόβλεψη περισσότερο σύγχυση και προβλήματα θα δημιουργήσει παρά ασφάλεια δικαίου.

7.2.7. Περιπτώσεις μικρής σημασίας

Στη παρ. 1 του άρθρου 6 της Σύμβασης δίνεται η δυνατότητα στα Συμβαλλόμενα Μέρη να εξαρτήσουν το αξιόποινο των προβλεπόμενων συμπεριφορών από την προϋπόθεση της κατοχής ενός τουλάχιστον συγκεκριμένου αριθμού συσκευών ή προγραμμάτων. Αντίστοιχη πρόβλεψη δεν υπάρχει στην Οδηγία, πλην όμως σε αυτή προβλέπεται η δυνατότητα τα κράτη

---

[144] Πράγματι κάθε άλλο παρά σπάνιο είναι το φαινόμενο εταιρίες που δραστηριοποιούνται στον κυβερνοχώρο να προκηρύσσουν εξαιρετικά μεγάλα «οικονομικά έπαθλα» σε hackers που εντοπίζουν και δηλώνου κενά ασφαλείας στα συστήματα τους. Πρόκειται επομένως για μια συχνή οικονομική – επαγγελματική δραστηριότητα ατόμων τα οποία δεν εργάζονται ως υπάλληλοι μια εταιρίας αλλά βιοπορίζονται από αυτό, ωφελώντας παράλληλα τόσο την συγκεκριμένη εταιρία όσο και την κοινωνία η οποία μέσω της πολιτείας έχει κρίνει την ασφάλεια των συστημάτων πληροφοριών ως έννομο αγαθό το οποίο χρήζει μάλιστα ποινικής προστασίας. Με την άκριτη ποινικοποίηση δηλαδή συμπεριφορών αυτοαναιρείται ο ίδιος ο σκοπός που θέλει να επιτύχει η πολιτεία με την ποινικοποίηση των συμπεριφορών αυτών. Η πρακτική αυτή μάλιστα είναι αναγκαίο όχι μόνο να διατηρηθεί αλλά και να προωθηθεί για να γίνει πιο ευρεία στο μέλλον καθώς ο αριθμός των blackhat hackers (ή αλλιώς crackers) υπερέχει συντριπτικά του προσωπικού των εταιριών λογισμικού που ασχολείται με την ασφάλεια των συστημάτων.

[145] Για το λόγο αυτό προτείνεται ότι όλες οι πράξεις του άρθρου 7 της Οδηγίας θα πρέπει να δικαιολογούνται (δηλ. ακόμα και χωρίς άδεια) όταν τελούνται για να δοκιμαστεί ή α προστατευθεί ένα πληροφοριακό σύστημα στο πλαίσιο μια προσωπικής ή επαγγελματικής χρήσης δεδομένου ότι αυτό δεν είναι αντίθετο με το περιεχόμενο του άρθρου 7 της Οδηγίας, γιατί το αδίκημα απαιτεί τέλεση πράξεων με σκοπό τη διάπραξη των εγκλημάτων που αυτή προβλέπει, ενώ εδώ ο σκοπός αυτός όχι μόνο δεν υπάρχει αλλά συντρέχουν επιπρόσθετα αντίθετα δεδομένα που αποβλέπουν στην διαφύλαξη του εννόμου αγαθού, βλ. βλ. Μ. Καϊάφα – Γκμπάντι, ο.π. σελ. 489 επ.. Ωστόσο μια τέτοια εξαίρεση στον κανόνα θέτει εν αμφιβόλω την ίδια την αποτελεσματικότητα και την αναγκαιότητα του κανόνα.

μέλη να μην ποινικοποιούν γενικά περιπτώσεις ήσσονος σημασίας, μια πρόβλεψη η οποία όπως έχει εκτεθεί υπάρχει σε όλα τα εγκλήματα που προβλέπονται από την Οδηγία.

