ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Πρόγραμμα Μεταπτυχιακών Σπουδών**

**«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»**

Ακαδημαϊκό έτος 2022-2023

**ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**
**της Αγγελικής Καλούδη (Α.Μ.: ΜΔΙ2116)**

# ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ: ΟΡΙΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟΡΡΗΤΟΥ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

**Επιβλέπουσα: Καθηγήτρια Λίλιαν Μήτρου**

Πειραιάς, Φεβρουάριος 2023

*Στους γονείς μου, Μαρία και Γιώργο και στον αδελφό μου, Μηνά.*

«Το Πανοπτικόν λειτουργεί σαν ένα είδος εργαστηρίου εξουσίας. Χάρη στους μηχανισμούς επιτήρησης, που διαθέτει, αποκτά ολοένα και μεγαλύτερη αποτελεσματικότητα και ικανότητα διείσδυσης στη συμπεριφορά των ατόμων.»

Μ. Φουκώ, Επιτήρηση και Τιμωρία, 1975

**ΕΥΧΑΡΙΣΤΙΕΣ**

Η εκπόνηση Μεταπτυχιακής Διπλωματικής Εργασίας δεν είναι μια απλή βιβλιογραφική αναζήτηση πηγών, αλλά αποτελεί έναν κοπιώδη εσωτερικό διάλογο με βάση τα δεδομένα και τη νομοθεσία, που καλλιεργεί την κριτική σκέψη, την αμφισβήτηση και την εξέλιξη. Στο ταξίδι αυτό δεν στάθηκα μόνη, αλλά είχα την ευκαιρία να συμπορευθώ με σημαντικούς συνταξιδιώτες και καθοδηγητές, που με βοήθησαν να το ολοκληρώσω.

Θα ήθελα να ευχαριστήσω την Επιβλέπουσα Καθηγήτριά μου, κυρία Λίλιαν Μήτρου, για την πολύτιμη βοήθειά της, τις παρατηρήσεις και το γόνιμο διάλογο.

Η οικογένειά μου ήταν αυτή που με βοήθησε ψυχικά και πρακτικά να ολοκληρώσω αυτό το πόνημα και τους ευχαριστώ πολύ για την στήριξη.

Ιδιαίτερες ευχαριστίες αξίζουν και στους φίλους μου, που με συντρόφευσαν στις ανησυχίες μου και ειδικά σε όσους από αυτούς είναι γνώστες των τεχνολογικών ζητημάτων για την σημαντική αρωγή τους στα τεχνολογικά θέματα των κατασκοπευτικών λογισμικών, στα οποία ως νομικός υστερούσα.

**ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ**

**ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ**

ECHR: European Court of Human Rights

EPRS: European Parliamentary Research Service

FDPIC: Federal Data Protection and Information Commissioner

GDPR: General Data Protection Regulation

Ibid: ibidem

p.p.: page

ΑΔΑΕ: Αρχή Διασφάλισης Απορρήτου Επικοινωνιών

Αιτ. Σκ.: Αιτιολογική σκέψη

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΑΠ: Άρειος Πάγος

Βλ.: Βλέπε

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

Γνμδ: Γνωμοδότηση

ΔΣΑΠΔ: Διεθνές Σύμφωνο για Ατομικά και Πολιτικά Δικαιώματα

Εδ.: εδάφιο

ΕΔΔΑ: Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων

ΕΕ: Ευρωπαϊκή Ένωση

ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

Εκδ.: εκδόσεις

Επ. : Επόμενα

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση Δικαιωμάτων Ανθρώπου

ΕΥΠ: Εθνική Υπηρεσία Πληροφοριών

ΕφτΚ: Εφημερίδα της Κυβέρνησης

Κ.ά.: Και άλλα

Κ.λπ.: Και λοιπά

ΚΝοΒ: Κώδικας Νομικού Βήματος

Κοκ: Και ούτω καθεξής

ΚΠοινΔ: Κώδικας Ποινικής Δικονομίας

Ν.: Νόμος

Οδ. : Οδηγία

ΟΕ Ά. 29: Ομάδα Εργασίας του άρθρου 29

ΟΗΕ: Οργανισμός Ηνωμένων Εθνών

Οπ.: Όπου παραπάνω

Παρ.: Παράγραφος

Περ.: περίπτωση

Π.χ.: Παραδείγματος χάριν

ΠΚ: Ποινικός Κώδικας

ΠΝΠ: Πράξη Νομοθετικού Περιεχομένου

Σ: Σύνταγμα

ΣτΕ: Συμβούλιο της Επικρατείας

Στοιχ.: στοιχείο

Τ.: Τόμος

Τεύχ.: τεύχος

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

**ΠΕΡΙΛΗΨΗ**

Η παρούσα διπλωματική εργασία φιλοδοξεί να αναλύσει την χρήση των λογισμικών κατασκοπείας, τις επιπτώσεις αυτών στα ανθρώπινα δικαιώματα και να παραθέσει το ισχύον νομικό πλαίσιο, που προστατεύει τα άτομα από την αλόγιστη χρήση τους. Σε συνάρτηση με τις τρέχουσες εξελίξεις σχετικά με την νόμιμη διαδικασία άρσης του απορρήτου και τις επιπτώσεις των λογισμικών κατασκοπείας στον τομέα της κυβερνοασφάλειας και του κυβερνοεγκλήματος, γίνεται αναφορά και στις προκλήσεις που γεννιούνται από την εκθετική τεχνολογική ανάπτυξή τους σε διάφορους τομείς όπως το ηλεκτρονικό έγκλημα, η εργασία, η διαφήμιση κ.ά. Το αντικείμενο της διπλωματικής δεν περιορίζεται στην απλή παράθεση εθνικών νομικών διατάξεων, αλλά επιχειρεί να ξεφύγει από τα εγχώρια δρώμενα και αφουγκράζεται τη γενικότερη τάση χρήσης κατασκοπευτικών λογισμικών παγκοσμίως και τους κινδύνους που ελλοχεύει για την προστασία του απορρήτου και των προσωπικών δεδομένων.

## ΕΙΣΑΓΩΓΗ

Ο ψηφιακός μετασχηματισμός και οι καινοτομίες στον τομέα της τεχνολογίας, πληροφορικής και επικοινωνιών ενίσχυσαν την συνδεσιμότητα και την πρόσβαση σε υπηρεσίες. Παράλληλα, αύξησαν τη δυνατότητα των Κρατών για παρακολούθηση και παρέμβαση στα ανθρώπινα δικαιώματα και τις θεμελιώδεις ελευθερίες των πολιτών. Οι πρόσφατες εξελίξεις σχετικά με τα λογισμικά κατασκοπείας τόσο στην Ελλάδα αλλά και στον υπόλοιπο κόσμο ανέδειξαν την ανάγκη έναρξης συζητήσεως διεπιστημονικού ενδιαφέροντος, τόσο νομικού και τεχνολογικού αλλά και κοινωνικού.

Η χρήση τέτοιων παρεμβατικών μορφών τεχνολογίας όχι μόνο προσβάλλει την απόλαυση του δικαιώματος της ιδιωτικότητας αλλά και την ίδια την ιδεολογία της αυτονομίας και της φυσικής ακεραιότητας των ατόμων. Οι μορφές παρακολούθησης, που έχουν διαδοθεί έως σήμερα τορπιλίζουν επίσης την ίδια την αρχή του κράτους δικαίου και την αξιοπιστία των θεσμών.

Πράγματι, οι λόγοι εθνικής ασφάλειας και η διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων δικαιολογούν καταρχάς την χρήση μορφών παρακολούθησης και την άρση του απορρήτου των επικοινωνιών. Οι μυστικές υπηρεσίες έχουν έννομο συμφέρον να αποκτήσουν πρόσβαση στις απαραίτητες πληροφορίες, συμπεριλαμβανομένων των μεταδεδομένων, για να προλάβουν, να ερευνήσουν και να καταστείλουν το έγκλημα ή να καταπολεμήσουν τους κινδύνους που σχετίζονται με την εθνική ασφάλεια. Αυτό δε σημαίνει ότι το πεδίο δράσης των κρατών αναφορικά με τους λόγους εθνικής ασφάλειας για τους οποίους μπορεί να παρακολουθείται κάποιος είναι απεριόριστο.[1] Τα κράτη δεσμεύονται από τα εθνικά και τα διεθνή ή και τα ευρωπαϊκά όργανα, τους θεσμούς και τη νομοθεσία. Τόσο η ΕΣΔΑ αλλά και το ελληνικό Σύνταγμα επιτάσσει στα κράτη μια αρνητική υποχρέωση, να απέχουν από κάθε πράξη παραβίασης των θεμελιωδών ατομικών δικαιωμάτων, αλλά και τη θετική υποχρέωση να τα προασπίζονται με κάθε ενέργεια.

Η ευρεία χρήση μυστικών συστημάτων παρακολούθησης, λογισμικών κατασκοπείας και λογισμικών άρσης τηλεπικοινωνιών πάντα δημιουργεί χώρο για περαιτέρω κρατική αυθαιρεσία, διακινδυνεύοντας την απόλαυση θεμελιωδών δικαιωμάτων και ελευθεριών

[1] Council of Europe / European Court of Human Rights, *"National Security and European Case-Law"*, 2013, p.p 2. Διαθέσιμο στο: https://rm.coe.int/168067d214 [Ημερομηνία πρόσβασης: 3/1/2023].

όπως το δικαίωμα στο απόρρητο, την ελευθερία της έκφρασης κ.ά.[2] Οι συνέπειες της μαζικής ή και της στοχευμένης παρακολούθησης μέσω τον λογισμικών κατασκοπείας μπορεί να είναι καταστροφικές. Η χρήση υψηλής τεχνολογίας μέσων παρακολούθησης χρησιμοποιείται ήδη σε αυταρχικά κράτη για την επίθεση κατά πολιτικών αντιπάλων και την καταστολή της ελευθερίας της έκφρασης και της πληροφόρησης. Οι πρόσφατες εξελίξεις απέδειξαν ότι τα λογισμικά κατασκοπείας χρησιμοποιούνται και από δημοκρατικές κοινωνίες, εγείροντας περισσότερα ερωτηματικά και δημιουργώντας μια σύγχρονη φουκωϊκή «πανοπτική κοινωνία»[3], όπου οι πολίτες επιτηρούνται συνεχώς, ακόμα και σε ιδιωτικές στιγμές τους και έχουν μάθει να δρουν ανελεύθεροι γνωρίζοντας ότι ενδέχεται πάντα κάποιος να παρακολουθεί τη ζωή τους.

Στο πρώτο κεφάλαιο επιχειρείται μια πρώτη τεχνολογική προσέγγιση του όρου λογισμικών κατασκοπείας, της λειτουργίας και της ιστορικής τους εξέλιξης καθώς και μια σύγκριση με την πρακτική που ακολουθείται σε άλλες χώρες του κόσμου ως προς αυτά. Στο δεύτερο κεφάλαιο γίνεται εκτενής αναφορά στις χρήσεις των κατασκοπευτικών λογισμικών σε διάφορους τομείς και περιγράφεται συνοπτικά η τρέχουσα επικαιρότητα σε συνάρτηση με δύο πολύ γνωστά λογισμικά, Predator και Pegasus. Το τρίτο κεφάλαιο προσπαθεί να απαντήσει στο μείζον ερώτημα: εάν είναι νόμιμη η χρήση των λογισμικών κατασκοπείας. Για το λόγο αυτό αναλύονται σημαντικές νομικές διατάξεις του Συντάγματος, της ΕΣΔΑ και του Ποινικού Κώδικα, ενώ περιγράφεται και επιγραμματικά η νόμιμη διαδικασία άρσης του απορρήτου με βάση το ν. 2225/94. Το τέταρτο κεφάλαιο αναφέρεται στις σύγχρονες προκλήσεις από την χρήση κατασκοπευτικών λογισμικών, στα εξωτερικά στοιχεία της επικοινωνίας, στις μαζικές παρακολουθήσεις, στην κυβερνοασφάλεια, εν αναμονή του Κανονισμού e-Privacy και του νέου νόμου σχετικά με την άρση του απορρήτου.

[2] Βλ. Κεφάλαιο 3 παρ. 3.2

[3] Μ. Φουκώ, *«Επιτήρηση και τιμωρία. Η γέννηση της φυλακής»*, Εκδόσεις Ράππα, Αθήνα 1989, σελ. 265-266. Την ιδέα του Πανοπτικού ανέπτυξε ο φιλόσοφος Τζέρεμι Μπένθαμ. Πρόκειται για την αρχιτεκτονική μιας φυλακής, η οποία είναι τέτοια που επιτρέπει τη συνεχή επιτήρηση των κρατουμένων και την ανεξέλεγκτη εξουσία των ισχυρών. Οι κρατούμενοι τότε αναγκάζονται να δρουν στα πλαίσια της νομιμότητας και των επιταγών των υπεύθυνων λόγω του φόβου της παρακολούθησης. Η ιδέα δεν εφαρμόστηκε ποτέ πρακτικά.

## ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ: ΕΙΣΑΓΩΓΗ ΣΤΑ ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ

### 1.1. Η έννοια των Κατασκοπευτικών λογισμικών

Τα κακόβουλα λογισμικά εν γένει (malware) αποτελούν είδος λογισμικού σχεδιασμένου σκοπίμως με τρόπο ώστε να προκαλέσει πρόβλημα σε έναν υπολογιστή ή δίκτυο και συσκευή και να διαρρεύσει προσωπικά δεδομένα των χρηστών, να αποκτήσει πρόσβαση σε πληροφορίες και συστήματα, στερώντας την πρόσβαση του χρήστη σε πληροφορίες ή να παρέμβει εν αγνοία του χρήστη στην ασφάλεια του υπολογιστή ή οποιουδήποτε άλλου δικτύου π.χ. ενός δικτύου επικοινωνίας. Οι επιθέσεις μέσω κακόβουλων λογισμικών αποτελούν ένα είδος εγκλήματος στον κυβερνοχώρο μεταξύ άλλων εγκλημάτων που διαπράττονται μέσω υπολογιστή. Οι τύποι κακόβουλου λογισμικού δεν είναι συγκεκριμένοι, λόγω της ραγδαίας τεχνολογικής εξέλιξης. Έως σήμερα αναφέρονται ως είδη κακόβουλων λογισμικών οι ιοί των υπολογιστών, τα σκουλήκια (worms), οι δούρειοι ίπποι (trojan horses), το ransomware, τα λογισμικά κατασκοπείας, τα λογισμικά διαφημίσεων.[4]

Τα κατασκοπευτικά λογισμικά ή τα λογισμικά κατασκοπείας (spyware) είναι ένα είδος κακόβουλου λογισμικού (malware) το οποίο με κρυφό τρόπο εγκαθίσταται σε μια συσκευή όπως ένα κινητό τηλέφωνο ή ένας υπολογιστής χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο παράλληλα με την χρήση από τον νόμιμο χρήστη και χωρίς να το ξέρει ο ίδιος. Το λογισμικό κατασκοπείας είναι στην ουσία μορφή κακόβουλου λογισμικού, που στοχεύει στη συλλογή πληροφορίων, ήτοι προσωπικών δεδομένων και στην αποστολή τους σε τρίτα μέρη, με τέτοιο τρόπο ώστε να βλάψουν τον χρήστη π.χ. μέσω της παραβίασης της ιδιωτικότητας ή της διακινδύνευσης της ασφάλειας της ακεραιότητας και της εμπιστευτικότητας του δικτύου ή της συσκευής που βάλλουν. Η συμπεριφορά αυτή δε συνίσταται αποκλειστικά σε παράνομο κακόβουλο λογισμικό, αλλά ενδέχεται να προκύπτει και από νόμιμα λογισμικά. Μερικές φορές δηλαδή τα κατασκοπευτικά λογισμικά μπορεί να περιλαμβάνονται μαζί με γνήσιο νόμιμο λογισμικό, να προέρχονται από κακόβουλο

[4] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies January 2023 "*The impact of Pegasus on fundamental rights and democratic processes*" σελ. 13. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf [Ημερομηνία πρόσβασης: 14/2/2023]

ιστότοπο ή να έχουν προστεθεί στη λειτουργία του γνήσιου νόμιμου λογισμικού.[5] Οι ιστότοποι εμπλέκονται άμεσα με τα λογισμικά κατασκοπείας μέσω π.χ. της παρακολούθησης του ιστού, ενώ δεν είναι επίσης απίθανο να επηρεαστεί και το σκληρό λογισμικό (hardware) ενός υπολογιστή.

Τα κατασκοπευτικά λογισμικά έχουν την ικανότητα να κρύβονται, ώστε να μην μπορεί το θύμα να τα εντοπίσει εύκολα. Με αυτόν τον τρόπο συγκεντρώνουν στοιχεία για τον χρήστη, όπως το ιστορικό ιστοσελίδων που επισκέπτεται, κωδικούς πρόσβασης, ακόμη και αριθμούς πιστωτικών καρτών. Τα στοιχεία αυτά αποτελούν προσωπικά δεδομένα των χρηστών κάποια μάλιστα ανήκουν και σε ειδικές κατηγορίες προσωπικών δεδομένων, όπως τα τραπεζικά δεδομένα αλλά και δεδομένα που ο ίδιος ο χρήστης μπορεί να αποκαλύπτει σε μια τηλεφωνική συνομιλία που παρακολουθείται από κάποιο κατασκοπευτικό λογισμικό.[6] Επίσης, τα κατασκοπευτικά λογισμικά μπορούν να αλλάζουν τις ρυθμίσεις του χρήστη χωρίς την συγκατάθεσή του και να εκτελούν κακόβουλες δραστηριότητες, όπως όλα τα κακόβουλα λογισμικά.

Ενώ λοιπόν, ο όρος κατασκοπευτικό λογισμικό παραπέμπει στην χρήση αυτών των λογισμικών για κατασκοπεία των συσκευών, οι λειτουργίες των λογισμικών κατασκοπείας μπορεί να επεκτείνονται πέραν από την απλή κατασκοπεία. Τα κατασκοπευτικά λογισμικά δεν είναι απίθανο να παρεμβαίνουν και να παρεμποδίζουν τον έλεγχο που έχει ο χρήστης στη συσκευή του, εγκαθιστώντας επιπλέον λογισμικά ή ανακατευθύνοντας τους φυλλομετρητές. Κάποια από τα κατασκοπευτικά λογισμικά αλλάζουν τις ρυθμίσεις της συσκευής, γεγονός που επηρεάζει την ίδια τη λειτουργία της συσκευής και μπορεί να προκαλέσει χαμηλή ταχύτητα, μη εξουσιοδοτημένες αλλαγές στον φυλλομετρητή ή αλλαγές στο λογισμικό του υπολογιστή.

---

[5] Για παράδειγμα η πρακτική του Facebook και άλλων ιστότοπων παρακολούθησης της δραστηριότητας περιήγησης των χρηστών να εμφανίζουν διαφημιστικά ανάλογα με τις προτιμήσεις και τα ενδιαφέροντα των χρηστών ή και της πρόσφατες αναζητήσεις. Βλ. CNet News (2011) *«Τα κουμπιά "Μου αρέσει", "tweet" αποκαλύπτουν τους ιστότοπους που επισκέπτεστε»*. Διαθέσιμο στο: https://www.cnet.com/videos/like-tweet-buttons-divulge-sites-you-visit/ [Ημερομηνία πρόσβασης: 3/1/2023] .

[6] Foti D. σε Bachmaier, L.; Ruggeri W. S. (2022) *"Investigating and Preventing Crime in the Digital Era"* σελ. 156 επ. Διαθέσιμο στο: https://doi.org/10.1007/978-3-031-13952-9 [Ημερομηνία πρόσβασης: 3/1/2023].

Μερικές ενδεικτικές λειτουργίες που επιτελούν τα κατασκοπευτικά λογισμικά σε υπολογιστή είναι μεταξύ άλλων η αλλαγή της αρχικής σελίδας του φυλλομετρητή (browser), η αλλαγή της λίστας αγαπημένων σελιδοδεικτών του φυλλομετρητή (browser), η προσθήκη νέων γραμμών εργαλείων στον φυλλομετρητή (browser), η εμφάνιση παραθύρων με ανεπιθύμητες διαφημίσεις κ.ά. Αυτές οι ενέργειες επηρεάζουν τη συμπεριφορά της συσκευής με τέτοιο τρόπο, ώστε ακόμα και η επανεκκίνηση του υπολογιστή να μην μπορεί να επαναφέρει τις προηγούμενες ρυθμίσεις. Οι επιθέσεις αυτές ονομάζονται πειρατεία του φυλλομετρητή (browser hijacking).[7] Τα λογισμικά κατασκοπείας συνήθως ξεκινούν κατά την εκκίνηση του υπολογιστή και καταλαμβάνουν ταυτόχρονα την μνήμη και υπολογιστική ισχύ, ενώ αρκετές φορές απενεργοποιούν σκοπίμως το τείχος προστασίας (firewall), αδρανοποιώντας τυχόν ανταγωνιστικό λογισμικό κατασκοπείας.

Υπάρχουν ορισμένες χώρες, όπως η Γερμανία στις οποίες τα κατασκοπευτικά λογισμικά χρησιμοποιούνται ή κατασκευάζονται από την ίδια την κυβέρνηση. Αυτά τα λογισμικά ονομάζονται "govware" και είναι συνήθως κακόβουλα λογισμικά, που χρησιμοποιούνται για την υποκλοπή επικοινωνιών από τον στόχο. Στις ΗΠΑ χρησιμοποιείται ο όρος "Policeware" ως είδος κατασκοπευτικού λογισμικού από κρατικούς φορείς για παρόμοιους σκοπούς.[8] Υπάρχουν επίσης, χώρες όπως όπως η Ελβετία και η Γερμανία που έχουν αναπτύξει συγκεκριμένο νομικό πλαίσιο που διέπει τη χρήση τέτοιων λογισμικών.[9]

---

[7] Tanenbaum, A. (2009) «*Σύγχρονα Λειτουργικά Συστήματα» 3η έκδοση* Κλειδάριθμος. Σελ. 792–796.

[8] Reimer, J. Ars Technica (2007) *" The tricky issue of spyware with a badge: meet 'policeware "*.Διαθέσιμο στο: https://arstechnica.com/information-technology/2007/07/will-security-firms-avoid-detecting-government-spyware/ [Ημερομηνία πρόσβασης: 3/1/2023]

[9] Cupa, B. *"Trojan Horse Resurrected: On the Legality of the Use of Government Spyware"*, LISS 2013, σελ. 419–428. Διαθέσιμο στο: https://www.zora.uzh.ch/id/eprint/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf [Ημερομηνία πρόσβασης: 3/1/2023]

### 1.2. Ιστορική εξέλιξη των Κατασκοπευτικών λογισμικών και τα είδη τους

Ο όρος spyware εμφανίστηκε πρώτη φορά το 1995 σε μια ανάρτηση στο Usenet[10], το οποίο καυτηρίαζε το επιχειρηματικό μοντέλο της Microsoft. Το λογισμικό κατασκοπείας αρχικά, υποδήλωνε λογισμικό που προοριζόταν για σκοπούς κατασκοπείας και κυρίως κάμερες.[11] Ωστόσο, στις αρχές του 2000 ο ίδιος όρος χρησιμοποιήθηκε από τον ιδρυτή των Zone Labs , Gregor Freund, σε ένα δελτίο τύπου για το Zone Alarm Personal Firewall. [12] Ένας γονέας που χρησιμοποιούσε το ZoneAlarm για την εκπαίδευση των παιδιών του ειδοποιήθηκε ότι το Reader Rabbit , ένα λογισμικό εκπαίδευσης που εμπορευόταν η Mattel, η γνωστή εταιρεία παιχνιδιών, έστελνε κρυφά δεδομένα πίσω στη Mattel.[13]

Το 2005 η AOL και η National Cyber-Security Alliance εξέδωσαν μελέτη σύμφωνα με την οποία πάνω από τους μισούς υπολογιστές των χρηστών που συμμετείχαν στην έρευνα είχαν μολυνθεί με κάποιο είδος spyware. Συντριπτικό ποσοστό των ερωτηθέντων χρηστών που είχαν μολυνθεί με spyware ανέφεραν ότι αγνοούσαν την ύπαρξη του και ανέφεραν ότι δεν είχαν δώσει άδεια για την εγκατάσταση του.[14] Μέχρι το 2006, τα λογισμικά κατασκοπείας είχαν καταφέρει να γίνουν η πιο σημαντική απειλή ασφαλείας για συστήματα υπολογιστών. Οι υπολογιστές στους οποίους ο Internet Explorer ήταν το κύριο πρόγραμμα

---

[10] Το Usenet είναι ένα σύστημα συζήτησης διαθέσιμο για υπολογιστές παγκοσμίου εμβέλειας στο οποίο οι χρήστες μπορούν να συζητούν, να αναρτούν απόψεις και άρθρα, τα οποία τα διαβάζει ο καθένας.

[11] Staff Report Federal Trade Commission, March 2005 *"Monitoring Software on Your PC: Spyware, Adware, and Other Software"* σελ. 2

[12] Sharon, W. CNET (2004) *"The spyware inferno"*. Διαθέσιμο στο: https://www.cnet.com/tech/services-and-software/the-spyware-inferno/ [Ημερομηνία πρόσβασης: 3/1/2023]

[13] Hawkins, D.; US News & World Report (2000) *"Privacy Worries Arise Over Spyware in Kids' Software"*. Διαθέσιμο στο: https://web.archive.org/web/20131103060440/http://www.usnews.com/usnews/culture/articles/000703/archive_015408.htm [Ημερομηνία πρόσβασης: 3/1/2023]

[14]America Online & The National Cyber Security Alliance (2005) *"AOL/NCSA Online Safety Study"*.Διαθέσιμο στο: https://web.archive.org/web/20051213090601/http://www.staysafeonline.info/pdf/safety_study_2005.pdf [Ημερομηνία πρόσβασης: 3/1/2023]

περιήγησης ήταν ιδιαίτερα ευάλωτοι σε τέτοιες επιθέσεις, όχι μόνο επειδή το συγκεκριμένο πρόγραμμα περιήγησης ήταν το πιο ευρέως χρησιμοποιούμενο, αλλά επειδή διέθετε στενή ενσωμάτωση με τα Windows, με αποτέλεσμα το spyware να έχει άμεση πρόσβαση σε καίρια σημεία του συστήματος. Ο συνδυασμός άγνοιας των χρηστών σχετικά με αυτές τις αλλαγές στο πρόγραμμα περιήγησης τους και η υπόθεση του Internet Explorer ότι όλα τα στοιχεία των πιθανών αλλαγών είναι καλοήθη, συντέλεσαν στη σημαντική εξάπλωση του spyware.

Η χρήση του όρου "spyware" τελικά με τον καιρό μειώθηκε καθώς η πρακτική της κατασκοπείας των χρηστών έχει υιοθετηθεί όλο και περισσότερο από μεγάλους ιστότοπους, εταιρείες data mining και κράτη. Αυτή η πρακτική γενικά δεν βρίσκει ιδιαίτερα νομικά εμπόδια έως και σήμερα με αποτέλεσμα να δρουν ανεξέλεγκτα και να υποχρεώνουν τους χρήστες να παρακολουθούνται, έμμεσα ή άμεσα.

Οι κατηγορίες των κατασκοπευτικών λογισμικών δεν είναι συγκεκριμένες, καθώς λόγω της ταχύτατης τεχνολογικής εξέλιξης και της παρασκηνιακής τους δράσης η απόκτηση πλήρους γνώσης γι' αυτά καθίσταται δυσχερής έως και αδύνατη.[15] Μερικά από τα είδη των κατασκοπευτικών λογισμικών είναι το λογισμικό κατασκοπείας για μάρκετινγκ, το οποίο συλλέγει και στέλνει τις πληροφορίες, συνήθως με σκοπό την στοχευμένη διαφήμιση σε συγκεκριμένες μηχανές· τα κατασκοπευτικά λογισμικά παρακολούθησης, τα οποία τοποθετούνται εσκεμμένα από τις εταιρείες για παράδειγμα στους υπολογιστές ή στα τηλέφωνα των υπαλλήλων ώστε να τους παρακολουθούν· το κλασικό κακόβουλο λογισμικό.[16] Η λειτουργία αυτών των λογισμικών διαφέρει από παρακολούθηση της ηλεκτρονικής δραστηριότητας των υποκειμένων έτσι ώστε π.χ. οι διαφημιστές να μπορούν να καταγράψουν τα ενδιαφέροντά σας μέχρι παρακολούθηση της πληκτρολόγησης και γενικά όλης της χρήσης μιας συσκευής.

Τα κατασκοπευτικά λογισμικά μπορούν να δράσουν σαν το adware, τα συστήματα παρακολούθησης, το tracking, συμπεριλαμβανομένης της παρακολούθησης του ιστού (web

[15] Stouffer, C. Norton (2021): *"Spyware: What is spyware + how to protect yourself"* Διαθέσιμο στο: https://us.norton.com/blog/malware/spyware [Ημερομηνία πρόσβασης: 3/1/2023]

[16] Βλ. παρ. 1.1

tracking), και τους δούρειους ίππους (trojans)[17]. Το adware παρακολουθεί το ιστορικό και τις λήψεις με σκοπό να προβλέψει τα προϊόντα και τις υπηρεσίες που οι χρήστες πιθανώς να εμφανίζουν ενδιαφέρον για διαφημιστικούς λόγους. Οι δούρειοι ίπποι είναι ένα είδος κακόβουλου λογισμικού που παίρνει την μορφή νόμιμου λογισμικού. Όπως ο ελληνικός δούρειος ίππος, έτσι κι αυτό παραπλανά τον χρήστη, ώστε να του επιτρέψει την είσοδο στο σύστημα και στην συσκευή, δρώντας ως ένα αρχείο ή ένα λογισμικό αναβάθμισης, ενώ μετά καταστρέφει ή κλέβει τα δεδομένα. Το web tracking είναι μια κοινή πρακτική, που χρησιμοποιείται για να παρακολουθείται η διαδικτυακή δραστηριότητα, κυρίως για διαφημιστικούς σκοπούς. Τα συστήματα παρακολούθησης ως λογισμικά κατασκοπείας μπορούν να καταγράψουν οτιδήποτε κάνει ο χρήστης μιας συσκευής και κάθε τι που θα πει σε μια τηλεφωνική συνομιλία από το chat, mails, κινήσεις πληκτρολογίου μέσω key logger, διαλόγους, ιστοσελίδες που επισκέφθηκε κ.λπ. Αυτές οι τέσσερις κατηγορίες δεν αποκλείουν η μία την άλλη και έτσι πολλά διαφορετικά είδη λογισμικού μπορεί να συνυπάρχουν σε ένα σύστημα, ενώ ο τρόπος μόλυνσης είναι σχεδόν ίδιος για όλες αυτές τις κατηγορίες. Ο απώτερος σκοπός αυτών των λογισμικών είναι να εγκατασταθούν και να προσβάλουν το σύστημα χωρίς να εντοπιστούν από τον χρήστη και χωρίς να μπορούν να αφαιρεθούν με ασφάλεια.

Τα λογισμικά κατασκοπείας χρησιμοποιούνται ευρέως για να υποκλέψουν πληροφορίες, προσωπικά δεδομένα, των χρηστών και να αποθηκεύσουν τις διαδικτυακές κινήσεις των χρηστών, ενώ πολλές φορές χρησιμοποιούνται ως αναδυόμενα διαφημιστικά παράθυρα (pop-up ads). Όποτε το κατασκοπευτικό λογισμικό χρησιμοποιείται για κακόβουλες ενέργειες, η παρουσία του στο σύστημα αποκρύπτεται από τον χρήστη του συστήματος και ο τελευταίος αδυνατεί να το ανιχνεύσει. Ορισμένα λογισμικά κατασκοπείας, όπως τα keyloggers ή λογισμικά παρακολούθησης τηλεφώνων, ενδέχεται να εγκατασταθούν από τον ίδιο κάτοχο μιας συσκευής π.χ. έναν εργοδότη σκόπιμα για την παρακολούθηση των χρηστών π.χ. των υπαλλήλων μιας εταιρείας.

[17] University of Essex (2013) "*Spyware*". Διαθέσιμο στο: https://web.archive.org/web/20131101154446/https:/www.justice.gov.tr/ejournal/pdf/cybercrime_essay.pdf [Ημερομηνία πρόσβασης: 3/1/2023]

### 1.3. Η δράση των Κατασκοπευτικών λογισμικών και οι τρόποι αντιμετώπισης τους.

Τα κατασκοπευτικά λογισμικά δεν εξαπλώνονται απαραίτητα με τον ίδιο τρόπο όπως οι ιοί, αλλά σε γενικές γραμμές ακολουθούν το ίδιο μοτίβο μόλυνσης όπως και τα λοιπά κακόβουλα λογισμικά. Το λογισμικό κατασκοπείας εγκαθίσταται μόνο του σε ένα οποιοδήποτε σύστημα, εξαπατώντας τον χρήστη ή εκμεταλλευόμενο την «τρωτότητα» του συστήματος. Τα περισσότερα λογισμικά εγκαθίστανται εν αγνοία του χρήστη χρησιμοποιώντας τακτικές εξαπάτησης, όπως για παράδειγμα η προβολή της εικόνας ενός δήθεν επιθυμητού λογισμικού.

Συχνοί τρόποι εξάπλωσης είναι μέσω της εγκατάστασης προγραμμάτων όπως τα προγράμματα ανταλλαγής αρχείων (peer-to-peer) είτε με την εγκατάσταση πρόσθετων add-ons, προγραμμάτων που ενισχύουν τον φυλλομετρητή (browser). Μπορεί να εμφανίζονται σε έναν υπολογιστή με τη μορφή γραμμών εργαλείων, κουμπιών αναζήτησης, κινούμενων εικόνων κ.ά. Επίσης, είναι δυνατή η μόλυνση από λογισμικό κατασκοπείας από την επίσκεψη σε ιστοτόπους, οι οποίοι προσπαθούν να κατεβάσουν και να εγκαταστήσουν αυτόματα στον υπολογιστή τέτοια λογισμικά.

Άλλες κοινές τακτικές μόλυνσης είναι η χρήση ενός δούρειου ίππου, δηλαδή μικροεφαρμογών κατασκοπείας με χαρακτηριστικά κοινών λογισμικών. Ορισμένοι κατασκευαστές κατασκοπευτικών λογισμικών μολύνουν ένα σύστημα μέσω οπών ασφαλείας στο πρόγραμμα περιήγησης και έτσι όταν ο χρήστης πλοηγείται σε μια ιστοσελίδα που ελέγχεται από τον κατασκευαστή του εν λόγω λογισμικού, η σελίδα περιέχει κώδικα που επιτίθεται στο πρόγραμμα περιήγησης και αναγκάζει τη λήψη του λογισμικού.

Όπως προαναφέρθηκε[18] η λειτουργία των Windows επιτρέπει την δράση των λογισμικών κατασκοπείας ήδη από την εκκίνηση του υπολογιστή. Το λογισμικό κατασκοπείας μπορεί να εκμεταλλευτεί αυτή τη δυνατότητα για να παρακάμψει τις προσπάθειες αφαίρεσης του από τους χρήστες. Τα λογισμικά κατασκοπείας συνήθως συνδέονται από κάθε θέση στο μητρώο, που επιτρέπει την εκτέλεση. Μόλις εκτελεστεί, το λογισμικό κατασκοπείας θα ελέγχει περιοδικά εάν κάποιος από αυτούς τους συνδέσμους έχει αφαιρεθεί και σε περίπτωση που αυτό συμβεί τα λογισμικά κατασκοπείας έχουν την ικανότητα να αποκαθίστανται αυτόματα Αυτό διασφαλίζει ότι το λογισμικό θα εκτελεστεί σε κάθε

[18] Βλ. παρ. 1.1

περίπτωση κατά την εκκίνηση του λειτουργικού συστήματος, ακόμη και αν αφαιρεθούν ορισμένες από τις συνδέσεις.

Τα κατασκοπευτικά λογισμικά συνήθως προσβάλλουν τις συσκευές με πολλαπλές μολύνσεις. Συχνά φαινόμενα της μόλυνσης είναι η ανεπιθύμητη συμπεριφορά του συστήματος, η υποβάθμιση της απόδοσης, μείωση της ταχύτητας του δικτύου και της σταθερότητας του συστήματος π.χ. πάγωμα εφαρμογών, δυσκολία στην εκκίνηση του υπολογιστή και σφάλματα στην χρήση. Τις περισσότερες φορές τα κατασκοπευτικά λογισμικά δεν γίνονται αντιληπτά από τον χρήστη, ο οποίος υποθέτει ότι τα διάφορα προβλήματα σχετίζονται με παροχή ελαττωματικού προϊόντος. Οι περισσότεροι χρήστες καταφεύγουν στη βοήθεια τεχνικών και μηχανικών πληροφορικής ή αγοράζουν νέο υπολογιστή επειδή ο υπάρχων είναι πλέον πολύ «αργός». Εξάλλου, τα συστήματα που έχουν μολυνθεί σε μεγάλο βαθμό ενδέχεται να απαιτούν ολοκληρωτική επανεγκατάσταση του λογισμικού τους προκειμένου να επανέλθουν σε πλήρη λειτουργικότητα.

Επιπλέον, κάποια λογισμικά κατασκοπείας απενεργοποιούν το τείχος προστασίας και το λογισμικό προστασίας από ιούς ή αλλοιώνουν τις ρυθμίσεις ασφαλείας, γεγονός που καθιστά το σύστημα πιο επιρρεπές. Άλλωστε, ορισμένα κατασκοπευτικά λογισμικά αδρανοποιούν ή και καταργούν ανταγωνιστικά προγράμματα, μιας και όσο περισσότερα προβλήματα δημιουργούνται στο σύστημα από αυτά τα λογισμικά τόσο αυξάνεται η πιθανότητα οι χρήστες να προβούν σε ενέργειες για την κατάργηση των προγραμμάτων.[19]

Ως απάντηση στα λογισμικά κατασκοπείας, μια μικρή βιομηχανία έχει ξεπηδήσει, που ασχολείται με λογισμικό anti-spyware . Προγραμματιστές και εταιρείες έχουν κυκλοφορήσει προϊόντα που έχουν σχεδιαστεί για την αφαίρεση ή τον αποκλεισμό με ασφαλή τρόπο των κατασκοπευτικών λογισμικών.[20] Η χρήση λογισμικού anti-spyware έχει γίνει απαραίτητο

[19] Edelman, B. (2005) *"Direct Revenue Deletes Competitors from Users' Disks"* Διαθέσιμο στο: https://www.benedelman.org/news-120704/7 [Ημερομηνία πρόσβασης: 3/1/2023]

[20] Προγραμματιστές και ορισμένες εταιρείες έχουν κυκλοφορήσει προϊόντα που έχουν σχεδιαστεί την αντιμετώπιση των κατασκοπευτικών λογισμικών. Μεγάλες εταιρείες προστασίας από ιούς όπως η Symantec, PC Tools, κ.ά. έχουν προσθέσει δυνατότητες προστασίας από λογισμικό υποκλοπής στα υπάρχοντα προϊόντα προστασίας από ιούς. Ωστόσο, οι εταιρείες προστασίας από ιούς εξέφρασαν απροθυμία να προσθέσουν λειτουργίες κατά των λογισμικών κατασκοπείας, επικαλούμενες αντιδράσεις από δημιουργούς κατασκοπευτικών λογισμικών.

στοιχείο πρακτικών ασφάλειας υπολογιστών, ειδικά για υπολογιστές που χρησιμοποιούν Microsoft Windows. Τα προγράμματα anti-spyware, όπως ονομάζονται, καταπολεμούν τα κατασκοπευτικά λογισμικά με δύο τρόπους: είτε παρέχοντας προστασία σε πραγματικό χρόνο μέσω σάρωσης όλων των απειλών που εντοπίζονται και αποκλεισμό του είτε καταργούν τα είδη υπάρχοντα λογισμικά που βρίσκονται εγκατεστημένα στη συσκευή.

Τα προγράμματα που χρησιμοποιούνται για την αντιμετώπιση των κατασκοπευτικών λογισμικών επιθεωρούν το μητρώο του λογισμικού του υπολογιστή, τα αρχεία του λειτουργικού συστήματος και αφαιρούν αρχεία και καταχωρήσεις που ταιριάζουν με μια λίστα αρχείων κατασκοπευτικών λογισμικών.[21] Η προστασία σε πραγματικό χρόνο από λογισμικό κατασκοπείας ομοιάζει με την προστασία έναντι των ιών σε πραγματικό χρόνο: το λογισμικό σαρώνει τα αρχεία δίσκου και αποκλείει τη δραστηριότητα στοιχείων που αντιπροσωπεύουν λογισμικό κατασκοπείας. Απαραίτητη κρίνεται η τήρηση βάσης δεδομένων απειλών, ενώ επειδή κυκλοφορούν συνέχεια νέα λογισμικά κατασκοπείας οι προγραμματιστές και κατασκευαστές anti-spyware προσπαθούν να τα ανακαλύπτουν, να τα αξιολογούν και να τα προσθέτουν στη λίστα των γνωστών κατασκοπευτικών λογισμικών. Ως εκ τούτου, αυτά τα προγράμματα είναι περιορισμένης χρησιμότητας όταν δε γίνονται τακτικές ενημερώσεις. Πρέπει όμως να τονιστεί ότι εάν ένα κατασκοπευτικό λογισμικό δεν είναι μπλοκαρισμένο και καταφέρει να εγκατασταθεί μόνο του, μπορεί να αντισταθεί στις προσπάθειες τερματισμού ή απεγκατάστασής του.[22] Έτσι, το ίδιο το λογισμικό μπορεί να μπλοκάρει την λειτουργία του λογισμικού ασφάλειας. Αξίζει να σημειωθεί ότι ορισμένα λογισμικά κατασκοπείας μπορούν ακόμα και να μπλοκάρουν τη

---

[21] «*Πληροφορίες σχετικά με Spyware (Λογισμικα Κατασκοπειας) και Τρόποι Αφαίρεσης*» Διαθέσιμο στο: https://ioys.gr/spyware-%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%AC-%CE%BA%CE%B1%CF%84%CE%B1%CF%83%CE%BA%CE%BF%CF%80%CE%B5%CE%AF%CE%B1%CF%82/ [Ημερομηνία πρόσβασης: 3/1/2023]

[22] Επιπλέον, ορισμένα κατασκοπευτικά λογισμικά λειτουργούν σε ζεύγη. Όταν ένα λογισμικό anti-spyware καταφέρει να μπλοκάρει ένα λογισμικό κατασκοπείας το ζεύγος του θα επέμβει για το διορθώσει.

