ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ

ΣΠΟΥΔΩΝ (ΔΠΜΣ)

«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΜΑΚΕΔΟΝΙΑΣ

ΚΑΙ

ΤΜΗΜΑΤΟΣ ΝΟΜΙΚΗΣ ΔΗΜΟΚΡΙΤΕΙΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΡΑΚΗΣ

Master of Science in «Law and Informatics»

ΜΑΘΗΜΑ: ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Διδάσκων Καθηγητής: Θεοχάρης Δαλακούρας

Φοιτήτρια: Μαρία Δαλαμπίρα-Κίπριγλη

(mli18019)

ΘΕΜΑ

«Η ποινική αντιμετώπιση του κακόβουλου λογισμικού»

Θεσσαλονίκη, Μάρτιος 2024

Η ΠΟΙΝΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Μαρία Δαλαμπίρα-Κίπριγλη

Πτυχίο της Νομικής Σχολής του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης, 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής: Θεοχάρης Δαλακούρας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 1η/03/2024

Θεοχάρης Δαλακούρας	Γεώργιος Δανιήλ	Νικόλαος Σαββίδης
.....	.....	.....

Μαρία Δαλαμπίρα-Κίπριγλη

Περίληψη

Στη σύγχρονη εποχή, η ανάπτυξη της τεχνολογίας είναι ραγδαία· το διαδίκτυο και οι ηλεκτρονικοί υπολογιστές, αλλά και τα νέα συστήματα πληροφοριών (έξυπνα τηλέφωνα –smartphones, τάμπλετ κλπ.), έχουν γίνει αναπόσπαστο μέρος της καθημερινότητας, κάνοντας πολύ πιο εύκολη τη ζωή των ανθρώπων στο σύνολό της. Ωστόσο, παράλληλα με τη διευκόλυνση που προσφέρει η τεχνολογία στη ζωή του ανθρώπου, έχουν αναπτυχθεί και ορισμένες νέες μορφές εγκληματικότητας, οι οποίες συνιστούν σημαντική απειλή στην ασφάλεια του «κυβερνοχώρου», καθώς επωφελούνται από την σύγχρονη τεχνολογία και τα διάφορα μέσα που αυτή παρέχει, με σκοπό την πρόκληση βλάβης ή αλλοίωσης των συστημάτων πληροφοριών και των δεδομένων τους, αλλά και την τέλεση των παραδοσιακών εγκλημάτων, όπως, για παράδειγμα, η απάτη με η/υ. Στο πλαίσιο αυτό, η διεθνής και ευρωπαϊκή νομοθεσία, καθώς και ο Έλληνας νομοθέτης, σε μια προσπάθεια επικαιροποίησης και προσαρμογής στα νέα δεδομένα αλλά και εναρμόνισης του δικαίου, εισήγαγαν νέες μορφές αξιόποινων συμπεριφορών, με σκοπό την αποτελεσματική αντιμετώπιση των νέων αυτών μορφών εγκληματικότητας. Σκοπός της παρούσας εργασίας είναι αφενός να παρουσιάσει ευσύνοπτα τις βασικές μορφές του ηλεκτρονικού εγκλήματος, αφετέρου να εστιάσει τη μελέτη στη περίπτωση του κακόβουλου λογισμικού και της ποινικής του αντιμετώπισης.

Λέξεις Κλειδιά: [τεχνολογία, σύστημα πληροφοριών, κυβερνοχώρος, εγκληματικότητα, ηλεκτρονικό έγκλημα, ΕΕ, ποινικό δίκαιο]

Abstract

In modern times, the development of technology is rapid· the internet and computers, but also new information systems (smart phones - smartphones, tablets, etc.) have become an integral part of everyday life, making life much easier for people as a whole. However, alongside the facilitation of human life by technology, certain new forms of crime have also developed, which pose a significant threat to cyber security, as they take advantage of modern technology and the various means it provides, to damage or alter information and data systems, but also to commit traditional crimes such as, for example, computer fraud. In this context, international and European legislation, as well as the Greek legislator, in an effort to update and adapt to the new data and harmonize the law, introduced new forms of criminal behaviour, in order to effectively deal with these new forms of crime. The aim of this paper is to present the basic forms of cybercrime in a concise manner, and to focus the study on the case of malware and its criminal treatment.

Keywords: [technology, information system, cyberspace, crime, e-crime, EU, criminal law]

Περιεχόμενα

	Περίληψη	3
	Abstract	4
	Εισαγωγικά	7
1.1	Προβληματική και Στόχοι	7
1.2	Μεθοδολογία και Συνεισφορά	8
1.3	Διάρθρωση της Μελέτης	9
2	Προσέγγιση του κακόβουλου λογισμικού από τη σκοπιά του ποινικού δικαίου	11
2.1	Ηλεκτρονικό Έγκλημα - Γενική Επισκόπηση	11
2.1.1	Ορισμός Ηλεκτρονικού Εγκλήματος	12
2.1.2	Χαρακτηριστικά Γνωρίσματα Ηλεκτρονικού Εγκλήματος	14
2.2	Μορφές Ηλεκτρονικού Εγκλήματος	17
2.2.1	Διάκριση των ηλεκτρονικών εγκλημάτων σε γνήσια και μη γνήσια	17
2.2.2	Εννοιολογική προσέγγιση του “κακόβουλου λογισμικού”	19
3	Το νομοθετικό πλαίσιο	29
3.1	Η διεθνής και ενωσιακή ρύθμιση	29
3.1.1	Η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα και λοιπά νομοθετήματα	29
3.1.2	Η Οδηγία 2013/40/ΕΕ	34
3.2	Το ισχύον ελληνικό νομοθετικό πλαίσιο	40
3.2.1	Η διάταξη του άρθρου 19 του Συντάγματος	40
3.2.2	Ο Ν. 4411/2016	42
3.2.3	Οι επιμέρους διατάξεις του Ποινικού Κώδικα	44
3.2.4	Πρόσφατη τροποποίηση με τον Ν. 5002/2022	62
3.2.5	Δικονομική αντιμετώπιση	67
4	Νομικές Δυσχέρειες στην ποινική αντιμετώπιση των υποθέσεων κακόβουλου λογισμικού	76

Συμπερασματικές παρατηρήσεις 81

Βιβλιογραφία/Αρθρογραφία 85

Ελληνική 85

Ξενόγλωσση 89

Εισαγωγικά

1.1 Προβληματική και Στόχοι

Η ταχεία εξέλιξη της τεχνολογίας είναι αδιαμφισβήτητη και αλματώδης. Μεταξύ των πολλών επιτευγμάτων της, το διαδίκτυο ξεχωρίζει ως μια σημαντική δύναμη που έχει διαποτίσει κάθε πτυχή της ανθρώπινης δραστηριότητας, προσφέροντας εύκολη πρόσβαση σε πληροφορίες και εργασία. Με την αφθονία των νέων δεδομένων, η παρουσία των υπολογιστών έχει καταστεί απαραίτητη τόσο σε επαγγελματικό όσο και σε προσωπικό περιβάλλον, ιδιαίτερα στις ανεπτυγμένες χώρες. Ωστόσο, ενώ το Διαδίκτυο έχει επιφέρει αξιοσημείωτη πρόοδο, εγκυμονεί επίσης πολλούς κινδύνους λόγω της εγγενούς ανωνυμίας του, η οποία διευκολύνει τις παράνομες δραστηριότητες.

Κατά συνέπεια, μια νέα μορφή εγκλήματος, γνωστή ως κυβερνοέγκλημα, έχει εμφανιστεί και συνεχίζει να δυναμώνει εν μέσω της παρατεταμένης παγκόσμιας οικονομικής ύφεσης. Η αντιμετώπιση αυτού του ζητήματος θέτει σημαντικές προκλήσεις για τις αρχές, κυρίως λόγω του διφορούμενου νομικού πλαισίου και της έλλειψης εμπειρογνωμοσύνης μεταξύ εκείνων που εμπλέκονται στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Αν και έχουν γίνει προσπάθειες για τον περιορισμό αυτού του διαρκώς εξελισσόμενου εγκληματικού φαινομένου, η αποτελεσματικότητα αυτών των μέτρων παραμένει αμφίβολη.

Μία από τις πιο σημαντικές απειλές για τα συστήματα υπολογιστών που έχει προκύψει ως αποτέλεσμα αυτού του νέου κύματος εγκληματικής συμπεριφοράς είναι το κακόβουλο λογισμικό (malware), το οποίο συνιστά «ένα πρόγραμμα που εισάγεται σε ένα σύστημα, συνήθως κρυφά, με σκοπό να διακυβεύσει την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των δεδομένων, των εφαρμογών ή του λειτουργικού συστήματος του θύματος ή να ενοχλήσει ή να διαταράξει με άλλο τρόπο το θύμα».[1]

[1] *Souppaya, M., Scarfone, K.* Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication SP 800-83, July 2013.

Ως εκ τούτου, γίνεται αντιληπτό ότι η απειλή που θέτει το κακόβουλο λογισμικό θέτει σε κίνδυνο προγράμματα εφαρμογών, προγράμματα κοινής ωφέλειας, όπως προγράμματα επεξεργασίας και μεταγλωττιστές και προγράμματα σε επίπεδο πυρήνα. Ακόμα, μπορεί να γίνει χρήση του σε παραβιασμένους ή κακόβουλους ιστότοπους και διακομιστές, ή σε ειδικά κατασκευασμένα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (spam) ή άλλα μηνύματα, που στοχεύουν να εξαπατήσουν τους χρήστες να αποκαλύψουν ευαίσθητα προσωπικά στοιχεία.

Στο πλαίσιο αυτό, το ιδιαίτερο ενδιαφέρον της παρούσας μελέτης επικεντρώνεται στην προβληματική της απειλής που ενυπάρχει στη χρήση ή εμπορία κακόβουλου λογισμικού, το οποίο μπορεί να προσβάλει πληθώρα ηλεκτρονικών συστημάτων και συστημάτων πληροφορίας, αλλά να οδηγήσει και στη προσβολή προσωπικών και ευαίσθητων δεδομένων. Συνεπώς, κρίθηκε σκόπιμο να γίνει αρχικά μια συνοπτική επισκόπηση του ηλεκτρονικού εν γένει εγκλήματος, παραθέτοντας τις βασικές μορφές της εγκληματικής συμπεριφοράς που εμπεριέχονται στην έννοια του ηλεκτρονικού εγκλήματος.

Εν συνεχεία, κρίθηκε σκόπιμο η μελέτη να εστιάσει στην εξέταση της έννοιας του κακόβουλου λογισμικού στο πλαίσιο του κυβερνοχώρου, ξεκινώντας με την παράθεση των διαφόρων τύπων κακόβουλου λογισμικού και των μέσων που χρησιμοποιεί για να διαδοθεί, όπως ιοί, σκουλήκια και δούρειοι ίπποι. Η μελέτη της θεματικής συνεχίζεται με μια ευσύνοπτη περιγραφή του νομοθετικού, διεθνούς – ενωσιακού- ελληνικού, πλαισίου που ρυθμίζει την ποινική, κυρίως, αντιμετώπιση του επίμαχου φαινομένου.

Τέλος, κρίθηκε αναγκαίο να γίνει μια συνοπτική αναφορά και στις νομικές δυσχέρειες που έχουν παρατηρηθεί αναφορικά με την εισαγωγή ποινικών υποθέσεων κακόβουλου λογισμικού στα εγχώρια δικαστήρια, ολοκληρώνοντας τη μελέτη της θεματικής με ορισμένες συμπερασματικές παρατηρήσεις και προτάσεις.

1.2 Μεθοδολογία και Συνεισφορά

Η παρούσα μελέτη επιχειρεί να αναλύσει την προβληματική της νέας μορφής εγκληματικής συμπεριφοράς, του κυβερνοεγκλήματος, εστιάζοντας στην

περίπτωση του κακόβουλου λογισμικού. Μέσω της έρευνας και της μεθοδολογίας, η παρούσα μελέτη θα εξετάσει το νομικό πλαίσιο που διέπει τη ρύθμιση του κυβερνοεγκλήματος, ως μορφής ηλεκτρονικού εγκλήματος, καθώς επίσης και τις εξειδικευμένες ρυθμίσεις που άπτονται της περίπτωσης του κακόβουλου λογισμικού, το οποίο συνιστά την βασική θεματική της μελέτης, μέσω μιας σειράς διεθνών συμβάσεων και οδηγιών αλλά και των διατάξεων του ελληνικού δικαίου που εφαρμόζονται στην προκειμένη περίπτωση. Για την εξέταση του νομικού πλαισίου και την ποινική αντιμετώπιση του φαινομένου του κακόβουλου λογισμικού θα χρησιμοποιηθούν κείμενα σχετικά με την τρέχουσα κατάσταση του δικαίου. Επιπλέον, μια βιβλιογραφική έρευνα θα παρέχει το μεγαλύτερο μέρος της ραχοκοκαλιάς της νομικής προσέγγισης.

Η συνεισφορά της παρούσας μελέτης συνοψίζεται ως εξής:

1. Μελέτη της έννοιας του κυβερνοεγκλήματος και δη του κακόβουλου λογισμικού ως εγκληματικής συμπεριφοράς στο πλαίσιο του ηλεκτρονικού εγκλήματος.

2. Εξέταση του νομοθετικού κειμένου για το κυβερνοέγκλημα, εστιάζοντας στις ρυθμίσεις για το κακόβουλο λογισμικό σε διεθνές/ενωσιακό και εθνικό επίπεδο.

3. Συνοπτική παρουσίαση των βασικών νομικών δυσχερειών στη ποινική αντιμετώπιση των υποθέσεων περί κακόβουλου λογισμικού, για περαιτέρω κατανόηση των ελλείψεων του νομοθετικού πλαισίου.

4. Προτάσεις για προστασία και για αντιμετώπιση της εγκληματικής συμπεριφοράς με περισσότερη αποτελεσματικότητα.

1.3 Διάρθρωση της μελέτης

Η θεματική της παρούσας μελέτης επικεντρώνεται στην προσέγγιση του φαινομένου του κακόβουλου λογισμικού από τη σκοπιά του ποινικού δικαίου. Συγκεκριμένα, στο πρώτο κεφάλαιο (πέραν του εισαγωγικού) επιχειρείται μια γενική επισκόπηση της έννοιας του ηλεκτρονικού εγκλήματος και των επιμέρους μορφών τέλεσής του, στον κυβερνοχώρο όπου εξελίσσονται οι νέες αυτές μορφές εγκληματικότητας. Εν συνεχεία, γίνεται εξειδικευμένη αναφορά στην

εννοιολογική προσέγγιση του κακόβουλου λογισμικού ως εγκληματικής συμπεριφοράς.

Στην επόμενη ενότητα, εξετάζεται το νομοθετικό πλαίσιο που διέπει τη ρύθμιση του κυβερνοεγκλήματος και, συνακόλουθα, της εγκληματικής συμπεριφοράς μέσω κακόβουλου λογισμικού. Ειδικότερα, εξετάζεται το διεθνές και ευρωπαϊκό νομοθετικό πλαίσιο, ήτοι οι βασικές Συμβάσεις και Οδηγίες που κατευθύνουν την ποινική αντιμετώπιση του φαινομένου, με μεγαλύτερη έμφαση στη Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα και τα πρόσθετα πρωτόκολλά της καθώς και στην Οδηγία 2013/40/ΕΕ. Ακόμη, εξετάζεται και η ρύθμιση του Έλληνα νομοθέτη, εκκινώντας από τη συνταγματική διάταξη που έχει εφαρμογή αλλά και τις διατάξεις του ισχύοντος ποινικού κώδικα. Περαιτέρω, γίνεται αναφορά στους Ν. 4411.2016 και Ν.5002/2022 με τους οποίους επήλθαν ουσιώδεις τροποποιήσεις και επικαιροποιήσεις αναγκαίες για την αποτελεσματική καταπολέμηση του φαινομένου.

Στο τέταρτο και τελευταίο κεφάλαιο της παρούσας γίνεται συνοπτική αναφορά στις βασικές νομικές δυσχέρειες αναφορικά με την αντιμετώπιση των εγκλημάτων του κυβερνοχώρου στο ποινικό χώρο, κυρίως λόγω της ανάγκης για τεχνικό εξειδικευμένο υπόβαθρο και εμπειρογνωσία.

Τέλος, γίνεται αναφορά σε ορισμένες συμπερασματικές παρατηρήσεις και προτάσεις για προστασία οι οποίες προάγουν την ανάπτυξη της συζήτησης για το κυβερνοέγκλημα εν γένει και την αποτελεσματικότητα στη καταπολέμηση του φαινομένου μέσω της ανάδειξης των βασικών προβληματικών και ελλείψεων στο νομοθετικό πλαίσιο και τη ποινική αντιμετώπιση του κακόβουλου λογισμικού.

2 Προσέγγιση του κακόβουλου λογισμικού από τη σκοπιά του ποινικού δικαίου

2.1 Ηλεκτρονικό Έγκλημα– Γενική επισκόπηση

Με την άφιξη της εποχής των υπολογιστών, η ανθρωπότητα πέτυχε μια αξιοσημείωτη τεχνολογική πρόοδο που έφερε επανάσταση στους τομείς της επικοινωνίας, της ασφάλειας και της παροχής υπηρεσιών. Ωστόσο, η εξέλιξη αυτή είχε αδιανόητες συνέπειες, ειδικά όσον αφορά το εγκληματικό φαινόμενο, οι οποίες ξεδιπλώθηκαν σταδιακά.

Αρχικά, η εξέλιξη του ηλεκτρονικού εγκλήματος ήταν αργή λόγω του υψηλού κόστους και της περιορισμένης πρόσβασης στις νέες τεχνολογίες. Ωστόσο, η έκρηξη αυτού του φαινομένου σημειώθηκε στα τέλη της δεκαετίας του 1990, καθώς η χρήση προσωπικών υπολογιστών άρχισε να εξαπλώνεται. Με την πάροδο του χρόνου, οι υπολογιστές και το διαδίκτυο έγιναν ολοένα και πιο διαδεδομένα, σε σημείο που πολύ λίγα άτομα παραμένουν αποσυνδεδεμένα από τον διαδικτυακό κόσμο, καθώς οι σύγχρονες τάσεις στην ψυχαγωγία, την επικοινωνία, τις επιχειρηματικές λειτουργίες και την παροχή υπηρεσιών υπαγόρευσαν την αναγκαιότητα γνώσης και χρήσης των Η/Υ.

Δυστυχώς, αυτή η παρουσία της τεχνολογίας που υπήρξε τομή στη καθημερινότητα των ανθρώπων οδήγησε επίσης σε έξαρση της ηλεκτρονικής εγκληματικής δραστηριότητας. Η ικανότητα των χρηστών να αποθηκεύουν τεράστιο όγκο προσωπικών δεδομένων, τραπεζικών λογαριασμών, φωτογραφιών και άλλων ευαίσθητων πληροφοριών στους διαδικτυακούς τους χώρους ή σε προσωπικές συσκευές αποθήκευσης έχει καταστήσει περιττή τη φυσική παρουσία του δράστη στον τόπο τέλεσης της πράξης προσβολής.

Έτσι, λοιπόν, τεράστια δίκτυα πληροφοριακών συστημάτων και τεράστιοι όγκοι δεδομένων γίνονται στόχοι επίθεσης, καθώς οι δράστες μπορούν να εκμεταλλευτούν, να εξαπατήσουν, να εκβιάσουν, να παρακολουθήσουν και να κερδίσουν παράνομα οικονομικό πλεονέκτημα ή να βλάψουν ανυποψίαστα θύματα χωρίς να απομακρυνθούν από τον δικό τους φυσικό χώρο. Οι συνεχώς διευρυνόμενες ευκαιρίες για τους εγκληματίες του κυβερνοχώρου αποτελούν σημαντική πρόκληση, καθώς οι νομοθετικές επεμβάσεις για την καταπολέμηση

αυτών των εγκλημάτων πάντοτε ακολουθούν την εμφάνισή αυτών, δίνοντας στους δράστες ένα μικρό πλεονέκτημα.

2.1.1 Ορισμός ηλεκτρονικού εγκλήματος

Ο ορισμός του ηλεκτρονικού εγκλήματος ήρθε μετά από πολλές προσπάθειες καθώς υπήρξαν διάφοροι όροι για την περιγραφή της ίδιας κατηγορίας εγκλημάτων στα πλαίσια ενός νεοφυούς και ραγδαία εξελισσόμενου φαινομένου, με αποτέλεσμα την κατά βάση ανυπαρξία ενός κοινώς αναγνωρισμένου ορισμού μέσα από κάποιο νομοθετικό κείμενο, τόσο στην ελληνική όσο και στη Διεθνή και Ευρωπαϊκή έννομη τάξη.

Έχουν γίνει διάφορες προσπάθειες για τον ορισμό του εγκλήματος στον κυβερνοχώρο, με τους Forester και Morrison να προτείνουν για πρώτη φορά το 1994 ότι πρόκειται για εγκληματική πράξη που διαπράττεται κυρίως με χρήση υπολογιστή.[2] Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) έκανε επίσης μια προσπάθεια να ορίσει το έγκλημα στον κυβερνοχώρο ως οποιαδήποτε «παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που έχει σχέση με την αυτόματη επεξεργασία και τη μεταφορά στοιχείων».[3]

Ωστόσο, ο παραπάνω ορισμός δέχθηκε κριτική από μερίδα της θεωρίας[4] για τη γενικότητα και την ασάφειά του, καθιστώντας τον ακατάλληλο για την οριοθέτηση των συγκεκριμένων εγκλημάτων στον κυβερνοχώρο. Κατά συνέπεια, ελλείψει ενός καθολικά αποδεκτού ορισμού, έχουν διατυπωθεί αρκετοί όροι όπως το «πληροφορικό έγκλημα», το «ηλεκτρονικό έγκλημα», το «δικτυακό έγκλημα» και «έγκλημα του κυβερνοχώρου», με επικρατέστερο στην ελληνική επιστήμη τον όρο «ηλεκτρονικό έγκλημα».

Αξιοσημείωτη είναι η τριπλή διάκριση που έκανε ο Αγγελής το 2000[5], η οποία κατηγοριοποιεί τα εγκλήματα που σχετίζονται με υπολογιστές σε τρεις

---

[2] *Βλαχόπουλος Κ.*, Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2007, σελ. 8, υποσ. 1.

[3] *Λάζου, Γ.,* Πληροφορική & Έγκλημα, Νομική Βιβλιοθήκη, Αθήνα 2001, σελ. 51 και *Βασιλάκη, Ε.,* Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών : η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του ν. 1805/88 /, Α. Ν. Σάκκουλας, Αθήνα 1993, σελ. 3, όπου παραπέμπει σε *OECD*, Computer Related Crime: Analysis of legal policy, Paris, 1986.

[4] *Μυλωνόπουλος, Χρ.*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Α. Ν. Σάκκουλας, Αθήνα 1991, σελ. 13-14.

[5] *Αγγελής, Ι.,* Διαδίκτυο (internet) και ποινικό δίκαιο, Έγκλημα στον Κυβερνοχώρο (cybercrime–interne tcrime), ΠοινΧρ 2000, σελ. 678.

ομάδες. Η πρώτη κατηγορία είναι το ηλεκτρονικό έγκλημα ως νέα μορφή εγκληματικής δραστηριότητας, το οποίο αναφέρεται στην κατάχρηση των δυνατοτήτων του ηλεκτρονικού υπολογιστή. Η δεύτερη κατηγορία περιλαμβάνει εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές, ως μια παραλλαγή των υφιστάμενων αδικημάτων, που όμως συγκεκριμένα διαπράττονται με τη χρήση υπολογιστών. Στη παραπάνω κατηγορία αποδίδεται και ο προαναφερθείς ορισμός του ΟΟΣΑ. Τέλος, η τρίτη κατηγορία είναι το ηλεκτρονικό έγκλημα (έγκλημα στο κυβερνοχώρο), μια ειδικότερη μορφή ηλεκτρονικού εγκλήματος που πάντα περιλαμβάνει τη χρήση του διαδικτύου για την τέλεση του εγκλήματος.

Η διεθνής ορολογία έχει επίσης επινοήσει αντίστοιχους όρους όπως «computer crime», «computer related crime», «cybercrime» και «internet related crime».[6] Μεταξύ αυτών, ο όρος cybercrime (κυβερνοέγκλημα) είναι ο επικρατέστερος, δεδομένης της συχνής χρήσης του και της έμφασης στους υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο, αλλά κυρίως επειδή αυτός ο όρος έχει υιοθετηθεί επίσημα από τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.[7]

Στην ελληνική θεωρία, όπως προαναφέρθηκε, έχει επικρατήσει ο όρος «ηλεκτρονικό έγκλημα». Η επικράτηση αυτή μπορεί να αποδοθεί στο γεγονός ότι ο πρώτος νόμος που ψηφίστηκε στην Ελλάδα σχετικά με αυτά τα αδικήματα (ν. 1805/1988) αφορούσε κυρίως εγκλήματα που συνδέονται άμεσα με υπολογιστές (παραβιάσεις προγραμμάτων υπολογιστών, απάτη με η/υ) και διαπράχθηκαν με τη χρήση τους (computer crimes). Αυτός ο νόμος θεσπίστηκε σε μια εποχή που οι υπολογιστές ήταν το κυρίαρχο τεχνολογικό επίτευγμα, πριν από την ευρεία χρήση του διαδικτύου. Ωστόσο, με την υιοθέτηση της Σύμβασης του Συμβουλίου

[6] *Βλαχόπουλου, Κ.,* Ηλεκτρονικό έγκλημα: μορφές, πρόληψη, αντιμετώπιση, Νομική Βιβλιοθήκη, Αθήνα 2007, σελ. 9 επ.

[7] *Clough, J.*, Principles of cybercrime, Cambridge University Press, Cambridge – New York 2010, σελ. 9.

της Ευρώπης, ο όρος «κυβερνοέγκλημα» έχει αποκτήσει ευρεία χρήση και στην ελληνική επιστήμη.[8]

2.1.2 Χαρακτηριστικά γνωρίσματα Ηλεκτρονικού Εγκλήματος

Γίνεται κατανοητό ότι η βασική διαφορά του ηλεκτρονικού εγκλήματος από το συμβατικό είναι η χρήση του ηλεκτρονικού μέσου τέλεσης της αξιόποινης πράξης όπως ο ηλεκτρονικός υπολογιστής, το κινητό τηλέφωνο κ.ο.κ. Εν προκειμένω, το ηλεκτρονικό μέσο τέλεσης μπορεί να λειτουργεί ως στόχος της επίθεσης, ήτοι το θύμα, μπορεί να αποτελέσει το μέσο της διάπραξης της επίθεσης, ως εργαλείο- όπλο, και, τέλος, μπορεί να αποτελεί το βοηθητικό μέσο για την διάπραξη του εγκλήματος, ως αποθηκευτικός χώρος προσωπικών δεδομένων.

Λαμβάνοντας υπόψη τις ανωτέρω σκέψεις, το ηλεκτρονικό έγκλημα μπορεί να διακριθεί σε τρεις βασικές κατηγορίες οι οποίες αφορούν α) τα εγκλήματα που διαπράττονται τόσο σε συμβατικό περιβάλλον όσο και σε περιβάλλον υπολογιστών, β) τα εγκλήματα που διαπράττονται με τη χρήση του Η/Υ αλλά χωρίς δικτύωση και γ) τα εγκλήματα που έχουν να κάνουν αποκλειστικά με τη χρήση του Διαδικτύου.

Αναγνωρίζοντας τα διακριτά χαρακτηριστικά του ηλεκτρονικού εγκλήματος, δεν μπορεί κανείς να υποτιμήσει την επιτακτική ανάγκη για εξειδικευμένη νομοθεσία μέσω υιοθέτησης ειδικών ποινικών νόμων για την αντιμετώπιση αυτών των αδικημάτων αλλά και τις αντικειμενικές δυσκολίες που αποτελούν τροχοπέδη στη διεκπεραίωση αυτής της ανάγκης.

Το ηλεκτρονικό έγκλημα λειτουργεί με ιδιαίτερα χαρακτηριστικά[9], που συμβαίνουν γρήγορα και ταυτόχρονα σε διάφορες πλατφόρμες, παρακάμπτοντας τις χρονοβόρες διαδικασίες που σχετίζονται με τα παραδοσιακά εγκλήματα. Ο δράστης λειτουργεί από την ασφάλεια του προσωπικού του χώρου, χωρίς να υπάρχει ανάγκη φυσικής του έκθεσης στον

[8] Βλ. ενδεικτικά *Αγγελή, Ι.,* Διαδίκτυο (internet) και ποινικό δίκαιο, Έγκλημα στον Κυβερνοχώρο (cybercrime–internet crime), ΠοινΧρ 2000, σελ. 675 επ., *του ιδίου,* Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο, ΠοινΔικ 2001, σελ. 1293 επ.