Η τελευταία αυτή δυνατότητα που παρέχεται από την Οδηγία είναι εξαιρετικά αόριστη και ορθώς δεν ενσωματώθηκε αυτούσια στα σχετικά άρθρα του Π.Κ.. Πλην όμως, ο Έλληνας νομοθέτης έχει τη δυνατότητα να εξειδικεύσει την έννοια αυτή προσδιορίζοντας συγκεκριμένες περιπτώσεις οι οποίες μπορούν να θεωρηθούν ως ήσσονος σημασίας. Μια τέτοια περίπτωση είναι και αυτή της κατοχής μη επαρκούς αριθμού προγραμμάτων υπολογιστών ή κωδικών ή κατ' ορθότερη διατύπωση γενικά η τέλεση των προβλεπόμενων συμπεριφορών επί μη επαρκούς αριθμού αντικειμένων. Η σημασία μια τέτοιας πρόβλεψης θα ήταν ότι συμπεριφορές οι οποίες δεν αφορούν ένα αξιόλογο αριθμό αντικειμένων δεν θα ήταν καν καταρχήν άδικες. Ο περιορισμός αυτός του αξιοποίνου είναι σύμφωνος με το γεγονός ότι λόγω του πολύ προγενέστερου σταδίου σε σχέση με την βλάβη των προστατευόμενων εννόμων αγαθών, η τέλεση των εγκλημάτων αυτών εναπόκειται σε μεγάλο βαθμό στην απόδειξη συνδρομής των απαιτούμενων υποκειμενικών στοιχειών, κάτι το οποίο κάθε άλλο παρά εύκολο είναι, με αποτέλεσμα να κινούνται ποινικές διαδικασίες κατά των «δραστών» για πράξεις για τις οποίες σπάνια θα καταδικάζονται.

Ωστόσο, ο Έλληνας νομοθέτης αδιαφορώντας για τις ως άνω δυνατότητες του και τις δεδομένες αποδεικτικές δυσχέρειες που δύνανται συχνά να οδηγούν σε ατελέσφορες ποινικές διώξεις, δεν θέσπισε καμία περίπτωση περιορισμού του αξιόποινου χαρακτήρα των προπαρασκευαστικών πράξεων.

7.2.8. Προγράμματα σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των βασικών εγκλημάτων - Η φύση των προγραμμάτων ως «διπλής χρήσης»

Όπως αναφέρθηκε, εκτός από τους κωδικούς και τα παρόμοια στοιχεία με τα οποία μπορεί να αποκτηθεί πρόσβαση σε ένα πληροφοριακό σύστημα, αντικείμενο των προπαρασκευαστικών πράξεων μπορεί να αποτελέσουν και προγράμματα υπολογιστών. Στην σκέψη 72 της Αιτιολογικής Έκθεσης της Σύμβασης που αφορά τις συγκεκριμένες προπαρασκευαστικές πράξεις επισημαίνεται σχετικά με τον όρο πρόγραμμα υπολογιστή, ότι αυτός αφορά εν προκειμένω προγράμματα που είναι για παράδειγμα σχεδιασμένα να αλλάξουν ή ακόμη και να καταστρέψουν δεδομένα ή να παρεμβληθούν στην λειτουργία των συστημάτων, όπως προγράμματα ιών, ή προγράμματα σχεδιασμένα ή προσαρμοσμένα να αποκτήσουν πρόσβαση σε συστήματα υπολογιστών.

Ωστόσο ο τρόπος με τον οποίο τα προγράμματα αυτά θα χρησιμοποιηθούν δεν εξαρτάται από τη φύση τους αλλά από τη βούληση του χρήστη του. Έτσι έχει επικρατήσει για τα προγράμματα με τα οποία μπορούν να τελεστούν εγκλήματα που στρέφονται κατά της

ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους ο όρος ότι πρόκειται για προγράμματα διπλής χρήσης (dual use) καθώς αυτά δύνανται να εξυπηρετούν και τον ακριβώς αντίθετο σκοπό του ελέγχου και της βελτίωσης της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους.

Σύμφωνα με την σκέψη 73 της Αιτιολογικής Έκθεσης της *Σύμβασης «[έ]να σημαντικό ζήτημα που απασχόλησε τη συντακτική επιτροπή της Σύμβασης ήταν το κατά πόσο η συσκευή (ή το πρόγραμμα υπολογιστή) θα πρέπει να είναι σχεδιασμένη αποκλειστικά ή συγκεκριμένα για την διάπραξη εγκλημάτων, ως εκ τούτου αποκλείοντας από το πεδίο εφαρμογής του νόμου συσκευές διπλής χρήσης (dual use) […] [η] άποψη αυτή κρίθηκε ως εξαιρετικά στενή και η υιοθέτηση της θα μπορούσε να έχει ως συνέπεια ανυπέρβλητα αποδεικτικά εμπόδια τα οποία ουσιαστικά θα καθιστούσαν την διάταξη αδρανή και μη εφαρμόσιμη πλην ελαχίστων περιπτώσεων […] [η] αντίθετη άποψη κατά την οποία η διάταξη θα έπρεπε να καταλαμβάνει συμπεριφορές που αφορούν όλες τις συσκευές ακόμα και αν παράγονται ή διανέμονται νόμιμά απορρίφθηκε εξίσου, λόγω του υπερβολικού εύρους της […] [σ]την τελευταία αυτή περίπτωση μόνο το υποκειμενικό στοιχείο του δόλου της τέλεσης εγκλήματος με υπολογιστή θα ήταν καθοριστικό για την επιβολή ποινής, κάτι το οποίο δεν υιοθετήθηκε ούτε αναφορικά με την παραχάραξη νομισμάτων […] [ω]ς εκ τούτων ως μέση λύση προκρίθηκε οι συσκευές να είναι αντικειμενικά σχεδιασμένες ή προσαρμοσμένες πρωτίστως με σκοπό την τέλεση εγκλημάτων, ρύθμιση η οποία συνήθως δεν θα καταλαμβάνει περιπτώσεις συσκευών διπλής χρήσης»*.

