ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Κωνσταντίνας Κατσούρη (Α.Μ.: ΜΔΙ 2323)

ΤΑ ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ ΥΠΟ ΤΗΝ ΟΠΤΙΚΗ ΤΟΥ ΑΡΘΡΟΥ 19 ΤΟΥ ΣΥΝΤΑΓΜΑΤΟΣ ΚΑΙ ΤΟΥ Ν. 5002/2022

SPYWARE UNDER THE VIEWPOINT OF Art. 19 OF THE CONSTITUTION AND Law 5002/2022

Επιβλέπουσα:

Καθηγήτρια: Δρ. Αικατερίνα Παπανικολάου

Πειραιάς, Σεπτέμβριος 2025

Στους γονείς μου, Γιώργο και Ζωή, και τον αδελφό μου, Αδριανό, για την αμέριστη στήριξή τους.

«Πρέπει να επιδιώκουμε την ελευθερία και όχι μόνο την ασφάλεια, αν όχι για κάποιον άλλο λόγο, επειδή μόνο η ελευθερία μπορεί να καταστήσει την ασφάλεια ασφαλή.»

Karl Popper, 1902 - 1994

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΔΑΕ: Αρχή Διασφάλισης Απορρήτου Επικοινωνιών

Αιτ. Σκέψη: Αιτιολογική Σκέψη

ΑΠ: Άρειος Πάγος

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Βλ.: Βλέπε

Γ.Γ.: Γενικός Γραμματέας

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

Γνωμ: Γνωμοδότηση

ΔΑΕΕΒ: Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας

ΔΕΕ: Δικαστήριο της Ευρωπαϊκής Ένωσης

ΔΣΑΠΔ: Διεθνές Σύμφωνο για Ατομικά και Πολιτικά Δικαιώματα

ΕΑΔ: Εθνική Αρχή Διαφάνειας

ΕΔΔΑ: Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου

ΕΕ: Ευρωπαϊκή Ένωση

ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

ΕισΑΠ: Εισαγγελία Αρείου Πάγου

Επ.: επόμενα

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση Δικαιωμάτων Ανθρώπου

ΕΣΡ: Εθνικό Συμβούλιο Ραδιοτηλεόρασης

ΕΥΠ: Εθνική Υπηρεσία Πληροφοριών

Κλπ.: και λοιπά

Λ.χ.: Λόγου Χάρη

ΜΜΕ: Μέσα Μαζικής Ενημέρωσης

ΜΠλ: Μονομελές Πλημμελειοδικείο

Ν.: Νόμος

Ο.π.: Όπως παραπάνω

ΟλΑΠ: Ολομέλεια Αρείου Πάγου

ΟλΣτΕ: Ολομέλεια Συμβουλίου της Επικρατείας

Π.Δ.: Προεδρικό Διάταγμα

Π.Κ.: Ποινικός Κώδικας

Παρ.: Παράγραφος

Σ.: Σύνταγμα

Σελ.: Σελίδα

ΣτΕ: Συμβούλιο της Επικρατείας

ΣυμβΠλημ: Συμβούλιο Πλημμελειοδικών

ΤΝΠ: Τράπεζα Νομικών Πληροφοριών

Τομ.: Τόμος

ΦΕΚ: Φύλλο Εφημερίδας Κυβερνήσεως

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία φιλοδοξεί να παρουσιάσει μια συνεκτική μελέτη των λογισμικών κατασκοπείας στην σύγχρονη ψηφιακή εποχή και ειδικότερα, την έννοια αυτών, τα είδη και τις εφαρμογές τους, τους κινδύνους, που "εγκυμονεί" η αυθαίρετη χρήση τους, για τα θεμελιώδη δικαιώματα, καθώς και το συνταγματικό και εν γένει νομοθετικό πλαίσιο προστασίας των ατόμων, από την παράνομη εφαρμογή τους, ιδίως υπό το πρίσμα του άρθρου 19 του Συντάγματος και των διατάξεων του Ν. 5002/2022. Παρατίθενται, ακόμη, οι τάσεις της νομολογίας του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου, οι οποίες, μη υπάρχοντος εισέτι αποκρυσταλλωμένου κανονιστικού πλαισίου, αποτελούν ασφαλή πυξίδα για την οριοθέτηση του εύρους της νόμιμης χρήσης τους, δοθέντος ότι η ραγδαίως εξελισσόμενη τεχνολογική πρόοδος γεννά διαρκώς νέες προκλήσεις για τα ανθρώπινα δικαιώματα, ενώ στην συνέχεια ακολουθεί εκτενής αναφορά σε περιπτώσεις εφαρμογής των κατασκοπευτικών λογισμικών, που η αποκάλυψή τους απασχόλησε ευρέως την κοινή γνώμη, ενόψει της εμπλοκής σε αυτές κρατικών αρχών. Η μελέτη ολοκληρώνεται με την αποτίμηση των προπαρατεθέντων και ιδίως, του βαθμού ικανοποιητικής και αποτελεσματικής νομοθετικής προστασίας, έναντι της αυθαίρετης και καταχρηστικής εφαρμογής λογισμικών κατασκοπείας. Ας σημειωθεί ότι, η παρούσα διπλωματική εργασία, αποτελεί προϊόν μελέτης και έρευνας των βιβλιογραφικών και ιστορικών πηγών της έως τον Αύγουστο του έτους 2025.

ABSTRACT

This paper aspires to present a coherent study of spyware in the modern digital era and, in particular, their concept, their types and applications, the risks that their arbitrary use poses for fundamental rights, as well as the constitutional and general legislative framework for the protection of individuals from their illegal application, especially in the light of article 19 of the Constitution and the provisions of Law 5002/2022. The trends of the case law of the European Court of Human Rights are also cited, which, in the absence of a crystallized regulatory framework, constitute a safe compass for defining the scope of their lawful use, given that the rapidly evolving technological progress is constantly generating new challenges for human rights, while an extensive reference to cases of application of spyware follows, the disclosure of which has widely concerned public opinion, in view of the involvement of state authorities in them. The study concludes with the assessment of the aforementioned and in particular, the degree of satisfactory and effective legislative protection against the arbitrary and abusive application of spyware. It should be noted that this paper is the product of a study and research of its bibliographical and historical sources up to August 2025.

ΕΙΣΑΓΩΓΗ

Οι τεχνολογικές καινοτομίες, που με αλματώδεις ρυθμούς διαδέχονται η μία την άλλη, δεν συνέβαλαν μόνο στην πρόοδο των κοινωνιών, αλλά παράλληλα γέννησαν πληθώρα προκλήσεων για την ανθρωπότητα.

Στο πλαίσιο αυτό, τα σύγχρονα τεχνολογικά μέσα, αποτελούν συχνά χρήσιμο εργαλείο για την τέλεση εγκληματικών πράξεων, καθιστώντας πιο επιτακτική από ποτέ την ανάγκη διαφύλαξης της ασφάλειας των ανθρώπων, των κρατών, καθώς και των δημοκρατικών θεσμών. Προς την κατεύθυνση αυτή, οι Αρχές επιβολής του νόμου λαμβάνουν ολοένα και περισσότερα μέτρα, για την πρόληψη και καταστολή, ιδίως του οργανωμένου εγκλήματος.

Στην προσπάθεια τούτη, τα συστήματα επιτήρησης αποτελούν σημαντικό όπλο για την αντιμετώπιση εγκληματικών συμπεριφορών και ένα νέο πρότυπο αστυνόμευσης, η λεγόμενη αστυνόμευση με γνώμονα τις πληροφορίες[1], άρχισε να κερδίζει έδαφος. Η επιτήρηση αυτή επιτρέπει στις Αρχές επιβολής του νόμου, να χρησιμοποιούν πιο επεμβατικές και εξελιγμένες τεχνολογικά υπηρεσίες, μέσω των οποίων είναι δυνατή η απόκτηση δεδομένων, ενίοτε σε μαζική κλίμακα.

Ωστόσο, η πρόσφατη ιστορία, απέδειξε ότι τέτοια συστήματα επιτήρησης, μπορούν να αποτελέσουν σημαντική απειλή για τα θεμελιώδη δικαιώματα, αλλά και τους δημοκρατικούς θεσμούς. Με το πρόσχημα της «νόμιμης ψηφιακής επιτήρησης», άλλοτε για λόγους εθνικής ασφάλειας, άλλοτε για την διακρίβωση σοβαρών ποινικών αδικημάτων, πολιτικοί, κρατικοί αξιωματούχοι, επιφανή πρόσωπα, αλλά και απλοί πολίτες, γίνονται στόχος παράνομης και αυθαίρετης παρακολούθησης, με συνέπεια όχι μόνο την καταστρατήγηση των θεμελιωδών δικαιωμάτων τους, αλλά και την ευθεία διατάραξη του κράτους δικαίου.

Οι αποκαλύψεις του Αμερικανού Edward Snowden, πρώην εργαζομένου της Εθνικής Υπηρεσίας Ασφάλειας των Η.Π.Α. και της CIA, περί χρήσης προγραμμάτων μαζικής παρακολούθησης εκ μέρους της Αμερικανικής και της Βρετανικής Κυβέρνησης, με την συνεργασία κορυφαίων εταιρειών τηλεπικοινωνιών, με στόχο την υποκλοπή και αποθήκευση

[1] Vogiatzoglou P. (2019), «*Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity*». European Journal of Law and Technology, Vol 10, Issue 1, 2019. [Ημ. Πρόσβασης 18.8.2025]

του συνόλου της επικοινωνίας, εκατομμυρίων ανθρώπων, έφεραν στο φως ένα αόρατο, αλλά εξαιρετικά επικίνδυνο και αδίστακτο σύστημα παρακολούθησης, ικανό να «επιτηρεί» και να επεμβαίνει με τρόπο μυστικό και συνάμα βίαιο στην ιδιωτική ζωή ολόκληρης της ανθρωπότητας.

Οι συνέπειες της αλόγιστης και αυθαίρετης χρήσης λογισμικών κατασκοπείας αποδεικνύονται ολέθριες, δοθέντος ότι οι θιγόμενοι λαμβάνουν γνώση της επιτήρησης των επικοινωνιών τους σπανίως (ενδεχομένως και ποτέ). Η ισχυρή, μάλιστα, διεισδυτική τους ικανότητα να συλλέγουν τεράστιο όγκο δεδομένων, καθιστά την εφαρμογή τους, πλέον επικίνδυνη.

1. ΤΑ ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ

1.1 Έννοια, είδη και τρόπος δράσης κατασκοπευτικών λογισμικών

Σύμφωνα με έναν κοινώς αποδεκτό ορισμό, με τον όρο λογισμικό κατασκοπείας (spyware), νοείται μια κατηγορία κακόβουλου λογισμικού (malware), που έχει σχεδιαστεί για να έχει πρόσβαση και να βλάπτει μια συσκευή, χωρίς τη συγκατάθεση του χρήστη[2].Τα κατασκοπευτικά λογισμικά (spyware) αποτελούν είδος κακόβουλου λογισμικού, που συλλέγουν πληροφορίες από ένα υπολογιστικό σύστημα χωρίς την συγκατάθεση του χρήστη[3]. Στην πράξη, το λογισμικό κατασκοπείας εισέρχεται κρυφά στην ηλεκτρονική συσκευή ενός χρήστη, συλλέγει δεδομένα από αυτήν και τον χρήστη και τα στέλνει σε τρίτα μέρη, χωρίς τη συγκατάθεση ή εν αγνοία του, με τρόπο βλαπτικό προς αυτόν, την ιδιωτικότητά του, την ασφάλεια, την ακεραιότητα ή την εμπιστευτικότητα του δικτύου.

Τα λογισμικά κατασκοπείας συλλέγουν προσωπικές και ευαίσθητες πληροφορίες, τις οποίες στέλνουν σε διαφημιστές, εταιρείες συλλογής δεδομένων ή κακόβουλους παράγοντες, με σκοπό το κέρδος. Μπορούν να παρακολουθούν τις διαδικτυακές δραστηριότητες των χρηστών, να υποκλέπτουν προσωπικά στοιχεία ή να εμφανίζουν ανεπιθύμητες διαφημίσεις. Δύνανται να εξαπλωθούν μέσω μολυσμένων αρχείων ή email ή μπορεί να συνδυαστούν με άλλο λογισμικό και να εγκατασταθούν, χωρίς να το γνωρίζει ο χρήστης. Μπορούν, επίσης, να κατεβάσουν άλλα κακόβουλα προγράμματα από το Διαδίκτυο και να τα εγκαταστήσουν στη συσκευή του χρήστη[4].

Τα spyware είναι μια από τις πιο συχνά χρησιμοποιούμενες μεθόδους κυβερνοεπιθέσεων, με αυξημένη δυσκολία εντοπισμού και δυνατότητα πρόκλησης σοβαρής βλάβης στα δίκτυα επικοινωνιών. Επίσης, καθιστούν τις επιχειρήσεις ευάλωτες σε παραβιάσεις

---

[2] *What is spyware*, Fortinet. Διαθέσιμο σε: https://www.fortinet.com/resources/cyberglossary/spyware. [Ημ. Πρόσβασης 11.8.2025]

[3] *Spyware*, CISA. Διαθέσιμο σε: https://www.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf. [Ημ. Πρόσβασης 11.8.2025]

[4] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 - January 2023, «*The impact of Pegasus on fundamental rights and democratic processes*», σελ. 13. Διαθέσιμο σε: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf. [Ημ. Πρόσβασης 13.6.2025]

δεδομένων, επηρεάζουν συχνά την απόδοση των συσκευών και του δικτύου και διαταράσσουν τη δραστηριότητα των χρηστών[5].

Το αξιοπρόσεκτο είναι ότι σε ορισμένες περιπτώσεις, λογισμικά κατασκοπείας («policeware») χρησιμοποιούνται από κρατικές αρχές (λ.χ. την αστυνομία), με σκοπό την διευκόλυνση των ερευνών τους, για την εξιχνίαση εγκλημάτων[6], με αμφιλεγόμενες, ωστόσο, επιπτώσεις στα ανθρώπινα δικαιώματα.

Ο όρος "spyware" εμφανίστηκε για πρώτη φορά σε διαδικτυακές συζητήσεις τη δεκαετία του 1990, αλλά μόλις στις αρχές της δεκαετίας του 2000, οι εταιρείες κυβερνοασφάλειας τον χρησιμοποίησαν για να περιγράψουν ανεπιθύμητο λογισμικό, που κατασκόπευε τη δραστηριότητα των χρηστών και των υπολογιστών τους. Το πρώτο λογισμικό προστασίας από spyware κυκλοφόρησε τον Ιούνιο του 2000 και τέσσερα (4) χρόνια αργότερα, οι σαρώσεις έδειξαν ότι τα συστήματά περίπου του 80% των χρηστών του διαδικτύου είχαν επηρεαστεί από λογισμικό κατασκοπείας, σύμφωνα με έρευνα της America Online και της National Cyber Security Alliance. Ωστόσο, το 89% εξ αυτών των χρηστών δεν γνώριζαν την ύπαρξη spyware και το 95% δεν είχε δώσει άδεια για την εγκατάστασή του[7].

Οι συνηθέστεροι τρόποι μόλυνσης ενός υπολογιστικού συστήματος είναι:

α) με ηλεκτρονικό "ψάρεμα" (phishing): πρόκειται για μια μορφή παραβίασης της ασφάλειας, κατά την οποία το spyware εισέρχεται στο σύστημα, όταν ο χρήστης κλικάρει έναν ύποπτο σύνδεσμο ή ένα άγνωστο επικίνδυνο συνημμένο αρχείο,

β) με πλαστογράφηση ταυτότητας: συνδυάζεται με το phishing και κάνει τα μη εξουσιοδοτημένα email να φαίνονται ότι προέρχονται από νόμιμους χρήστες ή εταιρικές ηλεκτρονικές διευθύνσεις,

γ) με ελεύθερο λογισμικό ή κοινόχρηστο λογισμικό: εισέρχεται στο σύστημα, όταν ένας χρήστης εγκαθιστά λογισμικό που είναι δωρεάν, αλλά στο οποίο έχει προστεθεί επιπλέον λογισμικό κατασκοπείας,

---

[5] *What is spyware*, ο.π.

[6] Reimer J. (2007), «*The tricky issue of spyware with a badge: meet 'policeware'*» Διαθέσιμο σε: https://arstechnica.com/information-technology/2007/07/will-security-firms-avoid-detecting-government-spyware/. [Ημ. Πρόσβασης 11.8.2025]

[7] Ibidem.

δ) με παραπλανητικό λογισμικό: αυτό διαφημίζεται ως ωφέλιμο για το σύστημα, υποσχόμενο μια αξία που δεν υφίσταται (λ.χ. προγράμματα οδήγησης συσκευών (drivers), λογισμικό βελτίωσης της απόδοσης του συστήματος, λογισμικό προστασίας από ιούς), αλλά στην πραγματικότητα οδηγεί στην κλοπή εμπιστευτικών πληροφοριών από το σύστημα[8].

Καθώς η καταγραφή όλων των τύπων spyware είναι εξαιρετικά δυσχερής, ακριβώς λόγω της ποικιλομορφίας τους, καθώς και της δυσκολίας ανίχνευσής τους, στην παρούσα εργασία θα γίνει αναφορά στους πιο κοινούς τύπους[9] λογισμικών κατασκοπείας:

α) Adware: παρακολουθεί το ιστορικό του προγράμματος περιήγησης του χρήστη και τις λήψεις του, ώστε να προβλέψει, ποια προϊόντα ή υπηρεσίες τον ενδιαφέρουν. Αυτά τα δεδομένα μπορούν να πωληθούν σε διαφημιστές ή να χρησιμοποιηθούν απευθείας, για την προβολή στοχευμένων διαφημίσεων, συχνά με τη μορφή ενοχλητικών αναδυόμενων παραθύρων (pop up) ή banner.

β) Trojan: τύπος κακόβουλου λογισμικού, που «μεταμφιέζεται» σε νόμιμο λογισμικό. Όπως ο Δούρειος Ίππος στην Ελληνική Μυθολογία, τα Trojan αποκτούν πρόσβαση σε συσκευές, με τη μορφή καλοηθών ενημερώσεων ή αρχείων, έχοντας τη δυνατότητα να διαταράξουν το σύστημα, να υποκλέψουν δεδομένα ή να παράσχουν σε έναν hacker απομακρυσμένη πρόσβαση σε αυτό.

γ) System monitors: έχουν σχεδιαστεί, για να καταγράφουν την δραστηριότητα του χρήστη, συλλέγοντας πληροφορίες, λ.χ. για την ηλ. αλληλογραφία του χρήστη, το προφίλ του στα μέσα κοινωνικής δικτύωσης και την περιήγηση σε ιστοσελίδες. Μορφή τέτοιου spyware, αποτελούν τα λεγόμενα keyloggers, τα οποία παρακολουθούν και καταγράφουν οτιδήποτε πληκτρολογεί ο χρήστης στην συσκευή.

δ) Rootkits: επιτρέπουν στους εισβολείς να διεισδύσουν σε βάθος στις συσκευές εκμεταλλευόμενοι τρωτά σημεία ασφαλείας ή συνδεόμενοι σε μηχανήματα ως διαχειριστές. Τα rootkits είναι συχνά δύσκολο ή ακόμη και αδύνατο να εντοπιστούν. Παρόλο που μπορεί να μην προκαλούν προφανή ζημιά στο σύστημα, τα rootkits παρέχουν στους κυβερνοεγκληματίες τη

---

[8] *«Τι είναι το Spyware στην Κυβερνοασφάλεια;»* Διαθέσιμο σε: https://www.geeksforgeeks.org/ethical-hacking/what-is-spyware-in-cyber-security/. [Ημ. Πρόσβασης 11.8.2025]

[9] Birchall M. (2025), *"What is spyware? How to detect it and protect yourself"*, Norton. Διαθέσιμο σε: https://us.norton.com/blog/malware/spyware. [Ημ. Πρόσβασης 11.8.2025]

δυνατότητα να ελέγχουν εξ αποστάσεως το λειτουργικό σύστημα, χωρίς ανίχνευση, θέτοντας σε κίνδυνο το δίκτυο και τα προσωπικά στοιχεία του χρήστη.

ε) RedShells: εγκαθίστανται σε μια συσκευή κατά την εγκατάσταση συγκεκριμένων παιχνιδιών υπολογιστή και παρακολουθούν την δραστηριότητα του χρήστη, για σκοπούς μάρκετινγκ, χωρίς σαφή συγκατάθεση, συνδέοντας την διαδικτυακή δραστηριότητα με τη χρήση παιχνιδιών, εγείροντας ανησυχίες για την προστασία της ιδιωτικής ζωής.

στ) Tracking cookies: παρακολουθούν την δραστηριότητα του χρήστη σε διάφορους ιστότοπους. Μπορεί να είναι καλοήθη, συμβάλλοντας στην εξατομίκευση της εμπειρίας του χρήστη, αλλά μπορεί και να λειτουργήσουν κακόβουλα, συλλέγοντας και κοινοποιώντας τα δεδομένα για στοχευμένη διαφήμιση.

ζ) Web beacons: μικροσκοπικά, αόρατα γραφικά ενσωματωμένα σε email ή ιστότοπους. Παρακολουθούν, αν ο χρήστης έχει ανοίξει ένα μήνυμα ή έχει επισκεφθεί μια σελίδα. Χρησιμοποιούνται συχνά για νόμιμες αναλύσεις μάρκετινγκ, αλλά οι κυβερνοεγκληματίες μπορούν επίσης να τα εκμεταλλευτούν για παρακολούθηση.

Αναφορικά με τον τρόπο δράσης των λογισμικών κατασκοπείας, όπως ήδη εκτέθηκε, εκείνο που τα χαρακτηρίζει είναι η δυνατότητά τους, να διεισδύουν στην συσκευή (κινητό τηλέφωνο, Η/Υ κλπ.), εν αγνοία και χωρίς την συγκατάθεση του χρήστη. Μετά την εγκατάστασή τους αποκτούν πρόσβαση και συλλέγουν δεδομένα (όπως η δραστηριότητα του χρήστη στο πληκτρολόγιο, το ιστορικό περιήγησης, η αλληλογραφία, τα αρχεία του, ενώ ορισμένα από αυτά μπορούν ακόμη και να ενεργοποιήσουν το μικρόφωνο ή την κάμερα της συσκευής καταγράφοντας τα σχετικά δεδομένα ήχου η/και εικόνας), τα οποία εν συνεχεία αποστέλλουν σε τρίτα μέρη (κυβερνοεγκληματίες ή hackers), με σκοπό την παρακολούθηση της δραστηριότητας του χρήστη, την υποκλοπή προσωπικών του δεδομένων ή προκειμένου να του αποσπαστούν χρηματικά ποσά[10].

Συχνά η εγκατάσταση των spyware λαμβάνει χώρα, όταν ο χρήστης κλικάρει σε επικίνδυνο σύνδεσμο, μολυσμένο αρχείο (phishing) ή ψεύτικο ιστότοπο (spoofed websites) ή ακόμη κι όταν επιχειρήσει να εγκαταστήσει καλοήθες λογισμικό (downloading software), το οποίο όμως έχει παραποιηθεί από hacker.

[10] Birchall M. (2025), ο.π.

Κι ενώ τα λογισμικά κατασκοπείας έχουν σχεδιαστεί, ώστε να μην είναι ανιχνεύσιμα, εντούτοις μπορεί να προκαλέσουν προβλήματα στη συσκευή, όπως μειωμένη απόδοση, υψηλή κατανάλωση ενέργειας, εμφάνιση μη αναμενόμενων αναδυόμενων παραθύρων ή ασυνήθιστη κατανάλωση δεδομένων. Η αναγνώριση αυτών των προειδοποιητικών ενδείξεων μπορεί να συμβάλλει στη λήψη προληπτικών μέτρων, προς αποτροπή την παραβίασης του απορρήτου ή της ασφάλειας των δεδομένων.

Θα πρέπει να καταστεί σαφές ότι, τα λογισμικά κατασκοπείας δεν αποτελούν άνευ ετέρου παράνομα λογισμικά. Ο προορισμός τους μπορεί να είναι νόμιμος, ωστόσο η δυνατότητα κατάχρησής τους, για εκτός του νόμου σκοπούς αποτελεί σοβαρότατο κίνδυνο.