[9] *Αγγελής* (2000), ό.π., και *Mitchell S./ Baker E.* (1998) Private Intrusion Response, Harvard Journal of Law & Technology, Volume 11, Number 3, σελ. 707 επ.

τόπο της προσβολής, αξιοποιώντας αυτά τα ιδιαίτερα χαρακτηριστικά για να αποτελέσει ακόμη μεγαλύτερη απειλή, απαιτώντας άμεση νομοθετική δράση και παρέμβαση.

Αυτά τα ιδιαίτερα χαρακτηριστικά περιλαμβάνουν την ευκολία και την ανωνυμία που παρέχεται στον δράστη, την ταχύτητα με την οποία διαπράττονται τα εγκλήματα, τη δυνατότητα διασυνοριακής εγκληματικής δραστηριότητας και την έλλειψη προληπτικής αντίδρασης από τις διωκτικές αρχές και τα θύματα, οι οποίοι αδρανούν στην αντιμετώπιση αυτών των φαινομένων. Ο επιτιθέμενος έχει άφθονες ευκαιρίες να καλύψει τα ίχνη του πριν καν το θύμα αντιληφθεί την επίθεση. Επιπλέον, το διασυνοριακό έγκλημα εκ φύσεως ενέχει τον κίνδυνο διαφορετικών νομικών προσεγγίσεων στην αντιμετώπιση από τα διάφορα κράτη στα οποία τελέστηκε το έγκλημα, με συχνό αποτέλεσμα την πιθανή ατιμωρησία του δράστη. Επιπλέον, οι εταιρείες που παρέχουν τα μέσα για αυτά τα εγκλήματα συχνά δίνουν προτεραιότητα στη φήμη τους έναντι της βοήθειας στις έρευνες, παραμένοντας σιωπηλοί για περιστατικά και αμελώντας να τα καταγγέλλουν προκειμένου να διατηρήσουν την εμπορική τους αξία. Τέλος, οι δράστες εκμεταλλεύονται κοινά καθημερινά αντικείμενα που έχουν δυνατότητα πρόσβασης στο διαδίκτυο (διαδίκτυο των πραγμάτων - IoT) και προγράμματα λογισμικού, όπως υπολογιστές, smartphone smartwatches, e- banking, mails, i-cloud κ.ο.κ., στα οποία τα άτομα εκτίθενται αυτοβούλως πρόθυμα.

Τα εγκλήματα κατά της ιδιοκτησίας και των προσωπικών δεδομένων βαίνουν ολοένα αυξανόμενα, καθώς βασίζονται στην οικειοθελή έκθεση των θυμάτων στο διαδίκτυο, τα οποία στη σύγχρονη εποχή μοιράζονται πρόθυμα μια πληθώρα προσωπικών πληροφοριών στο διαδίκτυο, χωρίς να εξετάζουν ποιος μπορεί να τις δει ή πώς μπορεί να τις εκμεταλλευτεί. Κατά συνέπεια, γίνεται αντιληπτό ότι ο ίδιος ο εθισμός των δυνητικών θυμάτων στις απεριόριστες δυνατότητες του Διαδικτύου χρησιμεύει ως κερκόπορτα για τη διάπραξη του εγκλήματος στον κυβερνοχώρο.

Οι συμπεριφορές των δραστών μπορούν να ταξινομηθούν σε τρεις κατηγορίες: α) εξωτερικές απειλές, οι οποίες περιλαμβάνουν επιθέσεις από άτομα εκτός του συστήματος, όπως hackers, vandals κλπ, σε β) εσωτερικές απειλές, οι

οποίες αναφέρονται σε επιθέσεις που εκτελούνται από άτομα που βρίσκονται εντός του εμπιστευτικού περιβάλλοντος, όπως εργαζόμενοι σε μια εταιρεία· και γ) η κοινωνική μηχανική, ένα είδος επίθεσης που αξιοποιεί τον ανθρώπινο παράγοντα για να διεισδύσει σε διαδικτυακά συστήματα και δύναται να εμπεριέχει και τις δύο παραπάνω προαναφερθείσες κατηγορίες. Εντούτοις, είναι αδύνατο να καταρτιστεί ένας εξαντλητικός κατάλογος όλων των εγκλημάτων που μπορούν να διαπραχθούν χρησιμοποιώντας ηλεκτρονικές συσκευές, καθώς η ταχεία ανάπτυξή τους σε συνδυασμό με την ευφυΐα και την επινοητικότητα του μέσου ανθρώπου οδηγεί στη συνεχή εμφάνιση νέων αδικημάτων.

Είναι προφανές ότι η πρόοδος της τεχνολογίας όχι μόνο οδηγεί στην εφεύρεση νέων ηλεκτρονικών εγκλημάτων που ήταν προηγουμένως άγνωστα στο ευρύ κοινό, αλλά διευκολύνει επίσης τον εκσυγχρονισμό των μεσών τέλεσης των ήδη υπαρχόντων (συμβατικών) αδικημάτων, είτε εμπίπτουν στην αρμοδιότητα γενικού ποινικού δικαίου είτε στους ειδικούς ποινικούς νόμους. Από αυτή τη σύντομη, δε, εισαγωγή, γίνονται εμφανείς δύο κατηγορίες εγκλημάτων: α) τα γνήσια ηλεκτρονικά εγκλήματα που δημιουργήθηκαν μόνο με την εμφάνιση των ηλεκτρονικών υπολογιστών και συσκευών και β) τα μη γνήσια ηλεκτρονικά εγκλήματα που προϋπήρχαν και τώρα διευκολύνονται από τη χρήση ηλεκτρονικών υπολογιστών ως μέσα τέλεσης τους. Οι εν λόγω κατηγορίες εγκλημάτων θα εξεταστούν αυτοτελώς στην επόμενη ενότητα.

2.2 Μορφές ηλεκτρονικού εγκλήματος

2.2.1 Διάκριση των ηλεκτρονικών εγκλημάτων σε γνήσια και μη γνήσια

Όπως προαναφέρθηκε, η βασική ταξινόμηση των ηλεκτρονικών εγκλημάτων τα διακρίνει σε αυτά που διαπράττονται με τη χρήση ηλεκτρονικού υπολογιστή, με ή χωρίς ταυτόχρονη χρήση του διαδικτύου, και σε αυτά που διαπράττονται αποκλειστικά μέσω διαδικτύου. Τα δεύτερα ονομάζονται κυβερνοεγκλήματα.

Στην κατηγορία των γνήσιων κυβερνοεγκλημάτων εντάσσονται εγκλήματα, τα οποία δεν υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και λοιπών συστημάτων πληροφοριών και του διαδικτύου. Αυτά διαπράττονται αποκλειστικά στο διαδίκτυο δηλαδή στον κυβερνοχώρο, επηρεάζουν τα παραδοσιακά έννομα αγαθά αλλά απαιτούν χωριστή ταξινόμηση λόγω των ιδιαίτερων χαρακτηριστικών τους και την διαφοροποίηση στη νομοτυπική τους μορφή, διαφορετικά θα έπρεπε να εφαρμοστεί αναλογικά αλλά κυρίως ανεπίτρεπτα και άδικα ό,τι ισχύει για το προϋπάρχον παραδοσιακό-συμβατικό αδίκημα. Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας συνιστά η περίπτωση της απάτης με η/υ (386Α ΠΚ), που διαφοροποιείται σε σχέση με την απάτη του άρ. 386 ΠΚ, καθώς η προσβολή του εννόμου αγαθού της περιουσίας δεν πραγματοποιείται με την παραπλάνηση κάποιου προσώπου όπως συμβαίνει στη νομοτυπική μορφή του παραδοσιακού εγκλήματος, αλλά με την επέμβαση σε ένα πρόγραμμα η/υ ή στα στοιχεία αυτού. Άλλο παράδειγμα είναι η διάδοση παιδικής πορνογραφίας μέσω συστημάτων πληροφοριών (άρ. 348 Α ΠΚ).

Η δεύτερη κατηγορία περιλαμβάνει εγκλήματα που προσβάλλουν παραδοσιακά έννομα αγαθά και μπορούν να διαπραχθούν τόσο στον φυσικό χώρο, όσο και στον κυβερνοχώρο. Χαρακτηριστικά παραδείγματα αυτής της κατηγορίας στοιχειοθετούν οι προσβολές με τη μορφή εξύβρισης (361 ΠΚ), δυσφημιστικών (362-363 ΠΚ) ή ρατσιστικών σχολίων (άρ. 1, 2 του ν. 927/1979) που γίνονται από ορισμένους (κυρίως ανώνυμους) χρήστες προς κάποιους άλλους μέσω διάφορων διαδικτυακών πλατφορμών κοινωνικής δικτύωσης (social media, fora κλπ.). Αυτά είναι τα μη γνήσια κυβερνοεγκλήματα, στα οποία το διαδίκτυο χρησιμοποιείται απλώς ως μέσο τέλεσης του συμβατικού αδικήματος.

Τέλος, η τρίτη ομάδα περιλαμβάνει ορισμένα εγκλήματα, η τέλεση των οποίων διαπράττεται αποκλειστικά σε περιβάλλον ηλεκτρονικού υπολογιστή, χωρίς να είναι απαραίτητη η παρουσία του διαδικτύου, με το πρόσθετο στοιχείο ότι στην εν λόγω κατηγορία η προσβολή στοχεύει στα ηλεκτρονικά δεδομένα που είτε οδηγούν σ' ένα εξειδικευμένο, σχετικό αποκλειστικά με τα δεδομένα, έννομο αγαθό είτε συνδέονται πάντως άρρηκτα με ένα άλλο έννομο αγαθό. Χαρακτηριστικά παραδείγματα της εν λόγω κατηγορίας είναι η μη εξουσιοδοτημένη πρόσβαση σε αρχεία προσωπικών δεδομένων που τηρούνται ηλεκτρονικά (προσβολή δεδομένων προσωπικού χαρακτήρα) και παραβιάσεις της νομοθεσίας περί πνευματικής ιδιοκτησίας (ν. 2121/1993) που σχετίζονται με προγράμματα ηλεκτρονικών υπολογιστών. Αυτά τα αδικήματα προσβάλλουν τα ίδια τα πληροφοριακά συστήματα και τα δεδομένα που περιέχουν. Οι επιθέσεις περιλαμβάνουν κυρίως μη εξουσιοδοτημένη πρόσβαση ή παραβίαση εμπιστευτικών και απόρρητων δεδομένων (γνωστό ως hacking), καθώς και ενέργειες που διακόπτουν ή εμποδίζουν τη χρήση υπολογιστή ή την πρόσβαση δεδομένων (όπως αλλαγές κωδικού πρόσβασης). Επιπλέον, οι προκείμενες επιθέσεις-πράξεις προσβολής συνίστανται και σε πράξεις που οδηγούν σε «φθορά» των ηλεκτρονικών υπολογιστών ή των εξαρτημάτων τους, καθώς και σε παράνομες πράξεις όπως η αντιγραφή, η αλλοίωση ή η εξάλειψη δεδομένων (ιδιαίτερα διαδεδομένη μετά από μολύνσεις από ιούς).

Αυτή η εργασία στοχεύει να εμβαθύνει κυρίως στο αδίκημα της επίθεσης των συστημάτων πληροφοριών με κακόβουλο λογισμικό (malware) και ως εκ τούτου θα αναλυθεί εκτενέστερα στη συνέχεια η εξειδικευμένη αυτή περίπτωση ηλεκτρονικού εγκλήματος.

2.2.2 Εννοιολογική προσέγγιση του «κακόβουλου λογισμικού»

Από τις πιο διαδεδομένες μορφές επιθέσεως κατά των δεδομένων ενός συστήματος πληροφοριών είναι η προσβολή μέσω κακόβουλου λογισμικού, η οποία (προσβολή) συνίσταται στη διαγραφή, φθορά, αλλοίωση, εξάλειψη ή αποκλεισμό πρόσβασης του ατόμου στο σύστημα πληροφοριών. Ο διεθνής όρος

για το κακόβουλο λογισμικό, ήτοι ο όρος «malware»[10]αποτελεί συντόμευση του όρου malicious software (κακόβουλο λογισμικό) και σκοπός του είναι η επίθεση σε έναν αυτόνομο ή συνδεδεμένο σε δίκτυο υπολογιστή, για την κλοπή πληροφοριών ή ταυτότητας, για κατασκοπεία και για διακοπή των υπηρεσιών. Συνεπώς, πρόκειται για προγράμματα, τα οποία εισβάλλουν στο σύστημα πληροφοριών του ηλεκτρονικού υπολογιστή και δύνανται να παραβιάσουν την ασφάλεια του με σκοπό κυρίως την υποκλοπή προσωπικών δεδομένων.

Οι σημαντικότερες, δε, και πιο διαδεδομένες κατηγορίες κακόβουλου λογισμικού είναι οι «ιοί» ("viruses"), τα «σκουλήκια» ("worms"), οι «Δούρειοι Ίπποι» ("Trojan horses") κ.λπ., ενώ υπάρχουν και άλλα είδη, λιγότερα συνηθισμένα στην χρήση, όπως η λογική βόμβα, τα βακτήρια, τα scareware, τα bots-zombies, τα rootkits κ.α. Εν συνεχεία θα παρατεθούν ορισμένες πληροφορίες για τα βασικά είδη κακόβουλου λογισμικού, ήτοι τους ιούς, τα ηλεκτρονικά σκουλήκια και τους δούρειους ίππους, αλλά θα γίνει και συνοπτική αναφορά σε μερικά είδη κακόβουλου λογισμικού που έγιναν πιο συνηθισμένα τα τελευταία χρόνια, μετά την εμφάνιση της πανδημίας του κορονοϊού, όπου υιοθετήθηκε η εργασία από απόσταση, όπως για παράδειγμα τα spam στην ηλεκτρονική αλληλογραφία των εργαζομένων από το σπίτι.

Ειδικότερα, οι «ιοί» (viruses) συνιστούν το πιο διαδεδομένο και σύνηθες στη χρήση είδος κακόβουλου λογισμικού, αποτελούνται δε από ένα πρόγραμμα το οποίο επισυνάπτει τον εαυτό του στα αρχεία του υπολογιστή, μέσω μιας διαδικασίας που είναι γνωστή ως «μόλυνση», χρησιμοποιώντας μακροεντολές για να εκτελέσει τον κακόβουλο κώδικά του. Με το άνοιγμα ή την εκτέλεση αυτού του αρχείου, ο ιός ενεργοποιείται και οι επόμενες ενέργειές του εξαρτώνται από τον συγκεκριμένο προγραμματισμό του. Ορισμένοι ιοί προκαλούν σημαντική βλάβη στην απόδοση του συστήματος, γίνονται αντιληπτοί στον χρήστη, ενώ άλλοι παραμένουν δυσδιάκριτοι. Κατά συνέπεια, η απώλεια δεδομένων είναι μια κοινή επίπτωση πέρα από τις λειτουργικές διακοπές που προκαλούνται στον η/υ.

[10] *Saeed, I.A., Selamat, A. και Abuagoub, A.M.* (2013). A survey on malware and malware detection systems. International Journal of Computer Applications, σελ. 67(16).

Οι ιοί έχουν τη μοναδική ικανότητα να διεισδύουν και να καταστρέφουν προγράμματα υπολογιστών, εξαπλώνοντας γρήγορα και προκαλώντας δυσλειτουργίες του συστήματος ή ακόμα και πλήρη καταστροφή. Αυτά τα κακόβουλα προγράμματα μπορούν να εισβάλουν στον σκληρό δίσκο του υπολογιστή, να προκαλέσουν καθολική καταστροφή ή δυσλειτουργίες σε στοιχεία λογισμικού, ακόμη και να χειριστούν ή να διαγράψουν άλλα αρχεία ή τμήματα του λογισμικού και προγράμματα. Το πιο χαρακτηριστικό τους χαρακτηριστικό είναι η ικανότητά τους να πολλαπλασιάζονται ακατάπαυστα, δίνοντάς τους τη δυνατότητα να διαδίδονται αβίαστα από το ένα σύστημα στο άλλο και να αναπαράγονται από υπολογιστή σε υπολογιστή χωρίς τη βοήθεια εξωτερικού προγράμματος ή αρχείου.[11] Οι ιοί, ως μια μορφή κακόβουλου λογισμικού, συνεχίζουν να προκαλούν προβλήματα παγκοσμίως, ωστόσο, πιο τρομερές απειλές έχουν εμφανιστεί τον τελευταίο καιρό.

Μία από τις πιο σημαντικές απειλές στον τομέα του κακόβουλου λογισμικού είναι η παρουσία σκουληκιών ("worms")[12]. Αυτά τα κακόβουλα προγράμματα όχι μόνο επιβαρύνουν τα δίκτυα με άσκοπη δραστηριότητα, αλλά έχουν επίσης τη δυνατότητα γρήγορης αναπαραγωγής και πρόσβασης σε προσωπικές πληροφορίες. Σε αντίθεση με τους ιούς, τα «σκουλήκια» δεν χρειάζεται να προσαρτηθούν σε ένα αρχείο για να διαδοθούν, παρότι και αυτά συνιστούν προγράμματα η/υ που αυτο-αναπαράγονται και εξαπλώνονται σε ευρεία κλίμακα σε όλο το διαδίκτυο. Έτσι, τα «σκουλήκια» μπορούν να πολλαπλασιάζονται χωρίς να απαιτείται κάποια ενέργεια από το χρήστη, μεταφέροντας άλλα προγράμματα (συνήθως ιούς) στο σύστημα πληροφοριών του η/υ.[13]

---

[11] *Βλαχόπουλος*, ό.π., σελ. 47 επ.

[12] *Ομοίως*, σελ. 50 επ.

[13] Το πιο διαδεδομένο «σκουλήκι» ονομαζόταν «ILOVEYOU» και εξαπλωνόταν στον η/υ του θύματος μέσω e-mail, με θέμα ILOVEYOU και ένα συνημμένο αρχείο LOVE-LETTER-FORYOU. TXT.VPS, το οποίο εφόσον ανοιγόταν από τον χρήστη διέγραφε αρχεία του η/υ και όριζε ως αρχική σελίδα στον φυλλομετρητή (browser) του υπολογιστή μια ιστοσελίδα σε ένα διακομιστή στις Φιλιππίνες. Με το άνοιγμα της αρχικής σελίδας εγκαθίστατο αυτόματα ένας «Δούρειος Ίππος» μέσω του οποίου οι δράστες υπέκλεπταν τους κωδικούς πρόσβασης του χρηστή. Το «σκουλήκι» αυτό υπολογίζεται ότι εξαπλώθηκε σε περίπου 45 εκατομμύρια υπολογιστές και εκτιμάται ότι προκάλεσε την μεγαλύτερη οικονομική καταστροφή στην ιστορία των ίων των η/υ, με συνολικές ζημιές άνω τα 9.000.000.000$. Βλ. σχετικά *Βλαχόπουλου*, ό.π. σελ. 47 επ.

Τα σκουλήκια εξαπλώνονται γρήγορα σε ένα δίκτυο, εκμεταλλευόμενοι τυχόν υφιστάμενα τρωτά σημεία ασφαλείας σε υπολογιστές ή δίκτυα. Σε αντίθεση με τους ιούς, τα σκουλήκια μπορούν να μολύνουν μια συσκευή μέσω ενός ληφθέντος αρχείου ή μιας σύνδεσης δικτύου πριν πολλαπλασιαστούν και εξαπλωθούν γρήγορα. Αυτό ενέχει κίνδυνο για την ομαλή λειτουργία των μολυσμένων συστημάτων και μπορεί ακόμη και να οδηγήσει σε απώλεια ευαίσθητων δεδομένων. Επιπλέον, τα σκουλήκια καταναλώνουν μεγάλη ποσότητα εύρους ζώνης δικτύου, γεγονός που μπορεί να οδηγήσει σε ζημιές, όπως επιβράδυνση των συνδέσεων δικτύου, ακόμη και χωρίς παρεμβολές στο σύστημα του η/υ ή κλοπή δεδομένων.

Μια άλλη σημαντική απειλή αποτελούν οι δούρειοι ιοί ή οι «Δούρειοι Ίπποι» (Trojans horses), που ονομάστηκαν από τη διάσημη ιστορία του Δούρειου Ίππου. Αυτό το κακόβουλο λογισμικό μεταμφιέζεται σε φαινομενικά αθώα προγράμματα που φορτώνονται στο σκληρό δίσκο του η/υ και εκτελείται κανονικά μαζί με τα υπόλοιπα προγράμματα, συχνά με τη μορφή παιχνιδιών, με σκοπό την υποκλοπή προσωπικών πληροφοριών των χρηστών του Διαδικτύου. Με την εκμετάλλευση ενός μυστικού σημείου εισόδου, οι εισβολείς αποκτούν πρόσβαση στα συστήματα και μπορούν να ανακτήσουν προσωπικές πληροφορίες. Μόλις εγκατασταθεί ένας δούρειος ίππος στον υπολογιστή ενός θύματος, ο δράστης (χάκερ) μπορεί να έχει πρόσβαση στο σύστημα πληροφοριών, στον σκληρό δίσκο ή στο email του. Οι χρήστες, χωρίς να γνωρίζουν την εξαπάτηση, παρέχουν άθελά τους στον χάκερ τα στοιχεία σύνδεσής τους (όνομα χρήστη και κωδικό πρόσβασης). Είναι επίσης σύνηθες για τους χάκερ να χρησιμοποιούν δούρειους ίππους ως μέσο για να αποκτήσουν πρόσβαση σε πολλούς υπολογιστές και να προκαλέσουν εκτεταμένες επιθέσεις άρνησης εξυπηρέτησης (DDOS).[14]

Εκτός από τα βασικά αυτά είδη κακόβουλου λογισμικού, πλέον έχουν γίνει ιδιαίτερα γνωστά και άλλα είδη επιθέσεων, τα οποία άρχισαν να εξαπλώνονται

[14] «(Df-service attack, DoS attack) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες». Ορισμός διαθέσιμος στην ιστοσελίδα: https://el.wikipedia.org/wiki/Επιθέσεις_άρνησης_υπηρεσιών Ανακτήθηκε στις 29.06.2023.

τα τελευταία χρόνια με τη ραγδαία αύξηση της τεχνολογίας και των μέσων κοινωνικής δικτύωσης. Ένα από αυτά είναι και τα λεγόμενα «spam», όπου πρόκειται για την αποστολή ανεπιθύμητης ηλεκτρονικής αλληλογραφίας, στα πλαίσια επιχειρηματικής δραστηριότητας, η οποία περιέχει κακόβουλο και ορισμένες φορές κατασκοπευτικό λογισμικό.[15]

Η ανεπιθύμητη ηλεκτρονική αλληλογραφία αποτελεί μία πραγματική μάστιγα στον χώρο των ηλεκτρονικών επικοινωνιών που εκτός από ενοχλητική είναι και παράνομη κατ' εφαρμογή των διατάξεων του ελληνικού Ν 3471/2006[16] (άρθρο 4 παρ.5) για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, σε μια προσπάθεια ενσωμάτωσης της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Ωστόσο, παρότι στην χώρα μας υπάρχει και το σχετικό νομοθετικό πλαίσιο, υπόθεση αφορώσα το αδίκημα της αποστολής ανεπιθύμητης ηλεκτρονικής αλληλογραφίας τέθηκε στο αρχείο με την αιτιολογία ότι αυτή δεν αποτελεί αξιόποινη πράξη, γεγονός που κρίθηκε ως ατυχές.[17]

Εξέχον παράδειγμα ανεπιθύμητης αλληλογραφίας, η οποία εκτός από ενοχλητική είναι και παράνομη και οδηγεί στη διάπραξη αξιόποινων πράξεων είναι και το γνωστό «ψαρέματος» (phising), ήτοι μια ενέργεια εξαπάτησης μέσω της αποστολής ηλεκτρονικών μηνυμάτων σε χρήστες του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, όπως για παράδειγμα μια τράπεζα ή κάποια άλλη δημοφιλή ηλεκτρονική υπηρεσία, που ζητά από το θύμα να αποκαλύψει προσωπικά στοιχεία όπως τα διαπιστευτήρια του, έναν αριθμό πιστωτικής κάρτας ή άλλες ευαίσθητες πληροφορίες. Έτσι, ο δράστης καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία,

---

[15] Το 2021 εντοπίστηκαν 283 δισεκατομμύρια μηνύματα spam από συνολικά 336,41 δισεκατομμύρια μηνύματα που στάλθηκαν, ενώ εκτιμάται ότι μέχρι το 2025, οι χάκερς θα έχουν προκαλέσει οικονομικές απώλειες άνω των 10,5 τρισεκατομμυρίων δολαρίων. Δεδομένα διαθέσιμα στην ιστοσελίδα: <https://marketsplash.com/el/statistika-anepithymitis-allilografias/> Ανακτήθηκε στις 29.06.2023.

[16] *Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997* (ΦΕΚ Α 133/28.06.2006).

[17] *Μεταξάκης Ε.,* Η ποινική αντιμετώπιση της ανεπιθύμητης αλληλογραφίας επ αφορμή της ΠραξΑρχειοθΕισΠρΑθ τηηςλεκτρονικής, ΠοινΔΙκ 2015, σελ. 681 επ.

και την άγνοια του χρήστη, τον εξαπατά με σκοπό την αθέμιτη απόκτηση προσωπικών και ευαίσθητων δεδομένων και απώτερο συνήθως στόχο την παράνομη απόκτηση οικονομικού οφέλους.[18] Σε άλλες περιπτώσεις, το phishing λειτουργεί για σκοπούς spamming, για την προώθηση κακόβουλου λογισμικού ή για την προώθηση διαφημιστικών στο πλαίσιο εμπορικού σκοπού. Καθώς το διαδίκτυο είναι μη ελεγχόμενο, δεν υπάρχει κάποια ενιαία κρατική ή άλλη αντίστοιχη αρχή, που μπορεί να ελέγχει το περιεχόμενό του διαδικτύου πριν αυτό δημοσιευθεί.

Ωστόσο, έχουν γίνει ορισμένες νομοθετικές ρυθμίσεις οι οποίες αποσκοπούν στην αναστολή αυτών των αξιόποινων πράξεων που διαπράττονται μέσω Διαδικτύου. Συγκεκριμένα, το 2005 θεσπίστηκε στις Ηνωμένες πολιτείες η «Anti-Phishing Act»[19], νομοθεσία που καταδικάζει σε ποινή φυλάκισης 5 ετών την κλοπή ταυτότητας μέσω παραποιημένων εταιρικών ιστοσελίδων ή μηνυμάτων ηλεκτρονικού ταχυδρομείου, ενώ το 2006 θεσπίστηκε το «Fraud Act» στο Ηνωμένο Βασίλειο, ορίζοντας την ηλεκτρονική απάτη ως αδίκημα το οποίο τιμωρείται με ποινή φυλάκισης έως και 10 ετών και απαγορεύει ρητά τη δημιουργία ή κατοχή εργαλείων ηλεκτρονικού «ψαρέματος».[20] Αναφορικά, δε, με την ελληνική νομοθεσία, το «phishing» θεωρείται ότι υπάγεται μέχρι στιγμής στο παραδοσιακό αδίκημα της απάτης του άρθρου 386 ΠΚ,[21] εφόσον προϋποτίθεται η γνώση και θέληση των δραστών σχετικά με την παράνομη δραστηριότητά τους.[22]

---

[18] *Spring, T., Spam Slayer*: Do You Speak Spam?, PC World Article (2003), *Felix, J., Hauck, C.*, 'System Security: A Hacker's Perspective', Interex Proceedings 8: 6 (1987).

[19] S.472 - Anti-phishing Act of 2005. Νομοθεσία διαθέσιμη στην ιστοσελίδα https://www.congress.gov/bill/109th-congress/senate-bill/472 Ανάκτηση 29.06.2023.

[20] Fraud Act 2006 (c 35). Νομοθεσία διαθέσιμη στην ιστοσελίδα https://www.legislation.gov.uk/ukpga/2006/35/contents Ανάκτηση 29.06.2023.

[21] «1. *Όποιος με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή.».*

[22] *Stevenson, RLB,* 'PLUGGING THE "PHISHING" HOLE: LEGISLATION VERSUS TECHNOLOGY ', Duke L. & Tech. Rev., (2005).

Πλέον γνωστά έχουν γίνει και τα λογισμικά κατασκοπίας (spywares), η επικράτηση των οποίων στη στόχευση τόσο ατόμων όσο και εταιρειών έχει σημαντικό οικονομικό αντίκτυπο. Το λογισμικό κατασκοπίας, γνωστό ως spyware, εξυπηρετεί τη συλλογή πληροφοριών από ανυποψίαστα θύματα και τη μετάδοσή τους στον απομακρυσμένο υπολογιστή του εισβολέα. Αυτή η παράνομη συλλογή δεδομένων πραγματοποιείται χωρίς καμία μορφή εξουσιοδότησης ή άδειας, καθώς το κακόβουλο λογισμικό λειτουργεί κρυφά στο σύστημα του θύματος χωρίς να διακόπτει τις κανονικές του λειτουργίες. Σε ορισμένες περιπτώσεις, τα spyware παρέχουν ακόμη και απομακρυσμένη πρόσβαση στον δράστη-χάκερ, επιτρέποντάς του να εμπλακεί σε στοχευμένη κλοπή πολύτιμων δεδομένων.

