ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό Έτος 2025-2026

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Της Ειρήνης Ντόβα

(Α.Μ.: ΜΔΙ2440)

ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ ΥΠΟ ΤΗΝ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΙΑΚΗ ΟΠΤΙΚΗ-ΔΙΑΠΙΣΤΩΜΕΝΗ ΧΡΗΣΗ ΚΑΙ ΠΡΩΤΟΒΟΥΛΙΕΣ ΔΙΑΧΕΙΡΙΣΗΣ

Επιβλέπουσα:

Παπανικολάου Αικατερίνα

Πειραιάς, Ιούλιος 2026

Πίνακας Περιεχομένων

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ 4

ΠΕΡΙΛΗΨΗ 6

ABSTRACT 8

ΕΙΣΑΓΩΓΗ 9

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ: ΕΙΣΑΓΩΓΗ ΣΤΑ ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ 12

1.1 Ορισμοί – Γενική περιγραφή 12

1.2 Εξέλιξη του φαινομένου 14

1.3 Σύγχρονες μορφές κατασκοπευτικού λογισμικού 16

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ: ΤΡΟΠΟΣ ΚΑΙ ΠΕΔΙΟ ΔΡΑΣΗΣ ΚΑΤΑΣΚΟΠΕΥΤΙΚΩΝ ΛΟΓΙΣΜΙΚΩΝ 18

2.1 Τρόπος δράσης κατασκοπευτικών λογισμικών 18

2.2 Μηχανισμοί αντιμετώπισης 22

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ: ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ ΚΑΤΑΣΚΟΠΕΥΤΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ 26

3.1 Απάτη με υπολογιστή- Ηλεκτρονικά εγκλήματα 26

3.2 Ηλεκτρονικό εμπόριο 29

3.3 Περιπτώσεις χρήσης spyware στην Ευρωπαϊκή Ένωση 32

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ: ΗΘΙΚΑ ΚΑΙ ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΧΡΗΣΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΚΑΤΑΣΚΟΠΕΙΑΣ 38

4.1 Ηθικά ζητήματα και ηλεκτρονική τεχνολογία 38

4.2 Παραβιάσεις θεμελιωδών δικαιωμάτων 40

4.3 Δικαίωμα προστασίας προσωπικών δεδομένων 42

4.4 Δικαίωμα προστασίας απορρήτου των επικοινωνιών 44

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ: ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΚΑΤΑΣΚΟΠΕΙΑΣ ΣΤΗΝ ΕΕ 47

5.1 Νομικά ζητήματα 47

5.2 Προστασία επικοινωνιών και διαδικασία άρσης του απορρήτου των επικοινωνιών 51

5.3 Προστασία προσωπικών δεδομένων 53

5.4 Εξέλιξη του λογισμικού κατασκοπείας και Τεχνητή Νοημοσύνη 54

5.5 Περιπτώσεις νόμιμης χρήσης του λογισμικού κατασκοπείας 56

ΚΕΦΑΛΑΙΟ ΕΚΤΟ: ΑΠΑΙΤΟΥΜΕΝΕΣ ΝΟΜΙΚΕΣ ΚΑΙ ΘΕΣΜΙΚΕΣ ΠΡΩΤΟΒΟΥΛΙΕΣ 60

6.1 Επάρκεια νομικού πλαισίου ΕΕ 60

6.2 Επάρκεια σε Εθνικό πλαίσιο 64

ΣΥΜΠΕΡΑΣΜΑΤΑ 66

ΕΠΙΛΟΓΟΣ.....71
ΒΙΒΛΙΟΓΡΑΦΙΑ.....72

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΔΑΕ: Αρχή Διασφάλισης Απορρήτου Επικοινωνιών

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

ΔΑΕΕΒ: Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας

ΔΕΕ: Δικαστήριο της Ευρωπαϊκής Ένωσης

ΔΣΑΠΔ: Διεθνές Σύμφωνο για Ατομικά και Πολιτικά Δικαιώματα

ΕΑΚ: Εθνική Αρχή Κυβερνοασφάλειας

ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

ΕΔΔΑ: Ευρωπαϊκό Δικαστήριο Δικαιωμάτων Ανθρώπου

ΕΕ: Ευρωπαϊκή Ένωση

ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

Εκδ.: εκδόσεις

ΕΡΑ: Εθνική Ρυθμιστική Αρχή

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση Δικαιωμάτων Ανθρώπου

ΕΣΠΔ: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

ΕΥΠ: Εθνική Υπηρεσία Πληροφοριών

κ.ά.: Και *άλλα*

Κ.λπ.: Και λοιπά

Κ-Μ: Κράτη Μέλη

Ν.: Νόμος

Οδ. : Οδηγία

ΟΗΕ: Οργανισμός Ηνωμένων Εθνών

ΠΑΔ: Παρατηρητήριο Ανθρωπίνων Δικαιωμάτων

ΠΔ: Προεδρικό Διάταγμα

Παρ.: Παράγραφος

Π.χ.: Παραδείγματος χάριν

ΠΚ: Ποινικός Κώδικας

Σ: Σύνταγμα

ΤΝ: Τεχνητή Νοημοσύνη

ΤΠΕ: Τεχνολογιών Πληροφοριών και Επικοινωνιών

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

BEREC: Body of European Regulators for Electronic Communications

GDPR: General Data Protection Regulation

ECHR: European Court of Human Rights

ENISA: European Union Agency for Cybersecurity

FDPIC: Federal Data Protection and Information Commissioner

HRW: Human Right Watch

IE: Internet Explorer

NIS: Network and Information Systems

OHCHR: Office of the High Commissioner for Human Rights.

p.: page

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία, έχει σκοπό, να εξετάσει τα υφιστάμενα κατασκοπευτικά λογισμικά υπό το Ενωσιακό κανονιστικό πλαίσιο, εστιάζοντας τόσο στις μορφές που εμφανίζονται, όσο και στις επιπτώσεις που προκαλούν σε μεμονωμένα άτομα ή κοινωνικές ομάδες, αναλύοντας τα νομικά ζητήματα που ανακύπτουν και αποτυπώνονται μέσα από παραδείγματα διαπιστωμένης χρήσης τους.

Για το λόγο αυτό, αναλύεται το ισχύον θεσμικό και ρυθμιστικό πλαίσιο της Ευρωπαϊκής Ένωσης, στον τομέα που αφορά τα εν λόγω λογισμικά, ενώ παράλληλα αξιολογείται η αποδοτικότητα των σχετικών πρωτοβουλιών που έχουν αναπτυχθεί έως σήμερα. Εκτός από τη σχετική νομολογία στην ΕΕ, σαφώς και αναλύεται το σχετικό ισχύον εθνικό δίκαιο, καθόσον αυτό εναρμονίζεται και συμβαδίζει με το αντίστοιχο Ενωσιακό, αλλά αναζητούνται επίσης και άλλα νομοθετικά πλαίσια πέραν των αναφερομένων χώρων, είτε γιατί μπορεί να αποβούν χρήσιμα για την παραγωγή και εφαρμογή τους εντός της ΕΕ ή ακόμη να υπάρχει η γνώση τους σε περιπτώσεις που η ΕΕ απαιτηθεί να θεσπίσει ένα πλαίσιο, για αυτά όταν εισάγονται και χρησιμοποιούνται από τα Κράτη Μέλη.

Η τεχνολογία κατασκευής κατασκοπευτικού λογισμικού επίσης, θα αποτελέσει αντικείμενο της παρούσας μελέτης, τόσο γιατί αποτελεί μέρος του συνόλου μιας ευρύτερης τεχνολογικής ηλεκτρονικής δομής, όσο και το γεγονός ότι για ορισμένες τεχνικές και λογιστικά συστήματα, ήδη υπάρχουν κανονιστικά συστήματα στην ΕΕ που διέπουν τη λειτουργία τους. Έτσι έννοιες όπως αυτές του ηλεκτρονικού εμπορίου, απάτης με υπολογιστή, κυβερνοασφαλειας και Τεχνητής Νοημοσύνης, συμπεριλαμβάνονται λόγω άμεσης συνάφειας και συνύπαρξης με το εξεταζόμενο αντικείμενο.

Επίσης, κρίνεται σκόπιμο, να υπάρχει αναφορά αλλά και διαχωρισμός στη χρήση του λογισμικού κατασκοπείας, όχι τόσο από την πλευρά των στόχων, αλλά κυρίως των φορέων εκμετάλλευσης του λογισμικού κατασκοπείας, με ιδιαίτερη μνεία σε κυβερνητικούς φορείς και υπηρεσίες επιβολής του νόμου, με αναφορά σε χαρακτηριστικές και αμφιλεγόμενες περιπτώσεις εφαρμογής τους.

Στον πυρήνα της παρούσας μελέτης, ιδιαίτερο κεφάλαιο προς εξέταση, θα αποτελέσει το θέμα της παραβίασης και της προστασίας των ατομικών και κοινωνικών θεμελιωδών ελευθεριών, συνεξεταζόμενα με την προστασία του απορρήτου των επικοινωνιών και των προσωπικών δεδομένων.

Απώτερος σκοπός της διπλωματικής εργασίας, είναι μέσα από τα αποτελέσματα των πτυχών που εξετάζονται και αναλύονται, να εξαχθούν τεκμηριωμένα συμπεράσματα, τα οποία θα αποφαίνονται, κατά πόσο τα κανονιστικά και νομοθετικά κείμενα της Ευρωπαϊκής Ένωσης, επαρκούν για τη ρύθμιση της απόκτησης, λειτουργίας και εφαρμογής των κατασκοπευτικών λογισμικών, ή απαιτείται η ανάληψη περαιτέρω πρωτοβουλιών για την ενίσχυσή τους.

ABSTRACT

This master's thesis examines spyware from a European Union perspective, focusing on the forms and extent of its documented use, as well as the legal issues arising from it. Furthermore, the thesis analyzes the institutional and regulatory framework of the European Union (hereinafter: EU) applicable to spyware, while also assessing the effectiveness of the initiatives that have been developed to date to address this phenomenon.

It should be noted that the scope of this thesis is not confined to the national legal order but extends beyond it, taking into account the broader global trend in the use of spyware and the risks this entails for the protection of the confidentiality of communications and personal data.

Moreover, the thesis explores how spyware is often used as a tool for surveillance, the circumvention of safeguards, and political control, leading to the infringement of fundamental rights and the undermining of democratic institutions.

The thesis concludes with the findings derived from the overall analysis and evaluation of these issues, along with the relevant reflections.

ΕΙΣΑΓΩΓΗ

Είναι γεγονός ότι η συνεχώς παρατηρούμενη ραγδαία εξάπλωση της ψηφιακής τεχνολογίας, έχει μεταβάλει σε σημαντικό βαθμό τον τρόπο με τον οποίο οι άνθρωποι επικοινωνούν, ανταλλάσσουν, επεξεργάζονται μηνύματα και πληροφορίες και αποκτούν πρόσβαση σε αυτές. Η είσοδος νέων τεχνολογιών, δεν επιφέρει μόνο θετικά αποτελέσματα, αλλά συχνά ακολουθείται από εξελιγμένες εγκληματικές δραστηριότητες. Με την εφεύρεση για παράδειγμα του τηλεφώνου, εμφανίστηκαν οι υποκλοπές, ενώ η χρήση του αυτοκίνητου, οδήγησε σε άλλες μορφές παρανομίας, όπως η οδήγηση υπό την επήρεια μέθης. Διαπιστώνεται έτσι ότι, τα νέα εγκλήματα που διαπράττονται με νέες τεχνολογίες, δεν είναι τίποτα άλλο παρά μια εξελιγμένη εκδοχή των εγκλημάτων, που ήδη απασχολούσαν την κοινωνία και εμφανίζονται με νέα μορφή[1].

Έτσι η ένταξη και η εκτεταμένη χρήση ψηφιακών εργαλείων στην καθημερινότητά μας, παρά τα αδιαμφισβήτητα οφέλη της, είναι συνυφασμένη με τη σημαντική αύξηση κινδύνων, για την ασφάλεια των πληροφοριακών συστημάτων. Η πολυπλοκότητα του λογισμικού υπολογιστών, επιτρέπει σε επιτήδειους, τη χρήση τους ως αυτοτελή ψηφιακά προγράμματα ή τμήματα αυτών για την ανάπτυξη τεχνολογιών παρακολούθησης, με το κατασκοπευτικό λογισμικό να αποτελεί χαρακτηριστικό παράδειγμα, του τρόπου που τα εξελιγμένα εργαλεία κυβερνοχώρου χρησιμοποιούνται για την παρακολούθηση, τον έλεγχο και την καταστολή συγκεκριμένων πληθυσμιακών ομάδων.

Το κατασκοπευτικό λογισμικό (spyware), αποτελεί ειδική κατηγορία κακόβουλου λογισμικού, έχει σκοπό να παρακολουθεί αθόρυβα τη συμπεριφορά των χρηστών, να καταγράφει τις συνήθειες περιήγησης στο διαδίκτυο, καθώς επίσης και να αποσπά τα ευαίσθητα δεδομένα τους, όπως π.χ. κωδικούς πρόσβασης. Συνήθως, οι πληροφορίες που υποκλέπτονται, αποστέλλονται πίσω στον διανομέα του spyware, όπου χρησιμοποιούνται για στοχευμένη διαφήμιση ή μελέτες μάρκετινγκ.[2] Μέσω αυτών, επιτυγχάνεται η μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικές συσκευές των χρηστών-στόχων, με σκοπό την παρακολούθηση της δραστηριότητάς τους, τη συλλογή προσωπικών τους δεδομένων ή και συχνά τον πλήρη έλεγχο των συσκευών αυτών. Αν και η χρήση τέτοιων τεχνολογιών δύναται, υπό προϋποθέσεις, να θεωρηθεί θεμιτή για λόγους Εθνικής Ασφάλειας ή

[1] Simmons R (2016) The Failure of the Computer Fraud and Abuse Act: Time to Take a New Approach to Regulating Computer Crime, George Washington Law Review, Vol. 84: 1703, 2 February 2016, p.1704

[2] Dynamic Spyware Analysis, Available at. https://bitblaze.cs.berkeley.edu/papers/usenix07.pdf

καταπολέμησης σοβαρών αδικημάτων,[3] η ανεξέλεγκτη και καταχρηστική εφαρμογή τους, οδηγεί στη δημιουργία μιας νέας πραγματικότητας, με σοβαρές συνέπειες για την προστασία των προσωπικών δεδομένων, την ελευθερία της έκφρασης και γενικά τη δημιουργία ρωγμών στη θωράκιση των δημοκρατικών θεσμών.

Ζητήματα που άπτονται της ασφάλειας και του σεβασμού των ανθρωπίνων δικαιωμάτων, αποτελούν απαρχής απαραβίαστο θεμέλιο για το άτομο και την κοινωνία γενικότερα, σε όλες τις πολιτισμένες κοινωνικές ομάδες. Η διαπιστωμένη αυξανόμενη χρήση κατασκοπευτικών λογισμικών, αποτελεί ζήτημα μείζονος σημασίας για την Ευρωπαϊκή Ένωση (ΕΕ), καθώς θίγει άμεσα αξίες και αρχές, στις οποίες είναι δομημένη η Ενωσιακή έννομη τάξη. Ειδικότερα, η συστηματική και μυστική παρακολούθηση των υποκειμένων, πλήττει τον πυρήνα των θεμελιωδών δικαιωμάτων, τα οποία κατοχυρώνονται στο Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕΕ), ιδίως το δικαίωμα στο σεβασμό της ιδιωτικής ζωής και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Η στοχοποίηση πολιτικών προσώπων, δημοσιογράφων και κοινωνικών φορέων, επηρεάζει άμεσα την άσκηση της ελευθερίας της έκφρασης και του δικαιώματος στην πληροφόρηση, υπονομεύοντας την εμπιστοσύνη των πολιτών στους δημοκρατικούς θεσμούς και την ποιότητα των δημοκρατικών διαδικασιών. [4]

Η ΕΕ, καλείται να προβεί στην αντιμετώπιση του φαινόμενου των κατασκοπευτικών λογισμικών, με την εκπόνηση ενός ενιαίου και συμπαγούς κανονιστικού πλαισίου, αφού μέχρι σήμερα τουλάχιστον, δεν έχει υπάρξει ειδική και ενιαία ρύθμιση, για τη χρήση τους. Αντίθετα, η αντιμετώπιση του εν λόγω ζητήματος, πραγματοποιείται μάλλον αποσπασματικά, μέσω άλλων κανονιστικών πράξεων και κειμένων, όπως ΧΘΔΕΕ, ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), ο Κανονισμός για την Τεχνητή Νοημοσύνη (ΤΝ), οι οποίες μεταξύ άλλων, περιλαμβάνουν διατάξεις για την προστασία των ατομικών και κοινωνικών δικαιωμάτων.

[3] Setting spyware standards after the Pegasus scandal, EPRS | European Parliamentary Research Service Hendrik Mildebrath, November 2024 available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766262/EPRS_BRI(2024)766262_EN.pdf

[4] The impact of Pegasus on fundamental rights and democratic processes, IPOL, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 -January 2023 available at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

Η ανάλυση των υφιστάμενων νομοθετικών προαναφερόμενων ευρωπαϊκών κειμένων, μαζί με αποφάσεις του Δικαστηρίου της ΕΕ (ΔΕΕ) και του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ), που αντιμετωπίζουν το θέμα του λογισμικού κατασκοπείας, αν και επίπονη κρίνεται αναγκαία, καθόσον οι διατάξεις τους που έχουν αποδειχτεί αποτελεσματικές δύναται να συμπεριληφθούν σε ένα ενιαίο ανεξάρτητο νομοθετικό κείμενο. Παράλληλα για τον έλεγχο και την επιβολή του νόμου, κρίνεται σκόπιμη η αξιολόγηση των συσταθέντων μηχανισμών προστασίας, ως προς την επάρκεια και την αποτελεσματικότητά τους.

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ: ΕΙΣΑΓΩΓΗ ΣΤΑ ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ

1.1 Ορισμοί – Γενική περιγραφή

Ο όρος κακόβουλο λογισμικό (malware), χρησιμοποιείται για να περιγράψει κάθε μορφή κώδικα ή προγράμματος, που έχει σχεδιαστεί για να επιτρέπει στον εισβολέα ,την πρόκληση σημαντικής ζημιάς ή καταστροφής προγράμματος σε υπολογιστές, κινητές ηλεκτρονικές συσκευές και δίκτυα ή την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε αυτές, με σκοπό την απόσπαση πληροφοριών, τις οποίες διαθέτει σε τρίτους με χρηματικό αντάλλαγμα ή ακόμη μπορεί και να εκβιάζει τους νόμιμους χρήστες των προσβαλλομένων προγραμμάτων[5]. Σύμφωνα με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών/ European Union Agency for Cybersecurity (ENISA), ένα πρόγραμμα θεωρείται κακόβουλο, εφόσον πληροί ένα από τα δύο ακόλουθα κριτήρια: είτε είναι εχθρικό ή παρεμβατικό, είτε έχει εγκατασταθεί σε ηλεκτρονική συσκευή, χωρίς τη συναίνεση του χρήστη. Οι επιθέσεις μέσω κακόβουλων λογισμικών, αποτελούν συχνό φαινόμενο στο κυβερνοχώρο, αποτελώντας πλέον ένα από τα σημαντικότερα εγκλήματα που διαπράττονται μέσω υπολογιστή. Οι τύποι κακόβουλων λογισμικών ποικίλλουν, δεδομένης της διαρκούς και αλματώδους ανάπτυξης της τεχνολογίας. Συναντάται με διάφορες μορφές εκ των οποίων, οι περισσότερο γνωστές είναι ο ιός (virus), το σκουλήκι (worm), ο Δούρειος Ίππος (Trojan Horse), το λογισμικό παρακολούθησης (spyware), το διαδικτυακό ρομπότ (bot), το λυτρισμικό (ransomware) και τα Rootkits[6].

Όπως βλέπουμε λοιπόν, το κατασκοπευτικό λογισμικό (spyware), αποτελεί μια μορφή κακόβουλου λογισμικού και ορίζεται ως ένα κακόβουλο πρόγραμμα, το οποίο εγκαθίσταται σε μια ηλεκτρονική συσκευή, με κύριο σκοπό την παρακολούθηση και καταγραφή της δραστηριότητας του χρήστη, χωρίς τη γνώση ή τη συναίνεσή του. Από πλευράς δε ορολογίας, συναντάται και ως κακόβουλο λογισμικό κατασκοπείας. Η λειτουργία του, βασίζεται στην εκμετάλλευση δυνατότητων του πληροφοριακού συστήματος, με αποτέλεσμα τη συλλογή δεδομένων, που αφορούν τη συμπεριφορά και τις ενέργειες του χρήστη. Το λογισμικό κατασκοπείας, δύναται να επηρεάζει τη λειτουργία και την ασφάλεια της ηλεκτρονικής συσκευής ή του δικτύου, καθώς και να διευκολύνει τη διαβίβαση ευαίσθητων ή ιδιωτικών πληροφοριών σε τρίτα πρόσωπα, εν αγνοία του χρήστη. Η εξάπλωσή του, μπορεί να πραγματοποιείται μέσω της ενσωμάτωσης του σε ένα φαινομενικά νόμιμο λογισμικό, μέσω

[5] https://www.microsoft.com/en-us/security/business/security-101/what-is-malware
[6] https://www.kaspersky.com/resource-center/threats/types-of-malware

παραπλανητικών εφαρμογών, μέσω Δούρειων Ίππων ή με την εκμετάλλευση ευπαθειών των πληροφοριακών συστημάτων[7]. Καθίσταται λοιπόν σαφές, ότι το κατασκοπευτικό λογισμικό, συνιστά σοβαρή απειλή για την ιδιωτικότητα, την ασφάλεια και την ακεραιότητα των δεδομένων και την εμπιστευτικότητα των ηλεκτρονικών επικοινωνιών.

Αν και δεν είναι εύκολη η διατύπωση διαφοροποιήσεων μεταξύ του κατασκοπευτικού λογισμικού από του κακόβουλου, εντούτοις δύναται αυτό να εστιαστεί σε δύο κυρίως λεπτομέρειες. Στο γεγονός ότι το πρώτο εισχωρεί στον υπολογιστή του χρήστη, χωρίς την αντίληψη ή τη συναίνεσή του και λειτουργεί χωρίς να απαιτηθεί κάποια περαιτέρω ενέργεια στο υπολογιστικό σύστημα. Το δεύτερο έχει να κάνει με τη λειτουργία του προσβαλλόμενου υπολογιστή, όπου το spyware σε αντίθεση με τους άλλους τύπους malware, δεν προκαλεί κάποια βλάβη[8].

Τα εν λόγω λογισμικά έχουν το ιδιαίτερο χαρακτηριστικό, ότι λειτουργούν κρυφά και αθέατα, αφήνοντας ελάχιστα έως και μηδαμινά ίχνη στη μολυσμένη συσκευή, γεγονός που καθιστά τον άμεσο και εύκολο εντοπισμό τους από το θύμα, εξαιρετικά δυσχερή [9]. Με τον τρόπο αυτό, διεισδύουν στις ηλεκτρονικές συσκευές των χρηστών και αποκτούν πρόσβαση σε ένα ευρύ φάσμα πληροφοριών, συμπεριλαμβανομένων, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, ιστορικό κλήσεων και δεδομένα περιήγησης στο διαδίκτυο. Δεν αποκλείεται, μάλιστα, η πρόσβαση και σε δεδομένα που προέρχονται από κρυπτογραφημένες εφαρμογές ανταλλαγής μηνυμάτων, όπως το WhatsApp. Οι πληροφορίες αυτές αποτελούν δεδομένα προσωπικού χαρακτήρα, με ορισμένα εξ' αυτών να εντάσσονται σε ειδικές κατηγορίες προσωπικών δεδομένων, όπως τραπεζικά στοιχεία, καθώς και δεδομένα, τα οποία ο ίδιος ο χρήστης αποκαλύπτει κατά τη διάρκεια τηλεφωνικών συνομιλιών του, οι οποίες δύνανται να παρακολουθούνται από κάποιο κατασκοπευτικό λογισμικό.

Η χρήση του κατασκοπευτικού λογισμικού, δεν περιορίζεται στην απλή παρακολούθηση των ηλεκτρονικών συσκευών των χρηστών, αλλά οι λειτουργίες του δύνανται να εκτείνονται σημαντικά πέραν αυτής. Ειδικότερα, με την ενσωμάτωση ενός κατασκοπευτικού λογισμικού σε μια ηλεκτρονική συσκευή, δεν αποκλείεται η εγκατάσταση επιπρόσθετων κακόβουλων λογισμικών ή λειτουργικών ενοτήτων, οι οποίες ενισχύουν την δυνατότητα του δράστη, να αποκτήσει εξ' αποστάσεως τον πλήρη έλεγχο της συσκευής, να προβαίνει αιφνιδίως στην

[7] Θεοχάρης Ι. Δαλακούρας, Ηλεκτρονικό Έγκλημα , Νομική Βιβλιοθήκη, σελ.9.
[8] https://www.cybersecurity-automation.com/what-is-the-difference-between-malware-vs-spyware/
[9] Dynamic Spyware Analysis, Available at. https://bitblaze.cs.berkeley.edu/papers/usenix07.pdf

ενεργοποίηση του μικροφώνου ή της κάμερας, να παρακολουθεί την καταγραφή του πληκτρολογίου, καθώς και να τροποποιεί ή να διαγράφει αποθηκευμένα δεδομένα. Συνεπώς, το κατασκοπευτικό λογισμικό, δύναται να μετατραπεί σε ένα εργαλείο διαρκούς και πλήρους επιτήρησης του χρήστη, συνοδευόμενο από άκρως σοβαρές επιπτώσεις στην ιδιωτική του ζωή και την προστασία των προσωπικών του δεδομένων[10].

Τέλος, αξίζει να επισημανθεί ότι, ορισμένες φορές, η χρήση των κατασκοπευτικών λογισμικών, υπερβαίνει τα όρια της ιδιωτικής παρακολούθησης και μετατρέπεται σε εργαλείο κρατικών φορέων, με το οποίο επιτυγχάνεται η συστηματική παρακολούθηση των χρηστών-στόχων, γεγονός το οποίο συνεπάγεται σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και καθιστά αναγκαία την ενδελεχή νομική αξιολόγηση τους.

1.2 Εξέλιξη του φαινομένου

Το κακόβουλο λογισμικό εμφανίζεται να προσδιορίζεται αρχικά εννοιολογικά σε σειρά διαλέξεων του μαθηματικού Τζον φον Νόιμαν (John von Neumann), στα τέλη της δεκαετίας του 1940 και αργότερα το 1966, με τη δημοσίευση της θεωρίας των «Αυτοαναπαραγόμενων Αυτόματων, (Theory of Self-Reproducing Automata)». Η εργασία ήταν ένα νοητικό πείραμα, που προέβλεπε ότι θα ήταν δυνατό για έναν τμήμα κώδικα υπολογιστή, να αντιγράψει τον εαυτό του και να προκαλέσει βλάβη σε άλλους υπολογιστές, με μόλυνση νέων ξενιστών, όπως ακριβώς λειτουργεί και ένας βιολογικός ιός[11]. Η πρώτη εφαρμογή κακόβουλου λογισμικού έγινε στην πράξη το 1971, με τον πρώτο ιό στον κόσμο, τον Creeper. Με τα δεδομένα σήμερα, ο εν λόγω ιός θα μπορούσε να χαρακτηριστεί ως «σκουλήκι», αφού είχε την ιδιότητα να εξαπλώνεται σε άλλους υπολογιστές, μέσα από τοπικά δίκτυα. Ο Creeper αναπτύχθηκε από τον Bob Thomas, ο οποίος εργαζόταν σε μια εταιρεία που ονομάζεται BBN Technologies, ως εφαρμογή για λογισμικό κινητών, που μπορούσε να μεταδίδεται αυτόματα μεταξύ υπολογιστών σε ένα δίκτυο. Ο ιός Creeper δεν προκαλούσε βλάβη σε υπολογιστικά συστήματα, παρά μόνο άφηνε το μήνυμα «Είμαι ο Creeper πιάσε με αν μπορείς» και προσπαθούσε να εντοπίσει άλλον συνδεδεμένο υπολογιστή για να μεταπηδήσει[12] .

[10] https://www.sei.cmu.edu/documents/266/2005_019_001_50318.pdf

[11]https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

[12] https://www.avg.com/en/signal/history-of-viruses

Μέσα σε λίγα χρόνια, οι μολύνσεις εξαπλώθηκαν ευρέως και μέχρι τα μέσα της δεκαετίας του 2000, μεγάλος αριθμός χρηστών, χρησιμοποιούσαν παραβιασμένα συστήματα, χωρίς να το συνειδητοποιούν. Αυτό που ξεκίνησε ως ενόχληση, έγινε πιο σοβαρό στις δεκαετίες του 2010 και του 2020, καθώς το spyware εξελίχθηκε σε πλατφόρμες επιτήρησης πλήρους κλίμακας, ως κυβερνητικό εργαλείο.