1.1.1 Ειδικά ως προς τον τρόπο δράσης του λογισμικού Pegasus

Με αφορμή τις αποκαλύψεις περί παρακολούθησης δημοσιογράφων, πολιτικών, δικηγόρων, ακτιβιστών και εν γένει κρατικών αξιωματούχων εντός της Ε.Ε., με την χρήση του λογισμικού Pegasus, το Ευρωπαϊκό Κοινοβούλιο, δημοσίευσε το 2022, την μελέτη[11] του με τίτλο «*Europe's PegasusGate – Countering spyware abuse*», σχετικά με την χρήση του συγκεκριμένου λογισμικού σε χώρες της Ευρωπαϊκής Ένωσης, τους κινδύνους που αυτή ελλοχεύει και προτεινόμενους τρόπους αντιμετώπισης αυτών.

Σε αυτή, αναδεικνύεται ότι η πρόκληση, που θέτουν τα λογισμικά κατασκοπείας, εν γένει, σχετίζεται με το γεγονός ότι η παραδοσιακή υποκλοπή δεδομένων, που επιτυγχανόταν μέσω κοριού, διαφέρει σημαντικά από την παραβίαση (hacking) των σύγχρονων ψηφιακών συσκευών, δεδομένου ότι η τελευταία επιτρέπει:

α) τη συλλογή μεγαλύτερου όγκου πληροφοριών: εκτός από την πρόσβαση σε μηνύματα στην, υπό επίθεση, συσκευή, πλέον μπορεί κάποιος να αποκτήσει επίσης πρόσβαση και ενδεχομένως να χειριστεί όλες τις πληροφορίες, που είναι αποθηκευμένες σε αυτήν.

β) την υπέρβαση των τεχνολογιών κρυπτογράφησης: στις σύγχρονες εφαρμογές επικοινωνιών μεταξύ χρηστών, τα αρχικά μηνύματα πριν αποσταλούν κρυπτογραφούνται, ήτοι μετατρέπονται σε κείμενο, το οποίο δεν είναι κατανοητό από τρίτους και για την ανάκτησή τους

[11] «*Europe's PegasusGate – Countering spyware abuse*», Μελέτη του Ευρωπαϊκού Κοινοβουλίου (2022), σελ. 3-6. Διαθέσιμη σε: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729397. [Ημ. Πρόσβασης 14.6.2025]

απαιτείται να αποκρυπτογραφηθούν, χρησιμοποιώντας ένα μυστικό κλειδί, το οποίο είναι διαθέσιμο μόνο στον αποδέκτη (διατερματική κρυπτογράφηση). Με τη χρήση hacking καθίσταται δυνατή η παράκαμψη της κρυπτογράφησης, καταγράφοντας τα αρχικά μηνύματα πριν αυτά κρυπτογραφηθούν. Όταν οι εγκληματικές δραστηριότητες βασίζονται σε προηγμένες τεχνολογίες κρυπτογράφησης, μπορεί να δικαιολογείται το hacking συσκευών, για την αντιμετώπιση των σοβαρότερων εγκλημάτων και απειλών για την εθνική ασφάλεια. Ωστόσο, ελλείψει αυστηρών περιορισμών και αποτελεσματικών ελέγχων, η πρακτική της παραβίασης συσκευών, μάλλον δεν συνάδει με το νομικό πλαίσιο της ΕΕ και γενικότερα με τη διατήρηση της δημοκρατίας και των ανθρωπίνων δικαιωμάτων[12].

Σχετικά με το Pegasus: Το Pegasus είναι ένα λογισμικό ικανό να παραβιάσει κινητά τηλέφωνα και να συλλέξει τεράστιες ποσότητες δεδομένων, που αποθηκεύονται ή υποβάλλονται σε επεξεργασία από το σύστημα-στόχο. Ο κατασκευαστής του, ο Όμιλος NSO, το διαφήμισε ως εργαλείο για «κυβερνοπόλεμο» και οι New York Times το χαρακτήρισαν περίτεχνα ως «το πιο ισχυρό κυβερνοόπλο στον κόσμο». Σύμφωνα με τον συνιδρυτή της NSO, Shalev Hulio, τέτοιες τεχνολογίες έχουν καταστεί απαραίτητες, εξαιτίας της κρυπτογράφησης των ηλεκτρονικών επικοινωνιών, που αρνούνται στις κυβερνήσεις την πρόσβαση σε ιδιωτικές επικοινωνίες (πρόβλημα «απόκρυψης»). Σε σύγκριση με τις μαζικές παρακολουθήσεις, οι οποίες στοχεύουν στη συλλογή και ανάλυση αδιακρίτως τεράστιων ποσοτήτων δεδομένων, το Pegasus εκμεταλλεύεται τρωτά σημεία σε κινητά τηλέφωνα προκαθορισμένων χρηστών, δεν απαιτεί τη συμμετοχή παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών και συνδυάζει μια ποικιλία εργαλείων ηλεκτρονικής επιτήρησης. Δίνει τη δυνατότητα στους χειριστές του να διαβάζουν μηνύματα κειμένου, να παρακολουθούν κλήσεις, να συλλέγουν κωδικούς πρόσβασης, να εντοπίζουν τοποθεσίες, να έχουν πρόσβαση και να καταγράφουν συσκευές μικροφώνου και κάμερας, καθώς και να συλλέγουν πληροφορίες από εφαρμογές, χωρίς να το αντιλαμβάνεται ο στόχος, ακόμη και διασυνοριακά («εξωεδαφική εμβέλεια»).

Το λογισμικό λαμβάνεται και εγκαθίσταται αυτόματα στη συσκευή-στόχο, αφού ο χειριστής του, είτε (i) παραπλανήσει τον στόχο, ώστε να κλικάρει, σε έναν δυσδιάκριτο

[12] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 - January 2023, ο.π. σελ. 21-22.

σύνδεσμο εκμετάλλευσης («σύνδεσμος ηλεκτρονικού «ψαρέματος» SMS), είτε (ii) εξαπατήσει τη συσκευή-στόχο, ώστε να συνδεθεί σε ένα ψεύτικο δίκτυο κινητής τηλεφωνίας, γνωστό ως IMSI catcher, είτε (iii) εκμεταλλευτεί μια άγνωστη εγγενή ευπάθεια της συσκευής-στόχου, δηλαδή χωρίς ενέργεια από τον χρήστη αυτής.

Μόλις το λογισμικό διεισδύσει στο σύστημα, απενεργοποιεί τους μηχανισμούς προστασίας και τις ενημερώσεις ασφαλείας. Η μολυσμένη συσκευή, στη συνέχεια, μεταδίδει τα συλλεγμένα δεδομένα πίσω σε έναν διακομιστή δεδομένων Pegasus, μέσω του «Δικτύου Ανωνυμοποιημένης Μετάδοσης Pegasus» – πιθανώς ενός ιδιόκτητου συστήματος της NSO, που αποσκοπεί στην απόκρυψη της ταυτότητας του χειριστή (π.χ. κυβέρνηση ενός κράτους).

Η διεπαφή χρήστη (Pegasus' interface) είναι εύχρηστη, μερικές φορές απαιτώντας μόνο την εισαγωγή ενός αριθμού τηλεφώνου-στόχου. Σύμφωνα με πληροφορίες, η NSO εισήγαγε βιομετρικούς ελέγχους για να διασφαλίσει, ότι μόνο εξουσιοδοτημένα άτομα θα μπορούσαν να έχουν πρόσβαση στο σύστημα, μετά από κατάχρηση από έναν υπάλληλό της.

Η NSO ισχυρίζεται ότι παρέχει μόνο το λογισμικό και δεν το «λειτουργεί» και υποτίθεται ότι δεν έχει καμία εικόνα για τη χρήση του λογισμικού, αλλά οι ειδικοί ασφαλείας το αμφισβητούν αυτό. Σε συνέντευξη του, ο Shalev Hulio εξήγησε ότι η NSO μπορεί να έχει πρόσβαση στο σύστημα και να διεξάγει εγκληματολογική έρευνα για πιθανές καταχρήσεις, μόνο κατόπιν αιτήματος ή με την άδεια των κυβερνήσεων-πελατών. Η NSO μπορεί, ωστόσο, να τερματίσει εξ αποστάσεως το σύστημα Pegasus όταν υποψιάζεται κατάχρηση («kill switch»).

Σύμφωνα επίσης με την NSO, η τελευταία παραχωρεί άδεια χρήσης του λογισμικού της μόνο σε ελεγμένες κυβερνήσεις και το εξάγει, μέσω εταιρικών οντοτήτων με έδρα το Ισραήλ, τη Βουλγαρία και την Κύπρο, σε κυβερνήσεις, μόνο για νόμιμη χρήση και αποκλειστικά για σκοπούς πρόληψης και διερεύνησης εγκλημάτων και τρομοκρατίας, ενώ αρνήθηκε να πουλήσει το προϊόν της σε περίπου 90 χώρες, λόγω ανησυχίας για πιθανή παραβίαση των ανθρωπίνων δικαιωμάτων.

Ωστόσο, οι έρευνες των Ευρωπαϊκών Οργάνων ανέδειξαν ότι κατασκοπευτικά λογισμικά (όπως το Pegasus και άλλα) έχουν χρησιμοποιηθεί από κρατικούς φορείς με παραπλανητικό τρόπο, μέσω της μεταμφίεσης σε νόμιμο πρόγραμμα, αρχείο ή περιεχόμενο («Δούρειος Ιππος»), όπως λ.χ. μέσω ψευδών μηνυμάτων από δημόσιους οργανισμούς. Έχει μάλιστα διαπιστωθεί, ότι σε ορισμένες περιπτώσεις δημόσιες αρχές έχουν συνεργαστεί με

ιδιωτικούς παρόχους τηλεφωνίας, προκειμένου να διαβιβάσουν κακόβουλο περιεχόμενο στη συσκευή του στοχοποιούμενου προσώπου, το οποίο, εκμεταλλευόμενο τα τρωτά σημεία του συστήματος ασφαλείας του δικτύου και χωρίς τη διάδραση του στόχου, μπορεί να απομακρύνει όλα τα ίχνη της παρουσίας του, μετά την απεγκατάσταση και μέσω της ανωνυμοποίησης του συνδέσμου μεταξύ απομακρυσμένων χειριστών και του διακομιστή[13].

1.2 Εφαρμογές – Χρήσεις Λογισμικών Κατασκοπείας

Τα λογισμικά κατασκοπείας μπορεί να αποτελέσουν πολύτιμο εργαλείο, για την καταπολέμηση του εγκλήματος, αλλά όταν τα χρησιμοποιούν λανθασμένα οι κυβερνήσεις γίνονται τεράστιος κίνδυνος για το κράτος δικαίου και τα θεμελιώδη δικαιώματα[14].

Χαρακτηριστική η περίπτωση Pegasus. Η NSO ισχυρίζεται ότι σύμφωνα με τις συμβατικές της ρήτρες, το Pegasus μπορεί να χρησιμοποιηθεί μόνο για την καταπολέμηση της τρομοκρατίας και του εγκλήματος, ωστόσο η πραγματικότητα αποδεικνύει ότι το Pegasus χρησιμοποιείται και για άλλους σκοπούς. Κατά δήλωσή της, έχει πουλήσει το Pegasus σε 60 κυβερνητικές υπηρεσίες σε 40 χώρες. Η έκταση της χρήσης (και της κατάχρησης) του Pegasus προέκυψε για πρώτη φορά μέσα από μια έρευνα του 2018[15] από το Citizen Lab του Πανεπιστημίου του Τορόντο, η οποία ανακάλυψε στοιχεία, που δείχνουν ότι το Pegasus χρησιμοποιείται σε 45 χώρες, μερικές από τις οποίες βρίσκονται υπό αυταρχικά καθεστώτα. Σύμφωνα με έκθεση του 2021 που εκδόθηκε από το Pegasus Project —μια συνεργατική πρωτοβουλία που αναλήφθηκε από περισσότερους από 80 δημοσιογράφους από 17 οργανισμούς μέσων ενημέρωσης σε 10 χώρες, υπό τον συντονισμό του Forbidden Stories, με την τεχνική υποστήριξη της Διεθνούς Αμνηστίας— το κατασκοπευτικό λογισμικό Pegasus έχει

---

[13] Σύσταση του Ευρωπαϊκού Κοινοβουλίου της 15ης Ιουνίου 2023 προς το Συμβούλιο και την Επιτροπή σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (2023/2500(RSP)). Διαθέσιμη σε: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EL.html. [Ημ. Πρόσβασης 14.7.2025]

[14] Δήλωση Προέδρου Εξεταστικής Επιτροπής του Ευρωπαϊκού Κοινοβουλίου για τη διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού (PEGA).

[15] Marczak B., Scott-Railton J., McKune S., Razzak A.B., Deibert R., (18.9.2018), *"HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries"*, Citizen Lab. Διαθέσιμο σε https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/. [Ημ. Πρόσβασης 29.8.2025]

χρησιμοποιηθεί ευρέως από κυβερνήσεις σε όλο τον κόσμο, για να στοχεύσει ακτιβιστές ανθρωπίνων δικαιωμάτων, προσωπικότητες της αντιπολίτευσης, δικηγόρους, δικαστές και ξένους ηγέτες. Το Pegasus Project δημοσίευσε, επίσης, μια λίστα με 50.000 αριθμούς τηλεφώνου, που φαίνεται να ανήκουν σε άτομα, που είχαν επιλεγεί από τους πελάτες της ισραηλινής NSO Group ως πιθανοί στόχοι παρακολούθησης. Το Ευρωπαϊκό Κοινοβούλιο συγκρότησε την Εξεταστική Επιτροπή PEGA, επιφορτισμένη με τη διερεύνηση της χρήσης του Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης. Σύμφωνα με την έρευνα της Επιτροπής, προκύπτουν ισχυρά στοιχεία για τη χρήση του Pegasus στην ΕΕ. Φαίνεται ότι η NSO Group έχει πωλήσει τα προϊόντα της σε 22 τελικούς χρήστες σε τουλάχιστον 14 κράτη μέλη, μεταξύ των οποίων η Πολωνία, η Ουγγαρία, η Ισπανία και οι Κάτω Χώρες. Δύο κράτη μέλη, η Κύπρος και η Βουλγαρία, χρησίμευσαν ως εξαγωγικοί κόμβοι, για το κατασκοπευτικό λογισμικό[16].

Καθίσταται φανερό, ότι τα λογισμικά κατασκοπείας, παρά τις διαβεβαιώσεις των κατασκευαστών τους για την νομιμότητα του προορισμού τους, εντούτοις έχουν αποτελέσει, στα χέρια των Αρχών πολλών κρατών, «βόμβα» για τα ανθρώπινα δικαιώματα, καθώς μετατρέπονται σε όπλο, που επιλέγουν οι καταπιεστικές κυβερνήσεις, για να φιμώσουν δημοσιογράφους, να επιτεθούν σε ακτιβιστές και να συντρίψουν την διαφωνία[17].

Συνιστούν, ακόμη, βασικό μέσο για την διάπραξη κυβερνοεγκλημάτων[18] και κυβερνοεπιθέσεων[19]. Το λογισμικό κατασκοπείας, δεδομένων των τεχνικών χαρακτηριστικών του, ήτοι της ισχυρής διεισδυτικής του ικανότητας, εν αγνοία του χρήστη και της ικανότητάς του να συλλέγει δεδομένα, σε μεγάλο εύρος, αποτελεί σημαντικό εργαλείο διάπραξης αδικημάτων, όπως η ηλεκτρονική απάτη και η κλοπή ταυτότητας. Τα αδικήματα αυτά τελούνται με την

---

[16] Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 - January 2023, ο.π., σελ. 25-26.

[17] Agnès Callamard, Γ.Γ. της Διεθνούς Αμνηστίας.

[18] Το κυβερνοέγκλημα διακρίνεται σε κυβερνοέγκλημα εν γένει (αξιόποινη πράξη με χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών) και κυβερνοέγκλημα stricto sensu (αξιόποινη πράξη μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών, όπου το δίκτυο και το πληροφοριακό σύστημα, αποτελούν όχι μόνο το μέσο, αλλά και το προσβαλλόμενο αγαθό).

[19] Κυβερνοεπίθεση είναι οποιαδήποτε κακόβουλη ενέργεια, που λαμβάνει χώρα μέσω ηλεκτρονικού υπολογιστή ή δικτύου και σκοπό έχει την τροποποίηση, καταστροφή, κλοπή, υποκλοπή ή και την μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες του νόμιμου κατόχου.

χρήση κακόβουλου λογισμικού ή μέσω phishing, με σκοπό ο παραβάτης να υποκλέψει πληροφορίες, που σχετίζονται με την ταυτότητα του θύματος, προκειμένου να τελέσει περαιτέρω αδικήματα, λ.χ. απάτη με πιστωτική κάρτα.

Ιδιαίτερα διαδεδομένη είναι η χρήση λογισμικών κατασκοπείας στο τομέα των διαφημίσεων και του marketing. Όπως, ήδη, εκτέθηκε, τα λογισμικά adware, μπορούν να εισέλθουν νόμιμα στη συσκευή ενός χρήστη, όταν εγκαθιστά ορισμένα δωρεάν προγράμματα ή εφαρμογές, όπως παιχνίδια, με τη μορφή αναδυόμενων παραθύρων διαφημίσεων. Καθώς, στην πράξη, τίποτα δεν είναι δωρεάν, όσοι δημιουργούν δωρεάν προγράμματα και εφαρμογές, πρέπει με κάποιο τρόπο να αποκομίσουν κέρδος, το οποίο συνίσταται στην προώθηση διαφημίσεων μέσω adware, συνήθως εν αγνοία του χρήστη.

Το adware, ωστόσο, μπορεί να αποδειχθεί εξαιρετικά επικίνδυνο. Τούτο συμβαίνει, όταν τα αναδυόμενα παράθυρα, όχι μόνο προωθούν διαφημίσεις, αλλά παράλληλα συλλέγουν δεδομένα και πληροφορίες, προκειμένου ο χρήστης να γίνει στόχος προσαρμοσμένων διαφημίσεων. Η συνεχής παρακολούθηση των διαδικτυακών δραστηριοτήτων των χρηστών βοηθά στην εξατομίκευση των διαφημίσεων. Όσο πιο εξατομικευμένη είναι μια διαφήμιση, τόσο αυξάνονται οι πιθανότητες να κλικάρει ο χρήστης σε αυτήν. Ορισμένα λογισμικά adware έχουν σχεδιαστεί να προκαλούν σκόπιμη ανακατεύθυνση, για την προώθηση συγκεκριμένων ιστότοπων. Άλλα πάλι, έχουν σχεδιαστεί για να κάνουν περισσότερα από την απλή προβολή ανεπιθύμητων διαφημίσεων και πιο συγκεκριμένα για να εγκαθιστούν κρυφά επικίνδυνα προγράμματα, όπως Trojans και ransomware[20].

Την πιο διαδεδομένη μορφή adware αποτελούν τα γνωστά σε όλους cookies[21]. Κάποια εξ αυτών, τα λεγόμενα tracking cookies αποτελούν εν δυνάμει κίνδυνο, για τον χρήστη,

---

[20] Το ransomware (λυτρισμικό) έχει σχεδιαστεί για να κρυπτογραφεί αρχεία από μια συσκευή, καθιστώντας τα αρχεία αυτά, καθώς και τα συστήματα, που βασίζονται σε αυτά, μη προσβάσιμα. Προκειμένου να αποκατασταθεί η πρόσβαση των χρηστών στα κλειδωμένα αρχεία, οι δράστες απαιτούν λύτρα (συνήθως σε κρυπτονομίσματα). Το ransomware αποτελεί μάστιγα των κυβερνοεπιθέσεων, ιδίως για τις επιχειρήσεις, κλειδώνοντας κρίσιμα εταιρικά συστήματα και προκαλώντας απώλεια τζίρου, εξαιτίας του παγώματος των συστημάτων παραγωγής ή των eshops (αν όχι εξαιτίας της καταβολής των λύτρων) και διαρροή δεδομένων πελατών.

[21] 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 ιστοτόπος ανακτά τις εν λόγω πληροφορίες σε κάθε επίσκεψη προκειμένου να προσφέρει σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων

συλλέγοντας και κοινοποιώντας τα δεδομένα του για στοχευμένη διαφήμιση. Η ΑΠΔΠΧ έχει δημοσιεύσει συστάσεις[22] προς τους υπεύθυνους επεξεργασίας δεδομένων, σχετικά με την χρήση cookies, αποδίδοντας ιδιαίτερη έμφαση στο δικαίωμα συγκατάθεσης του χρήστη, κατόπιν έγκαιρης και πλήρους ενημέρωσής του.

1.3 Μέτρα Προστασίας έναντι Κατασκοπευτικών Λογισμικών

Η προστασία έναντι των λογισμικών κατασκοπείας επιτυγχάνεται κατ' αρχάς με την χρήση αξιόπιστου λογισμικού anti-spyware, με σκοπό την, εκ των προτέρων, ανίχνευση κατασκοπευτικού λογισμικού και τον αποκλεισμό του. Σημαντική κρίνεται η έγκαιρη ενημέρωση του λειτουργικού συστήματος της συσκευής, ώστε να καλυφθούν τα τρωτά σημεία ασφαλείας, που συχνά εκμεταλλεύεται το spyware. Σκόπιμη θα ήταν, επιπροσθέτως, η χρήση προγράμματος αποκλεισμού αναδυόμενων παραθύρων (pop-up blocker), ώστε να εξαλειφθούν οι πιθανότητες κλικαρίσματος κακόβουλων διαφημίσεων. Ο χρήστης, ακόμη θα πρέπει να λαμβάνει και να εγκαθιστά εφαρμογές, μόνο από το επίσημο κατάστημα του λειτουργικού συστήματος της εκάστοτε συσκευής, αποφεύγοντας την εγκατάσταση λογισμικού από άλλες πλατφόρμες, καθώς συχνά από αυτές μεταφέρεται κεκαλυμμένα κακόβουλο λογισμικό.

Ιδιαίτερη προσοχή απαιτείται ακόμη και κατά την διαδικασία αποδοχής των cookies. Η συγκατάθεση στην περίπτωση αυτή θα πρέπει να παρέχεται στοχευμένα και μόνο σε αξιόπιστους ιστότοπους. Αυτονόητο είναι ότι ο χρήστες δεν θα πρέπει σε καμία περίπτωση να κλικάρουν σε συνδέσμους, που λαμβάνουν μέσω email ή μηνυμάτων SMS, ενώ περαιτέρω θα πρέπει να αγνοούν ύποπτα μηνύματα από άγνωστους αποστολείς, τα οποία συνοδεύονται συχνά από συνημμένα αρχεία, τα οποία κατ' ουσίαν χρησιμοποιούνται για phishing.

πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει σε αυτή (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, κ.λπ.). Διακρίνονται σε first – party cookies (εγκαθίστανται από τον ίδιο τον πάροχο της ιστοσελίδας) και third-party cookies (δημιουργούνται από άλλους ιστότοπους και μπορεί να αποτελούν κατασκοπευτικά λογισμικά, μέσω των οποίων καταγράφεται η δραστηριότητα του χρήστη και συλλέγονται δεδομένα, τα οποία ενδεχομένως πωλούνται).

[22]«*Συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες*», Γ/ΕΞ/1525/25.2.2020 Δελτίο Τύπου ΑΠΔΠΧ. Διαθέσιμο σε: https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythynon-epexergasias-dedomenon-me-tin-eidiki. [Ημ. Πρόσβασης 13.8.2025]

Ας σημειωθεί, βέβαια, ότι ακόμη και η λήψη των, ως άνω, μέτρων προστασίας, αποδεικνύεται συχνά ανεπαρκής να διαφυλάξει την ασφάλεια συσκευών και συστημάτων από τον κίνδυνο λογισμικών κατασκοπείας, καθώς λόγω των τεχνικών χαρακτηριστικών τους, ιδίως εξαιτίας της ισχυρής διεισδυτικότητάς τους και της αυξημένης δυσχέρειας εντοπισμού τους, τα κατασκοπευτικά λογισμικά είναι σε θέση να στοχοποιήσουν εύκολα τους χρήστες, χωρίς μάλιστα πολλές φορές, οι τελευταίοι να προβούν σε οποιαδήποτε πλημμελή ενέργεια. Για τον λόγο αυτό, κρίνεται σκόπιμη και απολύτως αναγκαία η εισαγωγή αποτελεσματικού ρυθμιστικού πλαισίου, το οποίο θα οριοθετήσει την δυνατότητα χρήσης τους, τουλάχιστον από τους κρατικούς φορείς και θα προβλέψει ενδεχομένως την εκ του σχεδιασμού (by design) ύπαρξη συγκεκριμένων τεχνικών χαρακτηριστικών των λογισμικών κατασκοπείας, ώστε να δύναται να καταγραφεί η νομιμότητα της δραστηριότητάς τους.