Ένα παράδειγμα τέτοιου λογισμικού είναι το εξειδικευμένο κακόβουλο λογισμικό πρόγραμμα «Καταγραφής πλήκτρων» (keylogger), το οποίο παρακολουθεί και καταγράφει σχολαστικά κάθε πάτημα πλήκτρων από το θύμα, όπως οι διάφορες ιστοσελίδες που έχει επισκεφτεί, οι κωδικοί πρόσβασής του σε αυτές, ακόμα και τα e-mails που αυτός συντάσσει. Κατά συνέπεια, κρίσιμα διαπιστευτήρια, συμπεριλαμβανομένων εκείνων που σχετίζονται με τραπεζικούς λογαριασμούς, όπως κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών, μπορούν να κλαπούν αβίαστα. Φυσικά, η πράξη της κατασκοπείας εκτείνεται πέρα από την παρακολούθηση των πλήκτρων, καθώς υπάρχει λογισμικό ικανό να καταγράφει βίντεο από κάμερες web, στιγμιότυπα οθόνης, ακόμη και ήχο από μικρόφωνα. Η καταγραφή, δε, όλων των ενεργειών του χρήστη μέσω της καταγραφής των πατημάτων του πληκτρολογίου του πραγματοποιείται μέσω spyware που εκτελείται χωρίς να αφήνει ίχνη του δράστη και στη συνέχεια οι πληροφορίες αποστέλλονται στον εισβολέα (hacker) ακόμα και με e- mail.[23]

Συνεπώς, γίνεται αντιληπτό ότι ο η αύξηση των κακόβουλων λογισμικών όπως τα «σκουλήκια» και οι «ιοί» έχει διευκολύνει σημαντικά και τη μαζική διάδοση ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Κατά συνέπεια, μόλις εγκατασταθούν, επιτρέπουν στους εισβολείς να αναλάβουν τον έλεγχο των παραβιασμένων συστημάτων υπολογιστών, μετατρέποντάς τα στα λεγόμενα

[23] *Βλαχόπουλος,* ό.π. σελ. 52.

botnet «δίκτυα προγραμμάτων ρομπότ» που κρύβουν την πραγματική ταυτότητα του αποστολέα.[24]Αυτά τα δίκτυα συχνά ενοικιάζονται σε spammers, phishers και πωλητές spyware για δόλιους και εγκληματικούς σκοπούς.[25]

Με την απότομη άνοδο των τιμών των κρυπτονομισμάτων που παρατηρήθηκε το 2017 αναδύθηκε και το κακόβουλο λογισμικό με τον ιό Cryptocurrency Miner, το οποίο διεισδύει στο σύστημα ενός θύματος προκειμένου να οικειοποιηθεί ένα μέρος της επεξεργαστικής του ισχύος, το οποίο στη συνέχεια χρησιμοποιείται για τη δημιουργία νέων μονάδων ενός κρυπτονομίσματος. Αυτή η διαδικασία περιλαμβάνει την εκτέλεση περίπλοκων μαθηματικών πράξεων και τεχνικών επίλυσης προβλημάτων, που εκμεταλλεύονται αποτελεσματικά την ισχύ που έχει παραβιαστεί. Συγκεκριμένα, οι υπολογιστές που λειτουργούν με λειτουργικό σύστημα Windows και τα smartphone που χρησιμοποιούν σύστημα Android είναι ιδιαίτερα ευάλωτοι, καθώς αποτελούν ευκολότερους στόχους. Μια πτυχή που έχει συμβάλει στη δημοτικότητα των cryptominers τα τελευταία χρόνια είναι ότι οι κυβερνοεγκληματίες δεν χρειάζεται να διαθέτουν προηγμένη τεχνογνωσία στον τομέα. Ενώ μπορεί να αποφέρουν σχετικά μέτρια κέρδη για τον εισβολέα, η προσβασιμότητα και η ευκολία εφαρμογής τους είναι αναμφισβήτητα πλεονεκτήματα.

Το Adware, ένα κακόβουλο λογισμικό, το οποίο λειτουργεί συλλέγοντας δεδομένα σχετικά με τη χρήση υπολογιστή του θύματος και χρησιμοποιώντας αυτές τις πληροφορίες για την εμφάνιση σχετικών διαφημίσεων. Αν και αυτή η λειτουργία μπορεί να φαίνεται ακίνδυνη, μπορεί να έχει πρόσθετα αρνητικά αποτελέσματα. Για παράδειγμα, μπορεί να επιβραδύνει αισθητά την απόκριση

[24] «Η λέξη botnet προέρχεται από τις λέξεις robot και network. Το botnet είναι ένα δίκτυο υπολογιστών, το οποίο έχουν μολύνει οι hackers με κακόβουλο λογισμικό. Στόχος τους είναι η εκτέλεση εργασιών (στο διαδίκτυο) χωρίς την άδεια και τη γνώση των θυμάτων. Όταν ένα bot επιτίθεται σε έναν υπολογιστή, ο χειριστής του μπορεί να πάρει τον έλεγχο της συσκευής καθώς και των υπόλοιπων συσκευών που βρίσκονται στο botnet. Τα botnets είναι πολύ δημοφιλή μεταξύ των hackers γιατί μπορούν να χρησιμοποιηθούν για πολλές απάτες. Μπορούν να χρησιμοποιηθούν για τη διανομή spam emails, για την εξάπλωση ιών, για την κλοπή δεδομένων, για επιθέσεις σε υπολογιστές και servers και άλλα.» Ορισμός διαθέσιμος στην ιστοσελίδα https://www.secnews.gr/189228/botnet-prostasia-epitheseis/ Ανάκτηση 29.06.2023.

[25] ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΣΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ Σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού. COM(2006) 688 τελικό, σελ.3.

του συστήματος του η/υ του θύματος. Επιπλέον, έχει τη δυνατότητα να ανακατευθύνει το πρόγραμμα περιήγησης του θύματος σε αναξιόπιστους ιστότοπους, οι οποίοι ενδέχεται να περιέχουν άλλους ιούς που προκαλούν περαιτέρω προβλήματα. Ωστόσο, είναι σημαντικό να σημειωθεί ότι δεν είναι όλα αυτά τα προγράμματα κακόβουλα. Επομένως, είναι σημαντικό για κάθε σύστημα να διαθέτει κάποια μορφή προστασίας που σαρώνει τακτικά για αυτά τα προγράμματα.[26]

Ένα ακόμη επικίνδυνο είδος κακόβουλου λογισμικού, γνωστό ως Fileless Malware, ήτοι κακόβουλο πρόγραμμα χωρίς αρχεία, διαφέρει εντελώς στη λειτουργία με τα προηγουμένως αναφερόμενα κακόβουλα λογισμικά, καθώς χρησιμοποιεί αξιόπιστο/έμπιστο λογισμικό για να μολύνει ένα υπολογιστικό σύστημα, ενώ δεν αφήνει ίχνη σε αρχεία, γεγονός που καθιστά εξαιρετικά δύσκολο τον εντοπισμό του. Αντί να αποκτά πρόσβαση στον σκληρό δίσκο, αυτό το κακόβουλο λογισμικό δεν επηρεάζει τα αρχεία του η/υ αλλά χρησιμοποιεί απευθείας τη μνήμη του υπολογιστικού συστήματος. Επιπλέον, κατά την επανεκκίνηση του συστήματος το λογισμικό αυτό εξαφανίζεται εντελώς.

Ένα άλλο είδος κακόβουλου λογισμικού, γνωστό με τον όρο "Λογική βόμβα" (Logic bomb), αναφέρεται σε ένα είδος κακόβουλου προγράμματος που μπορεί να εγκατασταθεί και να παραμείνει αδρανές στη μνήμη μιας συσκευής έως ότου μια συγκεκριμένη ώρα ή ενέργεια χρήστη να το ενεργοποιήσει. Μόλις ενεργοποιηθεί, η «βόμβα λογικής» απελευθερώνει έναν ιό που μπορεί να διαγράψει αρχεία, να προκαλέσει βλάβη στο σύστημα ή ακόμα και να οδηγήσει σε πλήρη κατάρρευσή του.[27]

Ο τελευταίος τύπος κακόβουλων λογισμικών, και ο πιο επικίνδυνος, είναι το Blended Malware το οποίο συνδυάζει διάφορες τεχνολογίες από όλους τους προηγούμενους τύπους κακόβολου λογισμικού. Αυτά τα εξελιγμένα λογισμικά δημιουργούνται από επαγγελματίες υψηλής εξειδίκευσης και είναι δύσκολο να αναλυθούν και να σαρωθούν για προστασία. Ενδέχεται να ενσωματώνουν ένα μείγμα κακόβουλου κώδικα, ιών, τύπου worm, adware και cryptominers.

---

[26] *Βλαχόπουλος,* ό.π. σελ. 53.

[27] *Ομοίως*, σελ. 53.

Τελικά, απειλές όπως spam, spyware και malware διαβρώνουν την εμπιστοσύνη και την ασφάλεια της κοινωνίας της πληροφορίας, με σημαντικές οικονομικές συνέπειες παγκοσμίως. Ενώ ορισμένα κράτη μέλη έχουν αναλάβει πρωτοβουλίες, υπάρχει έλλειψη συνολικών προσπαθειών σε επίπεδο ΕΕ για την αντιμετώπιση αυτής της συνεχιζόμενης εξέλιξης. Είναι, συνεπώς, επιτακτική η ανάγκη να ενταθούν τα μέτρα επιβολής προκειμένου να συλληφθούν όσοι σκόπιμα παραβιάζουν το νόμο. Ο κλάδος πρέπει επίσης να λάβει πρόσθετα μέτρα, εκτός από τις προσπάθειες επιβολής του νόμου. Είναι ζωτικής σημασίας να προωθηθεί η συνεργασία σε εθνική κλίμακα, τόσο εντός όσο και μεταξύ των κυβερνήσεων και του κλάδου.

Είναι ανάγκη επίσης να αναληφθούν ερευνητικές πρωτοβουλίες για την ενίσχυση της προστασίας της ιδιωτικής ζωής και της ασφάλειας στις ηλεκτρονικές επικοινωνίες. Με την ολοκληρωμένη εφαρμογή των προσδιοριζόμενων δράσεων, είναι δυνατός ο μετριασμός των απειλών που υπονομεύουν επί του παρόντος τα πλεονεκτήματα της κοινωνίας της πληροφορίας και της οικονομίας.

Στην επόμενη ενότητα, εξετάζεται αναλυτικά το νομοθετικό πλαίσιο για το εν γένει ηλεκτρονικό έγκλημα-«κυβερνοέγκλημα» καθώς επίσης και οι ειδικότερες διατάξεις που έχουν εφαρμογή στην εν θέματι περίπτωση του κακόβουλου λογισμικού, σε διεθνές/ενωσιακό αλλά και σε εθνικό επίπεδο, αναδεικνύοντας έτσι αφενός την πρόοδο που έχει γίνει νομοθετικά τα τελευταία χρόνια σε μια προσπάθεια καταπολέμησης και καταστολής του φαινομένου, αλλά αφετέρου εξετάζονται και οι ελλείψεις και οι δυσχέρειες που προκύπτουν από τα κενά στις νομοθεσίες και την εφαρμογή τους από τα κράτη και δη την Ελλάδα.

3 Το νομοθετικό πλαίσιο

3.1 Η διεθνής και ενωσιακή ρύθμιση

3.1.1 Η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα και λοιπά νομοθετήματα

Σε αυτό το σημείο, κρίνεται σκόπιμο να παρουσιαστεί ένα ολοκληρωμένο νομοθετικό πλαίσιο (τόσο εγχώριας όσο και υπερεθνικής νομοθεσίας, συμπεριλαμβανομένων των ευρωπαϊκών νόμων και οδηγιών) που αφορά την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Όσον αφορά στην ποινική αντιμετώπιση του «ηλεκτρονικού εγκλήματος» εντός του ελληνικού νομικού πλαισίου, διακρίνεται η ύπαρξη διάσπαρτων διατάξεων εντός του Ποινικού Κώδικα και άλλων ειδικών νόμων, όπως θα αναλυθεί παρακάτω. Ωστόσο, δεν θα μπορούσε να υποστηριχθεί ότι η Ελλάδα συμβαδίζει και συμμορφώνεται με τα διεθνή δεδομένα και τις απαιτήσεις.[28]

Η πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος εντός του ευρωπαϊκού χώρου αναλήφθηκε από το Συμβούλιο της Ευρώπης στο Στρασβούργο, κατά το έτος 1976, στο πλαίσιο του Συνεδρίου για τις Εγκληματολογικές πλευρές του Οικονομικού Εγκλήματος. Ωστόσο, καθοριστική για την επακόλουθη πρόοδο ήταν η αποφασιστική δράση που έλαβε το Συμβούλιο της Ευρώπης αναφορικά με τη νομοθεσία για το έγκλημα στον κυβερνοχώρο το 1996, όπου εκδόθηκαν δύο συστάσεις: (α) Σύσταση αριθ. R(89) για την αντιμετώπιση του εγκλήματος που διαπράττεται με τη χρήση η/υ και (β) Σύσταση No R(95) για την αντιμετώπιση ποινικών δικονομικών προβλημάτων που σχετίζονται με την τεχνολογία των η/υ. Αυτές οι συστάσεις έθεσαν τις βάσεις για τη θέσπιση της Σύμβασης του 2001 για τον Κυβερνοχώρο.[29]

Σε διεθνές επίπεδο, οι εργασίες για τη δημιουργία μιας Σύμβασης για τον Κυβερνοχώρο (Convention on Cybercrime) ξεκίνησαν το 1997, με τη σύσταση

[28] *Καργόπουλος, Α.* (2018). Πρωτοδίκης, Εθνικός Εμπειρογνώμονας στον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ε.Ε., Κυβερνοέγκλημα: Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου. Έρευνα διαθέσιμη στο <https://www.esdi.gr › epimorfosi › kargopoulos> στα πλαίσια της εκπαίδευσης των Δικαστικών και Εισαγγελικών Λειτουργών στην Εθνική Σχολή Δικαστών.

[29] *Βλαχόπουλος Κ.,* Ηλεκτρονικό Έγκλημα. Μορφές, Πρόληψη, Αντιμετώπιση, Νομική Βιβλιοθήκη, Εκδ. 2007, σελ. 135 επ.

Επιτροπής αποτελούμενης από ειδικούς στον τομέα του ηλεκτρονικού εγκλήματος. Η επιτροπή ήταν επιφορτισμένη με τον έλεγχο των νομοθετικών ζητημάτων που προκύπτουν από τις αυξανόμενες και διαρκώς διευρυνόμενες εγκληματικές δραστηριότητες στον κυβερνοχώρο. Παρόλο που η επιτροπή είχε αρχικά στόχο να ολοκληρώσει τις εργασίες της έως το 1999, οι περίπλοκες δυσκολίες που αντιμετώπιζαν τα μέλη της επέβαλαν νέα προθεσμία το έτος 2000.

Το τελικό κείμενο της «Σύμβασης για το Έγκλημα στον Κυβερνοχώρο», υπογράφηκε στη Βουδαπέστη στις 23 Νοεμβρίου 2001[30], από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου και από τις Ηνωμένες Πολιτείες, τον Καναδά, την Νότιο Αφρική και την Ιαπωνία. Τέθηκε, δε, σε ισχύ την 1η Ιουλίου 2004, ενώ από τη χώρα μας υπογράφηκε και κυρώθηκε 15 περίπου έτη αργότερα, με τον πρόσφατο Ν. 4411/2016, παράλληλα με τη μεταφορά στην ελληνική έννομη τάξη και της Οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, η οποία είχε υπογραφεί ήδη από την 23η Νοεμβρίου 2001.

Η Σύμβαση της Βουδαπέστης είναι γραμμένη σε ουδέτερη γλώσσα και ορολογία και γίνεται προσπάθεια να συμπεριλάβει και τις μελλοντικές τεχνολογίες, δεδομένης και της συνεχούς εξέλιξης του κυβερνοεγκλήματος. Σκοπός της είναι δε και η εναρμόνιση των νομοθεσιών των συμμετεχόντων κρατών, ο 'εμπλουτισμός των δικονομικών διατάξεων με νέες μεθόδους και η ισχυροποίηση των διακρατικών συνεργασιών, η προώθηση της δικαστικής συνδρομής και η εγκαθίδρυση ενός δικτύου, το οποίο θα λειτουργεί σε εικοσιτετράωρη βάση'.[31]

Ειδικότερα, στο κείμενο της Σύμβασης του Συμβουλίου της Ευρώπης για τα εγκλήματα του κυβερνοχώρου, περιλαμβάνονται σημαντικές διατάξεις όπου προβλέπονται ιδιαίτερα εγκλήματα. Στα άρθρα 2-6 γίνεται αναφορά σε αδικήματα κατά της ασφάλειας, της ακεραιότητας και της λειτουργίας των ψηφιακών δεδομένων και των πληροφοριακών συστημάτων, όπως: (α) η παράνομη πρόσβαση σε δεδομένα (άρθρο 2), (β) η υποκλοπή διαβιβαζόμενων

[30] *Walden I.*, Harmosing Computer Crime Laws in Europe, European Journal of Crime, Criminal Law and Criminal Justice, Vol 12 (2004), σελ. 321-336: 324.

[31] *Καργόπουλος, Α*. (2018), ό.π.

δεδομένων (άρθρο 3), (γ) η παρέμβαση (διαγραφή-αλλοίωση-βλάβη) σε δεδομένα (άρθρο 4), (δ) η παρέμβαση σε συστήματα υπολογιστών (άρθρο 5), (ε) η κακή χρήση συσκευών με σκοπό την τέλεση εγκλημάτων όπως τα προηγούμενα (άρθρο 6). Στα άρθρα 7-10 απαριθμούνται αδικήματα, τα οποία τελούνται με την χρήση υπολογιστών, όπως (στ) η πλαστογραφία που σχετίζεται με Η/Υ (άρθρο 7), (ζ) η απάτη που σχετίζεται με Η/Υ (άρθρο 8), (η) η πορνογραφία ανηλίκων και συναφή εγκλήματα (άρθρο 9), (θ) παραβάσεις σχετικές με την πνευματική ιδιοκτησία (άρθρο 10).

Το κυρίως κείμενο της Σύμβασης συνοδεύεται και από μια Επεξηγηματική Αναφορά (Explanatory Report)[32], στην οποία παρέχονται συμπληρωματικές πληροφορίες για κάθε άρθρο, καθώς και αιτιολόγηση των επιλογών των συντακτών της Σύμβασης για τις συγκεκριμένες διατάξεις που περιλήφθηκαν. Τέλος, στη Σύμβαση συμπληρώθηκε το 2002 ένα Πρόσθετο Πρωτόκολλο, σχετικά με την Ποινικοποίηση Πράξεων Ρατσισμού και Ξενοφοβίας που διαπράττονται μέσω ηλεκτρονικού υπολογιστή, οι οποίες δεν είχαν περιληφθεί στο τελικό κείμενο της αρχικής Σύμβασης, λόγω του ότι πρόκειται για ένα σύνθετο και πολύπλοκο ζήτημα.

Στο Πρόσθετο Πρωτόκολλο γίνεται προτροπή σε όσους το υπογράψουν και το θέσουν σε ισχύ, να υιοθετήσουν σχετικά νομοθετικά μέτρα που να ποινικοποιούν α) τη διάδοση ρατσιστικού και ξενοφοβικού υλικού, με τη χρήση ηλεκτρονικών υπολογιστών, β) τη διάδοση ρατσιστικών και ξενοφοβικών απειλών ή υβριστικών συνθημάτων, μέσω τέτοιων συστημάτων και γ) τη χρησιμοποίηση τέτοιων συστημάτων, για τη διάδοση υλικού, το οποίο αρνείται, ελαχιστοποιεί, εγκρίνει ή δικαιολογεί πράξεις γενοκτονίας ή εγκλημάτων ενάντια στην ανθρωπότητα, όπως αυτά ορίζονται από τη διεθνή νομοθεσία.

Περαιτέρω, ακόμα ένα σημαντικό κείμενο στη νομοθεσία σχετικά με το κυβερνοέγκλημα εν γένει είναι και η Απόφαση-Πλαίσιο 2005/222/ΔΕΥ «για τις

[32] Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185. Κείμενο διαθέσιμο στην ιστοσελίδα: <https://rm.coe.int/16800cce5b> Ανάκτηση 30.06.2023.

επιθέσεις κατά συστημάτων πληροφοριών»,[33] όπου γίνεται με προσπάθεια προσέγγισης των εθνικών νομοθεσιών, με σκοπό την αντιμετώπιση των μείζονος βαρύτητας φαινομένων, χωρίς να εμποδίζεται η προστασία των προσωπικών δεδομένων. Εν προκειμένω, η Απόφαση-Πλαίσιο περιλαμβάνει διάφορους ορισμούς («σύστημα πληροφοριών», «ηλεκτρονικά δεδομένα» κ.λπ.) και διατάξεις σχετικά με αδικήματα που σχετίζονται με μη εξουσιοδοτημένη πρόσβαση σε σύστημα πληροφοριών (άρθρο 2), αλλοίωση δεδομένων και παράνομη παρεμβολή σε σύστημα και σε δεδομένα (άρθρο 4). Αντιμετωπίζει επίσης θέματα ηθικής αυτουργίας, τη συνέργεια και τη απόπειρα, για τις κυρώσεις, τις επιβαρυντικές περιστάσεις, την ευθύνη και τις κυρώσεις κατά νομικών προσώπων, τη δικαιοδοσία κ.λπ.

Ιδιαίτερα σημαντική είναι και η Απόφαση-Πλαίσιο 2001/413/ΔΕΥ «για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών», η οποία εστιάζει στην καταπολέμηση της απάτης και της πλαστογραφίας σχετικά με τα μέσα πληρωμής χωρίς μετρητά (ιδίως πιστωτικών καρτών, ταξιδιωτικών επιταγών, συναλλαγματικών κ.λπ.), με στόχο τη διασφάλιση της ασφάλειας των συναλλαγών έναντι διεθνών δόλιων δραστηριοτήτων. Προβλέπονται ακόμη αδικήματα σχετιζόμενα με ηλεκτρονικούς υπολογιστές (εισαγωγή, αλλοίωση, διαγραφή, εξάλειψη δεδομένων, παρέμβαση σε Η/Υ κ.λπ.). Αυτά τα εγκλήματα αναφέρονται συνήθως με διεθνώς αναγνωρισμένους όρους όπως " cracking", ήτοι αλλαγή κωδίκων πρόσβασης και αθέμιτη παράκαμψη των μέτρων ασφαλείας ώστε να καθίσταται δυνατή η διείσδυση τρίτων σε πληροφοριακά συστήματα επιχειρήσεων ή οργανισμών και η παράνομη αντιγραφή τους με σκοπό το οικονομικό όφελος, "hacking", ήτοι παράνομη πρόσβαση ή παρέμβαση σε σύστημα πληροφοριών χωρίς την επιδίωξη οικονομικού οφέλους αλλά για μόνη την ικανοποίηση της παράκαμψης των συστημάτων ασφαλείας (άρθρα 2, 3 της Σύμβασης, άρθρο 2 της Α-Π 2005/222/ΔΕΥ), "ID theft", ήτοι κλοπή ταυτότητας, στην οποία εντάσσεται το μείζον μέρος των περιπτώσεων ηλεκτρονικής απάτης, μέσω της οποίας υφαρπάσσονται τα στοιχεία που επιτρέπουν στο δράστη να ενεργεί συναλλαγές

[33] *Ζημιανίτης Δ.,* Δίκαιο στην Ψηφιακή Εποχή της Ένωσης Ελλήνων Νομικών e-Θέμις, εκδ. Νομική Βιβλιοθήκη 2012, σελ. 164 επ.

επ' ονόματι του θύματος και εν αγνοία εκείνου," phishing", γνωστό ως «ψάρεμα», ήτοι μορφή απάτης, όπου το θύμα παραπλανάται να γνωστοποιεί στοιχεία της πιστωτικής κάρτας ή του λογαριασμού του στο δράστη και τέλος, " pharming", γνωστό ως «καλλιέργεια», που αποτελεί πιο εξελιγμένη μορφή phising, στην οποία γίνεται με απατηλά μέσα, χωρίς επίδραση στη βούληση του θύματος αλλά με επηρεασμό του προγράμματος του Η/Υ, αναδρομολόγηση των δεδομένων του θύματος σε άλλη ιστοσελίδα από εκείνη που επεδίωκε να επισκεφθεί ο παθών, κ.λπ.[34]

Επιπλέον, άξια αναφοράς είναι και η Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών σχετικά με την καταπολέμηση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (spam), του κατασκοπευτικού λογισμικού (spyware) και του κακόβουλου λογισμικού (malware)[35] είναι επίσης σημαντική, καθώς αφορά τη στρατηγική της ασφαλούς κοινωνίας της πληροφορίας[36]η οποία αποσκοπεί στη βελτίωση της ασφάλειας των εν γένει δικτύων και πληροφοριών, ενώ ταυτόχρονα προτρέπει τον ιδιωτικό τομέα να αντιμετωπίσει τις αδυναμίες των δικτύων και των συστημάτων πληροφοριών οι οποίες δύνανται να αποτελέσουν στόχο των δραστών των παραπάνω ηλεκτρονικών εγκλημάτων.

Αξιοσημείωτη είναι και η ανακοίνωση της Επιτροπής σχετικά με την ανασκόπηση του κοινοτικού πλαισίου κανονιστικών ρυθμίσεων, [37] σχετικά με την εισαγωγή νέων κανόνων για την ενίσχυση της ασφάλειας και της προστασίας της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Στην εν λόγω ανακοίνωση γίνεται αναφορά στην εξέλιξη των ανεπίκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα (spam) καθώς και του κατασκοπευτικού και του κακόβουλου λογισμικού.[38] Στο κείμενό της εμπεριέχονται οι προσπάθειες που

---

[34] Βλ. σχετικά *Ζάννης Α.,* Το διαδικτυακό έγκλημα, εκδ. Α. Σάκκουλα 2005, σελ. 63, *Αργυρόπουλος Α*., Ηλεκτρονική εγκληματικότητα, εκδ. Α. Σάκκουλα 2001, σελ. 137-138. –*Walden,* ο.π., σελ. 334, *Παναεοφύτου Α.*, Ποινικό Δίκαιο, Κράτος και Τεχνολογικοί Κίνδυνοι, εκδ. Α. Σάκκουλα 1997, σελ. 279 επ.

[35] COM (2006) 688, τελικό.

[36] COM (2006) 251, τελικό

[37] COM (2006) 334, τελικό.

[38] COM (2004) 28, τελικό.

είχαν πραγματοποιηθεί μέχρι εκείνη τη χρονική στιγμή για την αντιμετώπιση των ανωτέρω απειλών, ενώ προσδιόριζε και τις περαιτέρω μελλοντικές δράσεις, μεταξύ των οποίων είχε προταθεί η ενίσχυση της κοινοτικής νομοθεσίας, η επιβολή του νόμου, η συνεργασία στο εσωτερικό των κρατών μελών καθώς και μεταξύ τους, ο πολιτικός και οικονομικός διάλογος με τρίτες χώρες, πρωτοβουλίες του κλάδου και οι δραστηριότητες Ε&Α.

Τέλος, σε ευρωπαϊκό επίπεδο υπάρχουν αρκετές οδηγίες, οι οποίες στοχεύουν στην αντιμετώπιση ειδικών μορφών κυβερνοεγκλήματος, όπως η Οδηγία 2011/93/ΕΕ για την παιδική πορνογραφία, η Οδηγία 2017/541 για την καταπολέμηση της τρομοκρατίας και η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά πληροφοριακών συστημάτων, η οποία θα εξεταστεί αυτοτελώς παρακάτω.

3.1.2 Η Οδηγία 2013/40/ΕΕ

Η Οδηγία 2013/40/ΕΕ[39] για τις επιθέσεις κατά πληροφοριακών συστημάτων, αναφέρει στο προοίμιό της ότι η σύμβαση αυτή λειτουργεί ως νομικό πλαίσιο για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών.

Συγκεκριμένα, οι στόχοι της παρούσας οδηγίας, όπως εκτίθενται στο προοίμιο αρ.1 της Οδηγίας, είναι «η προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων, και η βελτίωση της συνεργασίας μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, καθώς και των αρμόδιων ειδικευμένων οργανισμών της Ένωσης και φορέων της Ένωσης, όπως η Eurojust, η Ευρωπόλ και το Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος, καθώς και ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).»