Η λέξη spyware, αποτέλεσε για πρώτη φορά αντικείμενο δημοσίου ενδιαφέροντος τον Οκτώβριο του 1995 και συγκεκριμένα στο Usenet[13], ένα παγκόσμιο σύστημα συζήτησης στο Διαδίκτυο, που επιτρέπει στους χρήστες να δημοσιεύουν μηνύματα και να κατεβάζουν αρχεία, οργανωμένα σε διάφορες κατηγορίες, γνωστές ως ομάδες συζήτησης. Στις αρχές του 2000, ο ίδιος όρος χρησιμοποιήθηκε από τον ιδρυτή της εταιρείας Zone Labs, Gregor Freund, σε ένα δελτίο ειδήσεων για το Zone Alarm Personal Firewall, σηματοδοτώντας την έναρξη της σύγχρονης χρήσης της λέξης. Την ίδια εποχή το έργο OptOut του Steve Gibson, άρχισε να στρέφει την προσοχή στο λογισμικό κρυφής παρακολούθησης, συνδέοντας τον όρο «spyware» με την έννοια της Κυβερνοασφάλειας[14].

Το 2005 η American Online (AOL) και η National Cyber-Security Alliance (NCSA), δημοσίευσαν μια μελέτη, σύμφωνα με την οποία, περισσότεροι από τους μισούς υπολογιστές των χρηστών που συμμετείχαν στην έρευνα, είχαν μολυνθεί με κάποιο είδος κατασκοπευτικού λογισμικού είχαν ένα τέτοιο πρόγραμμα στον οικιακό τους υπολογιστή. Η ερώτηση που τέθηκε στους ερωτηθέντες ήταν κατά πόσο γνώριζαν την ύπαρξη spyware ή adware στον υπολογιστή τους και το 46% είπε ναι. Στη συνέχεια, η ομάδα AOL/NCSA, πέρασε και έκανε μια άμεση σάρωση του οικιακού υπολογιστή των ατόμων που συμμετείχαν στην έρευνα, για να ελέγξει την απάντησή του και διαπιστώθηκε σε πολύ περισσότερους ανθρώπους (ποσοστό 62%) υπήρξε εισβολή spyware ή adware. Στη συνέχεια η ομάδα AOL/NCSA, έδειξε σε κάθε ερωτηθέντα τα αποτελέσματα της σάρωσης και έκανε μερικές επόμενες ερωτήσεις, όπου το 92% των ερωτηθέντων, δήλωσε ότι δεν γνώριζε για την ύπαρξη των προγραμμάτων και το 91%, ότι δεν είχε δώσει άδεια σε κάποιον να εγκαταστήσει αυτά τα προγράμματα [15] .

[13] Ιδρυτές του Usenet, υπήρξαν δύο μεταπτυχιακοί φοιτητές του Πανεπιστημίου Duke, οι Tom Truscott και ο Jim Ellis, οι οποίοι συνέλαβαν την ιδέα το 1979 και υλοποιήθηκε το 1980, με το οποίο επιδίωκαν τη διασυνοριακή ανταλλαγή πληροφοριών, αποτελώντας ουσιαστικά την πρώτη διαδικτυακή κοινότητα.

[14] https://guardiandigital.com/resources/blog/spyware

[15] https://www.pewresearch.org/internet/2006/02/22/invasion-of-the-computer-snatchers/

Με την πάροδο των χρόνων, το κατασκοπευτικό λογισμικό εξελίχθηκε σε έναν από τους πιο διαδεδομένους όρους και συνάμα, μια από τις σημαντικότερες απειλές στο Διαδίκτυο. Η εξέλιξη αυτή, είχε ως αποτέλεσμα τη διαρκή αύξηση των επιθέσεων σε πληροφοριακά συστήματα, με συχνό στόχο υπολογιστές που χρησιμοποιούσαν ως κύριο πρόγραμμα περιήγησης τον Internet Explorer (IE), ο οποίος, κατά την περίοδο εκείνη, παρουσίαζε περιορισμένες δυνατότητες ασφαλείας, γεγονός που καθιστούσε ευκολότερη την εξάπλωση του φαινομένου αυτού. [16]

1.3 Σύγχρονες μορφές κατασκοπευτικού λογισμικού

Στο πλαίσιο αυτό, το ενδιαφέρον μετατοπίζεται από τη γενική ιστορική εξέλιξη του λογισμικού κατασκοπείας στις μορφές που δύναται να παρουσιαστεί. Οι κατηγορίες του κατασκοπευτικού λογισμικού ποικίλλουν, καθώς ο αριθμός των παραλλαγών του δεν μπορεί να προσδιοριστεί με ακρίβεια, λόγω της ραγδαίας ανάπτυξης της τεχνολογίας και κυρίως της πολυπλοκότητας του διαδικτύου. Οι επιτιθέμενοι χρησιμοποιούν ολοένα και πιο προηγμένα τεχνολογικά μέσα, με απώτερο σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης στην κινητή συσκευή του θύματος και την παρακολούθησή του εν αγνοία του. Συγκεκριμένα, η κάθε μορφή κατασκοπευτικού λογισμικού, έχει σχεδιαστεί για να επιτελεί μια συγκεκριμένη λειτουργία. Οι πιο διαδεδομένες μορφές είναι οι εξής:

- **Adware:** Το λογισμικό αυτό εμφανίζει ανεπιθύμητες διαφημίσεις στην οθόνη του υπολογιστή ή της κινητής συσκευής του χρήστη. Συγκεκριμένα, ανακατευθύνει τα αποτελέσματα αναζήτησης σε ιστότοπους διαφημιστικού περιεχομένου και συλλέγει δεδομένα χρηστών για σκοπούς μάρκετινγκ. Ορισμένες μορφές του είναι ιδιαίτερα παρεμβατικές και δύναται να λειτουργήσουν ως δίαυλος, για την ενσωμάτωση κακόβουλων λογισμικών. [17]

- **Information stealer/ Infostealer:** Αυτός ο τύπος κατασκοπευτικού λογισμικού, έχει σχεδιαστεί για να συλλέγει κρυφά ευαίσθητα δεδομένα από τη συσκευή του θύματος και να τα μεταφέρει σε τρίτους προς εκμετάλλευση. Ειδικότερα, δύναται να κλέψει προσωπικές πληροφορίες, όπως ονόματα χρήστη, κωδικούς πρόσβασης, οικονομικά στοιχεία, ιστορικό προγράμματος περιήγησης κλπ. [18].

---

[16] https://www.wired.com/story/internet-explorer-browser-dead/
[17] Kaspersky Διαθέσιμο στο: https://www.kaspersky.com/resource-center/threats/adware
[18] North Dakota Information Technology Διαθέσιμο στο: https://www.ndit.nd.gov/news/information-stealers

• **Keyloggers:** Οι καταγραφείς πληκτρολόγησης, αποτελούν μια κατηγορία κατασκοπευτικού λογισμικού, που χρησιμοποιείται για την υποκλοπή δεδομένων, όπως κωδικούς πρόσβασης, ονόματα χρήστη κλπ. Ειδικότερα, λειτουργούν καταγράφοντας τις πληκτρολογήσεις που πραγματοποιεί ο χρήστης στη μολυσμένη συσκευή του και στη συνέχεια, αποθηκεύουν τα δεδομένα σε ένα κρυπτογραφημένο αρχείο καταγραφής. [19]

• **Rootkits**: Πρόκειται για συλλογές λογισμικού, που επιτρέπουν στους εισβολείς να διεισδύουν στη συσκευή του θύματος, εκμεταλλευόμενοι ευπάθειες του συστήματος ή συνδεόμενοι σε μηχανήματα ως διαχειριστές. Μπορούν να αποκρύπτουν αρχεία, να συγκαλύπτουν την παρουσία ενός εισβολέα στο σύστημα ή να κρύβουν οποιεσδήποτε διεργασίες βρίσκονται σε εκτέλεση. Τα rootkits είναι συχνά δύσκολο ή και αδύνατο να εντοπιστούν και για το λόγο αυτό είναι ιδιαίτερα επικίνδυνα, επειδή έχουν σχεδιαστεί ακριβώς για να κρύβουν την παρουσία τους στη συσκευή που εγκαθίστανται.[20]

• **Trojan Horse Virus:** Πρόκειται για ένα λογισμικό, το οποίο ενσωματώνεται σε νόμιμα αρχεία ή εφαρμογές, με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης στη συσκευή του χρήστη. Σε ορισμένες περιπτώσεις, δύναται να χρησιμοποιεί την ονομασία ήδη υπαρχόντων ή τυπικών αρχείων του λειτουργικού συστήματος. Ο συγκεκριμένος τύπος κακόβουλου λογισμικού, λαμβάνει τη μορφή ενός φαινομενικά νόμιμου προγράμματος, γεγονός που καθιστά δυσχερή τον εντοπισμό του από το χρήστη, με αποτέλεσμα να έχουν ήδη προκληθεί σοβαρές ζημιές σε αυτή π.χ. κλοπή δεδομένων. [21]

• **Red Shell Spyware:** Είναι ένας τύπος κακόβουλου λογισμικού, που μεταφέρεται με την εγκατάσταση ορισμένων παιχνιδιών υπολογιστή (PC Games) και στη συνέχεια, παρακολουθεί τις διαδικτυακές δραστηριότητες των παικτών. Η ενσωμάτωσή του στα προγράμματα παιχνιδιών, γίνεται με πρόφαση τη βελτίωση της απόδοσής τους, χωρίς τη συγκατάθεση των χρηστών, που έχουν προμηθευτεί νόμιμα το παιχνίδι[22].

---

[19] Fortinet Διαθέσιμο στο https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers

[20] Malwarebytes, available at Rootkit | What is a Rootkit? | Malwarebytes

[21] Malicious software, Train the trainer reference guide, European Network and Information Security Agency (ENISA) σελ. 16, Διαθέσιμο στο: https://www.enisa.europa.eu/sites/default/files/all_files/Malicious%20software_Train%20the%20trainer%20guide.pdf

[22] https://www.avast.com/c-spyware

Σημειώνεται, ότι καμία κατηγορία δεν αποτελεί προϋπόθεση της άλλης, καθώς είναι ανεξάρτητες, γεγονός που σημαίνει ότι περισσότερες από μία, μπορούν να συνυπάρχουν ταυτόχρονα, σε μία ηλεκτρονική συσκευή.

Τέλος, υπογραμμίζεται, ότι πιθανόν να υπάρχουν και να λειτουργούν έγκυρες εφαρμογές spyware, που δεν χαρακτηρίζονται κακόβουλες. Για παράδειγμα, ο εργοδότης μιας επιχείρησης, μπορεί να χρησιμοποιεί spyware για την παρακολούθηση συσκευών υπαλλήλων, με στόχο την προστασία ιδιόκτητων πληροφοριών ή εμπορικών μυστικών, καθώς και για τη διασφάλιση της λειτουργίας του δικτύου της εταιρείας. Επίσης σε περιπτώσεις γονικού ελέγχου, όπου περιορίζεται η χρήση μιας συσκευής ή αποκλείεται ακατάλληλο περιεχόμενο, μπορεί να μιλάμε επίσης μια νόμιμη μορφή spyware[23].

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ: ΤΡΟΠΟΣ ΚΑΙ ΠΕΔΙΟ ΔΡΑΣΗΣ ΚΑΤΑΣΚΟΠΕΥΤΙΚΩΝ ΛΟΓΙΣΜΙΚΩΝ

2.1 Τρόπος δράσης κατασκοπευτικών λογισμικών

Ο τρόπος με τον οποίο λειτουργεί ένα κατασκοπευτικό λογισμικό, είναι σύνθετος και πολυδιάστατος και συχνά συγχέεται με τον τρόπο λειτουργίας των ιών. Ωστόσο, το κατασκοπευτικό λογισμικό, δεν έχει ως κύριο σκοπό την πρόκληση άμεσης βλάβης στη λειτουργία ενός συστήματος, αλλά την παρακολούθηση και συλλογή δεδομένων. Η λειτουργία του κατασκοπευτικού λογισμικού, ακολουθεί συνήθως μια διαδικασία τριών βασικών σταδίων. Αρχικά, διεισδύει στη συσκευή μέσω κακόβουλων εφαρμογών, μολυσμένων ιστότοπων ή συνημμένων αρχείων. Στη συνέχεια, αφού εγκατασταθεί, παρακολουθεί και καταγράφει τη δραστηριότητα του χρήστη, αξιοποιώντας τεχνικές όπως η καταγραφή πληκτρολογήσεων και η συλλογή δεδομένων περιήγησης. Τέλος, οι πληροφορίες που συγκεντρώνονται, αποστέλλονται στον εισβολέα, ο οποίος είτε τις χρησιμοποιεί για περαιτέρω κακόβουλες ενέργειες, είτε τις παραχωρεί με τίμημα σε τρίτους[24].

Μεγάλος αριθμός χρηστών υπολογιστών και ηλεκτρονικών συσκευών, συχνά συγχέουν το κακόβουλο λογισμικό και το κατασκοπευτικό λογισμικό, έχοντας την εντύπωση ότι πρόκειται για το ίδιο πράγμα. Αυτό συμβαίνει, γιατί μπορεί μερικές φορές και τα δύο, να χρησιμοποιούν κοινές μεθόδους προσκόλλησης σε ένα πρόγραμμα ή ένα email. Η

[23] https://www.avast.com/c-spyware
[24] https://www.enterprisenetworkingplanet.com/security/what-is-spyware/

αλήθεια είναι, ότι το κακόβουλο λογισμικό και το spyware ως μια υποκατηγορία του πρώτου, εργαλειοποιούνται από εισβολείς, (χακερς/hackers), για την κλοπή ευαίσθητων πληροφοριών από έναν μολυσμένο υπολογιστή. Υπάρχουν διαφορές μεταξύ τους, όπως αναφέρθηκαν και με εκ νέου επισήμανση ότι, το spyware χρησιμοποιεί την κίνηση ιστού για την εξάπλωσή του και χωρίς την σχετική ενημέρωση και συναίνεση του χρήστη, στοχεύοντας σε αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης και άλλες προσωπικές πληροφορίες χωρίς τη συγκατάθεσή του. Συνήθως, ένα κατασκοπευτικό λογισμικό, καταλήγει να διεισδύει σε μια ηλεκτρονική συσκευή, εξαιτίας κάποιας συγκεκριμένης ενέργειας του χρήστη, όπως το πάτημα ενός κουμπιού σε ένα αναδυόμενο παράθυρο, η εγκατάσταση ενός πακέτου λογισμικού ή η αποδοχή προσθήκης λειτουργιών σε ένα πρόγραμμα περιήγησης στο διαδίκτυο. Οι εισβολείς μπορούν να εισάγουν ενσωματωμένους κώδικες σε νόμιμους ιστότοπους, οι οποίοι με τη σειρά τους μεταφέρουν κακόβουλο λογισμικό που φιλοξενούν, σε άλλους ιστότοπους κατά τις επισκέψεις που δέχονται. Αυτές οι εφαρμογές, χρησιμοποιούν συχνά τεχνάσματα, για να παραπλανούν τους χρήστες και να τους οδηγούν στην εγκατάσταση τους, όπως ψεύτικα μηνύματα ειδοποίησης συστήματος ή κουμπιά που εμφανίζονται ως «ακύρωση», ενώ στην πραγματικότητα εγκαθιστούν κατασκοπευτικό λογισμικό [25].

Μια μέθοδος με την οποία ένα κατασκοπευτικό λογισμικό εγκαθίσταται και εξαπλώνεται σε ένα σύστημα, αποτελεί το “drive by download attack”. Αυτό μπορεί να συμβεί απλώς και μόνο με την επίσκεψη σε έναν νόμιμο αλλά παραβιασμένο ιστότοπο, χωρίς ο χρήστης να κατεβάσει ή να εκτελέσει κάποιο αρχείο συνειδητά. Όταν ο χρήστης εισέλθει στον ιστότοπο, ο κακόβουλος κώδικας εκμεταλλευόμενος τις αδυναμίες ή άλλα τρωτά σημεία του προγράμματος περιήγησης του χρήστη, επιτρέπει τη λήψη κατασκοπευτικού λογισμικού στον υπολογιστή του. Τα εισερχόμενα κακόβουλα αρχεία επιτρέπουν στους εισβολείς, να αποκτήσουν πλήρη πρόσβαση και έλεγχο του υπολογιστή του χρήστη, είτε για να κλέψουν πολύτιμες πληροφορίες, είτε για να εξαπολύσουν επιθέσεις εναντίον άλλων χρηστών στο διαδίκτυο. Για παράδειγμα σε ιστότοπους διαφημίσεων, όταν ένας χρήστης βλέπει μια διαφήμιση, το κακόβουλο λογισμικό μπορεί να μολύνει τον υπολογιστή του.

[25] https://www.cybersecurity-automation.com/what-is-the-difference-between-malware-vs-spyware/

Η Βελτιστοποίηση Μηχανών Αναζήτησης/Search Engine Optimisation (SEO), είναι μια άλλη τεχνική που χρησιμοποιείται συχνά σε συνδυασμό με τη μέθοδο drive-by download, η οποία αυξάνει τον αριθμό και την προτεραιότητα ως προς τη σειρά προβολής σε ένα ιστότοπο. Εύλογο είναι ότι μια ιστοσελίδα που εμφανίζεται στις πρώτες σειρές της μηχανής αναζήτησης και πιο συχνά, προτιμάται από τους χάκερς για ενσωμάτωση κακόβουλου λογισμικού. Υπάρχουν διαθέσιμα πακέτα κακόβουλου λογισμικού (malware kits), που έχουν στόχο συγκεκριμένα προγράμματα περιήγησης του διαδικτύου, εκμεταλλευόμενα τα τυχόν ελαττώματα του λογισμικού[26].

Επίσης, με το drive-by download attack, συνεργάζεται και μια άλλη διαδεδομένη μέθοδος, γνωστή ως bundleware, όπου το spyware ενσωματώνεται σε κατά τα λοιπά νόμιμο, συνήθως δωρεάν λογισμικό ή ενημερώσεις, που ο χρήστης εγκαθιστά, κατόπιν εσφαλμένης διαπίστωσης ότι διατίθενται από αξιόπιστες πηγές. Το εν λόγω λογισμικό, αποτελεί τμήμα άλλου λογισμικού και το οποίο το drive-by download, προσπαθεί να εγκαταστήσει μέσω από μια άσχετη ιστοσελίδα, που συχνά εμφανίζεται από διαφημίσεις τρίτων, για το άνοιγμα της οποίας ο χρήστης, πρέπει να αποδεχτεί τη φόρτωση άγνωστού προγράμματος που στην ουσία πρόκειται για το κακόβουλο λογισμικό bundleware. Η επιθετική τακτική drive-by download, χρησιμοποιεί τακτικές εξαναγκασμού, για να προσπαθήσει να κάνει τον χρήστη να αποδεχτεί το κατέβασμα του αρχείου spyware, πατώντας στο "Ναι" και όταν ο χρήστης δεν επιτρέπει τη λήψη, προβαίνει επανειλημμένα στο άνοιγμα παράθυρων σφάλματος[27].

Ένας άλλος τρόπος διάδοσης, αποτελεί το φαινόμενο του piggybacking.[28] Στον τομέα της Κυβερνοασφάλειας, ο όρος χρησιμοποιείται για να περιγράψει την πρακτική κατά την οποία, ένας εισβολέας εκμεταλλεύεται την ήδη νόμιμη και πιστοποιημένη πρόσβαση ενός χρήστη σε ένα σύστημα, προκειμένου να αποκτήσει μη εξουσιοδοτημένη πρόσβαση, χωρίς να υποβληθεί σε διαδικασία αυθεντικοποίησης. «Το να κρατάτε μια πόρτα ανοιχτή για το άτομο πίσω σας μπορεί να φαίνεται ευγενικό, αλλά μπορεί να οδηγήσει σε σοβαρή

[26]Australian Signals Directorate, "Mitigating Drive-by Downloads", Oct. 2021, p. 1,2 Available at https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Mitigating%20Drive-by%20Downloads%20%28October%202021%29.pdf

[27]https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?params=/context/sis_research/article/10899/&path_info=1076211.1076245.pdf

[28]https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/tailgating-piggybacking-attack/

παραβίαση της ασφάλειας στον χώρο εργασίας»[29]. Η πρόσβαση επιτυγχάνεται μέσα από ανοικτό (ξεκλείδωτο), μη ασφαλές δίκτυο (Wi-Fi). Επίσης ο χάκερ, μπορεί να αποκτήσει πρόσβαση μέσω ενός εξουσιοδοτημένου χρήστη, ο οποίος έχει συνδεθεί σε μια συσκευή και στη συνέχεια απομακρύνεται από το σύστημα, αφήνοντας ανοιχτό το πεδίο για τον «επιτιθέμενο», να εισέλθει και να αποσπάσει και στοιχεία αυθεντικότητας και άλλες πληροφορίες. Διευκρινίζεται ότι, σε ορισμένες περιπτώσεις, η πρακτική αυτή μπορεί να συνδυάζεται με την εγκατάσταση ενός φαινομενικά νόμιμου λογισμικού, μέσω του οποίου εγκαθίστανται ταυτόχρονα επιπρόσθετα κακόβουλα προγράμματα, χωρίς τη γνώση του χρήστη[30].

Ενδείξεις ότι ένας υπολογιστής μπορεί να έχει μολυνθεί με spyware, είναι η περίπτωση μια ξαφνική καταιγίδα αναδυόμενων διαφημίσεων, καθώς και η μεταφορά σε ιστότοπους, που δεν επιθυμεί ο χρήστης να εισέλθει και γενικά κάθε διαπιστούμενη μη τεχνική, επιβράδυνση της απόδοσης στην περιήγηση στο διαδίκτυο[31].

Μια άλλη παράμετρος που κρίνεται αναγκαίο να ληφθεί υπόψη στα μέχρι τώρα δεδομένα και εμπειρίες από τη δράση του κακόβουλου λογισμικού κατασκοπείας, είναι η ανάπτυξη της ΤΝ και κατά πόσο οι εφαρμογές της μπορούν να εξελίξουν περαιτέρω το φαινόμενο αυτό. Τα συστήματα Τεχνητής Νοημοσύνης μπορούν να προκαλέσουν αυξημένο κίνδυνο σε θέματα Κυβερνοασφάλειας λόγω της δυνατότητας ευρείας κλίμακας επεξεργασίας δεδομένων και της πολυπλοκότητας των συστημάτων που εμπλέκονται. Σε αντίθεση με τα παραδοσιακά συστήματα, τα μοντέλα αυτά είναι ιδιαίτερα ευάλωτα τόσο από πλευράς εκμετάλλευσης κατά τις διαδικασίες μάθησης, όσο και στα δεδομένα που χρησιμοποιούν για τη λειτουργία τους. Οι χάκερς ενδέχεται να χειραγωγήσουν ή να κάνουν κακή χρήση των συστημάτων Τεχνητής Νοημοσύνης μέσω της παρέμβασης στα δεδομένα ή παρακάμπτοντας τις προδιαγραφές των μοντέλων για την εξαγωγή ευαίσθητων πληροφοριών[32].

---

[29] https://www.dla.mil/About-DLA/News/News-Article-View/Article/3559637/piggybacking-can-open-doors-to-security-problems/

[30] https://cyberhoot.com/el/cybrary/piggybacking/

[31] California Department of Justice, Office of the Attorney General, "Tips for Consumers- Consumer Information Sheet 12", Jan. 2015, p.1 Available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/CIS_12_Computer_protection_DOJ.pdf

[32] European Data Protection Board (by Dr. Enrico GLEREAN), "Training curriculum on AI and data protection Fundamentals of Secure AI Systems with Personal Data", p.45, available at.

2.2 Μηχανισμοί αντιμετώπισης

Η προστασία από την εγκληματικότητα στο περιβάλλον του διαδικτύου και των υπολογιστών, μεμονωμένων ή δικτύων, προφανώς και αποτελεί μέλημα όλων όσων βρίσκονται στην πλευρά των στοχοποιημένων ατόμων ή ομάδων.

Για την αντιμετώπιση του φαινομένου αυτού, κυβερνητικοί οργανισμοί, εταιρείες και προγραμματιστές, έχουν αναπτύξει και θέσει σε εφαρμογή εξειδικευμένα λογισμικά anti-spyware, τα οποία έχουν σχεδιαστεί για την ανίχνευση, την αποτροπή, καθώς και τον εντοπισμό και την αφαίρεση των κατασκοπευτικών λογισμικών, από τις ηλεκτρονικές συσκευές. Τα εν λόγω λογισμικά, λειτουργούν τόσο προληπτικά, αποτρέποντας την εγκατάσταση κακόβουλων εφαρμογών, όσο και κατασταλτικά, καταργώντας τα ήδη υπάρχοντα λογισμικά που βρίσκονται εγκατεστημένα στη συσκευή. Ειδικότερα, η λειτουργία των λογισμικών anti-spyware, περιλαμβάνει τρία βασικά στάδια. Αρχικά, παρακολουθούν σε πραγματικό χρόνο τη συσκευή για ύποπτη δραστηριότητα, αποτρέποντας την εγκατάσταση απειλών. Στη συνέχεια, πραγματοποιούν περιοδικές σαρώσεις για τον εντοπισμό γνωστών spyware, ενώ τα πιο προηγμένα εργαλεία αξιοποιούν αλγορίθμους μηχανικής μάθησης για την ανίχνευση άγνωστων απειλών. Τέλος, μόλις εντοπιστεί μια απειλή, το λογισμικό ενημερώνει τον χρήστη και προχωρά στην οριστική αφαίρεσή της, διασφαλίζοντας την προστασία του συστήματος.[33]

Ένα πρόγραμμα anti-spyware, δεν αρκεί για την αποτελεσματική αντιμετώπιση και καταστολή του φαινομένου των κατασκοπευτικών λογισμικών. Στο πλαίσιο αυτό, καθοριστικό ρόλο διαδραματίζει και η συμπεριφορά των χρηστών κατά την περιήγησή τους στο Διαδίκτυο. Ειδικότερα, οι χρήστες οφείλουν να μεριμνούν για την τακτική ενημέρωση του λειτουργικού συστήματος και των εφαρμογών τους, καθώς και να επιδεικνύουν τη δέουσα προσοχή, κατά τη λήψη αρχείων και την επίσκεψή τους σε ιστοσελίδες αμφίβολης αξιοπιστίας. Ειδικότερα οι χρήστες είναι απαραίτητο να ακολουθούν ορισμένες βασικές αρχές, όπως:

https://www.dpa.gr/sites/default/files/2025-03/Fundamentals%20of%20Secure%20AI%20Systems%20with%20Personal%20Data%20clear.pdf

[33] https://www.huntress.com/cybersecurity-101/topic/anti-spyware

- **Εγκατάσταση Firewall**

Το firewall (τοίχος προστασίας), είναι ένα πρόγραμμα λογισμικού ή ένα κομμάτι υλικού που περιέχεται στα σύγχρονα λειτουργικά συστήματα και δεν επιτρέπει στους χάκερς την είσοδο και τη χρήση προγραμμάτων ενός υπολογιστή. Οι χάκερς ενεργούν στο Διαδίκτυο, όπως ορισμένοι τηλεπωλητές, που καλούν αυτόματα τυχαίους αριθμούς τηλεφώνου, στέλνοντας pings (κλήσεις), σε χιλιάδες υπολογιστές και αναμένοντας απαντήσεις. Τα τείχη προστασίας ενεργούν και δεν επιτρέπουν στον υπολογιστή να απαντήσει σε αυτές τις τυχαίες κλήσεις. Ένα τείχος προστασίας, εμποδίζει τις επικοινωνίες από και προς πηγές χωρίς την απαραίτητη άδεια και αυτό, είναι ιδιαίτερα σημαντικό σε συνδέσεις υψηλής ταχύτητας, στο διαδίκτυο.

- **Anti-spyware Software**

Η προστασία από spyware, περιλαμβάνεται σε ορισμένα προγράμματα λογισμικού προστασίας από ιούς, τα οποία πρέπει να ελέγχονται ως προς την τεκμηρίωση τους και τις προδιαγραφές τους. Υπάρχει και η επιλογή ενός αυτόνομου λογισμικού anti-spyware, το οποίο πρέπει να τηρείται επικαιροποιημένο, με τις αναβαθμίσεις της εταιρείας κατασκευής ικανό να σαρώνει την κίνηση στο διαδίκτυο και να εντοπίζει exploits (υποσύνολο κακόβουλου λογισμικού)[34].

Καλό είναι να αποφεύγεται το κατέβασμα από άγνωστους και αμφιβόλου αξιοπιστίας ιστότοπους και επίσης το άνοιγμα συνδέσεων σε αναδυόμενα παράθυρα και σε ανεπιθύμητα email.

- **Ασφάλεια ασυρμάτων δικτυών**

Το πρώτο βήμα ασφάλισης ασυρμάτων δικτύων, είναι η κρυπτογράφησή τους και για αυτό απαιτείται η επιλογή ενός ασύρματου δρομολογητή με λειτουργία κρυπτογράφησης. Απαιτείται η αλλαγή του προκαθορισμένου αριθμού εισόδου στο δίκτυο, καθώς οι χάκερς γνωρίζουν τους προκαθορισμένους κωδικούς πρόσβασης του εξοπλισμού. Επίσης τα δημόσια "hot spots" ενδέχεται να μην είναι ασφαλή και καλό είναι να αποφεύγεται η πρόσβαση σε αυτά και κυρίως η αποστολή ευαίσθητων προσωπικών πληροφοριών μέσω δημόσιου ασύρματου δικτύου.