2. ΕΡΜΗΝΕΥΤΙΚΗ ΑΝΑΛΥΣΗ ΑΡΘΡΟΥ 19 ΣΥΝΤΑΓΜΑΤΟΣ ΚΑΙ ΤΟΥ Ν. 5002/2022

2.1 Το άρθρο 19 του Συντάγματος

Σύμφωνα με τη διάταξη του άρθρου 19 του Συντάγματος[23]:

«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.»

Αντικείμενο προστασίας της ανωτέρω διάταξης αποτελεί το επικοινωνιακό απόρρητο, κατοχυρώνοντας όχι μόνο την ελευθερία της ανταπόκρισης ή επικοινωνίας, αλλά και το απολύτως απαραβίαστο αυτών, το οποίο, άλλωστε, ενδεικνύει η χαρακτηριστική διατύπωση του συντακτικού νομοθέτη με την χρήση όρων όπως: «απόλυτα απαραβίαστο», «εγγυήσεις», «λόγοι εθνικής ασφάλειας», «για την διακρίβωση ιδιαιτέρως σοβαρών εγκλημάτων».

Πρόκειται για ύψιστης σημαντικότητας δικαίωμα, αναγόμενο στον πυρήνα της ανθρώπινης υπόστασης[24] και άρρηκτα συνδεδεμένο με πλείστες ατομικές ελευθερίες[25], όπως η, εν γένει, προσωπική ελευθερία (άρθρο 5 Σ.), η ελευθερία της ιδιωτικής ζωής (άρθρο 9 παρ. 1 εδ. β' Σ.), η ελεύθερη ανάπτυξη της προσωπικότητας (άρθρο 5 παρ. 1 Σ.), η ελευθερία της γνώμης (άρθρο 10 ΕΣΔΑ), το δικαίωμα ελεύθερης πρόσβασης στη πληροφόρηση (άρθρο 5Α Σ.) και το δικαίωμα της πληροφοριακής αυτοδιάθεσης του ατόμου στον τομέα των ηλεκτρονικών

---

[23] ΦΕΚ Α' 211/24.12.2019. Διαθέσιμο σε: https://search.et.gr/el/fek/?fekId=605083.

[24] Παπανικολάου Α. (2022): *«Επικοινωνιακό απόρρητο: προβληματισμοί για τη διασφάλιση ενός κλασικού δικαιώματος στο πεδίο των σύγχρονων κατασκοπευτικών λογισμικών»*, Syntagmawatch. Διαθέσιμο στο: https://www.syntagmawatch.gr/trending-issues/epikoinwniako-aporrhto-provlhmatismoi-gia-th-diasfalish-enos-klasikou-dikaiwmatos-sto-pedio-twn-sygxronwn-kataskopeutikwn-logismikwn/. [Ημ. Πρόσβασης 11.6.2025]

[25] Μάνεσης Α. (1982), *«Συνταγματικά Δικαιώματα, τόμ. α' Ατομικές Ελευθερίες»* (πανεπιστημιακές παραδόσεις), δ' έκδοση, σελ. 232 επ.

επικοινωνιών (άρθρο 9Α Σ.)[26]. Ενόψει δε, του γεγονότος ότι προστατεύει την, ελεύθερη και εμπιστευτική προς ένα άλλο πρόσωπο (ανταποκριτή), εκδήλωση και ανακοίνωση των στοχασμών, ιδεών, συναισθημάτων, μετέχει και της πνευματικής ελευθερίας και διακίνησης ιδεών και στοχασμών (άρθρο 14 Σ.) Αξίζει να διευκρινιστεί πως, μολονότι το άρθρο 19 Σ. προϋποθέτει την ελευθερία του «επικοινωνείν», αυτή κατοχυρώνεται στα άρθρα 14, 5 και 5Α του Συντάγματος.

2.1.1 Ερμηνεία και διασάφηση επιμέρους όρων

Αποσαφηνίζοντας τους όρους **«ανταπόκριση»** και **«επικοινωνία»**, εκ πρώτης όψεως φαίνεται να ταυτίζονται[27], υπό την έννοια, ότι ο όρος «επικοινωνία» εμπεριέχει και την έννοια της «ανταπόκρισης», η οποία προσδιορίζεται ως η, εξ αποστάσεως, επικοινωνία με την χρήση τεχνικού μέσου, που την καθιστά εφικτή[28]. Στην πραγματικότητα, όμως, και με δεδομένο ότι το Σύνταγμα θα πρέπει να αποτελεί ένα ευέλικτο κείμενο, ώστε να μην απαιτείται η αναθεώρησή του, ο συντακτικός νομοθέτης στόχευσε στην ευρεία εννοιολογική κάλυψη, ώστε να διασφαλίσει, ότι η, εν λόγω, συνταγματική διάταξη θα μπορεί να τύχει εφαρμογής σε *κάθε ενδεχόμενο που δυνητικά θα προκύψει από την τεχνολογική εξέλιξη, συμπεριλαμβάνοντας κάθε τεχνικό – υπαρκτό ή δυνητικά υπαρκτό – σύστημα*[29]. Έτσι, με την υιοθετηθείσα εκδοχή, εξασφαλίστηκε η ευρυχωρία του συνταγματικού κανόνα, έτσι ώστε στην συμπεριληπτική έννοια της επικοινωνίας του άρθρου 19 Σ. να εμπεριέχεται σήμερα, χωρίς την παραμικρή ανάγκη ερμηνευτικών υπερβάσεων, το σύνολο των επικοινωνιακών εξελίξεων[30].

Ως προς την σημασία του όρου της επικοινωνίας, διακρίνουμε αφενός την, υπό ευρεία έννοια, επικοινωνία, η οποία υποδηλώνει κάθε ανθρώπινη σχέση, και την εν στην εννοία επικοινωνία, η οποία κατοχυρώνεται στη διάταξη του άρθρου 19 του Συντάγματος και περιλαμβάνει την μεταβίβαση μηνύματος, με συγκεκριμένο περιεχόμενο, μεταξύ αυτών που

---

[26] Τσόλιας Γ. (2013) «*Απόρρητο Ηλεκτρονικών Επικοινωνιών Ι - Συνταγματικό πλαίσιο προστασίας του απορρήτου στον τομέα των τηλεπικοινωνιών*». Σε Παύλου Σ., Σάμιο Θ. επιμ. Ειδικοί Ποινικοί Νόμοι. Αθήνα: Εκδόσεις Π.Ν. Σάκκουλα, σελ. 3.

[27] Παντελής Α. (2018), «*Εγχειρίδιο Συνταγματικού Δικαίου*», 4η έκδοση, Εκδοτικός Οίκος Λιβάνη, σελ. 511.

[28] Τσόλιας Γ. (2013), ο.π., σελ. 5.

[29] Παναγοπούλου Φ. (2023): «*Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 19*», σελ. 12, Syntagmawatch. Διαθέσιμο στο: https://www.syntagmawatch.gr/my-constitution/arthro-19/. [Ημ. Πρόσβασης 13.6.2025]

[30] Βενιζέλος Ε. (2022), «*Δικαστικός έλεγχος της συνταγματικότητας των νόμων και ερμηνεία του Συντάγματος – Μαθήματα Εμβάθυνσης στο Συνταγματικό Δίκαιο*», Εκδόσεις Σάκκουλας, 23 επ.

επικοινωνούν[31]. Η, εν στενή εννοία, επικοινωνία διακρίνεται, περαιτέρω, αφενός, στα *βασικά στοιχεία της*, ήτοι τα πρόσωπα που επικοινωνούν και το διαβιβαζόμενο μήνυμα και αφετέρου, στα *δευτερεύοντα στοιχεία της*, ήτοι το σήμα, το κανάλι, τα μέσα και τον μεταδότη[32]. Η, απορρέουσα εκ της διάταξης του άρθρου 19 Σ, προστασία, καταλαμβάνει την ελεύθερη και απόρρητη επικοινωνία, τόσο δια ζώσης και με άμεσο τρόπο, όσο και κάθε άλλου είδους ή μορφή της, ακόμη και μέσω δημόσιων ή ιδιωτικών δικτύων παροχής υπηρεσιών επικοινωνιών[33].

Κατ' ορθή δε ερμηνεία και δοθέντος, ότι ο συντακτικός νομοθέτης δεν προβαίνει σε καμία διάκριση μεταξύ εσωτερικών και εξωτερικών στοιχείων επικοινωνίας, στο πεδίο εφαρμογής του απορρήτου των επικοινωνιών υπάγονται όχι μόνον τα εσωτερικά στοιχεία της επικοινωνίας (το περιεχόμενο του μηνύματος αυτό καθ' αυτό), αλλά και τα εξωτερικά στοιχεία αυτής, δηλαδή τα μεταδεδομένα (metadata), όπως λ.χ. τα δεδομένα κινήσεως και θέσεως, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή, ο αριθμός τηλεφωνικής σύνδεσης των επικοινωνούντων, η διεύθυνση IP, η ημέρα, η ώρα, η διάρκεια και οι, εν γένει, συνθήκες της επικοινωνίας. Και τούτο, διότι τα μεταδεδομένα των ηλεκτρονικών επικοινωνιών παρέχουν τη δυνατότητα εξαγωγής ιδιαιτέρως ακριβών συμπερασμάτων, σε σχέση με την ιδιωτική ζωή των προσώπων, που επικοινωνούν, όπως είναι οι συνήθειες, οι μόνιμοι ή οι προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις των προσώπων αυτών και τα κοινωνικά περιβάλλοντα στα οποία τα πρόσωπα αυτά συχνάζουν[34], με συνέπεια, μέσω της επεξεργασίας των εξωτερικών στοιχείων, να μπορεί να ανασυντεθεί το λεγόμενο «βιοπορτραίτο» του επικοινωνούντος, ώστε να καθίσταται εφικτή η απεριόριστη εισβολή στα ιδιωτικά άδυτά του[35]. Έτσι, ακόμη και μία αναπάντητη τηλεφωνική κλήση ή ένα κενό γραπτό μήνυμα (SMS), υπάγονται στην προστατευτική σφαίρα του άρθρου 19 Σ., με την έννοια, ότι, ακόμη κι αν δεν υφίσταται περιεχόμενο, εντούτοις και μόνον, ότι κάποιος

---

[31] Βενιζέλος Ε. (2025), «*Το Ελληνικό Σύνταγμα*», τόμ. 1, Sakkoulas – Online.gr, σελ. 891. [Ημ. Πρόσβασης 8.8.2025]

[32] Ibidem, σελ. 891

[33] Παναγοπούλου Φ., ο.π., σελ. 12.

[34] Χελιουδάκης Λ. (2019): «*Διατήρηση Μεταδεδομένων Ηλεκτρονικών Επικοινωνιών: Το ευρωπαϊκό φάντασμα που θέλει να πάρει ξανά σάρκα και οστά*», Homo Digitalis. Διαθέσιμο στο: https://homodigitalis.gr/posts/4048/#1534226687868-199cba6f-d67a. [Ημ. Πρόσβασης 9.8.2025]

[35] Μαυρίας Κ. (1982), «*Το συνταγματικό δικαίωμα ιδιωτικού βίου*», Εκδόσεις Αντ. Ν. Σάκκουλα, σελ. 173.

κλήθηκε τηλεφωνικώς ή ότι έλαβε ένα κενό SMS (ενέργεια η οποία μπορεί να υποδηλώνει συγκεκριμένο γεγονός), είναι απόρρητα, ως *γεγονότα επικοινωνίας*[36].

Τα ανωτέρω επιβεβαιώνει πλήρως η πλούσια νομολογία τόσο του ΕΔΔΑ (Αποφάσεις *Big Brother Watch και λοιποί κατά Ην. Βασιλείου, Klass και λοιποί κατά Γερμανίας, P.G. and J.H. κατά Ην. Βασιλείου*), όσο και του ΔΕΕ (Υποθέσεις *Digital Rights Ireland Ltd* (C-293/12), *Tele 2 Sverige και Watson* (C-203/15 & C-698/2015)[37], *La Quadrature du Net* (C-511/18 & C-512/18) κλπ.), σύμφωνα με την οποία τα μεταδεδομένα επικοινωνίας προστατεύονται από το άρθρο 8 της ΕΣΔΑ και εξομοιώνονται πλήρως, ως προς την σπουδαιότητά τους για τον πυρήνα της ιδιωτικής ζωής, με το περιεχόμενο της επικοινωνίας καθ' εαυτό, εξ ου και θα πρέπει να τυγχάνουν ανάλογης, και σε καμία περίπτωση υποδεέστερης, προστασίας[38].

---

[36] ΣτΕ 1593/2016.

[37] Διαθέσιμη σε: https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EL. Το ΔΕΕ διαπιστώνει ότι: «*τα δεδομένα αυτά παρέχουν τα μέσα για τον προσδιορισμό … του προφίλ των προσώπων περί των οποίων πρόκειται, πληροφορία εξίσου ευαίσθητη, υπό το πρίσμα του σεβασμού της ιδιωτικής ζωής, με το περιεχόμενο αυτό καθ' αυτό των επικοινωνιών.*»

[38] Στην ελληνική έννομη τάξη διαπιστώθηκε επί μακρόν διχογνωμία του νομικού κόσμου ως προς το ζήτημα, αν τα μεταδεδομένα επικοινωνίας εντάσσονται στην προστατευτική σφαίρα του επικοινωνιακού απορρήτου. Σύμφωνα με τις υπ' αριθ. 9/2009, 12/2009 και 9/2011 Γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου, πέραν της κρίσης ότι το μονομερώς εγκληματικό περιεχόμενο μιας επικοινωνίας δεν απολαύει συνταγματικής προστασίας!!! περαιτέρω, τα εξωτερικά στοιχεία της επικοινωνίας (και η επικοινωνία μέσω διαδικτύου), δεν υπάγονται στο πεδίο προστασίας του απορρήτου των επικοινωνιών και κατ' επέκταση οι εισαγγελικές, ανακριτικές και προανακριτικές αρχές δικαιούνται να ζητούν από τους παρόχους πληροφορίες για τα εξωτερικά στοιχεία της επικοινωνίας, χωρίς περαιτέρω διατυπώσεις και χωρίς την τήρηση των προϋποθέσεων του Νόμου για την διαδικασία άρσης του απορρήτου. Πέραν των σφοδρών αντιδράσεων, της ανασφάλειας δικαίου και της πλήρους διάστασης της Νομολογίας του ΑΠ με αυτήν του ΕΔΔΑ και του ΔΕΕ, που προκάλεσαν οι ανωτέρω Γνωμοδοτήσεις, οδήγησαν αναπόφευκτα στην υποβολή, εκ μέρους ανακριτικών αρχών προς τους παρόχους υπηρεσιών επικοινωνίας, σωρηδόν αιτημάτων για την πρόσβαση στα μεταδεδομένα, και μάλιστα χωρίς την τήρηση της νόμιμης διαδικασίας, συνοδευόμενα τα αιτήματα αυτά συχνά, υπό την απειλή δίωξης των παρόχων, για τα αδικήματα της απείθειας και της υπόθαλψης εγκληματίας, σε περίπτωση μη συμμόρφωσης. Την τελευταία, ωστόσο, δεκαετία η νομολογία των Ελληνικών Δικαστηρίων (ΑΠ 1421/2010, ΣτΕ 1593/2016, ΣυμβΠλημμΑθ 613/2016, ΑΠ 1014/2020, ΟλΑΠ 4/2024) υιοθετεί σχεδόν παγιωμένα τη θέση ότι τα εξωτερικά στοιχεία της επικοινωνίας υπάγονται στην προστασία του απορρήτου και στους ειδικότερους όρους κάμψης αυτής, υπό τις προϋποθέσεις του Νόμου, συμμορφούμενη προς τις επιταγές της ευρωπαϊκής και διεθνούς έννομης τάξης.
Νομικό ζήτημα, ωστόσο, έχει εγείρει προσφάτως, η υπ' αριθ. 587/2025 απόφαση του ΣΤ' Ποινικού Τμήματος του Αρείου Πάγου, σύμφωνα με την οποία, τα παρελθοντικά δεδομένα (περιεχόμενο και μεταδεδομένα), αποθηκευμένα από παρόχους, σε τερματικό εξοπλισμό (λ.χ. υπολογιστή, κινητό τηλέφωνο κλπ.), μετά την ολοκλήρωση της επικοινωνίας ΔΕΝ τυγχάνουν προστασίας από το πεδίο του άρθρου 19 Σ., αλλά από διατάξεις για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων, με συνέπεια να μην απαιτείται, κατά την κρίση του ανωτέρω Δικαστηρίου, η τήρηση της διαδικασίας

Αναφορικά με την έννοια του όρου **«*απόρρητο*»,** αυτή θα μπορούσε να αποδοθεί ως «μυστικότητα», αποτελούμενη από το υποκειμενικό – προσωπικό στοιχείο (βούληση επικοινωνούντος) και το αντικειμενικό – κοινωνικό στοιχείο. Έτσι, απόρρητο επικοινωνίας «*υφίσταται εφόσον αυτός, που επικοινωνεί, εκδηλώνει μια βέβαιη υποκειμενική προσδοκία ότι το περιεχόμενο και τα στοιχεία της επικοινωνίας δεν θα περιέλθουν σε γνώση τρίτου και ότι η προσδοκία είναι τέτοια, ώστε η κοινωνία είναι πρόθυμη να την θεωρήσει εύλογη*[39]». Αν και ο χαρακτηρισμός μιας μορφής επικοινωνίας ως απόρρητης εναπόκειται στον κοινό νομοθέτη (λ.χ. επί επιστολής εντός κλειστού ή ανοιχτού φακέλου), εντούτοις το Σύνταγμα επιβάλλει την εφαρμογή του τεκμηρίου υπέρ του απορρήτου της επικοινωνίας, δηλαδή σε περίπτωση αμφιβολίας κάθε επικοινωνία τεκμαίρεται απόρρητη.

άρσης του επικοινωνιακού απορρήτου, υπό τις αυστηρές προϋποθέσεις των διατάξεων του Ν. 2225/1994 και ήδη του Ν. 5002/2022, με το σκεπτικό ότι ο συνταγματικός, αλλά και ο αναθεωρητικός νομοθέτης, δεν έχουν εκδηλώσει ρητώς τέτοια βούληση, μολονότι είχαν τη δυνατότητα να το πράξουν με αντίστοιχες συνταγματικές αναθεωρήσεις. Το Δικαστήριο, περαιτέρω, έκρινε ότι οι διατάξεις των σχετικών νομοθετημάτων για την άρση του απορρήτου των επικοινωνιών αφορούν αποκλειστικά μελλοντικές επικοινωνίες, κατ' αρχήν για διάστημα δύο (2) μηνών, με δυνατότητα παράτασης έως δέκα (10) μήνες, τηρουμένης της αρχής της αναλογικότητας, ενώ για τα παρελθοντικά δεδομένα, όπου οι επικοινωνίες έχουν ήδη λάβει χώρα, η άρση του απορρήτου μπορεί να διαταχθεί εξ αρχής για την αναγκαία περίοδο, έως δώδεκα (12) μήνες (Ν. 3917/2011) – χωρίς διαδοχικές παρατάσεις - καθώς τα δεδομένα αυτά καταστρέφονται αυτομάτως μετά το, εν λόγω, διάστημα. Όπως χαρακτηριστικά διαλαμβάνεται στο σκεπτικό της αποφάσεως. «*…, η ουσιώδης διαφοροποίηση της άρσης του απορρήτου για το μέλλον, σε σχέση με την άρση αυτού για το παρελθόν, έγκειται στο γεγονός ότι, στην πρώτη περίπτωση, (κατά την οποία υφίσταται μια δυναμική διαδικασία), η διάρκεια της άρσης εξαρτάται μεν από το υλικό της δικογραφίας (για την πρώτη χρονική περίοδο της άρσης), ενώ για τις επόμενες (δίμηνες συνήθως) παρατάσεις εξαρτάται κυρίως από τα προκύπτοντα ευρήματα κατά τη διάρκεια της μέχρι τότε παρακολούθησης του υπόπτου ή κατηγορουμένου, έτσι ώστε να αποφασίζεται κάθε φορά, αν είναι αναγκαίο ή όχι να συνεχίζεται η άρση του απορρήτου και η παρακολούθηση. Αντιθέτως, στη δεύτερη περίπτωση, (που αφορά σε μια στατική κατάσταση), τα ως άνω αρμόδια όργανα αποφαίνονται για τη διάρκεια της άρσης του απορρήτου των παρελθοντικών στοιχείων αποκλειστικά με βάση τα δεδομένα της δικογραφίας, έχοντας εποπτεία και γνώση από αυτήν του αναγκαίου συνολικού χρονικού διαστήματος της άρσης του απορρήτου.*». Ενόψει, ωστόσο, του γεγονότος ότι η, κατά τα ανωτέρω, κρίση του Δικαστηρίου θα οδηγούσε στην έκδοση αποφάσεως αντίθετης προς τις υπ' αριθ. 4/2024 και 5/2024 αποφάσεις της Ποινικής Ολομέλειας του ΑΠ, με τις οποίες έγινε δεκτό, ότι στο απόρρητο των επικοινωνιών υπάγεται το σύνολο των στοιχείων επικοινωνίας (περιεχόμενο και μεταδεδομένα), τα οποία εμπεριέχονται στον ψηφιακό εξοπλισμό των χρηστών αυτού, που διερευνώνται από τις δικαστικές και εισαγγελικές αρχές, με συνέπεια να απαιτείται για την άρση του η τήρηση των σχετικών διατάξεων του άρθρου 5 του προϊσχύσαντος Ν. 2225/1994 και ήδη του άρθρου 8 του Ν. 5002/2022, διαδοχικά ανά δίμηνο, για συνολικό χρονικό διάστημα δώδεκα (12) μηνών κατά τον Ν. 2225/1994 και δέκα (10) μηνών κατά τον Ν. 5002/2022, το ΣΤ' Ποινικό Τμήμα, παρέπεμψε την υπόθεση προς επίλυση στην Πλήρη Ολομέλεια του Αρείου Πάγου, η κρίση της οποίας μέχρι σήμερα εκκρεμεί.

[39] Βενιζέλος Ε., ο.π. σελ. 897.

Η προσθήκη του επιρρήματος «***απολύτως***» ***στον όρο*** «***απαραβίαστο***» ενδεικνύει την κατηγορηματική απαγόρευση κάθε μορφής παραβιάσεως του απορρήτου των επικοινωνιών, ενόψει και του υψηλού δείκτη διακινδύνευσής του, αλλά και τον διευρυμένο κύκλο των φορέων και των αποδεκτών του δικαιώματος, αποτελώντας έρεισμα, για την θεώρηση του τεκμηρίου υπέρ του απορρήτου της επικοινωνίας.

Από την διατύπωση ακόμη, του συντακτικού νομοθέτη, αναδεικνύεται αναμφίβολα η αμυντική πτυχή της προστασίας του απορρήτου, συνιστάμενη στην απαγόρευση των παραβιάσεων, ήτοι πράξεων με τις οποίες τρίτος επιτυγχάνει να παρέμβει στην επικοινωνία, έτσι ώστε ο ίδιος ή έτερο πρόσωπο να λάβει γνώση του διαβιβαζόμενου μηνύματος, χωρίς την βούληση των επικοινωνούντων[40]. Υπό το πρίσμα αυτό, δεν νοείται παραβίαση του απορρήτου της επικοινωνίας από επικοινωνούντα, ενόψει του γεγονότος ότι απόρρητο δεν υφίσταται έναντι του επικοινωνούντος και η συνταγματική απαγόρευση αναφέρεται σε τρίτους, ενώ ακόμη, δεν συνιστά παράβαση η λήψη γνώσεως του μηνύματος μετά το χρονικό σημείο λήξης του απορρήτου. Σημειωτέον δε, ότι η χρονική έκταση της προστασίας, είναι άρρηκτα συνδεδεμένη με το εκάστοτε μέσο επικοινωνίας. Έτσι, επί τηλεφωνικής επικοινωνίας το απόρρητο εκτείνεται και μετά το τέλος της επικοινωνίας, εν αντιθέσει με την περίπτωση των ηλεκτρονικών μηνυμάτων, όπου η προστασία του απορρήτου λήγει μόλις ο παραλήπτης λάβει γνώση του περιεχομένου του μηνύματος[41]. Εφόσον αυτά διατηρηθούν σε έντυπη μορφή ή σε ηλεκτρονική συσκευή, χωρίς την χρήση κωδικού πρόσβασης, προστατεύονται, με βάση τις διατάξεις των άρθρων 9 και 9Α του Συντάγματος[42].