Αρχικά θα πρέπει να επισημάνουμε είναι ότι η βούληση της Συντακτικής Επιτροπής της Σύμβασης είναι να μην εξαιρούνται κατ' αρχήν από το πεδίο εφαρμογής τα προγράμματα διπλής χρήσης. Την ίδια ακριβώς διατύπωση υιοθετούν και οι επιμέρους διατάξεις του Π.Κ. με τις οποίες ποινικοποιούνται οι προπαρασκευαστικές των εγκλημάτων που στρέφονται κατά πληροφοριακών συστημάτων και των δεδομένων τους πράξεις, όπου προβλέπεται ότι τα προγράμματα πρέπει να είναι σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των βασικών αυτών εγκλημάτων. Πράγματι αν εξαιρούνταν από το πεδίο εφαρμογής του νόμου τα προγράμματα διπλής χρήσης τότε ο νόμος δεν θα απαγόρευε τις προπαρασκευαστικές πράξεις επί κανενός προγράμματος καθώς ΟΛΑ τα προγράμματα που πλήττουν άμεσα την ασφάλεια των πληροφοριακών συστημάτων είναι διπλής χρήσης δεδομένου ότι μπορούν να χρησιμοποιηθούν για την τέλεση εγκληματικών πράξεων είτε σε κάθε περίπτωση για την προστασία από αυτές είτε για νόμιμες πράξεις που δεν έχουν καμία απολύτως σχέση με την ασφάλεια των συστημάτων και των δεδομένων τους (στις οποίες

μάλιστα συμπεριλαμβάνεται και η δημιουργία botnet[146]). Στην πράξη όμως τα προγράμματα αυτά εξαιρούνται από την εφαρμογή του νόμου καθώς ο μόνος τρόπος διάγνωσης του σκοπού για την επιτέλεση του οποίου είναι προσαρμοσμένα είναι με αναγωγή στην βούληση του δράστη, η οποία στο στάδιο των προπαρασκευαστικών ενεργειών είναι από εξαιρετικά δύσκολο έως ακατόρθωτο να διαπιστωθεί μέσω της αποδεικτικής διαδικασίας με αποτέλεσμα οι συμπεριφορές αυτές να μένουν ατιμώρητες, καθώς μάλιστα καθένας θα μπορούσε να ισχυριστεί ότι δημιουργεί, κατέχει ή προμηθεύεται τα προγράμματα αυτά επειδή δραστηριοποιείται ως ανεξάρτητος ελεγκτής της ασφάλειας πληροφοριακών συστημάτων, ή ότι διαθέτει τα προγράμματα αυτά στην αγορά για αυτό το σκοπό δεδομένου ότι δεν απαιτείται κάποια ειδική άδεια από τον αγοραστή ή των πωλητή (και δεν θα μπορούσε ούτε θα έπρεπε να απαιτείται, για τους λόγους που εκτέθηκαν ανωτέρω στο σχετικό χωρίο της παρούσας).

Τα μόνα προγράμματα που δεν είναι διπλής χρήσης είναι τα προγράμματα που αποσκοπούν έμμεσα στην τέλεση των βασικών εγκλημάτων με την εξαπάτηση του θύματος (συνήθως Δούρειοι Ίπποι, ή προγράμματα δημιουργίας phishing ή pharming) με σκοπό ο