[34] https://www.kaspersky.com/blog/exploits-problem-explanation/9448/

- **Ασφάλεια στις διαδικτυακές αγορές**

Πριν την αγορά προϊόντων και υπηρεσιών online, πρέπει να ελέγχεται ο ιστότοπος και μετά να γίνεται η εισαγωγή του αριθμού της πιστωτικής κάρτας ή άλλα προσωπικά στοιχεία. Ο πελάτης πρέπει να διαβάζει προσεκτικά την πολιτική απορρήτου και να ζητάει να εξαιρεθεί από την κοινοποίηση πληροφοριών. Εάν δεν υπάρχει δημοσιευμένη πολιτική απορρήτου, καλό είναι η πλατφόρμα να αποφεύγεται. Δίπλα και αριστερά του "https" στη γραμμή διευθύνσεων στο κάτω μέρος του παραθύρου του προγράμματος περιήγησης, υπάρχει ένα εικονίδιο λουκέτου, το οποίο όταν πατηθεί βγάζει το μήνυμα ασφαλής. Αυτό σημαίνει ότι οι πληροφορίες που εισέρχονται θα κρυπτογραφηθούν ή θα κωδικοποιηθούν, για προστασία από χάκερς καθώς, μετακινούνται στο Διαδίκτυο[35].

- **Περιορισμός των drive-by downloads**

Για τον μετριασμό των drive-by downloads, θα πρέπει να εφαρμοστούν οι ακόλουθες τεχνικές :

✓ Έλεγχος των εφαρμογών. Σε πολλά επιτυχημένα μοντέλα Κυβερνοασφάλειας, ο έλεγχος εφαρμογών αποτελεί σημαντική στρατηγική μετριασμού, που μπορεί να σταματήσει στις drive-by downloads, επιθέσεις.

✓ Ενημέρωση των εφαρμογών και ιδιαίτερα των τρωτών σημείων λειτουργικού συστήματος, ειδικά Java και Flash, οι οποίες πρέπει να ενημερώνονται τακτικά.

✓ Εφαρμογή ισχυρού φιλτραρίσματος από οργανισμούς και επιχειρήσεις, όλης της διαδικτυακής κίνησης, για πιθανώς κακόβουλες λήψεις και τις αποκλείει[36].

- **Ευθύνη παρόχων**

Με το Ν.5160/2024 (ΦΕΚ Α'/195/27-11-2024), ενσωματώθηκε η Οδηγία 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με μέτρα για υψηλό κοινό επίπεδο Κυβερνοασφάλειας σε ολόκληρη την Ένωση. Σύμφωνα με αυτόν (άρθρο 15), οι

[35] California Department of Justice, Office of the Attorney General, "Tips for Consumers- Consumer Information Sheet 12", Jan. 2015, p.1 Available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/CIS_12_Computer_protection_DOJ.pdf

[36] Australian Signals Directorate, "Mitigating Drive-by Downloads" , Oct. 2021, p. 1,2 Available at https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Mitigating%20Drive-by%20Downloads%20%28October%202021%29.pdf

πάροχοι ηλεκτρονικών υπηρεσιών και δικτύων, είναι υποχρεωμένοι να λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα, για την αποτροπή ενδεχομένων κινδύνων, τόσο για την ασφάλεια συστημάτων δικτύου και πληροφοριακών συστημάτων που χρησιμοποιούν για τις δραστηριότητές τους, όσο και για την παροχή των υπηρεσιών τους σε τρίτους, με σκοπό την πρόληψη ή ελαχιστοποίηση των επιπτώσεων στους αποδέκτες των υπηρεσιών τους ή σε άλλες υπηρεσίες και οργανισμούς.

Με το άρθρο 29 παρ.1, του ίδιου νόμου, ορίζεται ότι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) δύναται, στο πλαίσιο των αρμοδιοτήτων της, να επιβάλει στους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, τη λήψη ενισχυμένων μέτρων Κυβερνοασφάλειας. Με την παρ. 2 του ίδιου άρθρου, οι πάροχοι υποχρεώνονται να κοινοποιούν, αμελλητί, κάθε περιστατικό που έχει σημαντικό αντίκτυπο στη λειτουργία των δικτύων και υπηρεσιών στην ΑΔΑΕ, σύμφωνα με τους εκάστοτε ισχύοντες κανονισμούς της, καθώς και στην Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ).

- **Πιστοποίηση Τεχνολογιών Πληροφοριών και Επικοινωνιών**

Στον κανονισμό, 2019/881/ΕΕ, σχετικά με τον ENISA, στο άρθρο 47 αναφέρεται η πρόβλεψη, έτσι ώστε το κυλιόμενο πρόγραμμα εργασίας της Ένωσης να περιλαμβάνει κατάλογο υπηρεσιών και διαδικασιών Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ), που μπορούν να έχουν όφελος από τη συμπερίληψή τους στο πεδίο εφαρμογής ευρωπαϊκού συστήματος πιστοποίησης της Κυβερνοασφάλειας. Η προσθήκη στο πρόγραμμα, θα γίνεται με βάση τη διαθεσιμότητα και την ανάπτυξη των εθνικών συστημάτων πιστοποίησης της Κυβερνοασφάλειας, που καλύπτουν συγκεκριμένη κατηγορία προϊόντων, υπηρεσιών ή διαδικασιών ΤΠΕ και ιδίως όσον αφορά τον κίνδυνο κατακερματισμού τους, της ζήτησης στην αγορά, των εξελίξεων όσον αφορά τις κυβερνοαπειλές, καθώς και του σχετικού Ενωσιακού δικαίου και της πολιτικής τόσο της ΕΕ όσο και των Κρατών Μελών(Κ-Μ).

- **Ανίχνευση spyware**

Όπως προαναφέρθηκε το spyware αφήνει λίγα ψηφιακά ίχνη, καθιστώντας τις έρευνες για την ανίχνευση του εν λόγω λογισμικού δυσχερείς. Επίσης μαζί με τη διαπίστωση αυτή, δέον να ληφθεί υπόψη και το γεγονός ότι οι έρευνες είναι εξαρτώμενες σε μεγάλο βαθμό από αποφάσεις πολλών διοικητικών και δικαστικών αρχών, σε εθνικό αλλά και διεθνές επίπεδο. Εν τούτοις μια συντονισμένη ενέργεια όλων των εμπλεκομένων πλευρών, σε

τεχνικό αλλά και νομικό πλαίσιο, μπορεί να αποτελέσει ένα αίσθημα αποτροπής σε ενδεχόμενους εισβολείς.

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ: ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ ΚΑΤΑΣΚΟΠΕΥΤΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ

3.1 Απάτη με υπολογιστή- Ηλεκτρονικά εγκλήματα

Κοινό τόπο αποτελεί πλέον η διαπίστωση, ότι η ολοένα αυξανόμενη χρήση του διαδικτύου και των τεχνολογιών πληροφορικής και επικοινωνιών, διασυνδέεται ευθέως με την τέλεση παλιών και νεότερων μορφών ποινικών αδικημάτων. Το Κυβερνοέγκλημα παράγει απρόβλεπτες απειλές για την κοινωνική ευταξία, καθόσον στρέφεται τόσο κατά φυσικών και νομικών προσώπων που στηρίζονται στις νέες τεχνολογίες. Ενόψει τούτου ακριβώς του στοιχείου της παγκοσμιότητας των δεδομένων, το Κυβερνοέγκλημα εμφανίζεται ως διαφορετική από άποψη υφής και έκτασης απειλή για την ασφάλεια της κοινωνίας της πληροφορίας, αλλά και για μια σειρά εννόμων αγαθών και ελευθεριών των πολιτών παγκοσμίως.

Αναφερόμενοι στο ζήτημα της απάτης με υπολογιστή, κρίνεται σκόπιμο να ορίσουμε το χώρο και τα μέσα, που χρησιμοποιούνται για να πραγματοποιηθεί η απάτη. Έτσι αναγόμαστε στην έννοια του κυβερνοχώρου (cyberspace), ένας όρος που παραπέμπει σε ένα δίκτυο ηλεκτρονικών υπολογιστών, στο οποίο διακινούνται εικόνες, μηνύματα και πληροφορίες από τον έναν υπολογιστή στον άλλο[37]. Ο εν λόγω όρος αποδίδεται στο συγγραφέα επιστημονικής φαντασίας W. Gibson, αρχικά στο διήγημά του Burning Chrome το 1982 και αργότερα βιβλίο του Neuromancer το 1984, θέλοντας να αποτυπώσει το όραμά του, για ένα παγκόσμιο δίκτυο υπολογιστών που συνενώνει ανθρώπους και πληροφορίες[38].

Η απάτη σχετικά με υπολογιστές (computer related fraud), ορίζεται στο άρθρο 8 της σύμβασης του Συμβουλίου της Ευρώπης, για το έγκλημα στον κυβερνοχώρο European Treaty Series - No. 185), της 23-11-2001, που κυρώθηκε από τη χώρα μας στις 3-08-2016, ως η εισαγωγή, αλλοίωση, διαγραφή, καταστολή δεδομένων του υπολογιστή, καθώς και η παρέμβαση στο σύστημα του υπολογιστή, χωρίς να έχει αυτό το δικαίωμα, με δόλια ή αθέμιτη πρόθεση, με σκοπό την αποκόμιση οικονομικού οφέλους για λογαριασμό του ιδίου ή τρίτου προσώπου. Η εν λόγω σύμβαση είναι γνωστή ως Σύμβαση της Βουδαπέστης και στο 1ο άρθρο, ορίζει ως «σύστημα υπολογιστή μία συσκευή ή ένα σύνολο διασυνδεδεμένων

[37] Γ. Μπαμπινιώτης «Λεξικό της Νέας Ελληνικής Γλώσσας» έκδοση 2η , σελ. 968.
[38] https://www.britannica.com/topic/cyberspace

ή σχετιζόμενων συσκευών, μία ή περισσότερες από τις οποίες πραγματοποιεί αυτόματη επεξεργασία δεδομένων βάσει ενός προγράμματος»[39] .

Σε διεθνές επίπεδο η έννοια του ηλεκτρονικού εγκλήματος, αποδίδεται με τους γενικότερους όρους *e-crime* και *computer crime* και με τους ειδικότερους όρους *cybercrime* και *internet related crime*, οι οποίοι συνδέονται άρρηκτα με το στοιχείο του διαδικτύου[40]. Στην ελληνική γλώσσα αποδίδεται με το γενικό όρο «ηλεκτρονικό έγκλημα» και ειδικότερα με τους όρους «δικτυακό έγκλημα», «Κυβερνοέγκλημα» ή «έγκλημα του κυβερνοχώρου», οι οποίοι ενσωματώνουν το στοιχείο της δικτύωσης. Κατ' εφαρμογή των όρων αυτών, ως μορφές του ηλεκτρονικού εγκλήματος, νοούνται αφενός τα εγκλήματα που διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών και αφετέρου τα εγκλήματα που διαπράττονται ειδικά μέσω διαδικτύου και αναφέρονται ως κυβερνοεγκλήματα, συνιστώντας μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος.

Το ηλεκτρονικό έγκλημα δύναται να προσεγγισθεί υπό τριπλή θεώρηση, ήτοι: α) ως μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών, β) ως μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές και γ) ως μια εγκληματική πράξη που εκδηλώνεται με τη συμμετοχή καθ' οιονδήποτε τρόπο ενός ηλεκτρονικού υπολογιστή. Η τριπλή αυτή προσέγγιση είναι αναγκαία, καθόσον το ηλεκτρονικό έγκλημα δεν διακρίνεται από το «κοινό» ή «συμβατικό έγκλημα» μόνο σε σχέση με ηλεκτρονικό ή διαδικτυακό περιβάλλον διάπραξης.

Πέραν των εννοιολογικών προσδιορισμών, το Κυβερνοέγκλημα παρουσιάζει ορισμένα χαρακτηριστικά, τα οποία το διαφοροποιούν από το συμβατικό έγκλημα και εντείνουν την επικινδυνότητά του. Ως τέτοια ιδιαίτερα χαρακτηριστικά των εγκλημάτων στον κυβερνοχώρο αναφέρονται, σε σχέση με τον τρόπο τέλεσής τους, η ευκολία και η ανωνυμία, σε σχέση με το χρόνο τέλεσής τους η ταχύτητα, σε σχέση με τον τόπο τέλεσής τους ο διασυνοριακός χαρακτήρας και σε σχέση με την απόδειξη τέλεσής τους, η απροθυμία υποβολής καταγγελιών, καθώς και οι δυσχέρειες της διακρατικής συνεργασίας των διωκτικών αρχών. Η ευκολία τέλεσης των εν λόγω εγκλημάτων, είναι απόρροια τόσο του μέσου τέλεσης τους, που έχει πλέον καταστεί κοινό και διαδεδομένο στην πλειοψηφία των σύγχρονων κοινωνών, όσο και καθ' εαυτού του τρόπου προώθησης της εγκληματικής

[39] Ν.4411/2016 (ΦΕΚ Α΄142/3-8-2016), Κύρωση της σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, Εθνικό Τυπογραφείο.

[40] Θεοχάρης Ι. Δαλακούρας, Ηλεκτρονικό Έγκλημα, Ουσιαστικές και δικονομικές όψεις, σελ. 3, Εκδόσεις Νομική Βιβλιοθήκη, 2η ΄Έκδοση.

δράσης, που λαμβάνει χώρα από τον οικείο χώρο του δράστη και εκμηδενίζει την πιθανότητα αντίστασης από το θύμα.

Στο πλαίσιο αυτό, ιδιαίτερη σημασία αποκτά η εμφάνιση και η χρήση κατασκοπευτικών λογισμικών, τα οποία αξιοποιούν τις δυνατότητες της σύγχρονης τεχνολογίας, για την παράνομη παρακολούθηση και συλλογή δεδομένων. Η αυξημένη επικινδυνότητα τους έγκειται στο γεγονός ότι, κατά κανόνα, τα κατασκοπευτικά λογισμικά, εγκαθίστανται και λειτουργούν χωρίς τη συναίνεση του παρακολουθούμενου ατόμου, ενώ η τεχνική τους φύση καθιστά δυσχερή τον εντοπισμό τους, τόσο από τα θύματα όσο και από τους αρμόδιους φορείς. Το στοιχείο αυτό παρέχει στους δράστες αυξημένη ελευθερία κινήσεων, καθιστώντας την εν λόγω μορφή παραβατικότητας ιδιαίτερα ελκυστική.

Χαρακτηριστικό παράδειγμα εργαλειοποίησης του κατασκοπευτικού λογισμικού, αποτελεί η τραπεζική απάτη μέσω ηλεκτρονικής υποκλοπής. Κατά την πρακτική αυτή, οι δράστες, αξιοποιώντας τη μυστική παρακολούθηση της ηλεκτρονικής δραστηριότητας των θυμάτων, αποκτούν πρόσβαση σε ευαίσθητα οικονομικά δεδομένα. Κατά το χρονικό διάστημα του Ιουνίου-Ιουλίου 2023 [41], σημειώνεται ότι αρκετοί Ευρωπαίοι πελάτες διαφορετικών τραπεζικών ιδρυμάτων, στοχοποιήθηκαν από το SpyNote (ή SpyMax), ένα τραπεζικό Trojan για συσκευές Android, μέσω εκστρατειών phishing και smishing. Το εν λόγω κακόβουλο λογισμικό, συνδυάζει δυνατότητες απομακρυσμένης πρόσβασης με τεχνικές κοινωνικής μηχανικής (vishing), απαιτώντας δικαιώματα προσβασιμότητας προκειμένου να αποκτήσει εκτεταμένα προνόμια και να συλλέξει ευαίσθητα δεδομένα. Η διττή του λειτουργία, ως κατασκοπευτικό λογισμικό και ως εργαλείο τραπεζικής απάτης, αναδεικνύει τη διασύνδεση μεταξύ κατασκοπευτικών τεχνολογιών και οικονομικής εγκληματικότητας.

Η χρήση κατασκοπευτικών λογισμικών εντάσσεται στο ευρύτερο πλαίσιο κυβερνοαπειλών,[42] πλήττοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριακών συστημάτων. Υπό την έννοια αυτή τα κατασκοπευτικά λογισμικά αποτελούν κατ' εξοχήν εργαλεία Κυβερνοεπιθέσεων, καθώς επιτρέπουν την μη εξουσιοδοτημένη πρόσβαση, την παρακολούθηση και τη συλλογή δεδομένων, θέτοντας σε

[41] Lackshmanan, R., The Hacker News, (2023) "European Bank Costumers Targeted in SpyNote Android Trojan Campaign", Διαθέσιμο στο: European Bank Customers Targeted in SpyNote Android Trojan Campaign

[42] Σύμφωνα με το Ευρωπαϊκό Συμβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης οι κυριότερες κυβερνοαπειλές είναι οι απειλές κατά της διαθεσιμότητας, το λυτρισμικό και οι απειλές κατά δεδομένων Διαθέσιμο στο: https://www.consilium.europa.eu/el/topics/cybersecurity/

διακινδύνευση όχι μόνο την ιδιωτικότητα των ατόμων, αλλά και τη λειτουργική ακεραιότητα κρίσιμων υποδομών και θεσμών. Ως κυβερνοαπειλή,[43] νοείται οποιαδήποτε κακόβουλη δραστηριότητα, η οποία στοχεύει στην διακύβευση της ακεραιότητας, της εμπιστευτικότητας ή της διαθεσιμότητας των πληροφοριακών συστημάτων, δικτύων ή δεδομένων. Ειδικότερα, σύμφωνα με το άρθρο 2 περ. 8 του Κανονισμού 2019/881 κυβερνοαπειλή, συνιστά κάθε πιθανή περίσταση, συμβάν ή ενέργεια ικανή να καταστρέψει, να διαταράξει ή να επηρεάσει δυσμενώς, τα συστήματα δικτύου και πληροφοριών, τους χρήστες αυτών ή άλλα πρόσωπα. Διακριτή από την έννοια της κυβερνοαπιελής, είναι η έννοια της κυβερνοεπίθεσης, η οποία συνιστά την ενεργό εκδήλωση της απειλής μέσω συγκεκριμένης κακόβουλης ενέργειας. Ενώ η κυβερνοαπειλή παραπέμπει σε δυνητικό κίνδυνο, η κυβερνοεπίθεση προϋποθέτει πραγματική και μη εξουσιοδοτημένη επέμβαση σε σύστημα δικτύου και πληροφοριών, με αποτέλεσμα την πρόκληση βλάβης ή ουσιώδους διατάραξης της λειτουργίας του.

Καθίσταται συνεπώς σαφές, ότι η διαπιστωμένη χρήση των κατασκοπευτικών λογισμικών κλονίζει τον πυρήνα της Κυβερνοασφάλειας. Ως Κυβερνοασφάλεια [44] νοούνται οι δραστηριότητες, που απαιτούνται για την προστασία συστημάτων δικτύου και πληροφοριών, των χρηστών τους και λοιπών επηρεαζόμενων από κυβερνοαπειλές προσώπων. Σε Ενωσιακό πλαίσιο, η έννοια υπερβαίνει την απλή τεχνική προστασία και περιλαμβάνει κάθε παράνομη ή κακόβουλη ενέργεια, που πραγματοποιείται μέσω της τεχνολογίας, όπως η ηλεκτρονική απάτη, η διάδοση παράνομου περιεχομένου, η παραπληροφόρηση ή η παρέμβαση σε δημοκρατικές διαδικασίες.[45] Υπό το πρίσμα αυτό, τα κατασκοπευτικά λογισμικά δεν αποτελούν απλώς μέσο τέλεσης επιμέρους αξιόποινων πράξεων, αλλά διαπιστωμένη πρακτική με σοβαρότατες συνέπειες, όχι μόνο θεμελιώδη δικαιώματα, αλλά και τον ίδιο τον πυρήνα μιας δημοκρατικής έννομης τάξης.

3.2 Ηλεκτρονικό εμπόριο

Η αυξανόμενη χρήση του διαδικτύου, καθώς και η εξέλιξή του, οδήγησαν στην κορύφωση των συναλλαγών στο ηλεκτρονικό εμπόριο, όπως το γνωρίζουμε σήμερα. Πέραν αυτών, η χρήση των κινητών συσκευών και κυρίως των εξελιγμένης τεχνολογίας τηλεφώνων, συνέβαλαν σημαντικά στην αύξηση του αγοραστικού κοινού. Αξίζει να

[43] Ευρωπαϊκό Συμβούλιο της Ευρωπαϊκής Ένωσης Διαθέσιμο στο: https://www.consilium.europa.eu/en/policies/top-cyber-threats/?utm_source=chatgpt.com

[44] Κανονισμός 2019/881/ΕΕ Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον Οργανισμό, Άρθρο 2 περ. 1 Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32019R0881

[45] https://www.consilium.europa.eu/el/policies/cybersecurity/?utm_source=chatgpt.com#strategy

σημειωθεί ότι στις ΗΠΑ, περισσότεροι από το 40% των καταναλωτών, κάνουν μια παραγγελία στην Amazon και λαμβάνουν ένα δέμα την εβδομάδα[46]. Τα κατασκοπευτικά λογισμικά, έχουν πλέον εδραιωθεί στην αγορά και χρησιμοποιούνται ευρέως ως μέσο συλλογής δεδομένων προσωπικού χαρακτήρα, για σκοπούς διαφήμισης και ψηφιακού εμπορίου. Η χρήση τους, διευκολύνει τόσο τη νόμιμη όσο και τη μη εξουσιοδοτημένη πρόσβαση σε συσκευές-στόχους με σύνδεση στο διαδίκτυο, αποτελώντας σημαντικό εργαλείο επιτήρησης και εξαγωγής πληροφοριών, χωρίς τη συναίνεση των χρηστών. Σημειώνεται ότι οι εταιρείες που τα διαθέτουν, υποστηρίζονται από έναν ολοένα και πιο ποικιλόμορφο κύκλο κυβερνητικών πελατών σε παγκόσμια κλίμακα. Από όλες τις χώρες του κόσμου, έχει διαπιστωθεί, ότι τουλάχιστον 80 έχουν προμηθευτεί κακόβουλο λογισμικό παρακολούθησης από εμπορικούς προμηθευτές, ενώ 14 από τις 27 χώρες της ΕΕ, έχουν προμηθευτεί κατασκοπευτικό λογισμικό της Ισραηλινής εταιρείας NSO Group[47].

Μία από τις πιο αμφιλεγόμενες μορφές διαδικτυακής διαφήμισης, αποτελούν τα αναδυόμενα παράθυρα (pop-ups). Τα αναδυόμενα παράθυρα, διαφοροποιούνται ουσιωδώς από άλλες μορφές διαδικτυακής διαφήμισης, γεγονός που τα έχει καταστήσει, αφενός αντικείμενο έντονων αντιπαραθέσεων, αφετέρου ιδιαίτερα δημοφιλές εργαλείο μάρκετινγκ[48]. Σε αντίθεση με τις συμβατικές διαδικτυακές διαφημίσεις, οι οποίες φιλοξενούνται και ελέγχονται από τον ίδιο τον ιστότοπο στον οποίο προβάλλονται, το αναδυόμενο παράθυρο ελέγχεται από τρίτο, απομακρυσμένο διαφημιζόμενο και εμφανίζεται σε ξεχωριστό παράθυρο ή καρτέλα στην οθόνη του χρήστη. Το αναδυόμενο παράθυρο μπορεί να σχετίζεται με την ιστοσελίδα που επικαλύπτει, καθώς, πολλοί ειδησεογραφικοί και εταιρικοί ιστότοποι, λειτουργούν ως διαφημιστές για αναδυόμενα παράθυρα τους, ή μπορεί να μην έχει καμία σχέση με το περιβάλλον περιήγησης του χρήστη. Η δεύτερη αυτή κατηγορία αναδυόμενων παραθύρων, συνδέεται συχνά με την εγκατάσταση adware, δηλαδή λογισμικού που υποστηρίζεται από την προβολή διαφημίσεων και το οποίο εγκαθίσταται στον υπολογιστή ή τη συσκευή του χρήστη, πολλές φορές σε συνδυασμό με άλλο πρόγραμμα, που ο ίδιος επιθυμεί να χρησιμοποιήσει. Στις περιπτώσεις αυτές, η προβολή διαφημίσεων δεν εξαρτάται από τον ιστότοπο που επισκέπτεται ο χρήστης, αλλά

[46] https://www.bigcommerce.com/articles/ecommerce/sustainable-ecommerce/
[47] Mythical Beasts p. 6
[48] Too Many Open Windows? Exploring the Privacy Implications of Pop-Up Ads, Emily Woodward Deutsch, σελ. 8 Διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=894080

ενεργοποιείται απευθείας από το εγκατεστημένο λογισμικό, γεγονός που εγείρει ζητήματα διαφάνειας και προστασίας του ηλεκτρονικού απορρήτου.

Παράλληλα, ιδιαίτερο ενδιαφέρον παρουσιάζουν και τα cookies[49]. Αν και ο αρχικός σκοπός τους ήταν καθαρά λειτουργικός, περιορίζονταν δηλαδή στην αποθήκευση προτιμήσεων ή στοιχείων σύνδεσης του χρήστη διευκολύνοντας την πλοήγηση του, σήμερα χρησιμοποιούνται για σκοπούς ανάλυσης διαδικτυακής συμπεριφοράς και στοχευμένης διαφήμισης. Στο πλαίσιο αυτό, ιδιαίτερη έμφαση αποκτούν τα third-party cookies, τα οποία επιτρέπουν σε τρίτους παρόχους διαφημιστικών υπηρεσιών, να συλλέγουν πληροφορίες σχετικά με τις ιστοσελίδες που επισκέπτεται ο χρήστης, το ιστορικό περιήγησης του, τον χρόνο παραμονής του σε συγκεκριμένο περιεχόμενο και τις διαδικτυακές του αγορές. Έπειτα προβαίνουν στην στη σκιαγράφηση του εκάστοτε χρήστη (profiling), όπου οι πληροφορίες αυτές, αξιοποιούνται για την προβολή εξατομικευμένων διαφημίσεων.

Στο Ενωσιακό δίκαιο, τα cookies ρυθμίζονται από τον Γενικό Κανονισμό Προστασίας Δεδομένων 679/2016/ΕΕ και την Οδηγία 2002/58/ΕΕ, για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (ePrivacy), σύμφωνα με τις οποίες απαιτείται η προηγούμενη, ρητή, συγκεκριμένη και ελεύθερη συγκατάθεση του χρήστη, για την αποθήκευση ή πρόσβαση σε πληροφορίες στη συσκευή του, εκτός εάν πρόκειται για τα απολύτως αναγκαία cookies. Κατά συνέπεια, ενώ τα cookies αποτελούν ένα νόμιμο εργαλείο του ψηφιακού μάρκετινγκ, η κατάχρησή τους ή η χρήση τους χωρίς έγκυρη συγκατάθεση, μπορεί να μετατραπεί σε μηχανισμό αθέμιτης παρακολούθησης, θίγοντας το δικαίωμα στην ιδιωτικότητα και το ηλεκτρονικό απόρρητο.

Τέλος, πρέπει να διακριθούν οι τεχνολογίες εμπορικής επιτήρησης, όπως το adware και τα cookies, από τα εξελιγμένα κατασκοπευτικά λογισμικά τύπου Pegasus ή Predator. Ενώ τα τελευταία στοχεύουν στην αθέατη διείσδυση σε συσκευές, με σκοπό την πλήρη παρακολούθηση του χρήστη, τα εργαλεία εμπορικής επιτήρησης λειτουργούν κυρίως στο πλαίσιο της ψηφιακής διαφήμισης και της δημιουργίας προφίλ. Ωστόσο, η μαζική και συστηματική συλλογή δεδομένων μέσω των τελευταίων δύναται, υπό προϋποθέσεις, να

[49] Σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) τα cookies είναι μικρά αρχεία κειμένου με πληροφορίες, τα οποία αποθηκεύονται από τον διακομιστή (server) ενός ιστότοπου στην τερματική συσκευή (υπολογιστής, κινητό τηλέφωνο κλπ.) ενός επισκέπτη/χρήστη κατά την πλοήγηση σε αυτό. Ο ιστοτόπος ανακτά τις εν λόγω πληροφορίες σε κάθε επίσκεψη προκειμένου να προσφέρει σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει σε αυτή (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, κ.λπ.).

δημιουργήσει φαινόμενα εκτεταμένης επιτήρησης, εγείροντας σοβαρά ζητήματα διαφάνειας, προστασίας της ιδιωτικότητας και ουσιαστικής συγκατάθεσης.