Εκτός της αμυντικής διάστασης, το επικοινωνιακό απόρρητο ενέχει θετική και ενεργητική – πολιτική διάσταση. Η πρώτη συνίσταται στην υποχρέωση της Πολιτείας να λαμβάνει θετικά μέτρα για την προστασία της, ενώ η δεύτερη αντικατοπτρίζει την σπουδαιότητα του απορρήτου των επικοινωνιών για θεμελιώδεις αξίες του δημοκρατικού πολιτεύματος[43].

---

[40] Παπαδόπουλος Ν. (2017), «*Ερμηνεία Άρθρου 19 Σ.*», σε Φ. Σπυρόπουλο/Ξ. Κοντιάδη/Χ. Ανθόπουλο/ Γ. Γεραπετρίτη, *Σύνταγμα, Κατ᾽ άρθρο ερμηνεία*, Εκδόσεις Σάκκουλα, σελ. 480.
[41] Δαγτόγλου Π. (2012), «*Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα*», Εκδόσεις Σάκκουλα, σελ. 357.
[42] ΟλΑΠ 1/2017.
[43] Βενιζέλος Ε., ο.π. σελ. 901.

2.1.2 Φορείς και Αποδέκτες του Δικαιώματος

Φορείς του δικαιώματος στο επικοινωνιακό απόρρητο, όπως προκύπτει και από την εμφατική διατύπωση του συντακτικού νομοθέτη, είναι κάθε φυσικό πρόσωπο, ανεξαρτήτως εθνικότητας ή χωρικής εκτάσεως της επικοινωνίας εντός ή εκτός Ελληνικής Επικράτειας, αλλά και τα Νομικά Πρόσωπα Ιδιωτικού και Δημοσίου Δικαίου, τα τελευταία δε, στο μέτρο που δύνανται να θεωρηθούν ως φορείς συνταγματικών δικαιωμάτων (λ.χ. στις περιπτώσεις αυτοδιοίκητου, ήτοι σε ανώτατα εκπαιδευτικά ιδρύματα ή ΟΤΑ). Πρόκειται για δικαίωμα που ισχύει υπέρ όλων και έναντι όλων[44].

Αποδέκτης του δικαιώματος, όμως δεν είναι μόνο το Κράτος, καθώς έχει πάψει να διατηρεί το μονοπώλιο των επικοινωνιών, μεγάλος μέρος των οποίων παρέχεται πλέον από ιδιώτες. Έτσι το δικαίωμα του επικοινωνιακού απορρήτου τριτενεργεί, κατ' άρθρο 25 παρ. 1 εδ. γ' Σ.

2.1.3 Η Εθνική Ασφάλεια και η Διακρίβωση Ιδιαίτερα Σοβαρών Εγκλημάτων ως Περιορισμοί του Δικαιώματος

Ο απόλυτος χαρακτήρας της προστασίας του δικαιώματος στο απόρρητο των επικοινωνιών, κάμπτεται στις, περιοριστικά αναφερόμενες από τον ίδιο τον συντακτικό νομοθέτη, περιπτώσεις, ήτοι: α) για λόγους εθνικής ασφάλειας και β) για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Έτσι στον κοινό νομοθέτη εναπόκειται, με, εκτελεστικό του άρθρου 19 Σ., νόμο, ο προσδιορισμός των εγγυήσεων, υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο των επικοινωνιών, εφόσον, όμως, συντρέχει μια εκ των ανωτέρω περιπτώσεων (υπό στοιχεία α) και β)).

Από την γραμματική διατύπωση του β' εδαφίου της παρ. 1 του άρθρου 19 Σ., συνάγεται ότι, για την άρση του επικοινωνιακού απορρήτου, απαιτείται προηγούμενη εντολή δικαστικού λειτουργού, καθώς και ότι ο εκτελεστικός νόμος θα πρέπει να καθορίζει με ακρίβεια και σαφήνεια τη διαδικασία άρσης του απορρήτου, πάντοτε με σεβασμό στις Αρχές της αναλογικότητας και της μη προσβολής του πυρήνα του δικαιώματος[45].

---

[44] Παπαδόπουλος Ν., ο.π., σελ. 481.

[45] Χρυσόγονος Κ./Βλαχόπουλος Σ. (2017), «*Ατομικά και Κοινωνικά Δικαιώματα*», 4η αναθεωρημένη έκδοση, Εκδόσεις Νομική Βιβλιοθήκη, σελ. 302.

Καθίσταται σαφές, ότι οι εξαιρέσεις της εθνικής ασφάλειας και της διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων, ενέχουν τον κίνδυνο αυθαίρετης και καταχρηστικής ερμηνείας και εφαρμογής. Ιδίως η έννοια της εθνικής ασφάλειας παραμένει εξαιρετικά αόριστη και ασαφής και ο κίνδυνος κατάχρησής της ορατός, δεδομένου ότι η άρση απορρήτου, που διενεργείται εκ του λόγου τούτου, βασίζεται σε άκρως απόρρητα στοιχεία, των οποίων η ακεραιότητα και αξιοπιστία είναι δυσχερές να εξασφαλιστεί.

Κατά την παρ. 2 του άρθρου 8 της ΕΣΔΑ, περιορισμός του δικαιώματος στον ιδιωτικό βίο, δικαιολογείται, κατόπιν νομοθετικής πρόβλεψης, στο μέτρο, που σε μια δημοκρατική κοινωνία, *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».* Διαπιστώνει κανείς, ότι εν προκειμένω, η έννοια της εθνικής ασφάλειας συγκεκριμενοποιείται σε μεγαλύτερο βαθμό από ό,τι στην εθνική έννομη τάξη, όπου ο ορισμός της έννοιας της εθνικής ασφάλειας δεν έχει παγιωθεί και γίνεται δεκτό ότι σχετίζεται με την προάσπιση της Χώρας από εξωτερικές απειλές και σε καμία περίπτωση με την δημόσια ασφάλεια[46]. Έτσι, *«ο πυρήνας της εθνικής ασφάλειας συνάπτεται με την υπόσταση του κράτους στις εξωτερικές του σχέσεις. Από την πλευρά αυτή, η εθνική ασφάλεια διακρίνεται δίχως άλλο από την δημόσια ασφάλεια, που αφορά την προστασία του πολιτεύματος, των συντεταγμένων εξουσιών και των κρατικών οργάνων γενικότερα από εσωτερικές απειλές, αλλά και από την δημόσια τάξη που αποβλέποντας στο έννομο αγαθό της "κοινής ειρήνης", επιδιώκει πρώτιστα την προάσπιση της ιδιωτικής παρά της πολιτικής κοινωνίας [...] η εθνική ασφάλεια, ως έννομο αγαθό, συνδέεται και με την προστασία των ενόπλων δυνάμεων, πιθανώς των σωμάτων ασφαλείας, καθώς και των πολιτικών υπηρεσιών (αντικατασκοπείας και πληροφοριών εν γένει), που έχουν ως κύρια αποστολή την προάσπισή της, και οι οποίες είναι ασφαλώς δυνατό να απειληθούν και έσωθεν. Στο σημείο ακριβώς αυτό βρίσκεται η ομοιότητά της εθνικής με τη δημόσια ασφάλεια [...]»*[47]

---

[46] Τσίρης Π. (2002), «*Η συνταγματική κατοχύρωση του δικαιώματος του απορρήτου των επικοινωνιών*», Εκδόσεις Αντ. Ν. Σάκκουλα, σελ. 110 επ.

[47] Αλιβιζάτος Ν. (1987), «*Η συνταγματική θέση των ενόπλων δυνάμεων, Ι. Η αρχή του πολιτικού ελέγχου*», Εκδόσεις Αντ. Ν. Σάκκουλα, σελ. 199 επ.

Ήδη, σύμφωνα με το άρθρο 3 στοιχ. α' του Ν. 5002/2022[48], σε μια προσπάθεια αποκρυστάλλωσης της έννοιας, «*Λόγοι εθνικής ασφάλειας είναι οι λόγοι που συνάπτονται 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*». Πρόκειται για ενδεικτική απαρίθμηση των λόγων εθνικής ασφάλειας, μιας και η εξαντλητική αναφορά αυτών, καθίσταται πρακτικά αδύνατη, από την άλλη, παραμένει ο ασαφής χαρακτήρας της έννοιας. Αξιοσημείωτο είναι ότι, προκειμένου να προσδιοριστεί η έννοια της εθνικής ασφάλειας, *χρησιμοποιούνται πρόσθετες αόριστες νομικές έννοιες (βασικές λειτουργίες του κράτους, θεμελιώδη συμφέροντα των Ελλήνων πολιτών) ή αναφέρονται απλώς τομείς της κρατικής δράσης (εθνική άμυνα, εξωτερική πολιτική, ενεργειακή ασφάλεια κυβερνοασφάλεια), χωρίς ειδικότερο προσδιορισμό και διευκρινίσεις, με αποτέλεσμα να περιπλέκεται έτι περισσότερο το ζήτημα, αντί να περιορίζεται. Είναι, πάντως, θετικό ότι ο προσδιορισμός των πεδίων της κρατικής δράσης γίνεται με αναφορά σε εξωτερικές και όχι αμιγώς εσωτερικές καταστάσεις του κράτους*[49].

Ομοίως αόριστη κρίνεται και η έννοια των «ιδιαίτερα σοβαρών εγκλημάτων», η οποία σε κάθε περίπτωση είναι στενότερη της έννοιας του κακουργήματος. Η λίστα των αδικημάτων, για τα οποία είναι επιτρεπτή η άρση του απορρήτου έχει κατ' επανάληψη τροποποιηθεί. Έτσι, σύμφωνα με τη διάταξη του άρθρου 6 του Ν. 5002/2022, η άρση του επικοινωνιακού απορρήτου, εκτός από συγκεκριμένα κακουργήματα, προβλέπεται και για την διακρίβωση ορισμένων πλημμελημάτων, γεγονός το οποίο θέτει κρίσιμους προβληματισμούς, κατά πόσον τα, εν λόγω, πλημμεληματικού χαρακτήρα αδικήματα, δύνανται να χαρακτηριστούν ως ιδιαίτερα σοβαρά αδικήματα, με συνέπεια να τίθεται εν αμφιβόλω η πλήρωση του κριτηρίου του «ποιοτικού νόμου», που θέτει η Νομολογία του ΕΔΔΑ, σύμφωνα με την οποία το εθνικό δίκαιο θα πρέπει όχι απλώς να εγγυάται την προσβασιμότητα και την προβλεψιμότητα κατά την εφαρμογή του, αλλά θα πρέπει να εξασφαλίσει ότι τα μέτρα παρακολούθησης επιβάλλονται μόνο, όταν αυτό κρίνεται αναγκαίο σε μια δημοκρατική κοινωνία, με επαρκείς και αποτελεσματικές εγγυήσεις

[48] Ν. 5002/2022, ΦΕΚ Α' 228/ 9.12.2022. Διαθέσιμος σε: https://search.et.gr/el/fek/?fekId=554496.

[49] Μαντζούφας Π. (21.9.2024), «*Το συνταγματικό πλαίσιο του δικαιώματος επικοινωνίας και οι προϋποθέσεις άρσης του απορρήτου για λόγους εθνικής ασφάλειας*». Διαθέσιμο στο: https://www.constitutionalism.gr/to-sintagmatiko-plaisio-tou-dikaiomatos-epikoinonias/. [Ημ. Πρόσβασης 10.8.2025]

κατά της κατάχρησης του νόμου από την κρατική εξουσία[50]. Στην πράξη, με τον Ν. 5002/2022 διευρύνθηκε σημαντικά, σε σύγκριση με τον Ν. 2225/1994, ο κύκλος των αδικημάτων, για την διακρίβωση των οποίων είναι επιτρεπτός ο περιορισμός του δικαιώματος στο επικοινωνιακό απόρρητο, με συνέπεια η εξαίρεση να αποτελεί σχεδόν τον κανόνα.

2.1.4 Η Ανεξάρτητη Αρχή Διασφάλισης Απορρήτου Επικοινωνιών

Η συνταγματική πρόβλεψη Ανεξάρτητης Εποπτικής Αρχής, με έργο την διασφάλιση του επικοινωνιακού απορρήτου, στην παρ. 2 του άρθρου 19 Σ., υπαγορεύθηκε από την ανάγκη θεσμικής εγγύησης του δικαιώματος. Ο ανεξάρτητος χαρακτήρας του εποπτικού οργάνου ενισχύει την αξιοπιστία, την αντικειμενικότητα, την ακεραιότητα και την διαφάνεια της διαδικασίας άρσης απορρήτου, από τις δικαστικές αρχές, αρκεί *να διασφαλιστεί ότι το εποπτικό όργανο έχει αποτελεσματική πρόσβαση στις λεπτομέρειες των δραστηριοτήτων παρακολούθησης που έχουν αναληφθεί (Kennedy κατά Ηνωμένου Βασιλείου, 2010, § 165- Roman Zakharov κατά Ρωσίας [GC], 2015, §§ 275-285) και ότι οι εξουσίες του, σε σχέση με τις τυχόν διαπιστωθείσες παραβάσεις*[51] είναι ανάλογες και πρόσφορες να εξασφαλίσουν την αποτελεσματικότητα της δράσης του και του σκοπού του.

Η συγκρότηση και λειτουργία της Αρχής, καθορίζεται επί τη βάσει του άρθρου 101Α Σ., σύμφωνα με το οποίο απαιτείται η έκδοση οργανικού νόμου αναφορικά με την θητεία, την προσωπική και λειτουργική ανεξαρτησία των μελών της. Με τον Ν. 3115/2003 συνεστήθη η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) ως Ανεξάρτητη Αρχή. για την προστασία του σχετικού δικαιώματος και μεταξύ άλλων, προσδιορίστηκαν οι αρμοδιότητές της (άρθρο 6). Αυτές συνοπτικά διακρίνονται σε αρμοδιότητες ελέγχου, κανονιστικές, έμμεσης συμμετοχής στη διαδικασία άρσης του απορρήτου, γνωμοδοτικές, επιβολής διοικητικών κυρώσεων, εσωτερικές για την εύρυθμη λειτουργία της.

Βασική αρμοδιότητα της ΑΔΑΕ, που συνέχεται άμεσα με το αντικείμενο της παρούσας εργασίας, αποτελεί ο έλεγχος των όρων και της διαδικασίας άρσης του επικοινωνιακού απορρήτου, στο πλαίσιο του οποίου είναι δυνατή η διενέργεια, αυτεπαγγέλτως ή κατόπιν

---

[50] ΕΔΔΑ 2021, *Big Brother Watch και λοιποί κατά Ην. Βασιλείου,* §334. Διαθέσιμη στο: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}.

[51] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, §676. Διαθέσιμο σε: https://ks.echr.coe.int/web/echr-ks/article-8.

καταγγελίας, τακτικών ή έκτακτων ελέγχων εγκαταστάσεων, τεχνικού εξοπλισμού, αρχείων, βάσεων δεδομένων, εγγράφων της ΕΥΠ ή άλλων δημοσίων, αλλά και ιδιωτικών υπηρεσιών, οργανισμών και επιχειρήσεων, που δραστηριοποιούνται στον τομέα της ανταπόκρισης και επικοινωνίας. Ας σημειωθεί, βέβαια, ότι, σύμφωνα με τον Ν. 3115/2003, η, κατά τα ανωτέρω, ελεγκτική αρμοδιότητα της ΑΔΑΕ, δεν επεκτείνεται στην εξέταση της κρίσης των δικαστικών αρχών, αλλά περιορίζεται στον έλεγχο της τήρησης της νομιμότητας της διαδικασίας[52].

Ως προς τούτη την πρόβλεψη του κοινού νομοθέτη, έχουν διατυπωθεί προβληματισμοί, κατά πόσον η συγκεκριμένη ρύθμιση, απηχεί πράγματι τη βούληση του συντακτικού νομοθέτη, η δικαστική κρίση, επί τη βάσει της οποίας διετάχθη η άρση του επικοινωνιακού απορρήτου, να εξαιρεθεί του πεδίου ελέγχου της ΑΔΑΕ. Κι αυτό γιατί, οι σταθμίσεις στις οποίες προβαίνει η Εισαγγελική Αρχή πρέπει από κάπου να ελέγχονται, καθώς η αρχή της αναλογικότητας, διέπει τη δράση όλων των οργάνων, που ασκούν κρατική εξουσία και δεν νοείται στη συνταγματική τάξη να υπάρξει οποιοδήποτε όργανο, που δεν έχει κανενός είδους έλεγχο στις ενέργειές του. *«Εν ολίγοις η ΑΔΑΕ έχει επιλεγεί από τον συντακτικό νομοθέτη, με βάση την ειδικότερη διάταξη της παρ. 2 του άρθρου 19 Σ., που είναι η μόνη εφαρμοστέα στα θέματα που αφορούν τον έλεγχο της προστασίας του απορρήτου των επικοινωνιών σε όλες της τις εκφάνσεις, ως θεσμική εγγύηση, με την οποία περιβάλλεται το απόρρητο των επικοινωνιών, αλλά και ως αντίβαρο εξουσίας απέναντι και στην δικαστική αρχή, στην οποία έχει ο ίδιος αναθέσει το έργο της εκδόσεως των διατάξεων άρσης του απορρήτου, σύμφωνα με το β΄ εδάφιο της παρ. 1 του αυτού συνταγματικού άρθρου»*[53].

Ας σημειωθεί, ότι παράλληλα με την ΑΔΑΕ, και άλλες Αρχές και Φορείς, όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), το Εθνικό Συμβούλιο Ραδιοτηλεόρασης (ΕΣΡ), ο Συνήγορος του Πολίτη, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), μπορούν να επιβάλλουν κυρώσεις με βάση τα ίδια πραγματικά περιστατικά, δίχως να παραβιάζεται η αρχή ne bis in idem (σύμφωνα με την οποία κανείς δεν

---

[52] Άρ. 6 παρ. 1 περ. στ' Ν. 3115/2003.

[53] Ράμμος Χ. (2024), *«Η Αρχή Διασφαλίσεως του Απορρήτου των Επικοινωνιών (ΑΔΑΕ): Ένα θεσμικό αντίβαρο για την προστασία της πιο ευαίσθητης πτυχής του ιδιωτικού βίου, στο πλαίσιο του 5ου ετήσιου forum του Κέντρου του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης για τον Ευρωπαϊκό Νομικό Πολιτισμό, 7 και 8 Δεκεμβρίου 2023»*, στο βιβλίο *«Η ιδιωτικότητα στην ψηφιακή εποχή»*, σελ. 115 επ. Εκδόσεις Νομική Βιβλιοθήκη.

διώκεται, ούτε τιμωρείται ποινικά για αδίκημα, για το οποίο έχει ήδη καταδικαστεί ή αθωωθεί, με οριστική απόφαση Ποινικού Δικαστηρίου), δεδομένου ότι εκάστη εκ των ανωτέρω Αρχών επιβάλλει κυρώσεις για την προστασία διαφορετικών εννόμων αγαθών[54].

2.1.5 Η συνταγματική απαγόρευση χρήσεως αποδεικτικών μέσων κατά παράβαση των άρθρων 19, 9 και 9Α του Συντάγματος

Δυνάμει της παρ. 3 του άρθρου 19 Σ. εισάγεται κατά τρόπο απόλυτο, άμεση απαγόρευση της χρήσης παρανόμως κτηθέντων αποδεικτικών μέσων, όχι μόνο κατά την ποινική, πολιτική και διοικητική δίκη, αλλά και κατά την διοικητική και πειθαρχική διαδικασία. Ο σκοπός της απαγόρευσης είναι κατ' αρχήν εύλογος, κατατείνοντας στην διαφύλαξη του κύρους των αποδείξεων[55].

Ωστόσο, η κάμψη του απαγορευτικού χαρακτήρα της ανωτέρω διάταξης θεωρείται επιβεβλημένη χάριν της προστασίας συνταγματικά υπέρτερων εννόμων αγαθών, όπως η ανθρώπινη ζωή ή αξία του ανθρώπου[56]. Έτσι, σε περίπτωση, που για την απόδειξη της αθωότητας κατηγορουμένου σε ποινική δίκη, τα μοναδικά αποδεικτικά προς τούτο μέσα, έχουν αποκτηθεί παρανόμως, προκρίνεται μια συσταλτική ερμηνεία της απαγόρευσης, που θέτει η παρ. 3 του άρθρου 19 Σ., με παράλληλη εφαρμογή της αρχής της αναλογικότητας[57].

---

[54] ΣτΕ 715/2013, μειοψηφούσα γνώμη στην ΣτΕ 1091/2015, ΣτΕ 3473/2017. Αντίθετα, έχει κρίνει το ΕΔΔΑ (βλ. Απόφαση Engel και λοιπών κατά Κάτω Χωρών, Απόφαση Zolotukhin κατά Ρωσίας), με το επιχείρημα, ότι αποφασιστικό κριτήριο της αρχής ne bis in idem, αποτελεί η ταυτότητα των πραγματικών περιστατικών και όχι η ταυτότητα του εννόμου αγαθού, ενόψει και της φύσης της επιβληθείσας κύρωσης (αν έχει εν τοις πράγμασι ποινικό χαρακτήρα) και ανεξάρτητα από τον νομικό χαρακτηρισμό της (λ.χ. ως διοικητική) στην εθνική έννομη τάξη).

[55] Μανωλεδάκης Ι. (2005), «*Το απόρρητο του ιδιωτικού βίου και η έλλογη ποινική προστασία του*», ΠοινΔικ, σελ. 732.

[56] Σύμφωνα με την ΑΠ 1/2001: «*εξαίρεση από τον, συνταγματικής ισχύος, κανόνα της απαγορεύσεως των εν λόγω αποδεικτικών μέσων ισχύει μόνο χάριν της προστασίας συνταγματικά υπέρτερων έννομων αγαθών, όπως είναι λ.χ. η ανθρώπινη ζωή. Κάθε άλλη εξαίρεση από την ως άνω απαγόρευση, εισαγόμενη τυχόν με διάταξη κοινού νόμου, όπως είναι και ο Ποινικός Κώδικας, είναι ανίσχυρη κατά το μέτρο που υπερβαίνει το κριτήριο της προστασίας συνταγματικά υπέρτερου έννομου αγαθού*» και ΑΠ 42/2004.

[57] Κατά την ΜΠλΣαμ 634/2012: «*νόμιμα λαμβάνεται υπόψη υπέρ του κατηγορουμένου, υπό τον περιορισμό της υπό της διατάξεως του άρθρου 25 §1 εδ. δ΄ του Συντ. θεσπιζόμενης αρχής της αναλογικότητας, παρανόμως ληφθέν αποδεικτικό μέσο, όταν στη συγκεκριμένη περίπτωση, λαμβανομένης υπόψη της βαρύτητας του εγκλήματος για το οποίο κατηγορείται, το αποδεικτικό αυτό μέσο είναι αναγκαίο και πρόσφορο για την απόδειξη της αθωότητας του. Εξ άλλου, υπό τις ίδιες αυτές προϋποθέσεις θα ληφθεί υπόψη κατά του κατηγορουμένου παρανόμως αποκτηθέν αποδεικτικό μέσο, όταν αυτό αποτελεί το μοναδικό ενδεχομένως αποδεικτικό μέσο στο οποίο το θύμα δύναται να στηρίξει την καταγγελία του (ΑΠ 611/2006 με*

Εκείνο, ωστόσο, που προκαλεί έντονο προβληματισμό είναι η αυθαίρετη επιλογή του κοινού νομοθέτη να προβλέψει τον περιορισμό της, κατά τα ανωτέρω, απόλυτης απαγόρευσης, με σκοπό την διακρίβωση σοβαρών εγκλημάτων, όπως κακουργηματικής φοροδιαφυγής ή διαφθοράς σε βάρος του Ελληνικού Δημοσίου, σύμφωνα με το άρθρο 65 του Ν. 4356/2015. Κατά την, εν λόγω, διάταξη: *«1. Στις περιπτώσεις πράξεων κακουργηματικού χαρακτήρα, που υπάγονται στην αρμοδιότητα του Εισαγγελέα Οικονομικού Εγκλήματος ή του Εισαγγελέα Εγκλημάτων Διαφθοράς, δεν εφαρμόζεται η παράγραφος 2 του άρθρου 177 του Κώδικα Ποινικής Δικονομίας, εφόσον το αποδεικτικό μέσο αφορά πληροφορίες ή στοιχεία, στα οποία οι ανωτέρω εισαγγελείς έχουν δικαίωμα πρόσβασης κατά τις διατάξεις του άρθρου 17Α παρ. 8 εδάφιο α΄ του ν. 2523/1997 και του άρθρου 2 παρ. 5 εδάφιο α΄ του ν. 4022/2011.*

2. Η χρήση του παραπάνω αποδεικτικού μέσου κατά την παραπομπή και τη δίκη γίνεται δεκτή εφόσον κριθεί αιτιολογημένα ότι: α) η βλάβη που προκαλείται με την κτήση του είναι σημαντικά κατώτερη κατά το είδος, τη σπουδαιότητα και την έκταση από τη βλάβη ή τον κίνδυνο που προκάλεσε η ερευνώμενη πράξη, β) η απόδειξη της αλήθειας θα ήταν διαφορετικά αδύνατη και γ) η πράξη με την οποία το αποδεικτικό μέσο αποκτήθηκε δεν προσβάλλει την ανθρώπινη αξία.»