---

[146] Δημιουργία botnet (δικτύων προγραμμάτων ρομπότ), όπως αναφέρεται στην σκέψη 27 του προοιμίου της Οδηγίας, είναι η πράξη της απόκτησης εξ αποστάσεως ελέγχου σε σημαντικό αριθμό υπολογιστών διά της μολύνσεως τους με κακόβουλο λογισμικό μέσω στοχευμένων επιθέσεων στον κυβερνοχώρο. Μόλις δημιουργηθεί, το προσβεβλημένο δίκτυο υπολογιστών, που συνιστά το «botnet», μπορεί να ενεργοποιείται εν αγνοία των χρηστών των εν λόγω υπολογιστών, με σκοπό την εξαπόλυση επιθέσεων στον κυβερνοχώρο μεγάλης κλίμακας, η οποία συνήθως μπορεί να προκαλέσει σοβαρές ζημίες. Σε σχέση με το ζήτημα της «διπλής χρήσης» αναφέρεται σχετικά στην ίδια σκέψη του Προοιμίου της Οδηγίας ότι *«[λ]αμβανομένων υπόψη των διαφορετικών τροπών με τους οποίους μπορούν να πραγματοποιηθούν οι επιθέσεις και της ταχείας εξέλιξης του υλισμικού και του λογισμικού, η παρούσα οδηγία αναφέρεται σε εργαλεία που μπορούν να χρησιμοποιηθούν για τη διάπραξη των αδικημάτων που απαριθμούνται στην παρούσα οδηγία […] [τ]έτοια εργαλεία μπορούν να περιλαμβάνουν το κακόβουλο λογισμικό —συμπεριλαμβανομένων των εργαλείων που μπορούν να δημιουργούν «botnet»[146]— το οποίο χρησιμοποιείται για τη διάπραξη επιθέσεων στον κυβερνοχώρο […] [α]κόμη και όταν ένα τέτοιο εργαλείο είναι κατάλληλο ή ιδιαιτέρως κατάλληλο για τη διάπραξη ενός εκ των αδικημάτων που ορίζονται στην παρούσα οδηγία, είναι πιθανό το εργαλείο να έχει παραχθεί για νόμιμο σκοπό […] [μ]ε αιτιολογία την ανάγκη να αποφευχθεί η ποινικοποίηση οσάκις τα εν λόγω εργαλεία παράγονται και διατίθενται στην αγορά για νόμιμους σκοπούς, όπως για τον έλεγχο της αξιοπιστίας των προϊόντων της τεχνολογίας πληροφοριών ή της ασφάλειας των συστημάτων πληροφοριών, εκτός από τη γενική απαίτηση της πρόθεσης, μια απαίτηση άμεσης πρόθεσης να χρησιμοποιήσει τα εργαλεία αυτά για να διαπράξει ένα ή περισσότερα εκ των αδικημάτων που ορίζονται στην παρούσα Οδηγία, πρέπει επίσης να πληρούται.»*

τελευταίος να δώσει τα στοιχεία πρόσβασης ή να εγκαταστήσει κακόβουλα προγράμματα. Τα προγράμματα αυτά αν και δεν πλήττουν άμεσα την ασφάλεια των πληροφοριακών συστημάτων αφού μεσολαβεί απαραιτήτως ενέργεια του θύματος και άρα με αυτά δεν τελούνται τα προβλεπόμενα από τα επιμέρους άρθρα που ποινικοποιούν τις προπαρασκευαστικές πράξεις βασικά εγκλήματα, εξυπηρετούν το σκοπό τέλεσης των εγκλημάτων αυτών και άρα εμπίπτουν στο εφαρμοστικό τους πεδίο με βάση τη γραμματική ερμηνεία. Συνεπώς τα προγράμματα αυτά είναι τα μόνα τα προγράμματα τα οποία μπορεί να θεωρηθεί ότι μπορούν να αποτελέσουν αντικείμενο των επιμέρους άρθρων που ποινικοποιούν τις προπαρασκευαστικές των εγκλημάτων που στέφονται κατά της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους πράξεων καθώς είναι τα μόνα τα οποία μπορούν να χαρακτηρισθούν ότι είναι σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των βασικών εγκληματών. Ωστόσο οι περιπτώσεις αυτές που δεν κινδυνεύει άμεσα η ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων τους, δύνανται να εγείρουν ακόμα εντονότερες ενστάσεις αναφορικά με την υπερβολική διεύρυνση του αξιοποίνου ακριβώς για τον λόγο ότι δύσκολα αποδεικνύεται ότι το έννομο αγαθό της ασφάλειας των πληροφοριακών συστημάτων και δεδομένων τους τίθεται υπό οποιοδήποτε κίνδυνο ώστε να είναι απαραίτητη η ποινικοποίηση των υπό κρίση συμπεριφορών ως έσχατη λύση, κατά τη βασική αρχή του ποινικού δικαίου, για την προστασία του.