διαδικασία σάρωσης, να κρύψουν τα αρχεία τους, ώστε να ελαχιστοποιήσουν τις πιθανότητες εντοπισμού κι ολοκληρωτικής αφαίρεσής τους.

Εκτός από τα γνωστά προγράμματα που χρησιμοποιούνται υπάρχουν και άλλοι τρόποι εντοπισμού και καταστολής των κατασκοπευτικών λογισμικών. Πολλοί χρήστες υπολογιστών ακολουθούν διάφορες πρακτικές εκτός από την εγκατάσταση αντίστοιχων προγραμμάτων π.χ. η εναλλαγή προγραμμάτων περιήγησης. Οι χρήστες επιλέγουν επίσης να εγκαταστήσουν τείχη προστασίας ή χρησιμοποιούν κινητό τηλέφωνο και υπολογιστή με φυσικό διακόπτη ή απομονωμένο ηλεκτρονικό διακόπτη που αποσυνδέει το μικρόφωνο ή και την κάμερα και τα διατηρεί σε αποσυνδεδεμένη θέση όποτε δεν χρησιμοποιούνται, περιορίζοντας τις πληροφορίες που μπορεί να συλλέξει το λογισμικό κατασκοπείας.

## ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ: ΧΡΗΣΕΙΣ ΚΑΤΑΣΚΟΠΕΥΤΙΚΩΝ ΛΟΓΙΣΜΙΚΩΝ

### 2.1. Ηλεκτρονικό έγκλημα και Κυβερνοασφάλεια

Τα κατασκοπευτικά λογισμικά συνδέονται με πληθώρα ηλεκτρονικών εγκλημάτων που είτε χρησιμοποιούν τον ηλεκτρονικό υπολογιστή ως μέσο για την εγκληματική πράξη είτε αποτελούν αυτά καθ' αυτά κυβερνοεγκλήματα. Η ανάπτυξη της τεχνολογίας κατέστησε δυνατή την τέλεση πολλών κλασσικών αδικημάτων με νέους τρόπους και σε νέες μορφές. Το ηλεκτρονικό έγκλημα, μια καινούργια κατηγορία εγκλημάτων, που προέκυψε από την εξέλιξη του ψηφιακού κόσμου, ορίζεται ως την εγκληματική πράξη, στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσης της πράξης.[23] Τα

[23] *Forester and Morrison 1994*. Η δίωξη ηλεκτρονικού εγκλήματος θεωρεί ως ηλεκτρονικό έγκλημα τις αξιόποινες εγκληματικές πράξεις, που τελούνται με την χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Μια άλλη προσέγγιση που επιχειρεί μια τριπλή εξειδίκευση ορίζει ως ηλεκτρονικό έγκλημα *τη νέα μορφή εγκλήματος, που διαπράττεται με την χρήση ηλεκτρονικών υπολογιστών ή την παραλλαγή των υπαρχόντων εγκλημάτων, που διαπράττονται με υπολογιστές ή την εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει με κάθε τρόπο ένας υπολογιστής.* Βλ. Αρκούδα, Ο. Διπλωματική Εργασία «*Απάτη μέσω ηλεκτρονικού υπολογιστή και συναφείς μορφές*

ηλεκτρονικά εγκλήματα μπορεί να τελούνται με τη χρήση ηλεκτρονικών υπολογιστών (computer crimes) ή μέσω του διαδικτύου (cyber crimes), τα λεγόμενα κυβερνοεγκλήματα, που αποτελούν ειδική κατηγορία των ηλεκτρονικών εγκλημάτων. Τα κατασκοπευτικά λογισμικά διευκόλυναν την τέλεση κοινών εγκλημάτων στον κυβερνοχώρο, όπως οι ηλεκτρονικές απάτες[24], η κλοπή ταυτότητας και αποτέλεσαν και τα ίδια μέσο για την δημιουργία νέων αδικημάτων, όπως η παρακώλυση λειτουργίας πληροφοριακών συστημάτων, εγκλήματα κατά της ασφάλειας των τηλεπικοινωνιών κ.ά.[25]

Η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ σε έρευνά της υπολόγισε ότι 27,3 εκατομμύρια Αμερικανοί έχουν πέσει θύματα κλοπής ταυτότητας. Γνωστό παράδειγμα σύνδεσης των κατασκοπευτικών λογισμικών με το έγκλημα της κλοπής ταυτότητας αποτελεί η υπόθεση του κατασκοπευτικού λογισμικού "CoolWebSearch".[26] Συγκεκριμένα, ερευνητές από την εταιρεία λογισμικού ασφαλείας Sunbelt Software ανακάλυψαν ότι οι κατασκευαστές του κατασκοπευτικού λογισμικού CoolWebSearch χρησιμοποίησαν το συγκεκριμένο λογισμικό για να διαβιβάσουν συνομιλίες, ονόματα χρηστών , κωδικούς πρόσβασης , τραπεζικές πληροφορίες και άλλα προσωπικά δεδομένα.

Τα λογισμικά κατασκοπείας συνδέονται άμεσα με μια σειρά κυβερνοεπιθέσεων και κυβερνοαπειλών στον κυβερνοχώρο. Το λογισμικό μπορεί να μολύνει ένα σύστημα και να

---

*εγκληματικότητας*», Νομική Σχολή ΑΠΘ, Θεσσαλονίκη 2017, σελ. 9. Και Αγγελής, Ι. «*Διαδίκτυο και ποινικό δίκαιο*», Ποινικά Χρονικά, 2000.

[24] Μερικοί κατασκευαστές λογισμικών κατασκοπείας αναφέρουν πέραν των γνωστών απατών μια μορφή απάτης με κλικ την απάτη των συνεργατών. Αυτή η μορφή εκτρέπει την πληρωμή των εσόδων από το μάρκετινγκ θυγατρικών εταιριών από τη νόμιμη θυγατρική στον προμηθευτή λογισμικού κατασκοπείας. Ο διαχειριστής του λογισμικού κατασκοπείας είναι το μόνο μέρος που κερδίζει από αυτό. Οι επιλογές του χρήστη ματαιώνονται, μια νόμιμη θυγατρική χάνει έσοδα, η φήμη των δικτύων βλάπτεται και οι πωλητές βλάπτονται από την υποχρέωση να πληρώσουν τα έσοδα της θυγατρικής σε μια «θυγατρική» που δεν είναι συμβαλλόμενο μέρος . Οι κινητές συσκευές, όπως τα τηλέφωνα μπορεί επίσης να είναι ευάλωτες σε λογισμικό φόρτισης , το οποίο χειραγωγεί τους χρήστες σε παράνομες χρεώσεις κινητής τηλεφωνίας.

[25] Βλ. αναλυτικά παρ. 3.5

[26] Ars Technica Ecker, C. (2005) *"Massive spyware-based identity theft ring uncovered"*. Διαθέσιμο στο: https://arstechnica.com/uncategorized/2005/08/5175/ [Ημερομηνία πρόσβασης: 3/1/2023]

επιτρέψει την πρόσβαση σε αυτό παρασκηνιακά και κρυφά ή να διαβιβάσει τα δεδομένα που συλλέγει μέσα από την παρακολούθηση σε hackers με σκοπό την κυβερνοεπίθεση, την κυβερνοαπειλή ή ακόμα και τον κυβερνοπόλεμο ακόμα και σε υποδομές ζωτικής σημασίας Πολλά κατασκοπευτικά λογισμικά τείνουν να παρέχουν απομακρυσμένη πρόσβαση του συστήματος σε hackers, προφανώς χωρίς την συγκατάθεση του χρήστη.

Κυβερνοαπειλή είναι κάθε κακόβουλη ενέργεια που έχει στόχο τη ζημία ή την κλοπή δεδομένων ή τη διατάραξη της ψηφιακής ασφάλειας γενικότερα. Μια κυβερνοαπειλή μπορεί να περιλαμβάνει επίθεση με κακόβουλα λογισμικά σε υπολογιστές, παραβιάσεις δεδομένων, επιθέσεις που αφορούν την άρνηση υπηρεσιών και άλλες μορφές επίθεσης.[27] Επίσης, μια κυβερνοαπειλή ενδέχεται να σχετίζεται με κυβερνοεπίθεση που έχει στόχο την πρόσβαση χωρίς προηγούμενη εξουσιοδότηση σε δεδομένα, τη βλάβη, τη διατάραξη ή την κλοπή πληροφοριών που αφορούν στοιχεία, λογισμικό υπολογιστών, πνευματική ιδιοκτησία ή οποιαδήποτε μορφή δεδομένα. Μάλιστα, μια κυβερνοαπειλή μπορεί να πραγματοποιείται είτε από χρήστες που ενεργούν από το χώρο ενός οργανισμού, ή από άγνωστους χρήστες που ενεργούν από απομακρυσμένους προορισμούς.[28]

Οι κυβερνοεπιθέσεις μπορεί να προέρχονται από διάφορους παράγοντες. Συγκεκριμένα, οι κυβερνοεπιθέσεις μπορεί να προέρχονται από εχθρικά κράτη,[29] τα οποία συνιστούν το

---

[27] Βλ. Tunggal, A. T. UpGuard (2021) *'What is a Cyber Threat'?* Διαθέσιμο στο: https://www.upguard.com/blog/cyber-threat Πρόσβαση στις 10-12-2021 [Ημερομηνία πρόσβασης: 2/1/2023]

[28] Βλ. Tunggal, A. T. ό.π

[29]Οι κυβερνοεπιθέσεις διαφέρουν σε σχέση με τον κυβερνοπόλεμο στο γεγονός ότι στον κυβερνοπολέμο υπάρχει η εμπλοκή κράτους το οποίο εξαπολύει μια επίθεση, η οποία επίθεση πρέπει να έχει θύματα, προσομοιάζοντας έτσι με πραγματικό πόλεμο. Τέτοιες επιθέσεις μπορεί να γίνουν σε κρίσιμες υποδομές όπως π.χ. σε νοσοκομεία ή σε μέσα μαζικής μεταφοράς. Η διάκριση μεταξύ κυβερνοπολέμου και κυβερνοεπίθεσης δεν είναι πάντα διακριτή. Τα κράτη και οι κυβερνήσεις ενδέχεται να χρησιμοποιούν κατασκοπευτικά λογισμικά για να επιτεθούν σε αντίπαλα κράτη, κατά τη διάρκεια πολέμου ή για να προκαλέσουν υβριδικό πόλεμο καταστρέφοντας υποδομές ζωτικής σημασίας, όπως συστήματα ασφαλείας. Στην τελευταία περίπτωση η ανακάλυψη του κράτους-θύτη είναι ιδιαίτερα δυσχερής. Βλ. Πιπύρος, Κ., Μήτρου, Λ. «*Κυβερνοεπίθεση ή Κυβερνοπόλεμος;*» ΔιΜΕΕ τ. 2/2018 Έτος 15ο

μεγαλύτερο κίνδυνο, εξαιτίας της ικανότητάς τους να χρησιμοποιούν με αρκετά αποτελεσματικό τρόπο τα μέσα της τεχνολογίας εναντίον δύσκολων στόχων όπως απόρρητα δίκτυα, υποδομές ζωτικής σημασίας. Ακόμη, τρομοκρατικές ομάδες εξαπολύουν κυβερνοεπιθέσεις εναντίον κρατικών συμφερόντων, οι οποίες θα ενταθούν καθώς αυτές οι ομάδες ενισχύονται με πιο καταρτισμένα τεχνολογικά άτομα. Ιδιαίτερη μορφή κυβερνοεπιθέσεων είναι εκείνες που πραγματοποιούνται από εταιρικούς κατασκόπους και οργανωμένες εγκληματικές οργανώσεις μέσω της βιομηχανικής κατασκοπείας, προκειμένου να καρπωθούν εμπορικά μυστικά ή να διεξάγουν νομισματική κλοπή σε μεγάλη κλίμακα. Επιπλέον, οι κυβερνοεπιθέσεις μπορεί να προέρχονται από hackers, οι οποίοι εκμεταλλεύονται ελαττώματα και ευπάθειες των συστημάτων, ώστε να αποκτήσουν πρόσβαση σε δεδομένα, χωρίς προηγούμενη εξουσιοδότηση.[30]

Η Κυβερνοασφάλεια, ήτοι η προστασία των συστημάτων δικτύου και των υπολογιστών καθώς και των δεδομένων από περιστατικά κυβερνοεπιθέσεων, περιστατικά για τα οποία μπορεί να είναι υπεύθυνα λογισμικά κατασκοπείας είναι πολύ σημαντική και αντιμετωπίζεται ήδη με σοβαρότητα από πολλά κράτη. Ειδικότερα, ο όρος της Κυβερνοασφάλειας περιλαμβάνει κάθε μέτρο που λαμβάνεται για τη διασφάλιση της προστασίας των πληροφοριακών συστημάτων και των χρηστών τους έναντι μη αδειοδοτημένης προσέγγισης, επιθέσεων και βλάβης, έτσι ώστε να διασφαλίζεται ότι τηρείται η «εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα» των δεδομένων.[31] Με την Κυβερνοασφάλεια προλαμβάνονται και εντοπίζονται συμβάντα που σχετίζονται με την ασφάλεια των συστημάτων, ενώ προβλέπονται και τρόποι αντίδρασης καθώς και η πορεία ανάκαμψης έπειτα ένα τέτοιο περιστατικό. Στα συμβάντα αυτά, τα οποία ενδέχεται να είναι είτε σκόπιμα είτε όχι, συγκαταλέγονται, π.χ. η τυχαία διάδοση πληροφοριών, οι επιθέσεις εναντίον επιχειρήσεων και σημαντικών οργανώσεων, η κλοπή προσωπικών δεδομένων, ή ακόμη και η παρεμβολή σε διαδικασίες δημοκρατικού χαρακτήρα όπως εκλογές. Τα

[30] Μπαλτά, Ι. Πανεπιστήμιο Πειραιά 2021-2022 ΜΔΕ *«Η κυβερνοασφάλεια στη σύγχρονη ψηφιακή εποχή»* σελ. 13 επ.

[31] Βλ. Ευρωπαϊκό Ελεγκτικό Συνέδριο (2019) Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια. Λουξεμβούργο σελ. 8 Διαθέσιμο στο: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf [Ημερομηνία Πρόσβασης 3/1/2023]

αποτελέσματα αυτών των συμβάντων μπορούν να βλάψουν με ποικίλους τρόπους πρόσωπα, φορείς και κοινότητες.[32]

Στην Ε.Ε, ο όρος της Κυβερνοασφάλειας δε συνδέεται μόνο με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, αλλά καλύπτει και κάθε παράνομη ενέργεια που συντελείται μέσω της τεχνολογίας στο χώρο του διαδικτύου. Έτσι, στην Κυβερνοασφάλεια μπορεί να εμπίπτουν κυβερνοεγκλήματα όπως η μόλυνση των υπολογιστών με ιούς ή η απάτη στα μέσα χρηματικών καταβολών, εκτός από τις πληρωμές με μετρητά και να έχουν στόχο όχι μόνο τα συστήματα αλλά και το περιεχόμενο, όπως και η διάδοση υλικού σεξουαλικού περιεχομένου ανηλίκων στο διαδίκτυο. Ακόμη, αντικείμενό της μπορεί να είναι ενέργειες παραπληροφόρησης μέσω διαδικτύου και εικασίες για παρεμβολές στις εκλογικές διαδικασίες.[33]

Τα κατασκοπευτικά λογισμικά βάλλουν επίσης κατά της ασφάλειας των πληροφοριών, αφού στην ουσία σκοπός τους είναι να υποκλέψουν δεδομένα των χρηστών. Ως ασφάλεια των πληροφοριών ορίζεται η διαφύλαξη των πληροφοριών ενός συστήματος πληροφοριών, από ενδεχόμενες βλάβες που μπορεί να μειώσουν την αξία τους. Επιπλέον, η ασφάλεια των πληροφοριών στοχεύει στη χορήγηση φερέγγυων πληροφοριών, στις οποίες οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση, όποτε είναι απαραίτητο.[34] Επιπλέον, η διαφύλαξη των δεδομένων στηρίζεται σε βασικά χαρακτηριστικά της ασφάλειας πληροφοριών, όπως την εμπιστευτικότητα, που σχετίζεται με τη διαφύλαξη της πληροφορίας από την αποκάλυψή της χωρίς εξουσιοδότηση, την ακεραιότητα που σχετίζεται με τη διαφύλαξη της πληροφορίας από πιθανή αλλαγή, μεταβολή ή διαγραφή της, χωρίς προηγούμενη εξουσιοδότηση, τη διαθεσιμότητα, που σχετίζεται με την προστασία της εξουσιοδοτημένης πρόσβασης, είτε για να γίνει κοινολόγηση είτε τροποποίηση, στην πληροφορία, χωρίς εμπόδια.[35]

---

[32] ibid

[33] Ibid

[34] Βλ. Μαυρίδης, Ι. (2015) «Ασφάλεια Πληροφοριών στο Διαδίκτυο.» Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, σελ. 16

[35] Ibid σελ. 17-18

### 2.2. Εμπόριο και Διαφήμιση

Όπως προαναφέρθηκε[36] τα κατασκοπευτικά λογισμικά εμφανίζουν μεγάλο όγκο παραπλανητικών αναδυόμενων παραθύρων διαφημίσεων. Αυτή η συμπεριφορά σχετίζεται με προγράμματα τύπου adware, ενώ άλλοι τύποι κατασκοπευτικών λογισμικών μπορεί να υποκλέπτουν, καταγράφουν, προωθούν σε τρίτους πληροφορίες σχετικές με τις διαδικτυακές προτιμήσεις και δραστηριότητες των χρηστών, όπως ποιους ιστότοπους, κάθε πότε και για πόσο επισκέπτονται οι χρήστες, ποιες διαφημίσεις επιλέγουν να δουν, ποια κριτήρια εισάγουν στις διαδικτυακές αναζητήσεις, κ.λπ. Σε αυτό το σημείο θα πρέπει, ωστόσο να γίνει ένας σημαντικός διαχωρισμός μεταξύ των παράνομων κατασκοπευτικών λογισμικών που χρησιμοποιούνται για διαφήμιση και των νόμιμων προγραμμάτων διαδικτυακής διαφήμισης (marketing) που μπορούν να παρακολουθούν προσωπικά δεδομένα, αλλά δε το κάνουν. Στην ουσία, αυτού του είδους τα προγράμματα συλλέγουν προσωπικά δεδομένα για διαφημιστικούς σκοπούς. Σε γενικές γραμμές, τα νόμιμα διαφημιστικά προγράμματα κινούνται εντός του πλαισίου της νομιμότητας και δεν παραβιάζουν το απόρρητο των προσωπικών δεδομένων.

Η χρήση των ιχνηλατών στο διαδίκτυο, εάν και δεν εμφανίστηκε πρόσφατα, αποτελεί τελευταία ένα σημαντικό ζήτημα, το οποίο τυγχάνει να έχει τεχνολογικές, νομικές αλλά και εμπορικές προεκτάσεις.[37] Αφορμή για να ανοιχτεί το θέμα αυτό ήταν βέβαια η ψήφιση του ΓΚΠΔ χωρίς ωστόσο οι ιχνηλάτες να διέπονται αποκλειστικά από τον αυτόν. Η ΑΠΔΠΧ ορίζει τα cookies ως εξής: *«Τα cookies είναι μικρά αρχεία κειμένου με πληροφορίες, τα οποία αποθηκεύονται από τον διακομιστή (server) ενός ιστοτόπου στην τερματική συσκευή (υπολογιστής, κινητό τηλέφωνο κλπ.) ενός επισκέπτη/χρήστη κατά την πλοήγηση σε αυτόν. Ο ιστότοπος ανακτά τις εν λόγω πληροφορίες σε κάθε επίσκεψη, προκειμένου να προσφέρει σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι*

[36] Βλ. παρ. 1.1

[37] Καρκατζούνης, Β. *«Google Analytics και προστασία προσωπικών δεδομένων Το ψήφισμα της Συνόδου των Εποπτικών αρχών προστασίας προσωπικών δεδομένων της Γερμανίας (Datenschutzkonferenz της 12.5.2020)»*, Επιθεώρηση Δικαίου Πληροφορικής, Τ. 1, 2020. Διαθέσιμο στο: http://ejournals.lib.auth.gr/infolawj/ [Ημερομηνία πρόσβασης 3/1/2023]

*προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει σε αυτή (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, κ.λπ.)».*[38]

Ωστόσο, παρά το γεγονός ότι ο ως άνω ορισμός φαίνεται επαρκής, πιο σωστό θα ήταν να προσμετρώνται πάντα οι διαρκείς εξελίξεις της τεχνολογίας και των χρησιμοποιούμενων κάθε φορά μεθόδων στο διαδίκτυο αλλά και μεθόδων παρακολούθησης.[39]Για παράδειγμα, αρχικά, στον ορισμό της ΑΠΔΠΧ ως τερματική συσκευή αποθήκευσης θεωρούταν μόνο ο υπολογιστής, ενώ, εν συνεχεία, προστέθηκε και το κινητό τηλέφωνο, αφού πλέον ο αριθμός των χρηστών που περιηγούνται στο διαδίκτυο μέσω του κινητού τους τηλεφώνου είναι εξαιρετικά μεγάλος. Στη συνέχεια, είναι εύλογο να προστεθούν κι άλλα τεχνολογικά επιτεύγματα, τα οποία αυτή την στιγμή πιθανότατα να αγνοούμε. Με τη χρήση των cookies, είναι δυνατό να εντοπίζεται η συσκευή του χρήστη, να καταγράφεται η κίνησή του κ.ά. ανάλογα με το εκάστοτε εργαλείο ανάλυσης δεδομένων που χρησιμοποιεί η ιστοσελίδα την οποία επισκέπτεται ο χρήστης. Η συλλογή τους γίνεται ύστερα από τη ρητή συγκατάθεση του χρήστη και κάθε φορά που ο χρήστης επισκέπτεται την ίδια ιστοσελίδα, το εκάστοτε λογισμικό «θυμάται» τις προτιμήσεις του χρήστη και προσαρμόζει το περιεχόμενο που εμφανίζονται εξατομικευμένα για τον κάθε χρήστη. [40]

Από τα παραπάνω καθίσταται σαφές ότι η χρήση των ιχνηλατών και δη των cookies αποτελεί μια γκρίζα ζώνη, ως προς το αν θεωρούνται κατασκοπευτικά λογισμικά και κατά πόσο είναι επίσης νόμιμα, την στιγμή που δεν υπάρχει και σαφής νομοθετική ρύθμιση. Τα tracking cookies[41] ενδεχομένως να αποτελούν κατασκοπευτικά λογισμικά, αλλά εξαρτάται από το είδος τους, καθώς δεν είναι όλα επιβλαβή και δεν παραβιάζουν όλα το απόρρητο των

[38] Διαθέσιμο στο : https://www.dpa.gr/index.php/el/cookies/plirofories/whatis_cookies [Ημερομηνία πρόσβασης: 3/1/2023]

[39] Καρκατζούνης, Β. «*Cookies και προστασία δεδομένων προσωπικού χαρακτήρα*», ΔΙΤΕ, 2/2019, σελ. 172.

[40] Παπαντώνη, Η. ΜΔΕ : «*Καθ' οδόν προς την υιοθέτηση του e-Privacy. Η προς ρύθμιση ύλη και τα διακυβεύματα του νέου κανονιστικού πλαισίου*» Πανεπιστήμιο Πειραιά, Πειραιάς 2022 σελ. 34

[41] Αποτελούν μια ειδική κατηγορία cookies που μπορεί να μοιράζονται από παραπάνω από έναν ιστότοπο. Χρησιμοποιούνται κυρίως για marketing και διαφημιστικούς σκοπούς, αλλά ακριβώς επειδή συλλέγουν πολύ προσωπικές πληροφορίες για τον χρήστη, όπως το ιστορικό πλοήγησης μπορεί εύκολα να θεωρηθούν καταχρηστικά.

προσωπικών δεδομένων. Τα First-party cookies[42] επίσης δεν είναι απαραίτητα λογισμικά κατασκοπείας. Πολλοί ιστότοποι μπορεί να ζητήσουν να αποδεχτεί ο χρήστης όλα τα cookies στην πρώτη επίσκεψη της ιστοσελίδας.[43] Αυτού του είδους τα cookies βοηθούν την ιστοσελίδα να τακτοποιήσει τη συχνότητα των επισκέψεων των χρηστών και συμβάλλουν στην απομνημόνευση των κωδικών πρόσβασης κ.ά, προσωποποιώντας την χρήση. Σε αντίθεση με τα προηγούμενα τα Third-party cookies συνήθως αποτελούν κατασκοπευτικά λογισμικά. Προέρχονται από ιστοσελίδες ή εξωτερικούς διακομιστές (servers), που δεν έχουν σχέση με την ιστοσελίδα που επισκέπτεται ο χρήστης και συχνά επιτρέπουν σε διαφημιστές να παρακολουθούν τις online δραστηριότητες των χρηστών ή επιτρέπουν σε εταιρείες ανάλυσης να συλλέγουν και να πωλούν τα δεδομένα των χρηστών.[44]

### 2.3. Οι παρακολουθήσεις μέσω των λογισμικών κατασκοπείας Predator και Pegasus

Κατασκοπευτικά λογισμικά εγκαθίστανται σε κινητές συσκευές, σε τηλέφωνα και υπολογιστές για την παρακολούθηση προσώπων του δημόσιου ή του ιδιωτικού βίο. Πολλές φορές η παρακολούθηση μέσω της χρήσης λογισμικών κατασκοπείας γίνεται υπό τον μανδύα της πρόληψης εγκλημάτων.

Για παράδειγμα το 2010 η υπόθεση WebcamGate,[45] είχε συγκλονίσει τη Φιλαδέλφεια των ΗΠΑ καθώς δύο λύκεια κατηγορήθηκαν ότι κατασκόπευαν κρυφά ανήλικους μαθητές, θέτοντας σε λειτουργία εξ αποστάσεως κάμερες ενσωματωμένες σε φορητούς υπολογιστές

---

[42] Αυτού του είδους τα cookies αυτομάτως αποθηκεύονται από τον ιστότοπο που επισκέπτεται ο χρήστης και συλλέγουν γενικές πληροφορίες, όπως την προτίμηση της γλώσσας.

[43] Χοντζόπουλος, Ι., Κακαβούλης, Κ. Homo Digitalis (2018): *«Τι είναι τα cookies; »*. Διαθέσιμο στο: https://www.homodigitalis.gr/posts/3079 [Ημερομηνία πρόσβασης: 3/1/2023]

[44] Τα προγράμματα προστασίας από κατασκοπευτικά λογισμικά συχνά αναφέρουν τα cookies HTTP των διαφημιστών ιστού , τα μικρά αρχεία κειμένου που παρακολουθούν τη δραστηριότητα περιήγησης, ως λογισμικό κατασκοπείας.

[45] Stanglin, D. Ondeadline (2010) "School district accused of spying on kids via laptop webcams". Διαθέσιμο στο: https://web.archive.org/web/20120913050816/http://content.usatoday.com/communities/ondeadline/post/2010/02/school-district-accused-of-issuing-webcam-laptops-to-spy-on-students/1 [Ημερομηνία πρόσβασης: 3/1/2023]

σχολικής λειτουργίας που χρησιμοποιούσαν οι μαθητές στο σπίτι. Τα σχολεία εγκατέστησαν στον υπολογιστή κάθε μαθητή το λογισμικό παρακολούθησης απομακρυσμένης ενεργοποίησης του LANrev, το οποίο περιελάμβανε το λογισμικό κατασκοπείας "TheftTrack". Ενώ το λογισμικό TheftTrack δεν ήταν ενεργοποιημένο από προεπιλογή, το πρόγραμμα επέτρεψε στη σχολική μονάδα να επιλέξει να το ενεργοποιήσει και να επιλέξει ποιες από τις δυνατότητες επιτήρησης ήθελε να ενεργοποιήσει το σχολείο. Με το TheftTrack τα σχολεία μπορούσαν να ενεργοποιήσουν κρυφά την κάμερα, που ήταν ενσωματωμένη στον υπολογιστή του κάθε μαθητή, να τραβήξουν κρυφά φωτογραφίες μέσω της κάμερας και να στείλουν τις φωτογραφίες στον διακομιστή του σχολείου. Το λογισμικό LANrev απενεργοποίησε τις κάμερες για όλες τις άλλες χρήσεις (π.χ. οι μαθητές δεν μπορούσαν να χρησιμοποιήσουν τις βιντεοκλήσεις) κι έτσι οι περισσότεροι μαθητές νόμιζαν ότι οι κάμερές τους απλά δεν λειτουργούσαν καθόλου. Εκτός από την παρακολούθηση της κάμερας, με το TheftTrack οι σχολικοί λειτουργοί τράβηξαν στιγμιότυπα οθόνης του υπολογιστή και τα έστειλαν στον διακομιστή του σχολείου αλλά και στιγμιότυπα άμεσων μηνυμάτων, περιήγησης στο διαδίκτυο, μουσικών playlist και γραπτών συνθέσεων. Τα σχολεία παραδέχτηκαν ότι τράβηξαν πάνω από 66.000 στιγμιότυπα ιστού και στιγμιότυπα οθόνης, συμπεριλαμβανομένων λήψεων μέσω web κάμερας μαθητών στα δωμάτιά τους.

Το καλοκαίρι του 2022 μια σειρά καταγγελιών γνωστών πολιτικών προσώπων και δημοσιογραφικών κύκλων σχετικά με παρακολουθήσεις τους από την τότε κυβέρνηση ήρθε στο προσκήνιο στην Ελλάδα με αφορμή δύο λογισμικά κατασκοπείας, το Pegasus και το Predator. Η διακρίβωση του παράνομου χαρακτήρα των τηλεφωνικών παρακολουθήσεων βρίσκεται έως και σήμερα στα χέρια της ελληνικής δικαιοσύνης. Ωστόσο, το σκάνδαλο ήταν τόσο μεγάλο λόγω της ιδιότητας των προσώπων που φέρονται να παρακολουθούνται, που στην κοινή γνώμη ταυτίστηκε με το ελληνικό Watergate.

Οι παρακολουθήσεις σημαίνοντος αντίπαλου πολιτικού προσώπου του Κυβερνώντος Κόμματος και άλλων πολιτικών στελεχών αλλά και δημοσιογράφων μέσω της ΕΥΠ το 2020, η οποία με βάση τον ισχύοντα νόμο[46] είχε περάσει στον έλεγχο του ίδιου του Πρωθυπουργού

[46] Ν. 4622/2019

είναι μια υπόθεση που ακόμα εκκρεμεί στην Ελλάδα.[47] Η όλη παρακολούθηση φαίνεται ότι έγινε μέσω των συστημάτων της ΕΥΠ και με την χρήση λογισμικών κατασκοπείας, που είχαν εγκατασταθεί στα τηλέφωνα των θυμάτων. Όταν έγινε αντιληπτή η παρακολούθηση των τηλεφώνων των θυμάτων τα ίδια τα θύματα ζήτησαν από την ΕΥΠ την άμεση ενημέρωσή τους, όμως η αλλαγή του νόμου από την κυβέρνηση δεν επέτρεπε την πληροφόρησή τους.

Το Μάρτιο του 2021 υπερψηφίστηκε στη Βουλή των Ελλήνων μία τροπολογία του Υπουργού Δικαιοσύνης σε κυβερνητικό νομοσχέδιο με την οποία καταργήθηκε με αναδρομική ισχύ η δυνατότητα πολιτών να πληροφορούνται από την ΑΔΑΕ την άρση του απορρήτου των επικοινωνιών τους από την ΕΥΠ, εφόσον η παρακολούθησή τους γινόταν για λόγους εθνικής ασφάλειας.

Για τις παρακολουθήσεις που φέρονται να έγιναν στα τηλέφωνα πολιτικών και δημοσιογράφων χρησιμοποιήθηκε το λογισμικό κατασκοπείας Predator, το οποίο είχε ήδη κατακριθεί για την χρήση του. Συγκεκριμένα ήδη το 2018 εισήχθη στην Κύπρο ένα βαν που δηλώθηκε ως μετεωρολογικός εξοπλισμός, αλλά χρησιμοποιούνταν για την παρακολούθηση έξυπνων τηλεφώνων.[48] Η δραστηριότητα επεκτάθηκε και στην Ελλάδα, ενώ στην εταιρία που προωθούσε το λογισμικό επιβλήθηκε το 2021 πρόστιμο για την παράνομη χρήση του βαν και το 2022 καταδικάστηκε για παραβιάσεις της ιδιωτικότητας και των προσωπικών δεδομένων.[49] Η ίδια εταιρεία στη συνέχεια συνεργάστηκε με την εταιρεία Cytrox που εμπορευόταν το λογισμικό Predator.[50] Στην Ελλάδα το λογισμικό αυτό

---

[47] Η Καθημερινή (2019): *«Η αρμοδιότητα της ΕΥΠ περνάει στον πρωθυπουργό».* Διαθέσιμο στο: https://www.kathimerini.gr/politics/1033159/i-armodiotita-tis-eyp-pernaei-ston-prothypoyrgo/ [Ημερομηνία πρόσβασης: 3/1/2023]

[48] Τέλλογλου, Τ., Τριανταφύλλου, Ε. Inside story (2022*): «Predator: Ο «κατάσκοπος» που ήρθε από την Κύπρο».* Διαθέσιμο στο: https://insidestory.gr/article/i-kypros-kai-o-tal-dilian [Ημερομηνία πρόσβασης: 4/1/2023].

[49] Benjakob, O. Inside story (2022). «*Η Intellexa παρακάμπτει τους ισραηλινούς κανόνες μέσω Αθήνας».* Διαθέσιμο στο: https://insidestory.gr/article/prosohi-den-dimosieyetaiwifi-aerodromion-kai-hakarisma-kiniton-tilefonon-i-skoteini-pleyra [Ημερομηνία πρόσβασης: 4/1/2023]

[50] Τριανταφύλλου, Ε. Inside story (2022). «*Το νέο λογισμικό κατασκοπίας Predator και οι δουλειές στην Ελλάδα».* Διαθέσιμο στο: https://insidestory.gr/article/neo-logismiko-kataskopeias-predator-kai-oi-doyleies-stin-ellada [Ημερομηνία πρόσβασης: 4/1/2023]

διακινήθηκε το Μάρτιο του 2020, όταν και ιδρύθηκε η εταιρεία Intellexa, μια εταιρεία με στενές σχέσεις με την ανωτέρω, λόγω της συμμέτοχής σε αυτήν κοινών μετόχων.[51] Ήδη η ΑΠΔΠΧ στην απόφασή της 2/2023 επέβαλε πρόστιμο στην εταιρεία για μη συμμόρφωση με το άρθρο 31 του ΓΚΠΔ, ήτοι σε περίπτωση ελέγχου από την Αρχή όταν υπάρχει κάποια καταγγελία, ο Υπεύθυνος Επεξεργασίας οφείλει να συνεργάζεται μαζί με την Αρχή και να παρέχει σε αυτήν όλα τα απαραίτητα στοιχεία. Σε έλεγχο που διενεργήθηκε από την ΑΠΔΠΧ στην εταιρεία, κατόπιν καταγγελίας για εγκατάσταση παράνομου λογισμικού παρακολούθησης κινητού τηλεφώνου η εταιρεία δεν παρείχε επαρκή στοιχεία στην Αρχή.[52]

Τον Ιούνιο του 2020 μετά από άδεια της αρμόδιας εισαγγελέως η ΕΥΠ αποφασίστηκε η παρακολούθηση του κινητού ενός Έλληνα δημοσιογράφου για λόγους εθνικής ασφάλειας, αρχικά για δύο μήνες και κατόπιν παράτασης μέχρι τον Οκτώβριο. Κατόπιν, προβλημάτων στη λειτουργία του κινητού του και έπειτα από πληροφόρηση από συναδέλφους κατήγγειλε την παρακολούθησή του στην ΑΔΑΕ, αιτούμενος να πληροφορηθεί αν παρακολουθείται. Εν συνεχεία, η ΕΥΠ ζήτησε την παύση της άρσης. Η ΑΔΑΕ με τη σειρά της ζήτησε από την ΕΥΠ να απαντήσει στο ερώτημα εάν με την ενημέρωση του δημοσιογράφου θα διακυβευόταν ο σκοπός της άρσης του απορρήτου. Η παρακολούθηση του κινητού του δημοσιογράφου διαπιστώθηκε ότι έγινε μέσω του λογισμικού Predator.[53]

---

[51] Τριανταφύλλου, Ε., Τέλλογλου Τ. Inside story (2022). «*Predatorgate: Ο δεύτερος μέτοχος της Intellexa AE*». Διαθέσιμο στο: https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae [Ημερομηνία πρόσβασης: 4/1/2023]

[52] ΑΠΔΠΧ 2/2023 διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2023-01/2_2023%20anonym.pdf [Ημερομηνία πρόσβασης: 14/2/2023]

[53] Ο δημοσιογράφος ανακάλυψε την παρακολούθηση των επικοινωνιών του μέσω του λογισμικού Predator, από το οποίο είχε μολύνει το κινητό του τηλέφωνο, έπειτα από έλεγχο που διενήργησε για λογαριασμό του, το "Citizen Lab" του Πανεπιστημίου του Τορόντο. Η ανάλυση του "Citizen Lab" εντόπισε την παρουσία του Predator, ενώ δεν απέκλεισε και το ενδεχόμενο και άλλων μολύνσεων. Ο δημοσιογράφος προχώρησε και σε επίσημο αίτημα προς την ΑΔΑΕ για να διερευνήσει τις διαπιστώσεις. Λίγες μέρες μετά τη δημοσίευση του ρεπορτάζ που αποδείκνυε την παρακολούθηση του δημοσιογράφου από την ΕΥΠ, διατάχθηκε η διενέργεια προκαταρκτικής εξέτασης για να ερευνηθεί πιθανή παραβίαση τηλεφωνικού απορρήτου.

Το καλοκαίρι του 2022 ο πρόεδρος αντίπαλου πολιτικού κόμματος της Κυβέρνησης, κατέθεσε μήνυση στον Άρειο Πάγο για παραβίαση προσωπικών δεδομένων, καθώς στο κινητό του τηλέφωνο εντοπίστηκε η παρουσία συνδέσμου που σχετίζεται με το παράνομο λογισμικό Predator. Ο εν λόγω πολιτικός είχε λάβει στο κινητό του τηλέφωνο ένα μήνυμα που τον προσκαλούσε να πατήσει έναν σύνδεσμο, τον οποίο και δεν πάτησε, διότι έτσι απέτρεψε την εγκατάσταση του λογισμικού Predator. Παρόμοιος ήταν και ο τρόπος των παρακολουθήσεων των υπόλοιπων προσώπων.

Ο αντίκτυπος ήταν τεράστιος. Η Κυβέρνηση δήλωσε άγνοια επί των παρακολουθήσεων, ενώ αμέσως δημοσιεύθηκε πράξη νομοθετικού περιεχομένου με την οποία καθιερώθηκε η εποπτεία της ΕΥΠ από δύο εισαγγελείς και ακρόαση του διοικητή της από την Επιτροπή θεσμών και διαφάνειας.[54] Παράλληλα, συστάθηκε εξεταστική επιτροπή και η υπόθεση εκκρεμεί έως σήμερα.