3.3 Περιπτώσεις χρήσης spyware στην Ευρωπαϊκή Ένωση

Όπως έχει προαναφερθεί, κύριος στόχος των κατασκοπευτικών λογισμικών αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα και η παράνομη συλλογή δεδομένων προσωπικού χαρακτήρα [50]. Ο πλήρης έλεγχος της συσκευής του θύματος, καθιστά εφικτή τη συλλογή όχι μόνο απλών προσωπικών δεδομένων, αλλά και πληροφοριών, οι οποίες, μολονότι δεν εντάσσονται ευθέως στις ειδικές κατηγορίες του άρθρου 9 του ΓΚΠΔ[51], η επεξεργασία τους ενδέχεται να δημιουργήσει σοβαρούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων. Ειδικότερα, η αθέμιτη απόκτηση κωδικών πρόσβασης σε διαδικτυακούς λογαριασμούς, στοιχείων τραπεζικών λογαριασμών, καθώς και δεδομένων πιστωτικών ή χρεωστικών καρτών, δύναται να οδηγήσει σε έμμεση αποκάλυψη κρίσιμων πτυχών της οικονομικής κατάστασης, των συναλλακτικών συνηθειών και εν γένει την οικονομική βλάβη του υποκειμένου.

Η παρακολούθηση των φυσικών προσώπων, δεν περιορίζεται μόνο σε θεωρητικό επίπεδο, καθώς εμπεριέχει σημαντικό πρακτικό αντίκτυπο. Εκθέσεις και μελέτες ερευνητικών οργανισμών, όπως το Citizen Lab του Πανεπιστημίου του Τορόντο, αποδεικνύουν, ότι τα λογισμικά κατασκοπείας, χρησιμοποιούνται για την συστηματική παρακολούθηση και την παράνομη συλλογή ευαίσθητων πληροφοριών σε φορείς, εταιρείες ακόμη και ιδιώτες.[52] Η στοχευμένη επιτήρηση μέσω προηγμένων τεχνολογικών εργαλείων, εγείρει ανησυχίες, καθώς δύναται να επεκταθεί σε όλες τις πτυχές της ζωής των

---

[50] Άρθρο 4 του 679/2016//ΕΕ ΓΚΠΔ: «*«δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου».*

[51] Σύμφωνα με το άρθρο 9 του ΓΚΠΔ ως ευαίσθητα δεδομένα θεωρούνται εκείνα που «*αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό».*

[52] The use of Pegasus and equivalent surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, pg. 8, February 2023, Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf

στοχευόμενων προσώπων. Χαρακτηριστικό παράδειγμα αποτελεί το περίφημο λογισμικό Pegasus, το οποίο αναπτύχθηκε από την ισραηλινή εταιρεία NSO Group. Η εν λόγω εταιρεία ισχυρίζεται, ότι διαθέτει το συγκεκριμένο λογισμικό σε «επιλεγμένες κυβερνήσεις» για «νόμιμη υποκλοπή», με σκοπό την καταπολέμηση της τρομοκρατίας και του οργανωμένου εγκλήματος. Ωστόσο, διεθνείς δημοσιογραφικές έρευνες, έχουν αναδείξει μια διαφορετική και ιδιαιτέρως ανησυχητική διάσταση της χρήσης του, αποκαλύπτοντας περιστατικά παρακολούθησης δημοσιογράφων, δικηγόρων, ηγετών της αντιπολίτευσης και υπερασπιστών ανθρωπίνων δικαιωμάτων[53]. Το Pegasus, είναι ένα βαθιά παρεμβατικό εμπορικό spyware, που μπορεί να δώσει σε έναν εισβολέα απομακρυσμένη πρόσβαση σε μια συσκευή, συμπεριλαμβανομένων των φωτογραφιών, των επαφών και των επικοινωνιών της. Μπορεί επίσης να ενεργοποιήσει την κάμερα και το μικρόφωνο, προσφέροντας οπτικά και ηχητικά εφέ από το περιβάλλον ενός στόχου. Ενδεικτική είναι η υπόθεση παραβίασης του κινητού τηλεφώνου του ιδρυτή της Amazon και ιδιοκτήτη της Washington Post, Jeff Bezos[54]. Ειδικότερα, το κακόβουλο αυτό λογισμικό φέρεται, ότι μπορεί να παραβιάσει σχεδόν οποιαδήποτε ηλεκτρονική συσκευή (iOS ή Android), χωρίς οποιαδήποτε ενέργεια του χρήστη (zero-click exploit)[55], επιτρέποντας στο χάκερ να έχει πλήρη πρόσβαση σε ευαίσθητες πληροφορίες, συμπεριλαμβανομένων μηνυμάτων ηλεκτρονικού ταχυδρομείου, τηλεφωνικών κλήσεων, ακόμα και κρυπτογραφημένων επικοινωνιών.

Ένα άλλο λογισμικό κατασκοπείας, που χρησιμοποιείται και από Κ-Μ της ΕΕ, αποτελεί και το Predator, το οποίο συνδέθηκε με την εταιρεία Cytrox [56],[57]. Η ειδοποιός διαφορά του από το Pegasus, έγκειται στην μεθοδολογία ενεργοποίησής του. Ειδικότερα, το Predator βασίζεται στην one-click τεχνική, προϋποθέτοντας την ενεργοποίηση ενός κακόβουλου συνδέσμου από τον χρήστη, προκειμένου να εγκατασταθεί στη συσκευή του.[58]

---

[53] European Data Protection Supervisor, The EU's independent data protection authority, Preliminary Remarks on Modern Spyware, 15 February 2022, pg. 5, Διαθέσιμο στο: Preliminary Remarks on Modern.pdf

[54] https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince

[55] https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware

[56] Η Cytrox είναι μια εταιρεία κυβερνοπαρακολούθησης, η οποία ιδρύθηκε το 2017 στα Σκόπια της Βόρειας Μακεδονίας και ανήκει στο δίκτυο Intellexa Consortium.

[57] https://www.in.gr/2024/01/08/stories/intellexa-kai-cytrox-ena-daidalodes-systima-ypoklopon-gia-varia-portofolia/#goog_rewarded

[58] The use of Pegasus and equivalent surveillance spyware, The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, February 2023, Pg. 17

Συνήθως, οι μυστικές υπηρεσίες, συχνά παρακολουθούν και υποκλέπτουν τις επικοινωνίες κατά τη μεταφορά, ενώ το spyware επιτρέπει την άμεση εξαγωγή δεδομένων επικοινωνίας που επεξεργάζεται το σύστημα-στόχος, παρακάμπτοντας τις κρυπτογραφήσεις των υπηρεσιών διαδικτυακής επικοινωνίας. Μετά τη μόλυνση του ηλεκτρονικού συστήματος στην προκειμένη περίπτωση του κινητού τηλεφώνου, το Predator επιτρέπει στους εισβολείς, να παρακολουθούν κάθε πτυχή του τηλεφώνου ενός στόχου, συμπεριλαμβανομένων κλήσεων, μηνυμάτων, φωτογραφιών και βίντεο. Ειδικοί στον τομέα της Κυβερνοασφάλειας από τη Citizen Lab και την Google, ανέφεραν ότι οι δράστες που αγοράζουν spyware Predator «πιθανώς έχουν κυβερνητική στήριξη»[59]. Η υπόθεση χρήσης Predator, εις βάρος δημοσιογράφων και πολιτικών προσώπων, ανέδειξε ζητήματα, διαφάνειας των δημοκρατικών θεσμών και ελέγχου των μηχανισμών παρακολούθησης. Καθίσταται συνεπώς σαφές, ότι τα κατασκοπευτικά λογισμικά δεν αποτελούν απλώς ένα εργαλείο με υψηλές τεχνολογικές προδιαγραφές, αλλά μπορεί να μετατραπούν σε μηχανισμούς σοβαρής προσβολής θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως όταν η χρήση τους δεν περιβάλλεται από αυστηρές εγγυήσεις νομιμότητας, αναγκαιότητας και αναλογικότητας.

Το λογισμικό Predator, έχει αποτελέσει και συνεχίζει να αποτελεί αντικείμενο έντονου δημόσιου διαλόγου και στην Ελλάδα. Μια σημαντική σελίδα της υπόθεσης αυτής, γράφηκε πρόσφατα με την καταδίκη ορισμένων εμπλεκομένων. Τέσσερα άτομα που διέθεσαν στην αγορά το λογισμικό αυτό, κρίθηκαν ένοχα και τους επιβλήθηκαν αυστηρές ποινές φυλάκισης από ελληνικό δικαστήριο, με αναστολή εν αναμονή του δικαιώματος έφεσης, για την υπόθεση των τηλεφωνικών υποκλοπών, που συγκλόνισε τη χώρα το 2022 και συγκεκριμένα για τα πλημμελήματα παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών και της παράνομης πρόσβασης σε προσωπικά δεδομένα και συνομιλίες. Αυτή η περίπτωση έγινε γνωστή ως το «Watergate της Ελλάδας», όπου το λογισμικό παρακολούθησης με την ονομασία Predator, χρησιμοποιήθηκε για την παρακολούθηση 87 ατόμων[60]. Μέσα στους κοινούς στόχους νόμιμης και παράνομης παρακολούθησης συγκαταλέγονται υπουργοί, υψηλόβαθμα πολιτικά στελέχη, δημοσιογράφοι, ένας εφοριακός, ένας εισαγγελέας, στελέχη των Ενόπλων Δυνάμεων και της Αστυνομίας και ένα υψηλόβαθμο τραπεζικό στέλεχος.

Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf

[59] https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf

[60] https://www.bbc.com/news/articles/cj6dx4886rpo

Η υπόθεση του Predator στην Ελλάδα, συνδέθηκε με την κυβέρνηση και μάλιστα με τον ίδιο το πρωθυπουργό της χώρας, καθόσον υπήρξαν σοβαρές ενδείξεις για εμπλοκή της Εθνικής Υπηρεσίας πληροφοριών(ΕΥΠ), στην οποία είναι ο άμεσος παριστάμενος. Σύμφωνα με το ρεπορτάζ του inside story, ο έλεγχος των δύο πραγματογνωμόνων που ορίστηκαν και του αντιεισαγγελέα του Αρείου Πάγου, έδειξε ότι από τα αυτά τα 87 πρόσωπα στα κινητά των οποίων έγινε απόπειρα εγκατάστασης παράνομου λογισμικού Predator, για τα 27 είχε εκδοθεί τουλάχιστον μία εντολή άρσης του απορρήτου από την ΕΥΠ, για λόγους Εθνικής Ασφάλειας. Δηλαδή, για περίπου διάστημα δύο ετών, έναν στους τρεις στόχους του Predator, τον παρακολουθούσε, ταυτόχρονα και επισήμως η ΕΥΠ[61].

Με αφορμή την Ελληνική περίπτωση χρήσης του Predator, το Παρατηρητήριο Ανθρωπίνων Δικαιωμάτων (Human Rights Watch HRW), κάλεσε την Ελλάδα να λάβει μέτρα για την προστασία των κατοχυρωμένων ατομικών δικαιωμάτων και ιδιαίτερα της ελευθερίας του τύπου και συγκεκριμένα να προβεί σε απαραίτητες νομοθετικές μεταρρυθμίσεις ως προς την επιτήρηση, όπως:

- Απαίτηση δικαστικής έγκρισης, για όλες τις εντολές επιτήρησης, από εξουσιοδοτημένους ανεξάρτητους δικαστές, οι οποίοι πριν την έγκριση να αξιολογούν την σκοπιμότητα, λαμβανομένων υπόψη των παραμέτρων της αναγκαιότητας και της αναλογικότητας του μέτρου.
- Εξασφάλιση συγκεκριμένων εγγυήσεων για αιτήματα επιτήρησης δημοσιογράφων, ιεράρχηση της προστασίας των πηγών και υποχρέωση ενημέρωσης μετά την επιτήρηση.
- Διασφάλιση ότι οι εισαγγελείς, υποχρεούνται να υποβάλουν γραπτό αίτημα, όταν ζητούν επιτήρηση για λόγους Εθνικής Ασφάλειας, το οποίο να περιλαμβάνει τεκμηριωμένους και ακριβείς ισχυρισμούς, ως προς τη νομιμότητα, την αναγκαιότητα και την αναλογικότητα του μέτρου επιτήρησης .
- Σαφέστερη νομική ρύθμιση, που να εξασφαλίζει απρόσκοπτα το δικαίωμα πρόσβασης σε πληροφορίες σχετικά με την επιτήρηση από κυβερνητικούς φορείς, επιτρέποντας στα άτομα να ζητούν και να λαμβάνουν λεπτομέρειες, σχετικά με τυχόν μέτρα επιτήρησης που λαμβάνονται εναντίον τους.

[61] https://www.tanea.gr/2024/07/26/greece/skandalo-ypoklopon-o-katalogos-ton-koinon-stoxon-eyp-kai-predator/

• Κατάργηση της υφιστάμενης τριετούς διάρκειας που εμποδίζει τα παρακολουθούμενα άτομα, να αποκτούν πρόσβαση σε πληροφορίες σχετικά με την επιτήρησή τους, που έγινε για λόγους Εθνικής Ασφάλειας.

• Ανάθεση της αποκλειστικής ευθύνης για τις αποκαλύψεις επιτήρησης στην ΑΔΑΕ.

• Ανάκληση του διατάγματος, που υπάγει τη Γενική Γραμματεία Ενημέρωσης και Επικοινωνίας, τον εποπτικό φορέα της δημόσιας ραδιοτηλεόρασης (ΕΡΤ) και του Αθηναϊκού-Μακεδονικού Πρακτορείου Ειδήσεων (ΑΜΝΑ), στην αρμοδιότητα του Γραφείου του Πρωθυπουργού ή διαφορετικά την έκδοση διατάγματος που να αποδεσμεύει την ΕΡΤ και το ΑΜΝΑ από τη Γενική Γραμματεία Ενημέρωσης και Επικοινωνίας, ώστε να διασφαλιστεί η ανεξαρτησία τους[62].

Άλλες περιπτώσεις χρήσης κατασκοπευτικού λογισμικού σε χώρες της ΕΕ, που καταγράφηκαν πριν το περιστατικό στην Ελλάδα, ήταν στην Πολωνία, στην Ουγγαρία και στην Ισπανία για παρακολούθηση δημοσιογράφων και μελών της αντιπολίτευσης[63]. Εισαγγελείς στην Πολωνία, απήγγειλαν κατηγορίες σε δύο πρώην αρχηγούς των μυστικών υπηρεσιών της χώρας, σχετικά με τη χρήση του spyware Pegasus, που πωλήθηκε από τον όμιλο NSO. Η Εθνική Εισαγγελία τους κατηγόρησε για πλημμελή άσκηση των καθηκόντων, διότι επέτρεψαν τη χρήση του εν λόγω λογισμικού, χωρίς να έχει προηγηθεί πιστοποίηση ασφάλειας σ' αυτό και χωρίς να προβλεφθεί η τεχνολογία που προστατεύει, την ασφάλεια των διαβαθμισμένων πληροφοριών. Σύμφωνα με την πολωνική νομοθεσία, τα συστήματα πληροφορικής, που επεξεργάζονται διαβαθμισμένες πληροφορίες πρέπει να είναι διαπιστευμένα, έτσι ώστε να διασφαλιστεί ότι οι χρήστες τους, έχουν τον αποκλειστικό έλεγχο επί των πληροφοριών που εισάγονται για επεξεργασία[64]. Στην έκθεση του Ευρωπαϊκού κοινοβουλίου της 13 Ιουνίου 2023, για τη διερεύνηση καταγγελιών υποκλοπών σε χώρες της ΕΕ, όσον αφορά την Ισπανία, αναφέρεται σε δύο περιστατικά εκ των οποίων στο πρώτο, στόχοι ήταν ο πρωθυπουργός, ο υπουργός Άμυνας, ο υπουργός Εσωτερικών και άλλοι υψηλόβαθμοι αξιωματούχοι, ενώ στη δεύτερη που καταγράφεται ως «CatalanGate», στοχοποιήθηκαν 65 άτομα, συμπεριλαμβανομένων πολιτικών προσωπικοτήτων από την

[62] https://www.hrw.org/report/2025/05/08/bad-worse/deterioration-media-freedom-greece
[63] https://www.theguardian.com/world/2023/may/09/eu-parliament-report-calls-for-tighter-regulation-of-spyware
[64] https://www.hks.harvard.edu/centers/carr-ryan/our-work/carr-ryan-commentary/spyware-cases-europe-and-africa-spotlight-privacy

περιφερειακή κυβέρνηση της Καταλονίας, μελών του κινήματος υπέρ της ανεξαρτησίας της Καταλονίας, βουλευτών του Ευρωπαϊκού Κοινοβουλίου, κα. δημόσια πρόσωπα, σύμφωνα με πληροφορίες από την Citizen Lab[65].

Το Σεπτέμβριο του 2022, μέλη του Ευρωπαϊκού Κοινοβουλίου που ερευνούσαν τη χρήση λογισμικού κατασκοπείας από κυβερνήσεις της ΕΕ, επέκριναν έντονα το Ισραήλ για έλλειψη διαφάνειας στην πώληση λογισμικού κατασκοπείας σε ευρωπαϊκές κυβερνήσεις, που το έχουν χρησιμοποιήσει παράνομα[66].

Το Μάρτιο του 2023, αξιωματούχος του Λευκού Οίκου, δήλωσε στο NBC, ότι τουλάχιστον σε πενήντα περίπου κυβερνητικούς υπάλληλους, που εργάζονται για τις Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ), σε περισσότερες από δέκα χώρες, διαπιστώθηκε εμπορικό κακόβουλο λογισμικό κατασκοπείας στα τηλέφωνά τους. Ο Λευκός Οίκος ανακοίνωσε επίσης, ότι ο «τότε» πρόεδρος Τζο Μπάιντεν, σκόπευε σύντομα να υπογράψει εκτελεστικό διάταγμα, το οποίο θα δεσμεύει τις εταιρείες παραγωγής spyware, να ακολουθούν τις απαιτούμενες προδιαγραφές, με στόχο τον περιορισμό της κατάχρησης του λογισμικού αυτού. Ο ίδιος αξιωματούχος δήλωσε ότι το διάταγμα, θα δίνει στον Λευκό Οίκο την εξουσία, να απαγορεύσει το λογισμικό μιας εταιρείας σε όλες τις ομοσπονδιακές υπηρεσίες, εάν διαπιστωθεί ότι έχει χρησιμοποιηθεί, για να στοχεύσει ακτιβιστές, να περιορίσει την πολιτική διαφωνία ή να κατασκοπεύσει Αμερικανούς πολίτες[67]. Το διάταγμα εκδόθηκε την 27 Μαρτίου 2023 (Executive Order 14093), με τίτλο «Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security/Απαγόρευση χρήσης από την κυβέρνηση των Ηνωμένων Πολιτειών εμπορικού λογισμικού κατασκοπείας που θέτει σε κίνδυνο την εθνική ασφάλεια».

Η εταιρεία META (Facebook), που κατέχει την εφαρμογή WhatsApp, κατέθεσε τον Οκτώβριο του 2019, αγωγή σε ομοσπονδιακό δικαστήριο της Καλιφόρνια, κατηγορώντας τον ισραηλινό κατασκευαστή κινητής τηλεφωνίας NSO Group, ότι δημιούργησε ένα exploit, που χρησιμοποιήθηκε πολλές φορές για να παγιδεύσει τα τηλέφωνα των ατόμων που χρησιμοποιούν την εφαρμογή. Η προσβολή εκμεταλλεύτηκε ένα ελάττωμα στις ηχητικές κλήσεις στο WhatsApp και δίνοντας την εντύπωση, ότι οι χρήστες ελάμβαναν μια συνηθισμένη κλήση, το κακόβουλο λογισμικό μόλυνε αθόρυβα τη συσκευή με spyware,

[65] https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EL.html
[66] https://www.israelnationalnews.com/news/360211
[67] https://www.nbcnews.com/tech/security/least-50-us-government-employees-hit-spyware-white-house-says-rcna76820

αποκτώντας πλήρη πρόσβαση σε αυτή. Σε ορισμένες δε περιπτώσεις συνέβη τόσο γρήγορα, που το τηλέφωνο του στόχου μπορεί να μην έλαβε καθόλου σήμα εισερχόμενης κλήσης. Όπως ανέφερε το ομοσπονδιακό δικαστήριο, περίπου 1.400 στοχευμένες συσκευές επηρεάστηκαν από την επίθεση. Σύμφωνα με ανακοίνωση του WhatsApp, οι περισσότεροι χρήστες δεν επηρεάστηκαν, αλλά υπογράμμισε ότι μεταξύ αυτών ήταν πάνω από εκατό υπερασπιστές των ανθρωπίνων δικαιωμάτων και δημοσιογράφοι. Στο ίδιο άρθρο επισημαίνεται, ότι η εφαρμογή του WhatsApp είναι πλήρως κρυπτογραφημένη από άκρο σε άκρο και θεωρείται σχεδόν αδύνατο να αποκτήσει κάποιος πρόσβαση στα μηνύματα, καθώς αυτά μεταδίδονται το διαδίκτυο. Για το λόγο αυτό, τα τελευταία χρόνια, οι κυβερνήσεις και οι εταιρείες λογισμικού κατασκοπείας για κινητά, στοχεύουν στην αφετηρία και το τέρμα του δικτύου, δηλαδή τις συσκευές από τις οποίες αποστέλλονται και λαμβάνονται τα μηνύματα [68].

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ: ΗΘΙΚΑ ΚΑΙ ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΧΡΗΣΗΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΚΑΤΑΣΚΟΠΕΙΑΣ

4.1 Ηθικά ζητήματα και ηλεκτρονική τεχνολογία

Μιλώντας για ζητήματα ηθικής στις ηλεκτρονικές υπηρεσίες και στο διαδίκτυο, αναζητούμε να προσδιορίσουμε το κανονιστικό πλαίσιο, που διέπει στη λειτουργία τους. Τα θέματα της ηθικής, κρίνεται απαραίτητο να συνεξεταστούν με αυτά της δεοντολογίας, η οποία ως όρος έχει συνάφεια με την ηθική, αλλά και την επιστήμη του δικαίου, η οποία θέτει το κανονιστικό πλαίσιο στον κυβερνοχώρο. Η ηθική είναι ένα σύστημα κανόνων συμπεριφοράς, που χαρακτηρίζει μια κοινωνική ομάδα και καθ' επέκταση και μια επαγγελματική ομάδα. Από την άλλη η δεοντολογία ως όρος, αφορά σε σύνολο κανόνων που ρυθμίζουν τον τρόπο που πρέπει να φέρεται μια κοινωνική ομάδα, καθώς και τις μεθόδους που ακολουθεί μια επαγγελματική ομάδα. Η δεοντολογία ως σύνολο κανόνων ταυτίζεται με την επιστήμη του δικαίου περισσότερο από την ηθική, η οποία σύμφωνα με τον Immanuel Kant[69] εκδηλώνεται με ορθό τρόπο, όταν ο άνθρωπος πράττει το καλό από καθήκον ως ελεύθερη ύπαρξη και όχι για κάποιο άλλο λόγο. Το δίκαιο αποτελείται από σύνολο κανόνων και η κύρια διαφορά του από τις φιλοσοφικές θεωρίες, είναι η

[68] https://www.business-humanrights.org/en/latest-news/court-document-reveals-locations-of-thousands-of-whatsapp-victims-targeted-by-nso-spyware/

[69] Michael J. Sandel, Δικαιοσύνη «Τι είναι το σωστό;», μεταφρ. Αλέξανδρος Κιουπκιόλης εκδ. Πόλις 2011, σελ. 164.

υποχρεωτικότητα που το χαρακτηρίζει και επιβάλει με σαφή τρόπο δεσμευτικότητα, ως προς την τήρηση αυτών των κανόνων[70] .

Το Εθνικό Συνέδριο Υπολογιστών και Αξιών, που πραγματοποιήθηκε το 1991, στο Southern Connecticut State University, είχε θέμα τις επιπτώσεις των υπολογιστών στην ασφάλεια, την ιδιοκτησία, το απόρρητο, τη γνώση, την ελευθερία και τις ευκαιρίες. Επίσης στα τέλη της δεκαετίας του 1990, μια άλλη θεωρία σχετικά με την ηθική των υπολογιστών, με το όνομα «σχεδιασμός υπολογιστή με ευαισθησία στην αξία», πρόβαλλε την εκδοχή, λαμβάνοντας υπόψη την εξέλιξη της τεχνολογίας ότι τα προβλήματα ηθικής από τη χρήση των υπολογιστών μπορούν να αποφευχθούν, εφόσον η νέα τεχνολογία μπορεί να προβλέψει ενδεχόμενες αλλοιώσεις στις ανθρώπινες αξίες και να ενσωματώσει μηχανισμούς που να αποτρέπουν να συμβεί κάτι τέτοιο[71] .

Αναμφισβήτητα το πεδίο της ΤΝ, θεωρείται από πλευράς εξέλιξης των υπολογιστικών συστημάτων και των ηλεκτρονικών τεχνολογιών και επικοινωνιών ότι κορυφαίο υφίσταται αυτή τη στιγμή και εκτός των θετικών αποτελεσμάτων που είναι ήδη εμφανή, το μέλλον προδιαγράφεται ακόμη πιο λαμπρό, καθόσον εταιρείες κολοσσοί, όπως η Amazon, η Alphabet, η Nvidia και άλλες επενδύουν δισεκατομμύρια δολάρια. Παρά τις ενέργειες δημιουργίας κανονιστικών πλαισίων ανά τον κόσμο, (η ΕΕ έχει εκδώσει τον AI Act/ Κανονισμός ΕΕ, 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου/ 13-06- 2024), υπήρξαν και υπάρχουν ανησυχίες σχετικά με την εφαρμογή της ΤΝ και τις συμπεριφορές της. Το κέντρο Ethics and Innovation, υπάγεται στο τμήμα Επιστήμης, Καινοτομίας και Τεχνολογίας (DSIT) του Ενωμένου Βασιλείου και έχει σκοπό να διασφαλίζει για την κοινωνία τα πιθανά οφέλη της τεχνολογίας. Τον Ιούνιο του 2019, με βάση οδηγό του Alan Turing (SUM values), εξέδωσε οδηγία για την κατανόηση της ΤΝ με ασφάλεια και σεβασμό στις ηθικές αξίες, που αναφέρονται στην αξιοπρέπεια των ατόμων, στην προστασία των κοινωνικών αξιών, τη δικαιοσύνη και το δημόσιο συμφέρον, ανοικτή ειλικρινή διασύνδεση χωρίς αποκλεισμούς κα φροντίδα για την ευημερία όλων[72] .

Θέματα δεοντολογίας περιλαμβάνονται και στις διατάξεις της ΕΕ για την προστασία προσωπικών δεδομένων. Η Οδ. 95/46 στις αιτ. σκ. 26,61 περιείχε πρόβλεψη για Κώδικες

---

[70] Παύλος Κ. Σούρλας, «Μια εισαγωγή στην επιστήμη του δικαίου», εκδ. Αντ. Ν. Σάκκουλα 1995, σελ. 51.

[71] Stanford Encyclopedia of Philosophy Archive, Computer and Information Ethics, Winter 2016 Edition Available (Computing and Human Values) at: https://plato.stanford.edu/archives/win2016/entries/ethics-computer

[72] https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety

Δεοντολογίας, ως χρήσιμο μέσο για να διευκολυνθεί η εφαρμογή τους. Επίσης ο ΓΚΠΔ, ενθαρρύνει την εκπόνηση Κωδίκων και παρέχει αναλυτικές οδηγίες για το περιεχόμενό τους[73].

4.2 Παραβιάσεις θεμελιωδών δικαιωμάτων

Ο όρος θεμελιώδη δικαιώματα, περιλαμβάνει ή υπονοεί και άλλους γνωστούς και σχετικούς όρους, όπως ατομικά δικαιώματα, συνταγματικά δικαιώματα, ατομικές ελευθερίες κα. Θεωρείται δε έναντι των άλλων πληρέστερος και εκτενέστερος καθόσον, η προστασία τους υπερβαίνει τα εθνικά επίπεδα και επιπλέον λέγοντας ατομικές ελευθερίες και ατομικά δικαιώματα, δεν αποδίδουν την κοινωνική διάσταση των δικαιωμάτων και περιορίζονται μόνο στην αμυντική διάσταση αυτών[74].

Η αναφορά στο Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ (ΧΘΔΕΕ), στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), στις αποφάσεις του ΔΕΕ και του Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ), κρίνεται απαραίτητη, ώστε με βάση την πρακτική και τα αποτελέσματα που επιφέρει η χρήση του κατασκοπευτικού λογισμικού, να γίνει αντιστοίχιση των δικαιωμάτων που παραβιάζονται[75].

Η παρακολούθηση και η επιτήρηση των ηλεκτρονικών συσκευών και λειτουργιών, επηρεάζει το δικαίωμα προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων των ανθρώπων, αλλά και άλλα θεμελιώδη δικαιώματα, όπως αυτό της ελευθερίας του λόγου, του συνεταιρίζεσθαι και του συνέρχεσθαι[76] και κατά συνέπεια πολιτικο-κοινωνικά δικαιώματα, που προϋποθέτουν την άσκηση των προηγούμενων. Η πολιτική συμμετοχή, μπορεί να επηρεαστεί από εξωτερικές παρεμβάσεις spyware, καθώς οι πολίτες που κατασκοπεύονται μπορούν να εκφοβιστούν, ώστε να απέχουν από πολιτικές διαδικασίες και ιδιαίτερα αυτές του εκλέγειν και εκλέγεσθαι, αλλά και σε άλλες δραστηριότητες και πολιτικές εκδηλώσεις.