7.2.9. Πλαίσιο ποινής

Στο άρθρο 9 της Οδηγίας ορίζεται ότι οι το ανώτατο όριο του πλαισίου ποινής όλων των προβλεπόμενων σε αυτή εγκλημάτων πρέπει να είναι τουλάχιστον 2 έτη. Στα εγκλήματα αυτά συμπεριλαμβάνονται και οι προπαρασκευαστικές πράξεις των εγκλημάτων που στρέφονται κατά πληροφοριακών συστημάτων και των δεδομένων τους. Επομένως ο Έλληνας νομοθέτης δεν είχε άλλη επιλογή από το να θέσει ως ανώτατο όριο της επαπειλούμενης με τα επιμέρους άρθρα που ποινικοποιούν τις προπαρασκευαστικές πράξεις τα δύο έτη φυλάκισης. Δεδομένου μάλιστα ότι οι ποινές που προβλέπονται από τα βασικά εγκλήματα είναι αυστηρότερες δεν φαίνεται να υπάρχει κάποιο εμφανές πρόβλημα στο βαθμό που δεν τιμωρείται κάποιος αυστηρότερα για την τέλεση της προπαρασκευαστικής πράξης σε σχέση με την ποινή που θα μπορούσε να του επιβληθεί για απόπειρα της τελευταίας, ένα ζήτημα ωστόσο που λόγω της γενικότητας των περιπτώσεων που καλύπτουν οι διατάξεις και της μη δυνατότητας θέσπισης κατώτερου ανώτερου ορίου, μόνο στο στάδιο της δικαστικής επιμέτρησης της ποινής μπορεί να λυθεί. Ωστόσο, σε κάθε περίπτωση, το γεγονός ότι επιβάλλεται από την Οδηγία κοινό κατώτερο ανώτερο όριο πλαισίου ποινής τόσο για τα βασικά εγκλήματα όσο και για τις προπαρασκευαστικές τους πράξεις περιορίζει την

ευελιξία του εθνικού νομοθέτη. Για το λόγο αυτό θα ήταν ορθότερο το πλαίσιο ποινής των προπαρασκευαστικών πράξεων να υπολογιζόταν με βάση το πλαίσιο ποινής των βασικών εγκλημάτων όπως συμβαίνει στην απόπειρα.

7.3. Συρροή με τα βασικά εγκλήματα

Δεδομένου ότι όπως προκύπτει από την ίδια την διατύπωση των υπό κρίση άρθρα αυτά προβλέπουν την ποινικοποίηση προπαρασκευαστικών πράξεων των βασικών εγκλημάτων στα οποία παραπέμπουν όταν οι πράξεις αυτές συρρέουν με τα τελευταία θα πρέπει να γίνει δεκτό ότι υπάρχει φαινομενική πραγματική συρροή και θα πρέπει ο δράστης να τιμωρηθεί μόνο για το βασικό έγκλημα ή την απόπειρα του καθώς η προπαρασκευαστική πράξη, η απαξία της οποία περιλαμβάνεται σε αυτά, θα απορροφηθεί ως πρότερη συντιμωρητή.

Περαιτέρω το ίδιο θα πρέπει να ισχύσει και σε περιπτώσεις στις οποίες ο δράστης δεν είναι και ο αυτουργός του βασικού εγκλήματος ή της απόπειράς του αλλά συμμέτοχος.

7.4. Συμπέρασμα

Όπως εκτέθηκε, ο όρος «χωρίς δικαίωμα» είναι κενός, καθώς πάρα το γεγονός ότι η εξειδίκευση του όρου αφέθηκε στους εθνικούς νομοθέτες των Κρατών Μελών στην Ελλάδα δεν υπάρχει ρυθμιστικό πλαίσιο που να ορίζει πότε κάποιος δεν έχει δικαίωμα στην τέλεση πράξεων οι οποίες είναι καθόλα νόμιμες και δυνητικά μπορούν να χρησιμοποιηθούν για την τέλεση εγκλημάτων που στρέφονται κατά συστημάτων πληροφοριών και των δεδομένων τους. Αυτό έχει ως συνέπεια το ίδιο το άρθρο να καθίσταται μη εφαρμόσιμο. Ωστόσο ένα ρυθμιστικό πλαίσιο σε κάθε περίπτωση θα πρέπει να μην περιορίζει την δράση όσων προβαίνουν ανεξάρτητα στον έλεγχο της προστασίας των συστημάτων πληροφοριών καθώς κάτι τέτοιο θα έχει το αντίθετο από το επιδιωκόμενο με τις σχετικές διατάξεις αποτέλεσμα ήτοι αντί να προστατεύεται το έννομο αγαθό της ασφάλειας των πληροφοριακών συστημάτων αυτό θα τίθεται σε πιο επισφαλή θέση. Οπότε γεννάται το ερώτημα αν θα πρέπει εν γένει να υπάρχει ρυθμιστικό πλαίσιο για την χορήγηση άδειας.

Για τους ανωτέρω λόγους κατά το γράφοντα, το άρθρο θα πρέπει να μείνει όπως έχει, ώστε φαινομενικά τουλάχιστον η Ελλάδα να είναι συμμορφωμένη με τις απαιτήσεις που έχει αναλάβει από την Σύμβαση και την Οδηγία, στην πράξη όμως να πρόκειται για ένα άρθρο το οποίο σε καμία περίπτωση δεν θα εφαρμόζεται όταν οι προπαρασκευαστικές πράξεις αφορούν προγράμματα διπλής χρήσης, αλλά και ούτε στις περιορισμένες περιπτώσεις που τα προγράμματα επιτελούν αποκλειστικά μεν το σκοπό της τέλεσης εγκλημάτων που στρέφονται κατά της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων τους, αλλά μόνο έμμεσα δε, διότι κάτι τέτοιο θα οδηγούσε σε υπερβολική και απαράδεκτη διεύρυνση του αξιοποίνου.