Το λογισμικό Pegasus[55] είναι κι αυτό ένα κατασκοπευτικό λογισμικό, που χρησιμοποιείται για την κατασκοπεία τηλεφώνων, χωρίς τη συναίνεση του χρήστη. Το λογισμικό αυτό στοχεύει όπως και το λογισμικό Predator στο να πείσει τον χρήστη να επιλέξει τον σύνδεσμο[56] που θα εγκαταστήσει το λογισμικό στη συσκευή, παραπλανώντας τον χρήστη. Ο σύνδεσμος αυτός μπορεί να αποσταλεί στον χρήστη μέσω μηνύματος και να φαίνεται απόλυτα φυσιολογικός, όμως επιλέγοντας τον σύνδεσμο, το λογισμικό «επιτίθεται» στο σύστημα ασφαλείας της συσκευής και εγκαθίσταται χωρίς τη γνώση ή την άδεια του χρήστη. Μόλις εγκατασταθεί ξεκινά να εκτελεί τις εντολές του χειριστή του και κοινολογεί

---

[54] ΕφτΚ Τεύχος Α' 152/09.08.2022 ΠΝΠ «*Επείγουσες διατάξεις για την ενίσχυση της ακεραιότητας στη λειτουργία της Εθνικής Υπηρεσίας Πληροφοριών*». Διαθέσιμο στο: https://www.in.gr/wp-content/uploads/2022/08/a4ba248e-4a90-4560-84e1-4c315b023853.pdf [Ημερομηνία πρόσβασης: 4/1/2023]

[55] Chawla, A. (2021) *"Pegasus Spyware: A Privacy Killer"*. Διαθέσιμο στο SSRN: https://ssrn.com/abstract=3890657 [Ημερομηνία πρόσβασης: 4/1/2023]. Το λογισμικό αυτό μπορεί να εγκατασταθεί εξ αποστάσεως σε iOS και Android λειτουργικά συστήματα. Αναπτύχθηκε από την ισραηλινή εταιρεία NSO Group η οποία πουλάει το λογισμικά σε κυβερνήσεις για νόμιμες παρακολουθήσεις, με σκοπό την αντιμετώπιση της τρομοκρατίας και του οργανωμένου εγκλήματος, όπως ισχυρίζεται η ίδια η εταιρία, παρά τις αμφιβολίες ότι χρησιμοποιείται και για άλλους σκοπούς.

[56] Βλ. Ibid. Η αρχική έκδοση του λογισμικού στόχευε άτομα αποστέλλοντας μηνύματα κειμένου, που θύμιζαν μηνύματα από τις οικογένειές τους, με υπερσυνδέσμους που οδηγούσαν σε τραπεζικούς λογαριασμούς, κ.ά.

προσωπικά δεδομένα, συμπεριλαμβανομένων κωδικών πρόσβασης, μηνυμάτων, αρχείων καταγραφής κλήσεων κ.λπ. από το σύστημα του θύματος. Ο διαχειριστής του μπορεί να αποκτήσει το υλικό πρόσβασης μέσω αυτού του λογισμικού, π.χ. να ενεργοποιήσει τη κάμερα και το μικρόφωνο της συσκευής του θύματος για την παρακολούθηση των δραστηριοτήτων του. Το Pegasus αναφέρθηκε για πρώτη φορά σε κινητά που βασίζονται σε IOS το 2016 με τη μορφή phishing[57]-μηνυμάτων κειμένου ή email ως μέσο μόλυνσης. Στην αρχή το λογισμικό αυτό είχε χρησιμοποιηθεί στοχεύοντας σε κυβερνητικά πρόσωπα, δημοσιογράφους, πολιτικούς και ανθρώπους με επιρροή[58]. Πλέον μπορεί να χρησιμοποιηθεί και σε σύστημα Android και έχει εξελιχθεί τόσο ώστε να μην χρειάζεται το κλικ[59] του χρήστη για να εγκατασταθεί.[60]

Τόσο το Predator όσο και ο Pegasus μπορούν να έχουν άμεση πρόσβαση σε όλες τις λειτουργίες του τηλεφώνου.[61] Ενδεικτικά μπορούν να υποκλέπτουν τηλεφωνικές κλήσεις, να παρακολουθούν την ομιλία σε πραγματικό χρόνο, να άρουν τα κενά νοημοσύνης με τη συλλογή νέων διαφορετικών πληροφοριών όπως αρχεία, κωδικοί πρόσβασης, επαφές κ.λπ., να ελέγχουν το εγγεγραμμένο περιεχόμενο στις συσκευές, ξεπερνώντας κρυπτογραφημένες πληροφορίες χρησιμοποιώντας ιδιόκτητα πρωτόκολλα SSL, να εξετάζουν όλες τις εφαρμογές του τηλεφώνου όπως π.χ. WhatsApp, Facebook, Skype, Viber, Messenger, να έχουν πρόσβαση στην τοποθεσία μέσω του GPS, να είναι ανεξάρτητα και να

---

[57] Το phising είναι μια μορφή απάτης κοινωνικής μηχανής, στην οποία ο θύτης μιμείται γνωστές οντότητες του θύματος με σκοπό να το παραπλανήσει και να αποσπάσει τις πληροφορίες που θέλει.

[58] Agrawal, M. & Varshney, G. & Kakandwar, S. & Pratap S., Kaushal & Verma, M. (2022). *"Pegasus: Zero-Click spyware attack -its countermeasures and challenges."* Διαθέσιμο στο https://www.researchgate.net/publication/357956844_Pegasus_Zero-Click_spyware_attack_-its_countermeasures_and_challenges [Ημερομηνία πρόσβασης: 4/1/2023] και Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies January 2023 "*The impact of Pegasus on fundamental rights and democratic processes"*, ό.π. σελ. 14.

[59] Chawla, A. (2021) *"Pegasus Spyware: A Privacy Killer"*, ό.π. Αυτή είναι η λεγόμενη τεχνολογία "zero-link".

[60] Το Pegasus μπορεί να εγκατασταθεί πλέον ακόμα και μέσω μιας αναπάντητης κλήσης, ενός μηνύματος, ή ενός email

[61] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies January 2023 "*The impact of Pegasus on fundamental rights and democratic processes"* ό.π. σελ. 25 επ.

δρουν αυτόνομα χωρίς την άδεια του παρόχου κινητής τηλεφωνίας, να εναλλάσσουν τις κάρτες SIM. Επομένως, γίνεται αντιληπτό ότι τα δεδομένα που μπορούν να συλλεγούν είναι εικόνες, κλήσεις, βίντεο, μηνύματα κάθε είδους, τοποθεσία ακόμα και διαγραμμένο περιεχόμενο.[62]

Το 2021, χάρη στη σύμπραξη ογδόντα και πλέον δημοσιογράφων[63] προερχόμενων από δεκαεπτά δημοσιογραφικές ενώσεις, δραστηριοποιούμενες σε δέκα χώρες και την τεχνική υποστήριξη της Διεθνούς Αμνηστίας, προέκυψαν αδιάσειστα στοιχεία για παρακολουθήσεις περίπου πενήντα χιλιάδων τηλεφωνικών αριθμών. Τότε, η Πρόεδρος της Ευρωπαϊκής Επιτροπής, Ursula von der Leyen δήλωσε, αναφορικά με τις παρακολουθήσεις που διενεργήθηκαν σε περισσότερες χώρες, με τη χρήση του παράνομου λογισμικού Pegasus ότι πρόκειται για πρακτικές «*απολύτως απαράδεκτες αντιβαίνουσες σε όλα τα επίπεδα, τους ευρωπαϊκούς κανόνες*», ενώ εξίσου κατηγορηματικά, επεσήμανε ότι η ελευθερία του τύπου αποτελεί καταστατική αξία που ανάγεται στον ευρωπαϊκό ενωσιακό πυρήνα.[64]

---

[62] Ενδιαφέρον παρουσιάζει πρόσφατη υπόθεση που αφορά τη χρησιμοποίηση του λογισμικού Pegasus από την ισραηλινή αστυνομία, στο πλαίσιο υπηρεσιακών ερευνών. Μεταξύ των υποκειμένων που επλήγησαν περιλαμβάνονται πολιτικά πρόσωπα, ενώ μέρος δε των πληροφοριών, αφορούσε τον σεξουαλικό προσανατολισμό ορισμένων εκ των παρακολουθούμενων υποκειμένων. Είναι προφανές ότι πληροφορίες αυτής της ειδικής κατηγορίας δεδομένων καταστρατηγούν κάθε έννοια αναλογικότητας.

[63] Βλ. Forbidden Stories *"About the Pegasus Project"*. Διαθέσιμο στο: https://forbiddenstories.org/about-the-pegasus-project/ [Ημερομηνία πρόσβασης: 4/1/2023]

[64] Βλ. European Parliament (2022) *"Pegasus and surveillance spyware"* – In-Depth analysis for the Pegasus Committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf [Ημερομηνία πρόσβασης: 4/1/2023] και
EPRS (2022) *"Europe's PegasusGate – Countering spyware abuse"*, σελ. 9 επ. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf [Ημερομηνία πρόσβασης: 4/1/2023].

### 2.4. Υποκλοπές δεδομένων

Τα λογισμικά κατασκοπείας σχεδόν πάντα στοχεύουν σε υποκλοπές προσωπικών δεδομένων,[65] τα περισσότερα από αυτά τα δεδομένα είναι ευαίσθητα ανήκουν δηλαδή στις ειδικές κατηγορίες προσωπικών δεδομένων.[66] Συνήθως, τα προσωπικά δεδομένα που συλλέγουν είναι δεδομένα σύνδεσης σε λογαριασμούς, κωδικοί πρόσβασης, προσωπικά στοιχεία τραπεζικών λογαριασμών και τραπεζικών καρτών κ.λπ. Ακόμη τα λογισμικά κατασκοπείας υποκλέπτουν, καταγράφουν και διαβιβάζουν σε τρίτους δεδομένα, που σχετίζονται με τη διαδικτυακή δραστηριότητα και τις προτιμήσεις των χρηστών.

Οι παρακολουθήσεις πολιτών μέσω λογισμικών κατασκοπείας εμπίπτουν στο ουσιαστικό και εδαφικό πεδίο εφαρμογής του ΓΚΠΔ και του νόμου 4624/2019, την εφαρμογή των οποίων εγγυάται η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Ωστόσο, η εφαρμογή της νομοθεσίας δεν είναι πάντα εύκολη αφού προσκρούει στα εξής εμπόδια :

Πρώτον, δεν έχει εντοπισθεί ο χειριστής του λογισμικού, ο οποίος ως υπεύθυνος επεξεργασίας αποτελεί το υποκείμενο των υποχρεώσεων για την προστασία προσωπικών δεδομένων. Ο πρόσφατος έλεγχος της εταιρείας Intellexa Α.Ε. δεν απέδωσε καρπούς, όπως αναφέρθηκε. Δεύτερον, αν υπεύθυνος επεξεργασίας είναι η ΕΥΠ, όπως προκύπτει από την έως τώρα δημοσιογραφική έρευνα, η ΑΠΔΠΧ έχει αποκλειστεί από τον έλεγχό αυτής, κι αυτό

---

[65] Άρθρο 4 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.*»

[66] Άρθρο 9 ΓΚΠΔ παρ.1: «*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 προσανατολισμό.*» Επίσης, αν και δε θεωρούνται ρητά ως ειδική κατηγορία προσωπικών δεδομένων τα δεδομένα που αφορούν ποινικές καταδίκες και τα οικονομικά δεδομένα λογίζονται και αντιμετωπίζονται ως ευαίσθητα προσωπικά δεδομένα.

παρότι η ΕΥΠ υποχρεούται από τον νόμο να τηρεί τη νομοθεσία για την προστασία των προσωπικών δεδομένων. Κατ' αυτόν τον τρόπο, τίθεται ζήτημα συμβατότητας αυτού του περιορισμού των αρμοδιοτήτων της ΑΠΔΠΧ, όχι μόνον με το άρθρο 57 του ΓΚΠΔ αλλά και με το άρθρο 9Α του Συντάγματος, με το άρθρο 8 της ΕΣΔΑ και με το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Τρίτον, αν υπεύθυνος επεξεργασίας είναι η ΕΥΠ, ο νομοθέτης έχει περιορίσει σε τέτοιο βαθμό το δικαίωμα ενημέρωσης των υποκειμένων της επεξεργασίας, ώστε να καθίσταται όχι απλά δυσχερής αλλά σχεδόν αδύνατη η αποτελεσματική άσκηση του. Επιπροσθέτως, τα λοιπά δικαιώματα που προβλέπονται από τον ΓΚΠΔ δεν μπορούν να ασκηθούν. Πέρα από ζητήματα συνταγματικότητας και συμβατότητας με την ΕΣΔΑ, το Σύνταγμα και τον Χάρτη, όπως θα αναλυθεί και στο επόμενο κεφάλαιο, ο περιορισμός αυτός δεν φαίνεται να είναι συμβατός και με το άρθρο 23 του ΓΚΠΔ.

Πάντως σε κάθε περίπτωση οι παρακολουθήσεις με το λογισμικό κατασκοπείας Predator εμπίπτουν στο ουσιαστικό και εδαφικό πεδίο εφαρμογής του ΓΚΠΔ, καθώς πρόκειται για επεξεργασία δεδομένων προσωπικού χαρακτήρα τα οποία περιλαμβάνονται σε σύστημα αρχειοθέτησης, δηλαδή στα κινητά τηλέφωνα των χρηστών (άρθρο 2 παρ. 1 ΓΚΠΔ) και παρότι ο υπεύθυνος επεξεργασίας μπορεί να μην βρίσκεται εντός της ελληνικής επικράτειας η επεξεργασίας προσωπικών δεδομένων Ελλήνων οδηγεί σε αυτήν τη διαπίστωση.[67] Η υποκλοπή των τηλεπικοινωνιών, μέσω της χρήσης του κατασκοπευτικού λογισμικού, εμπίπτει επίσης στο πεδίο εφαρμογής της Οδηγίας για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, Οδ. 2002/58/ΕΚ όπως έχει ενσωματωθεί στην ελληνική έννομη τάξη με τον Ν. 3471/2006 (άρθρο 3 παρ.1 του νόμου).

Επιπροσθέτως, σύμφωνα με το άρθρο 2 παρ. 2 περ. δ' του ΓΚΠΔ, εξαιρείται από το πεδίο εφαρμογής η επεξεργασία δεδομένων που τελείται *«από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια».* Η ρύθμιση αυτή εφαρμόζεται κατ' αρχήν για

[67] Μακρής Σπύρος *«Το Predator και τα προσωπικά δεδομένα. Οι πολλαπλές παραβιάσεις της εθνικής και ευρωπαϊκής νομοθεσίας και τα πρακτικά και νομικά προβλήματα για την εφαρμογή της».* Διαθέσιμο στο: https://www.constitutionalism.gr/to-predator-kai-ta-prosopika-dedomena/#_ftn22 [Ημερομηνία πρόσβασης: 2/7/2023]

τις δραστηριότητες των αστυνομικών και δικαστικών αρχών των Κρατών-μελών στον τομέα του ποινικού δικαίου. Αντί για τον ΓΚΠΔ εφαρμόζονται οι διατάξεις της εκάστοτε εθνικής νομοθεσίας που ενσωματώνουν την Οδηγία (ΕΕ) 2016/680, στην Ελλάδα πρόκειται για το ν. 4624/2019.

Προκειμένου να εφαρμοσθούν οι διατάξεις του ν. 4624/2019, η επεξεργασία πρέπει να τελείται από κάποια «αρμόδια αρχή» και συγκεκριμένα είτε από «*δημόσια αρχή αρμόδια για την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους*» είτε από «*δημόσιο ή ιδιωτικό, οργανισμό ή φορέα στον οποίο ανατίθενται ρόλος δημόσιας αρχής και η εκτέλεση δημοσίων εξουσιών για τους σκοπούς της πρόληψης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους*». Ανεξάρτητα του ποιος είναι ο χειριστής του Predator, οι διατάξεις αυτές δεν μπορούν να εφαρμοσθούν στην περίπτωση των παρακολουθήσεων μέσω του Predator, διότι η ΕΥΠ δεν θεωρείται τέτοια δημόσια αρχή, ενώ αν η παρακολούθηση τελείται από κάποιο ιδιωτικό φορέα, πρέπει αυτός να αναλαμβάνει την άσκηση αρμοδιοτήτων τέτοιας δημόσιας αρχής.

## ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ: ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΤΗΣ ΧΡΗΣΗΣ ΛΟΓΙΣΜΙΚΩΝ ΚΑΤΑΣΚΟΠΕΙΑΣ

### 3.1. Είναι νόμιμη η χρήση κατασκοπευτικών λογισμικών;

Σύμφωνα με τη Σύμβαση της Βουδαπέστης και την Οδ. 2013/40/ΕΕ αλλά και τον ελληνικό ΠΚ όπως θα εκτεθεί κατωτέρω, η παράνομη πρόσβαση σε σύστημα (hacking) είναι αξιόποινη συμπεριφορά.[68] Επιπλέον, παράνομη είναι και η αθέμιτη υποκλοπή δεδομένων, που

[68] Βλ. άρθρο 2 της Σύμβασης της Βουδαπέστης: «*Παράνομη πρόσβαση: Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος πρόσβαση στο σύνολο ή σε μέρος ενός συστήματος υπολογιστή, όταν αυτή διαπράττεται από πρόθεση. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση διάπραξης του εγκλήματος την παραβίαση μέτρων ασφαλείας, με την πρόθεση να αποκτηθούν δεδομένα υπολογιστή ή με άλλη αθέμιτη πρόθεση, ή σε σχέση με ένα σύστημα υπολογιστή που είναι συνδεδεμένο με ένα άλλο σύστημα υπολογιστή*». Αντίστοιχη αναφορά υπάρχει και στο άρθρο 3 της Οδ. 2013/40/ΕΕ: «*Παράνομη*

παραβιάζει το απόρρητο των τηλεφωνημάτων και της προφορικής συνομιλίας.[69] Το έγκλημα αυτό τιμωρείται και από τον ελληνικό ΠΚ στα άρθρα 370Α και 370Β. Η έννοια της παράνομης υποκλοπής[70] υπάρχει και στο άρθρο 6 της Οδ. 2013/40/ΕΕ[71] όπου στο προστατευτέο έννομο αγαθό είναι η εμπιστευτικότητα της ηλεκτρονικής επικοινωνίας.

Τα κατασκοπευτικά λογισμικά βάλλουν επίσης κατά της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας του συστήματος, πολλές φορές καταστρέφοντας

---

*πρόσβαση σε συστήματα πληροφοριών Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.*» Η διαφορά των δύο άρθρων έγκειται στο ότι στο πρώτο δεν προβλέπεται απαραίτητα η παραβίαση μέτρων ασφαλείας σε αντίθεση με τη ρύθμιση της Οδηγίας.

[69] Άρθρο 3 της Σύμβασης της Βουδαπέστης: «*Υποκλοπή: Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η υποκλοπή δια τεχνικών μέσων μη δημοσίων διαβιβάσεων δεδομένων υπολογιστή από και προς ή εντός ενός συστήματος υπολογιστή, περιλαμβανομένων και των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστή στο οποίο ευρίσκονται αυτά τα δεδομένα υπολογιστών, όταν αυτή διαπράττεται από πρόθεση. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση της διάπραξης του εγκλήματος την αθέμιτη πρόθεση, ή την επίτευξη σύνδεσης ενός συστήματος υπολογιστή με ένα άλλο σύστημα υπολογιστή.*»

[70] Σύμφωνα με την Αιτ. Σκ. 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.

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

τα δεδομένα που βρίσκονται αποθηκευμένα στο σύστημα και επεμβαίνοντας στην ορθή λειτουργία του συστήματος.[72]

Αυτό δεν σημαίνει αυτόματα ότι όλα τα κατασκοπευτικά λογισμικά είναι παράνομα. Πολλές εταιρείες κατασκευής κατασκοπευτικών λογισμικών μάλιστα λειτουργούν νόμιμα και εξυπηρετούν νόμιμους σκοπούς.[73] Η ίδια η κακή χρήση συσκευών μεταξύ αυτών και προγραμμάτων υπολογιστών τιμωρείται με βάση το άρθρο 6 της Σύμβασης της

---

[72] Βλ. άρθρο 4 της Σύμβασης της Βουδαπέστης: «*Παρεμβολές σε δεδομένα: 1. Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος βλάβη, διαγραφή, φθορά, αλλοίωση ή καταστολή δεδομένων υπολογιστών, όταν αυτή διαπράττεται από πρόθεση. 2. Ένα Συμβαλλόμενο Μέρος μπορεί να διατηρήσει το δικαίωμα να θέσει ως προϋπόθεση ύπαρξης εγκλήματος για την συμπεριφορά που περιγράφεται στην παρ . 1 την πρόκληση σοβαρής ζημίας.*» και άρθρο 5 της Σύμβασης της Βουδαπέστης: «*Παρεμβολές σε συστήματα: Κάθε συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος σοβαρή παρακώλυση της λειτουργίας ενός συστήματος υπολογιστή δια της εισαγωγής, διαβίβασης, βλάβης, διαγραφής, φθοράς, αλλοίωσης ή καταστολής δεδομένων υπολογιστή, όταν αυτή διαπράττεται από πρόθεση.*» Η διαφορά μεταξύ των δύο άρθρων είναι ότι το πρώτα αναφέρεται στις παρεμβολές σε συστήματα ενώ το δεύτερο αναφέρεται στις παρεμβολές στα ίδια τα δεδομένα. Αντίστοιχα είναι τα άρθρα 4 Οδ. 2013/40/ΕΕ: «*Παράνομη παρεμβολή σε σύστημα: Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.*» και άρθρο 5 Οδ. 2013/40/ΕΕ: «*Παράνομη παρεμβολή σε δεδομένα Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.*»

[73] Για παράδειγμα το Shameware, το λογισμικό λογοδοσίας, είναι ένα λογισμικό κατασκοπείας που λειτουργεί με τη γνώση του χρήστη, ή και με τη συγκατάθεσή του. Μπορεί να απαιτηθεί η εγκατάστασή του με σκοπό να ανιχνεύσει την προβολή πορνογραφίας ή άλλου περιεχομένου που κρίνεται ακατάλληλο και να το αναφέρει στις αρχές.

Βουδαπέστης[74] αλλά και τα εργαλεία μεταξύ αυτών και τα προγράμματα που έχουν σχεδιαστεί για την τέλεση των ανωτέρω αδικημάτων τιμωρούνται με βάση το άρθρο 7 της Οδ. 2013/40/ΕΕ.[75] Πολλοί έχουν κατακρίνει αυτές τις ρυθμίσεις με το επιχείρημα ότι ποινικοποιούν την τεχνολογία.

---

[74] *«Κακή χρήση συσκευών: 1. Κάθε συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η άνευ δικαιώματος και από πρόθεση διάπραξη των κάτωθι: α. Παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή άλλως διάθεση: ι. μιας συσκευής, περιλαμβανομένου και ενός προγράμματος υπολογιστή, σχεδιασμένης ή προσαρμοσμένης πρωτίστως με σκοπό τη διά πράξη κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5,ιι. ενός συνθηματικού ή κωδικού πρόσβασης, ή άλλου παρεμφερούς δεδομένου, με την χρήση του οποίου είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός συστήματος υπολογιστή, με πρόθεση να χρησιμοποιηθεί για τον σκοπό της διάπραξης κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5, και β. Κατοχή ενός αντικειμένου από τα αναφερόμενα στις παραγράφους α.ι και α.ιι ανωτέρω, με σκοπό τη διάπραξη κάποιου εκ των εγκλημάτων που περιγράφονται στα ως άνω Άρθρα 2 έως 5. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση να υπάρχει κατοχή ενός αριθμού τέτοιων αντικειμένων πριν θεμελιωθεί ποινική ευθύνη.*

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

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

[75] *«Εργαλεία που χρησιμοποιούνται για τη διάπραξη των αδικημάτων: Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η εκ προθέσεως παραγωγή, πώληση, προμήθεια προς χρήση, εισαγωγή, διανομή ή με άλλο τρόπο διάθεση ενός εκ των ακόλουθων εργαλείων χωρίς δικαίωμα και με την πρόθεση να χρησιμοποιηθούν προς διάπραξη οποιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις: α) πρόγραμμα υπολογιστή, που έχει σχεδιασθεί ή προσαρμοσθεί κατά κύριο λόγο με σκοπό τη διάπραξη οιουδήποτε εκ των αδικημάτων που αναφέρονται στα άρθρα 3 έως 6· β) συνθηματικού κωδικού υπολογιστή, κωδικού πρόσβασης ή παρόμοιων στοιχείων μέσω των οποίων μπορεί να αποκτηθεί πρόσβαση στο σύνολο ή σε μέρος συστήματος πληροφοριών.»*

Οι περισσότεροι κατασκευαστές κατασκοπευτικών λογισμικών δεν υφίστανται δυσμενείς συνέπειες λόγω του τρόπου με τον οποίο τα κατασκοπευτικά λογισμικά εγκαθίστανται σε μια συσκευή. Πλέον, ο νέος νόμος 5002/2002 ποινικοποίησε την κατοχή και την χρήση παράνομων λογισμικών κατασκοπείας με την εισαγωγή του άρθρου 370ΣΤ στον ελληνικό Ποινικό Κώδικα.[76] Ενώ πολλοί χρήστες ηλεκτρονικών υπολογιστών ισχυρίζονται ότι ποτέ δεν έδωσαν την άδεια τους για την εγκατάσταση κατασκοπευτικού λογισμικού στον υπολογιστή τους, οι δημιουργοί θεωρούν, ότι αυτό δεν ισχύει, καθώς πολλά κατασκοπευτικά λογισμικά που εγκαθίστανται μέσω λήψης εφαρμογών και άλλων νόμιμων λογισμικών σε έναν υπολογιστή, αναφέρονται στη σύμβαση αδειοδότησης και σχεδόν όλες τις φορές οι χρήστες πρέπει να επιλέξουν αν συναινούν ή όχι πριν την εγκατάσταση τις εφαρμογής ή του λογισμικού. Αν και σχεδόν πάντα οι χρήστες επιλέγουν ότι συμφωνούν χωρίς να διαβάσουν τους όρους χρήσης ή όσοι τους διαβάζουν δεν κατανοούν πλήρως το περιεχόμενο αυτών, οι κατασκευαστές των κατασκοπευτικών λογισμικών θεωρούν ότι πρόκειται για δεσμευτική συναίνεση. Με αυτόν τον τρόπο, το κατασκοπευτικό λογισμικό βρίσκεται στον υπολογιστή ενός χρήστης με έναν τουλάχιστον τυπικά νόμιμο τρόπο. Ωστόσο, το θέμα της συναίνεσης είναι ένα κρίσιμο ζήτημα, ειδικά όταν αυτή δίνεται μέσω προεπιλεγμένων κουτιών.

Παρόλη τη νομιμότητα ορισμένων κατασκοπευτικών λογισμικών εξακολουθούν να υπάρχουν λογισμικά κατασκοπείας που είναι παράνομα, όπως αυτά για τα οποία δε γίνεται καμία αναφορά στη συμφωνία αδειοδότησης. Επιπλέον, σημαντική είναι η διάκριση μεταξύ της νόμιμης διαδικασίας παρακολούθησης, μέσω των νομοθετικών εθνικών κειμένων και των ενωσιακών απαιτήσεων και της χρήσης λογισμικών κατασκοπείας, που καταστρατηγούν όχι μόνο θεμελιώδη ανθρώπινα δικαιώματα αλλά και τον ίδιο τον πυρήνα της δημοκρατίας.[77]

Το πλέον κρίσιμο είναι ότι αυτές οι μέθοδοι παρακολούθησης τείνουν να καθιερωθούν ακόμα και σε πολλές δημοκρατικές χώρες, αντικαθιστώντας τη νόμιμη διαδικασία άρσης του απορρήτου. Το φαινόμενο αυτό ξεκίνησε ήδη από το 2015, όταν το Ευρωπαϊκό

[76] Βλ. Κεφάλαια 3.5 και 4.4

[77] Βλ. Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies January 2023 "*The impact of Pegasus on fundamental rights and democratic processes"* ό.π. σελ. 29 σχετικά με την έννοια μιας «παρεμβατικής δημοκρατίας».

Κοινοβούλιο έθεσε ζήτημα αυστηροποίησης του νομικού πλαισίου σε σχέση με τον έλεγχο των εξαγωγών, τεχνικής βοήθειας, μεταφοράς κλπ. ειδών διπλής χρήσης, σε μια προσπάθεια να αντιμετωπιστεί η τάση χρήσης λογισμικών κατασκοπείας.[78] Η ελληνική επικαιρότητα των υποθέσεων που αναλύθηκαν ανωτέρω[79] απλώς επιβεβαιώνει τη γενικότερη τάση που επικρατεί. Η χρήση των λογισμικών κατασκοπείας και η τάση καθιέρωσής τους από τις κυβερνήσεις ως μέσου παρακολούθησης βάλλει κατά των καταστατικών αρχών και των συνταγματικά κατοχυρωμένων δικαιωμάτων και θέτει υπό αμφισβήτηση τον ίδιο τον πυρήνα της δημοκρατίας.

[78] Βλ. Κανονισμός (ΕΕ) 2021/821 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 2021 θέσπιση ενωσιακού συστήματος ελέγχου των εξαγωγών, της μεσιτείας, της τεχνικής βοήθειας, της διαμετακόμισης και της μεταφοράς ειδών διπλής χρήσης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021R0821 [Ημερομηνία πρόσβασης: 9/1/2023]

[79] Βλ. European Parliament (2022) *"Pegasus and surveillance spyware"* – In-Depth analysis for the Pegasus Committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies, ό.π. σελ. 7 επ.

### 3.2. Οι επιπτώσεις των λογισμικών κατασκοπείας στα ανθρώπινα δικαιώματα

#### *3.2.1.Οι επιπτώσεις των λογισμικών κατασκοπείας στο δικαίωμα προστασίας του απορρήτου των επικοινωνιών*

Το δικαίωμα στο απόρρητο των επικοινωνιών κατοχυρώνεται συνταγματικά στο άρθρο 19 του Συντάγματος[80] αλλά και καταστατικά στο άρθρο 8 της ΕΣΔΑ,[81] στο άρθρο 7 του ΧΘΔΕΕ[82] και στο άρθρο 17 του ΔΣΑΠΔ του ΟΗΕ.[83] Το άρθρο 19 του Συντάγματος ορίζει το δικαίωμα στο απόρρητο ως απολύτως απαραβίαστο, με μια ερμηνευτική δήλωση, ενώ στη συνέχεια παραθέτει περιοριστικά τις περιπτώσεις που αυτό μπορεί να καμφθεί, χωρίς ωστόσο ο συντακτικός νομοθέτης να πέφτει σε αντίφαση. Σύμφωνα με το Σύνταγμα το δικαίωμα στο απόρρητο μπορεί να καμφθεί μόνο εφόσον υπάρχει εκτελεστικός νόμος, οποίος να ορίζει τη διαδικασία άρσης του απορρήτου και για δύο αποκλειστικούς λόγους: για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, ήτοι κακουργημάτων. Η

---

[80] *«Απόρρητο επιστολών, ανταπόκρισης και επικοινωνίας: 1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.*

*2. Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1.*

*3. Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9 Α.»*

[81] *«Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής: 1. Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. 2. Δεν επιτρέπεται να υπάρξει επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.»*

[82] *«Σεβασμός της ιδιωτικής και οικογενειακής ζωής: Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του.»*

[83] *«1. Κανείς δεν υπόκειται σε αυθαίρετες ή παράνομες παρενοχλήσεις της ιδιωτικής του ζωής, της οικογένειας, της κατοικίας ή της αλληλογραφίας του, ούτε σε παράνομες προσβολές της τιμής και της υπόληψής του.*

*2. Κάθε πρόσωπο έχει δικαίωμα προστασίας από το νόμο έναντι τέτοιων παρενοχλήσεων ή προσβολών.»*

σχετική άδεια χορηγείται κατά κανόνα, μετά από απόφαση δικαστικής ή ανεξάρτητης αρχής η οποία θα διαθέτει εχέγγυα αμεροληψίας. Στην Ελλάδα η αρχή που έχει θεσπιστεί είναι η ΑΔΑΕ.

Με το άρθρο 19 παρ.1 εδ. α ειδικότερα κατοχυρώνεται το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας ως προέκταση του δικαιώματος στην προσωπική ελευθερία. Οι δύο συνιστώσες, ήτοι η ελευθερία της επικοινωνίας και το απόρρητο όλων των μορφών επικοινωνίας πρέπει να εξετάζονται κατά περίσταση και με βάση του αν τα ενδιαφερόμενα μέρη αποσκοπούσαν στη διατήρηση της επικοινωνίας τους ως μυστικής. Το δικαίωμα στην ελεύθερη διεξαγωγή της επικοινωνίας αποτελεί βέβαια προϋπόθεση της προστασίας του απορρήτου. Δεν μπορεί όμως να υπάρξει απόρρητο της πληροφορίας εάν δεν έχει προηγουμένως κατοχυρωθεί το δικαίωμα στην ελεύθερη επικοινωνία δηλαδή το δικαίωμα του ανθρώπου να επιλέγει το είδος το μέσο, και τον τρόπο της επικοινωνίας χωρίς να εμποδίζεται από ιδιωτική εξουσία. Εάν όμως οι ενδιαφερόμενοι δεν επιθυμούν τη μυστικότητα τότε θα μπορούσαμε να θεωρήσουμε ότι η προστασία της ελεύθερης έκφρασης είναι ανεξάρτητη από το δικαίωμα στην ιδιωτικότητα.

Είναι όμως δυνατόν να μην περιορίζεται η ελευθερία της επικοινωνίας[84] όταν η επικοινωνία τίθεται υπό επιτήρηση; [85] Αυτό είναι το μείζον ερώτημα στο οποίο καλείται πλέον ο νομοθέτης και δη ο συντακτικός νομοθέτης να δώσει απάντηση, όταν η επικοινωνία τελεί υπό την επιτήρηση των κατασκοπευτικών λογισμικών. Το Σύνταγμα κατοχυρώνει μεν το απόρρητο της επικοινωνίας με όποιο τρόπο και αν αυτή γίνεται λαμβανομένης υπόψη κάθε δυνατής μελλοντικής τεχνολογικής εξέλιξης και συνεπώς οι πληροφορίες που σχετίζονται με την επικοινωνία, όπως και τα εξωτερικά της στοιχεία υπάγονται στο απόρρητο.[86] Όμως, η ανάπτυξη των κατασκοπευτικών λογισμικών και η επιτήρηση των επικοινωνιών μέσω αυτών περιορίζει σε τεράστιο βαθμό το δικαίωμα στο απόρρητο της επικοινωνίας, μιας και

[84] Βλ. Π. Δαγτόγλου (2012) «*Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα*», 4η έκδ., εκδόσεις Σάκκουλας, Αθήνα, σελ. 352

[85] Όπως αναφέρει ο Χρυσόγονος οι δύο αυτές εκφάνσεις του δικαιώματος είναι τελικά άρρηκτα συνυφασμένες αφού η ελευθερία της επικοινωνίας δεν μπορεί παρά να είναι πλασματική όταν «…υπάρχει το ενδεχόμενο επιβολής κυρώσεων…». Βλ. Κ. Χρυσόγονος (2002) «*Ατομικά και κοινωνικά δικαιώματα*», 2η Εκδ. Σάκκουλα, Αθήνα-Κομοτηνή σελ.245

[86] Βλ. Γνμδ 1/2005 της ΑΔΑΕ: http://www.adae.gr/fileadmin/docs/nomoi/893-2005.pdf

η επικοινωνία δε διεξάγεται πλέον με ελευθερία και τα υποκείμενα παρακολουθούνται ανά πάσα ώρα και στιγμή. Η πιθανότητα κάποιο υποκείμενο του δικαιώματος να παρακολουθείται μέσω λογισμικών κατασκοπείας για οποιονδήποτε λόγο συνιστά κατάφωρη παραβίαση του συνταγματικά κατοχυρωμένου αυτού δικαιώματος του στο απόρρητο και όταν αυτή συντελείται μαζικά ενδέχεται να επιφέρει και καταστροφικές συνέπειες στην ελεύθερη επικοινωνίας των πολιτών.

Στο δεύτερο εδάφιο του Συντάγματος εισάγεται εξαίρεση θέτοντας το απόρρητο υπό την ειδική επιφύλαξη του νόμου, προβλέποντας ότι νόμος θα ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν θα δεσμεύεται από το απόρρητο όταν υπάρχουν λόγοι εθνικής ασφάλειας ή όταν αυτό χρειάζεται να γίνει για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Έτσι, σε αυτές τις περιπτώσεις η άρση του απορρήτου θα πραγματοποιείται μόνο με σχετική πρόβλεψη σε τυπικό νόμο ή κανονιστική πράξη ύστερα από νομοθετική εξουσιοδότηση με τον οποίο θα καθορίζονται τα κριτήρια τα οποία στη συνέχεια θα λάβει υπόψη της η δικαστική αρχή για να δώσει με τη σειρά της τη σχετική εντολή άρσης του απορρήτου.

Αντίστοιχα το άρθρο 8 της ΕΣΔΑ, η οποία κατέχει υπερνομοθετική ισχύ και ενσωματώθηκε στο εθνικό δίκαιο με βάση το άρθρο 28 του Συντάγματος θεσπίζει το δικαίωμα στην ιδιωτικότητα, κατά τρόπο ίδιο με το ελληνικό Σύνταγμα. Αξίζει να σημειωθεί ότι στο άρθρο 8 ΕΣΔΑ, το αναγκαίο μέτρο του περιορισμού του δικαιώματος συναρτάται οπωσδήποτε με τη δημοκρατική φυσιογνωμία της κοινωνίας, εντός της οποίας διεξάγεται η συζήτηση και λαμβάνεται η σχετική απόφαση της αρμόδιας – δικαστικής ή ανεξάρτητης – αρχής.

Όπως προαναφέρθηκε οι περισσότερες κατασκευάστριες εταιρίες λογισμικών κατασκοπείας ισχυρίζονται ότι τα προϊόντα τους προορίζονται αποκλειστικά για την καταπολέμηση του οργανωμένου εγκλήματος, τις απαγωγές, την τρομοκρατία κ.ά. [87] Στην πράξη όμως η πραγματικότητα διαψεύδει αυτές τις δηλώσεις, αφού τα κατασκοπευτικά λογισμικά καταλήγουν να λειτουργούν ως πανοπτικός μηχανισμός απόλυτου ελέγχου των τηλεφωνικών συσκευών και των υπολογιστών, καθώς πλέον η επικοινωνία δε συντελείται μόνο μέσω των τηλεφώνων αλλά και μέσω π.χ. email και εφαρμογών, γι' αυτό και δρουν προφανώς με εντελώς διαφορετικό τρόπο σε σχέση με τη διαδικασία της νόμιμης άρσης του

[87] Βλ. π.χ. την περιγραφή προϊόντος Pegasus: https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf.

απορρήτου, η οποία χαρακτηρίζει μόνο την καταγραφή συνομιλιών μεταξύ των παρακολουθούμενων μερών.

Σημαντική είναι και η αναφορά στις σύγχρονες προκλήσεις που προκύπτουν από την χρήση παράνομων λογισμικών κατασκοπείας από κρατικούς φορείς και κυβερνήσεις κατ' επίκληση λόγων εθνικής ασφάλειας.[88] Έτσι, τον Απρίλιο του 2022, η Ευρωπαϊκή Επιτροπή διευκρίνισε ότι η διαχείριση ζητημάτων εθνικής ασφάλειας –που φυσικά εκφεύγουν από το πεδίο του ενωσιακού δικαίου – εναπόκειται στις έννομες τάξεις των κρατών-μελών, ανοίγοντας τον ασκό του Αιόλου.[89]

Ωστόσο, σε ό,τι αφορά τα ζητήματα εθνικής ασφάλειας, υφίστανται εξίσου για τα κράτη – μέλη οι δεσμεύσεις που απορρέουν από την ΕΣΔΑ, καθώς επίσης και η νομολογία του ΕΔΔΑ χωρίς εξαιρέσεις. Εν προκειμένω, το ΕΔΔΑ έχει καταστήσει σαφές ότι τα ζητήματα αυτά δεν κείνται εν γένει εκτός της δικαιοδοσίας του. Ενώ δηλαδή, αναγνωρίζει ευρύ περιθώριο διακριτικής ευχέρειας στις εθνικές έννομες τάξεις ως προς τα μέτρα – ακόμη κι αν ως μέτρο επιλέγεται κάποιο λογισμικό κατασκοπείας- που επιλέγουν για την προστασία της εθνικής ασφάλειας,[90] επισημαίνει εντούτοις, εμφατικά ότι πρέπει να διερευνάται επαρκώς από τις αρμόδιες αρχές, η ύπαρξη της « αδήριτης ανάγκης» που στοιχειοθετεί τον συγκεκριμένο λόγο εθνικής ασφάλειας.[91]

---

[88] Έτσι για παράδειγμα, αιτιολόγησε η Ουγγαρία την πρόσφατη χρήση του κατασκοπευτικού λογισμικού Pegasus σε βάρος πολιτικών της αντιπολίτευσης και δημοσιογράφων. Συγκεκριμένα, στην Ουγγαρία όταν το αίτημα άρσης απορρήτου αφορά λόγους εθνικής ασφάλειας, αρκεί η υπογραφή του αρμόδιου υπουργού, χωρίς να απαιτείται προηγούμενη έγκριση της δικαστικής αρχής.

[89] Άρθρο 4 παρ. 2, τελευταίο εδάφιο Συνθήκης για την Ευρωπαϊκή Ένωση: «*η εθνική ασφάλεια παραμένει στην ευθύνη κάθε κράτους μέλους*».

[90] Στις αποφάσεις ΕΔΔΑ *Roman Zakharov v. Russia* και *Szabó and Vissy v. Hungary*, το Δικαστήριο επεσήμανε ότι όπου υπάρχει μυστικότητα της διαδικασίας, ο κίνδυνος αυθαιρεσίας είναι προφανής. Γι' αυτό το λόγο είναι απαραίτητο να υπάρχει σαφής και λεπτομερής νόμος σχετικά με τα μέτρα παρακολούθησης ιδίως όταν η τεχνολογία γίνεται ακόμα πιο περίπλοκη.