[39] ΟΔΗΓΙΑ 2013/40/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, L 218/8 EL 14.8.2013.

Αναφορικά, δε, με τις επιθέσεις κατά των συστημάτων πληροφοριών, η οδηγία διευκρινίζει στο προοίμιο (αρ.6) ότι «επιθέσεις στον κυβερνοχώρο μεγάλης κλίμακας μπορούν να προξενήσουν σημαντικές οικονομικές ζημίες, τόσο μέσω της διακοπής της λειτουργίας των συστημάτων πληροφοριών και των επικοινωνιών όσο και μέσω της απώλειας ή αλλοίωσης σημαντικών εμπορικών εμπιστευτικών πληροφοριών ή άλλων δεδομένων. Θα πρέπει να αποδίδεται ιδιαίτερη προσοχή στην αύξηση της ευαισθητοποίησης των καινοτόμων μικρών και μεσαίων επιχειρήσεων για απειλές σχετικές με αυτές τις επιθέσεις και για την ευπάθειά τους σε αυτές τις επιθέσεις, επειδή εξαρτώνται, σε μεγάλο βαθμό, από την ορθή λειτουργία και τη διαθεσιμότητα πληροφοριακών συστημάτων και συχνά έχουν περιορισμένους πόρους για την ασφάλεια των πληροφοριών», τονίζοντας έτσι τη σημασία του να υπάρχουν κοινοί ορισμοί και κοινή προσέγγιση στον τομέα αυτό ώστε να διασφαλισθεί η ενιαία εφαρμογή της οδηγίας στο εσωτερικό των κρατών μελών.

Γίνεται αντιληπτό ότι η εν λόγω οδηγία εστιάζει στη διατήρηση της ακεραιότητας και της διαθεσιμότητας των συστημάτων πληροφοριών και των δεδομένων τους, τα οποία κινδυνεύουν από κακόβουλα προγράμματα και ιούς. Η οδηγία βασίζεται εν μέρει στη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο του 2001, η οποία αποτελεί πρότυπο για την εθνική και περιφερειακή νομοθεσία και προωθεί τη συνεργασία εντός και εκτός της Ευρωπαϊκής Ένωσης. Εναρμονίζεται με τη Σύμβαση όσον αφορά την ποινικοποίηση των ίδιων αξιόποινων συμπεριφορών που στρέφονται κατά συστήματα πληροφοριών (αντί των συστημάτων η/υ) και των ηλεκτρονικών δεδομένων. Ωστόσο, η οδηγία ξεχωρίζει για τον δεσμευτικό της χαρακτήρα, σε αντίθεση με τη Σύμβαση, αφού τα κράτη μέλη είναι υποχρεωμένα να υιοθετήσουν την Οδηγία και να την μεταφέρουν στην εσωτερική τους έννομη τάξη.[40]

Η Οδηγία 2013/40/ΕΕ δημιουργήθηκε για να αντικαταστήσει την Απόφαση-Πλαίσιο 2005/222/ΔΕΥ, καθώς η τελευταία κρίθηκε ανεπαρκής για την

[40] Κατά το άρθρο 288 παρ. 3 ΣΛΕΕ «*Η οδηγία δεσμεύει κάθε κράτος μέλος στο οποίο απευθύνεται, όσον αφορά το επιδιωκόμενο αποτέλεσμα, αλλά αφήνει την επιλογή του τύπου και των μέσων στην αρμοδιότητα των εθνικών αρχών. Η απόφαση είναι δεσμευτική ως προς όλα τα μέρη της. Όταν ορίζει αποδέκτες, είναι δεσμευτική μόνο για αυτούς*». Βλ. και *Καϊάφα-Γκμπάντι, Μ.,* Στοιχεία Ενωσιακού Ποινικού Δικαίου και της ενσωμάτωσής του στην ελληνική έννομη τάξη, εκδ. Σάκκουλας, Αθήνα – Θεσσαλονίκη 2016, σελ. 232 επ.

αντιμετώπιση νέων μορφών επιθέσεων κατά των συστημάτων πληροφοριών και των δεδομένων αυτών εντός της ΕΕ, όπως είναι οι μαζικές επιθέσεις με τη μέθοδο "Botnet".[41] Επιπλέον, η οδηγία αποσκοπεί στην καταπολέμηση του οργανωμένου εγκλήματος, όπως διαφαίνεται από το προοίμιο αυτής, όταν οι επιθέσεις στον κυβερνοχώρο συμβαίνουν σε μεγάλη κλίμακα ή πλήττουν σημαντικό αριθμό συστημάτων πληροφοριών, ή όταν προκαλούνται σοβαρές ζημίες, και δη όταν στρέφονται κατά υποδομής ζωτικής σημασίας των κρατών-μελών ή της Ένωσης.

Εν προκειμένω, η Οδηγία αντιμετωπίζει διάφορες παράνομες δραστηριότητες όπως η παράνομη πρόσβαση (άρθρο. 3), η παράνομη παρεμβολή σε σύστημα (άρθρο 4) και σε εργαλεία, που χρησιμοποιούνται για την διάπραξη τέτοιου είδους αδικημάτων, η παράνομη παρεμβολή σε δεδομένα (άρθρο 5), και η παράνομη υποκλοπή (άρθρο 6). Επιπλέον, στο πλαίσιο καλύτερης καταπολέμησης του εγκλήματος στον κυβερνοχώρο, η Οδηγία τονίζει την ανάγκη περισσότερης διεθνούς συνεργασίας μεταξύ των δικαστικών αρχών και των αρχών επιβολής του νόμου.[42]

Ειδικότερα, όσον αφορά στο αδίκημα της παράνομης παρεμβολής σε σύστημα και σε δεδομένα η/υ (άρθρα 4 και 5 της Οδηγίας), που ενδιαφέρουν την παρούσα διπλωματική, σημειώνεται ότι σύμφωνα με το άρθρο 4 της Οδηγίας «*Τα κράτη*

---

[41] Βλ. σκέψη 5 του προοιμίου της Οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά των συστημάτων πληροφοριών, με ρητή αναφορά στη νέα μορφή μαζικών επιθέσεων με μολυσμένους η/υ (μέθοδος "Botnet"). Συγκεκριμένα, ο ευρωπαίος νομοθέτης τόνισε ότι «υπάρχουν στοιχεία που δείχνουν μια τάση διάπραξης όλο και πιο επικίνδυνων και επαναλαμβανόμενων επιθέσεων μεγάλης κλίμακας κατά συστημάτων πληροφοριών που συχνά μπορούν να έχουν ζωτική σημασία για τα κράτη μέλη ή για ειδικές δραστηριότητες του δημόσιου ή του ιδιωτικού τομέα. Η τάση αυτή συνοδεύεται από την ανάπτυξη όλο και πιο εξελιγμένων μεθόδων, όπως η δημιουργία και η χρήση των αποκαλούμενων «botnet» (δίκτυα προγραμμάτων ρομπότ), η οποία περιλαμβάνει διάφορα στάδια της αξιόποινης πράξης, καθένα από τα οποία μπορεί από μόνο του να θέσει σε σοβαρό κίνδυνο το δημόσιο συμφέρον. Η παρούσα οδηγία σκοπεύει, μεταξύ άλλων, στην εισαγωγή ποινικών κυρώσεων για τη δημιουργία των «botnet», ήτοι 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, όπως αναφέρεται στην παρούσα οδηγία. Τα κράτη μέλη θα πρέπει να μπορούν να ορίσουν τι συνιστά σοβαρή ζημιά σύμφωνα με το εθνικό τους δίκαιο και τις εθνικές τους πρακτικές, όπως διακοπή της λειτουργίας συστημάτων μεγάλης δημόσιας σημασίας ή σημαντική οικονομική ζημιά ή απώλεια δεδομένων προσωπικού χαρακτήρα ή ευαίσθητων πληροφοριών.».

[42] *Lawspot gr* (2018). Η προστασία του απορρήτου των επικοινωνιών: Ενημερωτικό υλικό από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών Με αφορμή τον Ευρωπαϊκό Μήνα για την Ασφάλεια στον Κυβερνοχώρο. Διαθέσιμο στο https://www.l awspot.gr/nomika nea/i prostasia toy aporritoy ton epikoinonion enimerotiko yliko apo tin arhi diasfalisis toy Ανάκτηση 30.06.2023.

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». Κατά τη διάταξη, δε, του άρθρου 5 «*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».*

Οι προαναφερθείσες διατάξεις τυποποιούν ως ποινικά αδικήματα κάθε ενέργεια που παραποιεί δεδομένα, δυνητικά θέτοντας σε κίνδυνο την ακεραιότητά τους. Αναφορικά, δε, με τα συστήματα, για να θεωρηθούν εγκληματική πράξη τέτοιες ενέργειες, πρέπει να παρεμποδίζουν ή να διακόπτουν σημαντικά τη λειτουργία του συστήματος. Ο βασικός σκοπός αυτών των διατάξεων, παρόμοιοι με αυτούς που περιγράφονται στη Σύμβαση για το έγκλημα στον κυβερνοχώρο, είναι η διασφάλιση των εννόμων αγαθών της ακεραιότητας και της προσβασιμότητας των συστημάτων πληροφοριών και των δεδομένων τους. Αυτά τα συστήματα και τα δεδομένα αντιμετωπίζουν απειλές από διάφορες επιβλαβείς συμπεριφορές, όπως η μόλυνση μέσω κακόβουλων προγραμμάτων («ιών» κλπ.).

Σε αντίθεση με τη Σύμβαση, η Οδηγία διακρίνεται ποινικοποιώντας την παράνομη παρεμβολή στο σύστημα και τα δεδομένα, αλλά μόνο σε περιπτώσεις που δεν κρίνονται «ήσσονος σημασίας περιπτώσεις». Αυτή η διάκριση απουσιάζει στη Σύμβαση. Ωστόσο, η σύμβαση προβλέπει επίσης ότι οι κυρώσεις επιβάλλονται μόνο όταν προκληθεί «σοβαρή ζημιά». Επομένως, βασικά, και τα δύο νομοθετικά κείμενα προσπαθούν να μετριάσουν την τιμωρία με συγκρίσιμο τρόπο. Εντούτοις, προβλέπεται και στη Σύμβαση ότι το αξιόποινο στοιχειοθετείται όταν έχει προκληθεί «σοβαρή βλάβη». Έτσι, δεν πρόκειται για

κάποια ουσιαστική διαφοροποίηση, καθώς και στα δύο νομοθετικά κείμενα επιχειρείται με παρόμοιο τρόπο ο περιορισμός του αξιοποίνου.[43]

Αξιοσημείωτο είναι και το άρθρο 8 παρ. 1 της Οδηγίας, σχετικά με την ηθική αυτουργία, την υποβοήθηση και την συνέργεια, κατά το οποίο *«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»,* ενώ κατά την παρ. 2 σχετικά με την απόπειρα θεσπίζεται ότι *«Τα κράτη μέλη εξασφαλίζουν ότι η απόπειρα διάπραξης αδικήματος που αναφέρεται στα άρθρα 4 και 5 να τιμωρείται ως ποινικό αδίκημα*».

Αρχικά, όσον αφορά στις διάφορες μορφές συμμετοχής σε εγκληματικές δραστηριότητες, η Οδηγία προβλέπει την τιμώρηση τους, χωρίς να αφήνει εξαιρέσεις για αδικήματα που προσβάλουν τα συστήματα πληροφοριών, προβλέποντας δηλαδή την τιμώρηση για όλα τα σχετικά αδικήματα. Κατά συνέπεια, τα κράτη μέλη της Ε.Ε. υποχρεούνται να χαρακτηρίσουν ως αξιόποινη πράξη ακόμη και την απλή συνεργασία στο προαναφερθέν αδίκημα που περιγράφεται στο άρθρο 8 παράγραφος 1, ήτοι τις προπαρασκευαστικές πράξεις παραγωγής, διανομής, πώλησης και άλλες συναφείς δραστηριότητες που λειτουργούν ως εργαλεία για την πραγματοποίηση επιθέσεων σε συστήματα πληροφοριών,[44] όπως και στην αντίστοιχη διάταξη που περιγράφεται στη Σύμβαση. Ωστόσο, αναφορικά με την απόπειρα, η Οδηγία προβλέπει την τιμώρηση μόνο για τα αδικήματα που περιγράφονται στα άρθρα 4 και 5, τα οποία σχετίζονται με την παράνομη παρέμβαση σε συστήματα πληροφοριών και ηλεκτρονικά δεδομένα.

Κατά συνέπεια, περιορίζεται σημαντικά με αυτό το τρόπο το υποχρεωτικό αξιόποινο της απόπειρας των εν λόγω αδικημάτων, καθώς δεν περιλαμβάνει τις λοιπές μορφές επιθέσεων, δηλαδή την παράνομη πρόσβαση σε πληροφοριακό σύστημα (άρθρο 3), τις πράξεις της υποκλοπής (άρθρο 6)[45], αλλά και τις

---

[43] *Καϊάφα-Γκμπάντι, Μ.*, 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. 489-500, κυρίως σελ. 493.

[44] *Καϊάφα-Γκμπάντι, Μ.,* (2016), ό.π., σελ. 240 επ.

[45] Εντούτοις, στη Σύμβαση για το Κυβερνοέγκλημα προβλέπεται η προτροπή προς τα κράτη μέλη να τιμωρούν ορισμένες μορφές υποκλοπής.

προπαρασκευαστικές πράξεις παραγωγής, διανομής, πώλησης κλπ. εργαλείων που χρησιμοποιούνται για τη διεξαγωγή επιθέσεων σε συστήματα πληροφοριών (άρθρο 7). Τούτο, δε, έχει σχολιασθεί εντόνως από την ελληνική θεωρία,[46] θεωρώντας την περιστολή αυτή του αξιοποίνου ως μια προσπάθεια περιορισμού της αυστηρότητας της τιμωρίας, σε αντίθεση με τη συνολική αντίληψη του εκτεταμένου φάσματος κυρώσεων που περιγράφεται στην προαναφερθείσα Οδηγία, όπως είχε προηγουμένως σημειωθεί σε σχέση με την περίπτωση της απόπειρας.

[46] *Καϊάφα-Γκμπάντι, Μ*. (2016), ό.π., σελ. 240 επ.

3.2 Το ισχύον Ελληνικό Νομοθετικό Πλαίσιο

3.2.1 Η διάταξη του άρθρου 19 του Συντάγματος

Σε συνταγματικό επίπεδο, συγκεκριμένα στο άρθρο 19, θεσπίζεται το θεμελιώδες δικαίωμα του ατόμου στο απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο το οποίο είναι απόλυτα απαραβίαστο. Εξαίρεση στο παραπάνω απαραβίαστο του θεμελιώδους αυτού ατομικού δικαιώματος μπορεί να θεσπιστεί για τη δικαστική αρχή και μόνο εφόσον υπάρχει ειδικός νόμος, όπου ορίζονται οι εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο, ήτοι για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Συνεπώς, από τα ανωτέρω προκύπτει ότι μόνο το δικαστικό σώμα διατηρεί την ελευθερία να παραβιάζει τα όρια της εμπιστευτικότητας, είτε πρόκειται για τη διασφάλιση της εθνικής ασφάλειας είτε για την εμβάθυνση στη σφαίρα των εξαιρετικά σοβαρών εγκλημάτων, αλλά και αυτό με την επιφύλαξη αυστηρών παραμέτρων που σκιαγραφούνται σε περιεχόμενο νόμου.

Το θέμα της άρσης του απορρήτου σύμφωνα με τις διατάξεις των Εισαγγελικών και Δικαστικών Αρχών αντιμετωπίστηκε κατά κύριο λόγο στον εκτελεστικό νόμο Ν. 2225/1994[47] του άρθρου 19 παρ.1 του Συντάγματος. Στο Ν. 2225/1994 και ειδικότερα στο άρθρο 3 και 4 αυτού αναφέρονται αντιστοίχως οι δύο περιπτώσεις όπου επιτρέπεται η άρση του απορρήτου από τις δικαστικές αρχές, ήτοι για λόγους εθνικής ασφάλειας (άρθρο 3) και για τη διερεύνηση σοβαρών αδικημάτων (άρθρο 4).

Η ιδιωτική σφαίρα ενός ατόμου αποτελείται κυρίως από τις ιδιωτικές του σχέσεις, καθώς αυτές οι συνδέσεις απαιτούν την ανταλλαγή διαφόρων μορφών επικοινωνίας, μεταξύ άλλων και της αποστολής μηνυμάτων. Το υποκείμενο κίνητρο είναι η προστασία αυτού του προσωπικού πεδίου ιδιωτικότητας και συνακόλουθα της μετάδοσης μηνυμάτων, από οποιαδήποτε παρέμβαση από τις δημόσιες αρχές, ιδιαίτερα όταν πρόκειται για παραβίαση της μυστικότητας και του απορρήτου αυτών των μηνυμάτων. Είναι σημαντικό να τονιστεί ότι το έννομο

[47] ΦΕΚ 121Α.

αγαθό που προστατεύεται σε αυτή τη περίπτωση δεν είναι το ίδιο το μήνυμα, καθώς αυτό προστατεύεται ήδη από το άρθρο 14 του Συντάγματος, το οποίο διασφαλίζει την ελευθερία έκφρασης και διάδοσης της γνώμης, αλλά το έννομο αγαθό που προστατεύεται σε αυτή τη διάταξη είναι το απόρρητο του μηνύματος, ήτοι η διατήρηση της εμπιστευτικότητας του μηνύματος.[48]

Εντούτοις, η σφαίρα προστασίας του απορρήτου δεν περιλαμβάνει μόνο τα γραπτά μηνύματα αλλά και κάθε μορφή ιδιωτικής επικοινωνίας (π.χ. τηλεφωνικές συνομιλίες κ.λπ.), εφόσον ο αποστολέας θέλει να παραμείνει ιδιωτικό το περιεχόμενό της. Στις περιπτώσεις όπου ίδιος ο αποστολέας επιθυμεί την δημοσιότητα της επικοινωνίας του, όπως για παράδειγμα στην περίπτωση μιας ανοικτής δημόσιας επιστολής στα μέσα κοινωνικής δικτύωσης, μίας δημοσιευμένης διαφήμισης, μίας αγγελίας κ.α., δεν μπορεί να τυγχάνει εφαρμογής το άρθρο 19 του Συντάγματος, το οποίο προϋποθέτει εμπιστευτικότητα της μορφής επικοινωνίας. Επιπλέον, είναι αναμφισβήτητο το γεγονός ότι οποιαδήποτε μορφή ιδιωτικής επικοινωνίας προστατεύεται, ανεξάρτητα από την εγγενή προσωπική ή επαγγελματική της φύση.[49]

Όπως έχει ήδη διατυπωθεί, υπάρχουν ορισμένοι περιορισμοί για τη διατήρηση της εμπιστευτικότητας της ιδιωτικής επικοινωνίας, ιδιαίτερα σε περιπτώσεις όπου έρχεται σε σύγκρουση με νόμους, τη δημόσια τάξη, την ασφάλεια του κράτους και τα χρηστά ήθη. Από το ίδιο το Σύνταγμα θεσπίζονται οι παράμετροι που διέπουν τη δημοσιοποίηση ιδιωτικής αλληλογραφίας από δικαστικά και εισαγγελικά όργανα. Ωστόσο, είναι επιτακτική ανάγκη να αναγνωρίσουμε ότι για να αποτραπεί οποιαδήποτε υπονόμευση των συνταγματικών δικαιωμάτων, είναι ζωτικής σημασίας να τηρούνται οι κατάλληλες εγγυήσεις. Διαφορετικά υπάρχει κίνδυνος καταστρατήγησης της συνταγματικής διάταξης.[50]

Σε θέματα που αφορούν την ηλεκτρονική επικοινωνία, που ενδιαφέρει και την παρούσα εργασία, σύμφωνα με την ισχύουσα νομοθεσία, τα ακόλουθα θεωρούνται ως απόρρητα: 1) Το περιεχόμενο της επικοινωνίας (περιεχόμενο

---

[48] *Δαγτόγλου, Π.* ΣΥΝΤΑΓΜΑΤΙΚΟ ΔΙΚΑΙΟ ΑΤΟΜΙΚΑ ΔΙΚΑΙΩΜΑΤΑ Α'. Εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα, 2005, σελ. 350 επ.

[49] Ομοίως.

[50] Ομοίως, σελ. 355 επ.

τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας, δεδομένων), 2) η ταυτότητα του καλούντος και του καλουμένου, παραλήπτη και αποστολέα και 3) τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός). Η διαδικασία για τη νόμιμη άρση του απορρήτου καθορίζεται λεπτομερώς στην ισχύουσα νομοθεσία με τον Ν. 5002/2022, που κατήργησε τα σχετικά άρθρα του Ν. 2225/1994, και στο π.δ. 47/2005 σε συνδυασμό με το άρ. 9 του Ν. 3115/2003. [51]

Τέλος, πρέπει να επισημανθεί ότι τυχόν παραβίαση της νομοθεσίας περί απορρήτου των επικοινωνιών συνεπάγεται την επιβολή διοικητικών κυρώσεων εις βάρος παρόχων ηλεκτρονικών επικοινωνιών, με τη μορφή σύστασης, χρηματικού προστίμου, ανάκλησης του δικαιώματος παροχής υπηρεσιών από την ΑΔΑΕ και άλλες Δημόσιες Αρχές, αναλόγως της σοβαρότητας της παραβίασης. Επομένως, κάθε χρήστης υπηρεσιών ηλεκτρονικών επικοινωνιών μπορεί, σε περίπτωση που παραβιάζεται το απόρρητο της επικοινωνίας του, να αιτηθεί έννομη προστασία.[52]

3.2.2 Ο Ν. 4411/2016

Στο πλαίσιο της επιδίωξης της διασφάλισης της ψηφιακής ακεραιότητας, τα άρθρα 4 και 5 της Σύμβασης της Βουδαπέστης υποστηρίζουν την επιτακτική ανάγκη να ποινικοποιήσουν τα Κράτη Μέρη οποιαδήποτε παράνομη παραβίαση δεδομένων. Αυτό περιλαμβάνει τη σκόπιμη (εκ προθέσεως) και μη εξουσιοδοτημένη (άνευ δικαιώματος[53]) πρόκληση βλάβης, διαγραφή, καταστροφή, μεταβολή ή απόκρυψη δεδομένων υπολογιστή. Το ίδιο

[51] Στις ήδη καταργηθείσες διατάξεις του Ν. 2225/1994 παραπέμπουν οι διατάξεις του Ν. 3917/2011 "Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις".

[52] *Lawspot gr* (2018), ό.π.

[53] Με την έκφραση «χωρίς δικαίωμα» αποκλείεται ήδη η αντικειμενική υπόσταση του εγκλήματος και δεν αίρειται απλώς ο άδικος χαρακτήρας της πράξης, αφού όταν αυτή συντρέχει το προστατευόμενο έννομο αγαθό, δεν προσβάλλεται καν. Βλ. *Μυλωνόπουλο Χ.*, Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Εκδ. Αντ. Ν. Σάκκουλα 1991, σελ 94 επ. και Λαμπάκη Χ., σε: *Χαραλαμπάκη* Α., ΠΚ – Ερμηνεία κατ' άρθρο, τ. 2, 2η εκδ. 2014, σελ. 2987.

υποστηρίζεται και στο πλαίσιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών.

Η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα και η Οδηγία 2013/40/ΕΕ, που έχουν κυρωθεί με τον Ν 4411/2016, έπαιξαν σημαντικό ρόλο στην επικαιροποίηση της ελληνικής ποινικής νομοθεσίας, γεγονός που μπορεί να διαπιστωθεί μέσω μιας σειράς τροποποιήσεων που ενσωματώθηκαν στο Ποινικό Κώδικα. Έτσι, με τον Ν. 4411/2016, και συγκεκριμένα με το άρθρο 1, ο έλληνας νομοθέτης κύρωσε τη Σύμβαση περίπου δεκαπέντε χρόνια μετά την υπογραφή της και μετέφερε στον ελληνικό ΠΚ τις προβλέψεις της Οδηγίας 2013/40/ΕΕ σε σχέση με τις προσβολές κατά των συστημάτων πληροφοριών, προσθέτοντας νέες διατάξεις και τροποποιώντας τις ήδη υπάρχουσες.

Όπως αναφέρεται δε και στην αιτιολογική έκθεση του νόμου, η ταχεία πρόοδος του Διαδικτύου (Internet), η ψηφιοποίηση και η διασύνδεση των συστημάτων πληροφοριών έχουν διευκολύνει σε μεγάλο βαθμό τις διασυνοριακές εγκληματικές δραστηριότητες. Ως εκ τούτου, είναι σημαντικό να επικαιροποιηθεί η εθνική νομοθεσία και να προωθηθούν οι διεθνείς συνεργασίες, με σκοπό την προσαρμογή των κρατών μελών σε αυτές τις νέες προκλήσεις και την προώθηση των διακρατικών συνεργασιών.

Ο Ελληνικός Ποινικός Κώδικας, μετά την ψήφιση του Ν. 4411/2016, περιλαμβάνει πλέον διατάξεις που στοχεύουν στην καταπολέμηση και καταστολή του εγκλήματος στον κυβερνοχώρο. Ειδικότερα, πλέον περιλαμβάνονται διατάξεις για την παρακώλυση λειτουργίας των πληροφοριακών συστημάτων (άρθρο 292Β Π.Κ), την παράνομη πρόσβαση σε πληροφοριακά συστήματα (άρθρο 370Γ παρ. 2 Π.Κ.), τη μη εξουσιοδοτημένη αντιγραφή προγραμμάτων ηλεκτρονικών υπολογιστών (άρθρο 370Δ ΠΚ), την παρακολούθηση, αποτύπωση μη δημοσίων διαβιβάσεων δεδομένων (άρθρο 370Ε Π.Κ.), την απάτη με ηλεκτρονικό υπολογιστή (άρθρο 386Α Π.Κ.) και την παιδική πορνογραφία (άρθρο 348 Α Π.Κ.) και τέλος τα άρθρα 379 (πρώην 381Α και 381Β) για τη φθορά ψηφιακών δεδομένων και τις προπαρασκευαστικές πράξεις φθοράς τους αντίστοιχα.

Η Ελληνική Νομοθεσία έχει υποστεί εκσυγχρονισμό και προσαρμογή σε ό,τι αφορά το έγκλημα στον κυβερνοχώρο. Λαμβάνοντας υπόψη τα νέα δεδομένα και τη πολυεπίπεδη αυτή νέα μορφή εγκληματικότητας που εξελίσσεται ραγδαίως, είναι σαφές ότι θα απαιτηθούν στο μέλλον πρόσθετα νομοθετικά μέτρα και περαιτέρω ευθυγράμμιση με τα ευρωπαϊκά δεδομένα, ιδίως για την προστασία ευάλωτων ατόμων (όπως τα παιδιά και τα άτομα που βρίσκονται σε μειονεκτική θέση, οικονομικά αδύναμοι πολίτες κ.λπ.).

Υπάρχουν ορισμένες μορφές, όπως η διάδοση κακόβουλου λογισμικού, που δεν αντιμετωπίζονται συγκεκριμένα στην ελληνική νομοθεσία με ειδικές νομικές διατάξεις, αλλά αντιθέτως αντιμετωπίζονται εντός του υφιστάμενου νομοθετικού πλαισίου. Η διάδοση, δηλαδή, κακόβουλου λογισμικού θα πρέπει να διέρχεται μέσα από το φίλτρο των υφιστάμενων διατάξεων και να καταλαμβάνεται, όπου είναι δυνατό, με βάση τα αποτελέσματα που κατάφερε. Ως εκ τούτου, γίνεται αντιληπτό ότι οι ισχύουσες ποινικές διατάξεις δεν επαρκούν για την αποτελεσματική καταπολέμηση αυτής της συνεχώς εξελισσόμενης και καινοτόμου μορφής εγκλήματος στον κυβερνοχώρο.