Τέλος, σχετικά, αξίζει να επισημανθεί ότι εντός του μήνα (Δεκέμβριος 2017) η Ολομέλεια του Ευρωπαϊκού Κοινοβουλίου θα συζητήσει την επιβολή ελέγχου στις εξαγωγές προγραμμάτων διπλής χρήσης από εταιρίες των Κρατών Μελών όπως συμβαίνει σε άλλες τεχνολογίες και υλικά που είναι δυνατό να προκαλέσουν μαζική καταστροφή αλλά χρησιμοποιούνται και για εμπορικούς λόγους (λ.χ. το ουράνιο). Σκοπός του ελέγχου αυτού είναι ο σεβασμός των ανθρωπίνων δικαιωμάτων από τις ευρωπαϊκές εταιρίας του και η μη συνεργασία τους με απολυταρχικά καθεστώτα λ.χ. για την παρακολούθηση των πολιτών τους. Πρακτικά ένας τέτοιος περιορισμός θα σήμαινε ότι οι ευρωπαϊκές εταιρίες απαγορεύεται να συμβάλλονται με μη εγκεκριμένα από την Ε.Ε. κράτη για την πώληση προγραμμάτων διπλής χρήσης.[147]

147 http://www.europarl.europa.eu/news/en/press-room/20161020IPR47885/eu-rules-needed-to-ensure-firms-respect-human-rights-abroad-say-meps
http://www.europarl.europa.eu/news/en/press-room/20171123IPR88705/preventing-authoritarian-regimes-from-spying-on-their-own-citizens

8. Αντί επιλόγου

Το φαινόμενο της κυβερνοεγκληματικότητας κάθε άλλο παρά στο τέλος του βρίσκεται Συνεπώς θα ήταν άστοχο η παρούσα εργασία να είχε έναν επίλογο. Αντί επιλόγου, λοιπόν, κρίνεται σκόπιμο να γίνει ένα συνοπτικό σχόλιο για τις μελλοντικές διατάξεις που θα πρέπει να θεσπισθούν για να συνοδεύσουν της εκτεθείσες στην παρούσα εργασία ώστε να υπάρχει μια πλήρης αντιμετώπιση του φαινομένου αυτού.

Ένα σημαντικό ζήτημα που δεν θίγεται ούτε από τη Σύμβαση, ούτε από την Οδηγία, ούτε ακόμα και από τον Ν. 44411/2016 είναι η ευθύνη των παρόχων ψηφιακών υπηρεσιών. Οι χρήστες των προγραμμάτων ψηφιακών υπηρεσιών εισάγουν σε αυτά στοιχεία ταυτοποίησης αλλά και άλλα προσωπικά δεδομένα τα οποία αποθηκεύονται σε βάσεις δεδομένων τις οποίες διατηρούν οι πάροχοι των ψηφιακών αυτών υπηρεσιών. Τα προγράμματα αυτά μπορεί να αφορούν από υπηρεσίες κοινωνικής δικτύωσης μέχρι τραπεζικές ή δημόσιες υπηρεσίες. Η διατήρηση λοιπόν της ασφάλειας τους είναι απαραίτητη για την ομαλή λειτουργία της κοινωνίας όπως αυτή έχει διαμορφωθεί και συνεχίζει να διαμορφώνεται με την επίδραση της τεχνολογίας.

Η ασφάλεια των πληροφοριακών συστημάτων των βάσεων δεδομένων των ψηφιακών υπηρεσιών αφορά τόσο την ομαλή λειτουργία τους όσο και τα δεδομένα τους. Η ασφάλεια των δεδομένων έχει δύο πτυχές, μια εσωτερική και μια εξωτερική. Η πρώτη αφορά το γεγονός ότι οι υπηρεσίες αυτές δεν πρέπει να συλλέγουν και να επεξεργάζονται προσωπικά δεδομένα των χρηστών τους χωρίς την συναίνεσή τους, καθώς έτσι εκτός του ότι οι χρήστες είναι σαν να έχουν εγκαταστήσει εν αγνοία τους κακόβουλο λογισμικό κατασκοπείας (spyware) εκτίθενται επίσης σε μεγαλύτερο κίνδυνο σε περίπτωση που κάποιος τρίτος αποκτήσει πρόσβαση στα δεδομένα αυτά ακόμα και από σφάλμα του ίδιου του χρήστη. Η δεύτερη πτυχή της ασφάλειας των βάσεων δεδομένων ψηφιακών υπηρεσιών αφορά τα μέτρα προστασίας που έχουν ληφθεί από τους παρόχους των υπηρεσιών αυτών για την αποτροπή τρίτων στο να αποκτήσουν πρόσβαση στα δεδομένα, είτε μέσω της εφαρμογής μεθόδων «κοινωνικής μηχανικής» στους υπαλλήλους του παρόχου είτε μέσω «hacking».