[91] Βλ. ΕΔΔΑ, *Dumitru Popescu v. Romania* 26 April 2007 παρ. 61 επ., *Amann v. Switzerland* 16 February 2000, παρ. 76, *Klass and others v. Germany*, 6 September 1978 παρ. 48

### *3.2.2.Οι επιπτώσεις των λογισμικών κατασκοπείας στο δικαίωμα προστασίας των προσωπικών δεδομένων*

Η προστασία της ιδιωτικότητας κατοχυρώνεται στο άρθρο 8 της ΕΣΔΑ, στο άρθρο 8 ΧΘΔΕΕ,[92] στο άρθρο 12 της Οικουμενικής διακήρυξης του ΟΗΕ[93], στο άρθρο 17 του ΔΣΑΠΔ και συνταγματικά στο άρθρο 9Α του ελληνικού Συντάγματος.[94] Το δικαίωμα προστασίας της ιδιωτικότητας ανάγεται σε θεμελιώδες δικαίωμα που εμπεριέχει και άλλα δικαιώματα και συνδέεται με την εύλογη προσδοκία των ανθρώπων για προστασία του ιδιωτικού του βίου. Πρόκειται για έναν συνδυασμό αρνητικής και θετικής ελευθερίας, για προστασία της ιδιωτικής ζωής έναντι των κρατικών παρεμβάσεων αλλά και των ιδιωτικών συμφερόντων εκμετάλλευσης της προσωπικής ζωής, ενώ η προστασία του δικαιώματος συνδέεται και με την απόλαυση των υπόλοιπων δικαιωμάτων.

Με το ψήφισμα της Ζ' Αναθεωρητικής Βουλής της 6ης Απριλίου 2001 προστέθηκε στο ελληνικό Σύνταγμα η διάταξη του άρθρου 9Α με την οποία η προστασία των προσωπικών δεδομένων στην Ελλάδα κατοχυρώθηκε και συνταγματικά. Η εξέλιξη της σύγχρονης τεχνολογίας και η ανάπτυξη νέων τεχνολογιών αυτοματοποιημένης συλλογής, επεξεργασίας και χρήσης προσωπικών πληροφοριών οδήγησε ήδη σε διεθνές επίπεδο σε μία σειρά από ρυθμίσεις προστασίας των προσωπικών δεδομένων. Ο Έλληνας νομοθέτης ακολούθησε αυτές τις ρυθμίσεις με ανάλογες νομοθετικές πρωτοβουλίες και με την αναθεώρηση του Συντάγματος του 2001 θεσμοθέτησε τις τάσεις της διεθνούς και

---

[92] *«Προστασία των δεδομένων προσωπικού χαρακτήρα: 1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.*

*2. 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 συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.*

*3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.»*

[93] *«Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.»*

[94] *«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.»*

ευρωπαϊκής νομοθεσίας και ανήγαγε με την εισαγωγή του νέου άρθρου την προστασία των προσωπικών δεδομένων σε αυτοτελές συνταγματικό δικαίωμα.

Η διάταξη αυτή έχει πεδίο εφαρμογής ευρύτερο από το άρθρο 9 Σ,[95] αφού αφορά κάθε είδους προσωπικά δεδομένα και όχι μόνον πληροφορίες που αφορούν την προσωπική ζωή του ατόμου. Έτσι, το Σύνταγμα καθιερώνει ένα αμυντικό δικαίωμα που θωρακίζει την ιδιωτική ζωή από εξωτερικές προσβολές και προστατεύει τα προσωπικά δεδομένα από τη συλλογή, επεξεργασία και χρήση τους και κατοχυρώνει, πλέον, και το λεγόμενο δικαίωμα της «πληροφοριακής αυτοδιάθεσης», ή αλλιώς «πληροφοριακού αυτοκαθορισμού» του ατόμου σε επίπεδο ανώτατης τυπικής ισχύος. Η διάταξη αυτή δεν συνεπάγεται μια καθολική απαγόρευση, αλλά έχει την έννοια της υποχρέωσης του νομοθέτη να διαμορφώσει το κατάλληλο νομικό πλαίσιο έτσι ώστε να καταστεί νόμιμη με τις προϋποθέσεις του νόμου.

Στην περίπτωση των κατασκοπευτικών λογισμικών γίνεται αντιληπτό ότι η παρέμβαση στην ιδιωτικότητα είναι τόσο ευρεία, που καταλαμβάνει ένα τεράστιο πεδίο προσωπικών δεδομένων και δη ευαίσθητων. Για παράδειγμα αν αναλογιστεί κανείς τις λειτουργίες των «έξυπνων» κινητών τηλεφώνων, γίνεται εύκολα αντιληπτό το απόθεμα πληροφοριών που αποθησαυρίζει η παγίδευση μιας τέτοιας συσκευής από λογισμικό κατασκοπείας. Υπό αυτή την έννοια, πράγματι, δεν αποτελεί υπερβολή η αναφορά στα σύγχρονα λογισμικά ψηφιακής επιτήρησης ως "game changer[s]".[96] Ο βαθμός διείσδυσής τους στο καθ' έκαστον περιβάλλον των τηλεφωνικών συσκευών, η πρόσβασή τους αδιακρίτως σε ό,τι συγκροτεί το σύνολο των δεδομένων που φιλοξενούνται στη συσκευή εισφέρει απλώς επιχειρήματα ενισχυτικά της αντίληψης περί σύγχρονου «κατασκοπευτικού καπιταλισμού» και

[95] « *Άσυλο της κατοικίας: 1. Η κατοικία του καθενός είναι άσυλο. Η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη. Καμία έρευνα δεν γίνεται σε κατοικία, παρά μόνο όταν και όπως ορίζει ο νόμος και πάντοτε με την παρουσία εκπροσώπων της δικαστικής εξουσίας.*

*2. Οι παραβάτες της προηγούμενης διάταξης τιμωρούνται για παραβίαση του οικιακού ασύλου και για κατάχρηση εξουσίας και υποχρεούνται σε πλήρη αποζημίωση του παθόντος, όπως νόμος ορίζει.* »

[96] Ingleton, D. The Guardian (2022) Amnesty International: *"The Pegasus Project: One year on, spyware crisis continues after failure to clamp down on surveillance industry"*. Διαθέσιμο στο: https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/ [Ημερομηνία πρόσβασης: 9/1/2023]

πληθωριστικής συρροής προσωπικών δεδομένων.[97] Μάλιστα, όπως προαναφέρθηκε η διείσδυση των κατασκοπευτικών λογισμικών σε όλες τις εφαρμογές ενός κινητού τηλεφώνου, αποκτώντας πρόσβαση σε όλα τα προσωπικά δεδομένα του χρήστη που βρίσκονται αποθηκευμένα σε αυτές, παραβιάζει τον πυρήνα της εν λόγω διάταξης, που δεν είναι άλλος από την προστασία της ιδιωτικότητας, την προστασία αυτών των δεδομένων που χαρακτηρίζουν μοναδικά και ταυτοποιούν το υποκείμενο και παραθέτουν πληροφορίες πολύ προσωπικές για το ίδιο, οι οποίες χωρίς τα κατασκοπευτικά λογισμικά ενδεχομένως να μην αποκαλύπτονταν ποτέ αυτοβούλως από το ίδιο το υποκείμενο.

Τα ζητήματα όμως που ανακύπτουν από την χρήση λογισμικών κατασκοπείας σε συνάρτηση με την προστασία των προσωπικών δεδομένων δεν σταματούν εκεί. Πρώτα από όλα βασικό ζήτημα αποτελεί η νομιμότητα της επεξεργασίας προσωπικών δεδομένων μέσω των λογισμικών κατασκοπείας. Η επεξεργασία προσωπικών δεδομένων που έχουν συλλεχθεί μέσω τέτοιων λογισμικών πρέπει να βασίζεται σε μια από τις νομικές βάσεις που προβλέπει το άρθρο 9 του ΓΚΠΔ και ο νόμος 4624/2019 για την επεξεργασία ευαίσθητων προσωπικών δεδομένων, αλλιώς είναι παράνομη. Συγκεκριμένα, αν χειριστής του εκάστοτε λογισμικού είναι η ΕΥΠ ή οποιαδήποτε παρεμφερής υπηρεσία, η επεξεργασία στερείται νομικής βάσης. Με την υπόθεση ότι το λογισμικό χρησιμοποιείται για λογαριασμό της ΕΥΠ, αυτή θα μπορούσε να επικαλεσθεί την περίπτωση ζ' της παραγράφου 2 του άρθρου 9 του ΓΚΠΔ ως νομική βάση της επεξεργασίας, ότι δηλαδή η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος. Η επίκληση αυτή απαιτεί την τήρηση σωρευτικά δύο προϋποθέσεων: να είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος και οι λόγοι δημοσίου συμφέροντος να είναι ανάλογοι προς τον επιδιωκόμενο στόχο, και να έχει βάση στο δίκαιο της Ένωσης ή κράτους μέλους, και ο κανόνας δικαίου να σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και να προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων. Και σε αυτό το σημείο εισέρχεται η

[97] Βλ. 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/#_ftn1 [Ημερομηνία πρόσβασης: 9/1/2023]

προστασία του δικαιώματος του απορρήτου των επικοινωνιών και ο όρος της εθνικής ασφάλειας.

Για να γίνει δεκτή η επίκληση αυτής της νομικής βάσης, πρέπει ο νόμος στον οποίο βασίζεται η επεξεργασία «*να θεσπίζει προδιαγραφές για τον καθορισμό του υπευθύνου επεξεργασίας, του είδους των δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία, των εκάστοτε υποκειμένων των δεδομένων, των οντοτήτων στις οποίες μπορούν να κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, των περιορισμών σκοπού, της περιόδου αποθήκευσης και άλλων συγκεκριμένων μέτρων για την εξασφάλιση σύννομης και δίκαιης επεξεργασίας*». Αυτές οι προδιαγραφές δεν υπάρχουν στην νομοθεσία για την άρση του απορρήτου, όπως τροποποιήθηκε με τον νόμο 5002/2022.

Πάντως αν αποδειχτεί ότι χειριστής του λογισμικού και άρα υπεύθυνος επεξεργασίας είναι η ΕΥΠ, τίθενται περιορισμοί στην άσκηση του δικαιώματος ενημέρωσης αλλά και των άλλων δικαιωμάτων που προβλέπει ο ΓΚΠΔ, ώστε να θίγεται ζήτημα περιορισμού του πυρήνα των δικαιωμάτων.

Από την άλλη με την υπόθεση ότι χειριστής του λογισμικού είναι ιδιωτική εταιρεία καμία από τις νομικές βάσεις που προβλέπει το άρθρο 9 του ΓΚΠΔ για την επεξεργασία ευαίσθητων προσωπικών δεδομένων δεν φαίνεται να μπορεί να δικαιολογήσει τη συλλογή και επεξεργασία δεδομένων από ιδιωτικό φορέα μέσω λογισμικού κατασκοπείας.

Σε συνάρτηση επίσης με τις αρχές του ΓΚΠΔ,[98] την προστασία εξ ορισμού και από τον σχεδιασμό,[99] την αρχή της ελαχιστοποιήσης και την απαίτηση της διενέργειας μελέτης αντικτύπου[100] τα κατασκοπευτικά λογισμικά υστερούν. Εγγενής κίνδυνος που καθιστά απαγορευτική τη χρήση τέτοιων λογισμικών αποτελεί ότι στην εργοστασιακή τους ρύθμιση δεν παράγονται με ενσωματωμένες προδιαγραφές (by design), που να καταλείπουν αξιόπιστα ίχνη και να εγγυώνται τη διατήρηση ακριβούς ιστορικού (στόχος, διάρκεια, έναρξη, λήξη του μέτρου κ.λπ.).[101]Αυτό σημαίνει ότι στο πλαίσιο των ελέγχων που οφείλουν

[98] άρθρο 5 ΓΚΠΔ

[99] άρθρο 25 ΓΚΠΔ

[100] άρθρο 35 ΓΚΠΔ

[101] Υπάρχουν ασαφείς αναφορές των εταιρειών παραγωγής που βεβαιώνουν ότι μπορούν να παραχθούν μοντέλα με χαρακτηριστικά που θα πληρούν ανάλογες προϋποθέσεις κρατικού ελέγχου.

να διενεργούν εκ των υστέρων, οι εποπτεύουσες αρχές δεν θα έχουν ποτέ διαθέσιμα στοιχεία για να ανατρέξουν στον τρόπο που υλοποιήθηκε το μέτρο της παρακολούθησης προκειμένου να αξιολογήσουν τη νομιμότητά του.[102] Η παραδοχή αυτή αρκεί για να ταξινομήσει τα λογισμικά κατασκοπείας στην κατηγορία των μη συμβατών μεθόδων προς τις αρχές που διέπουν τον περιορισμό του δικαιώματος εντός του κράτους δικαίου. Η απουσία θεσμικών αντίβαρων και λογοδοσίας, συνεπώς, εντός ενός συστήματος, το οποίο για τη διασφάλιση της νομιμότητας, επενδύει προεχόντως, στη λειτουργία των αμοιβαίων ελέγχων, ενισχύει τον κίνδυνο κατάχρησης και διεύρυνσης των παρακολουθήσεων με ψευδεπίγραφη ή ανύπαρκτη αιτιολογία. Πολλά επίσης, από τα προϊόντα κατασκοπευτικών λογισμικών, όπως για παράδειγμα το Pegasus είναι κατασκευασμένα με τέτοιο τρόπο, ώστε να αποφεύγουν τα τεχνικά και οργανωτικά μέτρα όπως την κρυπτογράφηση, τα πρωτόκολλα κ.ά.

### *3.2.3. Οι συσχετισμοί με άλλα θεμελιώδη δικαιώματα*

Λόγω της εύλογης προσδοκίας των πολιτών στην ιδιωτικότητα το δικαίωμα αυτό συνδέεται με άλλα θεμελιώδη δικαιώματα. Κατά τον Μάνεση η ατομική ελευθερία συνδέεται άμεσα με την ιδιωτική ζωή ως οιονεί προέκταση του ασύλου της κατοικίας και προστατεύει την ελεύθερη ανακοίνωση ιδεών και συναισθημάτων.[103] Επομένως, τα δύο αυτά δικαιώματα είναι άμεσα συνυφασμένα μεταξύ τους. Η παρέμβαση για παράδειγμα του κράτους ή κάποιου ιδιώτη στην προσωπική ζωή ενός πολίτη περιορίζει την ίδια του την ελευθερία και υποβαθμίζει την αξία του ανθρώπου να δρα αυτόνομα, να διαμορφώνει τις επιλογές του και

---

Πρόκειται ωστόσο, για δηλώσεις περιορισμένης αξιοπιστίας, οι οποίες πάντως, δεν αίρουν τον κίνδυνο κατάχρησης. Βλ. T. Kaldani; Z. Prokopets Information Society Department DGI (2022)04, Council of Europe *"PEGASUS SPYWARE and its impacts on human rights"* p.p. 3. Διαθέσιμο στο: https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8 [Ημερομηνία πρόσβασης: 3/1/2023] p.p. 6

[102] Βλ. EDPS (2022) *"Preliminary Remarks on Modern Spyware"*. Διαθέσιμο στο: https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf [Ημερομηνία πρόσβασης: 9/1/2023] σελ. 7 επ.

[103] Μάνεσης, Α. (1982) «*Συνταγματικά Δικαιώματα, Ατομικές Ελευθερίες*», Αθήνα, εκδ. Σάκκουλας σελ. 232

τον τρόπο με τον οποίο παρουσιάζει τον εαυτό του. Η προστασία του ιδιωτικού και οικογενειακού βίου, η προστασία του ασύλου της κατοικίας,[104] ο σεβασμός στην αξία του ανθρώπου,[105] το δικαίωμα ανάπτυξης προσωπικότητας και συμμετοχής στην κοινωνική, οικονομική και πολιτική ζωή[106] και η προστασία του πληροφοριακού αυτοπροσδιορισμού[107] συνδέονται άμεσα με το δικαίωμα στην ιδιωτικότητα και περιορίζονται από την χρήση των κατασκοπευτικών λογισμικών.

Καθώς, μάλιστα, η πραγματικότητα διαψεύδει τις δηλώσεις των κατασκευαστών λογισμικών κατασκοπείας αναφορικά με τον εμπορικό προορισμό των προϊόντων, το ζήτημα λαμβάνει έτι περαιτέρω ανησυχητικές διαστάσεις, κυρίως επειδή οι περιπτώσεις διαπιστωμένων παραβιάσεων σχετίζονται με ευαίσθητα πεδία του δημόσιου βίου. Όπως έχει προαναφερθεί, μεταξύ των θυμάτων περιλαμβάνονται κοινοβουλευτικοί και πολιτικοί αντίπαλοι ισχυρών κυβερνητικών αξιωματούχων, λειτουργοί της δικαιοσύνης, δημοσιογράφοι, ακτιβιστές κ.ά. Δεν είναι συνεπώς, η ετερογονία των σκοπών που ανησυχεί, ούτε μόνο η επεμβατικότητητα των χρησιμοποιούμενων μεθόδων, αλλά καταρχάς, η εκτός κανονιστικού πλαισίου και απολύτως ανεξέλεγκτη δράση τους.

Ακόμη και ξεκινώντας από την παραδοχή της τεχνολογικής ουδετερότητας, παραμένει ως πρόβλημα το γεγονός ότι η χρήση των υπό συζήτηση λογισμικών από τις πολιτειακές αρχές για λόγους αποτελεσματικής πρόληψης κυρίως, πάσχει σε δύο τουλάχιστον, επίπεδα. Κατά πρώτον, της χρήσης τους από τις υπηρεσίες πληροφοριών ή τις επιχειρησιακές αρχές της

---

[104] άρθρο 9 Σ.

[105] άρθρο 2 παρ. 1 Σ.

[106] άρθρο 5 παρ. 1 Σ.

[107] Το δικαίωμα του πληροφοριακού αυτοκαθορισμού ή της αυτοδιάθεσης πληροφοριών αποτελεί την δυνατότητα του ατόμου να γνωρίζει, να αποφασίζει και να συμπροσδιορίζει πότε και υπό ποιες προϋποθέσεις είναι δυνατή η επεξεργασία των πληροφοριών που τον αφορούν. Το άτομο δεν καθίσταται αυτόματα πληροφοριακό αντικείμενο, αλλά αναπτύσσει ελεύθερα την προσωπικότητά του και συμβάλλει στη δημοκρατική διαδικασία και την πληροφοριακή συγκρότηση της πολιτείας. Το δικαίωμα αυτό είναι γνωστό από τη νομολογία του Ομοσπονδιακού Συνταγματικού Δικαστηρίου της Γερμανίας. Αποτελεί ειδικότερη εκδήλωση του γενικού δικαιώματος αυτοδιάθεσης του ατόμου που εγγυώνται τα άρθρα 2 και 5 του Συντάγματος και παράλληλα εμπεριέχεται στο δικαίωμα-πλαίσιο της προσωπικότητας.

πολιτείας δεν προηγείται απόφαση της αρμόδιας – δικαστικής ή ανεξάρτητης – αρχής. Έτσι, η ουσιαστική κρίση για την ανάγκη επέμβασης στο δικαίωμα και η συνακόλουθη στάθμιση που απαιτείται κατά το ελληνικό Σύνταγμα και την ΕΣΔΑ, προϋποθέτουν απόφαση οργάνου που διαθέτει εχέγγυα προσωπικής και λειτουργικής ανεξαρτησίας. Σε καμία περίπτωση δε, τις εγγυήσεις αυτές δε διαθέτουν συλλήβδην τα όργανα της εκτελεστικής εξουσίας (π.χ. αστυνομικοί, τελωνειακοί υπάλληλοι ή στελέχη των υπηρεσιών πληροφοριών), τα οποία φαίνεται να έχουν τον πρώτο και τον τελευταίο λόγο, σε περιπτώσεις χρήσης των πρωτοποριακών κατασκοπευτικών λογισμικών από κρατικές υπηρεσίες.

Στην περίπτωση του λογισμικού Pegasus και του Predator δημοσιογραφικοί κύκλοι και ακτιβιστές τέθηκαν υπό παρακολούθηση με την χρήση των παράνομων αυτών μέσων. Ο ρόλος και η θεσμική θέση αυτών των κοινωνικών ομάδων είναι η ελεύθερη έκφραση απόψεων και η προάσπιση ανθρωπίνων δικαιωμάτων και ελευθεριών. Η παρακολούθηση αυτών κα των οικογενειών του μέσω των κατασκοπευτικών λογισμικών πέραν από παραβίαση της ιδιωτικότητας τους αποτελεί και κατάφωρη παραβίαση της ελευθερίας της έκφρασης και της ελευθερίας του τύπου. Το δικαίωμα στην ελευθερία της έκφρασης και της πληροφόρησης αποτελεί θεμελιώδες δικαίωμα, που θεμελιώνεται στο άρθρο 10 της ΕΣΔΑ[108] και στο άρθρο 5 Σ.[109] και συνδέεται άμεσα με την πεμπτουσία του δημοκρατικού

[108] *«Ελευθερία έκφρασης: 1. Παν πρόσωπον έχει δικαίωμα εις την ελευθερίαν εκφράσεως. Το δικαίωμα τούτο περιλαμβάνει την ελευθερίαν γνώμης ως και την ελευθερίαν λήψεως ή μεταδόσεως πληροφοριών ή ιδεών, άνευ επεμβάσεως δημοσίων αρχών και ασχέτως συνόρων. Το παρόν άρθρον δεν κωλύει τα Κράτη από του να υποβάλωσι τας επιχειρήσεις ραδιοφωνίας, κινηματογράφου ή τηλεοράσεως εις κανονισμούς εκδόσεως αδειών λειτουργίας.*

*2. Η άσκησις των ελευθεριών τούτων, συνεπαγομένων καθήκοντα και ευθύνας δύναται να υπαχθή εις ωρισμένας διατυπώσεις, όρους, περιορισμούς ή κυρώσεις, προβλεπομένους υπό του νόμου και αποτελούντας αναγκαία μέτρα εν δημοκρατική κοινωνία δια την εθνικήν ασφάλειαν, την εδαφικήν ακεραιότητα ή δημοσίαν ασφάλειαν, την προάσπισιν της τάξεως και πρόληψιν του εγκλήματος, την προστασίαν της υγείας ή της ηθικής, την προστασίαν της υπολήψεως ή των δικαιωμάτων των τρίτων, την παρεμπόδισιν της κοινολογήσεως εμπιστευτικών πληροφοριών ή την διασφάλισιν του κύρους και αμεροληψίας της δικαστικής εξουσίας.»*

[109] *«Ελεύθερη ανάπτυξη της προσωπικότητας, προσωπική ελευθερία: 1. Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και*

πολιτεύματος,. Κάθε κράτος οφείλει να προστατεύσει το δικαίωμα αυτό θετικά και αρνητικά, αποφεύγοντας δηλαδή πράξεις που θα το έθεταν ενδεχομένως σε κίνδυνο. Το δικαίωμα αυτό δεν είναι απόλυτο και γι' αυτό η παραβίαση του μπορεί να γίνει μόνο υπό τις προϋποθέσεις που θέτει ο νόμος.[110] Η επιτήρηση των δημοσιογράφων, ακτιβιστών και άλλων σημαντικών προσώπων θέτει σε κίνδυνο την ελευθερία της έκφρασης αυτών, ειδικά όταν διεξάγεται χωρίς τις απαραίτητες δικλείδες ασφαλείας. Παράλληλα, ο περιορισμός της ελευθερίας έκφρασης των δημοσιογράφων αποτελεί και περιορισμό της ελευθερίας έκφρασης του τύπου και κατ' επέκταση περιορισμό την ελευθερίας πληροφόρησης των πολιτών. Κατά αυτόν τον τρόπο η κρατική παρέμβαση είναι τέτοια που μπορεί να παρομοιαστεί με συγκεντρωτικά καθεστώτα που κατευθύνουν τις εξουσίες και παραβιάζουν θεμελιώδη δικαιώματα.[111]

Η παρακολούθηση ακτιβιστών αλλά και απλών πολιτών έχει επίσης συνέπειες στην ελεύθερη ανάπτυξη της προσωπικότητας, δικαίωμα άρρηκτα συνδεδεμένο με την δημοκρατία. Η χρήση των κατασκοπευτικών λογισμικών για παρακολούθηση των ιδεών των πολιτών περιορίζει την ελεύθερη σκέψη και την ίδια την ελεύθερη δράση των πολιτών και έχει ως σκοπό τη δημιουργία μοτίβων συμπεριφοράς ανάλογα με τις επιθυμίες του εκάστοτε ισχυρού. Επιπροσθέτως, ο αντίκτυπος της χρήσης του λογισμικού Pegasus για κατασκοπεία στοχευμένα γυναικών δημιουργεί κοινωνικές ασυμμετρίες και διογκώνει το χάσμα μεταξύ των φύλων.[112] Ακόμη, η χρήση λογισμικών κατασκοπείας για παρακολούθηση και επίθεση

---

*πολιτική ζωή της Χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη.»*

[110] Ο περιορισμός του δικαιώματος στην ελευθερία της έκφρασης μπορεί να γίνει υπό τις προϋποθέσεις του άρθρου 10 παρ. 2 ΕΣΔΑ.

[111] Σχετικά με την χρήση του λογισμικού Pegasus κατά δημοσιογράφων ο σκοπός παρακολούθησης ήταν η αποκάλυψη των δημοσιογραφικών πηγών. Μια τέτοια αποκάλυψη τόσο εμπιστευτικών δεδομένων βάλλει κατά της ελευθερίας του τύπου και κλυδωνίζει την δημοσιογραφική αμεροληψία και την αξιόπιστη πληροφόρηση των πολιτών.

[112] Ο αντίκτυπος της στοχευμένης παρακολούθησης γυναικών αντανακλά τις κοινωνικές ασυμμετρίες μεταξύ των φύλων. Η παρακολούθηση γυναικών μέσω λογισμικών κατασκοπείας μπορεί να οδηγήσει σε παράνομες και ανήθικες συμπεριφορές όπως εκβιασμό και διακίνηση πορνογραφικού υλικού κ.ά. Βλ. Kaldani, T.; Prokopets, Z. Information Society Department DGI (2022)04, Council of Europe *"PEGASUS SPYWARE and its impacts on human rights" ό.π.* p.p. 19

σε πολιτικούς αντιπάλους, αποτελεί σοβαρό κλυδωνισμό της δημοκρατίας. Γίνεται έτσι αντιληπτό ότι πέραν του δικαιώματος στο απόρρητο και της προστασίας των προσωπικών δεδομένων, η χρήση των κατασκοπευτικών λογισμικών δημιουργεί το φαινόμενο του chilling effect σε μια πληθώρα δικαιωμάτων και ελευθεριών, οδηγώντας εν τέλει σε κοινωνικό αποκλεισμό και σε κοινωνίες αυτολογοκρισίας και καχυποψίας.[113]

Εκτός από το δικαίωμα στην προστασία του ιδιωτικού βίου που βάλλεται από τη χρήση παράνομου λογισμικού, σε καθεστώς αδρανοποίησης (chilling effect) περιέρχονται και άλλα δικαιώματα, με πρώτο την ειδικότερη προστασία που απολαύουν τα προσωπικά δεδομένα ως επιμέρους έκφανση του ιδιωτικού βίου. Στην ΕΣΔΑ δεν υφίσταται αυτοτελής διάταξη περί προστασίας προσωπικών δεδομένων, όπως το άρθρο 8 του ΧΘΔΕΕ. Το ΕΔΔΑ έχει ωστόσο, αναγνωρίσει ότι η προστασία των προσωπικών δεδομένων συνδέεται άρρηκτα με την αποτελεσματική άσκηση του δικαιώματος στην ιδιωτική, οικογενειακή ζωή, καθώς επίσης και στην προστασία των επικοινωνιών του.

Σε ειδική πρόσφατη έκθεση του Ευρωπαϊκού Κοινοβουλίου πάντως,[114] επισημαίνεται ότι η έμμεση, αλλά αναπόφευκτη αδρανοποίηση συνεπεία παράνομων λογισμικών αφορά και άλλα δικαιώματα, όπως είναι η ελευθερία της έκφρασης και μάλιστα, στην ειδικότερη διάστασή της που συνδέεται με την άσκηση του δημοσιογραφικού λειτουργήματος ή την ακτιβιστική δράση. Ανεπηρέαστα δεν μένουν επίσης και δικαιώματα των οποίων η άσκηση ανάγεται στον απώτερο πυρήνα της προσωπικότητας, όπως ενδεικτικά η άσκηση της θρησκευτικής ελευθερίας, το δικαίωμα του συνέρχεσθαι και συνεταιρίζεσθαι, καθώς

---

[113] Για παράδειγμα, το δικαίωμα στην υγεία μπορεί επίσης να επηρεαστεί, καθώς τα άτομα μπορεί να αναγκαστούν να απέχουν από το διαμοιρασμό ευαίσθητων δεδομένων υγείας με γιατρούς, από το φόβο μήπως διαρρεύσουν. Εξάλλου η πανδημία δημιούργησε νέους κινδύνους, όπως την εγκατάσταση χωρίς συναίνεση στα κινητά τηλέφωνα πολιτών λογισμικού κατασκοπείας ανίχνευσης επαφών-κρουσμάτων από το Τμήμα Δημόσιας Υγείας της Μασαχουσέτης. Βλ. σχετικά Cawley, G., Boston Herald (2022) *"Massachusetts DPH, Google 'secretly' installed COVID 'spyware' onto 1M phones, lawsuit says"*. Διαθέσιμο στο: https://www.bostonherald.com/2022/11/18/massachusetts-dph-google-secretly-installed-covid-spyware-onto-1m-phones-lawsuit-says/ [Ημερομηνία πρόσβασης: 14/2/2023]. Ακόμα, το ίδιο μπορεί να ισχύσει για τη θρησκευτική ελευθερία και το δικαίωμα του συνέρχεσθαι και συνεταιρίζεσθαι.

[114] Βλ. Kaldani, T.; Prokopets, Z. Information Society Department DGI (2022)04, Council of Europe *"PEGASUS SPYWARE and its impacts on human rights"* ό.π. p.p. 15

ενδεχομένως και η συμμετοχή και αλληλεπίδραση στα κοινωνικά δίκτυα. Ο φόβος δηλαδή, ως υποκείμενη συνθήκη, δρα ανασχετικά, με ενδεχόμενο τελικά, την ακύρωση της βουλητικής λειτουργίας σε πεδία, όπου το υποκείμενο αισθάνεται εκτεθειμένο λόγω της διακινδύνευσης που παράγεται από τη δυναμική χρήση παράνομων λογισμικών.

### 3.3. Η νόμιμη διαδικασία άρσης του απορρήτου (ν. 2225/1994)

Σε αντίθεση με την χρήση παράνομων κατασκοπευτικών λογισμικών ο εθνικός ν. 2225/1994 όριζε τη νόμιμη διαδικασία άρσης του απορρήτου των επικοινωνιών. Πρόκειται για ένα νομοθέτημα που μετά τις τελευταίες εξελίξεις έχει κατακριθεί σε πολλά σημεία. Ο νόμος αυτός που αποτελεί επιταγή του Συντάγματος, όπως προαναφέρθηκε παραθέτει δύο συγκεκριμένες περιπτώσεις στις οποίες μπορεί να διαταχθεί η άρση του απορρήτου των επικοινωνιών εξαιρετικά και όχι ως κανόνας. Το άρθρο 3 αναφέρεται στους λόγους εθνικής ασφάλειας που επιτάσσουν την άρση του απορρήτου, ενώ το άρθρο 4 αναφέρεται στη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, κακουργημάτων και το άρθρο 5 ορίζει τη διαδικασία της άρσης του απορρήτου. Δεδομένου ότι η άρση απορρήτου πρόκειται για μια ειδική ανακριτική πράξη, στο άρθρο 3 υπάρχει μια περιοριστική απαρίθμηση σε ποιους μπορεί να απευθύνεται η αίτηση άρσης του απορρήτου. Στην Ελλάδα η πλειοψηφία των αιτημάτων κατατίθεται στην ΕΥΠ.[115]

Ο βασικός προβληματισμός εντοπίζεται στο γεγονός ότι ο λόγος της εθνικής ασφάλειας είναι μια αόριστη νομική έννοια, η οποία χρειάζεται περαιτέρω εξειδίκευση προκειμένου να διαταχθεί ένα μέτρο τόσο περιοριστικό της ιδιωτικότητας. Επιπλέον, στην Ελλάδα ο μεγαλύτερος όγκος των αιτήσεων για άρση του απορρήτου αφορά την εθνική ασφάλεια. Την απόφαση για την άρση του απορρήτου την παίρνει είτε ο Εισαγγελέας Εφετών μέσα σε 24 ώρες με διάταξη, η οποία πρέπει να περιέχει τα ελάχιστα στοιχεία που ορίζονται στο άρθρο 5 του νόμου. Προς συμμόρφωση με τα καταστατικά κείμενα αλλά και λόγω της σοβαρότητας του αντικειμένου η ύπαρξη ανεξάρτητης αρχής, της ΑΔΑΕ, η οποία εποπτεύει την όλη διαδικασία είναι άκρως σημαντική και ανταποκρίνεται στις απαιτήσεις της λογοδοσίας, του κράτους δικαίου και της δημοκρατίας. Όσον αφορά τους λόγους εθνικής ασφαλείας σε αντίθεση με το ελάχιστο περιεχόμενο που πρέπει να εμπεριέχεται στη διάταξη το άρθρο 3

[115] https://www.nis.gr/el

του νόμου παρ. 2 αναφέρει ότι για λόγους μυστικότητας, όταν η άρση του απορρήτου διατάσσεται για λόγους εθνικής ασφάλειας αυτοί μπορούν να παραλείπονται. Τέλος, στο ά. 5 του νόμου ορίζεται το χρονικό διάστημα για το οποίο μπορεί να παραταθεί η άρση του απορρήτου. Ενώ, για την άρση απορρήτου για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων η χρονική διάρκεια δεν μπορεί να υπερβαίνει τους 10 μήνες, στην περίπτωση της εθνικής ασφάλειας δεν υπάρχει ανώτατο χρονικό όριο για την παράταση. Γίνεται έτσι αντιληπτό ότι στο πεδίο της εθνικής ασφάλειας καταλείπεται μια ευρεία ελευθερία στο κράτος να παρεμβαίνει στο απόρρητο των πολιτών, αφού και ο ίδιος ο όρος είναι αρκετά γενικός και δεν εξειδικεύεται με καμία αιτιολογία και η άρση του απορρήτου μπορεί να συντελείται επ' αόριστο. Τα υποκείμενα μπορεί να μην πληροφορηθούν ποτέ ότι οι συνομιλίες τους έχουν παρακολουθηθεί, αφού για τους λόγους της εθνικής ασφάλειας δεν υπάρχει υποχρέωση ενημέρωσης όπως υπάρχει στην περίπτωση της διακρίβωσης εγκλημάτων,[116] ρύθμιση που είχε κατακριθεί ως αντισυνταγματική λόγω της αποστέρησης του δικαιώματος της αποτελεσματικής δικαστικής προστασίας από τα υποκείμενα.[117]

Στο άρθρο 4 του νόμου γίνεται μια σχεδόν αποκλειστική απαρίθμηση των εγκλημάτων για τη διακρίβωση των οποίων μπορεί να διαταχθεί η άρση του απορρήτου κι αυτό γιατί το δικαίωμα στο απόρρητο είναι απαραβίαστο. Το παράδοξο αυτής της διάταξης είναι ότι παρά την σχεδόν numerus clausus απαρίθμηση, προστέθηκαν επιπλέον τα οικονομικά εγκλήματα χωρίς να ορίζεται ποια ακριβώς εγκλήματα συμπεριλαμβάνονται τυχόν στην κατηγορία αυτή και αν εμπίπτουν σε αυτήν την κατηγορία και πλημμελήματα. Σε αντίθεση με τους λόγους εθνικής ασφάλειας στην περίπτωση της διακρίβωσης των ιδιαίτερα ειδεχθών εγκλημάτων η άρση του απορρήτου δε γίνεται εξ αρχής, αλλά απαιτείται και αιτιολογημένη γνώμη του Δικαστικού Συμβουλίου, απόρροια της αρχής της αναλογικότητας. Η αιτιολογία πρέπει γενικά να είναι συγκεκριμένη και δεν αρκεί η απλή παράθεση νομικών όρων. Η δυσκολία με τη διακρίβωση των εγκλημάτων έγκειται στο ότι υπάρχουν ορφανά εγκλήματα, που οι δράστες είναι άγνωστοι και γι' αυτούς δεν μπορεί να γίνει άρση του απορρήτου σε

[116] άρθρο 5 παρ. 9 ν. 2225/1994

[117] Ράμμος, Χ., Γκρίτζαλης, Σ., Παπανικολάου, Α., (2021) «*Αντίθεση του άρθρου 87 Ν. 4790/2021 προς τις εγγυήσεις της ΕΣΔΑ για διαφύλαξη του απορρήτου των επικοινωνιών*». Διαθέσιμο στο: https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/ [Ημερομηνία πρόσβασης: 12/1/2023]

αόριστο αριθμό, σε αντίθεση με τους λόγους εθνικής ασφάλειας για τους οποίους ο νόμος δεν ορίζει ότι χρειάζεται όνομα για να διαταχθεί η άρση. Το υποκείμενο μπορεί εφόσον πρόκειται για άρση απορρήτου στο πλαίσιο της διακρίβωσης εγκλήματος και εφόσον το μέτρο δεν βρίσκεται σε ισχύ και δε διακυβεύεται ο σκοπός του, δηλαδή η διακρίβωση της τέλεσης ιδιαίτερου σοβαρού εγκλήματος να αιτηθεί στην ΑΔΑΕ να ενημερωθεί για την άρση του απορρήτου του. Την αποφασιστική αρμοδιότητα την έχει ο Εισαγγελέας και ο ρόλος της ΑΔΑΕ είναι κυρίως εξασφαλιστικός.

### 3.4. Τα κριτήρια του ΕΔΔΑ: Η σημασία της αρχής της αναλογικότητας

Η προβληματική που αναπτύχθηκε σχετικά με τους περιορισμούς του δικαιώματος στο απόρρητο των επικοινωνιών αφορά το κατά πόσο μπορεί η άρση του απορρήτου ενός προσώπου να δικαιολογηθεί από τους λόγους της διακρίβωσης ενός εγκλήματος αλλά και περισσότερο τους λόγους εθνικής ασφάλειας. Στην περίπτωση δε των κατασκοπευτικών λογισμικών τα πράγματα περιπλέκονται ακόμη περισσότερο καθώς με την χρήση τους καταρρίπτονται όλες οι νομικές εγγυήσεις προστασίας του απορρήτου και των προσωπικών δεδομένων και η επέμβαση στην ιδιωτική σφαίρα του ατόμου είναι τόσο μεγάλη που δύσκολα μπορεί να δικαιολογηθεί. Ωστόσο, η ίδια η νομοθεσία και η νομολογία του ΕΔΔΑ έχει θέσει δικλείδες ασφαλείας στην περίπτωση περιορισμού της ιδιωτικότητας των ατόμων, που πολλοί θεωρούν ότι μπορεί να φανούν χρήσιμες στην προσπάθεια εξισορρόπησης της αλόγιστης χρήσης κατασκοπευτικών λογισμικών και των δικαιωμάτων των πολιτών. Ο ίδιος ο θεμιτός χαρακτήρας των περιορισμών, στους οποίους υπόκειται το δικαίωμα στην προστασία του ιδιωτικού βίου, σύμφωνα με το άρθρο 8 ΕΣΔΑ, συναρτάται με το μέτρο, «*το οποίον εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον, διά την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων*». Ομοίως και στο άρθρο 19 του ελληνικού Συντάγματος, σε συνδυασμό με τις διατάξεις του σχετικού εκτελεστικού νόμου[118]

[118] Ν. 2225/1994 (ΦΕΚ 121Α/20.07.1994)

συνάγεται ότι ο περιορισμός του επικοινωνιακού απορρήτου νοείται μόνο ως αναλογικό και έσχατο μέτρο.[119]

Η νομοθετική αυτή διατύπωση έχει απασχολήσει σε πλείστες υποθέσεις και τη νομολογία του ΕΔΔΑ. Το Δικαστήριο έχει συγκεκριμενοποιήσει τα κριτήρια με τα οποία μπορεί να περιοριστεί το ανωτέρω δικαίωμα.[120] Σε γενικές γραμμές το δίπολο του απασχολεί το ΕΔΔΑ κινείται γύρω από την ανάγκη εξασφάλισης διαφάνειας και της μυστικότητας των μέτρων ως απαίτηση της αποτελεσματικότητας της παρακολούθησης.[121] Αξιολογώντας ωστόσο, τον υψηλό βαθμό εξειδίκευσης και τεχνολογικής πολυπλοκότητας των σύγχρονων μεθόδων κατασκοπείας, το ΕΔΔΑ εκτιμά ήδη από τις αρχές της προηγούμενης δεκαετίας ότι η αυτοπροστασία των σύγχρονων κρατών έναντι τέτοιων απειλών –π.χ. της τρομοκρατίας –, καθιστά αναπόφευκτα ορισμένο βαθμό ανοχής ως προς την αδιαφάνεια των μέτρων παρακολούθησης. Έτσι, η εθνική ασφάλεια και η αντιμετώπιση της βαριάς εγκληματικότητας συνιστούν καταρχάς, συγγνωστό λόγο και αποδεκτή δικαιολογητική βάση σε σχέση με τον περιορισμό του δικαιώματος. Η δε αναλογικότητα του μέτρου εν προκειμένω, πρέπει κατά το ΕΔΔΑ, να συμβαδίζει με την «απόλυτη αναγκαιότητα για την προστασία των δημοκρατικών θεσμών».[122] Μόνο δηλαδή, η αναζήτηση κρίσιμων πληροφοριών νοείται ως επαρκώς νομιμοποιητική βάση του περιορισμού. Οτιδήποτε λιγότερο ή ποιοτικά διαφορετικό ελέγχεται ως προς την καταχρηστικότητα της έντασης παρέμβασης στο απόρρητο.[123]

---

[119] Βλ. ειδικότερα, στο άρθρο 4 παρ. 2 του νόμου που αφορά το πλαίσιο άρσης του απορρήτου για τη διακρίβωση των σοβαρών αδικημάτων που απαριθμούνται στη διάταξη: «*Η άρση στις περιπτώσεις αυτές είναι επιτρεπτή μόνο αν αιτιολογημένα το αρμόδιο δικαστικό συμβούλιο διαπιστώσει ότι η διερεύνηση της υπόθεσης ή η εξακρίβωση του τόπου διαμονής του κατηγορουμένου είναι αδύνατη ή ουσιωδώς δυσχερής χωρίς αυτήν».*

[120] Βλ. ΕΔΔΑ *Szabó and Vissy v. Hungary* 12 January 2016, παρ. 72-73, *Dragojević v. Croatia*, 15 January 2015, παρ. 94, *Zakharov v. Russia* ό.π., παρ. 272, Dumitru *Popescu c. Roumanie* (nº 2) ό.π., παρ. 68 επ.