3.2.3 Οι επιμέρους διατάξεις του Ποινικού Κώδικα

Υπό τον προϊσχύσαντα του Ν. 4416 ΠΚ, υποστηρίχθηκε η άποψη ότι ενδεχομένως θα μπορούσε ο Έλληνας νομοθέτης να είχε ομαδοποιήσει όλες τις επιθέσεις κατά των συστημάτων πληροφοριών και των ηλεκτρονικών δεδομένων σε ένα αυτοτελές κεφάλαιο. Μια τέτοια προσέγγιση θα τόνιζε επίσης τη σημασία της προστασίας των πληροφοριακών συστημάτων και των ηλεκτρονικών δεδομένων, ως αυτοτελή έννομα αγαθά, ειδικότερα αναφορικά με τις τρεις επιμέρους ιδιότητές τους, ήτοι την εμπιστευτικότητα (τη δυνατότητα του νομίμου κατόχου για αποκλεισμό της πρόσβασης ή χρήσης τρίτων), τη διαθεσιμότητα και την ακεραιότητά τους (τη δυνατότητα του νομίμου κατόχου

να τα έχει πάντα στη διάθεσή του με τη μορφή που έχουν και να ωφελείται της χρήσης τους ανά πάσα στιγμή).[54]

1. Κεφάλαιο 1ο του ΠΚ : Ο Ποινικός Νόμος

Το αρχικό βήμα σε αυτήν την ενημέρωση του εγχώριου νομικού πλαισίου μας για το έγκλημα στον κυβερνοχώρο περιλαμβάνει τη συμπερίληψη των ορισμών του "πληροφοριακού συστήματος" και των "ψηφιακών δεδομένων" στο άρθρο 13, και συγκεκριμένα στις περιπτώσεις στ' και ζ' του Ποινικού Κώδικα, αντιστοίχως, και διευρύνθηκε η έννοια του εγγράφου (περίπτωση γ').

Ειδικότερα, αναφορικά με τον ορισμό του πληροφοριακού συστήματος κατά τη διατύπωση του νέου άρθρου, αυτό ορίζεται ως εξής: *«πληροφοριακό σύστημα είναι η 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».*

Επίσης, προστέθηκε στο άρθρο 13 περ. γ' ΠΚ το εδάφιο: «*Έγγραφο 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»*.

Εν συντομία, για να συμβαδίσει με τις τεχνολογικές εξελίξεις σχετικά με το Διαδίκτυο και τον ηλεκτρονικό υπολογιστή ως μέσο τέλεσης αδικήματος, ο νομοθέτης διεύρυνε την έννοια του εγγράφου ώστε να συμπεριλάβει ενέργειες και συμπεριφορές που πραγματοποιούνται μέσω της χρήσης υπολογιστή,

[54] *Καϊάφα-Γκμπάντι Μ.,* Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, ό.π., σελ. 1077- 1078.

ενσωματώνοντάς τις έτσι στο πεδίο εφαρμογής των εγκλημάτων περί τα υπομνήματα. Μια τέτοια προσέγγιση έχει εφαρμοστεί σε διάφορα άλλα νομικά συστήματα. Είναι επιτακτική ανάγκη να επισημανθεί ωστόσο ότι, ενώ αυτό παρέχει μια λύση για την αντιμετώπιση πολλών παραβάσεων ως πλαστογραφία, υπεξαγωγή εγγράφου κ.λπ., πρέπει να αναγνωριστούν δύο ιδιαιτερότητες σε σχέση με το ηλεκτρονικό έγγραφο.

Λαμβάνοντας υπόψη τη διαιωνιστική λειτουργία του εγγράφου, είναι επιτακτική ανάγκη να αξιολογηθεί αρχικά η σταθερότητα της ενσωμάτωσης[55] του συγκεκριμένου συστήματος αποθήκευσης δεδομένων σε σχέση με την επικράτηση της προσωρινής αυτοματοποιημένης επεξεργασίας δεδομένων που γίνονται συχνά στους ηλεκτρονικούς υπολογιστές και το Διαδίκτυο. Επιπλέον, μια δεύτερη ιδιαιτερότητα που πρέπει να αντιμετωπιστεί είναι η εγγυητική λειτουργία του εγγράφου (σύνδεση των δεδομένων με ορισμένο εκδότη), στη περίπτωση που ένα ηλεκτρονικό έγγραφο φέρει ψηφιακή υπογραφή, όσο σπάνια και αν είναι αυτή η περίπτωση. Αντίθετα, στις υπόλοιπες περιπτώσεις, η αναγνώριση της ταυτότητας του εκδότη πρέπει να αναζητείται μέσω των ίδιων των δεδομένων, συμπεριλαμβανομένων στοιχείων όπως λογότυπα, πληροφορίες αποστολέα-παραλήπτη και στοιχεία ταυτότητας, παρά τις προκλήσεις που θέτει η φυσική καταγραφή των ηλεκτρονικών δεδομένων.

Συμπερασματικά, η διεύρυνση της έννοιας του εγγράφου στο άρθρο 13 ΠΚ συνιστά μια συνετή νομοθετική απόφαση, σε μια προσπάθεια εναρμόνισης του ελληνικού δικαίου με την τροχιά άλλων νομικών πλαισίων που παράλληλα προσφέρει λύσεις σε πολλές δυσχέρειες.

[55] *Κιούπη Δ.,* Δίκαιο στην Ψηφιακή Εποχή, Ένωσης Ελλήνων Νομικών e-Θέμις, εκδ. Νομική Βιβλιοθήκη 2012, σελ. 153.

2. Κεφάλαιο 14ο του ΠΚ : Εγκλήματα κατά συγκοινωνιών, τηλεπικοινωνιών και άλλων κοινωφελών εγκαταστάσεων (Άρθρα 290 - 298)

Το αδίκημα της παρακώλυσης πληροφοριακών συστημάτων (άρθρο 292Β ΠΚ), ήτοι της παρακώλυσης λειτουργίας πληροφοριακών συστημάτων και της παράνομης παρεμβολής σε συστήματα υπολογιστών, που συνεπάγεται τη σοβαρή παρεμπόδιση της λειτουργίας συστήματος υπολογιστή με την εισαγωγή, διαβίβαση, πρόκληση βλάβης διαγραφή, χειροτέρευση, μεταβολή ή απόκρυψη των δεδομένων υπολογιστή, εντάσσεται στο «ΔΕΚΑΤΟ ΤΕΤΑΡΤΟ ΚΕΦΑΛΑΙΟ» του ΠΚ το οποίο ασχολείται με εγκλήματα "κατά της ασφάλειας των συγκοινωνιών, των τηλεφωνικών επικοινωνιών και κατά των κοινωφελών εγκαταστάσεων", όπου προστατεύονται κοινωνικά (υπερατομικά) έννομα αγαθά.

Αντίθετα, η παρακώληση των πληροφοριακών συστημάτων αφορά την προστασία ατομικών έννομων αγαθών και, με εξαίρεση τη διακεκριμένη περίπτωση που περιγράφεται στην παράγραφο 2 περ. γ', δεν έχει καμία σχέση με τις κοινωφελείς εγκαταστάσεις.[56]

Υπό το πρίσμα των ανωτέρω, έχει ενσωματωθεί στον Ποινικό Κώδικα το άρθρο 292Β σχετικά με την Συγκεκριμένα, κατά το άρθρο 292Β ΠΚ ορίζεται ότι «*1. Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση και χρηματική ποινή.*

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική

[56] *Καϊάφα-Γκμπάντι, Μ.* (2016), ό.π., σελ. 248 επ.

ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.».

Από την ανωτέρω διάταξη του άρθρου μπορούμε να διακρίνουμε ότι ως υποκείμενο τέλεσης του εγκλήματος θεωρείται οποιοσδήποτε δεν έχει το δικαίωμα επέμβασης στη λειτουργία του συστήματος πληροφοριών, ενώ αντικείμενο της προσβολής είναι τα ψηφιακά δεδομένα. Η πράξη της προσβολής θεωρείται η παράνομη παρακώλυση της λειτουργίας πληροφοριακών συστημάτων, ενώ το προστατευόμενο έννομο αγαθό είναι η εξασφάλιση της δυνατότητας των χρηστών των ηλεκτρονικών υπολογιστών ή των υπολογιστικών συστημάτων να λειτουργούν προβλέψιμα και απαρεμπόδιστα.

Όπως διευκρινίζεται στο Άρθρο 60 της Επεξηγηματικής Έκθεσης της Σύμβασης για το Κυβερνοέγκλημα, η εν λόγω ρύθμιση προσπαθεί να επεκτείνει την ασπίδα προστασίας σε δεδομένα και συστήματα υπολογιστών, παραλληλίζοντας την προστασία που παρέχεται σε ενσώματα αντικείμενα. Έτσι, η ακεραιότητα και η εύρυθμη λειτουργία ή χρήση των αποθηκευμένων δεδομένων υπολογιστή ή των προγραμμάτων ηλεκτρονικών υπολογιστών θεωρείται δικαίως ως το προστατευόμενο έννομο αγαθό στην επίμαχη διάταξη. Συνεπεία τούτου, εντάσσεται στο προστατευτικό της πεδίο οποιαδήποτε νοητή εισαγωγή-μετάδοση κακόβουλων κωδικών, όπως λ.χ. οι ιοί και οι δούρειοι ίπποι, στο βαθμό συνεπάγονται τροποποίηση των δεδομένων. Η ρύθμιση, δε, αυτή θεωρείται ότι οφείλει να ποινικοποιεί μόνο τις σοβαρές κι εκ προθέσεως παρεμποδίσεις επικοινωνίας.[57] Ως σοβαρή παρεμπόδιση νοείται για παράδειγμα

[57] *Μαρκόπουλου Π.,* Η Σύμβαση για το Κυβερνοέγκλημα», Intellectum 4/2008, σελ. 47.

η αποστολή μεγάλου όγκου e-mail με στόχο την υπερφόρτωση του συστήματος και στη συνέχεια την κατάρρευσή του (mail bombing).

3. Κεφάλαιο 22ο του ΠΚ : Προσβολές ατομικού απορρήτου και επικοινωνίας

Στο κεφάλαιο αυτό τυποποιούνται οι επιθέσεις κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων υπολογιστών.

α) άρθρο 370 Α "Παραβίαση Του Απορρήτου Τηλεφωνικής Επικοινωνίας Και Προφορικής Συνομιλίας", όπως τροποποιήθηκε με τον Ν. 5002/2022

Το εδώ προστατευόμενο έννομο αγαθό είναι το δικαίωμα της ελεύθερης τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας, δηλαδή το δικαίωμα του καθενός να αποφασίζει ποιες περιστάσεις από την επικοινωνία του, πότε, υπό ποιες προϋποθέσεις και σε ποιους θα αποκαλυφθούν και θα γίνουν γνωστές. Σκοπός είναι η προστασία της ιδιωτικής ζωής, τόσο από αθέμιτες τεχνικές εισβολές που πραγματοποιούνται με την παρακολούθηση ή την αποτύπωση του προφορικού λόγου σε υλικό φορέα, όσο και από τη φανέρωση πληροφοριών που αποκτήθηκαν με τις παραπάνω πράξεις. Ως παραβίαση του απορρήτου της επικοινωνίας νοείται η παραβίαση της μυστικότητάς της και επομένως η λήψη γνώσης του περιεχομένου της ή και των εξωτερικών στοιχείων της επικοινωνίας (όπως των τηλεφωνικών αριθμών από και προς πραγματοποιούνται οι κλήσεις, η ημερομηνία και ώρα έναρξης και λήξης των τηλεφωνικών κλήσεων και διάρκεια αυτών, η ταυτότητα του συνδρομητή ή χρήστη της σύνδεσης, ο γεωγραφικός εντοπισμός).Η παραβίαση του απορρήτου γίνεται με παγίδευση ή με κατ' άλλον τρόπο παρέμβαση -σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού που χρησιμοποιείται για παροχή τέτοιων υπηρεσιών. Η κατ' άλλον τρόπο παρέμβαση γίνεται όταν ο δράστης δεν χρησιμοποιεί τεχνικά μέσα σε άμεση επαφή με τη συσκευή[58]. Εξ αντιδιαστολής η

[58] *Δαλακούρας, Θ.,* Ηλεκτρονικό Έγκλημα, Ουσιαστικές και δικονομικές όψεις, 2η έκδοση εμπλουτισμένη, εκδ. Νομική Βιβλιοθήκη, σελ. 31

παγίδευση σημαίνει την υλική επέμβαση του δράστη στη συσκευή, για παράδειγμα με την εγκατάσταση κάποιου πομπού.

Αυτές οι ενέργειες είναι αξιόποινες, όταν είναι αθέμιτες, δηλαδή χωρίς δικαίωμα (ΑΠ 954/2020). Η αποτύπωση των συνομιλιών σημαίνει την καταγραφή αυτών σε κάποιον υλικό φορέα με σταθερό τρόπο. Η αποτύπωση είναι αξιόποινη, όταν είναι σύμφωνα με τα παραπάνω αθέμιτη ή γίνεται χωρίς τη ρητή συναίνεση του συνομιλητή του δράστη (ΣτρατΘεσ 2/2022).

Ειδικά τεχνικά μέσα θεωρούνται αυτά τα οποία έχουν εξειδικευμένα τεχνικά χαρακτηριστικά, επειδή εξυπηρετούν τον σκοπό της υποκλοπής και παρακολούθησης συνομιλιών, και διακρίνονται από άλλα μέσα και συσκευές που έχουν πρωτίστως άλλη λειτουργία. Γι αυτό και η παρακολούθηση των συνομιλιών δεν έχει την έννοια της τυχαίας, ούτε της κρυφής, ακρόασης, αλλά της ακρόασης που γίνεται με υποδομή και οργάνωση.

Με τον Ν. 5002/2022 το αδίκημα αυτό τράπηκε σε κακούργημα, πράγμα το οποίο, αφενός παραβιάζει την αρχή της αναλογικότητας και δεν συμβαδίζει με την ιεραρχική ταξινόμηση των εννόμων αγαθών, και αφετέρου έρχεται σε αντίθεση με άλλες ευρωπαϊκές δικαιοταξίες, που το αντιμετωπίζουν -ορθότερα- ως πλημμέλημα.

β) άρθρο 370 Β "Παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα"

Το εδώ προστατευόμενο απόρρητο έχει τη μορφή -μέρους ή του συνόλου- συστήματος πληροφοριών (παρ. 1 περίπτωση πρώτη) ή ηλεκτρονικών δεδομένων (παρ. 1 περίπτωση δεύτερη) ή επιστημονικών ή επαγγελματικών απορρήτων επιχείρησης του δημόσιου ή ιδιωτικού φορέα (παρ. 3). Η προσβολή εκάστης μορφής αποτελεί διαφορετικό τρόπο τέλεσης της πράξης. Η προσβολή συνίσταται στην πρόσβαση, που έχει γίνει "κατά παράβαση μέτρου προστασίας" και "χωρίς δικαίωμα". Ως πρόσβαση νοείται η απλή προσπέλαση, χωρίς να ενδιαφέρει ο τρόπος με τον οποίο αυτή επιτεύχθηκε, για παράδειγμα με χρήση κακόβουλου λογισμικού, με φυσική επαφή με τη συσκευή ή με απομακρυσμένη πρόσβαση. Η τυχόν επέμβαση -αντιγραφή, διαγραφή, επεξεργασία-, που τυχόν λάβει χώρα μετά την πρόσβαση, είναι αδιάφορη.

Κατά παράβαση μέτρου προστασίας πρόσβαση είναι η πρόσβαση που έλαβε χώρα, όταν ο δράστης παρέκαμψε τα μέτρα προστασίας (παραδείγματος χάριν τους κωδικούς πρόσβασης ή το λογισμικό κρυπτογράφησης) που έθεσε ο φορέας του απορρήτου, ενώ χωρίς δικαίωμα πρόσβαση σημαίνει χωρίς αυτή να προβλέπεται από τον νόμο ή χωρίς να έχει συναινέσει και επιτρέψει αυτήν ο φορέας του απορρήτου.

Ο φορέας του σχετικού δικαιώματος προσδιορίζει ο ίδιος εκείνο που θεωρεί απόρρητο, στην έκταση που θέλει να το τηρήσει μυστικό από τρίτους, και για τον σκοπό αυτό απαιτείται να λαμβάνει κάποια αντικειμενικώς πρόσφορα μέτρα για τη διαφύλαξή του. Ειδικότερα στις επιχειρήσεις, τα απόρρητα συστήματα πληροφοριών ή ηλεκτρονικά δεδομένα μπορεί να είναι γνωστά μόνο σε στενά καθορισμένο κύκλο προσώπων, τα οποία είναι υποχρεωμένα για τη διαφύλαξη και τήρηση της μυστικότητάς τους.

Στην παράγραφο 1 και στην πρώτη περίπτωσή της τυποποιείται η περίπτωση του γνωστού ως hacking, όπου το κίνητρο του δράστη είναι περισσότερο η ικανοποίηση ότι έχει καταφέρει να εισβάλει στο σύστημα πληροφοριών παρόλες τις προσπάθειες αποτροπής, ενώ ένα παράδειγμα για την δεύτερη περίπτωση της ίδιας παραγράφου (κατά παράβαση μέτρου προστασίας και χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα) είναι το γνωστό ως phishing, όπου το θύμα της προσβολής παραδίδει το ίδιο τους κωδικούς πρόσβασης στον δράστη εξαιτίας παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, που του απέστειλε προηγουμένως ο δράστης.

γ) άρθρο 370 Γ

Το εδώ προστατευόμενο απόρρητο έχει τη μορφή στοιχείων ή προγραμμάτων υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα.

Επιπλέον το απόρρητο μπορεί να περιλαμβάνει και στοιχεία που ο κάτοχός τους επιθυμεί να παραμένουν απόρρητα, και έχει αποκλείσει την πρόσβαση σε άλλους προστατεύοντας επιπλέον τα στοιχεία αυτά και με μέτρα αποτροπής πρόσβασης.

Ως στοιχεία ή προγράμματα υπολογιστών νοούνται τα προγράμματα, δηλαδή το λογισμικό, και όλα τα επιμέρους δεδομένα ή οι πληροφορίες που περιέχονται στο εκάστοτε πρόγραμμα.

Με το άρθρο αυτό επιχειρείται η αποτροπή της βιομηχανικής κατασκοπείας, η οποία υλοποιείται με τις πράξεις της αντιγραφής αποτύπωσης, χρήσης, αποκάλυψης σε τρίτον ή με άλλον τρόπο παραβίασης. Αντιγραφή είναι η ενσωμάτωση του στοιχείου ή του προγράμματος σε υλικό φορέα, αποτύπωση είναι η αναπαραγωγή ενός ενσώματου μόνιμου αντιγράφου του προγράμματος ή των δεδομένων από κάποιο προϋπάρχον πρωτότυπο που αποτελεί ένα είδος αντιγραφής, χρησιμοποίηση είναι η χρήση των προγραμμάτων αυτών σύμφωνα με τον προορισμό τους και αποκάλυψη σε τρίτο είναι η ολική ή μερική γνωστοποίηση του λογισμικού ή των στοιχείων του κατά τρόπο που να επιτρέπει την εκμετάλλευσή τους.

Στις διακεκριμένες μορφές τυποποιούνται: (α) η περίπτωση όπου ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, δηλαδή συνδέεται με αυτόν με κάποια σχέση εργασίας, χωρίς να έχει επίδραση το είδος της, και (β) η περίπτωση όπου το απόρρητο έχει ιδιαίτερα μεγάλη οικονομική σημασία, είτε για τον φορέα του είτε για τον δράστη. Η αναφορά της διάταξης στην οικονομική σημασία του απορρήτου αναδεικνύει τη διάσταση των προγραμμάτων υπολογιστών ως ιδιαίτερου περιουσιακού αγαθού, που εκφράζει κάποια οικονομική αξία, ανάλογη με τη φύση του προγράμματος, το κόστος παραγωγής (επένδυσης για έρευνα ή και βελτίωση), κλπ[59].

δ) άρθρο 370 Δ

Η πρώτη μορφή τέλεσης είναι η χωρίς δικαίωμα αντιγραφή ή χρήση προγραμμάτων υπολογιστών (παρ. 1).

[59] *Βασιλάκη, Ε.,* Η καταπολέμηση της εγκληματικότητας μέσω των ηλεκτρονικών υπολογιστών, εκδ. Σάκκουλας, 1993, σελ. 96 επ. όπου υπάρχει ανάλυση των εννοιών του προγράμματος και του λογιστικού και εκφράζεται η θέση ότι το άρθρο 370Γ ΠΚ συνδέει λογιστικό και προγράμματα δημιουργώντας de lege lata ένα νέο περιουσιακό αγαθό, την πληροφορία όπως βρίσκεται στο λογιστικό ενός υπολογιστή.

Η δεύτερη μορφή τέλεσης είναι η χωρίς δικαίωμα πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του (παρ. 2).

Προστατευόμενο έννομο αγαθό είναι το δικαίωμα του καθενός να αποφασίζει σε ποια δεδομένα του θα αποκλείεται η πρόσβαση τρίτων, καθώς ο φορέας του σχετικού δικαιώματος προσδιορίζει ό,τι θέλει και σε όση έκταση θέλει να κρατήσει μυστικό από τους άλλους. Απαιτείται η αντιγραφή ή η χρήση ή η πρόσβαση να γίνεται χωρίς δικαίωμα και δη με την παραβίαση των απαγορεύσεων ή μέτρων ασφαλείας που έχει θέσει ο νόμιμος κάτοχος όπως μεταξύ άλλων η καθιέρωση κωδικού (password), που καταδεικνύει τη βούληση του κατόχου να αποκλείσει άλλους από την πρόσβαση σ' αυτά.

ε) άρθρο 370 Ε, όπως τροποποιήθηκε με τον Ν. 5002/2022

Το εδώ προστατευόμενο έννομο αγαθό είναι το απόρρητο της επικοινωνίας και η ιδιωτικότητα. Το αντικείμενο της προσβολής είναι τα δεδομένα, τα οποία πρέπει να μην προορίζονται για τον δράστη[60], δηλαδή δεν προορίζονται να γίνουν γνωστά σε αόριστο αριθμό ατόμων. Τέτοια δεδομένα που προορίζονται για συγκεκριμένο/ους αποδέκτη/ες μπορεί να είναι τα μηνύματα ηλεκτρονικής αλληλογραφίας ή η ανταλλαγή γραπτών μηνυμάτων σε πλατφόρμες στο διαδίκτυο (chat). Αυτά τα δεδομένα γίνονται αντικείμενο προσβολής κατά τη διαδικασία της διαβίβασής τους από, προς ή εντός πληροφοριακού συστήματος, και στον χρόνο που αυτή διαρκεί. Η διαβίβαση είναι η διαδικασία με την οποία ο αποστολέας/πομπός των ψηφιακών δεδομένων γνωστοποιεί αυτά στον παραλήπτη/δέκτη, ενώ οι ηλεκτρομαγνητικές εκπομπές προκύπτουν κατά τη λειτουργία ενός πληροφοριακού ή τηλεπικοινωνιακού συστήματος. Τα τεχνικά μέσα μπορεί να είναι είτε συσκευές είτε λογισμικό, των οποίων η εξειδικευμένη λειτουργία αποσκοπεί στην μη επιτρεπτή πρόσβαση στα δεδομένα κατά τη

[60] *Φιλόπουλος, Π.,* Η ποινική προστασία των τηλεπικοινωνιών - Μια πρώτη ερμηνευτική προσέγγιση των βασικών διατάξεων, ΤΝΠ Qualex, ΠοινΔικ, 4/2024, σελ. 483 επ.

χρονική στιγμή της μετάδοσής τους, πάντως δεν θεωρούνται ως τέτοια όλες οι συσκευές που χρησιμοποιούνται στις τηλεπικοινωνίες.

Οι μορφές διάπραξης του εγκλήματος είναι: (α) η παρακολούθηση, δηλαδή η όχι τυχαία ακρόαση ή ανάγνωση, ώστε ο δράστης να λάβει γνώση των διαβιβαζόμενων δεδομένων, (β) η αποτύπωση σε υλικό φορέα, δηλαδή η καταγραφή, (γ) η παρέμβαση, και (δ) η χρήση των δεδομένων που έχουν υποκλαπεί ή η χρήση του υλικού φορέα πάνω στον οποίο αυτά καταγράφηκαν.

Με τον Ν. 5002/2022 το αδίκημα αυτό τράπηκε σε κακούργημα, και ισχύουν τα όσα σημειώθηκαν και στο άρθρο 370 Α.

στ) άρθρο 370 ΣΤ "Απαγόρευση διακίνησης λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων", όπως προστέθηκε με τον Ν. 5002/2022

Με τη διάταξη αυτή αντιμετωπίζεται η διακίνηση συσκευών και λογισμικού που δύνανται να χρησιμοποιηθούν για τον σκοπό τέλεσης των πράξεων που περιγράφονται στις άνω διατάξεις.

4. Κεφάλαιο 23ο του ΠΚ - Εγκλήματα κατά περιουσιακών αγαθών (Άρθρα 372 - 459)

Στο πλαίσιο της προσπάθειας εναρμόνισης της ελληνικής νομοθεσίας με τις διατάξεις του άρθρου 4 της Σύμβασης και του άρθρου 5 της Οδηγίας, εισήχθη το άρθρο 381Α με την υιοθέτηση του Ν 4411/2016, το οποίο μετά την θέση σε ισχύ του Ν.4619/2019 κωδικοποιήθηκε στο άρθρο 379 ΠΚ.

Η διάταξη αυτή εισήχθη με στόχο τη διευκόλυνση της αυτόνομης προστασίας των ψηφιακών δεδομένων σε ένα πληροφοριακό σύστημα, την αποτροπή επιβλαβών πράξεων διαγραφής, καταστροφής, αλλοίωσης ή απόκρυψης, καθώς και από πράξεις που είτε καθιστούν ανέφικτη τη χρήση τους είτε αποκλείουν την πρόσβαση σε αυτά.

Υπό το προηγούμενο νομικό καθεστώς, τα δεδομένα που διατηρούνταν σε ένα πληροφοριακό σύστημα δεν θεωρούνταν «πράγμα» με την έννοια που του

αποδίδεται στο άρθρο 379 ΠΚ (πρώην άρθρο 381 ΠΚ) και επομένως δεν ενέπιπταν στο προστατευτικό πεδίο του άρθρου περί της φθοράς της ξένης ιδιοκτησίας.[61] Αυτό είχε ως αποτέλεσμα την έλλειψη προστασίας για τα ψηφιακά δεδομένα, όπου η προστασία χορηγούνταν μόνο εάν η φυσική συσκευή που περιείχε τα δεδομένα είχε καταστραφεί (σκληρός δίσκος, φορητή μνήμη κ.λπ.). Με τη νέα ρύθμιση του άρθρου 379 ΠΚ[62] αυτό το κενό θεραπεύεται, διασφαλίζοντας ολοκληρωμένη προστασία για τα ψηφιακά δεδομένα.

Εν προκειμένω, στο άρθρο 379 παρ.1 ΠΚ τυποποιείται το βασικό αδίκημα της φθοράς ψηφιακών δεδομένων, κατ' εφαρμογή του άρθρου 5 της Οδηγίας 2013/40/ΕΕ, ως εξής: *«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 δύο (2) έτη και χρηματική ποινή. Αν η ζημία που προκλήθηκε είναι ελαφρά, ο υπαίτιος τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.»*[63]

Στη παρ. 2 του ίδιου άρθρου ορίζεται ότι «*2. Η πράξη της παρ. 1 τιμωρείται: α) με φυλάκιση έως τρία (3) έτη και χρηματική ποινή, αν επλήγη μεγάλος αριθμός πληροφοριακών συστημάτων και η πράξη τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για τον σκοπό αυτόν, β) με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, ή αν τελέστηκε κατά πληροφοριακών συστημάτων που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται*

---

61 *Κιούπη Δ.,* Ποινικό Δίκαιο και Internet, Εκδ. Αντ. Σάκκουλα 1999, σελ. 140 επ. και *Μανωλεδάκης Ι./ Ν. Μπιτζιλέκης*, Εγκλήματα κατά της Ιδιοκτησίας, Εκδ. Σάκκουλα 2007, 13η εκδ. σελ. 268 επ.

62 Με τις τροποποιήσεις που επήλθαν με τον νέο Ν.4947/2022 στο Ποινικό Κώδικα και τον Κώδικα Ποινικής Δικονομίας.