Ο φόβος ότι κατασκοπεύονται, μπορεί να αναγκάσει τους ανθρώπους να απέχουν από το να θέσουν υποψηφιότητα για κάποιο αξίωμα ή από το να διεξάγουν μια αποτελεσματική προεκλογική εκστρατεία. Αυτό δε πιθανόν να επηρεάσει τα ποιοτικά αλλά

---

[73] Γιώργος Ν. Γιαννόπουλος, Εισαγωγή στη Νομική Πληροφορική, Νομική Βιβλιοθήκη, Αθήνα 2018, σελ. 98,99.

[74] Σπύρος Βλαχόπουλος, «Θεμελιώδη Δικαιώματα», Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2017, σ.5,6.

[75] Αρχικά προτάθηκε στο Συμβούλιο της Νίκαιας το 2000, τέθηκε όμως σε ισχύ ως μέρος της Συνθήκης της Λισσαβόνας την 1η Δεκεμβρίου 2009, διαθέσιμο σε https://www.consilium.europa.eu/el/policies/fundamental-rights/#charter

[76] Προστατεύεται από την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου(άρθρο 11).

και ποσοτικά χαρακτηριστικά μια πολιτικής ομάδας, αφού αυτή βασίζεται στη συμμετοχή και τις αντιδράσεις των πολιτών. Επιπλέον, εκδηλώνονται συχνά επιθέσεις και παρακολουθήσεις σε δημοσιογράφους, πολιτικούς και ακτιβιστές, πρόσωπα που διαδραματίζουν σημαντικό ρόλο στη δημόσια σφαίρα και η επιτήρηση τους δημιουργεί συνθήκες καταστολής, χειραγώγησης, εκβιασμού, παραποίησης και δυσφήμισης. Ακόμη και η ίδια εκλογική διαδικασία μπορεί να αλλοιωθεί, όταν οι πληροφορίες που υποκλέπτονται, χρησιμοποιούνται για χειραγώγηση και δυσφήμηση «ανεπιθύμητων» υποψηφίων εκλογικών παρατάξεων[77].

Σύμφωνα με το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα του ΟΗΕ (International Covenant on Civil and Political Rights), παραβιάζεται η ελευθερία της έκφρασης (άρθρο19), όταν άτομα, που γνωρίζουν ή υποπτεύονται ότι τελούν υπό επιτήρηση, αποφασίζουν υπό την πίεση αυτή να μην εκφράζουν τις απόψεις τους (π.χ. χρησιμοποιώντας τις συσκευές τους για να επικοινωνήσουν) ή να αποφύγουν την αναζήτηση πληροφοριών στο διαδίκτυο. Η καταχρηστική παρακολούθηση, προσβάλει το δικαίωμα προστασίας από επέμβαση στην ιδιωτικότητα, την οικογένεια, την κατοικία ή την αλληλογραφία (Άρθρο 17). Αυτό το δικαίωμα παραβιάζεται, όταν συλλέγονται πληροφορίες από μια ατομική συσκευή, διαβιβάζονται σε άλλους και υποβάλλονται σε επεξεργασία, χωρίς συναίνεση του ατόμου[78].

Το άρθρο 12 της Οικουμενικής Διακήρυξης των Ηνωμένων Εθνών για τα ανθρώπινα δικαιώματα, προστατεύει την ιδιωτική και την οικογενειακή ζωή, συμπεριλαμβανόμενης της κατοικίας και της αλληλογραφίας απέναντι σε αυθαίρετες παρεμβάσεις. Σαφώς λοιπόν η περίπτωση δημόσιας επιτήρησης, συνεπάγεται σημαντικούς κινδύνους για τα ανθρώπινα δικαιώματα και μπορεί να υπονομεύσει σημαντικά το δικαίωμα στην ιδιωτικότητα[79] και ως εκ τούτου τα κράτη που προβαίνουν σε δημόσια επιτήρηση, πρέπει να λαμβάνουν σοβαρά

[77] European Parliament/Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies "The impact of Pegasus on fundamental rights and democratic processes", Jan. 2023, p. 27, Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

[78] European Parliament, STUDY Requested by the PEGA Committee "The impact of Pegasus on fundamental rights and democratic processes", p.39, Available at. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

[79] Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Άρθρο 7) και Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (Άρθρο 8).

υπόψη τυχόν επιπτώσεις των ενεργειών τους, ώστε να διασφαλίζεται η αυστηρή συμμόρφωση με το διεθνές δίκαιο στα θεμελιώδη δικαιώματα[80].

Άλλα δικαιώματα που κατοχυρώνονται στον ΧΘΔΕΕ και ενδέχεται να επηρεαστούν από τη χρήση κατασκοπευτικού λογισμικού από κρατικούς φορείς, είναι το δικαίωμα της πρόσβασης στα προσωπικά του δεδομένα και το δικαίωμα της προστασίας αυτών (άρθρο 8), το δικαίωμα στην ελευθερία της έκφρασης (άρθρο 11), καθώς επίσης και το δικαίωμα της μη διάκρισης (άρθρο 21)[81].

4.3 Δικαίωμα προστασίας προσωπικών δεδομένων

Με το ψήφισμα της Ζ' Αναθεωρητικής Βουλής της 6ης Απριλίου του 2001, προστέθηκε στο ελληνικό Σύνταγμα η διάταξη 9Α, με την οποία κατοχυρώνεται η προστασία των δεδομένων προσωπικού χαρακτήρα, σύμφωνα με την οποία: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Το δικαίωμα προστασίας από τη συλλογή και επεξεργασία προσωπικών δεδομένων, έχει ειδικό χαρακτήρα και δεν αποτελεί απλή εξειδίκευση των υποχρεώσεων του κράτους απέναντι στα άλλα δικαιώματα, όπως προβλέπει το άρθρο 25 του Συντάγματος. Σημειώνεται, ότι και πριν από τη ρητή Συνταγματική κατοχύρωση του δικαιώματος, η εν λόγω προστασία βρισκόταν υπό την σκέπη γενικότερων διατάξεων, όπως αυτή του άρθρου 9 παρ. 1 ή του άρθρου 5 παρ. 1Σ ή σε συνδυασμό αυτών κατά περίπτωση, με την προστασία της ανθρώπινης αξίας (άρθρο 2 παρ. 1 Σ)[82]. Η εισαγωγή ιδιαίτερης διατάξεως για την προστασία προσωπικών δεδομένων και η προτίμηση του συντακτικού νομοθέτη, της μη φιλοξενίας του δικαιώματος σε ένα πλέγμα συνταγματικών διατάξεων, φανερώνει την ιδιαίτερη και αυτοτελή αξία του[83].

---

[80] Human Rights Council, "The right to privacy in the digital age", 4 Aug. 2022, p.13.

[81] European Parliament, Requested by the PEGA committee, "The use of Pegasus and equivalent surveillance spyware", Feb. 2023, p. 78.

[82] ΣΥΝΤΑΓΜΑ Ερμηνεία κατ' 'άρθρο, Άρθρο 9Α, Φερενίκη Παναγοπούλου, Ηλεκτρονική Έκδοση, Επιμέλεια Σπ. Βλαχόπουλος, Ξ. Κοντιάδης, Γ. Τασόπουλος, Ιανουάριος 2023, σελ. 6, Διαθέσιμο στο:https://www.syntagmawatch.gr/wp-content/uploads/2023/02/%CE%86%CF%81%CE%B8%CF%81%CE%BF-9%CE%91-%CE%9C%CE%95-COVER-1.pdf

[83] Το άρθρο 8 του ΧΘΔΕΕ αναγνωρίζει ρητώς την προστασία των δεδομένων προσωπικού χαρακτήρα ως αυτοτελές θεμελιώδες δικαίωμα, διακριτό από το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής.

Η σύνδεση της προστασίας προσωπικών δεδομένων με την προστασία του ιδιωτικού βίου, είναι αδιαμφισβήτητη, καθώς ο ιδιωτικός βίος εμπεριέχει την πληροφοριακή ιδιωτικότητα, χωρίς όμως να περιορίζεται σε αυτήν. Ειδικότερα, το άρθρο 9Α του Συντάγματος, παρέχει ένα ευρύτερο πεδίο εφαρμογής, καθώς αφορά κάθε είδους προσωπικά δεδομένα και όχι μόνο πληροφορίες που ανάγονται στον στενό πυρήνα της ιδιωτικής ζωής. Πρόκειται δηλαδή για ένα αμυντικό δικαίωμα με το οποίο, θεμελιώνεται πρωτίστως η προστασία του ατόμου έναντι της συλλογής, επεξεργασίας και χρήσης των δεδομένων του, αφετέρου δε κατοχυρώνεται και το δικαίωμα της πληροφοριακής αυτοδιάθεσης. Η διάταξη αυτή δεν συνεπάγεται απόλυτη απαγόρευση της επεξεργασίας δεδομένων, αλλά προβλέπει την υποχρέωση για τη διαμόρφωση ενός νομικού πλαισίου, ώστε η επεξεργασία να είναι νόμιμη και θεμιτή. Συνεπώς, η Συνταγματική αυτή κατοχύρωση, αντανακλά την ανάγκη θωράκισης του ατόμου, έναντι των διαρκώς αυξανόμενων δυνατοτήτων συλλογής και επεξεργασίας μεγάλου όγκου δεδομένων, λαμβανομένης υπόψη της ραγδαίας εξέλιξης της τεχνολογίας.

Η Συνταγματική αυτή ρύθμιση, συμπληρώνεται από το ευρωπαϊκό θεσμικό πλαίσιο και ιδίως από τον ΓΚΠΔ. Ειδικότερα, στο άρθρο 5 του ΓΚΠΔ ,κατοχυρώνονται οι βασικές αρχές επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως η αρχή της νομιμότητας, αντικειμενικότητας, διαφάνειας, η αρχή του περιορισμού του σκοπού, η αρχή ελαχιστοποίησης των δεδομένων κλπ. Οι αρχές αυτές, αποτελούν τον ακρογωνιαίο λίθο της θεσμικής αρχιτεκτονικής του ΓΚΠΔ και λειτουργούν ως δεσμευτικά όρια, οιασδήποτε μορφής επεξεργασίας, είτε αυτή διενεργείται από κρατικούς, είτε από ιδιωτικούς φορείς.

Καθίσταται σαφές, ότι η παρακολούθηση μέσω κατασκοπευτικών λογισμικών, συνιστά σοβαρή επέμβαση στην ιδιωτική σφαίρα του ατόμου, δεδομένου ότι συνεπάγεται τη συστηματική συλλογή δεδομένων πάσης φύσεως και δη ευαίσθητων. Εάν αναλογιστεί κανείς το εύρος των λειτουργιών ενός σύγχρονου «έξυπνου» κινητού τηλεφώνου, γίνεται εύκολα αντιληπτό το απόθεμα πληροφοριών που αποσπώνται, με την παγίδευση μιας τέτοιας συσκευής από λογισμικό κατασκοπείας. Υπό αυτή την έννοια, δεν αποτελεί υπερβολή η αναφορά στα σύγχρονα λογισμικά ψηφιακής επιτήρησης ως «game changer[s]»[84]. Ο βαθμός διείσδυσής στο λειτουργικό σύστημα της συσκευής και η δυνατότητα αδιάκριτης

[84]Σύμφωνα με τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων το κατασκοπευτικό λογισμικό Pegasus, λόγω των ιδιαίτερων χαρακτηριστικών του, συνιστά «game changer», καθώς προσφέρει επίπεδα εισβολής που δεν συγκρίνονται με προηγούμενα συστήματα και διαθέτει δυνατότητες που καθιστούν πολλά από τα υπάρχοντα νομικά και τεχνικά μέτρα αδρανή και ουσιαστικά αναποτελεσματικά.

πρόσβασης στο σύνολο των αποθηκευμένων δεδομένων, ενισχύουν τις ανησυχίες περί μιας νέας μορφής «κατασκοπευτικού καπιταλισμού» και μαζικής εκμετάλλευσης προσωπικών δεδομένων[85]. Υπό το πρίσμα αυτό, απαιτείται να εξεταστεί κατά πόσο θίγεται ο πυρήνας του δικαιώματος της προστασίας προσωπικών δεδομένων, ήτοι της ιδιωτικότητας και της πληροφοριακής αυτοδιάθεσης του ατόμου.

Τέλος, ζήτημα μείζονος σημασίας και εξαιρετικού νομικού ενδιαφέροντος, αποτελεί η νομιμότητα της εκάστοτε επεξεργασίας προσωπικών δεδομένων, μέσω των λογισμικών κατασκοπείας. Τα δεδομένα προσωπικού χαρακτήρα, ιδίως εκείνα που συλλέγονται με τέτοια εργαλεία προηγμένης τεχνολογίας, πρέπει να επεξεργάζονται αποκλειστικά στη βάση που προβλέπεται στο άρθρο 6 του ΓΚΠΔ, διαφορετικά δεν θεωρείται σύννομη. Ενόψει των ανωτέρω, η χρήση κατασκοπευτικών λογισμικών, είτε από δημόσιους είτε από ιδιωτικούς φορείς, εγείρει σοβαρές ανησυχίες ως προς τη συμβατότητά της με τις νόμιμες προϋποθέσεις επεξεργασίας και τις θεμελιώδεις αρχές του ΓΚΠΔ. Η έλλειψη διαφάνειας και ο βαθμός παρεμβατικότητας, καθιστούν εξαιρετικά δυσχερή την τήρηση της αρχής της διαφάνειας, της αναλογικότητας, της ελαχιστοποίησης των δεδομένων και της λογοδοσίας. Ως εκ τούτου, τα λογισμικά κατασκοπείας δοκιμάζουν τα όρια της Συνταγματικής και Ενωσιακής προστασίας των προσωπικών δεδομένων, θέτοντας ζήτημα ουσιαστικής διασφάλισης του πυρήνα του δικαιώματος.

4.4 Δικαίωμα προστασίας απορρήτου των επικοινωνιών

Η κρισιμότητα της προστασίας του επικοινωνιακού απορρήτου, ως πτυχή του δικαιώματος στην προστασία του ιδιωτικού βίου είναι αυταπόδεικτη. Πρόκειται για δικαίωμα που άπτεται του πυρήνα της ανθρώπινης υπόστασης και ως εκ τούτου δεν επιδέχεται εύκολους συμψηφισμούς και περιορισμούς, χωρίς ειδική, σαφή και εμπεριστατωμένη αιτιολογία. Η διασφάλιση της απρόσκοπτης άσκησής του, δεν συνιστά απλώς μια ατομική εγγύηση έναντι των κρατικών επεμβάσεων, αλλά αποτελεί αναγκαία προϋπόθεση, για την ουσιαστική πραγμάτωση κι άλλων συναφών θεμελιωδών δικαιωμάτων, όπως η ελευθερία της έκφρασης, η ελεύθερη ανάπτυξη της προσωπικότητας κοκ.

---

[85]Παπανικολάου, Α. Syntagmawatch (2022): «Επικοινωνιακό απόρρητο: προβληματισμοί για τη διασφάλιση ενός κλασικού δικαιώματος στο πεδίο των σύγχρονων κατασκοπευτικών λογισμικών». Διαθέσιμο στο: https://www.syntagmawatch.gr/trending-issues/epikoinwniako-aporrhto-provlhmatismoi-gia-th-diasfalish-enos-klasikou-dikaiwmatos-sto-pedio-twn-sygxronwn-kataskopeutikwn-logismikwn/#_ftn20

Σε εθνικό επίπεδο το απόρρητο των επικοινωνιών κατοχυρώνεται στο άρθρο 19 του ελληνικού Συντάγματος, σύμφωνα με το οποίο, αποτελεί ένα απολύτως απαραβίαστο δικαίωμα και η παράκαμψη αυτού επιτρέπεται, μόνο για λόγους Εθνικής Ασφάλειας ή για τη διερεύνηση ιδιαίτερα σοβαρών εγκλημάτων. Η έννοια της «Εθνικής Ασφάλειας», ως λόγου που δύναται να δικαιολογήσει την άρση του απορρήτου, αποσαφηνίζεται από το Νόμο 5002/2022, ο οποίος ρυθμίζει τη διαδικασία άρσης του απορρήτου των επικοινωνιών και τις σχετικές εγγυήσεις προστασίας. Ειδικότερα κατά το άρθρο 3 του οικείου νόμου, λόγοι Εθνικής Ασφάλειας, νοούνται εκείνοι που συνδέονται με την προστασία των βασικών λειτουργιών του κράτους και των θεμελιωδών συμφερόντων της χώρας, όπως ιδίως ζητήματα εθνικής άμυνας, εξωτερικής πολιτικής, ενεργειακής ασφάλειας και Κυβερνοασφάλειας. Αρμόδια για τον έλεγχο τήρησης των σχετικών εγγυήσεων, είναι η ΑΔΑΕ.

Σε διεθνές επίπεδο, στο άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου, κατοχυρώνεται το δικαίωμα κάθε προσώπου, στον σεβασμό της ιδιωτικής και της οικογενειακής του ζωής. Η οποιαδήποτε επέμβαση δημόσιας αρχής, επιτρέπεται μόνον εφόσον προβλέπεται από τον νόμο, επιδιώκει θεμιτό σκοπό και είναι απολύτως αναγκαία σε μια δημοκρατική κοινωνία, δηλαδή πληροί την αρχή της αναλογικότητας[86]. Το ΕΔΔΑ, έχει αποφανθεί επανειλημμένα, ότι τα συστήματα μυστικής παρακολούθησης συνιστούν σοβαρή επέμβαση στον πυρήνα του προστατευόμενού στο άρθρο 8, εννόμου αγαθού. Σύμφωνα με την παράγραφο 2 της οικείας διάταξης, μια τέτοια επέμβαση, δύναται να δικαιολογηθεί εφόσον είναι σύμφωνη με το νόμο, επιδιώκει έναν από τους περιοριστικά αναφερόμενους θεμιτούς σκοπούς (όπως η Εθνική Ασφάλεια, η δημόσια τάξη, η πρόληψη εγκλήματος) και ανταποκρίνεται σε επιτακτική κοινωνική ανάγκη, δηλαδή είναι αναλογική προς τον επιδιωκόμενο σκοπό. Κατά συνέπεια, η παρακολούθηση μέσω κατασκοπευτικών λογισμικών δύναται να θεωρηθεί θεμιτή, μόνο εφόσον πληρούνται σωρευτικά οι ανωτέρω προϋποθέσεις. Ειδικότερα, όταν η παρακολούθηση γίνεται από τις κρατικές αρχές για λόγους Εθνικής Ασφάλειας, το Δικαστήριο αναγνωρίζει στα Κ-Μ, ένα περιορισμένο περιθώριο εκτίμησης, ως προς τον προσδιορισμό των απειλών και των κατάλληλων μέσων αντιμετώπισης τους. Για την ορθή εφαρμογή του περιορισμού αυτού, το Δικαστήριο απαιτεί

[86] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, Right to respect for private and family life, 1st Edition, pg. 7 Διαθέσιμο στο: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/11/Guide-to-Art.-8-of-the-ECtHR-COE-and-ECtHR.pdf

την ύπαρξη επαρκών και αποτελεσματικών εγγυήσεων, όπως η εποπτεία από ανεξάρτητα όργανα, εξουσιοδοτημένα να επαληθεύουν, ακόμα και μέσω κάποιας αντιπαραθετικής διαδικασίας, ότι η εκάστοτε επίκληση απειλής για λόγους Εθνικής Ασφάλειας είναι εύλογη και τεκμηριωμένη. Συνεπώς, παρόλο που οι εθνικές αρχές απολαμβάνουν μια ελευθερία κινήσεων, το συμφέρον του κράτους για την προστασία της Εθνικής Ασφάλειας οφείλει να εξισορροπείται με τη σοβαρότητα της επέμβασης, στο δικαίωμα του ατόμου, καθώς και στο σεβασμό της ιδιωτικής του ζωής[87].

Αντίστοιχα σε Ενωσιακό επίπεδο, τα άρθρα 7 και 8 του ΧΘΔΕΕ, εμπεδώνουν ένα αυξημένο επίπεδο προστασίας της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα. Η σχετική νομολογία του ΔΕΕ, επιβάλλει την αυστηρή τήρηση των αρχών της νομιμότητας, της αναγκαιότητας και της αναλογικότητας, ιδίως όταν πρόκειται για τεχνολογικά προηγμένα μέσα επιτήρησης.

Παρά τις ρητές διαβεβαιώσεις των κατασκευαστριών εταιρειών, περί αποκλειστικού προορισμού των προϊόντων τους για την καταπολέμηση του οργανωμένου εγκλήματος, της τρομοκρατίας και άλλων μορφών βαριάς εγκληματικότητας (απαγωγές, κακοποίηση ανηλίκων κοκ), η πραγματικότητα καταδεικνύει, ότι η χρήση τους δεν εξαντλείται στην καταγραφή συνομιλιών κατόπιν σχετικής νόμιμης άδειας. Αντίθετα, λειτουργούν ως ένας μηχανισμός πλήρους ελέγχου της ηλεκτρονικής συσκευής, αποκτώντας πρόσβαση τόσο στο λειτουργικό της σύστημά, όσο και στις εγκαταστημένες εφαρμογές. Η πρόσβαση αυτή, μπορεί να οδηγήσει σε μαζική παρακολούθηση ατόμων και κατ' επέκταση στην αθέμιτη συλλογή πάσης φύσεως δεδομένων, τα οποία δύναται να αποκαλύψουν έμμεσα ή άμεσα ευαίσθητες πληροφορίες, οι οποίες άπτονται της οικογενειακής ζωής και εν γένει του ιδιωτικού βίου του υποκειμένου. Συνεπώς, το κρίσιμο νομικό ζήτημα το οποίο εγείρεται, αφορά τόσο την αποτελεσματικότητα των υφιστάμενων νομοθετικών εγγυήσεων, όσο και την πιθανή καταχρηστική επίκληση αυτών. Για το λόγο αυτό, απαιτείται επαναξιολόγηση των ορίων της κρατικής παρέμβασης, δεδομένης και της διαρκούς τεχνολογικής εξέλιξης, ούτως ώστε να διασφαλιστεί η αρχή της αναλογικότητας και η προστασία του πυρήνα του δικαιώματος.

[87] The impact of Pegasus on fundamental rights and democratic processes, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, January 2023, p. 42, Available at : https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ: ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΚΑΤΑΣΚΟΠΕΙΑΣ ΣΤΗΝ ΕΕ

5.1 Νομικά ζητήματα

Το ζήτημα της νομιμότητας της χρήσης κατασκοπευτικών λογισμικών, δε δύναται να απαντηθεί με απόλυτο και μονοσήμαντο τρόπο, αλλά απαιτείται η συστηματική ερμηνεία τόσο του Ενωσιακού, όσο και του Εθνικού πλαισίου προστασίας των πληροφοριακών συστημάτων και των θεμελιωδών δικαιωμάτων. Το θέμα δε αυτό καθίσταται περισσότερο πολύπλοκο, στις περιπτώσεις χρήσης τέτοιου λογισμικού από κυβερνητικούς οργανισμούς. Όπως ήδη αναφέρθηκε κατά κανόνα, η χρήση του, δεν είναι νόμιμη ούτε ως προς την τακτική που χρησιμοποιείται (παράνομη και εν αγνοία του χρήστη εισβολή), αλλά ούτε και κρινόμενη από το ανιδιοτελή σκοπό εφαρμογής τους, συλλογή ευαίσθητων πληροφοριών, παραβίαση ιδιωτικότητας, παρακολούθηση δεν μπορεί να χαρακτηριστεί ως νόμιμη. Κάποιες εξαιρέσεις όπως γονικής παρέμβασης για προστασία εθνικού συμφέροντος, αντιμετώπιση τρομοκρατικών απειλών, προστασία ανηλίκων ή από εταιρείες για προάσπιση νόμιμων και κατοχυρωμένων συμφερόντων τους ή ασφάλειας δικτύων, κινούνται στο πλαίσιο της νομιμότητας, χωρίς ενίοτε μέτρα προστασίας των θεμελιωδών δικαιωμάτων. Αφού λοιπόν αυτά τα κατασκοπευτικά λογισμικά, δεν χαρακτηρίζονται ως παράνομα, αρκετές εταιρείες κατασκευάζουν και διαθέτουν τα προϊόντα τους σε κρατικούς φορείς, στο πλαίσιο επιβολής του νόμου, με σκοπό την εξακρίβωση και καταπολέμηση σοβαρών ποινικών αδικημάτων ή την προστασία της εθνικής ασφάλειας όπως προαναφέρθηκε. Μάλιστα ορισμένες εταιρείες διαβεβαιώνουν, ότι τα λογισμικά κατασκοπείας διατίθενται αποκλειστικά μόνο σε κυβερνήσεις και επίσημους οργανισμούς για την επιβολή του νόμου και ότι η ευθύνη για τυχόν παρεκκλίσεις από τη νομιμότητα, βαραίνει αποκλειστικά τις αρχές που τις προμηθεύονται και τις χρησιμοποιούν[88]. Αν και η διαδικασία παραγωγής και απόκτησης θεωρείται νομικά αποδεκτή, εγείρονται θέματα ως προς τη νομιμότητα χρήσης τους και συγκεκριμένα ως προς τον τρόπο, το πλαίσιο και τις εγγυήσεις υπό τις οποίες αυτά χρησιμοποιούνται, δηλαδή παράγοντες που δεν αφορούν στη φύση κατασκευής τους και στην τεχνολογική τους υφή. Σαφώς απαιτείται διερεύνηση, όπου θα αποτυπώνονται οι διακριτές ευθύνες όλων των εμπλεκομένων, τόσο από πλευράς

[88] Εφημερίδα Εστία, «Ραγδαίες εξελίξεις. Παρέχουμε μόνο υπηρεσίες σε κυβερνήσεις και υπηρεσίες επιβολής του νόμου», αρ. φύλλου 43394, 14/3/2026.

σχεδίασης, παραγωγής και διάθεσης του εν λόγω προϊόντος, όσο χρησιμοποίησης αυτών συμπεριλαμβανομένης της αναγκαιότητας και του σκοπού.

- **Σύμβαση της ΕΕ για το Κυβερνοέγκλημα**

Με τη σύμβαση της ΕΕ για το έγκλημα στον κυβερνοχώρο (Σύμβαση Βουδαπέστης), που κυρώθηκε από το ελληνικό κοινοβούλιο με το νόμο 4411/2016 (ΦΕΚ 142/Α/3-8-2016, λαμβάνεται μέριμνα για την καταπολέμηση των εγκλημάτων που μπορούν να γίνουν αποκλειστικά με τη χρήση τεχνολογίας, όπου οι συσκευές καθίστανται τόσο εργαλείο τέλεσης, όσο και ο στόχος του εγκλήματος. Στην πρόβλεψη αυτή, συμπεριλαμβάνεται και η περίπτωση, όπου η τεχνολογία έχει χρησιμοποιηθεί για τη διευκόλυνση τέλεσης άλλου εγκλήματος, για παράδειγμα απάτης. Παρέχει επίσης κατευθυντήριες γραμμές στην εθνική νομοθεσία των Κ-Μ και λειτουργεί ως βάση για τη διεθνή συνεργασία μεταξύ των συμβαλλομένων[89]. Επιπλέον, στο άρθρο 2 της Σύμβασης της Βουδαπέστης, ορίζεται ότι «η εκ προθέσεως και χωρίς δικαίωμα πρόσβαση στο σύνολό του ή σε μέρος του πληροφοριακού συστήματος, συνιστά αξιόποινη πράξη». Σύμφωνα με την Αιτιολογική Έκθεση της Σύμβασης (Explanatory Report to the Convention on Cybercrime/23 Νοεμβρίου 2001), στην έννοια της υποκλοπής (interception), περιλαμβάνονται οι έννοιες της ακρόασης (listening), της παρακολούθησης (monitoring), της επιτήρησης (surveillence) και της καταγραφής (recording). Η υποκλοπή μπορεί επίσης να περιλαμβάνει την καταγραφή. Τα τεχνικά μέσα, περιλαμβάνουν ηλεκτρονικές συσκευές που είναι στερεωμένες σε γραμμές μεταφοράς, καθώς και συσκευές για τη συλλογή και καταγραφή ασύρματων επικοινωνιών. Επίσης, στην Αιτιολογική Έκθεση, αναλύεται η έννοια «μη δημόσιων μεταδόσεων», που αναφέρεται στο άρθρο 3 της Σύμβασης, «κάθε Συμβαλλόμενο Μέρος λαμβάνει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο η υποκλοπή, δια τεχνικών μέσων μη δημόσιων». Ο όρος μη δημόσιο, προσδιορίζει τη φύση της διαδικασίας μετάδοσης (επικοινωνίας) και όχι τη φύση των δεδομένων που μεταδίδονται. Τα δεδομένα που κοινοποιούνται, μπορεί να είναι δημόσια διαθέσιμες πληροφορίες, αλλά τα μέρη επιθυμούν να επικοινωνούν εμπιστευτικά. Επίσης, τα δεδομένα μπορούν να διατηρούνται μυστικά για εμπορικούς σκοπούς ή μέχρι να πληρωθεί η υπηρεσία, όπως στην συνδρομητική

[89] Council of Europe, "CONVENTION ON CYBERCRIME", Budapest 23 Nov, 2001.