[121] Βλ. Kaldani, T.; Prokopets, Z. Information Society Department DGI (2022)04, Council of Europe "PEGASUS SPYWARE and its impacts on human rights" ό.π. p.p. 16 επ.

[122] Αξίζει να σημειωθεί ότι η αρχή της αναλογικότητας θεσπίζεται και στο ελληνικό Σύνταγμα στο ά. 25 ως ειδικότερη έκφανση του κράτους δικαίου

[123] Βλ. ΕΔΔΑ *Szabó and Vissy v. Hungary*, ό.π. παρ. 72-73.

Το ΕΔΔΑ δεν εθελοτυφλεί στην υψηλή εξειδίκευση και τεχνική αρτιότητα των σύγχρονων μεθόδων κατασκοπείας που μετέρχονται όσοι επιβουλεύονται το έννομο αγαθό της εθνικής ασφάλειας ή της δημόσιας τάξης.[124] Η εξέλιξη αυτή της τεχνολογίας που οδηγεί σε πολλαπλασιασμό των διαθέσιμων μέσων παρακολούθησης καθιστά το δικαίωμα ακόμη πιο ευάλωτο και δυσχερέστερες κατά συνέπεια, τις αναγκαίες δικαστικές σταθμίσεις. Πολλώ δε μάλλον στην περίπτωση των υπό συζήτηση παράνομων λογισμικών, όπου την εγγενή μυστικότητα της διαδικασίας, ενισχύει ο μυστικός τρόπος λειτουργίας και χρήσης τους.[125]

Αυτά τα έξυπνα λογισμικά ακριβώς λόγω των τεχνικών τους χαρακτηριστικών και του βαθμού παρείσφρησης στο δικαίωμα, εγείρουν σημαντικές επιφυλάξεις ως προς τη στοιχειοθέτηση της αναγκαιότητάς τους, όταν επιδιώκεται η χρήση τους από κρατικές αρχές. Κατά πρώτον, όπως έχει ήδη επισημανθεί, το έλλειμμα συνίσταται στην απουσία προηγούμενης απόφασης – εκ μέρους της δικαστικής ή άλλης ανεξάρτητης – αρχής. Δεν είναι δηλαδή, δυνατόν να αξιολογηθεί η αναγκαιότητα του μέτρου δεδομένου ότι ελλείπει η προηγούμενη πραγματολογική αποτύπωση των γεγονότων εκείνων, τα οποία υπό κανονικές συνθήκες, θα ανέμενε κανείς να αχθούν ενώπιον του Δικαστή προκειμένου να πιστοποιηθεί η αδήριτη αναγκαιότητα για τη λήψη του μέτρου. Δηλαδή, ελλείπει η δικαστική στάθμιση ως προς τη δυνατότητα εκπλήρωσης του επιδιωκόμενου σκοπού με άλλο λιγότερο επαχθές ως προς τον βαθμό επέμβασής του, μέτρο, οι ειδικότερες δηλαδή προϋποθέσεις που συνιστούν την αρχή της αναλογικότητας.

Σε ό,τι λοιπόν αφορά τη συμβατότητά τους με την αρχή της αναλογικότητας, αξίζει να επισημανθεί καταρχάς, ότι η πρόσβαση στις «έξυπνες» συσκευές που διαθέτει η συντριπτική πλειονότητα των κατόχων κινητών τηλεφώνων σήμερα, θέτει από μόνη της ένα επί της αρχής ζήτημα. Αυτό συνίσταται στο γεγονός ότι όπως έχει ήδη εκτεθεί, οι συσκευές αυτές αποτελούν αποθετήριο πληθώρας δεδομένων – ακόμα και ειδικών κατηγοριών ή ευαίσθητων δεδομένων–, τα οποία μετά την μόλυνση από λογισμικά της κατηγορίας

---

[124] «*Highly sophisticated forms of espionage and by terrorism*» Βλ. *Big Brother Watch and others v. The United Kingdom*, 25 May 2021, παρ. 323 επ., *Szabó and Vissy v. Hungary* ό.π. παρ. 80, *Klass and others v. Germany*, ό.π. παρ. 48.

[125] Βλ. Kaldani, T.; Prokopets, Z. Information Society Department DGI (2022)04, Council of Europe "PEGASUS SPYWARE and its impacts on human rights" ό.π. p.p. 10 επ.

Pegasus, Predator κ.ά., καθίστανται προσβάσιμα ολοκληρωτικά στους επίδοξους εισβολείς. Εδώ, λοιπόν, παραμένει αμφίβολο ή ορθότερα, μάλλον προσήκει αρνητικής απάντησης αν και κατά πόσο για να υπηρετηθεί ο επιδιωκόμενος σκοπός εθνικής ασφάλειας ή ποινικής διερεύνησης, απαιτείται πρόσβαση στο σύνολο αδιακρίτως των διατηρούμενων εντός της συσκευής δεδομένων. Με άλλα λόγια, μοιάζει να βάλλεται ο πυρήνας του δικαιώματος, καθώς το υποκείμενο δικαίου και φορέας των πληττόμενων δεδομένων αποξενώνεται ολοσχερώς από την ουσία του δικαιώματος – μέτρο που εμφανώς αναιρεί την αρχή της αναλογικότητας, κατά τα εννοιολογικά της χαρακτηριστικά –.[126]

Είναι εξάλλου χαρακτηριστικό ότι σε πολλές αποφάσεις Του[127] εμμένει ρητά στην απαίτηση ύπαρξης άδειας από Ανεξάρτητη Αρχή ειδικά στην περίπτωση των μυστικών παρακολουθήσεων, προκειμένου να αποδεικνύεται η αναγκαιότητα και η αποτελεσματικότητα αυτού του τόσο παρεμβατικού στο δικαίωμα μέσου. Με την άδεια της αρχής πρέπει να αποδεικνύεται η ύπαρξη εύλογης υποψίας του συγκεκριμένου προσώπου που τίθεται υπό παρακολούθηση, με συγκεκριμένη αναφορά των γεγονότων που συντελούν στη δημιουργία υπόνοιας για τέλεσης σοβαρών εγκλημάτων ή για διακινδύνευση της εθνικής ασφάλειας της εκάστοτε χώρας. Επιπλέον, το ΕΔΔΑ έχει τονίσει την απαίτηση το μέτρο να ανταποκρίνεται σε αυτό που θεωρείται αναγκαίο σε μια δημοκρατική κοινωνία. Με αυτόν τον τρόπο τονίζει την ανάγκη ύπαρξης της αρχής της αναλογικότητας με όλα τα επιμέρους χαρακτηριστικά της ήτοι την εν στενή έννοια αναλογικότητα, την αρχή της προσφορότητας και καταλληλότητας του μέσου προς τον επιδιωκόμενο σκοπό, ο οποίος δεν μπορεί να επιτευχθεί με λιγότερο επαχθές μέτρο και την αρχή της αναγκαιότητας.[128]

Στη στοχευμένη παρακολούθηση, δηλαδή στην παρακολούθηση συγκεκριμένων προσώπων το ΕΔΔΑ έχει κρίνει ότι χρειάζονται ορισμένες ελάχιστες προϋποθέσεις, ώστε να θεωρείται νόμιμη. Έτσι, πρέπει να υφίσταται εθνικός νόμος που να προβλέπει την άρση του απορρήτου. Ο νόμος αυτός θα πρέπει να είναι σύμφωνος με τους κανόνες δικαίου μιας δημοκρατικής κοινωνίας, δηλαδή θα πρέπει να πληροί ορισμένα ποιοτικά κριτήρια. Ο νόμος λοιπόν θα πρέπει να είναι προσβάσιμος σε όλους τους πολίτες, σαφής για όλους και προβλέψιμος. Γι' αυτούς τους λόγους θα πρέπει να γίνεται ρητή αναφορά στη φύση και την

[126]EDPS (2022) *"Preliminary Remarks on Modern Spyware"*, ό.π. σελ. 8

[127] Βλ. ΕΔΔΑ Roman Zakharov v. Russia, ό.π. και Szabó and Vissy v. Hungary ό.π.

[128] Βλ. ΕΔΔΑ Klass and Others v. Germany, ό.π.

κατηγορία των παραβιάσεων για τη διακρίβωση ων οποίων μπορεί να διαταχθεί η άρση του απορρήτου αλλά και στις κατηγορίες των υποκειμένων των οποίων οι συνομιλίες μπορεί να επιτηρούνται. Θα πρέπει επίσης να ορίζεται επαρκώς η διάρκεια του μέτρου και η διαδικασία παρακολούθησης και αποθήκευσης των δεδομένων που συλλέγονται, τα μέτρα που παίρνει το κράτος όταν τα δεδομένα μεταφέρονται σε τρίτα μέρη, ποιος θα έχει την εποπτεία του μέτρου με τη θέσπιση ανεξάρτητης Αρχής αλλά και τι θα γίνει μετά το τέλος της παρακολούθησης (π.χ. διαγραφή και καταστροφή δεδομένων) και τα δικαιώματα γνωστοποίησης και αποκατάστασης των υποκειμένων.[129]

### 3.5. Ποινική προστασία από την χρήση των κατασκοπευτικών λογισμικών

Τα κατασκοπευτικά λογισμικά ανάλογα με το έννομο αγαθό που προσβάλλουν είναι υπεύθυνα για μια σειρά αξιόποινων συμπεριφορών. Πλέον το άρθρο 12 του ν. 5002/2022 εισήγαγε στον ελληνικό ποινικό κώδικα το άρθρο 370ΣΤ. [130] Μέχρι σήμερα η πώληση , η διακίνηση και η προμήθεια συσκευών παρακολούθησης ή παρόμοιων λογισμικών που χρησιμεύουν στην παρακολούθηση και στην υποκλοπή δεδομένων δεν ποινικοποιούνταν. Πλέον, με την εισαγωγή του εν λόγω άρθρου δεν ποινικοποιείται απλά η διακίνηση τους ως πλημμέλημα, αλλά και η κατοχή τους χωρίς να έχουν τεθεί σε χρήση ακόμα. Μάλιστα αυτού του είδους οι συσκευές σύμφωνα με το άρθρο πρέπει να προορίζονται για την τέλεση των

---

[129] Βλ. ΕΔΔΑ *Huvig v. France*, 24 April 1990; *Kruslin v. France*, 24 April 1990; *Valenzuela Contreras v. Spain,* 30 July 1998, *Weber and Saravia v. Germany* 29 June 2006.

[130] *«Άρθρο 370ΣΤ Απαγόρευση διακίνησης λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων:*

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

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

εγκλημάτων του οικείου κεφαλαίου του ελληνικού Ποινικού Κώδικα, ήτοι των προσβολών του ατομικού απορρήτου και του απορρήτου της επικοινωνίας.

Το απόρρητο των επικοινωνιών προστατεύεται με το άρθρο 370Α ΠΚ.[131] Η πρόβλεψη για την προστασία του απορρήτου των τηλεφωνημάτων θεσπίστηκε στην ελληνική έννομη τάξη με τον Ν. 1291/1982, ενώ έως τότε στον Ποινικό Κώδικα υπήρχε πρόβλεψη με το άρθρο 250 ΠΚ ποινικών κυρώσεων αναφορικά μόνο με τους τηλεφωνικούς υπαλλήλους.[132] Μέχρι σήμερα, το ά. 370Α έχει υποστεί πολλές τροποποιήσεις με τελευταία αυτή που ήρθε με το ν. 5002/2022, γεγονός το οποίο δικαιολογείται από τη διαρκή εξέλιξη της τεχνολογίας και των μέσων που χρησιμοποιούνται γι' αυτήν. Η ποινική προστασία του απορρήτου των επικοινωνιών και

---

[131] *«Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας: 1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών σταθερής ή κινητής τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή δεδομένα επικοινωνίας (κίνησης και θέσης) τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον, χωρίς τη ρητή συναίνεση του τελευταίου.*

*2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.*

*3. Όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.*

*4. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή.*

*5. Αν οι πράξεις των παραγράφων 1 και 3 συνιστούν παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, επιβάλλεται κάθειρξη.»*

[132] Βλ. άρθρο 250 καταργηθέντος με τον Ν. 4619/2019 ΠΚ «Παραβάσεις των τηλεφωνικών υπαλλήλων»

συνεπώς της ιδιωτικής ζωής του ατόμου που εκφράζεται μέσω της επικοινωνίας, καταδεικνύει τη μεγάλη σημασία της πραγματικής προστασίας του εννόμου αγαθού αυτού, την οποία ο νομοθέτης προσπαθεί να επιτύχει με τις διαρκείς τροποποιήσεις του άρθρου 370Α ΠΚ, έως και το 2022, ώστε να εναρμονίζεται η διάταξη αυτή με τα σύγχρονα τεχνολογικά δεδομένα. Άλλωστε, την ποινική προστασία του απορρήτου επιτάσσει και η Σύμβαση της Βουδαπέστης και η Οδ. 2013/40/ΕΕ όπως αναφέρθηκε ανωτέρω.

Ο ν. 3674/2008 πλήρωσε το κενό που δημιουργήθηκε λόγω της αποκάλυψης περίπου 100 τηλεφωνικών υποκλοπών σε βάρος πολιτών και κρατικών λειτουργών, μέχρι και του πρωθυπουργού της χώρας, το έτος 2005.[133] Έτσι, ενισχύθηκε το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, μέσω της θέσπισης συγκεκριμένων υποχρεώσεων για τους παρόχους, π.χ. την υποχρέωση κατάρτισης και εφαρμογής ειδικού σχεδίου πολιτικής ασφάλειας, την υποχρέωση καταγραφής των διαχειριστικών λειτουργιών που επιχειρούνται στο λογισμικό κάθε ψηφιακού κέντρου μεταγωγής[134] κ.ά., μέσω της θέσπισης αστικής ευθύνης[135] και της περιγραφής του εθνικού σχεδίου ασφάλειας των επικοινωνιών.[136] Επιπλέον, με το άρθρο 10 του Ν. 3674/2008 διευρύνθηκε το αξιόποινο του άρθρο 370Α ΠΚ, με το οποίο προστέθηκε στην αντικειμενική υπόσταση του εγκλήματος της παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών η αθέμιτη παρέμβαση σε «δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού», προκειμένου να συμπεριλάβει τις νέες τεχνολογικές εξελίξεις .

Τον ίδιο σκοπό εξυπηρετεί και η θέσπιση του άρθρο 370Ε ΠΚ,[137] που ενσωματώνει το άρθρο 3 της Σύμβασης της Βουδαπέστης και το άρθρο 6 της Οδ. 2013/40/ΕΕ. Το άρθρο αφορά τα

---

[133] Ι. Ιγγλεζάκης «Δίκαιο Πληροφορικής», έκδ. Σάκκουλα, 2018, σελ. 310.

[134] Βλ. άρθρο 3 Ν. 3674/2008 «Ειδικό σχέδιο πολιτικής ασφάλειας», και άρθρο 5 Ν. 3674/2008 «Καταγραφή διαχειριστικών λειτουργιών».

[135] Βλ. άρθρο 12 Ν. 3674/2008 «Αστική Ευθύνη»

[136] Βλ. άρθρο 13 Ν. 3674/2008 «Εθνικό σχέδιο ασφάλειας ηλεκτρονικών επικοινωνιών»

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

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

κλειστά κυκλώματα παρακολούθησης που χρησιμοποιούνται από τις μυστικές υπηρεσίες όπως την ΕΥΠ και την αστυνομία για παρακολούθηση. Με το άρθρο 9 του ίδιου νόμου προστέθηκε στον Ποινικό Κώδικα το άρθρο 292Α[138] με τίτλο «εγκλήματα κατά της

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

*[138] «1. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση σε σύνδεση ή σε δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, και με τον τρόπο αυτόν θέτει σε κίνδυνο την ασφάλεια των τηλεφωνικών επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή. Αν ο υπαίτιος της πράξης του προηγούμενου εδαφίου είναι ο εργαζόμενος ή συνεργάτης του παρόχου υπηρεσιών τηλεφωνίας, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή. Με την ποινή του προηγουμένου εδαφίου τιμωρείται και ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπός του ο οποίος αθέμιτα θέτει σε κίνδυνο την ασφάλεια των τηλεφωνικών επικοινωνιών.*

*2. Ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπος αυτού, ο οποίος παραβιάζει διάταξη κανονισμού της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) ή όρο της Γενικής Άδειας ή του δικαιώματος χρήσης ραδιοσυχνότητας ή του δικαιώματος χρήσης αριθμού, που αναφέρονται στην ασφάλεια των ηλεκτρονικών επικοινωνιών, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή.*

*3. Ο πάροχος υπηρεσιών τηλεφωνίας ή ο νόμιμος εκπρόσωπος αυτού ή ο κατά τον νόμο υπεύθυνος για τη διασφάλιση του απορρήτου των επικοινωνιών, που παραλείπει να λάβει τα αναγκαία μέτρα για την αποτροπή πράξης της παρ. 1, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή, εφόσον η πράξη τελέστηκε ή έγινε απόπειρα τέλεσής της, ανεξάρτητα αν θα τιμωρηθεί ο υπαίτιος.*

*4. Αν ο υπαίτιος των πράξεων των προηγούμενων παραγράφων είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον, τιμωρείται με φυλάκιση τουλάχιστον τριών (3) ετών και χρηματική ποινή. Εφόσον το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ, ο υπαίτιος τιμωρείται με κάθειρξη έως δέκα (10) έτη και χρηματική ποινή. Αν από τις πράξεις των προηγούμενων παραγράφων μπορεί να τεθούν σε κίνδυνο θεμελιώδεις αρχές και θεσμοί του Πολιτεύματος, όπως μνημονεύονται στο άρθρο 134 του Ποινικού Κώδικα ή απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή στην ασφάλεια εγκαταστάσεων κοινής ωφέλειας, επιβάλλεται κάθειρξη.*

*5. Όποιος αθέμιτα διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει προς εγκατάσταση ειδικά τεχνικά μέσα για την τέλεση των πράξεων της παρ. 1 ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους τιμωρείται με φυλάκιση έως δύο (2) έτη ή χρηματική ποινή.»*

ασφάλειας των τηλεφωνικών επικοινωνιών».[139] Στο έγκλημα αυτό ποινικοποιείται η χωρίς δικαίωμα πρόσβαση στο δίκτυο υπηρεσιών τηλεφωνίας με προστατευτέο έννομο αγαθό τόσο την ασφάλεια των επικοινωνιών όσο και το απόρρητο.[140]

Επιπλέον, όπως και στα ευρωπαϊκά νομοθετήματα έτσι και στον ελληνικό ποινικό κώδικα το hacking τυποποιείται ως αξιόποινη συμπεριφορά στο άρθρο 370Δ παρ. 1.[141] Στην παράγραφο αυτή ποινικοποιείται η χωρίς δικαίωμα αντιγραφή ή χρήση προγραμμάτων ηλεκτρονικού υπολογιστή, ενώ στις παρ. 2 και 3 του ίδιου άρθρου[142] ποινικοποιείται η παράνομη πρόσβαση στο σύστημα. Το προστατευτέο έννομο αγαθό αυτών των διατάξεων είναι κατ' άλλους το απόρρητο των δεδομένων είτε η ασφάλεια των συστημάτων. Η κύρια διαφορά του άρθρο 370Δ παρ. 1 ΠΚ από το άρθρο 370Γ ΠΚ[143] είναι ότι το πρώτο αφορά την

---

[139]Βλ. άρθρο 9 Ν. 3674/2008 «Τροποποιήσεις και προσθήκη άρθρου 292Α στον Ποινικό Κώδικα»

[140] Η χωρίς δικαίωμα πρόσβαση σε σύνδεση, δίκτυο, σύστημα λογισμικού παροχής υπηρεσιών τηλεφωνίας αφορά τόσο την κινητή τηλεφωνία αλλά και οποιαδήποτε διαθέσιμη επικοινωνία στο κοινό μέσω δικτύων παροχής υπηρεσιών τηλεφωνίας. Βλ. ΑΠ 916/2019

[141] *«1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.»*

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

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

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

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

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

αντιγραφή ή χρήση απόρρητων δεδομένων, θέτοντας ως βάση το απόρρητο κι όχι την ασφάλεια των δεδομένων.[144]

Όταν η χρήση των κατασκοπευτικών λογισμικών στοχεύει στην παρακώλυση της λειτουργίας του συστήματος π.χ. με τον αποκλεισμό του χρήστη από την πρόσβαση στο σύστημα ή την καταστροφή των αρχείων του τότε, μπορεί να στοιχειοθετηθεί το έγκλημα του άρθρο 292Β ΠΚ.[145] Η διακεκριμένη μορφή της παρ. 2 στοιχ. α αφορά την τέλεση του εγκλήματος με εργαλεία που στοχεύουν κατά βάση σε τέτοιες επιθέσεις όπως τα κατασκοπευτικά λογισμικά. Στον ποινικό κώδικα ποινικοποιείται στο άρθρο 292Γ[146] και η

---

[144] Επιπλέον, η πρόσβαση στα δεδομένα μπορεί να είναι νόμιμη π.χ. ο χρήστης να έχει συναινέσει στην εγκατάσταση ενός λογισμικού ή να έχει παραχωρήσει τους κωδικούς του.. Αν δεν είναι νόμιμη τότε υφίσταται και το έγκλημα της παράνομης πρόσβασης στα δεδομένα 370Β ή 370Δ παρ. 2 και 3.

[145] *«Παρακώλυση λειτουργίας πληροφοριακών συστημάτων:*

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

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

[146] *«Με φυλάκιση έως δύο έτη ή χρηματική ποινή τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκλημάτων του άρθρου 292 Β, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος.»*

κακή χρήση συσκευών, ειδικότερα προγραμμάτων υπολογιστών όπως λογισμικών που σχεδιάστηκαν για την τέλεση του άρθρο 292Β ΠΚ. Ειδικότερη διάταξη αποτελεί το άρθρο 292Ε ΠΚ,[147] που αφορά την παρακώλυση των τηλεπικοινωνιών μέσω της παρέμβαση σε υλικό πράγμα συσκευή, σύστημα ή δεδομένα.

### 3.6. Οι ρυθμίσεις της Οδ. 2002/58/ΕΚ και του Νόμου 3471/2006 σχετικά με τα λογισμικά κατασκοπείας

Η Οδ. 2002/58/ΕΚ[148] όπως αποκαλείται «ePrivacy Directive» (Οδηγία ePrivacy), η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον ν. 3471/2006 ρυθμίζει τους κανόνες για τις επικοινωνίες των πολιτών των κρατών-μελών της ΕΕ. Η εν λόγω οδηγία ήταν αυτή που έθεσε ουσιαστικά τα θεμέλια για την ικανοποιητική προστασία των δεδομένων στο πεδίο των επικοινωνιών, καλύπτοντας τις επικοινωνίες που λαμβάνουν χώρα τόσο μέσω σταθερής όσο και κινητής τηλεφωνίας αλλά και μέσω διαδικτύου. Μάλιστα στο άρθρο 95 του ΓΚΠΔ ορίζεται ρητά ότι ο ίδιος κανονισμός *«δεν επιβάλλει πρόσθετες υποχρεώσεις σε φυσικά ή νομικά πρόσωπα σε σχέση με την επεξεργασία όσον αφορά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό σε δημόσια δίκτυα επικοινωνίας στην Ένωση σε σχέση με θέματα τα οποία υπόκεινται στις ειδικές υποχρεώσεις με τον ίδιο στόχο που ορίζεται στην οδηγία 2002/58/ΕΚ»*. Ωστόσο, η ραγδαία τεχνολογική εξέλιξη στις ηλεκτρονικές επικοινωνίες, κυρίως με τη χρήση των νέων μορφών επικοινωνίας (π.χ. μέσω messenger, viber κ.λπ.), με τη διασύνδεση μηχανών και υπολογιστικών συστημάτων για την επίτευξη

---

[147] *«Παρακώλυση των τηλεπικοινωνιών: 1. Όποιος παρεμποδίζει ή διαταράσσει σε μεγάλη έκταση ή για μεγάλο χρονικό διάστημα τη λειτουργία εγκατάστασης παροχής στο κοινό υπηρεσιών τηλεφωνίας ή ηλεκτρονικών επικοινωνιών και ιδίως του διαδικτύου με αθέμιτη παρέμβαση σε πράγμα ή σε σύστημα πληροφοριών ή σε ηλεκτρονικά δεδομένα που εξυπηρετούν τη λειτουργία αυτής, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή.*

*2. Η παράγραφος 2 του προηγούμενου άρθρου εφαρμόζεται και για την πράξη της παραγράφου 1.*

*3. Αν η πράξη τελέστηκε από αμέλεια, επιβάλλεται χρηματική ποινή ή παροχή κοινωφελούς εργασίας.»*

[148] Οδ. 2002/58/ΕΚ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) Διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002L0058&from=EL [Ημερομηνία πρόσβασης: 12/1/2023]

επικοινωνίας, με την διεύρυνση του διαδικτύου των πραγμάτων και με την ανάπτυξη της τεχνητής νοημοσύνης είχε ως επακόλουθο τον εκσυγχρονισμό και τη διεύρυνση του πεδίου που κάλυπτε η οδηγία αλλά και την «αυστηροποίηση» των κανόνων μέσω ενός πιο δεσμευτικού και ενιαίου πλαισίου.

Σημαντική ήταν η θέσπιση του ν. 3431/2006 «Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις» και του ν. 3471/2006,[149] όπως τροποποιήθηκε με τον ν. 4070/2012, με τον οποίο, ενσωματώθηκε στην ελληνική έννομη τάξη η ePrivacy Directive και ο οποίος στοχεύει στην προστασία θεμελιωδών δικαιωμάτων των προσώπων και κυρίως της ιδιωτικής τους ζωής καθώς και τη θέσπιση των προϋποθέσεων εκείνων που θα συμβάλουν στην ορθή επεξεργασία των δεδομένων προσωπικού χαρακτήρα και στη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών. Ο νόμος αυτός εξακολουθεί να ισχύει στην ελληνική έννομη τάξη και στα άρθρα 4 και 5 απαγορεύει την χρήση δικτύων ηλεκτρονικών επικοινωνιών για τις αποθήκευση ηλεκτρονικών πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό του χρήστη, ιδίως με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων κ.ά. Εντούτοις, επιτρέπει την τεχνικής φύσεως αποθήκευση ή πρόσβαση μέσω αυτών όταν αποκλειστικός σκοπός είναι η διαβίβαση μιας επικοινωνίας μέσω δικτύου ή όταν αυτή είναι αναγκαία για την παροχή ζητηθείσας υπηρεσίας από τον χρήστη ή όταν εξυπηρετεί θεμιτούς σκοπούς.[150]

Στο άρθρο 4 παρ.2 του ν. 3471/2006 απαγορεύεται η άνευ αδείας ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης. Αυτού του είδους οι δραστηριότητες είναι εφικτές με τη λειτουργία διατάξεων όπως τα κατασκοπευτικά λογισμικά, δικτυακοί «κοριοί», κρυφά αναγνωριστικά στοιχεία. Η απαγόρευση αυτή ενισχύεται με την προσθήκη ότι η πρόσβαση στις επικοινωνίες εκτός φυσικά από τους χρήστες ή από τρίτους με τη συγκατάθεση των χρηστών μπορεί να γίνει μόνο εάν υπάρχει σχετική ρύθμιση στο νόμο.[151] Εδώ προφανώς ο νόμος αναφέρεται σε περιπτώσεις εξαιρέσεων που ακολουθούν και στις

[149] Ν. 3471/2006 - ΦΕΚ 133/Α/28-6-2006. Διαθέσιμος στο: https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/n-3471-2006.html [Ημερομηνία πρόσβασης: 12/1/2023]

[150] Αφορά κυρίως cookies με το σύστημα opt-out no prior consent

[151] Άρθρο 4 παρ. 2 ν. 3471/2006

οποίες θα αναφέρονται ρητά οι περιπτώσεις επεξεργασίας των προσωπικών δεδομένων, μέσα από συγκεκριμένες εγγυήσεις. Παρατηρείται και εδώ νομοτεχνικά ότι δεν γίνεται αναφορά στο άρθρο 19 του Συντάγματος, όπως γίνεται στην πρώτη παράγραφο του άρθρου 4 αλλά δεν μπορούμε παρά να θεωρήσουμε ότι ισχύει και σ 'αυτή την περίπτωση η ίδια προστασία.

Στο άρθρο 4 παρ. 4 του ν.3471/2006 όπως και στο άρθρο 5 παρ. 1 της Οδηγίας ePrivacy εντοπίζεται η ίδια εξαίρεση από την αρχή προστασίας του απορρήτου, με την πρόβλεψη της δυνατότητας τεχνικής αποθήκευσης, η οποία είναι αναγκαία για τη διαβίβαση της επικοινωνίας. Διευκρινίζεται στην αιτιολογική έκθεση[152] ότι αυτή η αποθήκευση περιλαμβάνει την αυτόματη, ενδιάμεση και παροδική αποθήκευση εφόσον γίνεται με μοναδικό σκοπό την πραγματοποίηση της μετάδοσης στο ηλεκτρονικό δίκτυο επικοινωνιών, υπό την προϋπόθεση ότι οι πληροφορίες δεν φυλάσσονται για διάστημα μεγαλύτερο από όσο απαιτείται για τη μετάδοση και για σκοπούς διαχείρισης της κίνησης και κατά τη διάρκεια της περιόδου αποθήκευσης διατηρούνται οι εγγυήσεις του απορρήτου.

Όσον αφορά την χρήση κατασκοπευτικών λογισμικών στο άρθρο 4 παρ. 5 ν. 3471/2006[153] προβλέπεται μία κατ' αρχάς απαγόρευση της χρήσης των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με

---

[152] Αιτ. σκ. 22 ePrivacy Directive

[153] *«5.Απαγορεύεται η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, ιδίως δε με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων. Κατ' εξαίρεση, επιτρέπεται η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Στην τελευταία αυτή περίπτωση η χρησιμοποίηση τέτοιων διατάξεων επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες, σύμφωνα με το άρθρο 11 του ν. 2472/1997, όπως ισχύει, και ο υπεύθυνος ελέγχου των δεδομένων παρέχει στον συνδρομητή ή χρήστη το δικαίωμα να αρνείται την επεξεργασία αυτή. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών, παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης.»*

την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων («κοριοί», ή web bugs), καθώς η εγκατάσταση αυτή εν αγνοία του συνιστά παραβίαση της ιδιωτικής ζωής και των προσωπικών δεδομένων του χρήστη.[154] Συγκεκριμένα ορίζεται ότι μόνο κατ' εξαίρεση, επιτρέπεται η οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών η οποία είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Αντίστοιχα το άρθρο 5 παρ.3 της Οδηγίας 2002/58/ΕΚ αναφέρεται σε κατασκοπευτικά λογισμικά, δικτυακούς «κοριούς», κρυφά αναγνωριστικά στοιχεία τα οποία αποθηκεύουν ή έχουν πρόσβαση σε πληροφορίες που σχετίζονται με φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί.

Η ePrivacy Directive, ωστόσο, στο άρθρο 5 παρ. 3 δεν αναφέρεται ρητά στον όρο προσωπικά δεδομένα, αλλά σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη. Ακολουθώντας αυστηρά το άρθρο 5 παρ.3 Οδηγίας 2002/58/ΕΚ[155] όπου κάνει λόγο για αποθήκευση πληροφοριών ή την απόκτηση προσβάσεως σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό του συνδρομητή ή χρήστη σε συνδυασμό με το προοίμιο της Οδηγίας 2002/58/ΕΚ που προβλέπει ότι ο τερματικός εξοπλισμός των χρηστών δικτύων ηλεκτρονικών επικοινωνιών και κάθε πληροφορία που αποθηκεύεται στον εξοπλισμό αυτόν συνιστούν μέρος της ιδιωτικής ζωής των χρηστών η οποία χρήζει προστασίας δυνάμει της ΕΣΔΑ[156] συνάγεται μία πολύ ευρύτερη εξήγηση της έννοιας

---

[154] Αιτιολογική Έκθεση του άρθρου 4 ν. 3471/.2006 ΚΝοΒ, σελ. 1461 επ.

[155] «*3. Τα κράτη μέλη μεριμνούν ώστε η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση προσβάσεως σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη να επιτρέπεται μόνον εάν παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας, και ο υπεύθυνος ελέγχου των δεδομένων τού παρέχει το δικαίωμα να αρνείται την επεξεργασία αυτή. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή διευκόλυνση της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής.*»

[156] Αιτιολογική σκέψη 24 της Οδ. 2002/58/ΕΚ

«πληροφορίες» όπου μπορούμε να συμπεραίνουμε ότι η Οδηγία ePrivacy έχει ισχύ σε κάθε είδους πληροφορίες των χρηστών και όχι μόνο αυτές οι οποίες θεωρούνται προσωπικές.

Όσον αφορά τις τεχνικές μεθόδους και τρόπους πρόσβασης και πάντα μέσα στα πλαίσια της τεχνολογικά ουδέτερης προσέγγισης της νομοθεσίας ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες, γίνεται στο προοίμιο της Οδηγίας ePrivacy αναφορά στους τρόπους πρόσβασης, άντλησης και αποθήκευσης αθέατων πληροφοριών από τον τερματικό εξοπλισμό των χρηστών δικτύων ηλεκτρονικών επικοινωνιών ή την ανίχνευση των δραστηριοτήτων τους με αναφορά και στα λεγόμενα «cookies». Συγκεκριμένα γίνεται αναφορά α. στα λεγόμενα κατασκοπευτικά λογισμικά, δικτυακοί «κοριοί», (web bugs) κρυφά αναγνωριστικά στοιχεία και άλλες παρόμοιες τεχνικές μεθόδους[157] που μπορούν να εισέλθουν στο τερματικό του χρήστη εν αγνοία του με σκοπό την πρόσβαση σε πληροφορίες, την αποθήκευση αθέατων πληροφοριών ή την ανίχνευση των δραστηριοτήτων του χρήστη,[158] και β. στα «cookies» με την διευκρίνιση ότι επιτρέπεται, μόνο για θεμιτούς σκοπούς εν γνώσει των χρηστών και με δυνατότητα αρνήσεως, η χρησιμοποίηση τέτοιων τεχνικών μεθόδων, όπως όταν πρόκειται π.χ. για την ανάλυση της αποτελεσματικότητας του σχεδιασμού και της παρουσίασης μιας ιστοσελίδας και τον έλεγχο της ταυτότητας χρηστών που πραγματοποιούν συναλλαγές σε απευθείας σύνδεση (on-line).[159]

Ο ν. 3471/2006 μεταφέροντας την Οδηγία 2002/58/ΕΚ εισάγει δύο βασικές προϋποθέσεις έτσι ώστε να είναι νόμιμη και επιτρεπτή η αποθήκευση πληροφοριών ή πρόσβαση σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη. [160]

---

[157] "devices" στο αγγλικό κείμενο ή "dispositifs" στο γαλλικό κείμενο της Οδ. 2002/58/ΕΚ.

[158] Αιτ. σκ. 24 της Οδ. 2002/58/ΕΚ

[159] Αιτ. σκ. 25 της Οδ. 2002/58/ΕΚ

[160] Σημαντική διαφοροποίηση υπάρχει μεταξύ της Οδηγίας και του ελληνικού νόμου καθώς στο προοίμιο της Οδηγίας σημειώνεται ότι σε κάθε περίπτωση η χρησιμοποίηση του κατασκοπευτικού λογισμικού πρέπει να χρησιμοποιείται μόνο όταν αυτό προορίζεται για θεμιτούς σκοπούς Βλ. σχετικά Αιτ. σκ. 24 της Οδ. 2002/58/ΕΚ Η πρώτη προϋπόθεση αφορά την χρησιμοποίηση τεχνικών αποθήκευσης, όπως τα "cookies", για να διευκολυνθεί η παροχή υπηρεσιών στην κοινωνία της πληροφορίας, η οποία θα πρέπει να επιτρέπεται υπό τον όρο ότι παρέχονται στους χρήστες σαφείς ακριβείς και εκτεταμένες πληροφορίες, ώστε να εξασφαλίζεται ότι είναι σε γνώση τους η αποθήκευση των πληροφοριών στον τερματικό εξοπλισμό που χρησιμοποιούν. β. Παρέχει στον χρήστη –

Ανακύπτει το ερώτημα σχετικά με το αν η συγκατάθεση του χρήστη ή του συνδρομητή σχετικά με την αποθήκευση των "cookies" ή παρόμοιων διατάξεων όπως κατασκοπευτικών λογισμικών στον τερματικό του εξοπλισμό πρέπει να εκφράζεται μία φορά για όλα τα μελλοντικά "cookies" και λογισμικά ή μπορεί να γίνει κάθε φορά ανάλογα με τις εκάστοτε επιθυμίες του κάθε χρήστη. Το ζήτημα περιπλέκεται, διότι είναι δυνατόν σε συγκεκριμένη περίπτωση πέρα από τον συνδρομητή να υπάρχουν ένας ή περισσότερο χρήστες. Στο προοίμιο της Οδ. 2002/58/ΕΚ αναφέρεται ότι όλοι οι χρήστες θα πρέπει να έχουν την ευκαιρία να αρνηθούν την αποθήκευση "cookies" ή παρόμοιων διατάξεων στον τερματικό τους εξοπλισμό. Η διευκρίνιση αυτή είναι ιδιαίτερα σημαντική σε περιπτώσεις όπου πρόσβαση στον τερματικό εξοπλισμό, και επομένως και σε κάθε είδους προσωπικά δεδομένα που έχουν αποθηκευθεί σε ένα τέτοιο εξοπλισμό, έχουν και άλλοι εκτός από τον πρωταρχικό χρήστη. Ο νόμος στο σημείο αυτό έχει κενό, ωστόσο τόσο στο προοίμιο της Οδηγίας, όσο και στην αιτιολογική έκθεση του ν. 3471/2006 αναφέρεται ότι οι πληροφορίες για τη χρήση διαφόρων διατάξεων που θα εγκατασταθούν στον τερματικό εξοπλισμό του χρήστη καθώς και το δικαίωμα να αρνηθεί αυτές τις διατάξεις, μπορούν να προσφέρονται μόνο μία φορά κατά τη διάρκεια της ίδιας σύνδεσης, και να καλύπτουν επίσης την μελλοντική ενδεχομένως χρήση αυτών των διατάξεων σε μεταγενέστερες συνδέσεις.[161]

Ωστόσο, δεν συμπεριλήφθηκε η έννοια της «προηγούμενης συγκατάθεσης» όπως στην περίπτωση της μη ζητηθείσας επικοινωνίας, που θα μπορούσε να κάνει πιο πλήρη την προστασία του απορρήτου. Σε κάθε περίπτωση και για την διευκόλυνση της πρόσβασης σε συγκεκριμένο περιεχόμενο ιστοσελίδων στο προοίμιο της Οδηγίας προβλέπεται η δυνατότητα να τίθεται ως όρος η ενημερωμένη αποδοχή "cookies" ή παρόμοιων τεχνικών αποθήκευσης, εφόσον χρησιμοποιούνται για σύννομο σκοπό, κάτι που δυσκολεύει αρκετά τους χρήστες.[162]

---

συνδρομητή το δικαίωμα να αρνείται την επεξεργασία αυτή. Τονίζεται ότι οι συνδρομητές και οι χρήστες έχουν το δικαίωμα να αρνούνται την επεξεργασία αυτή.

[161] Αιτ. σκ. 25 της Οδ. 2002/58/ΕΚ

[162] Βλ. Κίτσος, Π. «*Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών. Ενσωμάτωση των ρυθμίσεων της Ευρωπαϊκής Ένωσης στο Ελληνικό δίκαιο.*» ΠΑΜΑΚ, Θεσσαλονίκη 2011, σελ. 237 επ.