Η, ως άνω, διάταξη, η οποία συνιστά τυπικό νόμο, έρχεται σε πλήρη αντίθεση με την, αυξημένης τυπικής ισχύος, συνταγματική πρόβλεψη της παρ. 3 του άρθρου 19 Σ., συνιστώσα μη αποδεκτή νομικά, ιδιαίτερη μεταχείριση ορισμένων αδικημάτων.

2.2 Ο Νόμος 5002/2022

2.2.1 Ιστορική Εξέλιξη

Το νομοθετικό πλαίσιο της διαδικασίας άρσης του επικοινωνιακού απορρήτου εισήχθη αρχικώς με την θέση σε ισχύ του Ν. 2225/1994[58] για την προστασία της ελευθερίας και ανταπόκρισης και επικοινωνίας και άλλες διατάξεις και εν συνεχεία με τον Ν. 3115/2003[59],

σύμφωνη αγόρευση του Αντεισαγγελέα Α. Ζύγουρα ΠοινΔικ 2006, 857, ΝοΒ 2007, 150, ΠοινΧρ 2007, 895, Δ 2006, 927, Α. Ζύγουρας, ό.π., σελ. 1014,ΔιατΕισΕφΠειρ 110/2009 ΠοινΔνη 2010.1299, 2011.328 με παρατηρήσεις Γ. Μπουρμά).»

[58] Ν. 2225/1994 ΦΕΚ Α' 121/20.7.1994. Διαθέσιμος στο: https://search.et.gr/el/search-legislation/?legislationNumber=2225&selectYear=1994.

[59] Ν. 3115/2003 ΦΕΚ Α' 47/27.2.2003. Διαθέσιμος στο: https://search.et.gr/el/search-legislation/?legislationNumber=3115&selectYear=2003.

δυνάμει του οποίου προβλέφθηκε η ίδρυση της Ανεξάρτητης Αρχής Διασφάλισης Απορρήτου Επικοινωνιών και το Π.Δ. 47/2005[60] σχετικά με τις διαδικασίες, καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και την διασφάλιση του.

Ωστόσο, η, με αλματώδεις ρυθμούς, τεχνολογική πρόοδος, σε συνδυασμό με την αποκάλυψη του σκανδάλου παρακολούθησης του προέδρου πολιτικού κόμματος, δημοσιογράφων και άλλων πολιτών, μέσω κακόβουλου λογισμικού, κατέστησαν επιτακτική την ανάγκη επικαιροποίησης του κανονιστικού πλαισίου για την άρση του επικοινωνιακού απορρήτου, καθώς ο προϊσχύσας Νόμος αδυνατούσε να ανταποκριθεί στις σύγχρονες προκλήσεις.

2.2.2 Περιεχόμενο του Νόμου

Όπως, ήδη, εκτέθηκε ανωτέρω, ο νέος Νόμος διακρίνει τις περιπτώσεις άρσης απορρήτου, για λόγους εθνικής ασφάλειας (άρθρα 4 - 5) και για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων (άρθρα 6-8), προβλέποντας τα στάδια της διαδικασίας για κάθε μια εκ των περιπτώσεων αυτών.

Ειδικότερα, για την άρση απορρήτου, για λόγους εθνικής ασφάλειας, απαιτείται διάταξη του Εισαγγελικού Λειτουργού, που είναι αποσπασμένος στην Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ) και την Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας της Ελληνικής Αστυνομίας (ΔΑΕΕΒ), η οποία εκδίδεται κατόπιν σχετικού αιτήματος αποκλειστικά ενός εκ των δύο, ως άνω, Υπηρεσιών. Αξιοπρόσεκτο είναι το γεγονός, ότι η διάταξη του ανωτέρω Εισαγγελέα υποβάλλεται προς έγκριση και σε δεύτερο Εισαγγελικό Λειτουργό (Αντιεισαγγελέα του Αρείου Πάγου ή Εισαγγελέα Εφετών), μετά την έγκριση του οποίου εκκινεί η ισχύς της διατάξεως. Η συγκεκριμένη νομοθετική πρόβλεψη ετέθη προφανώς προς διασφάλιση της αντικειμενικότητας και της νομιμότητας της σχετικής εισαγγελικής διάταξης, η οποία θα ετίθετο υπό αμφισβήτηση, αν αρκούσε, για την άρση του απορρήτου για λόγους εθνικής ασφάλειας η κρίση ενός μονοπρόσωπου οργάνου και μάλιστα όχι ανεξάρτητου, αλλά ενσωματωμένου στις Υπηρεσίες που υποβάλλουν το αίτημα άρσης.

---

[60] Π.Δ. 47/2005 ΦΕΚ Α' 64/10.3.2005. Διαθέσιμο στο: https://search.et.gr/el/search-legislation/?legislationNumber=47&selectYear=2005.

Από την άλλη, επί ιδιαίτερα σοβαρών εγκλημάτων, η άρση του απορρήτου λαμβάνει χώρα κατόπιν ειδικά αιτιολογημένου βουλεύματος του αρμοδίου Δικαστικού Συμβουλίου, μετά από πρόταση του Εισαγγελέα, ενώ σε εξαιρετικά επείγουσες περιστάσεις την άρση μπορεί να διατάξει ο Εισαγγελέας ή ο Ανακριτής, οπότε υποχρεούνται εντός προθεσμίας τριών (3) ημερών να εισάγουν το ζήτημα στο αρμόδιο Δικαστικό Συμβούλιο, ώστε να ελεγχθεί η συνδρομή των εξαιρετικά επειγουσών περιστάσεων, ειδάλλως η ισχύς της διάταξης αίρεται αυτοδικαίως. Αν εντός ευλόγου χρόνου, που δεν μπορεί να υπερβαίνει τις πέντε (5) ημέρες συνολικά, δεν εκδοθεί βούλευμα, τα ευρήματα δεν είναι αξιοποιήσιμα.

Με τις ανωτέρω διατάξεις προβλέπονται ακόμη, μεταξύ άλλων, το περιεχόμενο των αιτημάτων και των σχετικών εισαγγελικών διατάξεων, καθώς και οι προϋποθέσεις γνωστοποίησης της επιβολής του μέτρου της άρσης. Πιο συγκεκριμένα, στην περίπτωση συνδρομής λόγων εθνικής ασφαλείας, η γνωστοποίηση πραγματοποιείται μετά την πάροδο τριών (3) ετών από την παύση της ισχύος της διάταξης, υπό την προϋπόθεση ότι δεν διακυβεύεται ο σκοπός για τον οποίο διετάχθη το μέτρο, ύστερα από αίτημα της ΑΔΑΕ, προς την ΕΥΠ και την ΔΑΕΕΒ. Επί του αιτήματος αποφαίνεται τριμελές όργανο, αποτελούμενο από εισαγγελικό λειτουργό της ΕΥΠ ή της ΔΑΕΕΒ, τον δεύτερο εισαγγελικό λειτουργό που εγκρίνει την διάταξη και τον Πρόεδρο της ΑΔΑΕ, προεδρεύοντος του ανώτερου ιεραρχικά ή αρχαιότερου εισαγγελικού λειτουργού.

Αναφορικά με την περίπτωση άρσης του επικοινωνιακού απορρήτου, για λόγους διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων, η γνωστοποίηση επιβολής του μέτρου πραγματοποιείται από την ΑΔΑΕ, μετά τη λήξη ισχύος του, και κατόπιν υποβολής σχετικού αιτήματος από τον θιγόμενο, εντός προθεσμίας εξήντα (60) ημερών, με τη σύμφωνη γνώμη του Εισαγγελέα του Αρείου Πάγου και υπό την προϋπόθεση ότι δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε.

Στον απόηχο του σκανδάλου παρακολούθησης αρχηγού αντιπολιτευόμενου κόμματος[61], δυνάμει της παρ. 3 του άρθρου 4 του, ως άνω, Νόμου, καθορίστηκε η διαδικασία άρσης του επικοινωνιακού απορρήτου πολιτικών προσώπων για λόγους εθνικής ασφάλειας, προβλέποντας ο νομοθέτης πρόσθετες εγγυήσεις, υπό τον φόβο στοχοποίησης πολιτικών

[61] Βλ. παρακάτω, ενότητα 5, σχετικά με το σκάνδαλο των υποκλοπών στην Ελλάδα.

προσώπων, μέσω της καταχρηστικής εφαρμογής μέτρων επιτήρησης εκ μέρους της ΕΥΠ[62]. Μεταξύ των πρόσθετων αυτών εγγυήσεων, περιλαμβάνεται: α) η δυνατότητα υποβολής αιτήματος για άρση του απορρήτου, αποκλειστικά και μόνο εκ μέρους της ΕΥΠ, με βάση συγκεκριμένα στοιχεία που καθιστούν άμεση και εξαιρετικά πιθανή την διακινδύνευση της εθνικής ασφάλειας και β) η υποβολή του σχετικού αιτήματος στον Πρόεδρο της Βουλής (ή κατά περίπτωση στον Πρόεδρο της τελευταίας Βουλής ή στον Πρωθυπουργό) προς παροχή σχετικής άδειας εντός 24 ωρών. Ωστόσο, η συγκεκριμένη νομοθετική πρόβλεψη εγείρει σοβαρά ζητήματα αμεροληψίας, δεδομένου ότι το όργανο, που αποφαίνεται για την παροχή άδειας επί αιτήματος άρσης του επικοινωνιακού απορρήτου πολιτικού προσώπου (κατά κανόνα ο Πρόεδρος της Βουλής), εκτός από μονοπρόσωπο, προέρχεται από την κυβερνητική πλειοψηφία.

Με τον ίδιο Νόμο, περαιτέρω, τροποποιήθηκαν τα άρθρα 370Α και 370Ε Π.Κ., προστέθηκε το άρθρο 370ΣΤ Π.Κ. για την διακίνηση λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων, παράλληλα προβλέφθηκε η σύσταση Επιτροπής Συντονισμού για θέματα Κυβερνοασφάλειας και τέλος τροποποιήθηκαν διατάξεις του Ν. 4624/2019[63].

2.2.3 Κριτική Θεώρηση του Νόμου και Προβληματισμοί

Παρά την προσπάθεια του νομοθέτη να παράσχει τις αναγκαίες εγγυήσεις, υπό τις οποίες δύναται να περιοριστεί το απόλυτο δικαίωμα του επικοινωνιακού απορρήτου, και μάλιστα σε μια εποχή, που η προστασία του δικαιώματος καθίσταται εξαιρετικά επισφαλής, λόγω των ραγδαίων τεχνολογικών εξελίξεων, αρκετές από τις προβλέψεις του, κρίνονται προβληματικές.

Η μη συμπερίληψη της αιτιολογίας, ως απαραίτητο στοιχείο του περιεχομένου της εισαγγελικής διάταξης, που επιβάλλει το μέτρο της άρσης του απορρήτου για λόγους εθνικής ασφάλειας, συνιστά ουσιώδη παράλειψη, εκ μέρους του νομοθέτη. Η αιτιολογία της σχετικής εισαγγελικής διατάξεως συνέχεται άμεσα με το Κράτος Δικαίου και αποτελεί ένδειξη στάθμισης, εκ μέρους της Δικαστικής Αρχής, των εννόμων αγαθών της εθνικής ασφάλειας και

---

[62] Σημειωτέον, με τον Ν. 4622/2019 (ΦΕΚ Α' 133/7.8.2019), η ΕΥΠ ετέθη υπό την άμεση εποπτεία του Πρωθυπουργού και υπό την ευθύνη του Γ.Γ. του Πρωθυπουργού.

[63] Ν. 4624/2019 (ΦΕΚ Α' 137/29.8.2019). Διαθέσιμος σε: https://search.et.gr/el/search-legislation/?legislationNumber=4624&selectYear=2019.

του δικαιώματος στο επικοινωνιακό απόρρητο, ώστε να διαπιστωθεί αν και σε ποιο βαθμό, ο εισαγγελικός λειτουργός εφάρμοσε την αρχή της αναλογικότητας[64]. Έτσι, η παράλειψη αναφοράς αιτιολογίας καθιστά αδύνατο τον έλεγχο της εισαγγελικής κρίσης και ειδικότερα, ότι δεν εμφιλοχώρησε υπέρβαση των ακραίων ορίων της διακριτικής ευχέρειας του εισαγγελικού λειτουργού, κατά την, εκ μέρους του, ερμηνεία της νομικής έννοιας της εθνικής ασφάλειας[65]. Είναι άλλο το ζήτημα της δημοσιοποίησης της αιτιολογίας της εισαγγελικής διάταξης, και εντελώς διαφορετικό η συμπερίληψη αυτής στο σώμα της διατάξεως, ώστε να καθίσταται δυνητικός ο έλεγχος της νομιμότητάς της. Η αιτιολογία θα πρέπει, σε κάθε περίπτωση, να είναι ειδική και εμπεριστατωμένη, αναλύοντας συγκεκριμένα πραγματικά περιστατικά της διερευνώμενης υπόθεσης, κατά τρόπο, που να καθίστανται σαφείς οι λόγοι για τους οποίους αφενός υπήρξε αναπόφευκτη η προσφυγή στο μέτρο, αφετέρου κρίθηκε αναποτελεσματική η χρήση ηπιότερων μέσων, μετά και την δέουσα εφαρμογή της Αρχής της αναλογικότητας.

Ζήτημα αντικειμενικότητας και αμεροληψίας, περαιτέρω, θέτει η πρόβλεψη του νομοθέτη, για την γνωστοποίηση επιβολής του μέτρου για λόγους εθνικής ασφάλειας, μετά την πάροδο τριών (3) ετών από την παύση της ισχύος του, κατόπιν απόφασης ενός τριμελούς οργάνου (αρμοδιότητα η οποία ανήκε στην ΑΔΑΕ και αφαιρέθηκε), απαρτιζόμενου από τρία μέλη, εκ των οποίων τα δύο (ήτοι οι δύο εισαγγελικοί λειτουργοί) έχουν κατ' ουσίαν ήδη εκφραστεί για την εφαρμογή του μέτρου και κατά συνέπεια, ευλόγως η κρίση τους εγείρει

---

[64] Αξιοσημείωτη η απόφαση του ΔΕΕ (C-349/21), σύμφωνα με την οποία δεν αντιτίθεται στην ευρωπαϊκή έννομη τάξη (αρ. 15 παρ. 1 Οδηγίας 2002/58/ΕΚ και αρ. 47 ΧΘΔΕΕ) «*η εθνική πρακτική σύμφωνα με την οποία οι δικαστικές αποφάσεις με τις οποίες χορηγείται άδεια για τη χρήση ειδικών μεθόδων συλλογής πληροφοριών, κατόπιν αιτιολογημένου και εμπεριστατωμένου αιτήματος των ποινικών αρχών, καταρτίζονται βάσει τυποποιημένου κειμένου χωρίς εξατομικευμένη αιτιολογία, όπου απλώς αναγράφεται, πέραν της χρονικής διάρκειας ισχύος των αδειών, ότι έχουν τηρηθεί οι προβλεπόμενες από τη νομοθεσία απαιτήσεις, περί των οποίων γίνεται λόγος στις αποφάσεις αυτές, υπό την προϋπόθεση ότι οι συγκεκριμένοι λόγοι βάσει των οποίων ο αρμόδιος δικαστής έκρινε ότι τηρούνταν οι προϋποθέσεις του νόμου, υπό το πρίσμα των πραγματικών και νομικών στοιχείων που χαρακτηρίζουν την προκειμένη περίπτωση, μπορούν να συναχθούν ευχερώς και επακριβώς από μια συνδυασμένη ανάγνωση της αποφάσεως και της αιτήσεως περί χορηγήσεως αδείας και υπό την προϋπόθεση ότι, μετά τη χορήγηση της άδειας, παρέχεται στο πρόσωπο εις βάρος του οποίου επετράπη η χρήση ειδικών μεθόδων συλλογής πληροφοριών, πρόσβαση στην αρχική αίτηση.*»

[65] ΟΛΑΔΑΕ (2022), «*Παρατηρήσεις της Ολομέλειας της ΑΔΑΕ επί του νομοσχεδίου για την διαδικασία άρσης του απορρήτου των επικοινωνιών, την κυβερνοασφάλεια και την προστασία των προσωπικών δεδομένων*», Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης, σελ. 2. Διαθέσιμο στο: https://www.constitutionalism.gr/paratiriseis-tis-olomeleias-tis-adae-epi-tou-nomosxediou-gia-tin-arsi-tou-aporitoy-ton-sinomilion/. [Ημ. Πρόσβασης 10.8.2025]

σοβαρές αμφιβολίες ως προς την αντικειμενικότητα και την ανεξαρτησία τους. Ακόμη, η διάρκεια των τριών (3) ετών, που θα πρέπει να παρέλθουν από την παύση της ισχύος του μέτρου, προκειμένου να επιτραπεί η γνωστοποίησή του, κρίνεται ιδιαίτερα μεγάλη και αλυσιτελής, ιδίως αν αναλογιστεί κανείς ότι ο Νόμος, θέτει ήδη ως βασική προϋπόθεση την μη διακύβευση του σκοπού του μέτρου. Γεννάται, συνεπώς, το εύλογο ερώτημα, ποιόν σκοπό εξυπηρετεί η παρέλευση τριών (3) ετών από την παύση της ισχύος του μέτρου, ως πρόσθετη προϋπόθεση ενημέρωσης του θιγόμενου, από τη στιγμή που, αν δεν πληρούται η βασική προϋπόθεση της μη διακινδύνευσης του σκοπού του μέτρου, η γνωστοποίησή του, δεν επιτρέπεται να λάβει χώρα, ακόμη και μετά την πάροδο της, κατά τα ανωτέρω, τριετίας. Στην πραγματικότητα η παρέλευση τόσο μεγάλου χρονικού διαστήματος οδηγεί αναπόφευκτα στην αποθάρρυνση του εκάστοτε υποκειμένου να ασκήσει το δικαίωμα αποτελεσματικής δικαστικής προστασίας.

Ακόμη, η ευρεία διακριτική ευχέρεια των κρατικών αρχών να παρατείνουν την διάρκεια της επιβολής του μέτρου άρσης του επικοινωνιακού απορρήτου, για λόγους εθνικής ασφάλειας, και μάλιστα για αόριστο χρονικό διάστημα, σύμφωνα με τη διάταξη της παρ. 4 του άρθρου 8 του Ν. 5002/2022[66], χαρακτηρίζεται ομοίως προβληματική και σε κάθε περίπτωση δυσανάλογα περιοριστική του δικαιώματος στο επικοινωνιακό απόρρητο, το οποίο μπορεί, δυνάμει της, εν λόγω, διατάξεως να αρθεί επ' αόριστον!

Τέλος, το γεγονός ότι δύο μονοπρόσωπα όργανα αποφαίνονται επί αιτήματος άρσης του απορρήτου για λόγους εθνικής ασφάλειας, και μάλιστα εντός ασφυκτικών χρονικών ορίων, θέτει και πάλι εν αμφιβόλω την αξιοπιστία της διαδικασίας. Και τούτο διότι, αφενός μεν, η ανεξαρτησία της κρίσης του, αποσπασμένου στην ΕΥΠ και την ΔΑΕΕΒ, Εισαγγελικού

---

[66] *«Η χρονική διάρκεια της άρσης του απορρήτου δεν μπορεί να υπερβαίνει τους δύο (2) μήνες. Παρατάσεις, οι οποίες δεν υπερβαίνουν κάθε φορά τους δύο (2) μήνες, μπορούν να διαταχθούν με τη διαδικασία, που προβλέπεται κατά περίπτωση, για την επιβολή του μέτρου και υπό τον όρο ότι εξακολουθούν να υφίστανται οι λόγοι της άρσης. Σε κάθε περίπτωση, η χρονική διάρκεια δεν μπορεί να υπερβαίνει συνολικά τους δέκα (10) μήνες. Υπέρβαση του ορίου του δευτέρου εδαφίου επιτρέπεται μόνο σε περιπτώσεις άρσης για λόγους εθνικής ασφάλειας, εφόσον στηρίζεται σε συγκεκριμένα στοιχεία που καθιστούν άμεση και εξαιρετικά πιθανή τη διακινδύνευση της εθνικής ασφάλειας και η εξακολούθηση της συνδρομής των στοιχείων αυτών επιβεβαιώνεται σε κάθε παράταση της ισχύος της άρσης. Μετά τη λήξη της διάρκειας της άρσης ή μετά τη λήξη του επιτρεπόμενου ανώτατου χρονικού ορίου της παύει αυτοδικαίως η άρση του απορρήτου. Σε κάθε περίπτωση, με διάταξη του οργάνου που επέβαλε την άρση διατάσσεται η παύση της και πριν από την πάροδο της ορισμένης διάρκειάς της, αν εκπληρώθηκε ο σκοπός ή εξέλειπαν οι λόγοι επιβολής του μέτρου.»*

Λειτουργού, λόγω της πλήρους ενσωμάτωσής του στις Υπηρεσίες αυτές, καθίσταται επισφαλής, αφετέρου δε, ο δεύτερος Εισαγγελικός Λειτουργός, καλείται επί της ουσίας να εγκρίνει ή να απορρίψει την διάταξη ενός συναδέλφου του, με όσο το δυνατόν πιο αμερόληπτο (;;;) τρόπο. Σε κάθε περίπτωση η έκδοση της διάταξης περί άρσης του απορρήτου, από το Δικαστικό Συμβούλιο (αντί των δύο εισαγγελικών λειτουργών) και για τις περιπτώσεις λόγων εθνικής ασφάλειας, (όπως ήδη προβλέπεται για την περίπτωση διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων), θα συνιστούσε σημαντική νομοθετική προσέγγιση, με θετικό πρόσημο, δοθέντος ότι το τριμελές δικαστικό όργανο εξασφαλίζει μεγαλύτερα εχέγγυα αντικειμενικότητας, αμεροληψίας και ανεξαρτησίας.

3. ΤΑ ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ ΥΠΟ ΤΟ ΠΡΙΣΜΑ ΤΟΥ ΆΡΘΡΟΥ 19 ΤΟΥ ΣΥΝΤΑΓΜΑΤΟΣ ΚΑΙ ΤΟΥ Ν. 5002/2022

Όπως θα αναλυθεί εκτενώς κατωτέρω, το ζήτημα των παρακολουθήσεων στη Χώρα μας, συντάραξε, όχι μόνο τον πολιτικό και δημοσιογραφικό κόσμο, αλλά και τους νομικούς κύκλους, δημιουργώντας εύλογες ανησυχίες για το Κράτος Δικαίου, τις αξίες και τους θεσμούς του δημοκρατικού πολιτεύματος και ανέδειξε την ανάγκη προστασίας θεμελιωδών ανθρωπίνων δικαιωμάτων (όπως το δικαίωμα στην προσωπικότητα, την ιδιωτική και οικογενειακή ζωή, η ελευθερία της έκφρασης, η ελευθερία του Τύπου κλπ.), τα οποία φαίνεται να διακυβεύτηκαν σοβαρά, από την χρήση λογισμικών κατασκοπείας.

3.1 Ο αντίκτυπος της χρήσης λογισμικών κατασκοπείας στα θεμελιώδη δικαιώματα

Ευλόγως αντιλαμβάνεται κανείς, ότι η θέση υπό επιτήρηση της επικοινωνίας, με οποιονδήποτε τρόπο, συνιστά περιορισμό της ελεύθερης άσκησης του δικαιώματος στο επικοινωνιακό απόρρητο. Η επικοινωνία σε μια τέτοια περίπτωση παύει να διεξάγεται υπό συνθήκες μυστικότητας, γεγονός το οποίο πλήττει ανεπανόρθωτα τον απαραβίαστο πυρήνα του συνταγματικού δικαιώματος. Πλην όμως, ο περιορισμός τούτος, επεκτείνεται και σε άλλα θεμελιώδη δικαιώματα και ανθρώπινες ελευθερίες, που φαίνεται να «θυσιάζονται» υπό το καθεστώς της παρακολούθησης.

3.1.1 Το δικαίωμα στον ιδιωτικό βίο

Το δικαίωμα στο επικοινωνιακό απόρρητο, όπως ήδη εκτέθηκε, δεν συνέχεται απλώς με το δικαίωμα στον ιδιωτικό βίο, αλλά αποτελεί ειδικότερη έκφανση αυτού.