τηλεόραση. Εκτός των άλλων ο όρος δεν εφαρμόζεται, καθώς εξαιρεί τις επικοινωνίες μέσω δημόσιων δικτύων[90].

- **Οδηγία 2013/40/ΕΕ**

Η Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις επιθέσεις κατά συστημάτων πληροφοριών, η οποία και αυτή ενσωματώθηκε στην ελληνική έννομη τάξη με το νόμο 4411/2016, αποσκοπεί στην εναρμόνιση της ποινικής νομοθεσίας των Κ-Μ και στη βελτίωση της συνεργασίας των αρμόδιων υπηρεσιών, τους με τους υπεύθυνους φορείς της ΕΕ, ενισχύοντας το ποινικό οπλοστάσιο έναντι επιθέσεων σε πληροφοριακά συστήματα[91]. Ειδικότερα, στο άρθρο 6 της παρούσης Οδηγίας, ρυθμίζεται η παράνομη υποκλοπή, σύμφωνα με το οποίο «Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα, σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών, από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις»[92]. Σύμφωνα με την Αιτ. Σκέψη 9 της Οδ. 2013/40/ΕΕ στην έννοια της υποκλοπής, περιλαμβάνεται ενδεικτικά η ακρόαση ή επιτήρηση του περιεχομένου των επικοινωνιών και η παροχή του περιεχομένου των δεδομένων είτε άμεσα, μέσω της πρόσβασης και χρήσης των συστημάτων πληροφοριών, είτε έμμεσα μέσω της χρήσης ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα.

- **Εμπλεκόμενες Ανεξάρτητες Αρχές**
  - ✓ **Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)**

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, είναι συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή (άρθρο 9Α του Συντάγματος), και έχει ως αποστολή τον έλεγχο της εφαρμογής του ΓΚΠΔ, του νόμου 4624/2019, του νόμου 3471/2006, καθώς και άλλων διατάξεων που διέπουν την προστασία του ατόμου από την επεξεργασία

---

[90] Αιτιολογική Έκθεση της Σύμβασης για το Κυβερνοέγκλημα, Παρ. 53, 54, π.10, Available at. https://rm.coe.int/16800cce5b

[91]Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, ΟΔΗΓΙΑ 2013/40/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ, «για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου», 14 Αυγ. 2013

[92] Θεοχάρης Ι. Δαλακούρας, Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Νομική Βιβλιοθήκη, 2η Έκδοση, σελ. 6.

δεδομένων προσωπικού χαρακτήρα. Πέραν τούτου συμβάλλει στην εφαρμογή του ΓΚΠΔ σε ολόκληρη την Ένωση και για το λόγο αυτό συνεργάζεται με τις εποπτικές αρχές των κρατών μελών της ΕΕ και με την Επιτροπή (άρθρο 51 παρ. 2, αιτ. σκ. 123 του ΓΚΠΔ άρθρο 10 του ν. 4624/2019). Η Αρχή εκπροσωπεί την Ελλάδα στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) και σε άλλες επιτροπές ή όργανα που έχουν ως αποστολή, την προστασία δεδομένων και συνεργάζεται επίσης με αντίστοιχες αρχές τρίτων χωρών και διεθνείς οργανισμούς (άρθρο 50 του ΓΚΠΔ, άρθρο 10 του ν. 4624/2019) [93].

- ✓ **Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)**

Έχει από το Σύνταγμα την αρμοδιότητα της διασφάλισης του απορρήτου των επικοινωνιών[94]. Συγκροτήθηκε με το άρθρο 1 του Ν. 3115/2003(ΦΕΚ 47/Α/27-2-2003), με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο, καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών, περιλαμβάνεται και ο έλεγχος της διαδικασίας άρσης του απορρήτου.

- ✓ **Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)**

Συνεργάζεται με κάθε εθνική δημόσια αρχή για θέματα κοινού ενδιαφέροντος, καθώς και με το Σώμα Ευρωπαίων Ρυθμιστών για τις Ηλεκτρονικές Επικοινωνίες (Body of European Regulators for Electronic Communications-BEREC), τις Εθνικές Ρυθμιστικές Αρχές (ΕΡΑ) άλλων Κ-Μ της ΕΕ ή τρίτων κρατών, καθώς και με διεθνείς φορείς. Τηρεί μητρώο παρόχων ενδιάμεσων ψηφιακών υπηρεσιών.

Εποπτεύει τους παρόχους ενδιάμεσων ψηφιακών υπηρεσιών, που υπάγονται στη δικαιοδοσία της Ελλάδας ως προς την τήρηση των υποχρεώσεων που επιβάλλει η Πράξη για τις Ψηφιακές Υπηρεσίες και ο Ν.5099/2024. Εξαιρούνται οι υποχρεώσεις που προβλέπονται στα άρθρα 26 (διαφήμιση) και 28 (προστασία ανηλίκων) της Πράξης, για τα οποία αρμοδιότητα έχουν το Εθνικό Συμβούλιο Ραδιοτηλεόρασης (ΕΣΡ) και η ΑΠΔΠΧ. Τηρεί μητρώο παρόχων ενδιάμεσων ψηφιακών υπηρεσιών και διενεργεί ακροάσεις για τη διαπίστωση παραλείψεων και την επιβολή κυρώσεων σε παρόχους ενδιάμεσων ψηφιακών υπηρεσιών, για παραβάσεις εφόσον απαιτηθεί[95].

---

[93] https://www.dpa.gr/el/arxi/armodiotites

[94] Το Άρθρο 19 παρ. 2 « Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1».

[95] Αρμοδιότητες ΕΕΤΤ, διαθέσιμο σε https://www.eett.gr/eett/schetika-me-tin-eett/armodiotites/

- ✓ **Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ)**

Τα καθήκοντα της Εθνικής Αρχής Κυβερνοασφάλειας, ορίζονται από το Ν. 5086/2024 (ΦΕΚ Α 23 – 14.02.2024) και το νέο εφαρμοστικό νόμο για την ενσωμάτωση της Οδηγίας NIS2, 2022/2555/ΕΕ. Η ΕΑΚ έχει ρόλο κανονιστικό, εποπτικό, συντονιστικό, συμβουλευτικό, ελεγκτικό και κυρωτικό. Εκπληρώνει έναν πολυδιάστατο ρόλο, για την ενίσχυση της Κυβερνοασφαλειας, διασφαλίζοντας την προστασία των εθνικών ψηφιακών υποδομών και την οικοδόμηση ενός ασφαλούς ψηφιακού διαδικτυακού συστήματος[96] .

- ✓ **Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ)**

Αποστολή έχει τη συλλογή, ανάλυση και κοινοποίηση πληροφοριών στις αρμόδιες αρχές, για την πρόληψη και την αντιμετώπιση κατασκοπείας και τρομοκρατικής απειλής, απειλών για την Κυβερνοασφάλεια, καθώς επίσης και απειλή κατά του δημοκρατικού πολιτεύματος, των θεμελιωδών ανθρωπίνων δικαιωμάτων, της εδαφικής ακεραιότητας της χώρας και της Εθνικής Ασφάλειας. Με το Προεδρικό Διάταγμα (ΠΔ) 81/2019 (ΦΕΚ Α' 119/08.07.2019), άρθρο 5 παρ. 3, η υπαγωγή της μεταφέρθηκε στον Πρωθυπουργό[97]. Στο άρθρο 4 του Ν. 5002/2022, περιγράφεται η διαδικασία απορρήτου από την ΕΥΠ, για λόγους Εθνικής Ασφάλειας.

5.2 Προστασία επικοινωνιών και διαδικασία άρσης του απορρήτου των επικοινωνιών

Η ανάγκη προστασίας τόσο της ιδιωτικής ζωής, όσο και των λοιπών θεμελιωδών δικαιωμάτων από τη χρήση κατασκοπευτικών λογισμικών, αποτελεί ζήτημα υψίστης σημασίας για την Ενωσιακή και κατ' επέκταση για την Εθνική έννομη τάξη. Στο σημείο αυτό, αξίζει να σημειωθεί ότι η αντιμετώπιση του φαινομένου αυτού, γίνεται μέσω ενός κατακερματισμένου και όχι ενός ενιαίου νομικού πλαισίου. Η πρώτη αξιοσημείωτη προσπάθεια της ΕΕ, αποτελεί η Οδηγία 2002/58/ΕΕ (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες),γνωστή και ως «ePrivacy Directive», η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με το Ν. 3471/2006 και έθεσε τις βασικές αρχές για την προστασία του απορρήτου των τηλεφωνικών και ηλεκτρονικών επικοινωνιών[98].

[96] https://cyber.gov.gr/eak/tautotita/

[97] «Η Εθνική Υπηρεσία Πληροφοριών η οποία συστάθηκε με το άρθρο 1 του ν.δ. 2421/1953 και μετονομάστηκε και οργανώθηκε με το ν. 1645/1986 και το ν. 3649/2008 (Α' 39) μεταφέρεται, ως σύνολο αρμοδιοτήτων, θέσεων, και προσωπικού, στον Πρωθυπουργό».

[98] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Σημειώνεται, ότι με το Ν. 5002/2022 (ΦΕΚ Α' 228/09.12.2022), «Διαδικασία άρσης του απορρήτου των επικοινωνιών, Κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών», εισήχθη η ποινική τυποποίηση, τόσο της παράνομης πρόσβασης σε σύστημα πληροφοριών, όσο και της απαγόρευσης διακίνησης λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων, όπως αυτά προβλέπονται στα άρθρα 370Β και 370ΣΤ του ελληνικού Ποινικού Κώδικα, αντίστοιχα[99]. Υπό το πρίσμα αυτό, η παρακολούθηση με μη εξουσιοδοτημένη εγκατάσταση και χρήση ενός κακόβουλου λογισμικού σε συσκευή τρίτου προσώπου, συνιστά καταρχήν παράνομη πράξη και πληροί τα στοιχεία της παράνομης πρόσβασης και υποκλοπής δεδομένων[100]. Στο άρθρο 6, περιγράφονται οι περιπτώσεις που επιβάλλεται άρση απορρήτου επικοινωνιών για προσβολή του δημοκρατικού πολιτεύματος, της διεθνούς υπόστασης της χώρας, περί εγκλημάτων κατά των πολιτειακών και πολιτικών οργάνων, εγκλημάτων κατά της δημόσιας τάξης, εγκλημάτων κατά της προσωπικής ελευθερίας, κατασκοπείας, τρομοκρατικών πράξεων, λογισμικού και συσκευών παρακολούθησης κ.α. Επίσης, στη διαδικασία άρσης περιλαμβάνονται και οι περιπτώσεις παρ. 5 του άρθρου 38 του Ν. 4624/2019 (ΦΕΚ Α' 137/29-08-2019), περί πρόσβασης και τήρησης των δεδομένων προσωπικού χαρακτήρα.

Στο άρθρο 13 του Νόμου αυτού, ορίζεται ότι με ΠΔ που εκδίδεται εντός τριών μηνών από την έναρξη ισχύος του παρόντος και μετά από πρόταση των Υπουργών Προστασίας του Πολίτη, Εθνικής Άμυνας και Ψηφιακής Διακυβέρνησης, ρυθμίζονται οι προϋποθέσεις υπό τις οποίες είναι επιτρεπτή η σύναψη συμβάσεων εκ μέρους κρατικών δομών, για την προμήθεια λογισμικών ή συσκευών παρακολούθησης που εμπίπτουν στο άρθρο 370ΣΤ του ΠΚ. Το σχετικό ΠΔ δεν έχει μέχρι σήμερα εκδοθεί και υπό το πρίσμα των πρόσφατων παρακολουθήσεων η παρουσία του αναμένεται να αποσαφηνίσει ορισμένες προβλέψεις του εν λόγω νόμου παρέχοντας περισσότερες λεπτομέρειες εφαρμογής του.

Σημειώνεται, ότι κατά το στάδιο διαβούλευσης του Νόμου, η ΑΔΑΕ επισήμανε εγγράφως, επιφυλάξεις για τις εισαγόμενες ρυθμίσεις στο νέο νομοθετικό πλαίσιο. Ιδιαίτερα δε αποφάνθηκε για την ανάθεση της αρμοδιότητας έκδοσης της άρσης του

[99] Λεωνίδας Γ. Κοτσαλής, Ποινικός Κώδικας. Νομική Βιβλιοθήκη, Έκδοση 22η, Αθήνα 2024, σ. 216, 218.

[100] Σύμφωνα με την Αιτ. Σκέψη 9 της Οδ. 2013/40/ΕΕ στην έννοια της υποκλοπής περιλαμβάνεται ενδεικτικά η ακρόαση ή επιτήρηση του περιεχομένου των επικοινωνιών και η παροχή του περιεχομένου των δεδομένων είτε άμεσα, μέσω της πρόσβασης και χρήσης των συστημάτων πληροφοριών, είτε έμμεσα μέσω της χρήσης ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα. Τέτοια τεχνικά μέσα λοιπόν, μπορεί να είναι τα λογισμικά κατασκοπείας.

απορρήτου για λόγους Εθνικής Ασφάλειας, σε εισαγγελικό λειτουργό και συγκεκριμένα σε εισαγγελέα εφετών, ο οποίος αποσπάται από φυσικό του χώρο, που είναι το δικαστήριο που ανήκει, και λειτουργεί πλέον στο περιβάλλον της ΕΥΠ και τη Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας (ΔΑΕΕΒ), και μάλιστα σε μακροχρόνια βάση (τρία έτη), έχει ως συνέπεια μια πιθανή ενσωμάτωση του δικαστικού λειτουργού, στο περιβάλλον και τη νοοτροπία που κυριαρχούν στις υπηρεσίες αυτές. Καταλήγοντας δε επισημαίνει, ότι αν και η διάταξη του άρθρου 4 του Νόμου, δεν είναι ευθέως αντισυνταγματική, ωστόσο απομακρύνεται από τη βούληση του συνταγματικού νομοθέτη[101].

5.3 Προστασία προσωπικών δεδομένων

Ο ΓΚΠΔ, έχει σκοπό την προστασία των φυσικών προσώπων, στην περίπτωση που τα δεδομένα τους υπόκεινται σε επεξεργασία από τον ιδιωτικό τομέα, αλλά και από το μεγαλύτερο μέρος του δημοσίου τομέα, επιτρέποντας στα άτομα να ελέγχουν καλύτερα τα δεδομένα προσωπικού χαρακτήρα τους. Στο άρθρο 4 παρ. 1 του Κανονισμού, περιγράφονται ως δεδομένα προσωπικού χαρακτήρα, κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Με τον όρο ταυτοποιήσιμο φυσικό πρόσωπο, νοείται εκείνο το πρόσωπο, του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, αριθμό ταυτότητας, σε δεδομένα θέσης, ή σε έναν ή και περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του[102].

Στο άρθρο 9 παρ. 1, του Κανονισμού απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων, με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο

[101] Σύνοδος της Ολομέλειας της, ΑΔΑΕ της 18-11-2022, προκειμένου να μελετήσει το νομοσχέδιο για την διαδικασία άρσης απορρήτου των Επικοινωνιών, την κυβερνοασφάλεια και την προστασία προσωπικών δεδομένων (που αναρτήθηκε για διαβούλευση στις 15.11.2022), διαθέσιμο σε https://www.constitutionalism.gr/wp-content/uploads/2022/11/PARATIRISEIS_ADAE_GIA_TO_NOMOSXEDIO_21-11-2022.pdf

[102] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016.

προσανατολισμό. Η ειδική διάταξη και η εξαίρεσή τους, από τα υπόλοιπα προσωπικά δεδομένα τους προσδίδει τον χαρακτηρισμό ως ευαίσθητα προσωπικά δεδομένα.

Με το Ν.4624/2019, ενσωματώθηκε στην εθνική νομοθεσία ο ΓΚΠΔ της ΕΕ. Στο άρθρο 38 του Νόμου με τίτλο ποινικές κυρώσεις, προβλέπονται αυστηρές ποινές από ένα έτος φυλάκιση ως και δέκα έτη κάθειρξη, για παραβιάσεις στα θέματα των προσωπικών δεδομένων. Στο κεφάλαιο Δ' του νόμου σχετικά με την προστασία των φυσικών προσώπων, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών .

Η προστασία των προσωπικών δεδομένων συνδέεται άμεσα μα το Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ και μάλιστα με το 8 αυτής, σύμφωνα με το οποίο:

- ✓ Κάθε άτομο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.
- ✓ Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους, που προβλέπονται από το Νόμο.
- ✓ Κάθε πρόσωπο, δικαιούται να έχει πρόσβαση στα δεδομένα που συλλέγονται και το αφορούν και να προβαίνει στη διόρθωσή τους.

5.4 Εξέλιξη του λογισμικού κατασκοπείας και Τεχνητή Νοημοσύνη

Η ΕΕ επιδεικνύοντας ιδιαίτερη ευαισθησία για την προστασία των δικαιωμάτων των πολιτών της και κατανοώντας τις απαιτήσεις για τη δημιουργία ασφαλών μοντέλων ΤΝ, δραστηριοποιήθηκε έγκαιρα και θέσπισε τον Κανονισμό Τεχνητής Νοημοσύνης, γνωστού ως AI Act. Εκδόθηκε από το Ευρωπαϊκό Συμβούλιο την 13 Ιουν 2024 (επίσημη υπογραφή), με έναρξη ισχύος την 1η Αυγούστου 2024 (η εφαρμογή των διατάξεων γίνεται τμηματικά σύμφωνα με το άρθρο 113, με πρόβλεψη το άρθρο 6 όπου αναφέρεται στα επίπεδα κινδύνου, να έλθει σε ισχύ την 2 Αυγούστου 2027). Ο σκοπός του εν λόγω Κανονισμού είναι η δημιουργία ενιαίου νομικού πλαισίου για τη διαχείριση των συστημάτων ΤΝ εντός της Ένωσης, κατά τρόπο που να προστατεύονται οι αξίες και τα θεμελιώδη δικαιώματα του ανθρώπου και παράλληλα να εξασφαλίζεται ο ανταγωνισμός[103].

[103] Κανονισμός ΕΕ, 1689/2024 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου/ 13-06- 2024

Στο άρθρο 5 του Κανονισμού, περιγράφονται ως απαγορευμένες πρακτικές, παρεμβατικές χρήσεις συστημάτων ΤΝ, μεταξύ άλλων όταν:

- Ακολουθούν παραπλανητικές τεχνικές, με σκοπό τη χειραγώγηση της συμπεριφοράς των ατόμων, ώστε να λαμβάνουν αποφάσεις, που διαφορετικά δεν θα είχαν λάβει, προκαλώντας σημαντική βλάβη.
- Εκμεταλλεύονται τα τρωτά σημεία ενός φυσικού προσώπου ή μιας συγκεκριμένης κοινωνικής ομάδας, με ιδιαιτερότητες (ηλικία, αναπηρία, κοινωνική ή οικονομική κατάσταση), με σκοπό να ελέγξει τη συμπεριφορά τους και να προκαλέσουν σημαντικές βλάβες στους ίδιους ή σε τρίτα πρόσωπα.
- Ταξινομούν τα φυσικά πρόσωπα, με βάση την κοινωνική τους συμπεριφορά, γνωστά, συναγόμενα ή προβλεπόμενα προσωπικά χαρακτηριστικά τους.
- Προβαίνουν σε εκτίμηση κινδύνου φυσικών προσώπων, για να προβλεφθεί ο κίνδυνος τέλεσης αξιόποινων πράξεων, με βάση αποκλειστικά την κατάρτιση προφίλ ή την αξιολόγηση και χαρακτηριστικών τους. (Εξαιρούνται όταν χρησιμοποιούνται για υποστήριξη ανθρώπινης αξιολόγησης, όταν ένα πρόσωπο εμπλέκεται σε εγκληματική δραστηριότητα, βάσει αντικειμενικών στοιχείων).
- Δημιουργούν ή επεκτείνουν βάσεις δεδομένων αναγνώρισης προσώπου, με τη χρήση μη στοχευμένης εξαγωγής εικόνων προσώπου, από το διαδίκτυο ή βίντεο CCTV.
- Συλλέγουν συναισθήματα φυσικών προσώπων, στους τομείς του χώρου εργασίας και των εκπαιδευτικών ιδρυμάτων. (Εξαίρεση αποτελεί όταν, τα στοιχεία προορίζονται να διατεθούν για ιατρικούς λόγους ή λόγους ασφαλείας).
- Χρησιμοποιούν συστήματα βιομετρικής κατηγοριοποίησης, που ταξινομούν φυσικά πρόσωπα, με βάση τα βιομετρικά δεδομένα τους, προς εξαγωγή συμπερασμάτων σχετικά με τη φυλή, τα πολιτικά φρονήματα, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό τους. (Η περίπτωση αυτή δεν ισχύει, για βιομετρικά δεδομένα που έχουν αποκτηθεί νόμιμα, για την επιβολή του νόμου). Επισημαίνεται, ότι η επιβολή του νόμου δεν δύναται να επικαλεστεί, στην εξ αποστάσεως βιομετρική ταυτοποίηση «σε πραγματικό χρόνο», σε δημόσια προσβάσιμους χώρους, εκτός ειδικών περιπτώσεων, τρομοκρατικής απειλής, απαγωγή, εμπορία και εξαφάνιση ανθρώπων, και για σοβαρές αξιόποινες πράξεις που τιμωρούνται στο εκάστοτε Κ-Μ, με ποινή στέρησης ελευθερίας τουλάχιστον τεσσάρων ετών.

Μάλιστα για το χαρακτηρισμό ενός συστήματος ΤΝ, υψηλού ή όχι κινδύνου, λαμβάνει υπόψη ο ενδεχόμενος, σημαντικός κίνδυνος βλάβης για την υγεία, την ασφάλεια, τα θεμελιώδη δικαιώματα φυσικών προσώπων, καθώς και τυχόν εμπλοκή, με σκοπό να επηρεάσουν ουσιωδώς το αποτέλεσμα λήψης αποφάσεων. Η παραβίαση στα θεμελιώδη δικαιώματα που προστατεύονται από τον ομώνυμο Χάρτη, έχει ιδιαίτερη σημασία για την ταξινόμηση ενός συστήματος ΤΝ ως υψηλού κινδύνου (αιτιολογική σκέψη 48).

Σύμφωνα με σχετική αναφορά του Ευρωπαϊκού Κοινοβουλίου, της 16 Φεβρουαρίου 2017 σε σύσταση προς την Επιτροπή σχετικά μα ρυθμίσεις Αστικού Δικαίου στον τομέα της ρομποτικής, ένα αυτόνομο μοντέλο ΤΝ π.χ. Ρομπότ, έχει μεγάλες πιθανότητες να προκαλέσει εγκληματικές ενέργειες ή κάποιο κακό. Από την άλλη πλευρά όμως, η τεχνολογία ΤΝ μπορεί να βοηθήσει στην αντιμετώπιση κυβερνοεπιθέσεων[104].

5.5 Περιπτώσεις νόμιμης χρήσης του λογισμικού κατασκοπείας

Στο πλαίσιο του δικαίου της ΕΕ, η στοχευμένη επιτήρηση σχετίζεται με τα δικαιώματα που κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, τις αρχές που ορίζονται στις Συνθήκες (όπως η δημοκρατία και το κράτος δικαίου) και διάφορες πράξεις του παράγωγου δικαίου της ΕΕ, όπως αυτές που αφορούν το δίκαιο προστασίας δεδομένων.

Σε διεθνές επίπεδο, η εξαγωγή κατασκοπευτικού λογισμικού, ρυθμίζεται από τη μη δεσμευτική συμφωνία Wassenaar (Arrangement Wassenaar), στην οποία συμμετέχουν όλα τα Κ-Μ της ΕΕ, εκτός από την Κύπρο. Η συμφωνία αυτή, που εγκρίθηκε το 1996, από 33 ιδρυτικές χώρες, είναι η πρώτη πολυμερής συμφωνία για τον έλεγχο εξαγωγών συμβατικών όπλων και ευαίσθητων αγαθών και τεχνολογιών διπλής χρήσης, “dual-use goods”. Το 2013 τροποποιήθηκε, ώστε να συμπεριλάβει θέματα τεχνολογίας, όπως, «λογισμικό εισβολής», «εξοπλισμός υποκλοπής ή παρεμβολής κινητών συσκευών» και «συστήματα επιτήρησης δικτύου πρωτοκόλλου Διαδικτύου[105]. Τα είδη διπλής χρήσης είναι αγαθά, λογισμικό και τεχνολογία, που μπορούν να χρησιμοποιηθούν τόσο για πολιτικές, όσο και για στρατιωτικές εφαρμογές. Στις 8 Σεπτεμβρίου 2025, η Ευρωπαϊκή Επιτροπή ενέκρινε κατ' εξουσιοδότηση με τον Κανονισμό 2025/2003/ΕΕ, επικαιροποίηση του καταλόγου στο παράρτημα του κανονισμού 2021/821 ελέγχου εξαγωγών ειδών διπλής χρήσης της ΕΕ, προσθέτοντας υλικά

[104] ΔΡ. ΓΕΩΡΓΙΟΣ Ι. ΖΕΚΟΣ, ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΑΝΤΑΓΩΝΙΣΜΟΣ (ΝΟΜΙΚΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ), Εκδ. ΣΑΚΚΟΥΛΑ, Αθήνα-Θεσσαλονίκη 2024, σελ. 112, 115.

[105] https://www.wassenaar.org/app/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf

εξελιγμένης ηλεκτρονικής τεχνολογίας, ηλεκτρονικούς υπολογιστές και λογισμικό[106]. Εδώ σημειώνεται, ότι τόσο στον αρχικό Κανονισμό, όσο και στις τροποποιήσεις που ακολούθησαν, κλείνοντας προς το παρόν τον κύκλο με την τελευταία αναφερόμενη, δεν διακρίνεται κάποια διάταξη που να εστιάζει σε χρήση κατασκοπευτικού λογισμικού.

Το Γραφείο του Ύπατου Αρμοστή του Οργανισμού Ηνωμένων Εθνών, για τα δικαιώματα του Ανθρώπου, Office of the High Commissioner for Human Rights (OHCHR), έχει επισημάνει, ότι οι περιορισμοί στα θεμελιώδη δικαιώματα, μπορούν να δικαιολογηθούν για λόγους Εθνικής Ασφάλειας μόνο, όταν προβλέπονται από το νόμο και είναι απαραίτητοι, για την επίτευξη ενός νόμιμου σκοπού και προσδιορίζοντας επακριβώς φύση της απειλής[107]. Ωστόσο, τόσο η Επιτροπή Ανθρωπίνων Δικαιωμάτων, όσο και η Γενική Συνέλευση του ΟΗΕ, έχουν επισημάνει, την ανάγκη διασφάλισης της προστασίας των ανθρωπίνων δικαιωμάτων, στο πλαίσιο της κρατικής επιτήρησης. Η Επιτροπή Ανθρωπίνων Δικαιωμάτων, έχει παρατηρήσει, ότι το δικαίωμα στην ιδιωτικότητα, απαιτεί την ύπαρξη ισχυρών και ανεξάρτητων συστημάτων εποπτείας όσον αφορά την επιτήρηση, την υποκλοπή και την πειρατεία και η Γενική Συνέλευση υπογράμμισε, ότι η επιτήρηση των ψηφιακών επικοινωνιών, πρέπει να είναι σύμφωνη με το διεθνές δίκαιο[108].

Αναζητώντας ένα έγκυρο ορισμό του όρου, «Εθνική Ασφάλεια/ National Security», διαπιστώνουμε ότι δεν υπάρχει κάτι επίσημο τουλάχιστον σε κείμενα της ΕΕ. Η Εθνική Ασφάλεια αναφέρεται στα 8, 10 και 11 της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου, ως ένας από τους θεμιτούς σκοπούς που μπορούν να δικαιολογήσουν τον περιορισμό των δικαιωμάτων, «σεβασμού της ιδιωτικής και οικογενειακής ζωής», «ελευθερίας έκφρασης» και «ελευθερίας του συνέρχεσθαι και του συνεταιρίζεσθαι», αντίστοιχα.[109]. Μέχρι σήμερα, το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων, δεν έχει δώσει κάποιο ορισμό για την Εθνική Ασφάλεια. Αντίθετα, η υφιστάμενη νομολογία, έχει

---

[106] Τα παραρτήματα V, VI, VII του Κανονισμού 2025/2003/ΕΕ, αναφέρονται σε Ηλεκτρονικά, Ηλεκτρονικούς Υπολογιστές και Τηλεπικοινωνίες και Ασφάλεια Πληροφοριών, αντίστοιχα.