### 3.7. Η σημασία του Κανονισμού e-Privacy

Η ανάπτυξη και η αύξηση χρήσης των κατασκοπευτικών λογισμικών συνδέεται εν μέρει, και με την χρονική καθυστέρηση ολοκλήρωσης του κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (e-Privacy).[163] Οι προϋποθέσεις και η διαδικασία νόμιμης άρσης του απορρήτου, όταν η επικοινωνία διενεργείται μέσω έξυπνων εφαρμογών,[164] είναι από τα ζητήματα των οποίων η ρύθμιση αναμένεται να προβλεφθεί στις διατάξεις του εν λόγω κανονισμού. Καθώς δε ο μεγαλύτερος όγκος των επικοινωνιών στις μέρες μας διεξάγεται όχι μέσω της ενσύρματης, ασύρματης ή κινητής τηλεφωνίας, αλλά μέσω δεδομένων και κυρίως μέσω εφαρμογών και του διαδικτύου, είναι αυταπόδεικτοι οι λόγοι για τους οποίους έχει υψηλό ενδιαφέρον ο διεμβολισμός του πεδίου από επίδοξους εισβολείς με τη χρήση παράνομων λογισμικών.

Δεν προσδοκά, ασφαλώς, κανείς πως η άφιξη του νέου κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες θα λύσει ως από μηχανής θεός τις παράνομες παρακολουθήσεις. Έχει σημασία, ωστόσο, να επισπευσθεί η ρύθμιση του πεδίου, καθώς μια τέτοια εξέλιξη αναμένεται τουλάχιστον να οριοθετήσει τις πηγές διακινδύνευσης του δικαιώματος θωρακίζοντας περαιτέρω την άσκησή του.

Η πρόταση Κανονισμού, στο άρθρο 4 παρ. 1, περ. γ, όσον αφορά στον ορισμό του «τερματικού εξοπλισμού» παραπέμπει στο άρθρο 1, περ. 1 της Οδ. 2008/63/ΕΚ της Επιτροπής. Κατά την αιτιολογική σκέψη 20 της πρότασης,[165] ο τερματικός εξοπλισμός του χρήστη αλλά και κάθε πληροφορία που σχετίζεται με τη χρήση του, ήτοι κάθε πληροφορία που υπόκειται σε επεξεργασία, αποθηκεύεται ή συλλέγεται ή κάθε πληροφορία που αποθηκεύεται και χρησιμεύει στη σύνδεση μεταξύ συσκευών ή/και στη σύνδεση με εξοπλισμό δικτύου, αποτελούν μέρος της ιδιωτικής σφαίρας του χρήστη και φυσικά ως τέτοιο θα πρέπει να αντιμετωπίζεται και να προστατεύεται. Γι' αυτό οι πληροφορίες που βρίσκονται

---

[163] Η πρόταση του Κανονισμού διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017PC0010&from=EN. [Ημερομηνία πρόσβασης: 19/1/2023]

[164] Γνωστές και ως over-the-top services –. Βλ. *"Body of European Regulator for Electronic Communications (BEREC) Report on OTT Services"*. Διαθέσιμο στο: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services [Ημερομηνία πρόσβασης: 19/1/2023]

[165] Και την αιτ. σκ. 24 της Οδ. 2002/58/ΕΚ.

αποθηκευμένες στον τερματικό εξοπλισμό του χρήστη θα πρέπει να προστατεύονται, σύμφωνα με το άρθρο 8 της πρότασης Κανονισμού, και να επιτρέπεται η επεξεργασία τους κατόπιν συγκατάθεσης του χρήστη και πάντοτε για ειδικά ορισμένους σκοπούς. Η ρύθμιση αυτή δικαιολογείται από το γεγονός ότι σε αυτές τις πληροφορίες πολλές φορές περιέχονται δεδομένα, τα οποία έχουν να κάνουν με πτυχές της προσωπικότητας του φυσικού προσώπου, όπως π.χ. είναι οι φωτογραφίες, η λίστα επαφών του κ.λπ.

Επιπλέον, στον τερματικό εξοπλισμό του χρήστη καταφέρνουν ποικιλοτρόπως να εισέρχονται διάφορες διατάξεις όπως κατασκοπευτικά λογισμικά, διαδικτυακοί κοριοί, τα "tracking cookies" κ.ά., οι οποίες συνήθως, χωρίς τη συγκατάθεση του χρήστη, έχουν πρόσβαση σε προσωπικά δεδομένα ή ανιχνεύουν δραστηριότητες του χρήστη, θέτοντας με τον τρόπο αυτό σε κίνδυνο την ιδιωτικότητά του. Στη διαδικτυακή καθημερινότητα, ωστόσο, πολλές φορές εισέρχονται τέτοιου είδους διατάξεις στον τερματικό εξοπλισμό του χρήστη, με τη συγκατάθεσή του και χρησιμοποιούνται για θεμιτούς σκοπούς. Οι πιο γνωστές διατάξεις, οι οποίες έχουν απασχολήσει τελευταία, όχι μόνο όσους μελετούν την ιδιωτικότητα και τα προσωπικά δεδομένα του χρήστη αλλά και τον ίδιο τον χρήστη λόγω της ολοένα και μεγαλύτερης διάδοσής τους, είναι τα λεγόμενα "cookies".

Με το άρθρο 5 παρ. 3 της υπό κατάργηση οδηγίας e-Privacy ορίζεται ότι η αποθήκευση και επεξεργασία των ήδη αποθηκευμένων πληροφοριών στον τερματικό εξοπλισμό του τελικού χρήστη, επιτρέπεται μόνο σε συνέχεια της ρητής του ως προς αυτό συγκατάθεσης. Προβλέπεται, ακόμη, και η περίπτωση κατά την οποία επιτρέπεται η αποθήκευση ή πρόσβαση και επεξεργασία, χωρίς τη λήψη ρητής προηγούμενης συγκατάθεσης από τον χρήστη, με μοναδικό όμως σκοπό τη διενέργεια ή τη διευκόλυνση διαβίβασης μιας επικοινωνίας μέσω του δικτύου ηλεκτρονικών επικοινωνιών ή σε περίπτωση που μία τέτοια ενέργεια θα ήταν απαραίτητη για την παροχή υπηρεσίας της Κοινωνίας της Πληροφορίας την οποία έχει αιτηθεί ο ίδιος ο χρήστης. Στην αιτ. σκ. 20 της πρότασης Κανονισμού, παρατηρείται ότι σχετικά με την επεξεργασία και αποθήκευση πληροφοριών στον τερματικό εξοπλισμό του χρήστη, για να είναι σύννομη, θα πρέπει είτε ο πάροχος να έχει πρώτα λάβει τη ρητή συγκατάθεση του τελικού χρήστη, είτε να πρόκειται για μία διαδικασία η οποία δικαιολογείται από κάποιον ειδικό σκοπό.

Με το άρθρο 8 της πρότασης Κανονισμού ορίζονται οι περιπτώσεις κατά τις οποίες επιτρέπεται η επεξεργασία και αποθήκευση των πληροφοριών του τερματικού εξοπλισμού

του χρήστη. Επιπλέον, απαγορεύεται και η συλλογή πληροφοριών, οι οποίες εκπέμπονται από τον τερματικό εξοπλισμό του τελικού χρήστη, ώστε να μπορεί να πραγματοποιηθεί σύνδεση με άλλη συσκευή ή με εξοπλισμό δικτύου πέραν των περιπτώσεων που η εν λόγω συλλογή πληροφοριών γίνεται στο πλαίσιο της πραγματοποίησης και διατήρησης της σύνδεσης αυτής, που ο τελικός χρήστης έχει δώσει τη συγκατάθεσή του, που είναι απαραίτητη για στατιστικούς σκοπούς -στην περίπτωση όμως αυτή πρέπει να ακολουθεί ανωνυμοποίηση ή διαγραφή των δεδομένων αμέσως μόλις εξυπηρετήσουν τον σκοπό τους- ή τέλος που είναι απαραίτητη για την παροχή της υπηρεσίας την οποία αιτήθηκε ο ίδιος ο τελικός χρήστης.

### 3.8. Το νομοθετικό πλαίσιο της Κυβερνοασφάλειας στην Ελλάδα

Στη χώρα μας το πλαίσιο της προστασίας της Κυβερνοασφάλειας, ειδικά της προστασίας της επικοινωνίας από λογισμικά κατασκοπείας είναι ελλιπές, σε αντίθεση με τις πρωτοβουλίες της ΕΕ. Ο Οργανισμός της ΕΕ για την Κυβερνοασφάλεια, (ENISA) είχε ήδη δημοσιεύσει από το 2019 μελέτη κινδύνων από την ηλεκτρονική παρακολούθηση, τις επιπτώσεις και τα περιστατικά κυβερνοεπιθέσεων, συγκαταλέγοντας την παρακολούθηση αυτή σε ένα από τους πιο σημαντικούς κινδύνους για την κυβερνοασφάλεια στην ΕΕ.[166] Το 2022 επίσης δημοσιεύθηκε το πλαίσιο κινδύνων του ENISA στο οποίο γινόταν εκτενής αναφορά στις επιπτώσεις από την χρήση του λογισμικού κατασκοπείας Pegasus στην κυβερνοασφάλεια και τα δικαιώματα των πολιτών.[167]

---

[166] ENISA Threat Landscape January 2019- April 2020 *"Cyber espionage"*. Διαθέσιμο στο: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-cyberespionage [Ημερομηνία πρόσβασης: 19/1/2023]

[167] ENISA Threat Landscape October 2022. Διαθέσιμο στο: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Ημερομηνία πρόσβασης: 19/1/2023]

Ο ν. 4070/2012[168] ρύθμισε τις υποχρεώσεις των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, σχετικά με την προστασία και την εύρυθμη λειτουργία των ηλεκτρονικών επικοινωνιών. Ειδικότερα, όπως ορίζεται στο άρθρο 37 του ανωτέρω νόμου, οι πάροχοι έχουν υποχρέωση να λαμβάνουν όλα τα πρόσφορα μέτρα, τεχνικού και οργανωτικού χαρακτήρα, προκειμένου να διασφαλιστεί ότι η διαχείριση των κινδύνων γίνεται με τον καταλληλότερο τρόπο, αναφορικά με την ασφάλεια των δικτύων και των υπηρεσιών.[169] Επίσης, η ασφάλεια που παρέχουν αυτά τα μέτρα πρέπει να είναι αντίστοιχη του υφιστάμενου κίνδυνου, ενώ τα μέτρα αυτά να πρέπει είναι τόσο μέτρα αποτροπής των κινδύνων όσο και ελαχιστοποίησης των συνεπειών από συμβάντα ασφαλείας που έχουν επιπτώσεις στους χρήστες και στα δίκτυα. Επιπλέον, οι πάροχοι πρέπει να λαμβάνουν τα αναγκαία μέτρα με σκοπό την αρτιότητα των δικτύων, ώστε η παροχή των υπηρεσιών να είναι ανεμπόδιστη και συνεχής. Μάλιστα, η οποιασδήποτε μορφή παραβίαση της ασφάλειας, της ακεραιότητας και της εμπιστευτικότητας των δικτύων που επηρεάζει σημαντικά τη λειτουργία τους θα πρέπει να αναφέρεται από τους παρόχους στην ΕΕΤΤ, η οποία ακολούθως οφείλει να γνωστοποιεί κάθε παράβαση σχετικά με την ασφάλεια ή την ακεραιότητα στην ΑΔΑΕ.

Παραπέρα, στις αρμοδιότητες της ΑΔΑΕ, περιλαμβάνεται ο τακτικός και έκτακτος έλεγχος των επιχειρήσεων, ο έλεγχος τήρησης της νομοθεσίας για την άρση του απορρήτου, η επιβολή διοικητικών κυρώσεων σε περίπτωση παραβιάσεων της σχετικής νομοθεσίας, ο έλεγχος καταγγελιών που αφορούν την παραβίαση του απορρήτου των επικοινωνιών, η έκδοση κανονιστικών διοικητικών πράξεων σχετικά με την προστασία του απορρήτου των

[168] Ν. 4070/2012 ΦΕΚ Α' 82/10.04.2012. Διαθέσιμος στο: https://www.kodiko.gr/nomothesia/document/117878/nomos-4070-2012 [Ημερομηνία πρόσβασης: 19/1/2023]

[169] Βλ. Law&Tech (2020) *«Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών»* Διαθέσιμο στο: https://lawandtech.eu/2020/04/27/%CF%80%CE%BF%CE%B9%CE%BF-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%80%CE%BB%CE%B1%CE%AF%CF%83%CE%B9%CE%BF-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7%CE%BD-%CE%B1%CF%83/ [Ημερομηνία πρόσβασης: 19/1/2023]

επικοινωνιών καθώς και η έκδοση γνωμοδοτήσεων και συστάσεων που άπτονται της αρμοδιότητάς.

Το 2013 η ΑΔΑΕ στην απόφαση 205/2013[170] εξειδίκευσε το περιεχόμενο των διατάξεων του άρθρου 37 ν. 4070/2012 σχετικά με την ασφάλεια και την ακεραιότητα των δικτύων και των υπηρεσιών ηλεκτρονικών επικοινωνιών, προβλέποντας τις υποχρεώσεις των παρόχων. Κατόπιν, ακολούθησε, ο ν. 4577/2018[171] που ενσωμάτωσε την Οδηγία 2016/1148/ΕΕ , με την οποία θεσπίστηκε το νομικό πλαίσιο για την εξασφάλιση υψηλού επιπέδου προστασίας στα συστήματα δικτύου και πληροφοριών, με στόχο τη βελτίωση της εσωτερικής αγοράς της ΕΕ. Σύμφωνα με το άρθρο 3 παρ. 2, αντικείμενο του ανωτέρω νόμου αποτελεί η ασφαλής λειτουργία και προστασία των συστημάτων δικτύου και πληροφοριών. Περαιτέρω, ο ν. 4577/2018 αναφέρεται σε απαιτήσεις ασφαλείας και κοινοποίησης με τις οποίες πρέπει να συμμορφώνονται αποκλειστικά οι φορείς που εκμεταλλεύονται την παροχή βασικών υπηρεσιών, και όσοι παρέχουν υπηρεσίες ψηφιακής τεχνολογίας σε υψηλής σημασίας φορείς.

Το 2019 η Υπουργική Απόφαση 1027/04-10-2019[172] έθεσε αντικειμενικά κριτήρια για τον ορισμό «των υπόχρεων φορέων βασικών υπηρεσιών» του ν. 4577/2018 και θεσπίζει τις υποχρεώσεις αυτών των παρόχων. Ειδικότερα, προβλέπεται : α)ευθύνη των οργανισμών για τις πράξεις ή παραλείψεις των συνεργατών που αυτοί οι οργανισμοί χρησιμοποιούν για

---

[170] Βλ. Απόφαση ΑΔΑΕ 205/2013 - ΥΕΚ 1742/Β/15-7-2013: «*Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*»
Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinoniestelephonia/apophase-adae-205-2013.html [Ημερομηνία πρόσβασης: 19/1/2023]

[171] Ν. 4577/2018 - ΥΕΚ 199/Α/3-12-2018: «*Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις*». Διαθέσιμο στο: https://www.kodiko.gr/nomothesia/document/474449/nomos-4577-2018 [Ημερομηνία πρόσβασης: 19/1/2023]

[172] Βλ. Υπουργική Απόφαση 1027/2019 - ΥΕΚ 3739/Β/8-10-2019: «*Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α 199)*». Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/upourgike-apophase-1027-2019-phek-3739b-8-10-2019.html [Ημερομηνία πρόσβασης: 19/1/2023]

διάφορες λειτουργίες των συστημάτων τους, β) υποχρέωση των οργανισμών για σχεδιασμό στρατηγικής ασφάλειας, γ) υποχρέωση των οργανισμών για σχεδιασμό ενός πλαισίου βασικών αναγκών ασφάλειας, προσανατολισμένο στις συγκεκριμένες ανάγκες και κινδύνους, δ) υποχρέωση των οργανισμών αντιμετώπισης των περιστατικών ασφάλειας και γνωστοποίησης αυτών στο CSIRT, στην Εθνική Αρχή Κυβερνοασφάλειας και στο κοινό.

## ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ: ΣΥΓΧΡΟΝΕΣ ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΣΥΓΚΡΙΤΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

### 4.1. Η αντιμετώπιση των κατασκοπευτικών λογισμικών στις έννομες τάξεις των ξένων χωρών

Στις περισσότερες χώρες του κόσμου η πρόσβαση ή η απόπειρα πρόσβασης στη συσκευή τρίτου χωρίς την άδεια του είναι παράνομη.[173] Σε χώρες όπως η Ισπανία, η Ελλάδα, η Ουγγαρία, η Πολωνία, η Γερμανία, η Γαλλία, η Ιταλία, η Ολλανδία η χρήση κατασκοπευτικών λογισμικών τιμωρείται με βάση τον εθνικό ποινικό κώδικα της κάθε χώρας ως παράνομη πρόσβαση αλλά και από τα οικεία Συντάγματα ως προς την παραβίαση του απορρήτου και των προσωπικών δεδομένων δεδομένης και της υιοθέτησης του ΓΚΠΔ. Επιπλέον, ορισμένες από αυτές τις χώρες έχουν θεσπίσει την άρση του απορρήτου ως ειδική ανακριτική πράξη μέσω των μυστικών υπηρεσιών ή και της κυβέρνησης ενίοτε και υπό την εποπτεία δικαστικών ή ανεξάρτητων αρχών.

Τα λογισμικά κατασκοπείας χρησιμοποιούνται ολοένα και περισσότερο ακόμα και σε δημοκρατικές κοινωνίες. Ο βαθμός νομιμότητας και επέμβασής τους στην ιδιωτική σφαίρα των πολιτών διαφέρει ανάλογα την έννομη τάξη και το κράτος. Πάντως, οι περισσότερες κυβερνήσεις[174] είτε φανερά είτε κρυφά χρησιμοποιούν όλο και περισσότερο λογισμικά κατασκοπείας για εθνικούς σκοπούς, σκοπούς πρόληψης εγκληματικότητας και

---

[173] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, December 2022 *"The use of Pegasus and equivalent surveillance spyware"*, σελ. 26 επ. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf [Ημερομηνία πρόσβασης: 3/1/2023 ]

[174] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, May 2022 *"Pegasus and surveillance spyware"*. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf [Ημερομηνία πρόσβασης: 3/1/2023]

τρομοκρατίας αλλά και για λιγότερο νόμιμους σκοπούς, όπως η παρακολούθηση πολιτικών αντιπάλων. Επιπλέον, δεν είναι δυνατόν να γνωρίζουμε με ακριβή αριθμό τα λογισμικά κατασκοπείας που ενδέχεται να χρησιμοποιεί ένας ιδιώτης π.χ. ένας εργοδότης που θέλει να ελέγχει τους υπαλλήλους του ή τα social media που χρησιμοποιούμε ή ένας πάροχος τηλεπικοινωνίας με τον οποίο συμβαλλόμαστε.

Μεταξύ των χωρών εντός της ΕΕ, όπου φαίνεται να έχει γίνει χρήση λογισμικού – τόσο από κρατικές υπηρεσίες και όσο και ιδιώτες– περιλαμβάνονται, πλην της χώρας μας, η Ουγγαρία[175], το Βέλγιο, η Βουλγαρία, η Γαλλία, η Γερμανία, η Εσθονία, η Ισπανία, η Ολλανδία, η Φινλανδία, και η Κύπρος[176]. Η περίπτωση της Γερμανίας έχει ειδικότερο ενδιαφέρον, καθώς φαίνεται ότι η γερμανική αστυνομία παραδέχθηκε, στο πλαίσιο κοινοβουλευτικής έρευνας, ότι είχε προμηθευθεί και χρησιμοποιήσει κατά την άσκηση των αρμοδιοτήτων της, έκδοση του λογισμικού Pegasus. Βεβαίωσε δε, ότι δεν πρόκειται για την εργοστασιακή έκδοση, καθώς η τελευταία δεν εναρμονίζεται με τα προαπαιτούμενα της γερμανικής νομοθεσίας περί προστασίας του δικαιώματος στην ιδιωτική ζωή. Ενδεικτικά, μεταξύ των στόχων παρακολούθησης στην ΕΕ περιλαμβάνονται ο Ισπανός πρωθυπουργός, Pedro Sánchez, ο Γάλλος πρόεδρος, Emmanuel Macron, στελέχη του καταλανικού αυτονομιστικού κινήματος, ο Didier Reynders, επίτροπος δικαιοσύνης στην Ευρωπαϊκή Ένωση, ο Charles Michel, ως πρωθυπουργός του Βελγίου κ.ά. Ενδιαφέρον έχει επίσης, η ομολογία της Πολωνικής κυβέρνησης, τον Ιανουάριο 2022 ότι πράγματι είχε προμηθευθεί το λογισμικό Pegasus, ωστόσο αρνήθηκε οποιαδήποτε παράνομη χρήση του.[177]

Ας σημειωθεί ενδεικτικά ότι στη Γερμανία υφίσταται από τον Ιούνιο του 2021, στο πλαίσιο εκσυγχρονισμού της νομοθεσίας που διέπει τη λειτουργία των εθνικών μυστικών

---

[175] Στην Ουγγαρία η χρήση του λογισμικού Pegasus έγινε για παγίδευση των επικοινωνιών εκατοντάδων δημοσιογράφων. Η αιτιολογία που αντιτάχθηκε από τις αρχές της χώρας, παρέπεμπε σε λόγους εθνικής ασφάλειας, χωρίς περαιτέρω εξειδίκευση.

[176] Βλ. Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, December 2022 *"The use of Pegasus and equivalent surveillance spyware"*, ό.π. σελ. 16 επ. Πρόκειται κυρίως για τα λογισμικά Pegasus, Predator, Cardiru.

[177] Βλ. EPRS (2022) *"Europe's PegasusGate – Countering spyware abuse"*, ό.π. σελ. 22 επ. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf [Ημερομηνία πρόσβασης: 4/1/2023]

υπηρεσιών, νομοθετικό πλαίσιο για τη χρήση κατασκοπευτικού λογισμικού. Στον ίδιο νόμο προβλέπεται επίσης, υποχρέωση των διαδικτυακών παρόχων για τεχνική συνδρομή στις υπηρεσίες που νομιμοποιούνται να ενεργοποιήσουν το εν λόγω λογισμικό.[178] Αντίστοιχη νομοθεσία υπάρχει επίσης, στη Σουηδία από τον Φεβρουάριο του 2020.[179] Ενώπιον τόσο των γερμανικών, όσο και των σουηδικών δικαστηρίων έχει ήδη αμφισβητηθεί, πάντως, η συμβατότητα των προαναφερόμενων νόμων σε σχέση με το οικείο Σύνταγμα της κάθε χώρας, την ΕΣΔΑ, καθώς επίσης και το ενωσιακό δίκαιο.

Δεν είναι άνευ σημασίας η υπενθύμιση ότι το Γερμανικό Ομοσπονδιακό Συνταγματικό Δικαστήριο είχε από το 2007 θεωρήσει νόμο του ομόσπονδου κρατιδίου της Βόρειας Ρηνανίας Βεστφαλίας, ο οποίος επέτρεπε την χρήση κατασκοπευτικού λογισμικού για εξ αποστάσεως παρακολούθηση ηλεκτρονικών επικοινωνιών ως μη συμβατό με το δικαίωμα στην ιδιωτικότητα. Στην πραγματικότητα, επρόκειτο για την πρώτη φορά που το Γερμανικό Συνταγματικό Δικαστήριο καθιέρωνε την «προστασία της εμπιστευτικότητας και ακεραιότητας των συστημάτων».[180]

### 4.2. Το περιεχόμενο της επικοινωνίας: η προστασία των εξωτερικών στοιχείων της επικοινωνίας και η πολυπλοκότητα των κατασκοπευτικών λογισμικών

Λόγω της τεχνολογικής εξέλιξης η έννοια της επικοινωνίας και το ποια δεδομένα συνιστούν περιεχόμενο της επικοινωνίας έχει διευρυνθεί τόσο, ώστε να καλύπτονται από το απόρρητο

---

[178] Βλ. Deutche Welle, (2021) *"Is Germany's spyware law a threat to press freedom?"*. Διαθέσιμο στο: https://www.dw.com/en/is-germanys-spyware-law-a-threat-to-press-freedom/a-59656164?utm_source=headtopics&utm_medium=news&utm_campaign=2021-10-29 [Ημερομηνία πρόσβασης: 4/1/2023]

[179] Βλ. Lindsey, N. CPO Magazine (2019), *"Swedish police given green light for spyware"*.Διαθέσιμο στο: https://www.cpomagazine.com/cyber-security/swedish-police-given-green-light-for-spyware/ [Ημερομηνία πρόσβασης: 4/1/2023]

[180] Federal Constitutional Court, BvR 370/07 και BvR 595/07, Διαθέσιμες στο: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html [Ημερομηνία πρόσβασης: 4/1/2023]. Στη γερμανική νομική παράδοση επικρατεί ιδιαίτερη ευαισθησία στα ζητήματα προστασίας προσωπικών δεδομένων, καθόσον είναι περιώνυμες οι καθολικές μέθοδοι επιτήρησης τόσο της ναζιστικής Gestapo, όσο και της Ανατολικογερμανικής Stasi.

στοιχεία που μέχρι πρότινος δεν αποτελούσαν καθαρά περιεχόμενο επικοινωνίας.[181] Με αφορμή τις πρόσφατες εξελίξεις αναδεικνύεται και σημαντικό τεχνοκρατικό έλλειμμα των δικαστών και των εν γένει νομομαθών, οι οποίοι και σε όποιες περιπτώσεις εξεδόθησαν εκ των υστέρων αποφάσεις περί άρσης του απορρήτου, με τη χρήση των επίμαχων λογισμικών, φαίνεται να μην δύνανται να αντιληφθούν πλήρως τους εγγενείς κινδύνους που παράγονται από τα ιδιοσυστασιακά χαρακτηριστικά του λογισμικού per se.[182] Πάντως και μόνο το γεγονός της διχογνωμίας που επικρατεί σχετικά με το τι αποτελεί το υπό προστασία περιεχόμενο της επικοινωνίας και αν τα μεταδεδομένα εμπίπτουν σε αυτό[183] υποδεικνύει την συστολή με την οποία αντιμετωπίζει το δίκαιο τις τεχνολογικές εξελίξεις και την αδυναμία του να ανταποκριθεί στις απαιτήσεις της, πόσο μάλλον όταν η τεχνολογία των κατασκοπευτικών λογισμικών είναι τόσο εξελιγμένη που δύσκολα μπορεί ένας νομικός ή μη να κατανοήσει.

Όπως προαναφέρθηκε, στην έννοια της συνταγματικά προστατευόμενης επικοινωνίας υπάγεται το επικοινωνιακό γεγονός σε όλη του την έκταση, ήτοι τόσο το περιεχόμενο της επικοινωνίας, όσο και τα στοιχεία που εξατομικεύουν τις περιστάσεις υπό τις οποίες λαμβάνει χώρα αυτή, δηλαδή τα μεταδεδομένα επικοινωνίας, με αποτέλεσμα ορθά να γίνεται λόγος για την προστασία του γεγονότος της επικοινωνίας.[184] Επομένως, ως εσωτερικά στοιχεία της επικοινωνίας νοούνται οι πληροφορίες, που ανταλλάσσουν τα μέρη,

---

[181] Ένα τέτοιο παράδειγμα αποτελεί κι η προσθήκη στον ελληνικό ΠΚ του άρθρου 13 των ηλεκτρονικών εγγράφων πέραν των εγγράφων με την υλική υπόσταση του χαρτιού.

[182] Βλ. Hostovsky Brandes, T. Verfassungsblog (2022): *"When your own spyware hits home – Israel's domestic NSO Scandal"*. Διαθέσιμο στο: https://verfassungsblog.de/when-your-own-spyware-hits-home/ [Ημερομηνία πρόσβασης: 17/1/2023]

[183] Διχογνωμία έχει επικρατήσει μεταξύ του ΑΠ και του ΣτΕ. Βλ. σχετικά Γνμδ Γ. Σανιδάς 9/2009 σύμφωνα με τον οποίο το διαδίκτυο (π.χ. συνομιλίες μέσω διαδικτυακών εφαρμογών Facebook, Messenger κ.ά.) δεν εμπίπτει στην επικοινωνία άρα δεν προστατεύεται από το απόρρητο. Διαθέσιμη στο: https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-09-2009/

[184] Τσόλιας, Γ. (2013) «*Απόρρητο Ηλεκτρονικών Επικοινωνιών ΙΙΙ -Συνταγματικό πλαίσιο προστασίας του απορρήτου στον τομέα των τηλεπικοινωνιών*». Σε Παύλου, Σ., Σάμιο, Θ. επιμ. Ειδικοί Ποινικοί Νόμοι, Αθήνα: Εκδόσεις Π.Ν. Σάκκουλας, σελ. 22.

μέσω δημόσιου δικτύου επικοινωνιών, οι οποίες αποσκοπούν στην επίτευξη της επικοινωνίας, δηλαδή το περιεχόμενο του φωνητικού μηνύματος, του κειμένου, της εικόνας, της ιστοσελίδας, των προγραμμάτων των Η/Υ, ενώ ως εξωτερικά στοιχεία της επικοινωνίας ή αλλιώς μεταδεδομένα νοούνται αυτά που παράγονται αυτοματοποιημένα από την χρήση των δημοσίων δικτύων ηλεκτρονικών επικοινωνιών κατά την επικοινωνία και παρέχουν πληροφορίες, που προσδιορίζουν τις συνθήκες και τις περιστάσεις, υπό τις οποίες αυτή διενεργείται, εξατομικεύοντάς την, δηλαδή τον τόπο, τον χρόνο, την ταυτότητα των επικοινωνούντων μερών, τη διάρκεια και τη συχνότητα της επικοινωνίας. Ειδικότερα, τα μεταδεδομένα επικοινωνίας έχουν διπλή υπόσταση, καθώς αποτελούν αφενός δεδομένα προσωπικού χαρακτήρα του χρήστη στον τομέα των ηλεκτρονικών επικοινωνιών και αφετέρου απόρρητα εξατομικευτικά στοιχεία της επικοινωνίας του, με αποτέλεσμα η υπαγωγή τους στο προστατευτέο πεδίο του επικοινωνιακού απορρήτου του άρθρο 19 Σ. να κρίνεται πληρέστερη, καθώς δυνάμει του τελευταίου τίθενται εγγυήσεις για οποιαδήποτε επέμβαση σε αυτά.[185] Είναι σαφές πλέον ότι τα μεταδεδομένα επικοινωνίας είναι τόσο άρρηκτα συνδεδεμένα με το περιεχόμενο, ώστε να μην υφίσταται επικοινωνία χωρίς αυτά, αποτελώντας αναπόσπαστο στοιχείο για την πραγματοποίησή της. Ως εκ τούτου, δεν μπορεί να νοηθεί απόρρητο της επικοινωνίας χωρίς την παράλληλη προστασία του απορρήτου των συνθηκών διεξαγωγής αυτής, αφού το άτομο δεν μπορεί να απολαμβάνει το δικαίωμα στο απόρρητο της ελεύθερης ανταπόκρισης και επικοινωνίας, όταν γνωρίζει ότι ανά πάσα στιγμή μπορεί να καταστεί γνωστό σε τρίτους με ποιον επικοινωνεί, πότε, με ποια συχνότητα και υπό ποιες περιστάσεις.[186]

Τα κατασκοπευτικά λογισμικά έχουν πρόσβαση πρωτίστως σε αυτά τα δεδομένα τα οποία και θεωρούνται άκρως σημαντικά για την εκπλήρωση του σκοπού της παρακολούθησης. Είναι πλέον αποδεκτό ότι στο σύγχρονο περιβάλλον επικοινωνίας τα μεταδεδομένα δύνανται να οδηγήσουν ακόμα και στην αναπαράσταση των σχέσεων μιας ολόκληρης κοινωνίας. Άλλωστε, στην περίπτωση των επικοινωνιών μέσω διαδικτύου η ταξινόμηση μεταξύ περιεχομένου και μεταδεδομένων επικοινωνίας γίνεται ακόμα δυσκολότερη, καθώς δεν αντικατοπτρίζει πλέον μια αυστηρή οριοθέτηση μεταξύ «ευαίσθητων» και «αβλαβών»

---

[185] Τσόλιας, Γ. (2004) «*Τα τηλεπικοινωνιακά δεδομένα υπό το πρίσμα του απορρήτου: προβληματισμοί εν όψει της ενσωμάτωσης της Οδηγίας 2002/58/ΕΚ*». ΔΙΤΕ (π. ΔΙΜΕΕ), (Τεύχος 3/2004), σελ. 14.

[186] Τσόλιας, Γ. (2013), ό.π., σελ. 37.

πληροφοριών για τα υποκείμενα, αφού πολλές υπηρεσίες, όπως το ηλεκτρονικό ταχυδρομείο περιέχουν αλληλουχίες πληροφοριών, που περιλαμβάνουν δεδομένα αναφορικά τόσο με το περιεχόμενο της επικοινωνίας όσο και με τα εξωτερικά στοιχεία αυτής, ήτοι π.χ. η περίπτωση του «θέματος» ενός e-mail, το οποίο αποτελεί περιεχόμενο, χωρίς ωστόσο να συμπεριλαμβάνεται στο βασικό κείμενο του μηνύματος.[187]

Είναι επίσης χαρακτηριστικό της σπουδαιότητας των μεταδεδομένων ότι καλύπτουν πληθώρα στοιχείων για το γεγονός της επικοινωνίας, όπως το γεωγραφικό πλάτος και μήκος, υψόμετρο του τερματικού σταθμού του αποστολέα ή του παραλήπτη, οποιαδήποτε πληροφορία ονομασίας, αρίθμησης ή διεύθυνσης των επικοινωνούντων μερών, τον όγκο, την αρχή, το τέλος ή τη διάρκεια της επικοινωνίας, με αποτέλεσμα να σχετίζονται με τα «συμφραζόμενα» αυτής, σε αντίθεση με το περιεχόμενό της. Ως εκ τούτου, τα μεταδεδομένα επικοινωνίας αποτελούν μια πλούσια πηγή προσωπικών πληροφοριών για τα υποκείμενα της επικοινωνίας, καθώς αποκαλύπτουν το «ποιος» (τα επικοινωνούντα μέρη), «πότε», πόσο καιρό και πόσο συχνά, (χρόνος, διάρκεια και συχνότητα), το «τι» (είδος επικοινωνίας, π.χ. τηλεφωνική κλήση, μήνυμα, e-mail), το «πώς» (η συσκευή επικοινωνίας που χρησιμοποιείται, π.χ. σταθερή τηλεφωνία, smartphone, tablet) και το «πού» (τοποθεσία των συσκευών που χρησιμοποιούνται) των μερών, που εμπλέκονται σε κάθε είδους επικοινωνία, αφήνοντας με αυτόν τον τρόπο πλούσια και αποκαλυπτικά ίχνη για την ιδιωτική ζωή των ατόμων σε καθημερινή βάση. Οι νέες κατηγορίες μεταδεδομένων, όπως δεδομένα γεωεντοπισμού, βιομετρικά δεδομένα, δεδομένα αναγνώρισης προσώπου και δακτυλικών αποτυπωμάτων αποκαλύπτουν ζωτικές πληροφορίες για τα υποκείμενα, ιδιαίτερα μάλιστα όταν συλλέγονται σε μεγάλη κλίμακα σε ολόκληρο τον πληθυσμό για σκοπούς παρακολούθησης.

Επιπλέον, η φύση των μεταδεδομένων επικοινωνίας είναι τέτοια που τα ανάγει σε πληροφοριακό χρυσό, λόγω της ευκολίας συλλογής και ανάλυσής τους, καθώς αποτελούν από τη φύση τους δομημένα δεδομένα με τυποποιημένη και προβλέψιμη μορφή, αφού

[187] Mitrou, L. (2007) *"Communications Data Retention: A Pandora's Box for Rights and Liberties?"*. Σε Acquisti, A., Gritzalis, S., Lambrinoudakis, C., Di Vimercati, S. Digital Privacy, Theory, Technologies and Practices. New York: Auerbach Publications, σελ 423. Διαθέσιμο στο: https://www.academia.edu/8379843/Communications_Data_Retention_A_Pandoras_Box_for_Rights_and_Liberties [Ημερομηνία πρόσβασης: 17/1/2023]

αποτυπώνουν κυρίως νούμερα, όπως τηλεφωνικούς αριθμούς, συντεταγμένες, ημερομηνία, ώρα και διάρκεια της επικοινωνίας, με αποτέλεσμα να μπορούν να υποβληθούν εύκολα σε ποσοτική ανάλυση σε μεγάλη κλίμακα. Η τυποποιημένη φύση τους έχει καταστήσει ακόμα πιο εύκολη την επεξεργασία τους με τη ραγδαία εξέλιξη της τεχνολογίας κατά τις τελευταίες δεκαετίες, την ψηφιακή εξόρυξη δεδομένων (data mining) μέσω εξελιγμένων υπολογιστικών προγραμμάτων και τη δυνατότητα συλλογής, αποθήκευσης κι επεξεργασίας τεράστιου όγκου δεδομένων προσωπικών επικοινωνιών, που μπορούν με ευχέρεια να μετατρέψουν αυτά τα ίχνη επικοινωνίας σε ουσιαστικές και ζωτικές πληροφορίες για τα υποκείμενα. Από την άλλη πλευρά, το περιεχόμενο της επικοινωνίας δεν διαθέτει δομημένη φύση, καθώς στερείται μιας κοινής ενιαίας μορφής, με αποτέλεσμα να είναι εξαιρετικά δύσκολο να υποστεί επεξεργασία με τον ίδιο αυτοματοποιημένο τρόπο, όπως τα μεταδεδομένα επικοινωνίας. Το περιεχόμενο επηρεάζεται άμεσα από υποκειμενικούς και απρόβλεπτους παράγοντες, αφού μπορεί να είναι αποτυπωμένο σε έμμεση ή δυσνόητη μορφή, μπορεί να εκφέρεται με υπονοούμενα ή σε γλώσσα, που δεν είναι εύκολα ή αυτόματα κατανοητή, έτσι ώστε η «ανάγνωση», η «ακρόαση» και η επεξεργασία του να αποτελεί δύσκολο εγχείρημα, δεδομένου μάλιστα ότι η κρυπτογράφησή του πραγματοποιείται ευκολότερα από τα μεταδεδομένα.[188]

Παρά δε το γεγονός ότι η τεχνική της αυτοματοποιημένης αποκρυπτογράφησης της επικοινωνίας έχει εξελιχθεί τεχνολογικά, εξακολουθεί από τη φύση της να αποτελεί μια δύσκολη και επιρρεπής σε σφάλματα διαδικασία, με αποτέλεσμα η απομαγνητοφώνηση και η εξόρυξη του περιεχομένου εκατοντάδων εκατομμυρίων επικοινωνιών ημερησίως να αποτελεί ακόμα πιο δύσκολο έργο. Δεν προκαλεί έκπληξη, λοιπόν, το γεγονός ότι στις περιπτώσεις επιτήρησης των επικοινωνιών ειδικά μέσω κατασκοπευτικών λογισμικών οι μυστικές υπηρεσίες πληροφοριών και οι Αρχές επιβολής του νόμου καταφεύγουν πρωτίστως στα μεταδεδομένα επικοινωνίας, αφού η συλλογή κι η επεξεργασία τους πραγματοποιείται πιο εύκολα, οικονομικά και αποδοτικά σε σύγκριση με την ανάλυση του περιεχομένου της επικοινωνίας, που δημιουργεί ανυπέρβλητες δυσκολίες λόγω της φύσης τους.[189]

---

[188] Bernal, P. (2016) *"Data gathering, surveillance and human rights: recasting the debate"*. Journal of Cyber Policy, 1(2). Σελ. 248

[189] Felten, E. (2013) "*Written Testimony"*, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act. United States Senate,, σελ. 6

Ακόμα, εφόσον τα κατασκοπευτικά λογισμικά έχουν άμεση πρόσβαση σε όλες τις εφαρμογές ενός συστήματος ή ενός τηλεφώνου τα μεταδεδομένα επικοινωνίας, που συλλέγονται σε ευρεία κλίμακα από τα ψηφιακά μέσα επικοινωνίας, όπως το Google, το Facebook και το Twitter αποτελούν ακριβές αποτυπώματα της καθημερινής ζωής των ατόμων, εμφανίζοντας παράλληλα τις εν λόγω πλατφόρμες ως ουδέτερους μεσολαβητές. Ως εκ τούτου, ο ψηφιακός μετασχηματισμός της επικοινωνίας πυροδότησε μια βιομηχανία, που χτίστηκε πάνω στη σπουδαιότητα και την ανεκτίμητη αξία των μεταδεδομένων επικοινωνίας, ήτοι σε αυτά τα αυτοματοποιημένα αρχεία καταγραφής, που αποτυπώνουν με ακρίβεια τις συνθήκες της επικοινωνίας . Άξιο μνείας αποτελεί το γεγονός ότι κατά την τελευταία δεκαετία, τα μεταδεδομένα χρησιμοποιούνται ευρέως από τον ιδιωτικό τομέα και την αγορά προσωπικών πληροφοριών για σκοπούς προσωποποιημένης διαφήμισης και άμεσου μάρκετινγκ, καθώς έχουν εμφανιστεί πάροχοι, που προσφέρουν υπηρεσίες παρακολούθησης μέσω λογισμικών, οι οποίες βασίζονται στη σάρωση μεταδεδομένων επικοινωνίας και ειδικότερα πληροφοριών σχετικών με τη γεωγραφική θέση του εξοπλισμού του χρήστη και προσφέρουν δυνατότητες, όπως ο προσδιορισμός του αριθμού των προσώπων, που διαμένουν σε μια συγκεκριμένη περιοχή. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για οχληρούς σκοπούς, όπως για την αποστολή εμπορικών μηνυμάτων σε τελικούς χρήστες κατά την είσοδό τους σε κάποιο κατάστημα, με εξατομικευμένες προσφορές ή ακόμα και για τη μακροπρόθεσμη παρακολούθηση ατόμων, συμπεριλαμβανομένων των επαναλαμβανόμενων επισκέψεων σε καθορισμένες τοποθεσίες.[190] Οι εν λόγω βιομηχανίες έχουν εκτινάξει στα ύψη την κερδοφορία τους, χρησιμοποιώντας τις πληροφορίες, που συνάγονται από τα μεταδεδομένα επικοινωνίας, με αποτέλεσμα να πιέζουν ασφυκτικά για τη δημιουργία βάσεων δεδομένων απαρτιζόμενων από αυτά. Με το πρόσχημα ότι οι χρήστες έχουν παράσχει συγκατάθεση για τη χρήση των εν λόγω δεδομένων, χωρίς βέβαια να έχουν κατανοήσει το επίπεδο διείσδυσής τους στην ιδιωτική τους ζωή, τα μεταδεδομένα επικοινωνίας αποθηκεύονται και χρησιμοποιούνται για εμπορικούς σκοπούς.