Τα ζητήματα αυτά, μεταξύ άλλων, πραγματεύονται ο Γενικός Κανονισμός 2016/679 της Ε.Ε για την Προστασία Δεδομένων και η Οδηγία 2016/1148 της Ε.Ε. για την ασφάλεια των πληροφοριακών συστημάτων.

Ο Γενικός Κανονισμός 2016/679 της Ε.Ε για την Προστασία Δεδομένων αφορά την προστασία προσωπικών δεδομένων και αποτελεί ένα πολύ σημαντικό βήμα προς την σωστή κατεύθυνση καθώς ρυθμίζει τα όρια της δράσης των παρόχων ψηφιακών υπηρεσιών, τα όργανα και τις αρχές ελέγχου της δράσης αυτής καθώς και τις συγκεκριμένες διαδικασίες

που πρέπει να ακολουθηθούν σε περίπτωση παραβίασης. Αυτό που δεν ορίζεται στον Κανονισμό αυτό είναι οι συγκεκριμένες ποινικές ή διοικητικές κυρώσεις που πρέπει να επιβληθούν στους παρόχους όταν δεν συμμορφώνονται με τις προβλεπόμενες ρυθμίσεις.

Από την άλλη, η Οδηγία 2016/1148 της Ε.Ε. για την ασφάλεια των πληροφοριακών συστημάτων προβλέπει τα όργανα που θα πρέπει να ιδρυθούν και τις διαδικασίες που θα πρέπει να ακολουθηθούν σε περιπτώσεις παραβίασης της ασφάλειας των πληροφοριακών συστημάτων παρόχων ψηφιακών υπηρεσιών, πλην όμως δεν προβλέπει συγκεκριμένα τα μέτρα ασφαλείας που θα πρέπει να λαμβάνονται από τους παρόχους αυτούς για την αποφυγή «συμβάντων» (ή αλλιώς διαταράξεων της λειτουργίας των υπηρεσιών) παρά μόνο αφηρημένα προβλέπει ως υποχρέωση των κρατών μελών την θεσμοθέτηση τέτοιου είδους μέτρων, η παραβίαση των οποίων θα πρέπει να επιφέρει την επιβολή ποινικών ή διοικητικών κυρώσεων.

Συνεπώς παρατηρείται ότι σε αντίθεση με την Σύμβαση και την Οδηγία, οι οποίες παρείχαν πολύ στενά περιθώρια ευελιξίας στους εθνικούς νομοθέτες, τα δύο νέα αυτά ευρωπαϊκά νομοθετήματα παρέχουν στους εθνικούς νομοθέτες τεράστια αν όχι απόλυτη διακριτική ευχέρεια αναφορικά με το ποιες συμπεριφορές πρέπει να ποινικοποιηθούν και πως ακριβώς, ειδικά στις περιπτώσεις μη συμμόρφωση με τη λήψη των απαραίτητων μέτρων ασφαλείας τα οποία δεν ρυθμίζονται καθόλου.

Το γεγονός αυτό πρόκειται να δημιουργήσει προβλήματα ανομοιομορφίας της ποινικής νομοθεσίας των Κρατών Μελών της Ευρωπαϊκής Ένωσης, κάποια από τα οποία μπορεί να μην έχουν απαραίτητες γνώσεις για την θεσμοθέτηση των σχετικών ποινικών διατάξεων. Για το λόγο αυτό είναι απολύτως βέβαιο ότι στο μέλλον θα εκδοθεί μια νέα ευρωπαϊκή οδηγία η οποία θα έχει ως σκοπό τη θέσπιση ελαχίστων κανόνων για τον ορισμό των ποινικών αδικημάτων και διοικητικών παραβάσεων που τελούνται από τους παρόχους ψηφιακών υπηρεσιών όταν δεν συμμορφώνονται με τις υποχρεώσεις που τους επιβάλει το κοινοτικό και το εθνικό ρυθμιστικό πλαίσιο, όπως ακριβώς συνέβη και με την Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

Βιβλιογραφία

Ι. Αγγελή, Διαδίκτυο (Internet) και Ποινικό Δίκαιο, ΠοινΧρ 2000, σελ. 675 επ.

Ι. Αγγελή, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime), ΠοινΔικ 2001, σελ. 1218 επ.

Ι. Αγγελή, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 2001, σελ. 1293 επ.