[107] HUMAN RIGHTS COMMITTEE Fifty-fourth session VIEWS, Communication No. 518/1992, 19 Jul 1995 par. 10.4, available at. https://hrlibrary.umn.edu/undocs/html/vws518.htm

[108] European Parliament, STUDY Requested by the PEGA Committee "The impact of Pegasus on fundamental rights and democratic processes", p.40, Available at. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

[109] «Η άσκηση των δικαιωμάτων αυτών δεν μπορεί να υπαχθεί σε άλλους περιορισμούς από εκείνους που προβλέπονται με νόμο και αποτελούν αναγκαία μέτρα, σε δημοκρατική κοινωνία, για την εθνική ασφάλεια, τη δημόσια ασφάλεια, την προάσπιση της τάξης και την πρόληψη του εγκλήματος,την προστασία της υγείας ή της ηθικής ή την προστασία των δικαιωμάτων και ελευθεριών τρίτων».

επικεντρωθεί στις προϋποθέσεις που δικαιολογούν παρεμβάσεις, στα δικαιώματα ενός ατόμου για λόγους Εθνικής Ασφάλειας.

Στο άρθρο 23 παρ. 1 του ΓΚΠΔ της ΕΕ, ορίζεται ότι στο δίκαιο της Ένωσης ή του Κ-Μ, στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας ή ο αρμόδιος για την επεξεργασία των δεδομένων, μπορεί να περιορίζονται με νομοθετική πράξη, οι υποχρεώσεις και τα δικαιώματα που προβλέπονται στα άρθρα του Κανονισμού και με δεδομένο ότι μια τέτοια παρέμβαση, λαμβάνει υπόψη την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία, για τη διασφάλιση μεταξύ άλλων της ασφάλειας του κράτους, της Εθνικής Άμυνας, της δημόσιας ασφάλειας, της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της πρόληψης και προστασίας από απειλές κατά της δημόσιας ασφάλειας.

Το ΕΔΔΑ έχει γνωμοδοτήσει ότι, για να είναι μια παρέμβαση στο δικαίωμα ενός ατόμου σύμφωνη με το νόμο, είναι απαραίτητο να υπάρχει πρόβλεψη παρέμβασης στο εθνικό δίκαιο, το οποίο πρέπει να είναι προσβάσιμο σε όλους και να περιέχει πρόβλεψη συνεπειών για τυχόν παρεκκλίσεις. Έχει επίσης αναγνωρίσει, ότι τα κράτη έχουν δικαίωμα, να πραγματοποιούν σε ορισμένες μορφές μυστικής παρακολούθησης επικοινωνιών, όπως στις τηλεπικοινωνίες ή την ταχυδρομική αλληλογραφία, για να αντιμετωπίζουν αποτελεσματικά περιπτώσεις κατασκοπείας ή τρομοκρατίας. Αποφαίνεται δε, ότι η επιλογή του τρόπου για την προστασία της Εθνικής Ασφάλειας, έγκειται στην διακριτική ευχέρεια των κρατών.[110]

Η τρομοκρατία και το οργανωμένο έγκλημα, αποτελούν σοβαρές απειλές εντός και εκτός των συνόρων της ΕΕ και ο έγκαιρος εντοπισμός απειλών, η πρόληψη και η δίωξή του, αποτελεί προτεραιότητα για τις κρατικές οντότητες, παγκοσμίως. Επίσης, προτεραιότητα για κάθε χώρα της ΕΕ, αποτελούν τα θέματα προστασίας πληροφοριών που άπτονται της Εθνικής Κυριαρχίας τους. Ως εκ τούτου η χρήση στις περιπτώσεις αυτές του κατασκοπευτικού λογισμικού είναι επιθυμητές και επιβάλλεται. Οι διαδικασίες αυτές,

[110] Council of Bars & Law Societies of Europe, "RECOMMENDATIONS ON THE PROTECTION OF FUNDAMENTAL RIGHTS IN THE CONTEXT OF 'NATIONAL SECURITY", 2019, p.6,7, available at. https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

πιθανόν να οδηγήσουν σε περιορισμούς στην άσκηση των θεμελιωδών δικαιωμάτων και ελευθεριών του ατόμου, οι οποίοι σύμφωνα με το άρθρο 52 παρ. 1 του ΧΘΔΕΕ, είναι αποδεκτές στο βαθμό που είναι αναλογικές και απαραίτητες. Πρέπει σε κάθε περίπτωση να προβλέπονται από το νόμο και να σέβονται τον πυρήνα των θεμελιωδών δικαιωμάτων και ελευθεριών που αναγνωρίζονται από τον Χάρτη και να ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η ΕΕ[111].

Στο σημείο αυτό, κρίνεται σκόπιμο να αναφερθούν κάποιες σημαντικές διαπιστώσεις, από τη σύσταση του Ευρωκοινοβουλίου προς το Συμβούλιο και την Επιτροπή, της 15 Ιουν. 2023, που προέκυψαν από τη διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης. Αναφέρει σκόπιμη χρήση κατασκοπευτικών λογισμικών από κρατικούς φορείς, με παραπλανητικό τρόπο, μέσω ενσωμάτωσής του σε νόμιμο πρόγραμμα, αρχείο ή περιεχόμενο («δούρειος ίππος»), όπως για παράδειγμα ψευδή μηνύματα από δημόσιους οργανισμούς και ότι σε ορισμένες περιπτώσεις δημόσιες αρχές, έχουν χρησιμοποιήσει παρόχους τηλεφωνίας για να διαβιβάσουν κακόβουλο περιεχόμενο στις συσκευές των προσώπων που στοχοποιούνται. Συμβουλεύει επίσης, ότι η παρακολούθηση με κατασκοπευτικό λογισμικό, δεν πρέπει να καταστεί ο κανόνας αλλά να παραμείνει εξαίρεση και να απαιτεί πάντα αποτελεσματική, δεσμευτική και ουσιαστική εκ των προτέρων δικαστική άδεια από αμερόληπτη και ανεξάρτητη δικαστική αρχή, η οποία πρέπει να διασφαλίζει ότι το μέτρο είναι αναγκαίο, αναλογικό και περιορίζεται αυστηρά σε περιπτώσεις που επηρεάζουν την Εθνική Ασφάλεια ή περιλαμβάνουν την τρομοκρατία και το σοβαρό έγκλημα[112].

Με αφορμή την επιτήρηση που παρατηρήθηκε στις περιπτώσεις των K-M, Ευρωβουλευτές υπογράμμισαν, ότι η παράνομη χρήση τέτοιων προγραμμάτων, θέτει σε κίνδυνο την ίδια τη δημοκρατία και ζήτησαν τη διεξαγωγή αξιόπιστων ερευνών και νομοθετικές ρυθμίσεις, ώστε να γίνεται καλύτερη εφαρμογή των υφιστάμενων κανόνων και να αποφεύγονται φαινόμενα κατάχρησης. Ζήτησαν επίσης, η χρήση του spyware να γίνεται αποκλειστικά μόνο σε εξαιρετικές περιπτώσεις, για σαφώς προκαθορισμένο σκοπό και για περιορισμένο χρονικό διάστημα, καθώς επίσης και τη δημιουργία ενός ανεξάρτητου

[111] EUROPEAN DATA PROTECTION SUPERVISOR, "Preliminary Remarks on Modern Spyware", 15 Feb 2022, available at. https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

[112] 2023/2500(RSP), available at. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EL.html

Ευρωπαϊκού τεχνολογικού εργαστηρίου, με αρμοδιότητα να διερευνά υποθέσεις παρακολούθησης και να παρέχει τεχνολογική υποστήριξη, όπως έλεγχο συσκευών και εγκληματολογικές μελέτες[113].

ΚΕΦΑΛΑΙΟ ΕΚΤΟ: ΑΠΑΙΤΟΥΜΕΝΕΣ ΝΟΜΙΚΕΣ ΚΑΙ ΘΕΣΜΙΚΕΣ ΠΡΩΤΟΒΟΥΛΙΕΣ

Στην ενότητα αυτή μνημονεύονται, όλες οι θεσμικές ενέργειες της ΕΕ, συμπεριλαμβανομένων νομοθετικών ρυθμίσεων, οδηγιών, συστάσεων και παράλληλα αυτές αντιστοιχούνται, με τις εθνικές ενέργειες σύμφωνα με τις υποχρεώσεις που απορρέουν από τις Ευρωπαϊκές δεσμεύσεις, αλλά και πέραν τούτων εφόσον λαμβάνονται από τα Κ-Μ.

6.1 Επάρκεια νομικού πλαισίου ΕΕ

Αρχίζοντας από την προστασία προσωπικών δεδομένων, συναντάμε δύο κύριους πυλώνες προστασίας, την Οδηγία 2002/58/ΕΚ, (e-privacy or cookie law), του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (Απόρρητο των Επικοινωνιών), η οποία τροποποιήθηκε με την Οδηγία 2009/136/ΕΚ της 25ης Νοεμβρίου 2009[114]. Στην παράγραφο 26 της τροποποίησης, αναφέρεται ότι οι αρμόδιες εθνικές αρχές πρέπει να συνεργάζονται με τους παρόχους, ώστε να συλλέγουν και να διανέμουν, πληροφορίες δημοσίου ενδιαφέροντος, σχετικά με τη χρήση των ηλεκτρονικών υπηρεσιών, όπως συμβουλές για παράνομη διάδοση και χρήση λογισμικού ή προστασία από κινδύνους διαρροής προσωπικών δεδομένων. Οι πληροφορίες αυτές μπορούν να συντονίζονται και με άρθρο 33, παρ. 1 της Οδηγίας 2002/22/ΕΚ (Οδηγία καθολικής υπηρεσίας), σύμφωνα με την οποία, εξασφαλίζεται ότι οι εθνικές κανονιστικές αρχές, λαμβάνουν υπόψη τις απόψεις των τελικών χρηστών, των καταναλωτών, καθώς και των επιχειρήσεων, που παρέχουν δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, για θέματα που άπτονται των δικαιωμάτων του συνόλου των τελικών χρηστών και των καταναλωτών των υπηρεσιών ηλεκτρονικών επικοινωνιών. Στο άρθρο 5 παρ. 1 της Οδηγίας, αναφέρεται ότι τα Κ-Μ, είναι απαραίτητο, μέσω της εθνικής νομοθεσίας, να κατοχυρώνουν

[113] https://www.protothema.gr/world/article/1382350/austirous-kanones-gia-ti-hrisi-kataskopeutikou-logismikou-enekrine-to-europaiko-koinovoulio/

[114] Οδηγία 2009/136/ΕΚ της 25ης Νοεμβρίου 2009, «για την τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών».

το απόρρητο των επικοινωνιών, που διακινούνται, στα δημόσια δίκτυα επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών[115]. Στο άρθρο 15 παρ.1, η Οδηγία δίνει τη δυνατότητα για εξαιρέσεις στο απόρρητο, όταν αυτό επιβάλλεται για τη διαφύλαξη της δημόσιας και Εθνικής Ασφάλειας.

Η Οδηγία 2002/58/ΕΚ και ο ΓΚΠΔ, είναι τα δύο βασικά νομικά πλαίσια της ΕΕ για την εξασφάλιση της πλήρους προστασίας των προσωπικών δεδομένων, με κύριες διαφορές το πεδίο εφαρμογής και τη νομική τους ισχύ. Η 2002/58/ΕΚ είναι Οδηγία, που σημαίνει ότι πρέπει να ενσωματωθεί στο εθνικό δίκαιο κάθε Κ-Μ, ενώ ο ΓΚΠΔ, ως Κανονισμός, που ισχύει χωρίς άλλη προϋπόθεση και ομοιόμορφα σε όλη την ΕΕ. Ως δε προς τα κακόβουλα λογισμικά κατασκοπείας, το άρθρο 9 του ΓΚΠΔ, προβλέπει τις προϋποθέσεις των εξαιρέσεων για την επεξεργασία της ειδικής κατηγορίας «ευαίσθητων» προσωπικών δεδομένων, που αφορούν μεταξύ άλλων σε ταυτοποίηση προσώπου, πολιτικές πεποιθήσεις, δεδομένα υγείας, γενετικά δεδομένα κα.

Η Οδηγία 2016/680/ΕΕ της 27ης Απριλίου 2016, έχει σκοπό τη ρύθμιση θεμάτων, για την εξασφάλιση της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων και την προστασία των φυσικών προσώπων στις περιπτώσεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές των Κ-Μ, όταν αυτό απαιτείται για την πρόληψη, διερεύνηση, ανίχνευση, την άσκηση δίωξης για ποινικά αδικήματα ή της επιβολής ποινικών κυρώσεων. Στο άρθρο 15 παρ. 1 της οδηγίας αυτής, αναγνωρίζεται το δικαίωμα στα Κ-Μ για τον περιορισμό του δικαιώματος πρόσβασης του υποκειμένου των δεδομένων, όταν αυτό επιβάλλεται για την παρεμπόδιση της πρόληψης και έρευνας ποινικών αδικημάτων, την προστασία της δημόσιας και της ασφάλειας, καθώς επίσης και την προστασία δικαιωμάτων και ελευθεριών του κοινωνικού συνόλου. Την ως άνω Οδηγία, ακολούθησε ο Κανονισμός 2018/1725/ΕΕ της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Δηλαδή, η διαφορά των δύο νομοθετημάτων, έγκειται στο γεγονός ότι το πρώτο αφορά την προστασία των προσωπικών δεδομένων στο πλαίσιο της ποινικής δικαιοσύνης και της

[115] Ειδικότερα τα Κ-Μ, «απαγορεύουν την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια».

επιβολής του νόμου, από αστυνομικές και δικαστικές αρχές και επιτρέπει ειδικές εξαιρέσεις λόγω της φύσης της ποινικής διαδικασίας. ενώ το δεύτερο τα θεσμικά όργανα της Ένωσης.

Η Οδηγία 2022/2555/ΕΕ της 14ης Δεκεμβρίου 2022, «σχετικά με μέτρα για υψηλό κοινό επίπεδο Κυβερνοασφάλειας (Network and Information Systems Directive/NIS2), εκδόθηκε για τη συμπλήρωση των κενών και αποκλίσεων, που παρατηρήθηκαν από την εφαρμογή της αντίστοιχης της προηγούμενης Οδηγίας 2016/1148/ΕΕ. Με τη νέα Οδηγία, επιδιώκεται η εξάλειψη των αποκλίσεων, σε θέματα χειρισμού μεταξύ των Κ-Μ και η παροχή ελάχιστων κατευθύνσεων, σχετικά με τη λειτουργία ενός συντονισμένου κανονιστικού πλαισίου, για την αποτελεσματική συνεργασία μεταξύ των αρμόδιων αρχών σε κάθε κράτος, σε υποχρεώσεις Κυβερνοασφάλειας, καθώς επίσης και τη θέσπιση αποτελεσματικών ένδικων μέσων και μέτρων επιβολής, που έχουν καθοριστική σημασία για την αποτελεσματική επιβολή των εν λόγω υποχρεώσεων. Προηγήθηκε ο Κανονισμός 2019/881/ΕΕ, της 17ης Απριλίου 2019, σχετικά με τον ENISA (European Union Agency for Cybersecurity/ Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της Κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών. Ο ENISA σύμφωνα με τον Κανονισμό 526/2013/ΕΕ, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, έχει σκοπό να συμβάλλει στην ανάπτυξη της Κυβερνοασφάλειας στην Ένωση, και ιδιαίτερα στο χώρο των ΜΜΕ και των νέων επιχειρήσεων.

Την 12 Αυγούστου 2013 και πριν τη σύμβαση της Βουδαπέστης, εκδόθηκε η Οδηγία 2013/40/ΕΕ με την οποία, επιχειρείται η προσέγγιση του ποινικού δικαίου των Κ-Μ στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες ως προς τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων, καθώς και η βελτίωση της συνεργασίας μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου[116]. Στις αρμόδιες υπηρεσίες, περιλαμβάνονται και οι εξειδικευμένοι οργανισμοί της Ένωσης, όπως η Eurojust, η Europol, το Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος και ο ENISA. Η Σύμβαση της Βουδαπέστης, στοχεύει στην εναρμόνιση ποινικών νόμων, τη διεθνή συνεργασία και την αποτελεσματικότερη δίωξη ψηφιακών εγκλημάτων, από την παράνομη πρόσβαση και την παρεμβολή σε δεδομένα και συστήματα, μέχρι την απάτη σε σχέση με υπολογιστές και τη διάδοση υλικού παιδικής κακοποίησης, καθώς και στις διαδικαστικές

[116] Θεοχάρης Ι. Δαλακούρας(2023), Ηλεκτρονικό Έγκλημα , Νομική Βιβλιοθήκη, σελ.2.

εξουσίες για τη διερεύνηση εγκλημάτων στον κυβερνοχώρο και τη διασφάλιση ηλεκτρονικών αποδεικτικών στοιχείων, για ανά κατηγορία εγκλήματος. Ειδικότερα στο άρθρο 6 της Συνθήκης, ορίζεται ότι κάθε συμβαλλόμενο μέρος, πρέπει να λάβει τα απαραίτητα νομοθετικά μέτρα έτσι ώστε να θεωρούνται ως ποινικά αδικήματα, οι άνομες πράξεις που διαπράττονται εκ προθέσεως και χωρίς δικαίωμα, στις ακόλουθες περιπτώσεις:

- Παραγωγής, πώλησης, προμήθειας για χρήση, εισαγωγής, διανομής ή με άλλο τρόπο διάθεσης:
  - ✓ Μιας συσκευής, συμπεριλαμβανομένου του προγράμματος υπολογιστή, που έχει σχεδιαστεί ή προσαρμοστεί, με σκοπό της διάπραξη οποιουδήποτε από τα αδικήματα, που ορίζονται σύμφωνα με τα Άρθρα 2 έως 5.
  - ✓ Ενός κωδικού πρόσβασης υπολογιστή, ενός κωδικού πρόσβασης ή παρόμοιων δεδομένων μέσω των οποίων, είναι δυνατή η πρόσβαση σε ολόκληρο ή σε οποιοδήποτε μέρος ενός συστήματος υπολογιστή, με πρόθεση να χρησιμοποιηθεί, για τον σκοπό της διάπραξης οποιουδήποτε από τα αδικήματα που ορίζονται στα Άρθρα 2 έως 5.
- Κατοχής ενός αντικειμένου που αναφέρεται παραπάνω, με πρόθεση να χρησιμοποιηθεί, για τον σκοπό της διάπραξης οποιουδήποτε από τα αδικήματα που ορίζονται στα Άρθρα 2 έως 5.

Ο Κανονισμός 2024/1689/ΕΕ, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13-06-2024, θεσπίστηκε για τη ρύθμιση θεμάτων της ΤΝ, γνωστού και ως AI Act. Προτεραιότητα του Κοινοβουλίου, με το εν λόγω νομοθέτημα, ήταν να διασφαλίσει ότι, εμφανιζόμενα και σχεδιαζόμενα συστήματα ΤΝ, που χρησιμοποιούνται στην ΕΕ, είναι ασφαλή, διαφανή, αμερόληπτα και φιλικά προς το περιβάλλον, και μπορούν να ιχνηλατηθούν. Επίσης τα συστήματα αυτά, θα πρέπει να επιβλέπονται από ανθρώπους και όχι να λειτουργούν, ως ανεξάρτητα αυτοματοποιημένα, έτσι ώστε να προλαμβάνονται μη επιθυμητά και επιβλαβή αποτελέσματα [117].

Η υπεροχή του Κοινοτικού δικαίου έναντι του Εθνικού, υπαγορεύει ότι όταν κάποιος Εθνικός Κανόνας, συγκρούεται με ένα Ενωσιακό, ανεξάρτητα αν ο πρώτος είναι πρωτόγεννούς ή παράγωγου δικαίου, ο Κανόνας της ΕΕ, υπερέχει του Εθνικού. Επίσης ο

[117] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Κανονισμός της ΕΕ σε σύγκριση με την Οδηγία, υπερτερεί ως προς το γεγονός ότι είναι δεσμευτικός, ως προς τις διατάξεις τους για όλα τα Κ-Μ, χωρίς να απαιτείται από αυτά περαιτέρω νομοθετική παρέμβαση. Ενώ η οδηγία είναι και αυτή δεσμευτική ως προς τα αποτέλεσμα, αλλά επαφίεται στο Κ-Μ να επιλέξει τον τρόπο που θα το επιτύχει[118].

6.2 Επάρκεια σε Εθνικό πλαίσιο

Με το Ν. 4411/2016 (ΦΕΚ Α΄142/3.8.2016), επικυρώθηκαν η σύμβαση της Βουδαπέστης και η Οδηγία 2013/40/ΕΕ, για το έγκλημα στον κυβερνοχώρο και επικαιροποιήθηκε η εθνική ποινική νομοθεσία, με την εισαγωγή των όρων ηλεκτρονικής τεχνολογίας και ψηφιακών δεδομένων στον ΠΚ (άρθρο 13) [119].

Στο άρθρο 292Α του ΠΚ, προβλέπονται ποινές για την αυθαίρετη πρόσβαση σε ηλεκτρονικά και τηλεφωνικά δίκτυα, καθώς και σε συστήματα και συσκευές, που χρησιμοποιούνται σε αυτά τα δίκτυα. Οι ποινές αυτές, καθίστανται αυστηρότερες στις περιπτώσεις που ο υπαίτιος, είναι εργαζόμενος ή συνεργάτης του παρόχου υπηρεσιών τηλεφωνίας. Ακολούθως στο άρθρο 292Γ, ποινικοποιούνται αυτοτελώς ,συμπεριφορές που κατατείνουν στην τέλεση των εγκλημάτων του άρθρου 292Β και ειδικότερα αυτών της παραγωγής, πώλησης, διανομής, εισαγωγής, κατοχής προγραμμάτων και συσκευών σχεδιασμένων ή προσαρμοσμένων, για την τέλεση των πράξεων του άρθρου αυτού.

Παράνομη πρόσβαση σε πληροφοριακό σύστημα, νοείται και η απλή πρόσβαση χωρίς απαραίτητα κάποιας άλλης μορφής κακόβουλη ενέργεια, περιπτώσεις δε πρόσβασης σε ψηφιακά δεδομένα, αποτελούν κατεξοχήν μορφή hacking, σύμφωνα με την αιτιολογική έκθεση του ν.4411/2016[120].

Με το άρθρο 370Β, τιμωρείται η παράνομη πρόσβαση σε μέρος ή στο σύνολο συστήματος πληροφοριών ή σε ηλεκτρονικά δεδομένα. Με το αντίστοιχο 370Γ ΠΚ,

---

[118] Βασίλειος Α. Χριστιανός, Εισαγωγή στο Δίκαιο της ΕΕ, Νομική Βιβλιοθήκη, Αθήνα 2011, σ.37,38, 156.

[119] Ως Πληροφοριακό σύστημα ορίζεται « συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών»., και Ψηφιακά δεδομένα «είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».

[120] Θεοχάρης Ι. Δαλακούρας(2023), Ηλεκτρονικό Έγκλημα , Νομική Βιβλιοθήκη, σελ.33.

τιμωρείται όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτους ή παραβιάζει προγράμματα που σχετίζονται με απόρρητα δεδομένα κρατικά ή εμπορικά επιστημονικά, συμμορφώνοντας το εθνικό δίκαιο με το άρθρο 3 της Οδηγίας και το άρθρο 2 της σύμβασης. Με το άρθρο 381Α ΠΚ, εναρμονίζεται η ελληνική νομοθεσία με τα άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας. Με τη νέα διάταξη αυτή, καλύπτεται ένα κενό της ελληνικής νομοθεσίας και προστατεύονται πλέον αυτοτελώς, τα ψηφιακά δεδομένα από επιθέσεις hacking με σκοπό την καταστροφή, διαγραφή ή αλλοίωσής τους[121].

Τα άρθρα 3 της Σύμβασης και 6 της Οδηγίας, αναφέρονται στην παράνομη υποκλοπή δεδομένων και κατά συνέπεια η παραβίαση του δικαιώματος του απορρήτου επικοινωνιών, από πληροφορικά συστήματα και δίκτυα. Οι εν λόγω διατάξεις ενσωματώθηκαν στην εθνική νομοθεσία, με άρθρο 370Δ ΠΚ, επιβάλλοντας αυστηρές ποινές κάθειρξης, μέχρι δέκα ετών. Η νέα αυτή διάταξη του άρθρου 370Δ ΠΚ, που αφορά γραπτά δεδομένα μέσω παραβίασης της φυσικής ή ψηφιακής αλληλογραφίας emails, SMS κα., εξισώνει τις ποινές, με αυτές που προβλέπονται στο άρθρο 370Α, με τίτλο «Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας» [122]. Το άρθρο αυτό, περιλαμβάνει διατάξεις για υποκλοπή με οποιονδήποτε τρόπο προφορικής συνομιλίας, από παρέμβαση σε συσκευή, σύνδεση, δίκτυο παροχής υπηρεσιών τηλεφωνίας, σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή υπηρεσιών αυτού του είδους. Με το άρθρο 370ΣΤ του ΠΚ, προβλέπεται ποινή φυλάκισης τουλάχιστον δύο ετών, για παραγωγή, διανομή ή προμήθεια προς χρήση λογισμικού ή συσκευών παρακολούθησης με δυνατότητα υποκλοπής. Με την ίδια ποινή, τιμωρείται και όποιος εξάγει ή εισάγει, έχει στην κατοχή του, διανέμει ή διακινεί το λογισμικό αυτού του είδους.

Η κρυπτογράφηση σε εθνικό πλαίσιο διέπεται από το ΓΚΠΔ (Άρθρο 32), το οποίο επιβάλλει την προστασία προσωπικών δεδομένων, από το ν. Ν.3674/2008 (ΦΕΚ 136/Α/10-07-2008) και την Απόφαση 165/2011 ΑΔΑΕ (ΦΕΚ Β' 2715/17-11-2011). Με το άρθρο 32, παρ. α), αναφέρεται ότι τηρουμένων των δικαιωμάτων και τις ελευθερίες των φυσικών προσώπων, ο

[121] Αλέξανδρος-Ιωάννης Καργόπουλος, Πρωτοδίκης, εθνικός εμπειρογνώμονας στον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ε.Ε., «Κυβερνο-έγκλημα: Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου», διαθέσιμο σε https://www.esdi.gr/nex/images/stories/pdf/epimorfosi/2018/kargopoulos.pdf

[122] Ως υποκλοπή ορίζεται όταν κάποιος « αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών».

υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία προσωπικών δεδομένων, εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, την κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα. Η δεύτερη περίπτωση αναφέρει ότι με διάταγμα, που εκδίδεται με πρόταση των Υπουργών Δικαιοσύνης και Μεταφορών και Επικοινωνιών, δύναται να υποχρεώνει τους παρόχους υπηρεσιών τηλεφωνίας, σε διαδικασία κρυπτογράφησης στα φωνητικά σήματα πληροφοριών, που μεταδίδονται από τα εκτός της εποπτείας τους φυσικά μέσα, όπως είναι οι οπτικές ίνες, οι αγώγιμες γραμμές μεταφοράς και τα σημεία ζεύξης. Το τρίτο νομοθέτημα, σύμφωνα με το άρθρο 1, επιβάλει κανόνες, σε όλα τα πρόσωπα που ασχολούνται με την παροχή δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών[123].

Η Οδηγία (ΕΕ) 2022/2555 (NIS2) για την Κυβερνοασφάλεια, ενσωματώθηκε στο ελληνικό δίκαιο με τον Νόμο 5160/2024 (ΦΕΚ Α 195 - 27.11.2024), με πρόβλεψη μεταξύ άλλων τη εκπόνηση Εθνικής Στρατηγικής Κυβερνοασφάλειας. Η Εθνική Στρατηγική Κυβερνοασφάλειας για τα έτη 2026-2030, εγκρίθηκε το Δεκέμβριο 2025, με απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης[124]. Με βάση τις διατάξεις της Εθνικής Αρχής Κυβερνοασφάλειας, η ΕΑΚ συνεργάζεται στενά μεταξύ άλλων με τη Διεύθυνση Δίωξης Κυβερνοεγκλήματος της Ελληνικής Αστυνομίας, την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η εξέλιξη του κακόβουλου λογισμικού κατασκοπείας, εντάσσεται στη εξέλιξη της τεχνολογίας των υπολογιστικών συστημάτων και ηλεκτρονικών δικτύων και εν γένει του διαδικτύου και ως εκ τούτου η χρήση του καθίσταται ευκολότερη και ευρύτερη και ως εκ τούτου, ο επιθυμητός και ο επιβαλλόμενος έλεγχος, καθίσταται δυσχερέστερος. Οι

[123] Επιβάλλεται ότι «όλα τα πρόσωπα που ασχολούνται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών, υποχρεούνται να διαθέτουν και να εφαρμόζουν Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών».