Σύμφωνα με την διάταξη του άρθρου 8 της ΕΣΔΑ, «*1. Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.*

2. Δεν επιτρέπεται να υπάρξη 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.», ενώ σύμφωνα με το άρθρο 7 του ΧΘΔΕΕ, «*Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του.»*

Η κατοχύρωση του δικαιώματος στην ελληνική έννομη τάξη εισάγεται μέσω της διάταξης του άρθρου 9 του Συντάγματος, σύμφωνα με την οποία: «*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.»

Στο α' εδάφιο της παρ. 1 του άρθρου 9 Σ. προστατευόμενο έννομο αγαθό αποτελεί η κατοικία, η έννοια της οποίας δεν ταυτίζεται με αυτήν της αστικής κατοικίας, αλλά περιλαμβάνει οποιονδήποτε χώρο, κύριο ή δευτερεύοντα, περιφραγμένο, που χρησιμοποιείται για την διαβίωση του ατόμου, αλλά και την άσκηση επαγγελματικής, οικονομικής, πολιτικής ή άλλης δράσης και δεν είναι ελευθέρως προσβάσιμοι στον καθένα[67]. Υπό τον όρο άσυλο νοείται η απαγόρευση της εισόδου και παραμονής των οργάνων της δημόσιας εξουσίας στην κατοικία του ατόμου, χωρίς τη γνώση ή παρά τη θέλησή του. Έτσι, η εγκατάσταση μικροφώνου παραβιάζει το άσυλο της κατοικίας, αλλά η παρακολούθηση των συνομιλιών την ιδιωτική και οικογενειακή ζωή, κατ' άρθρο 9 παρ. 1[68]. Βέβαια, το άσυλο της κατοικίας δεν είναι απόλυτα απαραβίαστο από την κρατική εξουσία και μπορεί υπό τις συγκεκριμένες, αυστηρές προϋποθέσεις του νόμου να καμφθεί, ώστε να μην εξαιρεθεί από την αξίωση ισχύος της έννομης τάξης[69].

Περαιτέρω, ως ιδιωτική ζωή, ορίζεται η ατομική ζωή του ανθρώπου και ως οικογενειακή η ζωή του ως μέλους της οικογένειας. Αμφότερες η ιδιωτική και η οικογενειακή ζωή, συναπαρτίζουν την «σφαίρα του απορρήτου» του ατόμου, στην οποία περιλαμβάνεται η

---

[67] Μάνεσης Α. (1981), «*Ατομικές Ελευθερίες*», Εκδοτικός Οίκος Σάκκουλα, σελ. 224 και Δαγτόγλου Π. (2012), ο.π. σελ. 343.

[68] Παντελής Α. 2018), ο.π., σελ. 493.

[69] Χρυσόγονος Κ. /Βλαχόπουλος Σ. (2017), ο. π., σελ. 288.

ερωτική ζωή, τα δεδομένα υγείας, το σύνολο των ιδιωτικών του σχέσεων κλπ. Αξίζει να σημειωθεί ότι η ιδιωτική και οικογενειακή ζωή, δεν προστατεύονται μόνο στο πλαίσιο της κατοικίας, ούτε το άτομο απεκδύεται της ιδιωτικότητάς του, με την είσοδό του σε δημόσιο χώρο[70].

Η μετάβαση των σύγχρονων κοινωνιών στον ψηφιακό κόσμο, ωστόσο, καθιστά επισφαλή την ιδιωτικότητα των ατόμων. Τα λογισμικά κατασκοπείας, αποτελούν χαρακτηριστική περίπτωση, πλήρους διάβρωσης του δικαιώματος στην ιδιωτικότητα, και παρά τις εγγυήσεις των κατασκευαστριών εταιρειών, ότι σκοπός της εφαρμογής τους είναι αποκλειστικά η πρόληψη και καταπολέμηση του οργανωμένου εγκλήματος, της τρομοκρατίας και των εν γένει μορφών βίας[71], η πράξη αποδεικνύει τα ακριβώς αντίθετα. Ιδίως αν αναλογιστεί κανείς τις τεχνικές δυνατότητες δράσης των λογισμικών κατασκοπείας, κάποια εκ των οποίων δεν απαιτούν καν τη σύμπραξη του υποκειμένου (λ.χ. λογισμικό Pegasus) για να ενεργοποιηθούν και να αποκτήσουν πρόσβαση στο σύνολο των δεδομένων μιας συσκευής (μηνύματα, κλήσεις, κωδικούς πρόσβασης, αρχεία, περιεχόμενο συνομιλιών κλπ.), αντιλαμβάνεται κανείς, τον υψηλότατο βαθμό τρωτότητας της ιδιωτικής σφαίρας του ατόμου.

Ακριβώς, λόγω, του ευρύτατου περιεχομένου του δικαιώματος στον ιδιωτικό βίο και των πολλαπλών εκφάνσεών του, γίνεται αντιληπτό, ότι τα κατασκοπευτικά λογισμικά, θέτουν κρίσιμους κινδύνους για πληθώρα θεμελιωδών δικαιωμάτων, που ανάγονται στον πυρήνα της προσωπικότητας.

3.1.2 Το δικαίωμα στα προσωπικά δεδομένα

Η έννομη προστασία των δεδομένων προσωπικού χαρακτήρα επιτυγχάνεται μέσα από ένα συμπαγές κανονιστικό πλαίσιο τόσο σε εθνικό, όσο και σε ευρωπαϊκό και διεθνές επίπεδο. Έτσι, στην ελληνική έννομη τάξη, σύμφωνα με το άρθρο 9Α του Συντάγματος, «*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*

---

[70] Παναγοπούλου Φ. (2023): «*Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 9*» Σε Βλαχόπουλο Σπ., Κοντιάδη Ξ., Τασόπουλο Γ. (επιμ.), Syntagmawatch, σελ. 15. Διαθέσιμο στο: https://www.syntagmawatch.gr/wp-content/uploads/2023/02/%CE%86%CF%81%CE%B8%CF%81%CE%BF-9-me-cover.pdf. [Ημ. Πρόσβασης 10.8.2025]

[71] Παπανικολάου Α. (2022), ο.π.

διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.», ενώ ο Ν. 4624/2019, αποτελεί την πράξη ενσωμάτωσης της Ευρωπαϊκής Νομοθεσίας για τα προσωπικά δεδομένα, στη χώρα μας. Στο ευρωπαϊκό και διεθνές πεδίο, το άρθρο 8 της ΕΣΔΑ, το άρθρο 8 του ΧΘΔΕΕ[72], ο Κανονισμός 679/2016/ΕΕ (ΓΚΠΔ)[73], η Οδηγία 680/2016/ΕΕ[74], το άρθρο 17 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα (ΔΣΑΠΔ)[75], διαγράφουν το πλαίσιο προστασίας των δεδομένων προσωπικού χαρακτήρα.

Στο σημείο αυτό, κρίνεται σκόπιμο να τονιστεί ότι από την διατύπωση του συντακτικού νομοθέτη στο άρθρο 9Α Σ., διακρίνεται ο αμυντικός χαρακτήρας του δικαιώματος, υπό την έννοια της αξίωσης αποχής του Κράτους από ενέργειες, που μπορούν να προσβάλλουν το δικαίωμα, χωρίς, όμως, τούτο να συνεπάγεται ότι η προστασία των προσωπικών δεδομένων τίθεται υπό διαπραγμάτευση και εξαρτάται από την βούληση του ατόμου, στην περίπτωση που αυτό σχετίζεται με την ανθρώπινη αξία[76].

Προσωπικό δεδομένο, σύμφωνα με το άρθρο 4 του ΓΚΠΔ, είναι 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,

---

[72] *«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.»*

[73] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμος σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&qid=1694157262478.

[74] Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, 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 και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. Διαθέσιμη σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680.

[75] *«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 υπόληψης του.*

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

[76] ΑΠΔΠΧ (3.7.2001), *Υπ' αριθ. 92/2001 Απόφαση σχετικά με την τηλεοπτική εκπομπή με την ονομασία «Μεγάλος Αδερφός» (Big Brother).* Διαθέσιμη στο: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/arheio-tileoptikis-paragogis-big-brother. [Ημ. Πρόσβασης 9.8.2025]

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. Τα προσωπικά δεδομένα διακρίνονται σε απλά και ευαίσθητα. Τα τελευταία δε, εκτίθενται περιοριστικά στο άρθρο 9 παρ. 1 του ΓΚΠΔ[77].

Μοναδικές νόμιμες βάσεις επεξεργασίας των προσωπικών δεδομένων, αποτελούν οι διατάξεις των άρθρων 5 και 6 του ΓΚΠΔ.

Έτσι, αν Δημόσια Αρχή, όπως η ΕΥΠ, εφαρμόζει σύστημα παρακολούθησης, μέσω κατασκοπευτικού λογισμικού, η επεξεργασία των δεδομένων θα μπορούσε να κριθεί νόμιμη, μόνο υπό το πρίσμα της περ. ζ' της παρ. 2 του άρθρου 9 του ΓΚΠΔ, ήτοι για λόγους ουσιαστικού δημόσιου συμφέροντος. Σε μια τέτοια περίπτωση, όμως, θα πρέπει αφενός να εξεταστεί, τι λογίζεται ως «ουσιαστικό δημόσιο συμφέρον» και κατά πόσον, για την εξασφάλισή του, είναι αναγκαία η εφαρμογή του λογισμικού κατασκοπείας, τηρουμένης της Αρχής της αναλογικότητας και δίχως να προσβάλλεται ο πυρήνας θεμελιωδών δικαιωμάτων.

Από την άλλη, η χρήση λογισμικού κατασκοπείας από ιδιώτη, δεν δύναται επουδενί να δικαιολογηθεί, με βάση το άρθρο 9 του ΓΚΠΔ.

Στην περίπτωση των κατασκοπευτικών λογισμικών, η δυνατότητά τους να διεισδύουν στις ηλεκτρονικές συσκευές, αποκτώντας πρόσβαση αδιακρίτως στο σύνολο των αποθηκευμένων αρχείων τους, σε συνδυασμό με το γεγονός ότι οι «έξυπνες συσκευές» (smart phones, smart watches), διαθέτουν ευρύτατο πεδίο λειτουργιών και μπορούν να χρησιμοποιηθούν, όχι μόνο για την διεξαγωγή επικοινωνιών, αλλά και για την συλλογή, αποθήκευση και εν γένει επεξεργασία πληθώρας δεδομένων[78], καθιστά την προστασία των δεδομένων αυτών εξαιρετικά επισφαλή.

---

[77] Ως τέτοια αυτά «*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.*»

[78] Παπανικολάου Α. (2022), ο.π.

Σύμφωνα, τέλος, με την Οδηγία 680/2016/ΕΕ, οι δραστηριότητες επιβολής του νόμου εμπίπτουν στο πεδίο εφαρμογής της, το οποίο διέπει την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες Αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.

Η επεξεργασία αυτή είναι σύννομη μόνον, εάν και στον βαθμό, που είναι απαραίτητη, για την εκτέλεση καθήκοντος, που ασκείται από Αρχή αρμόδια για τους σκοπούς που προβλέπονται στο άρθρο 1 παρ. 1 και βασίζεται στο δίκαιο της Ένωσης ή των κρατών μελών. Επιπλέον, η, εν λόγω, επεξεργασία πρέπει να πληροί τις αρχές προστασίας των δεδομένων (νομιμότητα, δικαιοσύνη, ελαχιστοποίηση, ακρίβεια, ασφάλεια κ.λπ.) που αναφέρονται στο άρθρο 4 της Οδηγίας. Οι μυστικές έρευνες δεν εξαιρούνται από την Οδηγία. Ωστόσο, σύμφωνα με την αιτιολογική σκέψη 26, οι εν λόγω έρευνες μπορούν να πραγματοποιούνται μόνο εφόσον ορίζονται από τον νόμο και συνιστούν απαραίτητο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία, με δέουσα συνεκτίμηση των έννομων συμφερόντων του ενδιαφερομένου. Συνεπώς, ο Χάρτης (ΧΘΔΕΕ) — με τις προϋποθέσεις που θέτει για τον περιορισμό των θεμελιωδών δικαιωμάτων — εφαρμόζεται πλήρως στις, εν λόγω, έρευνες και στα μέτρα που τις επιτρέπουν, όπως αναφέρεται στην αιτιολογική σκέψη 46: *Κάθε περιορισμός των δικαιωμάτων του υποκειμένου των δεδομένων πρέπει να συμμορφώνεται με το Χάρτη και με την ΕΣΔΑ, όπως ερμηνεύονται από τη νομολογία του Δικαστηρίου και του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων αντίστοιχα, ιδίως δε να σέβεται την ουσία των εν λόγω δικαιωμάτων και ελευθεριών.*

Σύμφωνα με την Μελέτη του Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, αναφορικά με τον αντίκτυπο του Pegasus (λογισμικού κατασκοπείας) στα θεμελιώδη δικαιώματα και τις δημοκρατικές διαδικασίες, προκειμένου να καθοριστεί, αν η χρήση του Pegasus μπορεί να είναι σύμφωνη με την Οδηγία και με τον Χάρτη, πρέπει να εξεταστεί, αν πληρούνται όλες οι απαιτήσεις τόσο της Οδηγίας, (όσο και του Χάρτη). Το επιτρεπτό της χρήσης του Pegasus —και παρόμοιων συστημάτων παραβίασης συσκευών— για σκοπούς επιβολής του νόμου πρέπει να εξετάζεται κατά περίπτωση, λαμβάνοντας υπόψη πολλαπλούς παράγοντες: τη σοβαρότητα του εγκλήματος ή του κινδύνου για την ασφάλεια, που πρέπει να διερευνηθεί ή να προληφθεί, τους περιορισμούς

υπό τους οποίους χρησιμοποιούνται οι λειτουργίες του συστήματος και το εφαρμοστέο εθνικό δίκαιο. Ωστόσο, φαίνεται, ότι το Pegasus δεν θα ήταν πιθανό να ικανοποιήσει την απαίτηση αναγκαιότητας, τόσο βάσει της οδηγίας όσο και βάσει του Χάρτη, εφόσον υπάρχουν εναλλακτικές λύσεις που επιτυγχάνουν τους σκοπούς επιβολής του νόμου με λιγότερο παρεμβατικούς και ασφαλέστερους τρόπους.

3.1.3 Το δικαίωμα στην ελευθερία της έκφρασης και στην ελευθερία του Τύπου

Ένα ακόμη θεμελιώδες δικαίωμα, το οποίο αποδεδειγμένα, επλήγη από την παράνομη χρήση λογισμικών κατασκοπείας στη Χώρα μας, είναι αυτό της ελευθερίας της έκφρασης και της ειδικότερης έκφανσης αυτής, της ελευθερίας του Τύπου, που κατοχυρώνονται στο άρθρο 14 του Συντάγματος[79].

---

[79] *«1. Καθένας μπορεί να εκφράζει και να διαδίδει προφορικά, γραπτά και δια του τύπου τους στοχασμούς του τηρώντας τους νόμους του Κράτους.*
2. Ο τύπος είναι ελεύθερος. Η λογοκρισία και κάθε άλλο προληπτικό μέτρο απαγορεύονται. 3. Η κατάσχεση εφημερίδων και άλλων εντύπων, είτε πριν από την κυκλοφορία είτε ύστερα από αυτή, απαγορεύεται. Κατ' εξαίρεση επιτρέπεται η κατάσχεση, με παραγγελία του εισαγγελέα, μετά την κυκλοφορία: α) για προσβολή της χριστιανικής και κάθε άλλης γνωστής θρησκείας,
β) για προσβολή του προσώπου του Προέδρου της Δημοκρατίας,
γ) για δημοσίευμα που αποκαλύπτει πληροφορίες για τη σύνθεση, τον εξοπλισμό και τη διάταξη των ενόπλων δυνάμεων ή την οχύρωση της Χώρας ή που έχει σκοπό τη βίαιη ανατροπή του πολιτεύματος ή στρέφεται κατά της εδαφικής ακεραιότητας του Κράτους, δ) για άσεμνα δημοσιεύματα που προσβάλλουν ολοφάνερα τη δημόσια αιδώ, στις περιπτώσεις που ορίζει ο νόμος. 4. Σ' όλες τις περιπτώσεις της προηγούμενης παραγράφου ο εισαγγελέας, μέσα σε είκοσι τέσσερις ώρες από την κατάσχεση, οφείλει να υποβάλει την υπόθεση στο δικαστικό συμβούλιο, και αυτό, μέσα σε άλλες είκοσι τέσσερις ώρες, οφείλει να αποφασίσει για τη διατήρηση ή την άρση της κατάσχεσης, διαφορετικά η κατάσχεση αίρεται αυτοδικαίως. Τα ένδικα μέσα της έφεσης και της αναίρεσης επιτρέπονται στον εκδότη της εφημερίδας ή άλλου εντύπου που κατασχέθηκε και στον εισαγγελέα. 5. Καθένας ο οποίος θίγεται από ανακριβές δημοσίευμα ή εκπομπή έχει δικαίωμα απάντησης, το δε μέσο ενημέρωσης έχει αντιστοίχως υποχρέωση πλήρους και άμεσης επανόρθωσης. Καθένας ο οποίος θίγεται από υβριστικό ή δυσφημιστικό δημοσίευμα ή εκπομπή έχει, επίσης, δικαίωμα απάντησης, το δε μέσο ενημέρωσης έχει αντιστοίχως υποχρέωση άμεσης δημοσίευσης ή μετάδοσης της απάντησης. Νόμος ορίζει τον τρόπο με τον οποίο ασκείται το δικαίωμα απάντησης και διασφαλίζεται η πλήρης και άμεση επανόρθωση ή η δημοσίευση και μετάδοση της απάντησης.
6. Το δικαστήριο, ύστερα από τρεις τουλάχιστον καταδίκες μέσα σε μία πενταετία για διάπραξη των εγκλημάτων που προβλέπονται στην παράγραφο 3, διατάσσει την οριστική ή προσωρινή παύση της έκδοσης του εντύπου και, σε βαριές περιπτώσεις, την απαγόρευση της άσκησης του δημοσιογραφικού επαγγέλματος από το πρόσωπο που καταδικάστηκε, όπως νόμος ορίζει Η παύση ή η απαγόρευση αρχίζουν αφότου η καταδικαστική απόφαση γίνει αμετάκλητη.
7. Νόμος ορίζει τα σχετικά με την αστική και ποινική ευθύνη του τύπου και των άλλων μέσων ενημέρωσης και με την ταχεία εκδίκαση των σχετικών υποθέσεων.
8. Νόμος ορίζει τις προϋποθέσεις και τα προσόντα για την άσκηση του δημοσιογραφικού επαγγέλματος. 9. Το ιδιοκτησιακό καθεστώς, η οικονομική κατάσταση και τα μέσα χρηματοδότησης των μέσων ενημέρωσης

Η ελευθερία της έκφρασης απηχεί, κατ' αρχήν, την συμμετοχή του ατόμου στην πολιτική ζωή της Χώρας, πέρα από τον έλεγχο της κρατικής εξουσίας και κάθε είδους διώξεις. Αποτελεί αρνητικό ατομικό δικαίωμα και εμπεριέχει πληθώρα άλλων ελευθεριών, όπως η ελευθερία του Τύπου, η ελευθερία της Τέχνης, της Επιστήμης και της παιδείας, η ελευθερία θρησκευτικής συνείδησης, η ελευθερία του συνέρχεσθαι και συνεταιρίζεσθαι. Η συνταγματική διάταξη του άρθρου 14 προστατεύει την έκφραση, ανεξάρτητα από το μέσο (προφορικά, γραπτά, δια τύπου ή ακόμη και συμβολικά) των στοχασμών, έννοια που αντικατοπτρίζει οτιδήποτε δηλωτικό της διανόησης, της ψυχικής κατάστασης, του συναισθηματικού κόσμου και της συγκινησιακής φόρτισης ενός προσώπου. Σκόπιμο είναι να διευκρινιστεί ότι «*η δημόσια εξουσία είναι υπόλογη με γνώμονα το δημόσιο συμφέρον και ο τύπος επιτελεί, ως δημόσιος φύλακας, εγγυητικό ρόλο ότι η δημόσια εξουσία δεν θα καταχραστεί την νομική της υπεροχή […]. Αντίθετα με την εξουσία, το άτομο δεν καθίσταται υπόλογο για την διάδοση των στοχασμών του και το περιεχόμενό τους. Στο πλαίσιο της νομικά οριοθετημένης ελευθερίας του, δικαιούται να λέει ό,τι θέλει, ακόμη κι αν σοκάρει, ενοχλεί ή προκαλεί....*[80]»

Η ελευθερία της έκφρασης αποτελεί εγγενές στοιχείο του δημοκρατικού πολιτεύματος, επιτελούσα εγγυητική προς αυτό λειτουργία, υπό την έννοια ότι μέσω αυτής ελέγχεται η τήρηση της νομιμότητας και των επιταγών του κράτους δικαίου, ενσαρκώνεται η συμμετοχή των προσώπων στη δημοκρατική διακυβέρνηση, υλοποιείται η αμφίδρομη σχέση κυβερνώντων

πρέπει να γίνονται γνωστά, όπως νόμος ορίζει. Νόμος προβλέπει τα μέτρα και τους περιορισμούς που είναι αναγκαίοι για την πλήρη διασφάλιση της διαφάνειας και της πολυφωνίας στην ενημέρωση. Απαγορεύεται η συγκέντρωση του ελέγχου περισσότερων μέσων ενημέρωσης της αυτής ή άλλης μορφής. Απαγορεύεται ειδικότερα η συγκέντρωση περισσότερων του ενός ηλεκτρονικών μέσων ενημέρωσης της αυτής μορφής, όπως νόμος ορίζει. Η ιδιότητα του ιδιοκτήτη, του εταίρου, του βασικού μετόχου ή του διευθυντικού στελέχους επιχείρησης μέσων ενημέρωσης είναι ασυμβίβαστη με την ιδιότητα του ιδιοκτήτη, του εταίρου, του βασικού μετόχου ή του διευθυντικού στελέχους επιχείρησης που αναλαμβάνει έναντι του Δημοσίου ή νομικού προσώπου του ευρύτερου δημόσιου τομέα την εκτέλεση έργων ή προμηθειών ή την παροχή υπηρεσιών. Η απαγόρευση του προηγούμενου εδαφίου καταλαμβάνει και κάθε είδους παρένθετα πρόσωπα, όπως συζύγους, συγγενείς, οικονομικά εξαρτημένα άτομα ή εταιρείες. Νόμος ορίζει τις ειδικότερες ρυθμίσεις, τις κυρώσεις που μπορεί να φθάνουν μέχρι την ανάκληση της άδειας ραδιοφωνικού ή τηλεοπτικού σταθμού και μέχρι την απαγόρευση σύναψης ή την ακύρωση της σχετικής σύμβασης, καθώς και τους τρόπους ελέγχου και τις εγγυήσεις αποτροπής των καταστρατηγήσεων των προηγούμενων εδαφίων.»

[80] Τασόπουλος Γ. (2023): «*Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 14*» Σε Βλαχόπουλο Σπ., Κοντιάδη Ξ., Τασόπουλο Γ. (επιμ.), Syntagmawatch, σελ. 23-24. Διαθέσιμο στο: https://www.syntagmawatch.gr/my-constitution/arthro-14/. [Ημ. Πρόσβασης 9.8.2025]

και κυβερνωμένων αναπτύσσονται ιδεολογίες και προωθείται οι κοινωνική πρόοδος[81]. Η έκφραση της κοινής γνώμης ως δείκτης των αντιδράσεων των πολιτών σε ζητήματα δημοσίου ενδιαφέροντος μπορεί να επιδράσει καθοριστικά στην λήψη αποφάσεων εκ μέρους της εξουσίας.

Αναλογιζόμενος κανείς τα ανωτέρω και αξιολογώντας την σπουδαιότητα της ελευθερίας της έκφρασης, όχι μόνο λόγω της συμβολής της στην ανάπτυξη της προσωπικότητας του ατόμου, αλλά και λόγω του εγγυητικού της ρόλου στην διαφύλαξη των δημοκρατικών αξιών και την κοινωνική εξέλιξη, καθίσταται αντιληπτή η σκοπιμότητα της χρήσης λογισμικών κατασκοπείας σε βάρος δημοσιογράφων. Τα περιστατικά παρακολούθησης ανθρώπων του Τύπου, που έρχονται στο φως, πληθαίνουν.