63 Υπό τη προηγούμενη μορφή του, ως άρθρο 381 ΠΚ, πριν την κωδικοποίηση του νέου ΠΚ, η σχετική διάταξη είχε ως εξής: «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.».*

ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.»,[64]ενώ στη παρ.3 ορίζεται ότι *«3. Με φυλάκιση έως δύο (2) έτη και χρηματική ποινή τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη του εγκλήματος της παρ. 1 κατασκευάζει, κατέχει, εισάγει ή διαθέτει: α) συσκευές ή πληροφοριακά συστήματα, πρωτίστως σχεδιασμένα ή ειδικά προσαρμοσμένα για τον σκοπό της διάπραξης του εγκλήματος της παρ. 1 ή 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. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση τις παραπάνω συσκευές ή προγράμματα υπολογιστή ή δεδομένα πριν τα χρησιμοποιήσει για τη διάπραξη του εγκλήματος του προηγούμενου εδαφίου.».*[65]

Καθώς υπό το νέο καθεστώς του ΠΚ άλλαξε το περιεχόμενο της διάταξης, ο Έλληνας νομοθέτης συμπεριέλαβε το άρθρο 379Α ΠΚ για την τυποποίηση του αδικήματος του άρθρου 379 αλλά και αυτών των άρθρων 372 παρ.1 και 375 παρ.1, στη διακεκριμένη μορφή τους, ήτοι στη διάπραξη του αδικήματος στο πλαίσιο εγκληματικής οργάνωσης. Συγκεκριμένα, στο εν λόγω άρθρο ορίζεται *«Τα πλημμελήματα της παρ. 1 του άρθρου 372 και του πρώτου εδαφίου της παρ. 1 του άρθρου 375 που αφορούν σε υλικά μέσα πληρωμής πλην των μετρητών, καθώς και των παρ. 1 και 2 του άρθρου 379, όταν τελούνται στο πλαίσιο εγκληματικής οργάνωσης, τιμωρούνται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή.».*

---

[64] Υπό τη προηγούμενη μορφή της η παρ. 2 όριζε ότι «*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.».*

[65] Υπό τη παλαιά της μορφή η παρ. 3 όριζε «*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»*, θεσπίζοντας ειδικότερη ρύθμιση σχετικά με την διάπραξη του εγκλήματος σε οργανωμένη δομή.

Η προαναφερθείσα διάταξη του άρθρου 379 και 379Α ΠΚ αντιμετωπίζει το προηγούμενο κενό στο ελληνικό δίκαιο παρέχοντας αυτόνομη και ρητή προστασία στα ψηφιακά δεδομένα έναντι πράξεων καταστροφής, διαγραφής, αλλοίωσης κ.λπ.[66] Αυτό διασφαλίζει ότι η προστασία των ψηφιακών δεδομένων δεν εξαρτάται αποκλειστικά από τις επιπτώσεις στο φυσικό τους μέσο (όπως σκληρός δίσκος ή φορητή μνήμη), όπως συνέβαινε προηγουμένως βάσει της διάταξης σχετικά με την φθορά ξένης ιδιοκτησίας σύμφωνα με το παλαιό άρθρο 381 ΠΚ. Έτσι, η διάταξη που εισήχθη με τη θέσπιση του Ν. 4411/2016 διορθώνει ουσιαστικά αυτή την κατάσταση και καθιερώνει την αυτοτελή προστασία του εννόμου αγαθού των ψηφιακών δεδομένων,[67] συγκεκριμένα την ακεραιότητα και διαθεσιμότητα των ψηφιακών δεδομένων που επεξεργάζεται ένα πληροφοριακό σύστημα.

Το αδίκημα του άρθρου 379 ΠΚ είναι διαζευκτικά μεικτό καθώς οι διάφοροι τρόποι τέλεσής του μπορούν να εναλλαγούν, σε μια προσπάθεια του νομοθέτη να συμπεριλάβει κάθε πιθανή μορφή προσβολής των ψηφιακών δεδομένων. Συγκεκριμένα, το αδίκημα της φθοράς ψηφιακών δεδομένων κατά την ισχύουσα νομοθεσία τελείται με έξι διαφορετικούς τρόπους και δη, με διαγραφή, καταστροφή, αλλοίωση, απόκρυψη ψηφιακών δεδομένων ενός συστήματος πληροφοριών ή με το να καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά.

Ωστόσο, με οποιοδήποτε τρόπο τέλεσης και αν πραγματοποιηθεί η αντικειμενική υπόσταση του αδικήματος, τούτο θα πρέπει να γίνει με τεχνικό τρόπο, για παράδειγμα με την αλλαγή του κωδικού πρόσβασης στο αρχείο όπου φυλάσσονται τα δεδομένα, και όχι με επέμβαση στον υλικό φορέα, όπως π.χ. με την καταστροφή του σκληρού του δίσκου. Τέτοιο είδος προσβολής είναι ορθότερο να αντιμετωπίζεται με τις κοινές διατάξεις των αντίστοιχων αδικημάτων, όπως δηλαδή της φθοράς ξένης ιδιοκτησίας αντίστοιχα (378 παρ.1 ΠΚ)[68] στο προκείμενο παράδειγμα της καταστροφής του σκληρού δίσκου του

---

[66] *Βαγενά, Ε.,* Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας 1 (2017), σελ. 29επ.

[67] *Βαγενά, Ε.,* ό.π., σελ. 35 και Αιτιολογική Έκθεση του ν. 4411/2016.

[68] «*1. Όποιος καταστρέφει ή βλάπτει ξένο (ολικά ή εν μέρει) πράγμα ή με άλλον τρόπο καθιστά ανέφικτη τη χρήση του τιμωρείται με φυλάκιση έως δύο έτη ή χρηματική ποινή και αν το πράγμα είναι*

ηλεκτρονικού υπολογιστή. Σημειώνεται, επιπλέον, ότι κατ' επιταγή της Οδηγίας, προβλέφθηκε η μη τιμώρηση των ιδιαίτερα ελαφρών περιπτώσεων ή κατά την Οδηγία των «ήσσονος σημασίας περιπτώσεων», σε μια προσπάθεια περιστολής του αξιοποίνου, ορίζοντας μόνο ως ποινή το χρηματικό πρόστιμο ή την παροχή κοινωφελούς εργασίας.

Ενώ στην αρχική μορφή του άρθρου, ήτοι υπό τη μορφή του ως άρθρο 381 ΠΚ, οριζόταν ρητώς ότι για την ποινική δίωξη του αδικήματος απαιτείται έγκληση, και δεν διωκόταν αυτό αυτεπαγγέλτως, κρίθηκε ότι η σχετική διάταξη έπρεπε να τροποποιηθεί και η κατ' έγκληση δίωξη της φθοράς ψηφιακών δεδομένων να αλλάξει, με σκοπό την αποτελεσματικότερη προστασία των υποκειμένων των δεδομένων. Ο Έλληνας νομοθέτης εναρμόνισε την διάταξη με γνώμονα το ενωσιακό δίκαιο, όπου πουθενά δεν αναφερόταν η μη δυνατότητα των εισαγγελέων να διώκουν αυτεπάγγελτα τα σχετικά εγκλήματα.

Σύμφωνα με την παρ. 2 του άρθρου 379 ΠΚ, όπου περιγράφονται τρεις διακεκριμένες περιπτώσεις πλημμελληματικού χαρακτήρα του βασικού αδικήματος της φθοράς ψηφιακών δεδομένων, ορίζεται ότι «*Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση έως τρία (3) έτη και χρηματική ποινή, αν επλήγη μεγάλος αριθμός πληροφοριακών συστημάτων και η πράξη τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για τον σκοπό αυτόν»* Έτσι, η πρώτη αυτή διακεκριμένη περίπτωση στοιχειοθετείται με τη χρήση εργαλείου, το οποίο έχει σχεδιασθεί «κατά κύριο λόγο» για την πραγματοποίηση επιθέσεων σε μεγάλο αριθμό πληροφοριακών συστημάτων, σε μια προσπάθεια πλήρους εναρμόνισης με την αντίστοιχη διάταξη στην Οδηγία 2013/44/ΕΕ.

Η δεύτερη διακεκριμένη μορφή της παρ. 2 (στοιχ. β΄) θεσπίζει αυξημένη ποινή (φυλάκιση τουλάχιστον ενός (1) έτους και σωρευτικά χρηματική ποινή) στις περιπτώσεις που προκλήθηκαν 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, ή αν τελέστηκε κατά πληροφοριακών συστημάτων που αποτελούν

ιδιαίτερα μεγάλης αξίας ή τοποθετημένο σε δημόσιο χώρο με φυλάκιση τουλάχιστον ενός έτους. Αν το πράγμα είναι μικρής αξίας ή η ζημία που προκλήθηκε είναι ελαφρά, ο υπαίτιος τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.».

μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες, κυρίως για σκοπούς εθνικής άμυνας, υγείας, συγκοινωνίες, μεταφορές και για ενέργεια. Μια χαρακτηριστική περίπτωση αυτής της διακεκριμένης μορφής του αδικήματος θα ήταν μια επίθεση με κακόβουλο λογισμικό (ιό) στο σύστημα μιας υπηρεσίας όπως η Δ.Ε.Η., με περαιτέρω διαγραφή όλων των δεδομένων που σχετίζονται με τη διανομή ρεύματος στους πολίτες.

Με τη παράγραφο 3 του άρθρου 379 ΠΚ θεσπίζεται και μια τρίτη διακεκριμένη μορφή του βασικού αδικήματος, η οποία θεμελιώνεται στον κίνδυνο που ενέχουν οι προπαρασκευαστικές πράξεις για την τέλεση του βασικού εγκλήματος. Συγκεκριμένα, η παρ.3 ορίζει *«με φυλάκιση έως δύο (2) έτη και χρηματική ποινή τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη του εγκλήματος της παρ. 1 κατασκευάζει, κατέχει, εισάγει ή διαθέτει: α) συσκευές ή πληροφοριακά συστήματα, πρωτίστως σχεδιασμένα ή ειδικά προσαρμοσμένα για τον σκοπό της διάπραξης του εγκλήματος της παρ. 1 ή 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. Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση τις παραπάνω συσκευές ή προγράμματα υπολογιστή ή δεδομένα πριν τα χρησιμοποιήσει για τη διάπραξη του εγκλήματος του προηγούμενου εδαφίου.».*

Συνεπώς, με την ανωτέρω διάταξη ποινικοποιούνται και οι προπαρασκευαστικές πράξεις επί τη βάσει του υπερχειλούς σκοπού του δράστη να χρησιμοποιήσει τα επίμαχα εργαλεία με δόλο διάπραξης των αδικημάτων κατά των συστημάτων πληροφοριών, ανάγοντας έτσι τις εν λόγω πράξεις σε ολοκληρωμένο έγκλημα και ενσωματώνοντας πλήρως το περιεχόμενο του άρθρου 7 της Οδηγίας 2013/40/ΕΕ. Ωστόσο, ο νομοθέτης σε μια προσπάθεια περιστολής του αξιοποίνου θεσπίζει απαλλαγή από κάθε ποινή, αν ο υπαίτιος των προκείμενων ενεργειών καταστρέψει με δική του θέληση τις παραπάνω συσκευές ή προγράμματα υπολογιστή ή δεδομένα πριν αυτά χρησιμοποιηθούν για την τέλεση του εγκλήματος.[69]Εντούτοις, επισημαίνεται ότι έχει διατυπωθεί η

[69] *Καϊάφα-Γκμπάντι, Μ.,* Ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ό.π., σελ. 494.

άποψη ότι η κατοχή, διάθεση κλπ. συσκευών και προγραμμάτων υπολογιστών που φέρουν τη νόμιμη άδεια κυκλοφορίας στο εμπόριο από τις αρμόδιες αρχές δεν θα πρέπει να συνιστούν αξιόποινη πράξη, ενώ παράλληλα υποστηρίχθηκε ότι η εν λόγω ποινικοποίηση θα πρέπει να αφορά και σε μεγαλύτερο αριθμό τέτοιων διακινούμενων συσκευών, στα προγράμματα υπολογιστών και στους κωδικούς, για να καλύπτεται και η περίπτωση πρόκλησης κινδύνου για την ασφάλεια των πληροφοριακών συστημάτων.[70]

Τέλος, στο άρθρο 379 ΠΚ προβλέπεται ως διακεκριμένη, η περίπτωση «φθοράς» ψηφιακών δεδομένων (καθώς και της κλοπής και της υπεξαίρεσης) που τελείται στα πλαίσια εγκληματικής οργάνωσης. Ειδικότερα, η διάταξη του άρθρου ορίζει ότι *«τα πλημμελήματα της παρ. 1 του άρθρου 372 και του πρώτου εδαφίου της παρ. 1 του άρθρου 375 που αφορούν σε υλικά μέσα πληρωμής πλην των μετρητών, καθώς και των παρ. 1 και 2 του άρθρου 379, όταν τελούνται στο πλαίσιο εγκληματικής οργάνωσης, τιμωρούνται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή».* Ωστόσο, επισημαίνεται ότι δεν ακολουθείται με ακρίβεια ο ορισμός της εγκληματικής οργάνωσης σύμφωνα με την απόφαση-πλαίσιο 2008/841/ΔΕΥ, στον ορισμό της οποίας περιλαμβάνεται και ο σκοπός προσπορισμού οικονομικού ή άλλου οφέλους.

Συμπερασματικά, παρατηρούμε ότι μετά την υιοθέτηση του νέου ΠΚ ο τρόπος προσέγγισης των εγκλημάτων που τελούνται μέσω διαδικτύου έχει αντιμετωπιστεί αποτελεσματικά. Ειδικότερα, όσον αφορά στις επιθέσεις με κακόβουλο λογισμικό, η εισαγωγή αυτοτελούς διάταξης στο ΠΚ και η αφαίρεση της πρόβλεψης για κατ' έγκληση ποινική δίωξη του αδικήματος έχουν συντελέσει σε μια πιο ολοκληρωμένη και εναρμονισμένη με το ενωσιακό δίκαιο και τις επιταγές της ραγδαίας εξέλιξης της τεχνολογίας ρύθμιση.

[70] *Χατζηνικολάου, Ν.*, Ποινικό Δίκαιο – Ειδικό Μέρος, εκδ. Π.Ν. Σάκκουλας, 2017, σελ.203.

3.2.4 Πρόσφατη τροποποίηση με τον Ν. 5002/2022

i. Συγκυρία

Στις 9 Δεκεμβρίου 2022 δημοσιεύτηκε στην Εφημερίδα της Κυβερνήσεως ο Ν. 5002/2022 με τίτλο «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών» ο οποίος επιφέρει σημαντικές αλλαγές στην υφιστάμενη νομοθεσία περί άρσης του απορρήτου. Η χρονική συγκυρία κατά την οποία έγινε η ψήφισή του χαρακτηρίζεται από την οξεία πολιτική αντιπαράθεση και την έντονη ανησυχία εξαιτίας της αποκάλυψης της υπόθεσης υποκλοπών των επικοινωνιών, με τη χρήση λογισμικού παρακολούθησης, πολιτικών προσώπων, κρατικών λειτουργών, δημοσιογράφων και άλλων προσώπων, με αποκορύφωμα την αποκάλυψη της τηλεφωνικής παρακολούθησης από την Εθνική Υπηρεσία Πληροφοριών, ενός ευρωβουλευτή και υποψήφιου αρχηγού κόμματος της κοινοβουλευτικής αντιπολίτευσης στη διάρκεια της εσωκομματικής διαδικασίας ανάδειξης της ηγεσίας του συγκεκριμένου κόμματος. Η απόπειρα μόλυνσης από κατασκοπευτικό λογισμικό ανακαλύφθηκε κατά τη διάρκεια ελέγχου του τηλεφώνου του από την αρμόδια υπηρεσία του Ευρωπαϊκού Κοινοβουλίου.

Το Ευρωπαϊκό Κοινοβούλιο αποφάσισε, στις 10 Μαρτίου 2022, να συστήσει εξεταστική επιτροπή σύμφωνα με το άρθρο 226ς ΣΛΕΕ, προκειμένου να διερευνήσει εικαζόμενες παραβάσεις ή περιπτώσεις κακοδιοίκησης κατά την εφαρμογή του δικαίου της Ένωσης όσον αφορά τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης («PEGA»). Η σχετική Έκθεση ("Έκθεση σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης") δημοσιεύτηκε στις 22-5-2023[71] και είναι καταπέλτης για τη χώρα μας.

[71]Η έκθεση είναι προσπελάσιμη στην ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου στην κατηγορία Επιτροπές, στον παρακάτω σύνδεσμο : https://www.europarl.europa.eu/committees/el/pega/documents/latest-documents, με ημερομηνία ανάρτησης 23-5-2023

Η υπόθεση αυτή ονομάστηκε “Predatorgate”, από την ονομασία του κατασκοπευτικού λογισμικού Predator, το οποίο βρέθηκε εγκατεστημένο στο κινητό τηλέφωνο του άνω αναφερόμενου ευρωβουλευτή, σύμφωνα, όμως, με την άνω Έκθεση της Επιτροπής «PEGA», φαίνεται πως έχουν χρησιμοποιηθεί και άλλα λογισμικά, όπως το Pegasus, από το οποίο έλαβε το όνομά της η Επιτροπή[72]. Αυτές οι εξελίξεις δρομολόγησαν την ψήφιση του Ν. 5002/2022, που θεωρήθηκε ως σπασμωδική ανταπόκριση στην ανάγκη αποτελεσματικής διασφάλισης της προστασίας του απορρήτου.

ii. Παρατηρήσεις επί των διατάξεων

Οι κύριοι στόχοι που επιδιώχθηκαν με την ψήφιση του νόμου είναι ο εκσυγχρονισμός της διαδικασίας άρσης του απορρήτου της επικοινωνίας (καταργούνται οι σχετικές διατάξεις του Ν. 2225/1994) και η βελτιστοποίηση της δράσης της ΕΥΠ (της Εθνικής Υπηρεσίας Πληροφοριών) μέσω της αναδιάρθρωσής της, η ενίσχυση των μέτρων για την κυβερνοασφάλεια εντός της χώρας, καθώς και η βελτίωση της ρύθμισης περί ποινικής μεταχείρισης της εμπορίας, κατοχής και χρήσης λογισμικών παρακολούθησης (άρθρο 1). Οι ρυθμίσεις, όμως, επικρίθηκαν έντονα από τη νομική κοινότητα, καθώς φαίνεται ότι η προστασία του απορρήτου δεν επιτυγχάνεται αποτελεσματικά.

Για πρώτη φορά, ο όρος "εθνική ασφάλεια" ορίζεται νομοθετικά (σύμφωνα με το άρθρο 3 παράγραφος 1) και περιλαμβάνει την προστασία των βασικών λειτουργιών του κράτους και των θεμελιωδών συμφερόντων των Ελλήνων πολιτών, όπως είναι -ενδεικτικά- τα θέματα σχετικά με την εθνική άμυνα, την εξωτερική πολιτική, την ενεργειακή ασφάλεια και την κυβερνοασφάλεια. Ο ορισμός αυτός δεν είναι επαρκώς σαφής, πρώτον επειδή η άνω απαρίθμηση είναι ενδεικτική, και δεύτερον επειδή, στην έννοια των “θεμελιωδών συμφερόντων των Ελλήνων πολιτών” μπορεί να εντάσσεται ένα μεγάλο εύρος ευλόγων συμφερόντων, τα οποία ενδεχομένως δεν μπορούν όλα να θεωρούνται ζητήματα εθνικής ασφάλειας. Υποστηρίζεται ότι είναι αναγκαία η

[72] Για τον τρόπο με τον οποίο αυτά τα λογισμικά μπορούν να εγκατασταθούν σε μία συσκευή βλ. *Κανέλλο, Λ.*, THE GDPR HANDBOOK (Για DPOs, Επιχειρήσεις & Οργανισμούς), Εκδότης: Νομική Βιβλιοθήκη, Έτος έκδοσης: 2023, σελίδα 147 υποσημειώσεις 235, 236,237.

σαφέστερη οριοθέτηση της έννοιας της εθνικής ασφάλειας[73], η οποία μάλιστα θα πρέπει να συμβαδίζει με τη νομολογία του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου και του Δικαστηρίου της Ευρωπαϊκής Ένωσης.

Το άρθρο 19 παρ. 1 Σ προβλέπει ότι το απόρρητο μπορεί να αρθεί για λόγους εθνικής ασφάλειας και για τη διακρίβωση τέλεσης σοβαρών εγκλημάτων. Για λόγους "αρχιτεκτονικής" υποστηρίζεται[74] ότι και οι λόγοι εθνικής ασφάλειας πρέπει να συναρτώνται με την ποινική δικαιοδοσία, δηλαδή να πρόκειται περί πράξεων που τυποποιούνται ως εγκλήματα κατά της εθνικής ασφάλειας στον Ποινικό Κώδικα. Οι διατάξεις που προστατεύουν τα έννομα αγαθά, όπως το δημοκρατικό πολίτευμα, την εδαφική ακεραιότητα, την άμυνα, τα κρατικά απόρρητα, και τα πολιτειακά όργανα στο μέτρο που επιτελούν βασικές λειτουργίες της πολιτείας, αυτές οριοθετούν την έννοια της εθνικής ασφάλειας.

Στο άρθρο 4 παρατηρούνται δύο σημεία που είναι κρίσιμα. Η εισαγγελική διάταξη που επιτρέπει την άρση του απορρήτου δεν απαιτείται να είναι ειδικά αιτιολογημένη, πράγμα που έρχεται σε αντίθεση με την αρχές της αναγκαιότητας και της αναλογικότητας. Επίσης, η εισαγγελική διάταξη που επιτρέπει την άρση του απορρήτου (αλλά και το αίτημα που υποβάλλεται από την αρμόδια υπηρεσία) δεν απαιτείται να καταγράφει το ονοματεπώνυμο του προσώπου για το οποίο αίρεται το απόρρητο.

Σε αντίθεση με το άρθρο 4, το άρθρο 6 που αφορά την άρση του απορρήτου με σκοπό τη διακρίβωση εγκλημάτων ορίζει ότι η εισαγγελική διάταξη ή το βούλευμα που επιτρέπει την άρση του απορρήτου καταγράφει το ονοματεπώνυμο του προσώπου για το οποίο αίρεται το απόρρητο. Εξαιτίας αυτής της διαφοράς, μπορεί να γεννηθεί ευλόγως το ερώτημα αν υπάρχει επιτρεπτή δυνατότητα μαζικών παρακολουθήσεων, την οποία το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου δεν απαγορεύει. Για να θεωρείται όμως

---

[73] *Συμεωνίδου-Καστανίδου, Ε.,* Ο ν. 5002/2022 σχετικά με την άρση του απορρήτου των επικοινωνιών (ΦΕΚ Α' 228/9-12-2022): κρίσιμες για τις θεμελιώδεις ελευθερίες "αστοχίες", ΠοινΔικ, 1/2023, σελ.. 108-115, Δημοσίευση: ΤΠΝ Qualex.

[74] *Στεφανόπουλος, Μ.,* Η άρση του απορρήτου της επικοινωνίας στο ελληνικό Σύνταγμα - Επιστροφή στα θεμελιώδη μέσω της συγκυρίας, Θεωρία και Πράξη Διοικητικού Δικαίου, 12/2023, σελ. 1276 επ., Δημοσίευση: ΤΝΠ Qualex

αυτή ανεκτή και επιτρεπτή, πρέπει απαραιτήτως να καθοριστούν με μεγάλη ακρίβεια και σαφήνεια οι προϋποθέσεις της. Κυρίως πρέπει να εκτίθενται αναλυτικά και πειστικά οι λόγοι για τους οποίους είναι αναγκαία μια τέτοια μαζική παρακολούθηση, και επιπλέον να διασφαλίζεται πως υπάρχει εποπτεία και έλεγχος της διεξαγωγής της.

Ως προς τα πολιτικά πρόσωπα προβλέπεται ειδική διαδικασία άρσης του απορρήτου (άρθρο 4 παρ. 3). Το αίτημα υποβάλλει αποκλειστικά η Εθνική Υπηρεσία Πληροφοριών Στον Πρόεδρο της Βουλής, ο οποίος χορηγεί τη σχετική άδεια. Επισημαίνεται ότι σε άλλες ευρωπαϊκές χώρες υπάρχουν ειδικές ρυθμίσεις όχι μόνο για πολιτικά πρόσωπα, αλλά και για πρόσωπα που ασκούν επαγγέλματα με διάσταση λειτουργήματος, όπως δημοσιογράφοι και δικηγόροι.

Σχετικά με την άρση του απορρήτου των επικοινωνιών με σκοπό τη διακρίβωση εγκλημάτων (άρθρο 6) παρατηρείται πως ο κατάλογος των εγκλημάτων, για τα οποία αυτή είναι επιτρεπτή, είναι πολύ περισσότερο διευρυμένος από τον κατάλογο των εγκλημάτων στα άρθρα 254-255 ΚΠΔ.

Πρέπει να σημειωθεί ότι υπάρχουν κενά στον τρόπο, με τον οποίο, ενημερώνεται το πρόσωπο του οποίου έχει αρθεί το απόρρητο, αλλά και στον τρόπο διαχείρισης του υλικού που συγκεντρώθηκε μετά την άρση του απορρήτου. Έχει σημειωθεί παραπάνω ότι η μετατροπή των αδικημάτων των άρθρων 370 Α και 370 Ε του ΠΚ σε κακουργήματα δεν δικαιολογείται με βάση την αρχή της αναλογικότητας.

Τέλος, πρέπει να γίνει αναφορά στη δυνατότητα προμήθειας λογισμικών και συσκευών παρακολούθησης από το Δημόσιο (άρθρο 13). Με νόμο και όχι με προεδρικό διάταγμα θα έπρεπε να καθορίζονται οι προϋποθέσεις της προμήθειας των λογισμικών αυτών[75].

[75] *Συμεωνίδου-Καστανίδου, Ε.,* Ο ν. 5002/2022 σχετικά με την άρση του απορρήτου των επικοινωνιών (ΦΕΚ Α' 228/9-12-2022): κρίσιμες για τις θεμελιώδεις ελευθερίες "αστοχίες", ό.π.

3.2.5 Δικονομική Αντιμετώπιση

Οι παραπάνω αναφερθείσες ιδιαιτερότητες του ηλεκτρονικού εγκλήματος και κυρίως του κυβερνοεγκλήματος σηματοδοτούν τις δυσκολίες που συναντώνται στη διαχείριση αυτών των εγκλημάτων από δικονομικής πλευράς. Οι πιο σημαντικές προκλήσεις είναι οι εξής: Η ευελιξία και η ταχύτητα διάπραξης των εγκλημάτων αυτών, σε βαθμό που συχνά δεν γίνονται αντιληπτά από τα θύματα των προσβολών, παρά μόνο μετά από την πάροδο μεγάλου χρόνου. Ο διασυνοριακός χαρακτήρας του διαδικτύου, πράγμα που αναδεικνύει την ανάγκη διακρατικής συνεργασίας. Η φύση των ψηφιακών δεδομένων, τα οποία είναι εξαιρετικά ευμετάβλητα. Η χρήση εργαλείων και λογισμικών για την απόκρυψη των διαδικτυακών ιχνών, για παράδειγμα με χρήση λογισμικού κρυπτογράφησης, με χρήση proxies για ανώνυμη πλοήγηση στο διαδίκτυο.

Η Σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο περιλαμβάνει στο δεύτερο μέρος της (άρθρα 14 έως 21) διατάξεις δικονομικού δικαίου, με τις οποίες προβλέπονται συγκεκριμένες διαδικασίες για την ποινική έρευνα και δίωξη των εγκλημάτων που ορίζονται στην ίδια τη Σύμβαση και εγκλημάτων που διαπράττονται με τη χρήση συστήματος υπολογιστή, αλλά και για τη συλλογή αποδεικτικών στοιχείων σχετικών με κάποιο αδίκημα, όταν τα στοιχεία έχουν ηλεκτρονική μορφή. Συνοπτικά τα μέτρα αυτά, τα οποία οφείλουν να υλοποιήσουν τα κράτη μέρη της Σύμβασης, είναι:

α) η κατά το άρθρο 16 "Κατεπείγουσα διατήρηση αποθηκευμένων δεδομένων υπολογιστών", με σκοπό να διαφυλαχθούν τα δεδομένα (συμπεριλαμβανομένων των δεδομένων κίνησης) που βρίσκονται σε ένα σύστημα υπολογιστή, όταν υπάρχει κίνδυνος απώλειας ή τροποποίησής τους, για χρονικό διάστημα 90 ημερών, και με την υποχρέωση τήρησης εχεμύθειας περί τη διαδικασία. Με αυτό τον τρόπο εξασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των δεδομένων.

β) η κατά το άρθρο 17 "Κατεπείγουσα διατήρηση και μερική αποκάλυψη στοιχείων κίνησης", η οποία αποσκοπεί στη διάθεση επαρκούς όγκου των δεδομένων που διαφυλάχθηκαν κατά το άρθρο 16 στις αρμόδιες αρχές του κράτους μέρους, ανεξάρτητα από τον αριθμό των παρόχων υπηρεσιών διαδικτύου που τυχόν μεσολαβούν.

γ) η κατά το άρθρο 18 "Διαταγή επίδειξης", η οποία αποτελεί μια μορφή ειδικής παραγγελίας[76] της δικαστικής αρχής σε φυσικό ή νομικό πρόσωπο που βρίσκεται εντός της επικράτειας, ώστε να χορηγήσει στην αρμόδια αρχή δεδομένα που βρίσκονται υπό τον έλεγχό του.