[190] Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων (2017) Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 10-1-2017 για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της Οδηγίας 2002/58/ΕΚ, 2017/0003, Αιτ. Σκ. 25.

Περαιτέρω, αποτελεί κοινή γνώση ότι τα μεταδεδομένα επικοινωνίας ανέκαθεν χρησιμοποιούνταν για στρατιωτικούς σκοπούς και λόγους στρατηγικής πολέμου, αφού για πάνω από έναν αιώνα οι στρατιωτικές δυνάμεις βασίζονται σε αυτά, προκειμένου να αποκωδικοποιήσουν τις τακτικές των εχθρών τους. Τις τελευταίες δε δεκαετίες τα εξωτερικά στοιχεία επικοινωνίας έχουν καταστεί σύνηθες εργαλείο για τη διαφύλαξη της δημόσιας ασφάλειας, την αντιμετώπιση της τρομοκρατίας και τη διερεύνηση εγκληματικών δραστηριοτήτων μέσω τις παρακολούθησής. Άλλωστε, στο πλαίσιο της παρακολούθησης των υποκειμένων, η προγνωστική ανάλυση και η συσχέτιση μοτίβων μεταδεδομένων με την πραγματική ή δυνητική συμπεριφορά των ατόμων παρέχει αποκαλυπτικές πληροφορίες για το ποιοι είμαστε και τι κάνουμε. Συνεπώς, ευχερώς διαγιγνώσκεται ότι οι κρατικές Αρχές και οι εθνικές μυστικές υπηρεσίες, έχοντας στη διάθεσή τους ισχυρούς διαθέσιμους πόρους όπως κατασκοπευτικά λογισμικά, μπορούν να προβούν στη συλλογή και επεξεργασία των μεταδεδομένων επικοινωνίας των πολιτών σε τεράστια κλίμακα και να χρησιμοποιήσουν τα εν λόγω δεδομένα τόσο σε εθνικό επίπεδο ενάντια στους πολίτες. Η συλλογή, η αποστολή και η αποθήκευση αυτών των προσωπικών δεδομένων από και σε λογισμικά κατασκοπείας με servers εκτός Ε.Ε. είναι επίσης ένα ιδιαίτερα σοβαρό πρόβλημα που ανακύπτει από την πολυπλοκότητα των λογισμικών κατασκοπείας. Κανείς δεν μπορεί να εγγυηθεί σε ποια χώρα θα διαβιβαστούν τα προσωπικά δεδομένα και αν η χώρα αυτή θα διαθέτει επαρκές επίπεδο προστασίας σύμφωνα με τις αποφάσεις τη Ευρωπαϊκής Επιτροπής και τις απαιτήσεις του ΓΚΠΔ.

### 4.3. Οι μαζικές παρακολουθήσεις

Άλλο ένα συναφές ζήτημα που εγείρεται δεδομένου ότι πλέον το εύρος των παρακολουθήσεων και οι δυνατότητες των λογισμικών κατασκοπείας δεν περιορίζονται σε στοχευμένα άτομα είναι οι μαζικές παρακολουθήσεις. Οι παρακολουθήσεις μέσω των λογισμικών κατασκοπείας υπερβαίνουν το ζωτικό πλαίσιο του στόχου, εκτεινόμενες σε κοντινά υποκείμενα δικαίου, όπως θα μπορούσε εντός του χώρου εστίασης, να είναι οι θαμώνες παρακείμενων τραπεζιών, οι συνομιλητές, η οικογένεια. Δεν αποκλείεται επίσης, μεταξύ των υποκλεπτόμενων συνομιλιών να περιληφθούν και επικοινωνίες του παρακολουθούμενου υποκειμένου με τον δικηγόρο του ή με τον γιατρό του, για παράδειγμα – κατηγορία επικοινωνίας, η οποία διέπεται από αυξημένη προστασία λόγω

επαγγελματικού απορρήτου[191]– ή επικοινωνία δημοσιογράφων με τις «πηγές» τους.[192] Και κατά τούτο, η υπέρβαση του μέτρου που συντελείται συνιστά απόκλιση από την αρχή της αναλογικότητας.

Σε ό,τι αφορά εξάλλου, τις θέσεις του ΕΔΔΑ[193] για τις μη στοχευμένες παρακολουθήσεις – «μαζικές», όπως άλλως έχει επικρατήσει να αποδίδονται,[194] το ΕΔΔΑ έχει και περί αυτών θέσει τα κριτήριά του.[195] Στην πρόσφατη απόφασή του Big Brother Watch and others v. The United Kingdom του 2021, επανερχόμενο το ΕΔΔΑ στο ζήτημα των μαζικών παρακολουθήσεων, επισημαίνει συνεκτιμώντας τις σύγχρονες απειλές και τους παράγοντες διακινδύνευσης της εθνικής ασφάλειας ότι καταρχάς, οι μη στοχευμένες παρακολουθήσεις δεν προσκρούουν επί της αρχής, στον κανονιστικό πυρήνα του δικαιώματος, υπό την προϋπόθεση ότι τηρούνται οι διαδικαστικές προϋποθέσεις του άρθρο 8 ΕΣΔΑ. Το ΕΔΔΑ δεν παραλείπει εντούτοις, να αναδείξει τον αυξημένο κίνδυνο αυθαιρεσίας που εγκυμονούν τέτοιες επιχειρησιακές πρακτικές. Για τον λόγο αυτό, προσδίδει ιδιαίτερη βαρύτητα στην ανάγκη εγγυήσεων που διατρέχουν καθ' ολοκληρίαν τη διαδικασία σε όλα δηλαδή, τα στάδια εφαρμογής του μέτρου μυστικής παρακολούθησης.[196] Η προσέγγιση αυτή του ΕΔΔΑ σημαίνει ότι σε εθνικό επίπεδο πρέπει να γίνεται έλεγχος του κριτηρίου της αναγκαιότητας και της αναλογικότητας σε κάθε στάδιο της άρσης. Επιπλέον,

---

[191] Βλ. ΕΔΔΑ, *Michaud v. France* 6 Décembre 2012, παρ. 172 επ. και ΕΔΔΑ *Kopp v. Switzerland* 25 March 1998, παρ. 73 επ.

[192] Βλ. ΕΔΔΑ, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands* 22 November 2012, παρ. 84 επ., *Fazil Ahmet c. Turquie* 5 Décembre 2006, παρ. 53

[193] ECHR Factsheet September 2022 *"Mass surveillance"*. Διαθέσιμο στο: https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf [Ημερομηνία πρόσβασης: 17/1/2023]

[194] "bulk interception", κατά τη διατύπωση του ΕΔΔΑ, σε αντιδιαστολή με "targeted interception". ΕΔΔΑ, *Ekimdzhiev and others v. Bulgaria* 11 January 2022, παρ. 291 επ., 394 επ., και ΕΔΔΑ *Centrum för Rättvisa v. Sweden*, 19 June 2018, παρ. 86 επ., ΕΔΔΑ *Big Brother Watch and others v. The United Kingdom*, 25 May 2021 παρ. 322 επ. Βλ. και Watt, E. *Verfassungsblog*, (2022) "*The legacy of the privacy versus security narrative in the ECtHR's jurisprudence*". Διαθέσιμο στο: https://verfassungsblog.de/os6-privacy-vs-security/ [Ημερομηνία πρόσβασης: 17/1/2023]

[195] Βλ. ΕΔΔΑ *Centrum för Rättvisa v. Sweden*, ό.π., παρ. 254-278, *Big Brother Watch and Others v. the United Kingdom*, ό.π. παρ. 340-364.

[196] "end-to-end safeguards", Βλ. *Big Brother Watch and others v. The United Kingdom*, ό.π., παρ. 350.

τονίζει ότι αυτός ο έλεγχος πρέπει να γίνεται υπό την εποπτεία ανεξάρτητης αρχής, που να έχει αυτήν την αρμοδιότητα.

Στη ίδια πρόσφατη απόφαση Big Brother and others v. the United Kingdom[197] ειδικά όταν οι μαζικές παρακολουθήσεις στρέφονται κατά δημοσιογράφων, των οποίων οι πηγές είναι απόρρητες, πριν από την έναρξη της διαδικασίας παρακολούθησης πρέπει να υπάρχει δικαστική άδεια η άδεια ανεξάρτητης αρχής που να δικαιολογεί την άρση του απορρήτου για λόγους δημοσίου συμφέροντος και εφόσον δεν υπάρχει λιγότερο επαχθές μέτρο. Το ΕΔΔΑ επισημαίνει ότι ακόμα και αν η παρακολούθηση δεν αφορά τις εμπιστευτικές πληροφορίες είναι πολύ πιθανόν στο πλαίσιο των μη στοχευμένων παρακολουθήσεων αυτές να αποτελέσουν «παράπλευρες απώλειες».

Ιδιαίτερα σημαντική ήταν η απόφαση του ΕΔΔΑ Zakharov v. Russia. Η υπόθεση αφορούσε την εγκατάσταση από τη ρωσική μυστική υπηρεσία ειδικού μηχανισμού στο κινητό τηλέφωνο ενός αρχισυντάκτη και ακτιβιστή. Η παράνομη παρακολούθηση των τηλεφωνικών συνομιλιών του και η ελλιπής πρόβλεψη του εθνικού νόμου οδήγησαν το ΕΔΔΑ στην κατάφαση της παραβίασης του άρθρο 8 της ΕΣΔΑ σε μια απόφαση σταθμό, που όρισε τα κριτήρια του άρθρο 8 της ΕΣΔΑ και την απαγόρευση των εν λευκώ παρακολουθήσεων. Ανάλογης σημασίας ήταν και η απόφαση ΕΔΔΑ Szabo and Vissy v. Hungary στην οποία κρίθηκε ότι η εγκατάσταση ειδικών λογισμικών παρακολούθησης με σκοπό την πρόληψη της τρομοκρατίας οδηγούσε στην επεξεργασία τεράστιου όγκου προσωπικών δεδομένων ακόμα και ατόμων εκτός του πεδίου εύρους της άρσης του απορρήτου, με αποτέλεσμα τις αδικαιολόγητες μαζικές παρακολουθήσεις πολιτών. Αυτού του είδους οι τεχνολογίες κρίθηκε από το ΕΔΔΑ ότι δεν πληρούν τα κριτήρια του άρθρο 8 της

[197] Αντίστοιχα στην απόφαση ΕΔΔΑ Klass and other v. Germany ό.π. στην οποία πέντε δικηγόροι κατήγγειλαν την παρακολούθηση των τηλεφωνικών τους συνομιλίων το ΕΔΔΑ έκρινε με βάση το κριτήριο της αναλογικότητας, ότι τα ιδιαίτερα μέσα παρακολούθησης που χρησιμοποιήθηκαν ήταν δικαιολογημένα από την γερμανική νομοθεσία και απολύτως αναγκαία για την προστασία της εθνικής ασφάλειας και την καταπολέμηση του εγκλήματος. Ανάλογα, εχέγγυα έκρινε το ΕΔΔΑ ότι υπήρχαν και στην υπόθεση ΕΔΔΑ Weber and Saravia v. Germany ό.π. στην οποία οι αιτούντες (δημοσιογράφος και τηλεφωνητής του) προσέβαλαν την ίδια την εθνική νομοθεσία που όριζε τα μέσα παρακολούθησης που μπορεί να χρησιμοποιήσει η Γερμανία.

ΕΣΔΑ, αλλά δεν υπήρχαν και κατάλληλα εχέγγυα από την ίδια την εθνική νομοθεσία, που να εγγυώνται την προστασία του απορρήτου από την χρήση τέτοιων τεχνολογιών.

Καθόσον λοιπόν, ούτε η σχεδιαστική αφετηρία, ούτε ο λειτουργικός προορισμός των κατασκοπευτικών λογισμικών παρέχουν εγγυήσεις για καταγραφή αποκλειστικά στοχευμένη στο παρακολουθούμενο άτομο, γίνεται εύκολα αντιληπτό ότι η διαδικασία υπολείπεται και ως προς τα ειδικότερα κριτήρια που θέτει το ΕΔΔΑ στο πεδίο των «στρατηγικών» άρσεων.[198]

Στην ελληνική έννομη τάξη υφίσταται το άρθρο 292Δ του ΠΚ[199] το οποίο ρυθμίζει τις προσβολές του απορρήτου του κοινού. Πρόκειται για ρύθμιση που αναφέρεται στη μαζική παραβίαση του απορρήτου από την οποία προκύπτει κοινός κίνδυνος.

### 4.4. Κριτική επισκόπηση του νέου νόμου 5002/2022 «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών.»

Σε απάντηση στις εγχώριες εξελίξεις η ελληνική κυβέρνηση έθεσε σε διαβούλευση στο τέλος του 2022 μια πρόταση νομοσχεδίου με τίτλο «*Διαδικασία άρσης του απορρήτου των*

---

198 Βλ. T. Kaldani; Z. Prokopets Information Society Department DGI (2022)04, Council of Europe *"PEGASUS SPYWARE and its impacts on human rights"* ό.π. σελ. 13 επ.

199 *«Προσβολές του απορρήτου των τηλεπικοινωνιών του κοινού: 1. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση σε σύνδεση ή σε δίκτυο παροχής στο κοινό υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας ή σε σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, εάν από την πράξη μπορεί να προκύψει κοινός κίνδυνος για το απόρρητο του περιεχομένου τηλεφωνικών ή ηλεκτρονικών επικοινωνιών ή των στοιχείων της θέσης ή κίνησης αυτών, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.*

*2. Αν ο δράστης της πράξης της προηγούμενης παραγράφου είναι πάροχος υπηρεσιών τηλεφωνίας ή ηλεκτρονικής επικοινωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος της διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή αποβλέπει να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος επιβάλλεται φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή.»*

*επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών»*.[200] Η πρόταση σχεδίου νόμου φιλοδοξεί να εξασφαλίσει την αναγκαία ισορροπία μεταξύ της προστασίας της ιδιωτικότητας και της εθνικής ασφάλειας, εντός του συνταγματικού πλαισίου και στη βάση των καλύτερων διεθνών πρακτικών. Ενισχύει τα δικαιώματα των πολιτών απέναντι στις απειλές που συνδέονται με την τεχνολογική εξέλιξη, εκσυγχρονίζοντας ταυτόχρονα το σχετικό νομοθετικό πλαίσιο που ανατρέχει στο 1994, αντιμετωπίζοντας τις ελλείψεις που διαπιστώθηκαν από τις πρόσφατες εξελίξεις. Η πρόταση σχεδίου υπερψηφίστηκε από τη Βουλή και πλέον αποτελεί τον ν. 5002/2022 που δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως.[201]

Σκοπός του νόμου, είναι η θωράκιση και ο εκσυγχρονισμός της διαδικασίας άρσης του απορρήτου των επικοινωνιών σύμφωνα με το άρθρο 19 Σ., η βελτιστοποίηση της δράσης της ΕΥΠ, η προστασία του απορρήτου των επικοινωνιών από λογισμικά παρακολούθησης, η οργανική και λειτουργική αναβάθμιση του επιπέδου κυβερνοασφάλειας στη χώρα, και η αποτελεσματικότερη προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Αντικείμενο ης πρότασης είναι η εξαντλητική ρύθμιση της διαδικασίας άρσης του απορρήτου των επικοινωνιών, η αναδιάρθρωση της ΕΥΠ, το νομικό πλαίσιο της εμπορίας, κατοχής και χρήσης απαγορευμένων λογισμικών παρακολούθησης, η σύσταση και λειτουργία Επιτροπής Συντονισμού για θέματα Κυβερνοασφάλειας, και η τροποποίηση των εθνικών ρυθμίσεων ενσωμάτωσης στην εθνική έννομη τάξη της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για 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.

---

[200] Η πρόταση σχεδίου νόμου είναι διαθέσιμη στο: http://www.opengov.gr/ministryofjustice/?p=16477 [Ημερομηνία πρόσβασης: 19/1/2023]

[201] Ν. 5002/2022 - ΦΕΚ 228/Α/9-12-2022: «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών» Διαθέσιμος στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-5002-2022.html [Ημερομηνία πρόσβασης: 19/1/2023]

Βασικά σημεία της πρότασης αποτελεί η προσθήκη ποινικών διατάξεων και η τροποποίηση των υπαρχουσών σχετικά με τη χρήση λογισμικών παρακολούθησης. Με το άρθρο 10 του ν. 5002/2022 τροποποιείται το άρθρο 370Α ΠΚ ως προς το πλαίσιο ποινής. Έτσι, η παραβίαση του απορρήτου της επικοινωνίας πλέον ορίζεται ως κακούργημα και όχι ως απλό πλημμέλημα που ήταν έως σήμερα,[202] η χρήση της πληροφορίας τιμωρείται ασχέτως αν ήταν αθέμιτη ή θεμιτή και προστίθεται η παρ. 5 σχετικά με την παραβίαση του στρατιωτικού και διπλωματικού απορρήτου της εθνικής ασφάλειας και της ασφάλειας των εγκαταστάσεων κοινής ωφέλειας. Με τον ίδιο τρόπο τροποποιείται στο άρθρο 11 του ν. 5002/2022 και το ά. 370Ε ΠΚ σχετικά με την παραβίαση των μη δημόσιων διαβιβάσεων και από πλημμέλημα γίνεται κακούργημα, ενώ προστίθεται και η παρ. 3 σχετικά με το στρατιωτικό και

[202] «*Παραβίαση του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας: 1.Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών σταθερής ή κινητής τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή δεδομένα επικοινωνίας (κίνησης και θέσης) τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον, χωρίς τη ρητή συναίνεση του τελευταίου.*

*2.Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων που δεν διεξάγεται δημόσια ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.*

*3.Όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.*

*4.Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών και χρηματική ποινή. 5.Αν οι πράξεις των παραγράφων 1 και 3 συνιστούν παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, επιβάλλεται κάθειρξη.»*

διπλωματικό απόρρητο.[203] Αντίστοιχα, η εμπορία και η απλή κατοχή, που σήμερα δεν ποινικοποιούνταν στην ελληνική νομοθεσία, χαρακτηρίζονται ως πλημμέλημα με βάση το άρθρο 12 του ν. 5002/2022, με την προσθήκη του άρθρο 370ΣΤ ΠΚ Τα απαγορευμένα λογισμικά[204] και συσκευές παρακολούθησης καταγράφονται σε ειδικό κατάλογο δημόσια προσβάσιμο και διαρκώς επικαιροποιούμενο, ενώ η προμήθεια λογισμικών παρακολούθησης από το Δημόσιο είναι δυνατή υπό τις προϋποθέσεις προεδρικού διατάγματος.

Ακόμα προς διόρθωση της υπαγωγής της ΕΥΠ απευθείας στον Πρωθυπουργό και με σκοπό την εύρυθμη λειτουργία της τίθενται νέες δικλείδες ασφαλείας. Για πρώτη φορά ιδρύονται η Ακαδημία Πληροφοριών και Αντικατασκοπείας με αποστολή την εκπαίδευση, επιμόρφωση και εξειδίκευση του προσωπικού και Μονάδα Εσωτερικού Ελέγχου για τον έλεγχο φαινομένων παράβασης καθήκοντος και διαφθοράς στην ΕΥΠ, ενώ προβλέπονται εγγυήσεις δημοσιότητας στη λειτουργία του Κέντρου Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας της ΕΥΠ. Τίθενται ειδικές προϋποθέσεις για την επιλογή του Διοικητή, ο οποίος μπορεί να είναι μόνο διπλωμάτης ή απόστρατος ανώτατος αξιωματικός. Ως προς τη λειτουργία της ΕΥΠ, η Αρχή Ασφαλείας Πληροφοριών (INFOSEC) της ΕΥΠ

---

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

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

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

[204] Βλ. άρθρα 13 και 14 ν. 5022/2022. Απαγορευμένα λογισμικά ή συσκευές παρακολούθησης θεωρούνται λογισμικά ή συσκευές με δυνατότητα υποκλοπής, καταγραφής και κάθε είδους άντλησης περιεχομένου ή και δεδομένων επικοινωνίας (κίνησης και θέσης), τα οποία καθορίζονται με απόφαση της Ολομέλειας της ΑΔΑΕ. Ο κατάλογος απαγορευμένων λογισμικών ή συσκευών παρακολούθησης επικαιροποιείται το αργότερο κάθε 6 μήνες. Επιπλέον, με ανακοίνωση του Διοικητή της ΕΥΠ, που αναρτάται στον ιστοχώρο της Υπηρεσίας ενημερώνεται το κοινό για τα απαγορευμένα λογισμικά, τον τρόπο δράσης τους και τα μέτρα προστασίας που δύναται να λάβει έναντι αυτών.

καθίσταται αρμόδια για τη σύνταξη πολιτικών ασφαλείας και οδηγιών διαχείρισης των διαβαθμισμένων πληροφοριών σε όλα τα δίκτυα και τους χώρους της Προεδρίας της Κυβέρνησης και των Υπουργείων σε συνεργασία μαζί τους, καθώς και για τη συνεχή ενημέρωσή τους σε θέματα ασφάλειας, ενώ καταργείται η δυνατότητα απόρρητων συμβάσεων στο Κέντρο Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας.

Η σημαντικότερη ίσως αλλαγή αφορά το πλαίσιο νόμιμη άρσης του απορρήτου. Όπως προκύπτει από το νόμο, ενώ έως σήμερα την αίτηση θα μπορούσε να υποβάλλει κάθε δημόσια αρχή, αίτηση για άρση απορρήτου για λόγους εθνικής ασφάλειας μπορεί να ζητήσει μόνο η ΕΥΠ ή η Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας της Ελληνικής Αστυνομίας. Παράλληλα, τίθεται με το νόμο ένα τριπλό φίλτρο εγγυήσεων για την άρση απορρήτου: α) τη διαδικασία επισπεύδει μόνο η ΕΥΠ ή η Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας της Ελληνικής Αστυνομίας που υποβάλλουν το αίτημα άρσης, β) διπλή εισαγγελική κρίση και γ) το αίτημα της άρσης πρέπει να στηρίζεται σε συγκεκριμένα στοιχεία που καθιστούν άμεση και εξαιρετικά πιθανή τη διακινδύνευση της εθνικής ασφάλειας.[205]

Με το νομοσχέδιο «λόγοι εθνικής ασφάλειας» αποτελούν λόγοι που σχετίζονται με « με την προστασία των βασικών λειτουργιών του κράτους και των θεμελιωδών συμφερόντων των Ελλήνων πολιτών, όπως, ιδίως, λόγοι σχετικοί με την εθνική άμυνα, την εξωτερική πολιτική, την ενεργειακή ασφάλεια και την κυβερνοασφάλεια».

Επιπρόσθετες δικλείδες τίθενται, επίσης για πρώτη φορά, όταν η άρση για λόγους εθνικής ασφάλειας αφορά πολιτικά πρόσωπα, οπότε απαιτείται άμεση και εξαιρετικά πιθανή διακινδύνευση της εθνικής ασφαλείας, καθώς και άδεια του Προέδρου της Βουλής. Ως «Πολιτικά πρόσωπα» θεωρούνται ο Πρόεδρος της Δημοκρατίας, τα μέλη της κυβέρνησης και οι υφυπουργοί, οι βουλευτές του εθνικού και του ευρωπαϊκού κοινοβουλίου, οι αρχηγοί των πολιτικών κομμάτων που εκπροσωπούνται στο εθνικό και το ευρωπαϊκό κοινοβούλιο και τα ανώτατα μονοπρόσωπα όργανα των ΟΤΑ Α’ και Β' βαθμού.

Έως το 2021, η ενημέρωση ήταν στη διακριτική ευχέρεια του αποφασίζοντος οργάνου, μόνο εφόσον δε διακυβευόταν ο σκοπός της άρσης. Έκτοτε δεν ήταν δυνατή η ενημέρωση όταν επρόκειτο για λόγους εθνικής ασφάλειας, ήταν όμως δυνατή για άρσεις προς διακρίβωση

[205] Βλ. άρθρο 4 ν.5002/2022

εγκλημάτων. Προβλέπεται πλέον, η υποχρεωτική γνωστοποίηση της άρσης για λόγους εθνικής ασφάλειας, μετά την πάροδο τριών ετών από την παύση της, υπό την προϋπόθεση ότι δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε η άρση, όπως αξιολογείται από ειδικό τριμελές όργανο με τη συμμετοχή των δύο εισαγγελικών λειτουργών και του προέδρου της ΑΔΑΕ.

Αναφορικά με τις άρσεις για διακρίβωση εγκλημάτων ο κατάλογος εγκλημάτων ήταν εξαιρετικά ευρύς και περιλάμβανε κακουργήματα και πλημμελήματα του ποινικού κώδικα και ειδικών ποινικών νόμων. Η άρση του απορρήτου επιτρέπεται πλέον μόνο σε εγκλήματα ιδιαίτερης απαξίας, κακουργήματα και ορισμένα σοβαρά πλημμελήματα, για τη διακρίβωση των οποίων ο περιορισμός του δικαιώματος στο απόρρητο της επικοινωνίας είναι αναγκαίος.[206] Ωστόσο, ο κατάλογος των πλημμελημάτων για τα οποία μπορεί να διαταχθεί η άρση του απορρήτου είναι ιδιαίτερα ευρύς, με αποτέλεσμα η συνταγματική πρόβλεψη του άρθρο 19 παρ. 1 Σ για την άρση του απορρήτου από εξαίρεση να γίνεται πλέον ο κανόνας.

Η σχετική διαδικασία δεν αλλάζει. Η άρση ορίζεται με βούλευμα του Συμβουλίου Εφετών ή Πλημμελειοδικών μετά από αίτηση του Εισαγγελέα ή του Ανακριτή. Μόνο σε εξαιρετικά επείγουσες περιπτώσεις, την άρση μπορεί να διατάξει ο Εισαγγελέας και ο Ανακριτής που στη συνέχεια υποχρεούνται να εισαγάγουν το ζήτημα με σχετική αίτηση στο Δικαστικό Συμβούλιο μέσα σε προθεσμία 3 ημερών. Η ΑΔΑΕ αποφασίζει αφού λήξει η άρση την ενημέρωση του υποκειμένου, με τη σύμφωνη γνώμη του Εισαγγελέα του Αρείου Πάγου και υπό την προϋπόθεση, ότι δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε το μέτρο της άρσης. Το μόνο που προστίθεται είναι ότι η ΑΔΑΕ απαντά επί του αιτήματος εντός 3 μηνών.

Η διαδικασία καταστροφής του υλικού παρακολούθησης τυποποιείται περαιτέρω καθώς έως σήμερα, προβλεπόταν η καταστροφή των αρχείων χωρίς όμως συγκεκριμένα χρονικά πλαίσια και συγκεκριμένες διαδικασίες. Για το περιεχόμενο της παρακολούθησης για λόγους εθνικής ασφάλειας, προβλέπεται καταρχήν αυτόματη διαγραφή μετά την πάροδο 6 μηνών από την παύση ισχύος της εισαγγελικής διάταξης. Ο φάκελος με το υλικό τεκμηρίωσης για την άρση, καταστρέφεται μετά την πάροδο 10 ετών από την παύση της εισαγγελικής διάταξης. Επιπλέον, υπάρχει δυνατότητα πλήρους ψηφιοποίησης του αρχείου

[206] άρθρο 6 ν. 5002/2022

για εύκολη αναζήτηση και περισσότερη ασφάλεια. Σε περίπτωση καταστροφής ή διαγραφής συντάσσεται σχετική έκθεση.[207]

Έως σήμερα οι άρσεις διατάσσονταν για δίμηνο με δυνατότητα ανανέωσης και δεν υπήρχε απώτατο χρονικό όριο για άρσεις για λόγους εθνικής ασφάλειας. Πλέον το όριο των 10 μηνών καταλαμβάνει και τις άρσεις για λόγους εθνικής ασφάλειας όπως και τις άρσεις για διακρίβωση εγκλημάτων, εκτός εάν η αίτηση στηρίζεται σε συγκεκριμένα στοιχεία που καθιστούν άμεση και εξαιρετικά πιθανή τη διακινδύνευση της εθνικής ασφάλειας .[208] Για τις άρσεις για διακρίβωση εγκλημάτων το περιεχόμενο σχετίζεται με τη δικογραφία και αποτελεί αποδεικτικό υλικό.[209]

Από το πεδίο της ρύθμισης δεν ήταν δυνατόν να εκφεύγει η κυβερνοασφάλεια που είναι άρρηκτα συνδεδεμένη με την χρήση λογισμικών κατασκοπείας.[210] Θεσπίζεται νέο αυστηρό πλαίσιο προστασίας της κυβερνοασφάλειας και ενισχύεται η προστασία των προσωπικών δεδομένων. Το πιο σημαντικό πρόβλημα είναι η πολυδιάσπαση των δομών κυβερνοασφάλειας στη χώρα. Για τον λόγο αυτό συστήνεται Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας, που λειτουργεί ως συντονιστικό όργανο μεταξύ: α) της Γενικής Διεύθυνσης Κυβερνοασφάλειας της Γενικής Γραμματείας Τηλεπικοινωνιών και Ταχυδρομείων του Υπουργείου Ψηφιακής Διακυβέρνησης, που έχει ορισθεί ως Εθνική Αρχή της Κυβερνοασφάλειας, β) της Διεύθυνσης Κυβερνοάμυνας του ΓΕΕΘΑ, που έχει ορισθεί ως αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών, γ) της Διεύθυνσης Κυβερνοχώρου της ΕΥΠ ως ομάδα αντιμετώπισης ηλεκτρονικών επιθέσεων και δ) της Ελληνικής Αστυνομίας. Οι αρμοδιότητες της Επιτροπής είναι: α) να παρέχει κατευθύνσεις σε περίπτωση εξαιρετικού συμβάντος που ενέχει στρατηγικό κίνδυνο, β) να συντονίζει, παρακολουθεί και αξιολογεί την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας, γ) να εγκρίνει το Εθνικό Σχέδιο Έκτακτης Ανάγκης, δ) να εισηγείται στο ΚΥ.Σ.Ε.Α. οποιοδήποτε θέμα άπτεται της Κυβερνοασφάλειας και ε) να αίρει τυχόν διαφωνίες ως προς τις αρμοδιότητες και τους ρόλους των φορέων Κυβερνοασφάλειας.

[207] άρθρο 5 ν. 5002/2022

[208] άρθρο 8 παρ. 4 ν. 5002/2022

[209] άρθρο 7 ν. 5002/2022

[210] Κεφάλαιο Ε' ν. 5002/2022

Στο Υπουργείο Ψηφιακής Διακυβέρνησης λειτουργεί Ενοποιημένο Κέντρο Αναφοράς Κυβερνοασφάλειας. Το Κέντρο έχει ως σκοπό την ανάπτυξη, υποστήριξη και ενδυνάμωση των ικανοτήτων σε εθνικό επίπεδο για την έγκαιρη ανίχνευση και αντιμετώπιση κυβερνοαπειλών σε όλη την επικράτεια, ιδίως μέσω της ενίσχυσης των δυνατοτήτων έγκαιρης προειδοποίησης, ανίχνευσης και αντιμετώπισης κυβερνοεπιθέσεων.[211] Για πρώτη φορά επίσης καταρτίζεται Εθνικό Σχέδιο Αποτίμησης Επικινδυνότητας Συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών για την αναγνώριση, ανάλυση και αποτίμηση των κινδύνων και των επιπτώσεών τους για την ασφάλεια των συστημάτων τεχνολογίας πληροφορικής και επικοινωνιών σε εθνικό επίπεδο. Το Σχέδιο εμπεριέχει την αναγνώριση, ανάλυση και αποτίμηση των κινδύνων και των επιπτώσεων τους για την ασφάλεια των συστημάτων τεχνολογίας πληροφορικής και επικοινωνιών σε εθνικό επίπεδο. Για την κατάρτιση του Σχεδίου λαμβάνεται υπόψη κάθε κατηγορία πιθανής απειλής, και ιδίως απειλές που σχετίζονται με κακόβουλες ενέργειες, φυσικά φαινόμενα, τεχνικές αστοχίες, δυσλειτουργίες ή ανθρώπινα λάθη, με σκοπό την αξιολόγηση της έκτασης και της κρισιμότητας των επιπτώσεων των απειλών αυτών σε εθνικό επίπεδο. Επιπλέον, η Εθνική Αρχή της Κυβερνοασφάλειας και η Διεύθυνση Κυβερνοχώρου μεριμνούν για την παρακολούθηση γνωστών απειλών και ευπαθειών συστημάτων πληροφορικής και επικοινωνιών και την παροχή ενημέρωσης σχετικά με αυτές.

Αίρονται, τέλος, ασάφειες στην ενσωμάτωση του σχετικού ενωσιακού πλαισίου για την προστασία των προσωπικών δεδομένων.[212] Επιπλέον, για την παρακολούθηση των σχετικών πολιτικών, συστήνεται στο Υπουργείο Δικαιοσύνης Μόνιμη Επιστημονική Επιτροπή Προσωπικών Δεδομένων με αποστολή: α) την παρακολούθηση των επιστημονικών και νομολογιακών εξελίξεων και του εθνικού και ενωσιακού νομικού πλαισίου προστασίας των δεδομένων προσωπικού χαρακτήρα, β) την υποβολή τεκμηριωμένων προτάσεων για την ανάληψη νομοθετικής δράσης στον τομέα αυτό, γ) την άσκηση καθηκόντων

[211] Lawspot (2022) *«Στη Βουλή το νομοσχέδιο για τη διαδικασία άρσης απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών»* Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/sti-voyli-nomoshedio-gia-ti-diadikasia-arsis-aporritoy-ton-epikoinonion-kyvernoasfaleia [Ημερομηνία πρόσβασης: 19/1/2023]

[212] Κεφάλαιο ΣΤ' ν. 5002/2022

νομοπαρασκευαστικού έργου και δ) την αντιπροσώπευση του Υπουργείου Δικαιοσύνης σε διεθνή όργανα.[213]

Εντούτοις, ανακύπτουν ορισμένα ζητήματα στο νέο νόμο, τα οποία είναι άξια αναφοράς μέχρι να δούμε πως θα εφαρμοστούν και στην πράξη. Πρώτα από όλα είναι ιδιαίτερα σημαντικό να τονιστεί ότι τα πολυπρόσωπα όργανα σίγουρα λειτουργούν καλύτερα από ένα μονοπρόσωπο όργανο, όπως ήταν ο ένας Εισαγγελέας που εξέδιδε την διάταξη άρσης του απορρήτου. Επομένως, η διπλή εισαγγελική κρίση είναι ένα θετικό πρώτο βήμα, αν και ίσως το Δικαστικό Συμβούλιο ίσως να ήταν καταλληλότερο, δεδομένης της εγγύησης ανεξαρτησίας του σε αντίθεση με τον ιδρυματικό χαρακτήρα ενός Εισαγγελέα αποσπασμένου στην ΕΥΠ.[214] Ωστόσο, η έλλειψη επαρκούς αιτιολογίας της διάταξης, που οδήγησε τον Εισαγγελέα στην πρόταξη του συλλογικού καλού έναντι του ατομικού δικαιώματος του απορρήτου, εξακολουθεί να είναι ίσως το σημαντικότερο πρόβλημα και στο νέο νόμο, που αντίκειται στον πυρήνα της δημοκρατίας. Ακόμα και ο δεύτερος Εισαγγελέας θα πρέπει να μπορεί να αντιλαμβάνεται τους λόγους που οδήγησαν τον πρώτο Εισαγγελέα στην άδεια άρσης απορρήτου, πόσο μάλλον όταν το ζήτημα φθάνει έως τον έλεγχο της ΑΔΑΕ και στην κρίση της ορθής στάθμισης της αρχής της αναλογικότητας. Ειδικά σε αντίθεση με την άρση σε περίπτωση διακρίβωσης εγκλημάτων, η άρση για λόγους εθνικής ασφαλείας εξακολουθεί να είναι αναιτιολόγητη και χωρίς αναφορά του προσώπου επί του οποίου διατάχθηκε η άρση,[215] γεγονός που αντίκειται στις αρχές της λογοδοσίας και της διαφάνειας, την στιγμή που η διάταξη δεν κοινοποιείται στα υποκείμενα και τηρείται γενικά το απόρρητο.

Η γνωστοποίηση του θιγόμενου στην περίπτωση άρσης του απορρήτου για λόγους εθνικής ασφάλειας είναι μια πρόοδος, ωστόσο η ένταξη των Εισαγγελέων που διέταξαν την άρση στη διαδικασία δεν παρέχει εχέγγυα ανεξαρτησίας και αφαιρεί από την ΑΔΑΕ την

[213] Καθημερινή (2022) «*Παρακολουθήσεις: Σε διαβούλευση το σχέδιο νόμου – Τι προβλέπει*» Διαθέσιμο στο: https://www.kathimerini.gr/politics/562138606/parakoloythiseis-se-diavoyleysi-to-schedio-nomoy-ti-provlepei/ [Ημερομηνία πρόσβασης: 19/1/2023]

[214] Βλ. Παρατηρήσεις Ολομέλειας ΑΔΑΕ επί της πρότασης σχεδίου νόμου 18/11/2022 διαθέσιμες στο: http://www.adae.gr/fileadmin/documents/PARATIRISEIS_ADAE_GIA_TO_NOMOSXEDIO_21-11-2022.pdf [Ημερομηνία πρόσβασης: 14/2/2023]

[215] Βλ. άρθρο 4 παρ.4 ν. 5002/2022

συνταγματικά και ευρωπαϊκά κατοχυρωμένη ανέκαθεν αρμοδιότητα της εποπτείας. Επιπλέον, στο νόμο αναφέρεται η απλή γνωστοποίηση της επιβολής του μέτρου και όχι της αιτιολογίας επιβολής του, τη στιγμή που οι 3 μήνες προθεσμία είναι ένα μεγάλο χρονικό διάστημα, όταν δε διακυβεύεται ο σκοπός της άρσης. Η γνωστοποίηση των λόγων άρσης είναι άκρως επιβεβλημένη καθώς συνδέεται με το συνταγματικά κατοχυρωμένο δικαίωμα των πολιτών στο άρθρο 20 Σ για αποτελεσματική δικαστική προστασία.

Επιπλέον, η εμπλοκή του Προέδρου της Βουλής στην διαδικασία δεν αποτελεί εχέγγυο ανεξαρτησίας παρά την προσθήκη ενός ακόμα οργάνου. Πώς δύναται άραγε ένα πρόσωπο που δεν εκπροσωπεί καν την Βουλή να συμμετέχει στη διαδικασία άρσης του απορρήτου και ειδικά όταν πρόκειται για άρση του απορρήτου μελών της Βουλής, δη της αντιπολίτευσης; Αξιοσημείωτη είναι η διαπλοκή μέσω της προσθήκης του Προέδρου της Βουλής στη διαδικασία, των λειτουργιών του πολιτεύματος και η καταστρατήγηση της ανεξαρτησίας και της διάκρισης της νομοθετικής από τη δικαστική εξουσία.

Ως προς την καθιέρωση στενής έννοιας της εθνικής ασφάλειας οι απόψεις διίστανται. Οι περισσότεροι θεωρητικοί κρίνουν ότι η έννοια της εθνικής ασφάλειας όπως και της δημοσίας τάξεως θα πρέπει λόγω της νομικής αοριστίας της να ορίζεται όσο πιο στενά γίνεται. Όμως, και κατά το ίδιο το ΕΔΔΑ κρίνεται ιδιαίτερα δύσκολη και ρευστή η ακριβής οριοθέτηση της έννοιας.[216] Για παράδειγμα, ανάλογα με την ιδεολογική προσέγγιση κάποιου θα μπορούσε ή δε θα μπορούσε να θεωρείται κίνδυνος για την εθνική ασφάλεια – και επομένως θα ήταν δυνατή η άρση του απορρήτου- η εισβολή προσφύγων στη χώρα.