Στη χώρα μας, η καταγγελία του δημοσιογράφου κ. Κουκάκη, ότι οι επικοινωνίες του είχαν γίνει στόχος επιτήρησης, άνοιξε τον ασκό του Αιόλου, αφού ακολούθησε όχι μόνον η καταγγελία του Ν. Ανδρουλάκη, αλλά και πάμπολλες ακόμη περιπτώσεις δημοσιογράφων, που ασχολήθηκαν εκτενώς με το ζήτημα των υποκλοπών, αλλά και στρατιωτικών και πολιτικών αξιωματούχων.

Η διερεύνηση εκ μέρους του Κουκάκη, στο πλαίσιο της δημοσιογραφικής του έρευνας, οικονομικών σκανδάλων, στα οποία εμπλέκονταν ισχυροί επιχειρηματίες, φαίνεται πως αποτέλεσε την βασική αιτία, για την οποία στοχοποιήθηκαν οι επικοινωνίες του. Αν και αρχικώς η κυβέρνηση αρνήθηκε την χρήση εκ μέρους της ΕΥΠ του κακόβουλου λογισμικού Predator, με το οποίο διαπιστώθηκε ότι επιτηρούνταν οι επικοινωνίες του δημοσιογράφου, λίγους μόλις μήνες μετά την αρχική καταγγελία, ο τότε Διοικητής της ΕΥΠ παραδέχθηκε, ότι η Υπηρεσία είχε θέσει υπό παρακολούθηση τις τηλεφωνικές επικοινωνίες του δημοσιογράφου, για λόγους εθνικής ασφαλείας. Η παρακολούθηση, μάλιστα, έληξε αιφνίδια, όλως συμπτωματικά την ημέρα, που ο κ. Κουκάκης απευθύνθηκε στην ΑΔΑΕ, ώστε να ενημερωθεί για ενδεχόμενη παρακολούθησή των τηλεφωνικών του επικοινωνιών.

[81] Τασόπουλος Γ. (2006): «Η κοινωνία και το Σύνταγμα στην Ελλάδα – Μεταξύ πολιτικού ενθουσιασμού και ευπρέπειας», Εκδόσεις Σάκκουλα, σελ. 149.

Στην Σύστασή του[82], το Ευρωπαϊκό Κοινοβούλιο, μεταξύ άλλων, τονίζει ότι στο πλαίσιο της καταπολέμησης του σοβαρού εγκλήματος και της τρομοκρατίας και αναγνωρίζοντας ότι η ικανότητα αυτή είναι ζωτικής σημασίας για τα κράτη μέλη, η προστασία των θεμελιωδών δικαιωμάτων και της δημοκρατίας είναι απαραίτητη· τονίζει, περαιτέρω, ότι η χρήση κατασκοπευτικού λογισμικού από τα κράτη μέλη πρέπει να είναι αναλογική, δεν πρέπει να είναι αυθαίρετη και η παρακολούθηση πρέπει να επιτρέπεται μόνο σε αυστηρά προκαθορισμένες περιστάσεις· θεωρεί ότι η ύπαρξη, σε πρότερο στάδιο, αποτελεσματικών μηχανισμών διασφάλισης της δικαστικής εποπτείας είναι κρίσιμης σημασίας για την προστασία των ατομικών ελευθεριών· επαναβεβαιώνει ότι τα ατομικά δικαιώματα δεν επιτρέπεται να διακυβεύονται, λόγω ανεξέλεγκτης πρόσβασης στην παρακολούθηση· υπογραμμίζει ότι εξίσου σημαντική είναι η ικανότητα του Δικαστικού Σώματος να ασκεί, σε μεταγενέστερο στάδιο, εύλογη και ουσιαστική εποπτεία στον τομέα των αιτημάτων παρακολούθησης για λόγους εθνικής ασφάλειας, προκειμένου να διασφαλιστεί η δυνατότητα ένστασης στη δυσανάλογη χρήση κατασκοπευτικού λογισμικού από τις κυβερνήσεις και τέλος, επισημαίνει ότι δεν πρέπει να στοχοποιούνται, μέσω κατασκοπευτικού λογισμικού, δεδομένα σε σχέση με την ελευθερία του Τύπου και την ελευθερία της έκφρασης των άλλων μέσων ενημέρωσης, εκτός αν υπάρχουν επαρκείς λόγοι, διαπιστωμένοι βάσει δικαστικής εποπτείας, οι οποίοι επιβεβαιώνουν τη συμμετοχή σε εγκληματικές δραστηριότητες ή προκύπτουν ζητήματα εθνικής ασφάλειας, που θα πρέπει να υπόκεινται σε κοινό πλαίσιο.

Το Ευρωπαϊκό Κοινοβούλιο, με αφορμή το κύμα περιστατικών παρακολούθησης δημοσιογράφων σε αρκετές χώρες της Ευρωπαϊκής Ένωσης, προχώρησε στην έκδοση του Κανονισμού[83] για την ελευθερία των μέσων ενημέρωσης, ο οποίος μόλις στις αρχές Αυγούστου 2025, ετέθη σε ισχύ.

---

[82] Σύσταση του Ευρωπαϊκού Κοινοβουλίου της 15ης Ιουνίου 2023 προς το Συμβούλιο και την Επιτροπή σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (2023/2500(RSP)). Διαθέσιμη σε: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EL.html.

[83] Κανονισμός (ΕΕ) 2024/1083 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Απριλίου 2024, για τη θέσπιση κοινού πλαισίου για τις υπηρεσίες μέσων ενημέρωσης στην εσωτερική αγορά και την τροποποίηση της οδηγίας 2010/13/ΕΕ (Ευρωπαϊκός Νόμος για την Ελευθερία των Μέσων Ενημέρωσης). Διαθέσιμος σε: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1083.

Αξιοπρόσεκτη είναι η αναφορά του Κανονισμού στα λογισμικά επιτήρησης των επικοινωνιών των δημοσιογράφων και των επιπτώσεων της εφαρμογής τους. «*Το λογισμικό παρεμβατικής παρακολούθησης, συμπεριλαμβανομένου, ιδίως, αυτού που συνήθως αναφέρεται ως «κατασκοπευτικό λογισμικό», αντιπροσωπεύει μια ιδιαίτερα επεμβατική μορφή παρακολούθησης των επαγγελματιών των μέσων ενημέρωσης και των πηγών τους. Μπορεί να χρησιμοποιηθεί για τη μυστική καταγραφή κλήσεων ή άλλη χρήση του μικροφώνου συσκευής τελικού χρήστη, την κινηματογράφηση ή φωτογράφιση φυσικών προσώπων, μηχανημάτων ή του περιβάλλοντος χώρου τους, την αντιγραφή μηνυμάτων, την πρόσβαση σε κρυπτογραφημένα δεδομένα περιεχομένου, την ανίχνευση της δραστηριότητας περιήγησης, την ανίχνευση γεωεντοπισμού ή τη συλλογή άλλων δεδομένων αισθητήρων ή την ανίχνευση δραστηριοτήτων σε πολλαπλές συσκευές τελικού χρήστη. **Έχει αποτρεπτικές συνέπειες για την ελεύθερη άσκηση των οικονομικών δραστηριοτήτων στον τομέα των μέσων ενημέρωσης. Διακυβεύει ιδίως τη σχέση εμπιστοσύνης των δημοσιογράφων με τις πηγές τους, η οποία αποτελεί την καρδιά του δημοσιογραφικού επαγγέλματος.** Δεδομένου του ψηφιακού και παρεμβατικού χαρακτήρα του, εν λόγω, λογισμικού και της χρήσης συσκευών διασυνοριακά, έχει ιδιαίτερα επιζήμιο αντίκτυπο στην άσκηση των οικονομικών δραστηριοτήτων των παρόχων υπηρεσιών μέσων ενημέρωσης στην εσωτερική αγορά. Ως εκ τούτου είναι αναγκαίο να διασφαλιστεί ότι οι πάροχοι υπηρεσιών μέσων ενημέρωσης, συμπεριλαμβανομένων των δημοσιογράφων, που δραστηριοποιούνται στην εσωτερική αγορά υπηρεσιών των μέσων ενημέρωσης μπορούν να απολαμβάνουν ισχυρή εναρμονισμένη προστασία, έναντι της ανάπτυξης παρεμβατικού λογισμικού παρακολούθησης στην Ένωση, μεταξύ άλλων όταν οι αρχές των κρατών μελών προσφεύγουν σε ιδιωτικούς φορείς για την ανάπτυξή του.*

*Το παρεμβατικό λογισμικό παρακολούθησης θα πρέπει να αναπτύσσεται **μόνον όταν δικαιολογείται από επιτακτικό λόγο δημόσιου συμφέροντος**, όταν προβλέπεται από το ενωσιακό ή εθνικό δίκαιο, όταν συμμορφώνεται με το άρθρο 52 παράγραφος 1 του Χάρτη, όπως ερμηνεύεται από το Δικαστήριο και με άλλους κανόνες ενωσιακού δικαίου, όταν έχει εγκριθεί εκ των προτέρων ή, σε εξαιρετικές και επείγουσες περιπτώσεις, έχει επιβεβαιωθεί στη συνέχεια από δικαστική αρχή ή ανεξάρτητη και αμερόληπτη αρχή λήψης αποφάσεων, όταν διενεργείται στο πλαίσιο ερευνών για αξιόποινες πράξεις που απαριθμούνται στο άρθρο 2 παράγραφος 2 της απόφασης-πλαισίου 2002/584/ΔΕΥ του Συμβουλίου … Σύμφωνα με την αρχή της αναλογικότητας, περιορισμοί*

στα δικαιώματα και τις ελευθερίες ατόμου δύνανται να επιβάλλονται μόνο εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού συμφέροντος που αναγνωρίζει η Ένωση. Επομένως, όσον αφορά ειδικά την ανάπτυξη λογισμικού παρεμβατικής παρακολούθησης, είναι αναγκαίο να εξακριβωθεί αν η σοβαρότητα της επίμαχης αξιόποινης πράξης φτάνει ένα συγκεκριμένο επίπεδο όπως και ορίζεται στον παρόντα κανονισμό, αν, κατόπιν εξατομικευμένης εκτίμησης όλων των κρίσιμων περιστάσεων δεδομένης υπόθεσης, η έρευνα για την εν λόγω αξιόποινη πράξη και η δίωξή της απαιτούν την ιδιαιτέρως επεμβατική παρέμβαση στα θεμελιώδη δικαιώματα και τις οικονομικές ελευθερίες, η οποία συνίσταται στην ανάπτυξη λογισμικού παρεμβατικής παρακολούθησης, αν υπάρχουν επαρκή αποδεικτικά στοιχεία για τη διάπραξη της συγκεκριμένης αξιόποινης πράξης και αν η ανάπτυξη λογισμικού παρεμβατικής παρακολούθησης είναι κρίσιμη για τη διαπίστωση των πραγματικών περιστατικών που σχετίζονται με την έρευνα για την εν λόγω αξιόποινη πράξη και τη δίωξή της.»[84]

3.2 Το νομικό πλαίσιο προστασίας έναντι των κατασκοπευτικών λογισμικών

Οι διατάξεις του άρθρου 19 Σ. και του Ν. 5002/2022, όπως εκτενώς αναλύθηκαν ανωτέρω, σε συνδυασμό με το άρθρο 8 της ΕΣΔΑ και τα άρθρα 7 και 8 του ΧΘΔΕΕ, συναπαρτίζουν το κανονιστικό πλέγμα, που ρυθμίζει τους όρους και της προϋποθέσεις, υπό τις οποίες δύναται να περιοριστεί το δικαίωμα στο απόρρητο των επικοινωνιών και το, εν γένει, δικαίωμα στον ιδιωτικό βίο, τηρουμένης πάντα της Αρχής της αναλογικότητας.

Εκκινώντας από την συνταγματική προστασία, όπως ήδη, εκτέθηκε ανωτέρω, και κατά την ρητή διατύπωση του συντακτικού νομοθέτη, η κάμψη του δικαιώματος στο επικοινωνιακό απόρρητο είναι νοητή, **μόνο για λόγους εθνικής ασφάλειας και διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων**, έννοιες με ευρύ περιεχόμενο, το οποίο εναπόκειται στον κοινό νομοθέτη να προσδιορίσει. Απόπειρα δε, τέτοιου προσδιορισμού συνιστά ο Ν. 5002/2022, ο οποίος επικαιροποίησε το προϊσχύσαν ρυθμιστικό πλαίσιο, σχετικά με την διαδικασία άρσης του επικοινωνιακού απορρήτου, ενώ εισήγαγε πλέγμα διατάξεων, για τα λογισμικά παρακολούθησης, σε μια προσπάθεια κατευνασμού των αντιδράσεων, που είχαν εκδηλωθεί ως απότοκο του σκανδάλου των παρακολουθήσεων.

[84] Αιτ. Σκέψεις 25 – 26 Κανονισμού (ΕΕ) 2024/1083.

Έτσι σε μια πρώτη προσπάθεια οριοθέτησης, ο Ν. 5002/2022 προβλέπει ότι «*Με προεδρικό διάταγμα, που εκδίδεται εντός τριών (3) μηνών από την έναρξη ισχύος του παρόντος, μετά από πρόταση των Υπουργών Προστασίας του Πολίτη, Εθνικής Άμυνας, Δικαιοσύνης και Ψηφιακής Διακυβέρνησης, καθορίζονται οι προϋποθέσεις υπό τις οποίες είναι επιτρεπτή η σύναψη συμβάσεων εκ μέρους κρατικών δομών για την προμήθεια λογισμικών ή συσκευών παρακολούθησης του άρθρου 370ΣΤ του Ποινικού Κώδικα για την εκπλήρωση των σκοπών τους, καθώς και επιπρόσθετοι όροι της χρήσης τους.*» (άρθρο 13), ενώ σύμφωνα με το άρθρο 14 του ίδιου Νόμου, τα, εν λόγω, λογισμικά ή συσκευές παρακολούθησης καταγράφονται σε ενδεικτικό κατάλογο που εκδίδει η Ολομέλεια της Α.Δ.Α.Ε. μετά από εισήγηση της Επιτροπής Συντονισμού για θέματα Κυβερνοασφάλειας του άρθρου 20, ο οποίος επικαιροποιείται το αργότερο κάθε έξι (6) μήνες και αναρτάται στον ιστότοπο της ΕΥΠ σχετικό ενημερωτικό υλικό για τα λογισμικά, τον τρόπο δράσης τους και τα μέτρα προστασίας που μπορούν να ληφθούν έναντι αυτών.

Αξίζει βέβαια να σημειωθεί, ότι μέχρι σήμερα, στην ελληνική έννομη τάξη δεν υφίσταται συνεκτικό ρυθμιστικό πλαίσιο, για την χρήση των λογισμικών παρακολούθησης, το επίμαχο Προεδρικό Διάταγμα με αντικείμενο τον καθορισμό των προϋποθέσεων, υπό τις οποίες είναι επιτρεπτή η σύναψη συμβάσεων εκ μέρους δημοσίων φορέων (ΕΥΠ, ΔΑΕΕΒ κλπ.) για την προμήθεια λογισμικών ή συσκευών παρακολούθησης, κατά το άρθρο 13 του Ν. 5002/2022, έως και σήμερα δεν έχει εκδοθεί, ενώ ούτε και η Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας, έχει παραδώσει, στην ΑΔΑΕ τον κατάλογο με τα διαθέσιμα λογισμικά spyware, ως όφειλε σύμφωνα με το άρθρο 14 του Ν. 5002/2022.

3.2.1 Η Οδηγία 2002/58/ΕΚ (e- Privacy Directive) και η ενσωμάτωσή της στην εθνική έννομη τάξη με τον Ν. 3471/2006

Η Οδηγία 2002/58/ΕΚ (e- Privacy Directive)[85], για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες αποτελεί την νομοθετική πρωτοβουλία της Ε.Ε. για την προστασία του απορρήτου των επικοινωνιών σταθερής και κινητής τηλεφωνίας[86].

Η ενσωμάτωση της, εν λόγω, Οδηγίας στο εθνικό δίκαιο, πραγματοποιήθηκε με την ψήφιση του Ν. 3471/2006[87] για την Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/1997.

Στο άρθρο 4 του Ν. 3471/2006, επισημαίνεται μεταξύ άλλων, η δυνατότητα άρσης του ηλεκτρονικού επικοινωνιακού απορρήτου, υπό τις προϋποθέσεις που θέτει η συνταγματική διάταξη του άρθρου 19 Σ, απαγορευμένης της ακρόασης, υποκλοπής, αποθήκευσης ή άλλου είδους παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης, εκτός αν προβλέπεται άλλως από το νόμο.

---

[85] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). Διαθέσιμη σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex:32002L0058.

[86] Σύμφωνα με την παρ. 1 του άρθρου 5 της ανωτέρω Οδηγίας, τα κράτη μέλη κατοχυρώνουν, μέσω της εθνικής νομοθεσίας, το απόρρητο των επικοινωνιών, που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης, απαγορεύοντας την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια, σύμφωνα με το άρθρο 15 παρ. 1 της Οδηγίας, ενώ κατά την παρ. 2 του ιδίου, ως άνω, άρθρου δεν επηρεάζεται οποιαδήποτε επιτρεπόμενη από το νόμο καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα.
Η Οδηγία, στο άρθρο 15, προβλέπει δυνατότητα των κρατών μελών να περιορίζουν τα δικαιώματα και τις υποχρεώσεις, που απορρέουν εξ αυτής, *εφόσον ο περιορισμός αυτός αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία για τη διαφύλαξη της εθνικής ασφάλειας (δηλαδή της ασφάλειας του κράτους), της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδείας χρησιμοποίησης του συστήματος ηλεκτρονικών επικοινωνιών, όπως προβλέπεται στο άρθρο 13 παράγραφος 1 της οδηγίας 95/46/ΕΚ.* Για το σκοπό αυτό, τα κράτη μέλη δύνανται, μεταξύ άλλων, να λαμβάνουν νομοθετικά μέτρα που θα προβλέπουν τη φύλαξη δεδομένων για ορισμένο χρονικό διάστημα για τους ανωτέρω λόγους, σύμφωνα με τις γενικές αρχές του κοινοτικού δικαίου, συμπεριλαμβανομένων αυτών που αναφέρονται στο άρθρο 6 παράγραφοι 1 και 2 της συνθήκης για την Ευρωπαϊκή Ένωση.

[87] Ν. 3471/2006 ΦΕΚ Α' 133/28.6.2006. Διαθέσιμος σε: https://search.et.gr/el/fek/?fekId=334206.

Περαιτέρω κατά την παρ. 3 του άρθρου: «*Επιτρέπεται η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων εμπορικής συναλλαγής ή άλλης επικοινωνίας επαγγελματικού χαρακτήρα, υπό την προϋπόθεση ότι και τα δύο μέρη, μετά από προηγούμενη ενημέρωση σχετικά με το σκοπό της καταγραφής, παρέχουν τη συγκατάθεσή τους. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, καθορίζεται ο τρόπος ενημέρωσης των μερών και παροχής της συγκατάθεσης, καθώς και ο τρόπος και ο χρόνος διατήρησης των καταγεγραμμένων συνδιαλέξεων και των συναφών δεδομένων κίνησης.*»

Σύμφωνα δε, με την παρ. 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.*»

Η αναφορά του νόμου σε «*κατασκοπευτικά λογισμικά, κρυφά αναγνωριστικά στοιχεία και άλλες παρόμοιες διατάξεις*», σχετίζεται ενδεικτικά με λογισμικά spyware, δικτυακούς «κοριούς» (web bugs), κρυφά αναγνωριστικά στοιχεία, cookies, κλπ, τα οποία 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, και συνιστούν ενδεχόμενη σοβαρή παραβίαση της ιδιωτικής ζωής του χρήστη. Το ζητούμενο είναι κατά πόσον τέτοιες διατάξεις χρησιμοποιούνται πράγματι για θεμιτούς σκοπούς (λ.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)) και υπό την προϋπόθεση ότι παρέχονται σαφείς και ακριβείς πληροφορίες στους χρήστες, για τον προορισμό τέτοιων διατάξεων, ώστε να έχουν την ευκαιρία να αρνηθούν την αποθήκευση «cookies» ή παρόμοιων διατάξεων στον τερματικό τους εξοπλισμό. Τούτο είναι ιδιαίτερα σημαντικό σε περιπτώσεις, όπου πρόσβαση στον τερματικό εξοπλισμό, και επομένως και σε κάθε είδους ευαίσθητα δεδομένα προσωπικού χαρακτήρα, που έχουν αποθηκευθεί σε έναν τέτοιο εξοπλισμό, έχουν και άλλοι, εκτός από τον πρωταρχικό χρήστη.[88].

Οι αλματώδεις εξελίξεις στον τομέα της τεχνολογίας καθιστούν αναγκαία την εισαγωγή ενός ομοιόμορφου, συνεκτικού ρυθμιστικού πλαισίου, για τις ηλεκτρονικές επικοινωνίες, με άμεση ισχύ σε όλα τα κράτη μέλη. Η έκδοση του ΓΚΠΔ αποτέλεσε κορυφαία προσπάθεια εκσυγχρονισμού του πλαισίου προστασίας των δεδομένων τα τελευταία χρόνια και η σχετική νομοθεσία, για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, πρέπει να προσαρμοστεί, ώστε να ευθυγραμμιστεί με τους νέους αυτούς κανόνες. Περαιτέρω, οι καταναλωτές και οι επιχειρήσεις βασίζονται όλο και περισσότερο σε νέες διαδικτυακές υπηρεσίες, που επιτρέπουν τις διαπροσωπικές επικοινωνίες, όπως η τηλεφωνία μέσω internet (Voice over IP), οι υπηρεσίες άμεσης ανταλλαγής μηνυμάτων και οι υπηρεσίες διαδικτυακού ηλεκτρονικού ταχυδρομείου. Αυτές οι επιφυείς («over-the-top» «OTT») υπηρεσίες γενικά δεν υπάγονται στο ισχύον πλαίσιο ηλεκτρονικών επικοινωνιών της Ένωσης, συμπεριλαμβανομένης της Οδηγίας e- Privacy, η οποία δεν συμβαδίζει με τις τεχνολογικές εξελίξεις, με αποτέλεσμα ένα κενό προστασίας των επικοινωνιών, που παρέχονται μέσω νέων υπηρεσιών.[89]

Προς την κατεύθυνση αυτή, η ψήφιση του Κανονισμού e- Privacy απασχόλησε για πολλά χρόνια την Ε.Ε., αποσκοπώντας, στη διασφάλιση της ομοιογενούς εφαρμογής του σε όλα τα κράτη μέλη και σε κάθε είδους υπευθύνους επεξεργασίας δεδομένων.

---

[88] Αιτ. Σκέψεις 24-25 της Οδηγίας e- Privacy.

[89] Ευρωπαϊκή Επιτροπή, Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, COM (2017) 010 final. Διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52017PC0010.

Σταχυολογώντας τα βασικά σημεία της Πρότασης του Κανονισμού, αυτά είναι: **α)** η διεύρυνση του πεδίου εφαρμογής στους τελικούς χρήστες που βρίσκονται εντός ΕΕ, ακόμη κι αν η επεξεργασία λαμβάνει χώρα εκτός ΕΕ ή ο πάροχος υπηρεσιών είναι εγκατεστημένος ή βρίσκεται εκτός της ΕΕ, **β)** το ενιαίο επίπεδο προστασίας για όλα τα φυσικά και νομικά πρόσωπα εντός ΕΕ, **γ)** η προστασία της επικοινωνίας όχι μόνο ως προς το περιεχόμενό της καθεαυτό, αλλά και ως προς τα εξωτερικά της στοιχεία, **δ)** η δυνατότητα πραγματικής επιλογής, όσον αφορά την αποδοχή cookies ή παρόμοιων αναγνωριστικών κωδικών. Η εξάρτηση της πρόσβασης σε δικτυακό τόπο από τη συγκατάθεση για τη χρήση cookies για πρόσθετους σκοπούς, ως εναλλακτική λύση αντί της επί πληρωμή πρόσβασης, θα επιτρέπεται, εάν ο χρήστης είναι σε θέση να επιλέξει μεταξύ της, εν λόγω, προσφοράς και ισοδύναμης προσφοράς του ίδιου παρόχου, που δεν συνεπάγεται συγκατάθεση για τα cookies. Προκειμένου να αποφεύγεται η επαναλαμβανόμενη συγκατάθεση για τα cookies, ο τελικός χρήστης θα μπορεί να δίνει τη συγκατάθεσή του για τη χρήση ορισμένων ειδών cookies, καταχωρώντας έναν ή περισσότερους παρόχους σε κατάλογο εγκεκριμένων παρόχων στις ρυθμίσεις του φυλλομετρητή.