δ) η κατά το άρθρο 19 "Έρευνα και κατάσχεση αποθηκευμένων δεδομένων υπολογιστή". Οι αρμόδιες αρχές των κρατών μερών ερευνούν και έχουν πρόσβαση σε σύστημα υπολογιστή ή σε μέρος αυτού, και στα δεδομένα που είναι αποθηκευμένα σε αυτόν, ή σε μέσο αποθήκευσης και στα εκεί αποθηκευμένα δεδομένα, αλλά και σε σύστημα υπολογιστή ή μέρος συστήματος που είναι προσιτό στο αρχικό σύστημα, και μπορούν να κατάσχουν το σύστημα υπολογιστή ή μέρος αυτού ή το μέσο αποθήκευσης, να εξασφαλίζουν την ακεραιότητα αυτών, να δημιουργούν αντίγραφα των δεδομένων, να αφαιρούν και καθιστούν απρόσιτα τα δεδομένα από το σύστημα, αλλά και να υποχρεώνουν όποια πρόσωπα γνωρίζουν τη λειτουργία των άνω συστημάτων ή κωδικούς ασφαλείας να παρέχουν πληροφορίες.

ε) η κατά το άρθρο 20 "Συλλογή δεδομένων κίνησης σε πραγματικό χρόνο" επιτρέπει στις αρμόδιες αρχές να συλλέγουν και καταγράφουν δεδομένα κίνησης σε πραγματικό χρόνο και να υποχρεώνουν τους παρόχους υπηρεσιών διαδικτύου σε συνεργασία και παροχή των άνω πληροφοριών και σε τήρηση εχεμύθειας.

[76] *Δαλακούρας, Θ.,* Ηλεκτρονικό Έγκλημα Ουσιαστικές και δικονομικές όψεις, 2η έκδοση εμπλουτισμένη, εκδ. Νομική Βιβλιοθήκη, 2023, σελ. 22.

στ) η κατά το άρθρο 21 "Άρση του απορρήτου των δεδομένων περιεχομένου". Τα κράτη μέρη έχουν την υποχρέωση να προβλέψουν τις περιπτώσεις σοβαρών εγκλημάτων, αναφορικά με τις οποίες θα επιτρέπεται άρση του απορρήτου, δηλαδή συλλογή ή καταγραφή δεδομένων περιεχομένου, σε πραγματικό χρόνο, είτε από τις αρμόδιες αρχές είτε από τους παρόχους υπηρεσιών διαδικτύου, οι οποίοι θα υποχρεούνται σε παροχή συνδρομής και σε τήρηση εχεμύθειας.

Η Ελλάδα όπως αναφέρθηκε κύρωσε τη Σύμβαση της Βουδαπέστης δυνάμει του Ν. 4411/2016, ενσωματώνοντας πολλές από τις προβλέψεις της στο εθνικό δίκαιο, όμως η άμεση εφαρμογή τους στην εθνική έννομη τάξη κάποιες φορές δεν είναι εφικτή χωρίς να προηγηθεί η κατάλληλη ενσωμάτωση. Ειδικά ως προς το ζήτημα της κατάσχεσης ψηφιακών δεδομένων, η ειδική ρύθμιση του άρθρου 265 του Κώδικα Ποινικής Δικονομίας που εισήχθη με τον Ν. 4620/2019, καλύπτει περιπτώσεις που δεν θα μπορούσαν να καλυφθούν με την επίκληση των γενικών διατάξεων. Δηλαδή, με την επίκληση των γενικών διατάξεων θα ήταν νόμιμη η κατάσχεση ενός ηλεκτρονικού υπολογιστή ως υλικού αντικειμένου, όμως δεν θα ήταν επιτρεπτή η ανάκτηση των ψηφιακών δεδομένων που θα περιείχε. Κατά τα λοιπά η έρευνα στις υποθέσεις αυτές διεξάγεται με βάση τις γενικές διατάξεις.

Οι περιπτώσεις α και β της παρ. 1 του άρθρου 265 αναφέρονται σε κατάσχεση συστήματος υπολογιστή, στο σύνολό του ή σε μέρος αυτού, και στα δεδομένα που είναι αποθηκευμένα εκεί, ή κατάσχεση μέσου αποθήκευσης δεδομένων, πάντως πρόκειται για περιπτώσεις όπου αυτά τα συστήματα υπολογιστή ή τα μέσα αποθήκευσης είναι προσβάσιμα σε φυσική μορφή σε αυτόν που διενεργεί την ανάκριση, δηλαδή υπάρχει φυσική επαφή με τους υλικούς φορείς των δεδομένων.

Η περίπτωση γ' εδάφιο α' αναφέρεται σε απομακρυσμένα συστήματα υπολογιστή, στο σύνολό τους ή σε μέρος αυτών, και στα εκεί αποθηκευμένα δεδομένα, ή σε απομακρυσμένα μέσα αποθήκευσης, και στα εκεί αποθηκευμένα δεδομένα. Όλα τα παραπάνω είναι διασυνδεδεμένα στο σύστημα υπολογιστή στο οποίο έχει φυσική πρόσβαση ο ανακρίνων.

Στο εδάφιο β' γίνεται αναφορά σε ψηφιακά δεδομένα που είναι αποθηκευμένα και προσβάσιμα μέσω συστήματος και υπηρεσιών νεφοϋπολογιστικής (cloud services), και δεν βρίσκονται σε φυσική εγγύτητα με αυτόν που διενεργεί την κατάσχεση. Γίνονται όμως αυτά προσβάσιμα με απομακρυσμένη πρόσβαση, επειδή το απομακρυσμένο σύστημα υπολογιστή ή το απομακρυσμένο μέσο αποθήκευσης δεδομένων είναι διασυνδεδεμένο στο σύστημα υπολογιστή στο οποίο έχει φυσική πρόσβαση ο ανακρίνων. Σχετικά με αυτή τη δυνατότητα υπάρχει μεγάλος προβληματισμός, για τον οποίο γίνεται λόγος παρακάτω.

Στην παράγραφο 2 ρητά απαιτείται να γίνεται χρήση ειδικού εξοπλισμού (είτε σε επίπεδο συσκευών είτε σε επίπεδο λογισμικού), ώστε να αποφευχθεί κάποια τυχαία καταστροφή ή αλλοίωση των δεδομένων. Δεν απαιτείται όμως η διαδικασία αυτή να διενεργείται και από προσωπικό αντίστοιχης εξειδίκευσης[77].

Η παράγραφος 3 προβλέπει τη σύνταξη ειδικής έκθεσης κατάσχεσης που αφορά στα ψηφιακά δεδομένα, και που είναι διακριτό έγγραφο σε σχέση με την έκθεση κατάσχεσης του υλικού φορέα των δεδομένων. Η ειδική έκθεση κατάσχεσης εξυπηρετεί την ελεγξιμότητα της όλης διαδικασίας. Σε αυτήν αναγράφεται και η μοναδική ψηφιακή ταυτότητα (hash value) των ψηφιακών δεδομένων, η οποία είναι ένα μοναδικό αλφαριθμητικό στοιχείο δημιουργούμενο με ειδικό αλγόριθμο. Αυτή είναι μια εγγύηση της ακεραιότητας των κατασχεθέντων ψηφιακών δεδομένων, καθώς σε κάθε στάδιο μπορεί να γίνει επαλήθευση της μοναδικής ψηφιακής ταυτότητάς τους και σύγκριση με αυτήν που έχει καταγραφεί στην ειδική έκθεση κατάσχεσης. Αν τα δύο αλφαριθμητικά ταυτίζονται, τότε βεβαιώνεται ότι δεν έχει γίνει επέμβαση στο κατασχεθέν ψηφιακό πειστήριο.

[77] *Ναζίρης, Ι.,* Η κατάσχεση των ψηφιακών δεδομένων, σε: Ηλεκτρονικό Έγκλημα Ουσιαστικές και Δικονομικές όψεις, 2η έκδοση εμπλουτισμένη, επιμέλεια Θεοχάρης Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, 2023

Στην παράγραφο 4 προβλέπεται η δημιουργία ενός αντιγράφου των κατασχεθέντων ψηφιακών δεδομένων, το οποίο θα βρίσκεται στη δικογραφία και θα είναι προσβάσιμο στους διαδίκους, και η δημιουργία ενός ασφαλούς αντιγράφου, το οποίο θα φυλάσσεται στο γραφείο πειστηρίων του δικαστηρίου και δεν θα προορίζεται για χρήση από τους διαδίκους, παρά μόνο από εκείνους που ασκούν καθήκοντα στην υπόθεση, και μάλιστα αυτό το ασφαλές αντίγραφο θα προστατεύεται και με κωδικούς πρόσβασης ή με κρυπτογράφηση (παράγραφος 5). Η δημιουργία αντιγράφου των κατασχεθέντων δεδομένων επιτρέπεται μόνο όταν υπάρχει ανάγκη να περιληφθούν σε άλλη δικογραφία (παράγραφος 6). Οι προβλέψεις αυτές εγγυώνται την ελεξγιμότητα, την αξιοπιστία, την επαληθευσιμότητα και την ακεραιότητα σε κάθε στάδιο της διαδικασίας.

Υπάρχει όμως ένας εύλογος προβληματισμός αναφορικά με τη δυνατότητα κατάσχεσης, που αφορά στα συστήματα υπολογιστή, στο σύνολό τους ή σε μέρος αυτών, ή στα μέσα αποθήκευσης, και στα δεδομένα που είναι αποθηκευμένα σε αυτά, που γίνονται προσβάσιμα με απομακρυσμένη πρόσβαση. Συγκεκριμένα, εντοπίζεται ο εξής κίνδυνος: εάν και κατά πόσο θα είναι δυνατός ο έλεγχος της τήρησης των νόμιμων διατυπώσεων του άρθρου 265 ΚΠΔ[78] και των λοιπών προϋποθέσεων του νόμου.

Η απομακρυσμένη πρόσβαση μπορεί να επιτευχθεί με πολλές τεχνικές μεθόδους, και μάλιστα ο χρήστης του συστήματος υπολογιστή ή ο ανακρίνων μπορεί να προσπελάσει τα δεδομένα με τρόπο ακώλυτο και άμεσο, χωρίς να είναι αισθητή η απόσταση ανάμεσα στη φυσική θέση του ανακρίνοντος και στην "τοποθεσία" των ψηφιακών δεδομένων, καθώς, ούτε χρονική καθυστέρηση ούτε κάποια δυσκολία υπάρχει στην προσπέλασή τους. Τα δεδομένα, όμως, είναι αποθηκευμένα σε έναν υλικό φορέα που βρίσκεται "κάπου αλλού". Διατυπώθηκε η παρακάτω διάκριση, που έχει να κάνει με τον " τόπο" αποθήκευσης των δεδομένων.

[78] *Δαλακούρας, Θ.,* Εισήγηση στην Εκδήλωση του Δικηγορικού Συλλόγου Αθηνών με θέμα: " Η ποινική δικηγορία μετά τις νέες αλλαγές σε ΠΚ - ΚΠΔ" στις 7-3-2024 στην Αθήνα.

Πρώτη περίπτωση: πρόκειται για ένα δίκτυο υπολογιστών ή και αποθηκευτικών μέσων, τα οποία είναι διασυνδεδεμένα μεταξύ τους, σε δίκτυο, με ζεύξη. Η ζεύξη μπορεί να είναι ενσύρματη (καλώδιο ή οπτικές ίνες) ή ασύρματη (ραδιοκύματα). Το δίκτυο μπορεί να είναι τοπικό δίκτυο ή και το διαδίκτυο. Ο αριθμός των υπολογιστών (τερματικών) μπορεί να είναι από μικρός έως και μεγάλος ή πολύ μεγάλος. Αυτή η περίπτωση δεν έχει δημιουργήσει όμως διχογνωμία σχετικά με το αν μπορούν να κατασχεθούν τα απομακρυσμένα ψηφιακά δεδομένα, καθώς η θετική απάντηση είναι ομόφωνη, γιατί κατά πλάσμα δικαίου θεωρείται ότι ο ανακρίνων έχει φυσική πρόσβαση σε αυτά.

Δεύτερη περίπτωση: πρόκειται για τις υπηρεσίες νεφοϋπολογιστικής (cloud services), κατά την οποία η τερματική συσκευή στην οποία έχει πρόσβαση ο ανακρίνων βρίσκεται συνδεδεμένη μέσω διαδικτύου και ασύρματα σε κάποιον υπολογιστή / εξυπηρετητή (server). Οι servers αποθηκεύουν μέσω διαδικτύου πολύ μεγάλες ποσότητες δεδομένων και τεράστιους αποθηκευτικούς χώρους, σε ειδικές εγκαταστάσεις. Ο χρήστης συνήθως δεν γνωρίζει την τοποθεσία των servers, παρά μόνο ενδιαφέρεται να κάνει χρήση του αποθηκευτικού χώρου.

Τα εν λόγω δεδομένα προστατεύονται από το απόρρητο των επικοινωνιών και αντιμετωπίζονται όπως τα δεδομένα κίνησης σε πραγματικό χρόνο και τα δεδομένα επικοινωνίας (πδ 47/2005), γι αυτό και πρέπει να προηγηθεί η διαδικασία της άρσης του απορρήτου τους, σύμφωνα με τις διατάξεις του νέου Ν. 5002/2022.

Η αρνητική άποψη θεωρεί ότι δεν μπορούν αυτά τα δεδομένα να κατασχεθούν ψηφιακά, όμως, μετά την άρση του απορρήτου τους, μπορεί να μνημονευθούν στη σχετική ειδική έκθεση ψηφιακής κατάσχεσης, χωρίς να περιγράφεται με λεπτομέρεια ο τρόπος μνημόνευσης[79].

[79] *Τσόγκας, Λ.,* Εισήγηση με θέμα "Ψηφιακή εποχή και δικαιοσύνη Σύγχρονες μορφές εγκληματικότητας - διεθνής συνεργασία - σύγχρονα μέσα", από το Επιμορφωτικό Σεμινάριο Δικαστικών Λειτουργών με θέμα "Ψηφιακή δικαιοσύνη: σύγχρονες προκλήσεις και προβληματισμοί", που διοργανώθηκε από την Εθνική Σχολή Δικαστικών Λειτουργών τον Φεβρουάριο του 2021. Η εισήγηση είναι δημοσιευμένη στην ιστοσελίδα της ΕΣΔΙ (https://www.esdi.gr/wp-content/uploads/images/stories/pdf/epimorfosi/2021/tsogas_2021.pdf)

Η καταφατική άποψη για τη δυνατότητα κατάσχεσης στηρίζεται στη γραμματική ερμηνεία του β' εδαφίου της περίπτωσης γ'[80] της παρ. 1 και θεωρεί ότι η πρόθεση του νομοθέτη ήταν να μπορεί να επιβληθεί και σε αυτά η ψηφιακή κατάσχεση, εφόσον έχει γίνει νόμιμη άρση του απορρήτου. Διαφορετικά, δεν θα είχε αναφερθεί ειδικά σε αυτά ο νομοθέτης. Στηρίζεται επίσης η άποψη αυτή στην ύπαρξη, στις παραγράφους 4 και 5, της φράσης "Η παρούσα ισχύει αναλόγως και στα ψηφιακά δεδομένα που αφορούν στα δεδομένα επικοινωνίας που περιλαμβάνονται στη δικογραφία", τα οποία δεδομένα επικοινωνίας μόνο μετά από άρση του απορρήτου τους μπορούν να ερευνηθούν.

Η ανάκτηση και αξιοποίηση ηλεκτρονικών αποδεικτικών στοιχείων έχει καταστεί εξαιρετικά σημαντική παράμετρος για την έρευνα, ακόμη και σε υποθέσεις που δεν αφορούν κυβερνοεγκλήματα, εξαιτίας της κυριαρχίας στην καθημερινότητά μας των εφαρμογών της τεχνολογίας. Τέτοια συλλογή ηλεκτρονικών αποδεικτικών στοιχείων, για παράδειγμα από αναρτήσεις στα μέσα κοινωνικής δικτύωσης που ο δράστης ή το θύμα της πράξης δημοσίευσαν, μπορεί να διενεργηθεί και από ανακριτικούς υπαλλήλους που δεν κατέχουν εξειδικευμένες γνώσεις πληροφορικής. Για τη συλλογή αυτών των στοιχείων μπορούν να χρησιμοποιηθούν πηγές ανοιχτής πρόσβασης, όπως τα μέσα κοινωνικής δικτύωσης. Μπορούν επίσης να αξιοποιηθούν τα εξωτερικά στοιχεία της διαδικτυακής επικοινωνίας (για παράδειγμα να εντοπιστούν οι ανταλλαγές μηνυμάτων ηλεκτρονικής αλληλογραφίας ή οι τηλεφωνικές κλήσεις μεταξύ προσώπων), εφόσον ακολουθηθούν οι διαδικασίες που προβλέπονται για την άρση του απορρήτου των επικοινωνιών.

Όταν πρόκειται για εγκλήματα του κυβερνοχώρου, η απαιτούμενη έρευνα χαρακτηρίζεται από υψηλή εξειδίκευση και αξιοποίηση ειδικών τεχνικών μέσων, δηλαδή λογισμικού ή άλλων εργαλείων και συσκευών. Είναι η λεγόμενη ψηφιακή έρευνα, που ακολουθεί τους κανόνες της επιστήμης της ψηφιακής εγκληματολογίας.

[80] *Κουδελή, Μ.,* Ζητήματα που άπτονται της κατάσχεσης ψηφιακών δεδομένων, σε : Ηλεκτρονικό Έγκλημα Ουσιαστικές και Δικονομικές όψεις, 2η έκδοση εμπλουτισμένη, επιμέλεια Θεοχάρης Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, 2023

Κατ' αναλογία με την ειδική ανακριτική πράξη της συγκαλυμμένης έρευνας, υπάρχει ανάγκη να θεσμοθετηθεί η συγκαλυμμένη "ψηφιακή" έρευνα. Οι λόγοι της αναγκαιότητας αυτής οφείλονται στην πολυπλοκότητα που χαρακτηρίζει την εγκληματική συμπεριφορά στο διαδίκτυο και τις μεθόδους απόκρυψης των ιχνών που μπορούν να αξιοποιήσουν οι δράστες. Ένα παράδειγμα είναι η διασύνδεση πληροφοριακών συστημάτων που χρησιμοποιούν οι δράστες απευθείας μέσω κόμβων (peer 2 peer) και όχι μέσω διακομιστή, δηλαδή αυτή η διασύνδεση δεν μπορεί να αποκαλυφθεί με την άρση του απορρήτου των επικοινωνιών[81].

Η επιστήμη της πληροφορικής παρέχει δυνατότητες και εργαλεία, που θα μπορούσαν να χρησιμεύουν στη διαλεύκανση τέτοιων εγκλημάτων και, υπό προϋποθέσεις, και στην πρόληψη εξαιρετικά πιθανών να τελεστούν πράξεων. Για να είναι αποδεκτά τα αποτελέσματα μιας τέτοιας έρευνας, πρέπει να καθορίζονται με εξαντλητική λεπτομέρεια οι προϋποθέσεις διεξαγωγής της, οι κανόνες που θα διέπουν τη δράση των αρχών, τα όρια της επέμβασης, η χρονική διάρκεια, η τύχη των συλλεγέντων δεδομένων μετά το πέρας της έρευνας, ιδίως των δεδομένων που δεν αφορούν στους δράστες, αλλά και η αξιοποίηση τυχόν τυχαίων ευρημάτων.

Αν και τα ζητήματα που αναφύονται στις υποθέσεις ηλεκτρονικού εγκλήματος και ειδικά κυβερνοεγκλήματος παρουσιάζουν μεγάλο βαθμό δυσκολίας, εξαιτίας της τεχνικής φύσης τους, ο ΚΠΔ δεν προβλέπει υποχρεωτικά την προσφυγή στους εξειδικευμένους επιστήμονες της πληροφορικής για την αποσαφήνιση των τεχνικών θεμάτων, ώστε να διορίζονται αυτοί ως πραγματογνώμονες από το δικαστήριο και να καταθέτουν εγγράφως έκθεση πραγματογνωμοσύνης.

[81] *Γκύζης, Δ.,* Ψηφιακή ανακριτική πράξη, σε : Ηλεκτρονικό Έγκλημα Ουσιαστικές και δικονομικές όψεις 2η έκδοση εμπλουτισμένη (επιμέλεια: Θεοχάρης Δαλακούρας), εκδ. Νομική Βιβλιοθήκη, 2023, σελ. 351 επ.

Το κενό καλύπτεται με εξέταση μαρτύρων. Οι μάρτυρες μπορεί να είναι είτε αστυνομικοί υπάλληλοι, οι οποίοι μπορεί να μην έχουν πάντα την κατάλληλη ειδίκευση, είτε μάρτυρες με ειδικές γνώσεις σύμφωνα με το άρθρο 203, οι οποίοι μπορεί να επιλέγονται μεν από τον κατάλογο των πραγματογνωμόνων, όμως δεν ισχύουν γι αυτούς οι λόγοι εξαίρεσης και τα κωλύματα διορισμού. Σε κάθε περίπτωση η μαρτυρία είναι προφορική, και δεν υπάρχει αντίστοιχο έγγραφο στον φάκελο της δικογραφίας, ώστε να μπορεί ο δικαστής να επανέλθει σε αυτό.

4 Νομικές δυσχέρειες στην ποινική αντιμετώπιση των υποθέσεων κακόβουλου λογισμικού

Η αντιμετώπιση του εγκλήματος στον κυβερνοχώρο θέτει σημαντικές προκλήσεις από την αρχή. Μία από τις πιο κρίσιμες δυσχέρειες είναι η ανάγκη τόσο νομικής κατάρτισης όσο και τεχνικών γνώσεων για την αποτελεσματική αντιμετώπιση αυτής της νέας μορφής εγκλήματος, από το στάδιο της προανάκρισης μέχρι τουλάχιστον την εκδίκαση τέτοιου είδους υποθέσεων. Ένα άλλο εξίσου σημαντικό εμπόδιο σχετικά με τις εν λόγω υποθέσεις είναι και η έλλειψη επαρκούς επιστημονικής βιβλιογραφίας και αρθρογραφίας, κάτι που είναι κατανοητό λαμβάνοντας υπόψη τη σχετικά πρόσφατη και συνεχώς εξελισσόμενη φύση του κυβερνοεγκλήματος. Αυτά τα προαναφερθέντα ζητήματα, μαζί με την επικράτηση της αγγλικής ορολογίας στην απόδοση τεχνικών όρων και ζητημάτων, σε συνδυασμό με την έλλειψη κατάρτισης των εμπλεκομένων, έχουν δημιουργήσει σημαντικό πρόβλημα στο ελληνικό νομικό σύστημα.

Είναι σύνηθες το φαινόμενο στις περιπτώσεις όπου οι ανακριτικές, διωκτικές και πρωτίστως αστυνομικές αρχές, ειδικά των Επαρχιακών Εισαγγελιών, αντιμετωπίζουν ένα αδίκημα που αφορά ηλεκτρονικό έγκλημα, τείνουν να διαβιβάζουν αμέσως τη δικογραφία στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, που βρίσκεται στην Αθήνα (με Υποδιεύθυνση στη Θεσσαλονίκη). Ωστόσο, αυτή η προσέγγιση οδήγησε σε υπερβολικό φόρτο εργασίας για την εξειδικευμένη υπηρεσία, ακόμη και για υποθέσεις που δεν απαιτούν απαραίτητα ειδική τεχνογνωσία πέρα από τις παραδοσιακές δικονομικές μεθόδους που χρησιμοποιούνται σε άλλα παραδοσιακά εγκλήματα.[82]

Για την αντιμετώπιση αυτού του φαινομένου, που υποδηλώνει γενικότερη απροθυμία ή και αδυναμία χειρισμού τέτοιων θεμάτων, παρενέβη η Εισαγγελία

[82] *Εγκύκλιος Εισαγγελίας Αρείου Πάγου* (2019). ΘΕΜΑ: «Παροχή οδηγιών σχετικά με την λειτουργία και αρμοδιότητες της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος και της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας Αποστολή ποινικών δικογραφιών και εισαγγελικών παραγγελιών που αφορούν μόνο σοβαρές υποθέσεις γνήσιων κυβερνοεγκλημάτων και εφ' όσον αυτές απαιτούν εξειδικευμένη τεχνική ή ψηφιακή έρευνα και υπάγονται στην αρμοδιότητα της υπηρεσίας». Διαθέσιμο στο <https://eisap.gr/sites/default/files/circulars/%CE%95%CE%93%CE%9A%CE%A5%CE%9A%CE%9B%CE%99%CE%9F%CE%A3%202 2019.pdf> Ανάκτηση 01.07.2023.

του Αρείου Πάγου και εξέδωσε την υπ' αριθμόν 2/2019 εγκύκλιο. Στην εγκύκλιο αυτή επισημαίνεται ότι σχεδόν όλες οι υποθέσεις που αφορούν τεχνολογίες πληροφορικής και επικοινωνιών αποστέλλονται στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος χωρίς κανένα κριτήριο ή αξιολόγηση πολυπλοκότητας ή ανάγκης εξειδικευμένων γνώσεων για τη διενέργεια προκαταρκτικών εξετάσεων ή προανάκρισης. Αξίζει, δε, να σημειωθεί ότι η τακτική αυτή έχει κάνει το έργο της συγκεκριμένης υπηρεσίας δυσχερέστερο, με αποτέλεσμα να παρεμποδίζεται η διερεύνηση σοβαρών υποθέσεων ηλεκτρονικών εγκλημάτων λόγω της εισροής ποινικών δικογραφιών ήσσονος σημασίας.[83]

Για τον μετριασμό του φαινομένου αυτού, ο Εισαγγελέας του Αρείου Πάγου ζήτησε τη συνδρομή των Εισαγγελικών Αρχών όλης της χώρας, τονίζοντας ότι η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.), με έδρα την Αθήνα, είναι αρμόδια για τη διερεύνηση γνήσιων υποθέσεων ηλεκτρονικών εγκλημάτων, όπως για παράδειγμα το αδίκημα της απάτης με υπολογιστή του άρθρου 386Α ΠΚ, καθώς και για την έρευνα, εξιχνίαση και δίωξη εγκλημάτων που διαπράττονται αποκλειστικά μέσω του Διαδικτύου, όπως το αδίκημα του άρθρου 379 ΠΚ για την φθορά ψηφιακών δεδομένων.

Έτσι, για να αναλάβει την διερεύνηση μιας τέτοιας υπόθεσης η εν λόγω Υπηρεσία, απαραίτητη προϋπόθεση είναι να απαιτούνται ειδικές γνώσεις τεχνικής ή ψηφιακής έρευνας για την εξαγωγή σχετικών πληροφοριών από τον κυβερνοχώρο, προκειμένου να ταυτοποιηθούν οι αρχικά άγνωστοι δράστες. Στην προαναφερθείσα εγκύκλιο ορίστηκε ρητά ότι μετά την ολοκλήρωση της δράσης της Υπηρεσίας, οι υπόλοιπες ανακριτικές διαδικασίες θα ανατίθενται αμελλητί στις αρμόδιες Αστυνομικές Υπηρεσίες μαζί με τις σχετικές δικογραφίες, για τις περαιτέρω ενέργειες προς την περάτωσή τους, όπως είναι ενδεικτικά η λήψη καταθέσεων από τους μάρτυρες, απολογίες κατηγορουμένων, ανωμοτί εξέταση υπόπτων, ταυτοποίηση στοιχείων, φυσική εξακρίβωση, εγχείρηση εγγράφων, απλή περιήγηση στο διαδίκτυο, εκτύπωση στοιχείων και αρχείων από το διαδίκτυο, ψηφιακό δίσκο ή USB, διενέργεια απομαγνητοφωνήσεων

[83] Εγκύκλιος ΕισΑΠ 2/2019.

τηλεφωνικών συνδιαλέξεων, οι οποίες έχουν καταγραφεί στα πλαίσια ποινικής έρευνας κ.ά.[84]

Αναφορικά με τα ζητήματα δικαιοδοσίας, γίνεται κατανοητό ότι οι προκλήσεις έγκειται στην ίδια τη φύση των εγκλημάτων που διαπράττονται στον κυβερνοχώρο που εξ ορισμού συνιστά ένα περιβάλλον διασυνοριακό το οποίο εξελίσσεται ραγδαία. Κατά συνέπεια, οποιαδήποτε αντιμετώπιση του φαινομένου σε εθνικό μόνο επίπεδο καθίσταται αυτομάτως ανεπαρκής και αναποτελεσματική. Η συλλογή ηλεκτρονικών αποδεικτικών στοιχείων, συγκεκριμένα, δημιουργεί σημαντικές δυσκολίες καθώς τα δεδομένα αλλάζουν συνεχώς και απαιτούνται εξειδικευμένες γνώσεις. Για να ξεπεραστούν αυτά τα εμπόδια, η διεθνής συνεργασία εντός του δικαστικού συστήματος καθίσταται επιτακτική. Ωστόσο, αυτό συχνά παρεμποδίζεται από τις διαφορές στα εθνικά νομικά συστήματα και τις συγκρούσεις που προκύπτουν σχετικά με τη δικαιοδοσία. Το κυβερνοέγκλημα, με τα μοναδικά του χαρακτηριστικά, αψηφά τις παραδοσιακές θεωρίες περί εδαφικότητας και εθνικής δικαιοδοσίας, δεδομένης της υπερεθνικής του φύσης στη σφαίρα του κυβερνοχώρου.