Ένα πολύ θετικό βήμα αποτελεί η τήρηση αρχείου κάτι που έως σήμερα δεν υπήρχε. Όμως, είναι ακατανόητο πως σύμφωνα με το άρθρο 4 παρ. 2 τελευταίο εδάφιο του νόμου δεν παρέχεται η δυνατότητα τήρησης αρχείου στις περιπτώσεις εθνικής ασφάλειας για τον δεύτερο Εισαγγελέα, θέτοντας ζητήματα διαφάνειας. Και πάλι όμως, παρά την απαγόρευση της χρήσης εμπορίας κ.λπ. των κατασκοπευτικών λογισμικών, το Δημόσιο υπό προϋποθέσεις μπορεί να προμηθεύεται και να χρησιμοποιεί τέτοια λογισμικά. Οι προϋποθέσεις αυτές δεν είναι συγκεκριμένες και σίγουρα δε λύνουν το πρόβλημα, το οποίο παραμένει να είναι η παραβίαση του απορρήτου και των προσωπικών δεδομένων των πολιτών από τις κυβερνήσεις. Κατά αυτόν τον τρόπο νομιμοποιείται για το Δημόσιο η χρήση

[216] ΕΔΔΑ, *Seks v. Croatia* 3 February 2022

των λογισμικών κατασκοπείας που παρανομοιούνται εν γένει, με εμπλοκή της ΕΥΠ στη διαδικασία, οργάνου που καλείται να χρησιμοποιήσει τα εν λόγω λογισμικά. Τέλος, για ακόμα μια φορά δεν γίνεται καμία αναφορά στα κατάλληλα οργανωτικά και τεχνικά μέτρα τα οποία θα πρέπει να έχουν τα λογισμικά κατασκοπείας, ώστε να συμμορφώνονται με τη νόμιμη επεξεργασία προσωπικών δεδομένων, που θεσπίζει ο ΓΚΠΔ, ενώ θα ήταν και προτιμότερο να κατοχυρωνόταν ένα ένδικο βοήθημα ενώπιον του ΣτΕ, με το οποίο τα θύματα άρσης του απορρήτου θα μπορούσαν να προσφύγουν στη δικαιοσύνη.

**ΣΥΜΠΕΡΑΣΜΑΤΑ**

Η παρείσφρηση των ισχυρών της εξουσίας αξιοποιώντας κάθε δυνατό μέσο ήταν πάντα διαχρονικό φαινόμενο σε όλες τι κοινωνίες. Το δίκαιο κρίνεται ως ουραγός στην προσπάθεια συγκερασμού των αντικρουόμενων συμφερόντων των ισχυρών και των δικαιωμάτων των μειονεκτούντων. Εν προκειμένω, η ειδική και εμπεριστατωμένη αιτιολογία της δικαστικής κρίσης ως προς την ανάγκη άρσης του απορρήτου, με έμφαση κυρίως, στον αναλογικό χαρακτήρα του μέτρου και στην αξιοποίησή του ως έσχατου και όχι ως ισοδύναμου μέσου είναι ένα απαραίτητο νομικό μέτρο ειδικά στην περίπτωση που η άρση του απορρήτου συντελείται με την χρήση του παρεμβατικού μέσου των λογισμικών κατασκοπείας.[217] Εξίσου σημαντική είναι η πραγματική εποπτεία εκ μέρους ανεξάρτητων φορέων ως προς τη διαδικασία και τους όρους άρσης του απορρήτου και φυσικά η αποτροπή του παραγκωνισμού της ως συστατικό στοιχείο των αρχών της δημοκρατίας,[218] τάση που

[217] Βλ. Παπανικολάου, Α. (2020) «*Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*», σελ. 22 επ. Διαθέσιμο σε: https://www.constitutionalism.gr/wp-content/uploads/2020/07/2020-07-papanikolaou-katerina-aporrito-epikoinonias.pdf [Ημερομηνία πρόσβασης: 19/1/2023]

[218] Βλ. αναφορικά με την πρόσφατη κατάργηση του δικαιώματος ενημέρωσης, όταν το μέτρο της άρσης έχει ληφθεί για λόγους εθνικής ασφάλειας. Βλ. Ράμμος, Χ., Γκρίτζαλης, Σ., Παπανικολάου, Α., (2021) «*Αντίθεση του άρθρου 87 Ν. 4790/2021 προς τις εγγυήσεις της ΕΣΔΑ για διαφύλαξη του απορρήτου των επικοινωνιών*», ό.π. και Παπανικολάου, Α. (2022) «*Άρση του επικοινωνιακού απορρήτου και υποχρέωση γνωστοποίησης: ένα δικαιοκρατικό ζήτημα σε εκκρεμότητα*», Επιθεώρηση Δημόσιας Διοίκησης. Διαθέσιμο στο: https://www.lawjournals.unic.ac.cy/index.php/pareview/article/view/35/24 [Ημερομηνία πρόσβασης: 19/1/2023]

φαίνεται να υιοθετήθηκε και στην γνωμοδότηση 1/2023 του Εισαγγελέα του ΑΠ.[219] Προς αυτή την κατεύθυνση, έχει σημασία να επισημανθεί και η κρισιμότητα του δικαιώματος της υπό προϋποθέσεων γνωστοποίησης της απόφασης περί άρσης στο υποκείμενο, προκειμένου να δοθεί στον τελευταίο η δυνατότητα διερεύνησης της νομιμότητας του μέτρου, στο πλαίσιο άσκησης του δικαιώματος δικαστικής προστασίας.

Ομοίως, η προσήλωση στις νομολογιακές αρχές του ΕΔΔΑ και του ΔΕΕ και στο νομικό αξιακό πλαίσιο που αυτές διαμορφώνουν, συνιστά ασφαλή πλοηγό για τα εθνικά δικαστήρια. Οπωσδήποτε δε, διασφαλίζει την ενότητα της νομολογίας των ευρωπαϊκών χωρών και την εμπέδωση αρχών που ενισχύουν τη συνοχή και την αποτελεσματικότητα σε ό,τι αφορά την προστασία του δικαιώματος. Η αυτοσυγκράτηση επίσης, των κρατικών αρχών σε σχέση με την επίκληση της εθνικής ασφάλειας ως λόγου άρσης του επικοινωνιακού απορρήτου συμβάλλει στην αποτροπή καταχρηστικής προσφυγής στο υπό συζήτηση περιοριστικό μέτρο.

Αναφορικά με την πολιτική διάσταση του θέματος, είναι γεγονός ότι η συζήτηση προς το παρόν, εξαντλείται στην καταγραφή μέτρων που θα μπορούσαν να δράσουν αποτρεπτικά εκπέμποντας το μήνυμα ότι η χρήση παράνομου λογισμικού, δεν είναι ανεκτή στο ευρωπαϊκό σύστημα νομικών κανόνων. Πέραν δηλαδή, της αυτονόητης ηθικής απαξίας τέτοιων πρακτικών, είναι σημαντικό να εμπεδωθεί ως απαρέγκλιτος κανόνας η αντίληψη

[219] Βλ. Γνμδ Εισαγγελέα Ντογιάκου, Ι 1/2023 ΑΠ, σχετικά με τις ελεγκτικές αρμοδιότητες των Ανεξάρτητων Αρχών και συγκεκριμένα της ΑΔΑΕ, διαθέσιμη στο: https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-1-2023/ [Ημερομηνία πρόσβασης: 14/2023]. Η Γνωμοδότηση έχει προκαλέσει θύελλα αντιδράσεων νομικών, πολιτικών και κοινωνικών, διότι στην ουσία αφαιρεί την αρμοδιότητα της ΑΔΑΕ να διενεργεί ελέγχους σε περίπτωση καταγγελίας, ενόψει και του νέου ν. 5002/2022 σχετικά με την άρση του απορρήτου και τα κατασκοπευτικά λογισμικά. Σύμφωνα με τον Εισαγγελέα του ΑΠ ο έλεγχος της Αρχής δεν είναι αναγκαίος εφόσον συγκροτείται νέο τριμελές όργανο αποτελούμενο από δύο Εισαγγελικούς λειτουργούς και τον Πρόεδρο της ΑΔΑΕ, το οποίο αποφασίζει για την άρση του απορρήτου. Η Γνωμοδότηση φαίνεται να αντίκειται πρωτίστως στην αρχή διάκρισης των λειτουργιών, αλλά παραβιάζει και το ίδιο το Σύνταγμα που θεσπίζει το θεσμό των Ανεξάρτητων Αρχών ως πυρήνα του ίδιου του δημοκρατικού πολιτεύματος και υπερβαίνει το πεδίο της γνωμοδοτικής αρμοδιότητας του Εισαγγελέα του ΑΠ.

ότι το αποδεικτικό υλικό που παράγεται από την χρήση κατασκοπευτικού λογισμικού συνιστά παράνομο αποδεικτικό μέσο – μη αξιοποιήσιμο συνεπώς, στο πλαίσιο της ποινικής διαδικασίας για τη στοιχειοθέτηση κατηγοριών –[220].

Η θέσπιση πάντως νομοθετικού πλαισίου σχετικά με τον περιορισμό διακίνησης και εξαγωγής λογισμικών αυτής της κατηγορίας είναι ένα θετικό βήμα. Η εποπτεία επί του πεδίου και η υπαγωγή των εταιριών που ειδικεύονται στην παραγωγή κατασκοπευτικού λογισμικού σε κοινούς περιοριστικούς κανόνες είναι αυτονόητο ότι θα δυσχεράνει τη λειτουργία της οικείας αγοράς ήδη στο επίπεδο της πηγής.

Για να μη δαιμονοποιείται, πάντως, η τεχνολογία καθαυτή, δεν θα ήταν άνευ αξίας ο προβληματισμός σε σχέση με την υπαγωγή των προαναφερόμενων λογισμικών σε κανονιστικές προϋποθέσεις, ικανές να εγγυηθούν την ελεγξιμότητα της χρήσης τους. Εάν και εφόσον διασφαλιστεί, δηλαδή, εκ του σχεδιασμού τους (by design) ότι η χρήση τους καταγράφεται με ακρίβεια και τα αποτυπώματά της είναι διαθέσιμα σε κάθε έλεγχο των αρμόδιων προς τούτο οργάνων, τότε ενδεχομένως αίρεται ή έστω περιορίζεται σημαντικά η καχυποψία και τα νομικά εμπόδια που καθιστούν επί του παρόντος, απαγορευτική την αξιοποίησή τους.

Σε κάθε περίπτωση, η συζήτηση περιλαμβάνει φυσικά και τον παιδαγωγικό ρόλο των ευρωπαϊκών οργάνων σχετικά με την εγρήγορση των πολιτών ως προς την οικειοθελή λήψη μέτρων εκ μέρους τους προκειμένου να διασφαλίσουν τα προσωπικά τους δεδομένα και ειδικότερα, το επικοινωνιακό απόρρητο. Κρίσιμη εν προκειμένω, είναι και η διάχυση της αντίληψης που συνδέει τους εγγυητικούς μηχανισμούς του απορρήτου με τον πυρήνα της δημοκρατίας και την αποτελεσματική άσκηση των ατομικών δικαιωμάτων. Όσο τα υποκείμενα δικαίου εμβαθύνουν στην ευθέως ανάλογη σχέση μεταξύ διασφάλισης του απορρήτου και δημοκρατικής νομιμότητας, τόσο περισσότερο απονομιμοποιείται η κανονικοποίηση παράνομων λογισμικών στη συνείδηση των υποψιασμένων χρηστών. Ο ρόλος της κοινωνίας των πολιτών δε θα πάψει ποτέ να είναι κρίσιμος, ειδικά στο πεδίο της προστασίας ευαίσθητων δικαιωμάτων ως συναρτώμενων με την ποιότητα καθαυτή της δημοκρατίας. Γι' αυτό πρωτίστως οι ίδιοι οι πολίτες πρέπει να μην εφησυχάζουν και να διεκδικούν τα αυτονόητα δικαιώματα τους. Η ανάπτυξη και η εφαρμογή τεχνολογιών

[220] Βλ. ΕΔΔΑ, *Dumitru Popescu v. Roumanie* ό.π. παρ. 61 επ.

παρακολούθησης πρέπει να συνοδεύεται από ισχυρά νομικά εχέγγυα που διασφαλίζουν επαρκή και αποτελεσματική προστασία στα άτομα αλλά και εξισορροπούν τα συμφέροντα του κράτους και των ιδιωτών με τα δικαιώματα και τις ελευθερίες των ατόμων. Η θεώρηση του τεχνολογικού ντετερμινισμού, ότι το δίκαιο ακολουθεί ασθμαίνοντας την τεχνολογία πρέπει να ανατραπεί. Ο σύγχρονες τάσεις αναδεικνύουν την ανάγκη, το δίκαιο να προλάβει τη ραγδαία χρήση λογισμικών κατασκοπείας.

Κι ενώ η κρισιμότητα του δικαιώματος στην προστασία του επικοινωνιακού απορρήτου ως κατάφαση δημοκρατικής λειτουργίας των θεσμών αποτελεί κοινό τόπο, η εκθετική διασπορά λογισμικών που το υπονομεύουν δεν επιτρέπει εφησυχασμό, ούτε υποβάθμιση του ζητήματος στο επίπεδο της ποινικής παραβατικότητας, όπως τουλάχιστον φαίνεται να είναι η τάση με τον πρόσφατο νόμο. Επιπλέον, η περιορισμένη μέχρι στιγμής, αποτελεσματικότητα διερεύνησής του προβλήματος, μάλλον επιτείνει την ανησυχία ως προς την ανάσχεση τού φαινομένου. Μένει να δούμε αν τα ανωτέρω μέτρα θα έχουν πραγματικό θετικό αντίκτυπο στη ραγδαία εξάπλωση της νέας τεχνολογίας και στην τάση αύξησης κατασκοπευτικών λογισμικών από τις κυβερνήσεις και τους ιδιώτες. Ωστόσο, ένα νομοθέτημα ειδικά σε ένα τόσο αμφίρροπο πεδίο δεν μπορεί να θεωρείται πανάκεια, καθώς τα κράτη τείνουν διαρκώς να καταπατούν τις ατομικές ελευθερίες των πολιτών.

Ο Μακιαβέλλι έγραφε στον Ηγεμόνα: « *Έναν ηγεμόνα πρέπει να τον φοβούνται και να τον αγαπούν. Αν δεν γίνεται και τα δύο, τότε καλύτερα μόνο να τον φοβούνται*». Η αίσθηση της διαρκούς παρακολούθησης των πολιτών πέραν της αποστέρησης των δικαιωμάτων τους είναι και η καλύτερη επιλογή για ένα καθεστώς, που θέλει να ελέγχει ολοκληρωτικά το λαό και να κατευθύνει τις κοινωνικές συμπεριφορές, αφού οι πολίτες μαθαίνουν να ζουν ανελεύθεροι με το φόβο της κατασκοπείας. Καθίσταται έτσι, ένας σύγχρονος τρόπος χειραγώγησης του λαού, μια νέα μορφή τεχνολογικού ολοκληρωτισμού μια μορφή δημοκρατικής αναπηρίας, που δεν πρέπει να υποτιμάται ή να περιορίζεται σε νομικά τεχνάσματα και πολιτικούς βερμπαλισμούς.

**ΒΙΒΛΙΟΓΡΑΦΙΑ**

**ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ**


1. Αγγελής, Ι. «*Διαδίκτυο και ποινικό δίκαιο*», Ποινικά Χρονικά, 2000
2. Αρκούδα, Ο. Διπλωματική Εργασία «*Απάτη μέσω ηλεκτρονικού υπολογιστή και συναφείς μορφές εγκληματικότητας*», Νομική Σχολή ΑΠΘ, Θεσσαλονίκη 2017
3. Δαγτόγλου, Π. (2012) «*Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα*», 4η έκδ., εκδόσεις Σάκκουλας, Αθήνα
4. Ιγγλεζάκης, Ι «*Δίκαιο Πληροφορικής*», έκδ. Σάκκουλα, 2018
5. Κίτσος, Π. «*Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών. Ενσωμάτωση των ρυθμίσεων της Ευρωπαϊκής Ένωσης στο Ελληνικό δίκαιο.*» ΠΑΜΑΚ, Θεσσαλονίκη 2011
6. Μάνεσης, Α. (1982) «*Συνταγματικά Δικαιώματα, Ατομικές Ελευθερίες*», Αθήνα, εκδ. Σάκκουλας
7. Μαυρίδης Ι. (2015) «*Ασφάλεια Πληροφοριών στο Διαδίκτυο*». Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
8. Μπαλτά, Ι. Πανεπιστήμιο Πειραιά 2021-2022 ΜΔΕ «*Η κυβερνοασφάλεια στη σύγχρονη ψηφιακή εποχή*»
9. Παπαντώνη, Η. ΜΔΕ : «*Καθ' οδόν προς την νιοθέτηση του e-Privacy. Η προς ρύθμιση ύλη και τα διακυβεύματα του νέου κανονιστικού πλαισίου*» Πανεπιστήμιο Πειραιά, Πειραιάς 2022
10. Παρατηρήσεις Ολομέλειας ΑΔΑΕ επί της πρότασης σχεδίου νόμου 18/11/2022 διαθέσιμες στο: http://www.adae.gr/fileadmin/documents/PARATIRISEIS_ADAE_GIA_TO_NOMOSXEDIO_21-11-2022.pdf [Ημερομηνία πρόσβασης: 14/2/2023]
11. Τσόλιας, Γ.(2013) «*Απόρρητο Ηλεκτρονικών Επικοινωνιών ΙΙΙ -Συνταγματικό πλαίσιο προστασίας του απορρήτου στον τομέα των τηλεπικοινωνιών*». Σε Παύλου, Σ., Σάμιο, Θ. επιμ. Ειδικοί Ποινικοί Νόμοι, Αθήνα: Εκδόσεις Π.Ν. Σάκκουλας
12. Φουκώ, Μ. «*Επιτήρηση και τιμωρία. Η γέννηση της φυλακής*», Εκδόσεις Ράππα, Αθήνα 1989

13. Χρυσόγονος, Κ. (2002) «*Ατομικά και κοινωνικά δικαιώματα*», 2η Εκδ. Σάκκουλα, Αθήνα-Κομοτηνή
14. Tanenbaum (2009) «*Σύγχρονα Λειτουργικά Συστήματα» 3η έκδ.* Κλειδάριθμος.

**Ιστοσελίδες**

1. «*Πληροφορίες σχετικά με Spyware (Λογισμικα Κατασκοπειας) και Τρόποι Αφαίρεσης*» Διαθέσιμο στο: https://ioys.gr/spyware-%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%AC-%CE%BA%CE%B1%CF%84%CE%B1%CF%83%CE%BA%CE%BF%CF%80%CE%B5%CE%AF%CE%B1%CF%82/ [Ημερομηνία πρόσβασης: 3/1/2023]
2. https://www.dpa.gr/index.php/el/cookies/plirofories/whatis_cookies [Ημερομηνία πρόσβασης 3/1/2023]
3. https://www.nis.gr/el

**Ελληνικά Νομοθετικά Κείμενα**

1. Ν. 5002/2022 - ΦΕΚ 228/Α/9-12-2022: «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών» Διαθέσιμος στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-5002-2022.html [Ημερομηνία πρόσβασης: 19/1/2023]
2. ΕφτΚ Τεύχος Α’ 152/09.08.2022 ΠΝΠ «*Επείγουσες διατάξεις για την ενίσχυση της ακεραιότητας στη λειτουργία της Εθνικής Υπηρεσίας Πληροφοριών*». Διαθέσιμο στο: https://www.in.gr/wp-content/uploads/2022/08/a4ba248e-4a90-4560-84e1-4c315b023853.pdf [Ημερομηνία πρόσβασης: 4/1/2023]
3. Ποινικός Κώδικας (Νόμος 4619/2019). Διαθέσιμος στο: https://www.lawspot.gr/nomikes-plirofories/nomothesia/poinikos-kodikas-nomos-4619-2019 [Ημερομηνία πρόσβασης: 9/1/2023]
4. Υπουργική Απόφαση 1027/2019 - ΥΕΚ 3739/Β/8-10-2019: «*Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α 199)*». Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/upourgike-apophase-1027-2019-phek-3739b-8-10-2019.html [Ημερομηνία πρόσβασης: 19/1/2023]

5. Ν. 4577/2018 - ΥΕΚ 199/Α/3-12-2018: «*Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις*». Διαθέσιμο στο: https://www.kodiko.gr/nomothesia/document/474449/nomos-4577-2018 [Ημερομηνία πρόσβασης: 19/1/2023]
6. Ν. 4070/2012 ΦΕΚ Α' 82/10.04.2012. Διαθέσιμος στο: https://www.kodiko.gr/nomothesia/document/117878/nomos-4070-2012 [Ημερομηνία πρόσβασης: 19/1/2023]
7. Ν. 3471/2006 - ΦΕΚ 133/Α/28-6-2006. Διαθέσιμος στο: https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/n-3471-2006.html [Ημερομηνία πρόσβασης: 12/1/2023]
8. Αιτιολογική Έκθεση του ά. 4 ν. 3471/2006 ΚΝοΒ

**Αποφάσεις – Γνωμοδοτήσεις**

1. ΑΠΔΠΧ 2/2023 διαθέσιμη στο: https://www.dpa.gr/sites/default/files/2023-01/2_2023%20anonym.pdf [Ημερομηνία πρόσβασης: 14/2/2023]
2. Γνμδ Εισαγγελέα Ντογιάκου, Ι 1/2023 ΑΠ, διαθέσιμη στο: https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-1-2023/ [Ημερομηνία πρόσβασης: 14/2023]
3. ΑΠ 916/2019
4. Απόφαση ΑΔΑΕ 205/2013 - ΥΕΚ 1742/Β/15-7-2013: «*Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*» Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinoniestelephonia/apophase-adae-205-2013.html [Ημερομηνία πρόσβασης: 19/1/2023]
5. Γνμδ Εισαγγελέα ΑΠ Γ. Σανιδάς 9/2009 https://eisap.gr/%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-09-2009/
6. Γνμδ 1/2005 της ΑΔΑΕ: http://www.adae.gr/fileadmin/docs/nomoi/893-2005.pdf

**Ευρωπαϊκά Κείμενα**


1. Κανονισμός (ΕΕ) 2021/821 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 2021 θέσπιση ενωσιακού συστήματος ελέγχου των εξαγωγών, της μεσιτείας, της τεχνικής βοήθειας, της διαμετακόμισης και της μεταφοράς ειδών διπλής χρήσης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021R0821 [Ημερομηνία πρόσβασης: 9/1/2023]

2. Ευρωπαϊκό Ελεγκτικό Συνέδριο (2019) «*Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια.*» Λουξεμβούργο Διαθέσιμο στο: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECU RITY_EL.pdf [Ημερομηνία Πρόσβασης 3/1/2023]
3. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων (2017) Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 10-1-2017 για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της Οδηγίας 2002/58/ΕΚ, 2017/0003
4. Πρόταση Κανονισμού (e-Privacy) COM(2017) 10 final διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017PC0010&from=EN. [Ημερομηνία πρόσβασης: 19/1/2023]
5. ΓΚΠΔ 2015/679 ΕΕ. Διαθέσιμος στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL [Ημερομηνία πρόσβασης: 9/1/2023]
6. Οδ. 2013/40/ΕΕ της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013L0040&from=HU [Ημερομηνία πρόσβασης: 3/1/2023]
7. Χάρτης Θεμελιωδών Δικαιωμάτων Ευρωπαϊκής Ένωσης (2010/C 83/02). Διαθέσιμος στο: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EL:PDF [Ημερομηνία πρόσβασης: 9/1/2023]
8. Οδ. 2002/58/ΕΚ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις

ηλεκτρονικές επικοινωνίες) Διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002L0058&from=EL [Ημερομηνία πρόσβασης: 12/1/2023]

9. Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο της 23/11/2001. Διαθέσιμη στο: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0 [Ημερομηνία πρόσβασης: 9/1/2023]
10. Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα. Διαθέσιμο στο: https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=4bd686e52 [Ημερομηνία πρόσβασης: 3/1/2023]
11. Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου. Διαθέσιμη στο: https://www.echr.coe.int/documents/convention_ell.pdf [Ημερομηνία πρόσβασης: 3/1/2023]

**Αρθρογραφία**

1. Benjakob, O. Inside story (2022). «*Η Intellexa παρακάμπτει τους ισραηλινούς κανόνες μέσω Αθήνας*». Διαθέσιμο στο: https://insidestory.gr/article/prosohi-den-dimosieyetaiwifi-aerodromion-kai-hakarisma-kiniton-tilefonon-i-skoteini-pleyra [Ημερομηνία πρόσβασης: 4/1/2023]
2. Lawspot (2022) «*Στη Βουλή το νομοσχέδιο για τη διαδικασία άρσης απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*» Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/sti-voyli-nomoshedio-gia-ti-diadikasia-arsis-aporritoy-ton-epikoinonion-kyvernoasfaleia [Ημερομηνία πρόσβασης: 19/1/2023]
3. Law&Tech (2020) «*Το Νομικό Πλαίσιο για την Ασφάλεια των Δικτύων / Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*» Διαθέσιμο στο: https://lawandtech.eu/2020/04/27/%CF%80%CE%BF%CE%B9%CE%BF-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CF%80%CE%BB%CE%B1%CE%AF%CF%83%CE%B9%CE%BF-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7%CE%BD-%CE%B1%CF%83/ [Ημερομηνία πρόσβασης: 19/1/2023]

4. Η Καθημερινή (2022) «*Παρακολουθήσεις: Σε διαβούλευση το σχέδιο νόμου – Τι προβλέπει*» Διαθέσιμο στο: https://www.kathimerini.gr/politics/562138606/parakoloythiseis-se-diavoyleysi-to-schedio-nomoy-ti-provlepei/ [Ημερομηνία πρόσβασης: 19/1/2023]
5. Η Καθημερινή (2019): «*Η αρμοδιότητα της ΕΥΠ περνάει στον πρωθυπουργό*». Διαθέσιμο στο: https://www.kathimerini.gr/politics/1033159/i-armodiotita-tis-eyp-pernaei-ston-prothypoyrgo/ [Ημερομηνία πρόσβασης: 3/1/2023]
6. Καρκατζούνης, Β. «*Google Analytics και προστασία προσωπικών δεδομένων Το ψήφισμα της Συνόδου των Εποπτικών αρχών προστασίας προσωπικών δεδομένων της Γερμανίας (Datenschutzkonferenz της 12.5.2020)*», Επιθεώρηση Δικαίου Πληροφορικής, Τ. 1, 2020. Διαθέσιμο στο: http://ejournals.lib.auth.gr/infolawj/ [Ημερομηνία πρόσβασης 3/1/2023]
7. Καρκατζούνης, Β. «*Cookies και προστασία δεδομένων προσωπικού χαρακτήρα*», ΔΙΤΕ, 2/2019
8. Μακρής Σπύρος «*Το Predator και τα προσωπικά δεδομένα. Οι πολλαπλές παραβιάσεις της εθνικής και ευρωπαϊκής νομοθεσίας και τα πρακτικά και νομικά προβλήματα για την εφαρμογή της*». Διαθέσιμο στο: https://www.constitutionalism.gr/to-predator-kai-ta-prosopika-dedomena/#_ftn22 [Ημερομηνία πρόσβασης: 22/7/2023]
9. 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/#_ftn1 [Ημερομηνία πρόσβασης: 9/1/2023]
10. Παπανικολάου, Α. (2022) «*Άρση του επικοινωνιακού απορρήτου και υποχρέωση γνωστοποίησης: ένα δικαιοκρατικό ζήτημα σε εκκρεμότητα*», Επιθεώρηση Δημόσιας Διοίκησης. Διαθέσιμο στο: https://www.lawjournals.unic.ac.cy/index.php/pareview/article/view/35/24 [Ημερομηνία πρόσβασης: 19/1/2023]
11. Παπανικολάου, Α. (2020) «*Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*». Διαθέσιμο σε: https://www.constitutionalism.gr/wp-content/uploads/2020/07/2020-07-papanikolaou-katerina-aporrito-epikoinonias.pdf [Ημερομηνία πρόσβασης: 19/1/2023]
12. Πιπύρος, Κ., Μήτρου, Λ. «*Κυβερνοεπίθεση ή Κυβερνοπόλεμος;*» ΔιΜΕΕ τ. 2/2018 Έτος 15ο

13. Ράμμος, Χ., Γκρίτζαλης, Σ., Παπανικολάου, Α., (2021) *«Αντίθεση του άρθρου 87 Ν. 4790/2021 προς τις εγγυήσεις της ΕΣΔΑ για διαφύλαξη του απορρήτου των επικοινωνιών»*. Διαθέσιμο στο: https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/ [Ημερομηνία πρόσβασης: 12/1/2023]
14. Τέλλογλου, Τ., Τριανταφύλλου, Ε. Inside story (2022*): «Predator: Ο «κατάσκοπος» που ήρθε από την Κύπρο».* Διαθέσιμο στο: https://insidestory.gr/article/i-kypros-kai-o-tal-dilian [Ημερομηνία πρόσβασης: 4/1/2023].
15. Τριανταφύλλου, Ε. Inside story (2022). *«Το νέο λογισμικό κατασκοπίας Predator και οι δουλειές στην Ελλάδα».* Διαθέσιμο στο: https://insidestory.gr/article/neo-logismiko-kataskopeias-predator-kai-oi-doyleies-stin-ellada [Ημερομηνία πρόσβασης: 4/1/2023]
16. Τριανταφύλλου, Ε., Τέλλογλου, Τ. Inside story (2022). *«Predatorgate: Ο δεύτερος μέτοχος της Intellexa AE».* Διαθέσιμο στο: https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae [Ημερομηνία πρόσβασης: 4/1/2023]
17. Τσόλιας, Γ. (2004) *«Τα τηλεπικοινωνιακά δεδομένα υπό το πρίσμα του απορρήτου: προβληματισμοί εν όψει της ενσωμάτωσης της Οδηγίας 2002/58/ΕΚ»*. ΔΙΤΕ (π. ΔΙΜΕΕ), (Τεύχος 3/2004)
18. Χοντζόπουλος, Ι., Κακαβούλης Κ. Homo Digitalis (2018): *«Τι είναι τα cookies;»*. Διαθέσιμο στο: https://www.homodigitalis.gr/posts/3079 [Ημερομηνία πρόσβασης: 3/1/2023]

**ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ**

1. Agrawal, M. & Varshney, G. & Kakandwar, S. & Pratap S., Kaushal & Verma, M. (2022). *"Pegasus: Zero-Click spyware attack -its countermeasures and challenges."* Διαθέσιμο στο https://www.researchgate.net/publication/357956844_Pegasus_Zero-Click_spyware_attack_-its_countermeasures_and_challenges [Ημερομηνία πρόσβασης: 4/1/2023]
2. Chawla, A. (2021) *"Pegasus Spyware: A Privacy Killer"*. Διαθέσιμο στο SSRN: https://ssrn.com/abstract=3890657 [Ημερομηνία πρόσβασης: 4/1/2023]
3. Mitrou, L. (2007) *"Communications Data Retention: A Pandora's Box for Rights and Liberties?"*. Σε Acquisti, A., Gritzalis, S., Lambrinoudakis, C., Di Vimercati, S. Digital Privacy, Theory, Technologies and Practices. New York: Auerbach Publications. Διαθέσιμο στο: https://www.academia.edu/8379843/Communications_Data_Retention_A_Pandoras_Box_for _Rights_and_Liberties [Ημερομηνία πρόσβασης: 17/1/2023]

4. Foti D. σε Bachmaier, L.; Ruggeri W. S. (2022) *"Investigating and Preventing Crime in the Digital Era"*. Διαθέσιμο στο: https://doi.org/10.1007/978-3-031-13952-9 [Ημερομηνία πρόσβασης: 3/1/2023]
5. Staff Report Federal Trade Commission, March 2005 *"Monitoring Software on Your PC: Spyware, Adware, and Other Software"*

**Αρθρογραφία**

1. Bernal, P. (2016) *"Data gathering, surveillance and human rights: recasting the debate"*. Journal of Cyber Policy, 1(2).
2. CNet News (2011) «*Τα κουμπιά "Μου αρέσει", "tweet" αποκαλύπτουν τους ιστότοπους που επισκέπτεστε*». Διαθέσιμο στο: https://www.cnet.com/videos/like-tweet-buttons-divulge-sites-you-visit/ [Ημερομηνία πρόσβασης: 3/1/2023]
3. Cupa, B. *"Trojan Horse Resurrected: On the Legality of the Use of Government Spyware"*, LISS 2013. Διαθέσιμο στο: https://www.zora.uzh.ch/id/eprint/81157/1/Cupa_Living_in_Surveillance_Societies_2012.pdf [Ημερομηνία πρόσβασης: 3/1/2023]
4. Deutche Welle, (2021) *"Is Germany's spyware law a threat to press freedom?"*. Διαθέσιμο στο: https://www.dw.com/en/is-germanys-spyware-law-a-threat-to-press-freedom/a-59656164?utm_source=headtopics&utm_medium=news&utm_campaign=2021-10-29 [Ημερομηνία πρόσβασης: 4/1/2023]
5. Felten, E. (2013) "*Written Testimony"*, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act. United States Senate
6. Hostovsky Brandes, T. Verfassungsblog (2022): *"When your own spyware hits home – Israel's domestic NSO Scandal"*. Διαθέσιμο στο: https://verfassungsblog.de/when-your-own-spyware-hits-home/ [Ημερομηνία πρόσβασης: 17/1/2023]
7. Ingleton D. The Guardian (2022) Amnesty International: *"The Pegasus Project: One year on, spyware crisis continues after failure to clamp down on surveillance industry"*. Διαθέσιμο στο: https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/ [Ημερομηνία πρόσβασης: 9/1/2023]

8. Lindsey N. CPO Magazine (2019), *"Swedish police given green light for spyware".*Διαθέσιμο στο: https://www.cpomagazine.com/cyber-security/swedish-police-given-green-light-for-spyware/ [Ημερομηνία πρόσβασης: 4/1/2023]
9. Reimer, J. Ars Technica (2007) *" The tricky issue of spyware with a badge: meet policeware "*. Διαθέσιμο στο: https://arstechnica.com/information-technology/2007/07/will-security-firms-avoid-detecting-government-spyware/ [Ημερομηνία πρόσβασης: 3/1/2023]
10. Stanglin D. Ondeadline (2010) *"School district accused of spying on kids via laptop webcams"*. Διαθέσιμο στο: https://web.archive.org/web/20120913050816/http://content.usatoday.com/communities/ondeadline/post/2010/02/school-district-accused-of-issuing-webcam-laptops-to-spy-on-students/1 [Ημερομηνία πρόσβασης: 3/1/2023]
11. University of Essex (2013) "*Spyware*". Διαθέσιμο στο: https://web.archive.org/web/20131101154446/https:/www.justice.gov.tr/e-journal/pdf/cybercrime_essay.pdf [Ημερομηνία πρόσβασης: 3/1/2023]
12. Watt E. Verfassungsblog, (2022) "*The legacy of the privacy versus security narrative in the ECtHR's jurisprudence"*. Διαθέσιμο στο: https://verfassungsblog.de/os6-privacy-vs-security/ [Ημερομηνία πρόσβασης: 17/1/2023]

**Ιστοσελίδες**

1. America Online & The National Cyber Security Alliance (2005) *"AOL/NCSA Online Safety Study"*.Διαθέσιμο στο: https://web.archive.org/web/20051213090601/http://www.staysafeonline.info/pdf/safety_study_2005.pdf [Ημερομηνία πρόσβασης: 3/1/2023]
2. Ars Technica C. Ecker (2005) *"Massive spyware-based identity theft ring uncovered"*. Διαθέσιμο στο: https://arstechnica.com/uncategorized/2005/08/5175/ [Ημερομηνία πρόσβασης: 3/1/2023]
3. Edelman, B. (2005) *"Direct Revenue Deletes Competitors from Users' Disks"* Διαθέσιμο στο: https://www.benedelman.org/news-120704/7 [Ημερομηνία πρόσβασης: 3/1/2023]
4. Forbidden Stories *"About the Pegasus Project"*. Διαθέσιμο στο: https://forbiddenstories.org/about-the-pegasus-project/ [Ημερομηνία πρόσβασης: 4/1/2023]

5. Hawkins, D. US News & World Report (2000) *"Privacy Worries Arise Over Spyware in Kids' Software"*. Διαθέσιμο στο: https://web.archive.org/web/20131103060440/http://www.usnews.com/usnews/culture/articles/000703/archive_015408.htm [Ημερομηνία πρόσβασης: 3/1/2023]
6. Sharon, W. CNET (2004) *"The spyware inferno"* Διαθέσιμο στο: https://www.cnet.com/tech/services-and-software/the-spyware-inferno/ [Ημερομηνία πρόσβασης: 3/1/2023]
7. Stouffer, C. Norton (2021): *"Spyware: What is spyware + how to protect yourself"* Διαθέσιμο στο: https://us.norton.com/blog/malware/spyware [Ημερομηνία πρόσβασης: 3/1/2023]
8. Tunggal, A. T. UpGuard (2021) *'What is a Cyber Threat'*? Διαθέσιμο στο:

   https://www.upguard.com/blog/cyber-threat Πρόσβαση στις 10-12-2021 [Ημερομηνία πρόσβασης: 3/1/2023]
9. περιγραφή προϊόντος Pegasus: https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf.

**Ευρωπαϊκά Κείμενα**

1. ENISA Threat Landscape October 2022. Διαθέσιμο στο: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Ημερομηνία πρόσβασης: 19/1/2023]
2. ECHR Factsheet September 2022 *"Mass surveillance"*. Διαθέσιμο στο: https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf [Ημερομηνία πρόσβασης: 17/1/2023]
3. Kaldani T.; Prokopets Z. Information Society Department DGI(2022)04, Council of Europe *"PEGASUS SPYWARE and its impacts on human rights"*. Διαθέσιμο στο: https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8 [Ημερομηνία πρόσβασης: 3/1/2023]
4. EPRS (2022) *"Europe's PegasusGate – Countering spyware abuse"*. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf [Ημερομηνία πρόσβασης: 4/1/2023]
5. EDPS (2022) "*Preliminary Remarks on Modern Spyware"*. Διαθέσιμο στο: https://edps.europa.eu/system/files/2022-02/22-02-

15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf [Ημερομηνία πρόσβασης: 9/1/2023]

6. European Parliament (2022) *"Pegasus and surveillance spyware"* – In-Depth analysis for the Pegasus Committee, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf [Ημερομηνία πρόσβασης: 4/1/2023]
7. ENISA Threat Landscape January 2019- April 2020 *"Cyber espionage"*. Διαθέσιμο στο: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-cyberespionage [Ημερομηνία πρόσβασης: 19/1/2023]
8. Council of Europe / European Court of Human Rights, *"National Security and European Case-Law"*, 2013. Διαθέσιμο στο: https://rm.coe.int/168067d214 [Ημερομηνία πρόσβασης: 3/1/2023]
9. "*Body of European Regulator for Electronic Communications (BEREC) Report on OTT Services".* Διαθέσιμο στο: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services [Ημερομηνία πρόσβασης: 19/1/2023]
10. Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies January 2023 "*The impact of Pegasus on fundamental rights and democratic processes"*. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf [Ημερομηνία πρόσβασης: 14/2/2023]
11. Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, December 2022 *"The use of Pegasus and equivalent surveillance spyware"*. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf [Ημερομηνία πρόσβασης: 3/1/2023 ]
12. Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, May 2022 *"Pegasus and surveillance spyware"*. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf [Ημερομηνία πρόσβασης: 3/1/2023]

**Νομοθεσία**

Οικουμενική διακήρυξη του ΟΗΕ. Διαθέσιμη στο: https://unric.org/el/%CE%BF%CE%B9%CE%BA%CE%BF%CF%85%CE%BC%CE%B5%CE%BD%CE%B9%CE%BA%CE%B7-%CE%B4%CE%B9%CE%B1%CE%BA%CE%B7%CF%81%CF%85%CE%BE%CE%B7-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B1-%CE%B1%CE%BD%CE%B8%CF%81%CF%89%CF%80%CE%B9-2/ [Ημερομηνία πρόσβασης: 9/1/2023]

**Αποφάσεις**

1. ΕΔΔΑ, *Seks v. Croatia* 3 February 2022
2. ΕΔΔΑ, *Ekimdzhiev and others v. Bulgaria* 11 January 2022
3. ΕΔΔΑ *Big Brother Watch and others v. The United Kingdom*, 25 May 2021
4. ΕΔΔΑ *Centrum för Rättvisa v. Sweden*, 19 June 2018
5. ΕΔΔΑ *Szabó and Vissy v. Hungary* 12 January 2016
6. ΕΔΔΑ *Dragojević v. Croatia*, 15 January 2015
7. ΕΔΔΑ *Roman Zakharov v. Russia* 4 December 2015
8. ΕΔΔΑ, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands* 22 November 2012
9. ΕΔΔΑ *Michaud v. France* 6 Décembre 2012
10. ΕΔΔΑ, *Dumitru Popescu v. Romania* 26 April 2007
11. Federal Constitutional Court, BvR 370/07 και BvR 595/07, Διαθέσιμες στο: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html [Ημερομηνία πρόσβασης: 4/1/2023]
12. ΕΔΔΑ *Fazil Ahmet c. Turquie* 5 Décembre 2006
13. ΕΔΔΑ *Weber and Saravia v. Germany* 29 June 2006
14. ΕΔΔΑ *Amann v. Switzerland* 16 February 2000
15. ΕΔΔΑ *Valenzuela Contreras v. Spain*, 30 July 1998
16. ΕΔΔΑ *Kopp v. Switzerland* 25 March 1998
17. ΕΔΔΑ *Huvig v. France*, 24 April 1990
18. ΕΔΔΑ *Kruslin v. France*, 24 April 1990

19. ΕΔΔΑ *Klass and others v. Germany*, 6 September 1978