Ι. Αγγελή, Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, ΠοινΔικ 8-9/2005, σελ. 1062 επ.

Δ. Π. Αγγελόπουλος, Κυβερνοχώρος - Το διεθνές «γίγνεσθαι» στο ελληνικό «είναι», ΕΛ.Ε.Σ.ΜΕ.

Α. Αργυρόπουλου, Ηλεκτρονική Εγκληματικότητα: τα αδικήματα της χωρίς άδεια απόκτησης δεδομένων (202a StBG), 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, 2001. [παραπέμπεται Αργυρόπουλου, Ηλεκτρονική Εγκληματικότητα, 2001]

Ε. Βασιλάκη, Τα φαινόμενα “Phishing”, “Pharming” και η ποινική τους αξιολόγηση, ΠοινΧρ 2007, σελ. 860.

Ε. Βασιλάκη, Η καταπολέμηση της εγκληματικότητας μέσω Η/Υ, 1993

Ι. Ιγγλεζάκη, Δίκαιο της Πληροφορικής, 2008

Μ. Καϊάφα – Γκμπάντι, Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, σελ. 489 επ.

Μ. Καϊάφα – Γκμπάντι, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμεν. 2007, σελ. 1058 επ.

Ι. Καράκωστα, Δίκαιο & Internet – Νομικά ζητήματα του Διαδικτύου, 2009

Δ. Κιούπη, Ποινικό δίκαιο και Internet, Ποινικά 57, 1999

Δ. Κιούπη, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα, Υπερ 2000, σελ. 959 επ.

Δ. Κιούπη, Οι διατάξεις του Ποινικού Κώδικα για το διαδικτυακό έγκλημα, 3ο Πανελλήνιο Συνέδριο της Ένωσης Ελλήνων Νομικών, e-ΘΕΜΙΣ, Το Δίκαιο στην ψηφιακή εποχή, σελ. 151 επ.

Δ. Κιούπη, Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ευρωπαϊκή Ένωση, Δικηγορικός Σύλλογος Πειραιά – Ένωση Ελλήνων Ποινικολόγων – Κέντρο

Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, Σύγχρονες εξελίξεις του Ευρωπαϊκού Οικονομικού Ποινικού Δικαίου, 2010, σελ. 191 επ.

Γ. Λάζου, Πληροφορική και Έγκλημα, 2001

Χ. Μυλωνόπουλου, Το Ευρωπαϊκό Ποινικό Δίκαιο μετά τη Συνθήκη της Λισαβόνας, Η ουσιαστική νομιμοποίηση του Ευρωπαϊκού Ποινικού Δικαίου και η σημασία της ποινικής δογματικής για τη διαμόρφωσή του, ΠοινΧρ 2011, σελ. 81 επ.

Χ. Μυλωνόπουλου, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991

Γ. Νούσκαλη, Ποινική Προστασία Προσωπικών Δεδομένων: Η Νομολογιακή Συμβολή στην Ερμηνεία Βασικών Όρων, 2007 [παραπέμπεται Νούσκαλη, Ποινική Προστασία Προσωπικών Δεδομένων, 2007].

Φ. Σπυρόπουλου, Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (hacking)

Ε. Συμεωνίδου – Καστανίδου, Επιθέσεις κατά συστημάτων πληροφοριών: Οι θέσεις της Ευρωπαϊκής Ένωσης για την ποινική τους αντιμετώπιση και το ελληνικό ποινικό δίκαιο, σε Πρακτικά 4ου Πανελλήνιου Συνεδρίου Ένωσης Ελλήνων Νομικών e-ΘΕΜΙΣ και Πανεπιστημίου Μακεδονίας, με θέμα: Δίκαιο Πληροφορικής: Legal Tech and Data Protection», 2013 σελ. 59 επ.

Ε. Συμεωνίδου – Καστανίδου, Το άρθρο 370Α Π.Κ. και οι πρόσφατες εξαγγελίες για την τροποποίησή του, ΠοινΔικ 2008, σελ. 462 επ.

Ε. Συμεωνίδου – Καστανίδου, Υπεξαίρεση και Λογιστικό Χρήμα, Υπερ. 1998, σελ. 937

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

Κ. Χατζηϊωάννου, Η ποινική αντιμετώπιση των προσβολών ηλεκτρονικών δεδομένων και συστημάτων πληροφοριών, 2013 (Διδακτορική Διατριβή)

K. Chatziioannou, the criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data

S. L. Hopkins, Cybercrime Convention: a positive beginning to a long road ahead, Journal of High Technology Law, 2003, σελ. 101-121

P. D. Venancio, Similarity and competition between cybercrimes related to computer data in the Council of Europe's Convention on Cybercrime, 2013

P. Sommer, Criminalising hacking tools, 2006