Προς αυτή την κατεύθυνση, η «Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, Για έναν ανοιχτό, ασφαλή και προστατευμένο κυβερνοχώρο»[85] έχει ως στόχο την προώθηση της διακρατικής συνεργασίας μεταξύ των κρατών μελών για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η βασική πτυχή είναι ο εξοπλισμός τους με τα απαραίτητα εργαλεία για τον εντοπισμό, τη διερεύνηση και τη δίωξη τέτοιων αδικημάτων.

Λαμβάνοντας υπόψη τα παραπάνω, ο ρόλος της Eurojust αποκτά ύψιστη σημασία. Αφιερωμένη στην αποτελεσματική αντιμετώπιση του εγκλήματος στον κυβερνοχώρο, η Eurojust διευκολύνει τη διακρατική συνεργασία. Για την επίσπευση των δικαστικών αιτημάτων, δεδομένης της εμπλοκής διαφόρων εθνικών νομικών συστημάτων και της άμεσης συμμετοχής της δικαστικής

[84] Εγκύκλιος ΕισΑΠ, 2019.

[85] 2021/2568(RSP). Resolution on the EU's Cybersecurity Strategy for the Digital Decade. Διαθέσιμο στο https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2021/2568(RSP). Ανάκτηση 02.07.2023.

εξουσίας σε επιχειρήσεις εγκλήματος στον κυβερνοχώρο, καταβάλλονται προσπάθειες για να εξασφαλιστεί η συλλογή παραδεκτών ηλεκτρονικών αποδεικτικών στοιχείων για μελλοντικές δικαστικές διαδικασίες.[86]

Άξιο αναφοράς είναι και το άρθρο 1 του Ν. 4285/2014. Το εν λόγω άρθρο, το οποίο προστέθηκε μετά το άρθρο 2 του Ν. 927/1979, ορίζει ότι στις περιπτώσεις των προαναφερθέντων άρθρων, ήτοι την καταπολέμηση του ρατσισμού, εκτελούνται με τη χρήση του διαδικτύου ή άλλων μέσων επικοινωνίας, η δικαιοδοσία ανήκει στην Ελληνική Επικράτεια. Ένας τέτοιος χαρακτηρισμός διατηρείται εφόσον η πρόσβαση στα προαναφερθέντα μέσα παρέχεται εντός των ελληνικών συνόρων, ανεξάρτητα από το τόπο εγκατάστασης τους και συνεπώς θεωρείται η Ελλάδα ως τόπος τέλεσης του αδικήματος. Με τη συμπερίληψη αυτής της διάταξης, καταβάλλεται προσπάθεια να εξαλειφθούν τυχόν διαφορές δικαιοδοσίας και να εδραιωθεί σταθερά η ελληνική δικαιοδοσία. Αυτό ισχύει όχι μόνο όταν ο δράστης χρησιμοποιεί υλικό από σύστημα πληροφορικής εντός της χώρας, αλλά και όταν το υλικό αποθηκεύεται σε σύστημα πληροφορικής που βρίσκεται στην Ελλάδα, ανεξάρτητα από τη φυσική τοποθεσία του δράστη εντός της επικράτειας.[87]

Ένα ακόμη σημαντικό ζήτημα σχετικά με την αποτελεσματική αντιμετώπιση του κυβερνοεγκλήματος είναι η ηλεκτρονική απόδειξη. Υπάρχουν τρεις κύριες μορφές ηλεκτρονικών αποδείξεων που χρησιμοποιούνται στις νομικές διαδικασίες. Η πρώτη κατηγορία περιλαμβάνει υλικό που προέρχεται από δημόσιους ιστότοπους και πλατφόρμες μέσων κοινωνικής δικτύωσης, προσβάσιμο σε όλους. Η δεύτερη κατηγορία περιλαμβάνει ψηφιακά μηνύματα και έγγραφα που δεν είναι ευρέως προσβάσιμα.

Τέλος, υπάρχουν τα δεδομένα που, όταν χρησιμοποιηθούν προσεκτικά, μπορεί να αποκαλύψουν την πηγή αλλά όχι το περιεχόμενο της επικοινωνίας ενός

---

[86] Eurojust (2020). Συνοπτική παρουσίαση. Διαθέσιμο στο https://www.eurojust.europa.eu/sites/default/files/2020 11/Cybercrime Report_Summary_EL.pdf Ανάκτηση 02.07.2023.

[87] Αιτιολογική Έκθεση Ν. 4285/2014, κυρίως άρθρα 2 και 3. «Τροποποίηση του ν. 927/1979 (Α' 139) και προσαρμογή του στην απόφαση πλαίσιο 2008/913/Δ ΕΥ της 28ης Νοεμβρίου 2008, για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου (L 328)». Διαθέσιμο στο https://lawdb.intrasoftnet.com/nomos/2_nomothesia_graph.php Ανάκτηση 01.07.2023.

ατόμου. Αντικείμενο ηλεκτρονικής απόδειξης μπορεί να είναι και κείμενα, εικόνες, φωτογραφίες κ.ά. Πηγές, δε, ηλεκτρονικών δεδομένων μπορεί να συνιστούν τα κινητά τηλέφωνα και υπολογιστές έως ιστότοπους κ.λπ. Αναφορικά, δε, με τα μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail), συνιστά ηλεκτρονική απόδειξη λόγω της προέλευσής τους από ηλεκτρονικά συστήματα και της συμπερίληψης μεταδεδομένων, ήτοι δεδομένα τα οποία προέρχονται από άλλα δεδομένα.[88]

Καταληκτικά, μπορούμε να πούμε ότι η ψηφιακή απόδειξη παίζει καθοριστικό ρόλο στον εντοπισμό και την καταδίκη των εγκληματιών στον κυβερνοχώρο. Κατά τη διάρκεια της πρώτης φάσης διερεύνησης, μπορούν να ληφθούν διάφορα μέτρα, όπως ανάλυση ύποπτου λογισμικού, ανάκτηση διαγραμμένων ή κατεστραμμένων αρχείων, αποκωδικοποίηση πληροφοριών και αναγνώριση χρηστών μέσω δεδομένων κίνησης. Η δεύτερη φάση περιλαμβάνει την παρουσίαση των ψηφιακών αποδεικτικών στοιχείων στις δικαστικές αίθουσες, είτε με έντυπα είτε με ηλεκτρονικά μέσα, ώστε να μπορούν να εξεταστούν παράλληλα με τα άλλα παραδοσιακά αποδεικτικά στοιχεία.

[88] *Μιχαηλίδου, Χ.* (2018). Κυβερνοέγκλημα και ηλεκτρονική απόδειξη ένας τρόπος εξακρίβωσης του ψηφιακού αποτυπώματός του. Ευρώπη με μια ματιά. Διαθέσιμο στο https://theartofcrime.gr/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1--%CE%BA%CE%B1%B9--%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%CE%BA%CE%AE--%CE%B1%CF%80%CF%8C%CE% Ανάκτηση 01.07.2023.

Συμπερασματικές παρατηρήσεις

Η ανάδειξη του εγκλήματος στον κυβερνοχώρο ως ταχέως εξελισσόμενου φαινομένου ξεπερνά τα γεωγραφικά όρια και διασφαλίζει την ανωνυμία των παραβατών. Η εξάπλωσή του είναι άμεσο αποτέλεσμα της ευρείας χρήσης του Διαδικτύου και της αυξανόμενης προόδου της τεχνολογίας, μέσω των οποίων έχουν δημιουργηθεί νέες μορφές εγκλημάτων, διαφορετικές από τις συμβατικές εγκληματικές συμπεριφορές και έχουν κάνει ακόμη και τους ενημερωμένους χρήστες του διαδικτύου επιρρεπείς στους κινδύνους αυτούς.

Αξίζει να επισημανθεί ότι, εντός της Ελλάδας, όπως προκύπτει από έρευνα που διεξήγαγε το ΕΚΚΕ,[89] στο πλαίσιο της διεθνούς πρωτοβουλίας γνωστής ως «World Internet Project», όπως δημοσιεύτηκε από την diaNEOSIS, 7 στους 10 Έλληνες έχουν πρόσβαση στο Διαδίκτυο, ποσοστό που φτάνει το 100% για τα νεαρά άτομα ηλικίας κάτω των 35 ετών. Επιπλέον, σύμφωνα με την ίδια έρευνα, το 11,5% των συμμετεχόντων επιβεβαιώνει ότι έχουν κληθεί να δώσουν ευαίσθητες πληροφορίες σχετικά με τραπεζικά ή άλλα προσωπικά στοιχεία στο διαδίκτυο, ενώ το 7,2% βεβαιώνει ότι έχει υποστεί διαδικτυακό εκφοβισμό ή παρενόχληση. Συμπερασματικά, σε ό,τι αφορά το ζήτημα της ιδιωτικής ζωής στη σφαίρα του διαδικτύου, ένα εντυπωσιακό 59,3% των ερωτηθέντων ισχυρίστηκε ότι "αισθάνεται ότι ελέγχει την ιδιωτικότητά τους στο διαδίκτυο", ενώ διασχίζει το εικονικό τοπίο, ενώ παραμένει ιδιαίτερα ενδιαφέρον το γεγονός ότι το 48,1% τάσσεται κατά της ενίσχυσης του κυβερνητικού ελέγχου στο διαδίκτυο πέρα από το σημερινό όριο. [90]

Έπειτα από την παρούσα μελέτη, διαπιστώθηκε ότι τα εγκλήματα στον κυβερνοχώρο είναι πλέον πιο συχνά από ποτέ, κάνοντας τον τομέα της κυβερνοασφάλειας να αναπτύσσεται με ταχύτατους ρυθμούς και τους κινδύνους ολοένα αυξανόμενους. Λόγω της ιδιάζουσας φύσης των εγκλημάτων στον κυβερνοχώρο, έχει δημιουργηθεί η ανάγκη να βρεθούν καινοτόμοι τρόποι και

[89] Εθνικό Κέντρο Κοινωνικών Ερευνών.

[90] *Νικολαΐδης, Η.* (2020). Οι Έλληνες και το ίντερνετ. Διαθέσιμο στο https://www.dianeosis.org/2020/06/oi ellines kai to internet/ Ανάκτηση 28.06.2023.

επικαιροποιημένες ρυθμίσεις για την αποτελεσματική αντιμετώπιση της νέας αυτής μορφής εγκληματικότητας.

Σε αυτό το πλαίσιο, έγινε μια προσπάθεια για την τεκμηρίωση των θεμελιωδών πτυχών του εγκλήματος στον κυβερνοχώρο τόσο σε εθνική όσο και σε ευρωπαϊκή-παγκόσμια κλίμακα. Οι πρωταρχικές προκλήσεις που εντοπίστηκαν έγκεινται στην έλλειψη μεγάλου αριθμού επιστημονικών πηγών, όχι μόνο στην ελληνική αλλά και στη ξενόγλωσση βιβλιογραφία, ενισχύοντας έτσι το επιχείρημα σχετικά με την συνεχόμενη και ολοένα αυξανόμενη εξέλιξη του ιδιαίτερου αυτού εγκληματικού φαινομένου.

Με την παραπάνω ανάλυση, περιγράφηκε με σαφήνεια και πληρότητα το ποινικό νομικό σύστημα της Ελλάδας σχετικά με τη δίωξη επιθέσεων σε πληροφοριακά συστήματα και στα ψηφιακά τους δεδομένα, ιδιαίτερα εκείνων που εκτελούνται μέσω κακόβουλου λογισμικού, επισημαίνοντας ταυτόχρονα την έκταση της ποινικής αντιμετώπισης αυτών των προσβολών από την ελληνική έννομη τάξη, στη προσπάθεια εναρμόνισης με το διεθνές-ενωσιακό δίκαιο. Ταυτόχρονα, πραγματοποιήθηκε μια ευσύνοπτη συγκριτική έρευνα, η οποία σκιαγραφεί τα θεμελιώδη διεθνή κείμενα στον τομέα του εγκλήματος στον κυβερνοχώρο, δηλαδή τη Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στον κυβερνοχώρο και την Οδηγία 2013/40/ΕΕ, επί της οποίας ο Έλληνας νομοθέτης στηρίχθηκε για τη τυποποίηση των αδικημάτων σχετικά με τα πληροφοριακά συστήματα.

Προς την κατεύθυνση αυτή γίνονται επιμελείς προσπάθειες για τον εκσυγχρονισμό της εθνικής νομοθεσίας και την εναρμόνισή της με τα ευρωπαϊκά πρότυπα δεδομένων, όλα προς επιδίωξη μιας αποτελεσματικής αντεγκληματικής πολιτικής. Αν και έχει σημειωθεί πρόοδος στη χώρα μας, η τρέχουσα προσέγγιση, με επίκεντρο τις Υπηρεσίες Δίωξης Ηλεκτρονικού Εγκλήματος κυρίως στην Αθήνα και τη Θεσσαλονίκη, έχει αποδειχθεί σε μεγάλο βαθμό αναποτελεσματική. Παρά τις αξιέπαινες προσπάθειες της Υπηρεσίας, υπάρχουν σημαντικές καθυστερήσεις στην επίλυση υποθέσεων και συσσώρευση υποθέσεων, με πολλές από αυτές τις υποθέσεις να μην απαιτούν καν την εξειδικευμένη τεχνολογική εμπειρογνωμοσύνη για την επίλυση τους.

Συνεπώς, είναι υψίστης σημασίας να επιτευχθούν σημαντικές τομές στην αποτελεσματική καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Τούτο μπορεί να επιτευχθεί μέσω της ταχείας ενσωμάτωσης των ευρωπαϊκών δεδομένων και του εκσυγχρονισμού του ανακριτικού συστήματος, με επίκεντρο την ταχεία συλλογή αποδεικτικών στοιχείων, διασφαλίζοντας παράλληλα την προστασία των ατομικών ελευθεριών. Επιτακτική θεωρείται και η συνεχής εκπαίδευση και ανάπτυξη τόσο των διωκτικών υπηρεσιών όσο και των χρηστών του Διαδικτύου, καθώς χρησιμοποιούν τις υπηρεσίες του διαδικτύου, είτε για προσωπικούς είτε για επαγγελματικούς σκοπούς.

Οι δυσχέρειες που αναφέρθηκαν στη παρούσα εργασία, σχετικά με τη συλλογή αποδεικτικών στοιχείων, τον εντοπισμό των ενόχων και την ανάγκη για διεθνή συνεργασία, λειτουργούν ως εμπόδιο τόσο στον περιορισμό αυτού του πολύπλευρου εγκληματικού φαινομένου όσο και στην καταγραφή όλων των αδικημάτων που τελούνται στο Διαδίκτυο, σημαντικό μέρος των οποίων δεν καταγγέλλονται και συνακόλουθα παραμένουν ανεξιχνίαστα. Η χρήση προηγμένων τεχνολογικών συστημάτων, σε συνδυασμό με την υψηλή τεχνογνωσία των δραστών, καθιστούν την καταπολέμηση του κυβερνοεγκλήματος ένα δύσκολο εγχείρημα.

Πέραν τούτων, παρατηρούνται και δυσκολίες στην ερμηνεία νέων τεχνολογικών και εξειδικευμένων όρων, πολλοί εκ των οποίων παραμένουν άγνωστοι στη νομική κοινότητα, ενώ προκύπτει και μια ευρύτερη παρατήρηση από την εξέταση των διεθνών και ευρωπαϊκών κειμένων, καθώς και από τις αποφάσεις που έλαβε ο Έλληνας νομοθέτης σχετικά με τον ΠΚ. Αυτή η παρατήρηση υποδηλώνει μια κυρίαρχη τάση για ποινικοποίηση ακόμη και καθημερινών δραστηριοτήτων που σχετίζονται με τη κατασκευή, κατοχή, πώληση κλπ. προγραμμάτων η/υ και άλλων ηλεκτρονικών συσκευών.

Ωστόσο, είναι επιτακτική ανάγκη να θυμόμαστε ότι σε μια δημοκρατική και προνομιακή κοινωνία, η χρήση του ποινικού δικαίου ως μέσο καταστολής θα πρέπει να είναι το έσχατο μέσο (ultima ratio) παρέμβασης σε ζητήματα που αφορούν έννομα αγαθά, δηλαδή να επιλέγεται μόνο αφού εξαντληθούν όλες οι άλλες επιλογές. Αντίθετα, η προσοχή θα πρέπει να στραφεί στην πρόληψη, τόσο

σε εθνική όσο και σε πανευρωπαϊκή κλίμακα, παρέχοντας ολοκληρωμένη και σαφή ενημέρωση στους ιδιώτες, φυσικά πρόσωπα και επιχειρήσεις, για την ενίσχυση της άμυνάς τους έναντι των αναδυόμενων μορφών πληροφοριακών επιθέσεων.

Συμπερασματικά, λαμβάνοντας υπόψη την παγκόσμια εμβέλεια του εν γένει εγκλήματος στον κυβερνοχώρο, αποτελεί ισχυρή απειλή τόσο για τα κράτη όσο και για τους ιδιώτες ατομικά, θέτοντας σε κίνδυνο μια πληθώρα περιουσιακών και προσωπικών εννόμων αγαθών. Ως εκ τούτου, συνίσταται σε κομβικό παράγοντα για την αποτελεσματική καταπολέμηση και καταστολή του εν λόγω φαινομένου της νέας μορφής εγκληματικότητας, τόσο η σφυρηλάτηση των διακρατικών συνεργασιών, όσο και ο εναρμονισμός των εθνικών νομοθεσιών στο εσωτερικό κάθε έννομης τάξης.

Βιβλιογραφία/Αρθρογραφία

Ελληνική

Αγγελής, Ι., Ασφάλεια Πληροφοριών, Εκδόσεις Νέων Πληροφοριών, Αθήνα 1995

Του ίδιου, Διαδίκτυο (internet) και ποινικό δίκαιο, Έγκλημα στον Κυβερνοχώρο (cybercrime–internet crime), ΠοινΧρ 2000, σελ. 675 επ.

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

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

Βαγενά, Ε., Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας 1 (2017)

Βασιλάκη, Ε., Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών : η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του ν. 1805/88, Α. Ν. Σάκκουλας, Αθήνα 1993

Βλαχόπουλος Κ., Ηλεκτρονικό έγκλημα: μορφές, πρόληψη, αντιμετώπιση, Νομική Βιβλιοθήκη, 2007

Γκύζης, Δ., Ψηφιακή ανακριτική πράξη, σε : Ηλεκτρονικό Έγκλημα Ουσιαστικές και δικονομικές όψεις 2η έκδοση εμπλουτισμένη (επιμέλεια: Θεοχάρης Δαλακούρας), εκδ. Νομική Βιβλιοθήκη, 2023

Δαγτόγλου, Π. ΣΥΝΤΑΓΜΑΤΙΚΟ ΔΙΚΑΙΟ ΑΤΟΜΙΚΑ ΔΙΚΑΙΩΜΑΤΑ Α'. Εκδόσεις Αντ. Ν. Σάκκουλα Αθήνα, 2005

Δαλακούρας, Θ., Ηλεκτρονικό Έγκλημα Ουσιαστικές και δικονομικές όψεις, 2η έκδοση εμπλουτισμένη, εκδόσεις Νομική Βιβλιοθήκη, 2023

Δαλακούρας, Θ., Εισήγηση στην Εκδήλωση του Δικηγορικού Συλλόγου Αθηνών με θέμα: " Η ποινική δικηγορία μετά τις νέες αλλαγές σε ΠΚ - ΚΠΔ" στις 7-3-2024 στην Αθήνα

Εγκύκλιος Εισαγγελίας Αρείου Πάγου (2019). «Παροχή οδηγιών σχετικά με την λειτουργία και αρμοδιότητες της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος και της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας Αποστολή ποινικών δικογραφιών και εισαγγελικών παραγγελιών που αφορούν μόνο σοβαρές υποθέσεις γνήσιων κυβερνοεγκλημάτων και εφ' όσον αυτές απαιτούν εξειδικευμένη τεχνική ή ψηφιακή έρευνα και υπάγονται στην αρμοδιότητα της υπηρεσίας».

Έκθεση σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης, με ημερομηνία έκδοσης 22-5-2023, από την Εξεταστική Επιτροπή «PEGA» του Ευρωπαϊκού Κοινοβουλίου που συστήθηκε προκειμένου να διερευνήσει εικαζόμενες παραβάσεις ή περιπτώσεις κακοδιοίκησης κατά την εφαρμογή του δικαίου της Ένωσης όσον αφορά τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης, προσπελάσιμη στην ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου στην κατηγορία Επιτροπές, στον σύνδεσμο https://www.europarl.europa.eu/committees/el/pega/documents/latest-documents, με ημερομηνία ανάρτησης 23-5-2023

Ζάννης Α., Το διαδικτυακό έγκλημα, εκδ. Α. Σάκκουλα, 2005

Ζημιανίτης Δ., Δίκαιο στην Ψηφιακή Εποχή της Ένωσης Ελλήνων Νομικών e-Θέμις, εκδ. Νομική Βιβλιοθήκη 2012

Καργόπουλος, Α. Πρωτοδίκης, Εθνικός Εμπειρογνώμονας στον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ε.Ε., Κυβερνοέγκλημα: Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου. 2018. Έρευνα διαθέσιμη στο <https://www.esdi.gr›epimorfosi›kargopoulos>

Καϊάφα-Γκμπάντι, Μ., Στοιχεία Ενωσιακού Ποινικού Δικαίου και της ενσωμάτωσής του στην ελληνική έννομη τάξη, εκδ. Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2016

Της ίδιας, 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.

Της ίδιας, Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμ. 2007, σελ. 1061 επ.

Κανέλλος, Λ., THE GDPR HANDBOOK (Για DPOs, Επιχειρήσεις & Οργανισμούς), Εκδότης: Νομική Βιβλιοθήκη, Έτος έκδοσης: 2023, σελίδα 147 υποσημειώσεις 235, 236,237.

Κιούπη Δ., Δίκαιο στην Ψηφιακή Εποχή, Ένωσης Ελλήνων Νομικών e-Θέμις, εκδ. Νομική Βιβλιοθήκη, 2012

Του ίδιου, Ποινικό Δίκαιο και Internet, Εκδ. Αντ. Σάκκουλα, 1999

Κουδελή, Μ., Ζητήματα που άπτονται της κατάσχεσης ψηφιακών δεδομένων, σε : Ηλεκτρονικό Έγκλημα Ουσιαστικές και Δικονομικές όψεις, 2η έκδοση εμπλουτισμένη, επιμέλεια Θεοχάρης Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, 2023

Λάζου, Γ., Πληροφορική & Έγκλημα, Νομική Βιβλιοθήκη, Αθήνα 2001

Μανωλεδάκης Ι./ Ν. Μπιτζιλέκης, Εγκλήματα κατά της Ιδιοκτησίας, Εκδ. Σάκκουλα, 2007

Μαρκόπουλου Π., Η Σύμβαση για το Κυβερνοέγκλημα», Intellectum 4/2008, σελ. 47

Μεταξάκης Ε., Η ποινική αντιμετώπιση της ανεπιθύμητης αλληλογραφίας επ αφορμή της ΠραξΑρχειοθΕισΠρΑθ της ηλεκτρονικής, ΠοινΔΙκ 2015, σελ. 681 επ.

Μιχαηλίδου, Χ. Κυβερνοέγκλημα και ηλεκτρονική απόδειξη ένας τρόπος εξακρίβωσης του ψηφιακού αποτυπώματός του. Ευρώπη με μια ματιά. 2018. Διαθέσιμο στο https://theartofcrime.gr

Μυλωνόπουλος, Χρ., Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, Α. Ν. Σάκκουλας, Αθήνα 1991

Ναζίρης, Ι., Η κατάσχεση των ψηφιακών δεδομένων, σε: Ηλεκτρονικό Έγκλημα Ουσιαστικές και Δικονομικές όψεις, 2η έκδοση εμπλουτισμένη, επιμέλεια Θεοχάρης Δαλακούρας, εκδ. Νομική Βιβλιοθήκη, 2023

Νικολαΐδης, Η. Οι Έλληνες και το ίντερνετ, 2020. Διαθέσιμο στο https://www.dianeosis.org/2020/06/oi ellines kai to internet/

Παναεοφύτου Α., Ποινικό Δίκαιο, Κράτος και Τεχνολογικοί Κίνδυνοι, εκδ. Α. Σάκκουλα 1997

Στεφανόπουλος, Μ., Η άρση του απορρήτου της επικοινωνίας στο ελληνικό Σύνταγμα - Επιστροφή στα θεμελιώδη μέσω της συγκυρίας, Θεωρία και Πράξη Διοικητικού Δικαίου, 12/2023, σελ. 1276, Δημοσίευση: ΤΝΠ Qualex

Συμεωνίδου-Καστανίδου, Ε., Ο ν. 5002/2022 σχετικά με την άρση του απορρήτου των επικοινωνιών (ΦΕΚ Α' 228/9-12-2022): κρίσιμες για τις θεμελιώδεις ελευθερίες "αστοχίες", ΠοινΔικ, 1/2023, σελ.. 108-115, Δημοσίευση: ΤΠΝ Qualex

Τσόγκας, Λ., Εισήγηση με θέμα "Ψηφιακή εποχή και δικαιοσύνη Σύγχρονες μορφές εγκληματικότητας - διεθνής συνεργασία - σύγχρονα μέσα", από το Επιμορφωτικό Σεμινάριο Δικαστικών Λειτουργών με θέμα "Ψηφιακή δικαιοσύνη: σύγχρονες προκλήσεις και προβληματισμοί", που διοργανώθηκε από την Εθνική Σχολή Δικαστικών Λειτουργών τον Φεβρουάριο του 2021. Η εισήγηση είναι δημοσιευμένη στην ιστοσελίδα της ΕΣΔΙ (https://www.esdi.gr/wp-content/uploads/images/stories/pdf/epimorfosi/2021/tsogas_2021.pdf)

Φιλόπουλος, Π., Η ποινική προστασία των τηλεπικοινωνιών - Μια πρώτη ερμηνευτική προσέγγιση των βασικών διατάξεων, δημοσίευση ΠοινΔικ, 4/2024, άντληση μέσω ΤΝΠ Qualex

Χαραλαμπάκη Α., ΠΚ – Ερμηνεία κατ' άρθρο, τ. 2, 2η εκδ., Νομική Βιβλιοθήκη, 2014

Χατζηνικολάου, Ν., Ποινικό Δίκαιο – Ειδικό Μέρος, εκδ. Π.Ν. Σάκκουλας, 2017

Eurojust (2020). Συνοπτική παρουσίαση. Διαθέσιμο στο https://www.eurojust.europa.eu/sites/default/files/2020 11/Cybercrime Report Summary EL.pdf

Lawspot gr. Η προστασία του απορρήτου των επικοινωνιών: Ενημερωτικό υλικό από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών Με αφορμή τον Ευρωπαϊκό Μήνα για την Ασφάλεια στον Κυβερνοχώρο (2018). Διαθέσιμο στο https://www.l awspot.gr/nomika nea/i prostasia toy aporritoy ton epikoinonion enimerotiko yliko apo tin arhi diasfalisis toy

Ξενόγλωσση

Clough, J., Principles of cybercrime, Cambridge University Press, Cambridge – New York 2010

Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185. Διαθέσιμο στην ιστοσελίδα: https://rm.coe.int/16800cce5b

Felix, J., Hauck, C., 'System Security: A Hacker's Perspective', Interex Proceedings 8: 6 (1987)

Mitchell S./ Baker E., Private Intrusion Response, Harvard Journal of Law & Technology, 1998, Volume 11, Number 3, σελ. 707 επ.

OECD, Computer Related Crime: Analysis of legal policy, Paris, 1986

Resolution on the EU's Cybersecurity Strategy for the Digital Decade. Διαθέσιμο στο https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2021/2568(RSP)

Saeed, I.A., Selamat, A. και Abuagoub, A.M. A survey on malware and malware detection systems. International Journal of Computer Applications, 2013, σελ. 67(16).

Souppaya, M., Scarfone, K. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication SP 800-83, July 2013

Spring, T., Spam Slayer: Do You Speak Spam? PC World Article, 2003

Stevenson, RLB, 'PLUGGING THE “PHISHING” HOLE: LEGISLATION VERSUS TECHNOLOGY ', Duke L. & Tech. Rev., 2005

Walden I., Harmosing Computer Crime Laws in Europe, European Journal of Crime, Criminal Law and Criminal Justice, Vol 12 (2004), σελ. 321-336: 324