[124] ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ, «Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026 – 2030», ΑΡ. ΠΡΩΤ. 2563/16.12.2025, διαθέσιμο σε https://cyber.gov.gr/wp-content/uploads/2025/12/%CE%95%CE%A3%CE%9A-2026-2030.pdf

νεοεμφανιζόμενες τεχνολογίες, βοηθούν στην ανάπτυξη νέων μορφών κακόβολου λογισμικού και κατά συνέπεια και λογισμικού επιτήρησης.

Η εκμετάλλευση του κατασκοπευτικού λογισμικού για κατασκοπεία, δεν είναι κατ' ανάγκη κακή και μπορεί να γίνει τόσο από ιδιωτικούς όσο και από κρατικούς φορείς και οργανισμούς. Στις περιπτώσεις προστασίας των δημοκρατικών θεσμών, της Εθνικής Κυριαρχίας, καταστολής εγκληματικότητας και προστασίας των πολιτών η χρήση του για παρακολούθηση και συλλογή πληροφοριών, κρίνεται επωφελής τηρουμένων των αναλογιών. Σημειώνεται, ότι στη νόμιμη χρήση του κατασκοπευτικού αν και το επιδιωκόμενο αποτέλεσμα ως προς τους επιτιθέμενους είναι διαφορετικό, όμως τα θεμελιώδη δικαιώματα και οι ελευθερίες των ατόμων προσβάλλονται, και ως εκ τούτου επιβάλλεται η τήρηση κανόνων αναλογικότητας.

Η εισβολή με κατασκοπικό λογισμικό για παρακολούθηση και επιτήρηση των ηλεκτρονικών συσκευών και των λειτουργιών εξυπηρέτησης, παραβιάζει το δικαίωμα προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων, αλλά και άλλα θεμελιώδη δικαιώματα, όπως αυτό της ελευθερίας του λόγου, καθώς και της ελεύθερης βούλησης και συμμετοχής σε πολιτικές και εκλογικές δραστηριότητες.

Η πιστοποίηση από τις εταιρείες λογισμικού, ότι το προϊόν που διαθέτουν στο εμπόριο, δεν μπορεί να χρησιμοποιηθεί είτε αυτοτελές ανεξάρτητο, είτε ως υποσύστημα άλλου λογισμικού για πράξεις επιτήρησης γενικά και κατασκοπείας, κρίνεται απαραίτητη. Ακόμη δε και στις περιπτώσεις προμήθειας από κρατικούς οργανισμούς, λογισμικού κατασκοπείας, είναι απαραίτητη σχετική πιστοποίηση, για αποσαφήνιση και τη δυνατότητα ελέγχου της χρήσης τους, σύμφωνα με τις προδιαγραφές του κατασκευαστή. Κατά αυτόν τον τρόπο, θα επιτυγχάνεται καλύτερα ο έλεγχος σε περιπτώσεις αθέμιτης χρήσης και θα αποδίδονται νομικές ευθύνες, όταν οι υποθέσεις παίρνουν τη δικαστική οδό. Επίσης, η αποποίηση ευθυνών, από τις εταιρείες θα καθίσταται εφικτή, εφόσον το προϊόν που διαθέτουν χειραγωγήθηκε από τρίτους χωρίς τη συναίνεσή τους.

Απαιτείται ρύθμιση τόσο στις εισαγωγές όσο και οι εξαγωγές στη ΕΕ, έτσι ώστε να αντιμετωπίζεται ενιαία η διακίνηση και η πιστοποίηση, των συστημάτων κατασκοπευτικού λογισμικού και του λογισμικού διπλής χρήσης.

Σύμφωνα με τη Συνθήκη για την Ευρωπαϊκή Ένωση, η Εθνική Ασφάλεια του κάθε Κ-Μ, αποτελεί αποκλειστική ευθύνη του ιδίου, τούτο όμως δεν αποκλείει οι δραστηριότητες

Εθνικής Ασφάλειας, να υπόκεινται στο δίκαιο της ΕΕ, όταν αφορούν σε διαδικασίες, που ρυθμίζονται από το δίκαιο της ΕΕ και ιδιαίτερα, αυτό που άπτεται των θεμελιωδών δικαιωμάτων και ελευθεριών των πολιτών. Ωστόσο, η εφαρμογή του δικαίου της ΕΕ στη χρήση κατασκοπευτικού λογισμικού, για σκοπούς Εθνικής Ασφάλειας, παρεμποδίζεται από το γεγονός, ότι οι δραστηριότητες Εθνικής Ασφάλειας, εξαιρούνται από το πεδίο εφαρμογής θεμελιωδών κανονιστικών πράξεων, όπως του ΓΚΠΔ και της Οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Η επίκληση από τους κυβερνητικούς οργανισμούς, εξαιρέσεων των περιορισμών που τίθενται από την κείμενη Ευρωπαϊκή νομοθεσία, για λόγους Εθνικής Άμυνας του κράτους, της δημόσιας ασφάλειας, της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, καθώς και μέτρων πρόληψης και προστασίας από απειλές κατά της δημόσιας ασφάλειας, όπως έχει διαπιστωθεί εκ του αποτελέσματος, δεν τίθεται με καλή πίστη από την πλευρά των Κ-Μ. Συγκεκριμένα όπως αποδεικνύεται από τις υποθέσεις που έχουν απασχολήσει το Ευρωκοινοβούλιο και τις συστάσεις που έχουν γίνει για συμμόρφωση, υπάρχει ασάφεια ως προς το σκοπό που πραγματοποιείται μια παρέμβαση με κατασκοπευτικό λογισμικό, καθώς και έλλειψη αυστηρού νομικού πλαισίου χρήσης και συγκεκριμένου χρονοδιαγράμματος.

Κατά συνέπεια , ο περιορισμός στην προστασία των δεδομένων των υποκειμένων σε κρατικές δραστηριότητες, δύσκολα μπορεί να συμπορευτεί παράλληλα τα θεμελιώδη δικαιώματα που περιέχονται στον Χάρτη και τις αρχές που περιέχονται στις Συνθήκες. Η ισορροπία που επιδιώκεται, στα νομοθετήματα που προβλέπουν τη χρήση λογισμικού κατασκοπείας από κυβερνητικούς δρώντες, ως προς την επιβαλλόμενη ανάγκη χρήσης και προστασία των θεμελιωδών δικαιωμάτων και ατομικών ελευθεριών του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ και της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου, δεν έχει όπως έχει αποτυπωθεί μέχρι σήμερα τουλάχιστον τα αναμενόμενα αποτελέσματα.

Αθροιστικά το πλαίσιο του δικαίου της ΕΕ, για την ηλεκτρονική επιτήρηση, περιλαμβάνει την πρόθεση για την προστασία των δικαιωμάτων, που κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων, στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου, τους Κανονισμούς, τις Οδηγίες και τις διάφορες συστάσεις που απευθύνονται στα Κ-Μ, κυρίως με αφορμή έννομες ενέργειες, που δε συνάδουν με το πνεύμα της δημιουργίας και λειτουργίας της ΕΕ.

Η επικρατούσα νομολογία στην ΕΕ, είναι πολυδιάστατη καθόσον αποτελείται από πλήθος νομοθετημάτων, όπως Κανονισμούς, Οδηγίες, αλλά και συμβάσεις/συνθήκες, μαζί με συστάσεις από το Ευρωκοινοβούλιο και άλλους φορείς της ΕΕ, όπως το ΕΔΔΑ. Για την εξέταση μιας υπόθεσης νομιμότητας ως προς τα θεμελιώδη δικαιώματα, ο αρμόδιος ερευνητής είναι απαραίτητο, να προστρέξει σε όλα αυτά τα νομικά κείμενα, να προσδιορίσει τα κοινά τους στοιχεία και να δώσει μια ερμηνεία, η οποία να διακρίνεται από αντικειμενικότητα, πληρότητα και αποτελεσματικότητα, γεγονός που καθίσταται εξαιρετικά δυσχερές, συνδυαζόμενο και με τις εκάστοτε εθνικές νομοθεσίες. Η ευρεία διάδοση και η χρήση κατασκοπευτικού λογισμικού, όπως έχει αποτυπωθεί από τα επίσημα κείμενα και τα όργανα της ΕΕ, σε συνδυασμό με την πολυπλοκότητά του και τη σοβαρότητα των επιπτώσεων στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα, ενισχύει την ανάγκη αντιμετώπισης του φαινομένου αυτού, με αυτόνομο νομοθέτημα.

Η ανάγκη λοιπόν ενός ενιαίου νομοθετικού κειμένου είναι επιτακτική, όπως στις περιπτώσεις του κανονισμού για τα προσωπικά δεδομένα ή τη ρύθμιση θεμάτων για την Τεχνητή Νοημοσύνη.

Ο ΓΚΠΔ της ΕΕ, σύμφωνα με τον οποίο επιτρέπεται, ο εκάστοτε υπεύθυνος επεξεργασίας ή ο αρμόδιος για την επεξεργασία των δεδομένων, να περιορίζονται με νομοθετική πράξη, οι υποχρεώσεις και τα δικαιώματα των υποκειμένων που προβλέπονται στα άρθρα του κανονισμού, δεν έχει μεταφερθεί με ακρίβεια και δεσμευτικότητα στα εθνικό δίκαιο των Κ-Μ, ώστε να υπάρχει η δέουσα προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών. Η ΕΕ απαιτείται, να διαμορφώσει ένα συνεκτικό ρυθμιστικό πλαίσιο για την αποτελεσματική αντιμετώπιση περιστατικών, αναφορικά με την εξουσιοδοτημένη παρακολούθηση και συλλογή δεδομένων.

Η σχετική Εθνική Νομολογία χρήζει αποσαφήνισης και συμπλήρωσης με περαιτέρω λεπτομέρειες, καθώς και την έκδοση του προβλεπόμενου ΠΔ.

Οι εντολές επιτήρησης, πρέπει να προέρχονται από εξουσιοδοτημένους ανεξάρτητους δικαστές, οι οποίοι προκειμένου και πριν εκχωρήσουν εγκριτική διαταγή, να αξιολογούν την σκοπιμότητα, λαμβανομένων υπόψη των παραμέτρων της αναγκαιότητας και της αναλογικότητας του μέτρου. Επίσης, είναι απαραίτητο οι εισαγγελικές αρχές να υποχρεούνται να υποβάλουν γραπτό αίτημα, όταν ζητούν επιτήρηση για λόγους Εθνικής

Ασφάλειας, το οποίο να περιλαμβάνει τεκμηριωμένα και ακριβή επιχειρήματα. Απαιτείται σαφέστερη νομική ρύθμιση, που να εξασφαλίζει το δικαίωμα πρόσβασης σε πληροφορίες σχετικά με την επιτήρηση από κυβερνητικούς φορείς, επιτρέποντας στα άτομα να ζητούν και να λαμβάνουν λεπτομέρειες, σχετικά με τυχόν μέτρα επιτήρησης που λαμβάνονται εναντίον τους.

Η έγκριση για άρση απόρρητου, από τις εισαγγελικές αρχές ιδιαίτερα σε περιπτώσεις που γίνεται για δημόσιο συμφέρον, πρέπει να είναι λεπτομερώς τεκμηριωμένες και ακριβείς ως προς την αναγκαιότητα και τη σκοπιμότητα που επιβάλλεται.

Οι Ανεξάρτητες Αρχές πρέπει να στελεχωθούν επαρκώς με κατάλληλο επιστημονικά προσωπικό και νομικά να διευρύνουν τη δικαιοδοσία τους, ώστε οι έρευνες που ενεργούν, καθώς και τα σχετικά πορίσματα που εκδίδουν να είναι δεσμευτικά για τις αρχές.

Η κρυπτογράφηση αποτελεί βασικό παράγοντα για την προστασία της ιδιωτικής ζωής και των ανθρωπίνων δικαιωμάτων στον ψηφιακό χώρο. Τόσο η ΕΕ όσο και τα Κ-Μ, πρέπει να απαιτούν από όλους τους εμπλεκόμενους, αλλά να συμβάλουν και οι ίδιοι, ώστε οι τεχνολογίες πληροφοριών και επικοινωνιών, να λαμβάνουν τα απαραίτητα μέτρα για την ασφαλή διακίνηση των προσωπικών δεδομένων και των ιδιωτικών μηνυμάτων και πληροφοριών[125]. Επίσης η δημιουργία ενός ενιαίου μηχανισμού ανίχνευσης και καταγραφής του αποτυπώματος Spyware, θα βοηθούσε κατά πολύ στη αποτροπή και τη μείωση των περιστατικών.

Τέλος, ζητήματα ηθικής και δεοντολογίας, υπεισέρχονται και στα θέματα χρήσης κατασκοπευτικού υλικού, τόσο σε ιδιωτικό και εμπορικό επίπεδο όσο και σε επίπεδο οργανισμών και επίσημων φορέων, καθόσον η ηθική προσέγγιση των θεμάτων που ανακύπτουν, αναμφισβήτητα θα συνδράμει στην προστασία των δικαιωμάτων του ανθρώπου και δύναται επίσης να αποτρέψει την εκμετάλλευση που επιτρέπουν τυχόν νομικά κενά.

[125] https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

ΕΠΙΛΟΓΟΣ

Τα κατασκοπευτικά λογισμικά χρησιμοποιούνται ευρέως στην ΕΕ, τόσο από ιδιωτικούς όσο και δημόσιους φορείς και δεδομένης της εξέλιξης της τεχνολογίας στις επικοινωνίες και τις πληροφορίες, εκτιμάται ότι η χρήση τους θα διευρυνθεί . Η νομολογία της Ένωσης και η ενσωμάτωσή της στο εθνικό δίκαιο αν και αποσπασματική, φαίνεται να καλύπτει τα θέματα προστασίας σε ιδιωτικό πλαίσιο, πλην όμως ένα ενιαίο ανεξάρτητο και δεσμευτικό κείμενο, θα μπορούσε να είναι πιο χρήσιμο και αποτελεσματικό. Ιδιαίτερες και λεπτομερέστερες διατάξεις και προβλέψεις σίγουρα απαιτούνται για την εφαρμογή τους από επίσημους φορείς.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Θεοχάρης Ι. Δαλακούρας, Ηλεκτρονικό Έγκλημα, Ουσιαστικές και δικονομικές όψεις, , Εκδόσεις Νομική Βιβλιοθήκη, 2η ΄Έκδοση, Αθήνα 2023
2. Γ. Μπαμπινιώτης «Λεξικό της Νέας Ελληνικής Γλώσσας» έκδοση 2η.
3. Michael J. Sandel, Δικαιοσύνη «Τι είναι το σωστό;», μεταφρ. Αλέξανδρος Κιουπκιόλης εκδ. Πόλις 2011.
4. Παύλος Κ. Σούρλας, «Μια εισαγωγή στην επιστήμη του δικαίου», εκδ. Αντ. Ν. Σάκκουλα 1995.
5. Σπύρος Βλαχόπουλος, «Θεμελιώδη Δικαιώματα», Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2017.
6. Λεωνίδας Γ. Κοτσαλής, Ποινικός Κώδικας. Νομική Βιβλιοθήκη, Έκδοση 22η, Αθήνα 2024.
7. Βασίλειος Α. Χριστιανός, Εισαγωγή στο Δίκαιο της ΕΕ, Νομική Βιβλιοθήκη, Αθήνα 2011.
8. Γιώργος Ν. Γιαννόπουλος, Εισαγωγή στη Νομική Πληροφορική, Νομική Βιβλιοθήκη, Αθήνα 2018.
9. ΔΡ. ΓΕΩΡΓΙΟΣ Ι. ΖΕΚΟΣ, ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΑΝΤΑΓΩΝΙΣΜΟΣ (ΝΟΜΙΚΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ), Εκδ. ΣΑΚΚΟΥΛΑ, Αθήνα-Θεσσαλονίκη 2024.

ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Simmons R (2016) The Failure of the Computer Fraud and Abuse Act: Time to Take a New Approach to Regulating Computer Crime, George Washington Law Review, Vol. 84: 1703, 2 February 2016.
2. Human Rights Council, “The right to privacy in the digital age”, 4 Aug. 2022

ΕΛΛΗΝΙΚΑ ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ

1. Ν.3471/2006 (ΦΕΚ 133/Α/28-06-2006), Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.
2. Ν.4411/2016 (ΦΕΚ Α΄142/3-8-2016), Κύρωση της σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.

3. ΠΔ 81/2019 (ΦΕΚ Α΄119/8-8-2019), Σύσταση, συγχώνευση, μετονομασία και κατάργηση Υπουργείων και καθορισμός των αρμοδιοτήτων τους - Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων.

4. Ν.4624/2019 (ΦΕΚ Α' 137/29-08-2019), Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

5. Ν.5086/2024 (ΦΕΚ Α' 23/14-02-2024), Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις.

6. Ν.5099/2024 (ΦΕΚ Α' 48/05-04-2024), ύψη μέτρων για την εφαρμογή του Κανονισμού (ΕΕ) 2022/2065 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 19ης Οκτωβρίου 2022 σχετικά με την ενιαία αγορά ψηφιακών υπηρεσιών και την τροποποίηση της Οδηγίας 2000/31/ΕΚ («Πράξη για τις ψηφιακές υπηρεσίες») και άλλες διατάξεις.

7. Ν. 5160/2024(ΦΕΚ Α΄195/27-11-2024), Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις.

ΕΥΡΩΠΑΙΚΑ ΚΕΙΜΕΝΑ

1. Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

2. Οδηγία 2009/136/ΕΚ της 25ης Νοεμβρίου 2009, «για την τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών».

3. Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, «για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου», 14 Αυγ. 2013.

4. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

5. Κανονισμός 2019/881/ΕΕ Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου , της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια»).

6. Οδηγία 2022/2555/ΕΕ, του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση.

7. Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη.

8. Council of Europe, "CONVENTION ON CYBERCRIME", Budapest 23 Nov, 2001.

9. Αιτιολογική Έκθεση της Σύμβασης για το Κυβερνοέγκλημα, Παρ. 53, 54, π.10, Available at. https://rm.coe.int/16800cce5b

10. European Parliament, Requested by the PEGA committee, "The use of Pegasus and equivalent surveillance spyware", Feb. 2023.

ΑΡΘΡΟΓΡΑΦΙΑ

1. Dynamic Spyware Analysis, p.1 Available at. https://bitblaze.cs.berkeley.edu/papers/usenix07.pdf
2. Setting spyware standards after the Pegasus scandal, EPRS | European Parliamentary Research Service Hendrik Mildebrath, November 2024 available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766262/EPRS_BRI(2024)766262_EN.pdf
3. The impact of Pegasus on fundamental rights and democratic processes, IPOL, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 -January 2023 available at

https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf5. https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html

4. North Dakota Information Technology Διαθέσιμο στο: https://www.ndit.nd.gov/news/information-stealers
5. Fortinet Διαθέσιμο στο https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers
6. Malwarebytes, available at Rootkit | What is a Rootkit? | Malwarebytes Malicious software, Train the trainer reference guide, European Network and Information Security Agency (ENISA) σελ. 16, Διαθέσιμο στο: https://www.enisa.europa.eu/sites/default/files/all_files/Malicious%20software_Train%20the%20trainer%20guide.pdf
7. Australian Signals Directorate, "Mitigating Drive-by Downloads" , Oct. 2021, p. 1,2 Available at https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Mitigating%20Drive-by%20Downloads%20%28October%202021%29.pdf
8. California Department of Justice, Office of the Attorney General, "Tips for Consumers- Consumer Information Sheet 12", Jan. 2015, p.1 Available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/CIS_12_Computer_protection_DOJ.pdf
9. European Data Protection Board (by Dr. Enrico GLEREAN), "Training curriculum on AI and data protection Fundamentals of Secure AI Systems with Personal Data", p.45, available at. https://www.dpa.gr/sites/default/files/2025-03/Fundamentals%20of%20Secure%20AI%20Systems%20with%20Personal%20Data%20clear.pdf, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0422
10. California Department of Justice, Office of the Attorney General, "Tips for Consumers- Consumer Information Sheet 12", Jan. 2015, p.1 Available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/CIS_12_Computer_protection_DOJ.pdf
11. Australian Signals Directorate, "Mitigating Drive-by Downloads" , Oct. 2021, p. 1,2 Available at https://www.cyber.gov.au/sites/default/files/2023-

03/PROTECT%20-%20Mitigating%20Drive-by%20Downloads%20%28October%202021%29.pdf

12. Lackshmanan, R., The Hacker News, (2023) "European Bank Costumers Targeted in SpyNote Android Trojan Campaign", Διαθέσιμο στο: European Bank Customers Targeted in SpyNote Android Trojan Campaign
13. The use of Pegasus and equivalent surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, pg. 8, February 2023, Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf
14. European Data Protection Supervisor, The EU's independent data protection authority, Preliminary Remarks on Modern Spyware, 15 February 2022, pg. 5, Διαθέσιμο στο: https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf
15. Stanford Encyclopedia of Philosophy Archive, Computer and Information Ethics, Winter 2016 Edition Available (Computing and Human Values) at: https://plato.stanford.edu/archives/win2016/entries/ethics-computer
16. European Parliament/Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies "The impact of Pegasus on fundamental rights and democratic processes", Jan. 2023, p. 27, Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf
17. European Parliament, STUDY Requested by the PEGA Committee "The impact of Pegasus on fundamental rights and democratic processes", p.39, Available at. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf
18. ΣΥΝΤΑΓΜΑ Ερμηνεία κατ' 'άρθρο, Άρθρο 9Α, Φερενίκη Παναγοπούλου, Ηλεκτρονική Έκδοση, Επιμέλεια Σπ. Βλαχόπουλος, Ξ. Κοντιάδης, Γ. Τασόπουλος, Ιανουάριος 2023, σελ. 6, Διαθέσιμο στο: https://www.syntagmawatch.gr/wp-content/uploads/2023/02/%CE%86%CF%81%CE%B8%CF%81%CE%BF-9%CE%91-%CE%9C%CE%95-COVER-1.pdf

19. Παπανικολάου, Α. Syntagmawatch (2022): «Επικοινωνιακό απόρρητο: προβληματισμοί για τη διασφάλιση ενός κλασικού δικαιώματος στο πεδίο των σύγχρονων κατασκοπευτικών λογισμικών». Διαθέσιμο στο: https://www.syntagmawatch.gr/trending-issues/epikoinwniako-aporrhto-provlhmatismoi-gia-th-diasfalish-enos-klasikou-dikaiwmatos-sto-pedio-twn-sygxronwn-kataskopeutikwn-logismikwn/#_ftn20

20. European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, Right to respect for private and family life, 1st Edition, pg. 7 Διαθέσιμο στο: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/11/Guide-to-Art.-8-of-the-ECtHR-COE-and-ECtHR.pdf

21. The impact of Pegasus on fundamental rights and democratic processes, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, January 2023, p. 42, Available at : https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

22. Εφημερίδα Εστία, «Ραγδαίες εξελίξεις. Παρέχουμε μόνο υπηρεσίες σε κυβερνήσεις και υπηρεσίες επιβολής του νόμου», αρ. φύλλου 43394, 14/3/2026

23. HUMAN RIGHTS COMMITTEE Fifty-fourth session VIEWS, Communication No. 518/1992, 19 Jul 1995 par. 10.4, available at. https://hrlibrary.umn.edu/undocs/html/vws518.htm

24. European Parliament, STUDY Requested by the PEGA Committee "The impact of Pegasus on fundamental rights and democratic processes", p.40, Available at. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

25. Council of Bars & Law Societies of Europe, "RECOMMENDATIONS ON THE PROTECTION OF FUNDAMENTAL RIGHTS IN THE CONTEXT OF 'NATIONAL SECURITY", 2019, p.6,7, available at. https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

26. EUROPEAN DATA PROTECTION SUPERVISOR, "Preliminary Remarks on Modern Spyware", 15 Feb 2022, available at. https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

ΙΣΤΟΣΕΛΙΔΕΣ

1. https://www.microsoft.com/en-us/security/business/security-101/what-is-malware [Ημερομηνία πρόσβασης 31-03-2026]

2. https://www.kaspersky.com/resource-center/threats/types-of-malware [Ημερομηνία πρόσβασης 31-03-2026]

3. https://www.cybersecurity-automation.com/what-is-the-difference-between-malware-vs-spyware/ [Ημερομηνία πρόσβασης 31-03-2026]

4. https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds [Ημερομηνία πρόσβασης 31-03-2026]

5. https://www.avg.com/en/signal/history-of-viruses [Ημερομηνία πρόσβασης 31-03-2026]

6. https://guardiandigital.com/resources/blog/spyware [Ημερομηνία πρόσβασης 11-04-2026]

7. https://www.pewresearch.org/internet/2006/02/22/invasion-of-the-computer-snatchers/ [Ημερομηνία πρόσβασης 31-03-2026]

8. https://www.wired.com/story/internet-explorer-browser-dead/[Ημερομηνία πρόσβασης 31-03-2026]

9. https://www.kaspersky.com/resource-center/threats/adware[Ημερομηνία πρόσβασης 31-03-2026]

10. https://www.avast.com/c-spyware [Ημερομηνία πρόσβασης 31-03-2026]

11. https://www.enterprisenetworkingplanet.com/security/what-is-spyware/ [Ημερομηνία πρόσβασης 31-03-2026]

12. https://www.cybersecurity-automation.com/what-is-the-difference-between-malware-vs-spyware/ [Ημερομηνία πρόσβασης 31-03-2026]

13. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?params=/context/sis_research/article/10899/&path_info=1076211.1076245.pdf [Ημερομηνία πρόσβασης 31-03-2026]

14. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/tailgating-piggybacking-attack/ [Ημερομηνία πρόσβασης 31-03-2026]

15. https://www.dla.mil/About-DLA/News/News-Article-View/Article/3559637/piggybacking-can-open-doors-to-security-problems/ [Ημερομηνία πρόσβασης 31-03-2026]

16. https://cyberhoot.com/el/cybrary/piggybacking/ [Ημερομηνία πρόσβασης 31-03-2026]

17. https://www.huntress.com/cybersecurity-101/topic/anti-spyware [Ημερομηνία πρόσβασης 31-03-2026]

18. https://www.britannica.com/topic/cyberspace [Ημερομηνία πρόσβασης 31-03-2026]

19. https://www.consilium.europa.eu/el/policies/cybersecurity/ [Ημερομηνία πρόσβασης 31-03-2026]

20. https://www.bigcommerce.com/articles/ecommerce/sustainable-ecommerce/ [Ημερομηνία πρόσβασης 31-03-2026]

21. https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf [Ημερομηνία πρόσβασης 31-03-2026]

22. https://www.bbc.com/news/articles/cj6dx4886rpo [Ημερομηνία πρόσβασης 31-03-2026]

23. https://www.tanea.gr/2024/07/26/greece/skandalo-ypoklopon-o-katalogos-ton-koinon-stoxon-eyp-kai-predator/ [Ημερομηνία πρόσβασης 31-03-2026]

24. https://www.hrw.org/report/2025/05/08/bad-worse/deterioration-media-freedom-greece [Ημερομηνία πρόσβασης 31-03-2026]

25. https://www.theguardian.com/world/2023/may/09/eu-parliament-report-calls-for-tighter-regulation-of-spyware [Ημερομηνία πρόσβασης 31-03-2026]

26. https://www.hks.harvard.edu/centers/carr-ryan/our-work/carr-ryan-commentary/spyware-cases-europe-and-africa-spotlight-privacy[Ημερομηνία πρόσβασης 31-03-2026]

27. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EL.html [Ημερομηνία πρόσβασης 31-03-2026]

28. https://www.israelnationalnews.com/news/360211 [Ημερομηνία πρόσβασης 31-03-2026]

29. https://www.nbcnews.com/tech/security/least-50-us-government-employees-hit-spyware-white-house-says-rcna76820 [Ημερομηνία πρόσβασης 31-03-2026]

30. https://www.business-humanrights.org/en/latest-news/court-document-reveals-locations-of-thousands-of-whatsapp-victims-targeted-by-nso-spyware/ [Ημερομηνία πρόσβασης 31-03-2026]

31. https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety [Ημερομηνία πρόσβασης 31-03-2026]

32. https://www.wassenaar.org/app/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf [Ημερομηνία πρόσβασης 31-03-2026]

33. https://www.protothema.gr/world/article/1382350/austirous-kanones-gia-ti-hrisi-kataskopeutikou-logismikou-enekrine-to-europaiko-koinovoulio/ [Ημερομηνία πρόσβασης 31-03-2026]

34. https://www.avast.com/c-spyware12.https://www.wto.org/library/events/event_resources/ecom_0106202310/177_639.pdf [Ημερομηνία πρόσβασης 31-03-2026]

35. https://www.eett.gr/eett/schetika-me-tin-eett/armodiotites/[Ημερομηνία πρόσβασης 31-03-2026]

36. https://www.dpa.gr/el/arxi/armodiotites [Ημερομηνία πρόσβασης 31-03-2026]

37. https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince [Ημερομηνία πρόσβασης 31-03-2026]

38. https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware [Ημερομηνία πρόσβασης 31-03-2026]

39. https://www.in.gr/2024/01/08/stories/intellexa-kai-cytrox-ena-daidalodes-systima-ypoklopon-gia-varia-portofolia/#goog_rewarded [Ημερομηνία πρόσβασης 31-03-2026]