Ωστόσο, οικονομικά συμφέροντα εταιρειών – κολοσσών, άσκησαν έντονες πιέσεις στην Ένωση, με αποτέλεσμα, μόλις στις αρχές του 2025, η Ευρωπαϊκή Επιτροπή να ανακοινώσει την απόφασή της, για απόσυρση της Πρότασης του Κανονισμού, αναδεικνύοντας την έλλειψη πολιτικής βούλησης των οργάνων της ΕΕ να αναμετρηθούν με τα ισχυρά οικονομικά συμφέροντα. Παράλληλα, όμως, αποκαλύπτεται και μια ανησυχητική πολιτική τάση, που δίνει προτεραιότητα στην μαζική παρακολούθηση, έναντι της ιδιωτικότητας, με το πρόσχημα της πρόληψης και καταστολής του οργανωμένου εγκλήματος (σεξουαλική κακοποίηση ανηλίκων κλπ.), μέτρα που σε κάθε περίπτωση θίγουν βάναυσα τα θεμελιώδη δικαιώματα[90].

[90] «*The ePrivacy Regulation proposal has been withdrawn, but the fight for your privacy is far from over*», 19.2.2025. Διαθέσιμο στο: https://edri.org/our-work/the-eprivacy-regulation-proposal-has-been-withdrawn-but-the-fight-for-your-privacy-is-far-from-over/. [Ημ. Πρόσβασης 12.8.2025]

3.2.2 Ο Ν. 4070/2012

Με τον Ν. 4070/2012[91] (Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών Δημοσίων Έργων και άλλες Διατάξεις), προβλέφθηκε[92] η υποχρέωση των παρόχων, δημοσίων δικτύων επικοινωνιών ή υπηρεσιών ηλεκτρονικών επικοινωνιών, να λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών. Τα μέτρα αυτά, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τον υφιστάμενο κίνδυνο, για την αποτροπή και ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφαλείας, που επηρεάζουν τους χρήστες και τα διασυνδεμένα δίκτυα και για την εξασφάλιση της ακεραιότητας των δικτύων, έτσι ώστε να διασφαλίζεται η συνέχεια της παροχής των υπηρεσιών, που διανέμονται μέσω των δικτύων αυτών. Η ΑΔΑΕ μάλιστα με κανονιστικές πράξεις, που εκδίδει, καθορίζει τα τεχνικά και οργανωτικά μέτρα, προς εκπλήρωση των ανωτέρω σκοπών του Νόμου[93]. Τυχόν παραβάσεις της ασφάλειας ή της ακεραιότητας των δικτύων κοινοποιούνται στην ΕΕΤΤ και στην ΑΔΑΕ, οι οποίες οφείλουν να ενημερώνουν με τη σειρά τους τον Ευρωπαϊκό Οργανισμό, για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

3.2.3 Η ποινική προστασία έναντι των λογισμικών κατασκοπείας

Ως προελέχθη, δυνάμει του άρθρου 12 του Ν. 5002/2022 εισήχθη η διάταξη του άρθρου 370ΣΤ του Π.Κ. , με την οποία ποινικοποιήθηκε το πρώτον η παραγωγή, διακίνηση, πώληση, εισαγωγή, εξαγωγή, αλλά και η κατοχή καθεαυτή λογισμικών, συσκευών παρακολούθησης και άλλων δεδομένων, με προορισμό την τέλεση αδικημάτων κατά του επικοινωνιακού απορρήτου.

Δυνάμει της διάταξης του άρθρου 370Α Π.Κ. θεμελιώνεται η προστασία της προφορικής συνομιλίας και του απορρήτου της τηλεφωνικής επικοινωνίας, που διεξάγονται μη δημόσια, δεν προορίζονται δηλαδή να καταστούν προσιτές σε αόριστο αριθμό προσώπων.

---

[91] Ν. 4070/2012 ΦΕΚ Α' 82/10.4.2012. Διαθέσιμος σε: https://search.et.gr/el/fek/?fekId=473837.

[92] Άρθρο 37 του Ν. 4070/2012, στο οποίο προβλέπονται επ' ακριβώς οι αρμοδιότητες και εξουσίες της ΑΔΑΕ και της ΕΕΤΤ, ως προς την εφαρμογή και τυχόν παραβίαση των μέτρων.

[93] Υπ' αριθ. 205/2013 Απόφαση της ΑΔΑΕ (ΦΕΚ Β' 1742/15.7.2013), με την οποία εξειδίκευσε το περιεχόμενο του άρθρου 37 του Ν. 4070/2012, σε εκτέλεση της ανωτέρω διατάξεως. Διαθέσιμη σε: https://adae.gov.gr/images/nomothetiko-plaisio/Kanonismos_FEK_1742_B_15_07_2013_asfaleia_akeraiotita__ADAE_205_2013_01.pdf.

Διαπιστώνεται αυστηροποίηση των ποινών και τα αδικήματα του, εν λόγω, άρθρου μετατρέπονται ξανά σε κακουργήματα, με απειλούμενη ποινή κάθειρξης έως δέκα (10) ετών, ενώ διαγράφεται η λέξη «αθέμιτα» και επιστρέφει η παρ. 5 του άρθρου που είχε καταργηθεί με προηγούμενη τροποποίηση, αφορώσα την παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή την ασφάλεια του κράτους. Ο νέος νόμος επαναλαμβάνει ουσιαστικά με κάποιες ελάχιστες διαφορές, την προγενέστερη διάταξη του άρθρου 370Α ΠΚ, που είχε διαμορφωθεί με το Ν. 3674/2008, δυνάμει του οποίου τα αδικήματα του άρθρου απέκτησαν κακουργηματικό χαρακτήρα, ο οποίος με, εκ των υστέρων, τροποποιήσεις είχε καταστεί πλημμεληματικός.

Το άρθρο 370Ε Π.Κ. προστατεύει το έννομο αγαθό της ελεύθερης ηλεκτρονικής επικοινωνίας, όπως και του απορρήτου, δηλαδή του εμπιστευτικού χαρακτήρα του περιεχομένου της, που κατοχυρώνεται συνταγματικά στο άρθρο 19 Σ. Η εγκληματική συμπεριφορά συνίσταται στην «υποκλοπή» («interception»), με τεχνικά μέσα, ψηφιακών δεδομένων ή ηλεκτρομαγνητικών εκπομπών, κατά τον χρόνο που αυτά διαβιβάζονται από, προς ή εντός πληροφοριακού συστήματος, δηλαδή κατά τη στιγμή ροής των δεδομένων. Έτσι, λοιπόν, τελεί το αδίκημα του άρθρου τούτου κάποιος, που παρεισφρύει στη διαδικτυακή συζήτηση δύο ή περισσότερων ατόμων και την παρακολουθεί ή την αποτυπώνει, κατά τη στιγμή, που λαμβάνει χώρα, είτε πρόκειται για βιντεοδιάσκεψη, για ανταλλαγή μηνυμάτων ή ηχητική επικοινωνία, σε εφαρμογές όπως «zoom», «viber» ή «messenger». Επίσης διαπράττει το έγκλημα, όποιος παρεισφρήσει και παρακολουθήσει τηλεοπτικό περιεχόμενο, που μεταδίδουν με απευθείας «ζωντανή» ροή, μέσω διαδικτύου («live streaming»), πλατφόρμες ταινιών – σειρών(λ.χ. μετάδοση προγράμματος αθλητικών αγώνων ή συναυλιών ή ταινιών κατά τη στιγμή που γίνεται ροή δεδομένων)[94].

Το επικοινωνιακό απόρρητο προστατεύει και η διάταξη του άρθρου 292Α Π.Κ., σύμφωνα με την οποία ποινικοποιείται, εκτός από την παραβίαση της ασφάλειας των τηλεφωνικών επικοινωνιών και ο κίνδυνος για τον απόρρητο χαρακτήρα των επικοινωνιών[95].

---

[94] Καράτσαλος Γ. (2023), «*Προσβολές εννόμων αγαθών σε ψηφιακό περιβάλλον και ποινική αντιμετώπισή τους*», ΕΣΔΙ, σελ. 17-18. Διαθέσιμο στο: https://www.esdi.gr/wp-content/uploads/2023/seminars/02/psifiaki_oikonomia/karatsalos_2023.pdf. [Ημ. Πρόσβασης 13.8.2025]

[95] ΑΠ 916/2019.

4. ΑΛΛΑ ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΩΣ ΠΡΟΣ ΤΑ ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ

4.1 Τα κριτήρια του ΕΔΔΑ για την νόμιμη χρήση των λογισμικών παρακολούθησης

Οι περιπτώσεις επιτήρησης, μέσω του λογισμικού Pegasus, έχουν εγείρει ποικίλα νομικά ζητήματα, εντός την ευρωπαϊκής έννομης τάξης, ιδίως ως προς την νομιμότητα χρήσης τέτοιων λογισμικών, ενόψει του γεγονότος ότι σε πολλές από αυτές τις περιπτώσεις δεν υπήρχε ή δεν ήταν προβλέψιμη σοβαρή και πραγματική απειλή για την εθνική ή δημόσια ασφάλεια, καθώς και ότι σε αρκετές έννομες τάξεις οι συνθήκες ανάπτυξης φαίνονται επιτρεπτικές και οι μηχανισμοί προσφυγής αναποτελεσματικοί. Τέτοιες περιπτώσεις «δοκιμάζουν» τα δικαιώματα στην προστασία δεδομένων και την ιδιωτικότητα, την ελευθερία της έκφρασης, την ελευθερία του Τύπου, την ελευθερία του συνεταιρίζεσθαι, τους μηχανισμούς προσφυγής στη δικαιοσύνη, τις δημοκρατικές διαδικασίες και τους Θεσμούς και ενδεχομένως τους κανόνες απόδειξης[96].

Σημαντική πυξίδα στην διαμόρφωση του πλαισίου νομιμότητας της χρήσης λογισμικών κατασκοπείας, μπορεί να αποτελέσει η πλούσια Νομολογία του ΕΔΔΑ, η οποία καθορίζει τα κριτήρια, επί τη βάσει των οποίων μπορεί να χαρακτηριστεί νόμιμος ο περιορισμός του δικαιώματος στον ιδιωτικό βίο και κατ' επέκταση στο δικαίωμα του επικοινωνιακού απορρήτου, υπό τις προϋποθέσεις της παρ. 2 του άρθρου 8 της ΕΣΔΑ, δηλαδή προς το συμφέρον της εθνικής ασφάλειας, της δημόσιας ασφάλειας ή της οικονομικής ευημερίας της χώρας, για την πρόληψη της διατάραξης της τάξης ή του εγκλήματος, για την προστασία της υγείας ή της ηθικής ή για την προστασία των δικαιωμάτων και των ελευθεριών των άλλων. Επιτρέπονται περιορισμοί, εάν είναι «σύμφωνοι με το νόμο» ή «ορίζονται από το νόμο» και είναι «απαραίτητοι σε μια δημοκρατική κοινωνία» για την προστασία ενός από τους στόχους που ορίζονται ανωτέρω[97].

Συνοπτικά, τα κριτήρια αυτά, αφορούν: i) την ύπαρξη σχετικής νομοθετικής πρόβλεψης στην εθνική έννομη τάξη, ii) την οριοθέτηση της έννοιας της εθνικής ασφάλειας και της φύσης των αδικημάτων, προς διακρίβωση των οποίων, δικαιολογείται ο περιορισμός του δικαιώματος, iii) τον καθορισμό του κύκλου προσώπων έναντι των οποίων μπορεί να ληφθεί το μέτρο παρακολούθησης, iv) τον προσδιορισμό της διάρκειας του μέτρου, v) την προηγούμενη

[96] «*Europe's PegasusGate – Countering spyware abuse*», ο.π., σελ. 17.
[97] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 1.

δικαστική άδεια, που διατάσσει το μέτρο, vi) την ύπαρξη ανεξάρτητου εποπτικού οργάνου, για τον έλεγχο της διαδικασίας εφαρμογής μέτρων περιορισμού του δικαιώματος, vii) τις προϋποθέσεις γνωστοποίησης της επιβολής του μέτρου στον θιγόμενο και viii) η τήρηση της Αρχής της αναλογικότητας, τόσο ως προϋπόθεση λήψης του μέτρου, όσο και κατά την διάρκεια της εφαρμογής του.

Εκκινώντας από το κριτήριο της ύπαρξης στο εθνικό δίκαιο σχετικού νόμου (basis in the domestic law), σύμφωνα με τον οποίο (νόμο) είναι ανεκτή η κάμψη του δικαιώματος στο επικοινωνιακό απόρρητο, το ΕΔΔΑ θέτει συγκεκριμένα ποιοτικά χαρακτηριστικά, τα οποία θα πρέπει να πληροί ο εθνικός νόμος (quality of law), ώστε να εξασφαλιστεί η συμβατότητα με τις απαιτήσεις της ΕΣΔΑ και η συμφωνία με την Αρχή του Κράτους Δικαίου (rule of law). Διευκρινίζεται, ότι η έννοια του «νόμου», εν προκειμένω, λογίζεται στην ευρύτερη εννοιολογική εκδοχή της και δεν ερμηνεύεται μόνο ως τυπικός, αλλά ως ουσιαστικός νόμος.

Κατά το ΕΔΔΑ, βασικά κριτήρια που θα πρέπει να ικανοποιεί ο εθνικός νόμος είναι η προσβασιμότητα (accessibility – δυνατότητα πρόσβασης στο νόμο) και η προβλεψιμότητα (foreseeability - δυνατότητα πρόγνωσης των συνεπειών του νόμου). Αναφορικά με την έννοια της προσβασιμότητας, αποδίδεται ως η δυνατότητα του ατόμου να λαμβάνει γνώση του περιεχομένου του νόμου με εύκολο και άμεσο τρόπο. Δεν απαιτείται, όμως, ο νόμος να είναι κατανοητός στον οποιονδήποτε, αλλά αρκεί να είναι κατανοητός στους ειδικούς, που διαθέτουν κατάλληλη γνώση αντίληψης του περιεχομένου τους[98].

Κατά το ΕΔΔΑ, η έννοια της προβλεψιμότητας δεν μπορεί να σημαίνει ότι ένα άτομο θα πρέπει να είναι σε θέση να προβλέψει, πότε οι αρχές είναι πιθανό να καταφύγουν σε τέτοια μέτρα, ώστε να μπορεί να προσαρμόσει τη συμπεριφορά του αναλόγως[99], καθώς σε μια τέτοια περίπτωση αναιρείται ο σκοπός επιβολής τους, αλλά ότι το εσωτερικό δίκαιο πρέπει να είναι επαρκώς προβλέψιμο, υπό την έννοια να παρέχει στα άτομα επαρκή ένδειξη, ως προς τις περιστάσεις και τις προϋποθέσεις υπό τις οποίες οι Αρχές δικαιούνται να καταφύγουν σε μέτρα,

---

98 ΕΔΔΑ, 1990, *Groppera Radio Ag και λοιποί κατά Ελβετίας*, § 68. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22ENG%22],%22appno%22:[%2210890/84%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-57623%22]}.

99 ΕΔΔΑ, 2022, *Adomaitis κατά Λιθουανίας*, §83. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-215168%22]}.

που επηρεάζουν τα δικαιώματά τους[100]. Έτσι, ο νόμος θα πρέπει να είναι σαφής και ακριβής, ώστε να παρέχει στους πολίτες επαρκείς ενδείξεις, για το εύρος της διακριτικής ευχέρειας, που παρέχεται στην εκτελεστική εξουσία ή σε έναν δικαστικό λειτουργό, ώστε να εξασφαλιστεί επαρκής προστασία έναντι αυθαίρετων παρεμβάσεων, ο κίνδυνος των οποίων είναι προφανής, όταν η εκτελεστική εξουσία δρα μυστικά[101].

Περαιτέρω, σχετικά με τον καθορισμό της έννοιας της εθνικής ασφάλειας, το ΕΔΔΑ έχει κρίνει, ότι εναπόκειται στο εθνικό δίκαιο να προσδιορίσει το περιεχόμενο της αόριστης αυτής έννοιας, πάντοτε, όμως, υπό τις γενικότερες προϋποθέσεις, που θέτει η ευρωπαϊκή νομοθεσία και νομολογία. Αναφορικά δε, με τα αδικήματα για την διακρίβωση των οποίων, δύναται να προβλέπεται το μέτρο της επιτήρησης, το ΕΔΔΑ επισημαίνει, ότι δεν απαιτείται εξαντλητική πρόβλεψη εκ μέρους του εθνικού νομοθέτη, εξαιτίας του γεγονότος, ότι οι απειλές της εθνικής ασφάλειας, μπορούν να είναι απρόβλεπτες, αλλά σε κάθε περίπτωση θα πρέπει τουλάχιστον να καθορίζεται ο κύκλος των αδικημάτων αυτών, με βάση τη φύση τους[102].

Σύμφωνα με το ΕΔΔΑ, θα πρέπει ο εθνικός νόμος να προσδιορίζει ρητά τον κύκλο προσώπων, στα οποία δύναται να επιβληθεί το μέτρο της επιτήρησης. Η συγκεκριμένη προϋπόθεση, που θέτει το Δικαστήριο, αποκτά ιδιαίτερη σημασία για τις μη στοχευμένες - μαζικές παρακολουθήσεις[103]. Όπως έχει κριθεί, παρακολουθήσεις μπορούν να διαταχθούν όχι μόνο σε σχέση με έναν ύποπτο ή έναν κατηγορούμενο, αλλά και σε σχέση με ένα άτομο, που μπορεί να έχει πληροφορίες για ένα αδίκημα ή μπορεί να έχει άλλες πληροφορίες, σχετικές με την ποινική υπόθεση, χωρίς όμως να αρκεί ως κριτήριο της επιβολής του μέτρου, η εδαφική

---

[100] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 20.

[101] ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*, §229. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22appno%22:[%2247143/06%22],%22itemid%22:[%22001-159324%22]} & ΕΔΔΑ, 2022, *Ekimdzhiev κατά Βουλγαρίας*, § 75. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-214673%22]}.

[102] ΕΔΔΑ, 2010, *Kennedy κατά Ην. Βασιλείου*, § 159. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-98473%22]}.

[103] Πρόκειται για την επιτήρηση των επικοινωνιών αδιακρίτως μεγάλου αριθμού ατόμων (ενδεχομένως και ολόκληρου έθνους), ακόμη και χωρίς ενδείξεις παραβατικότητας και έχει προδραστική λειτουργία, με στόχο τον εντοπισμό μελλοντικών απειλών και την επισήμανση ατόμων ως ύποπτων (βλ. Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 - January 2023, «*The impact of Pegasus on fundamental rights and democratic processes*», ο.π., σελ. 20)

έκταση των περιοχών που συνδέονται με το αδίκημα[104]. Ωστόσο, στην υπόθεση *Szabo and Vissy κατά Ουγγαρίας*[105], το ΕΔΔΑ, έκρινε ότι σύμφωνα με το Ουγγρικό δίκαιο, είναι δυνατόν, οποιοδήποτε άτομο να τεθεί υπό μυστική παρακολούθηση, καθώς η νομοθεσία δεν περιγράφει τις κατηγορίες προσώπων, των οποίων οι επικοινωνίες, στην πράξη, ενδέχεται να υποκλαπούν. Τουναντίον, ο σχετικός εθνικός νόμος προβλέπει, ότι η πρόταση για την επιβολή του μέτρου επιτήρησης, που υποβάλλεται στον αρμόδιο υπουργό της κυβέρνησης πρέπει να προσδιορίζει, είτε ονομαστικά, **είτε ως φάσμα προσώπων**, το άτομο ή τα άτομα, που αποτελούν τα υποκείμενα της παρακολούθησης ή/και οποιαδήποτε άλλη σχετική πληροφορία, που μπορεί να τα αναγνωρίσει. Ωστόσο, προκαλεί σοβαρή ανησυχία το γεγονός, ότι η έννοια των «ενδιαφερόμενων προσώπων που προσδιορίζονται ... ως μια σειρά προσώπων» μπορεί πράγματι να περιλαμβάνει οποιοδήποτε πρόσωπο και να ερμηνεύεται ως άνοιγμα του δρόμου, για την απεριόριστη παρακολούθηση μεγάλου αριθμού πολιτών. Το Δικαστήριο σημειώνει την απουσία οποιασδήποτε διευκρίνισης στην εσωτερική νομοθεσία, σχετικά με τον τρόπο εφαρμογής αυτής της έννοιας στην πράξη. Για το Δικαστήριο, η κατηγορία είναι υπερβολικά ευρεία, επειδή δεν υπάρχει καμία απαίτηση, κανενός είδους, για τις Αρχές να αποδείξουν την πραγματική ή υποτιθέμενη σχέση, μεταξύ των προσώπων ή της σειράς των «ενδιαφερόμενων» προσώπων και την πρόληψη οποιασδήποτε τρομοκρατικής απειλής. Ας σημειωθεί, ακόμη, ότι κατά το ΕΔΔΑ έννομο συμφέρον, για την ενεργοποίηση της παρεχόμενης από το άρθρο 8 της ΕΣΔΑ προστασίας, διαθέτει όχι μόνον το υποκείμενο, που αποδεδειγμένα οι επικοινωνίες του έχουν αποτελέσει αντικείμενο παρακολούθησης, αλλά και κάθε πρόσωπο, που, με βάση το εθνικό δίκαιο, μπορεί να αποτελέσει, εν δυνάμει, στόχο επιτήρησης[106].

Ως προς την διάρκεια της εφαρμογής του μέτρου, το ΕΔΔΑ επισημαίνει την αναγκαιότητα, εκ των προτέρων, καθορισμού του ακριβούς χρονικού διαστήματος της ισχύος του και των προϋποθέσεων παράτασής του, πέρα από την οποία, δεν θα είναι πλέον αναγκαία

---

[104] ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*, ο.π., §245.

[105] ΕΔΔΑ, 2016, *Szabo and Vissy κατά Ουγγαρίας*, §§ 66-67. Διαθέσιμο σε: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}

[106] ΕΔΔΑ, 1978, *Klass και λοιποί κατά Γερμανίας*, §34. Διαθέσιμη στο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}.

η εφαρμογή του μέτρου[107]. Βέβαια, στην υπόθεση *Kennedy κατά Ην. Βασιλείου*[108], το Δικαστήριο υιοθέτησε μια πιο διαλλακτική θέση, κρίνοντας ότι *«η συνολική διάρκεια τυχόν μέτρων παρακολούθησης θα εξαρτηθεί από την πολυπλοκότητα και τη διάρκεια της εν λόγω έρευνας και, υπό την προϋπόθεση ότι υπάρχουν επαρκείς εγγυήσεις, δεν είναι παράλογο να αφεθεί το θέμα αυτό στη διακριτική ευχέρεια των αρμόδιων εγχώριων αρχών.»*

Όπως, περαιτέρω, έχει αποφανθεί το ΕΔΔΑ, ενόψει του αντικτύπου της επιβολής του μέτρου επιτήρησης στα θεμελιώδη δικαιώματα, η ύπαρξη προηγούμενης άδειας δικαστικού οργάνου, που διατάσσει αυτήν, αποτελεί σημαντικό εχέγγυο για την νομιμότητά της, καθώς χρησιμεύει στον περιορισμό της διακριτικής ευχέρειας των αρχών επιβολής του νόμου στην ερμηνεία των γενικών όρων, μέσω μιας καθιερωμένης δικαστικής ερμηνείας των όρων ή μια καθιερωμένη πρακτική για την επαλήθευση του, κατά πόσον υπάρχουν επαρκείς λόγοι, για την παρακολούθηση των επικοινωνιών ενός συγκεκριμένου ατόμου σε κάθε περίπτωση[109]. Κατά το ΕΔΔΑ, *«ο δικαστικός έλεγχος προσφέρει κατά κανόνα, τις πλέον ακλόνητες εγγυήσεις ανεξαρτησίας, αμεροληψίας και τήρησης της ορθής διαδικασίας.»*[110]

Το Δικαστήριο έχει επίσης υπογραμμίσει τη σημασία μιας Αρχής, που έχει την εξουσία να εγκρίνει τη χρήση μυστικής παρακολούθησης, η οποία να είναι σε θέση να επαληθεύει *«την ύπαρξη εύλογης υποψίας κατά του εν λόγω προσώπου, ιδίως εάν υπάρχουν πραγματικές ενδείξεις για την υποψία ότι το, εν λόγω, πρόσωπο σχεδιάζει, διαπράττει ή έχει διαπράξει εγκληματικές πράξεις ή άλλες πράξεις, που ενδέχεται να οδηγήσουν σε μέτρα μυστικής παρακολούθησης»* και *«εάν η αιτούμενη παρακολούθηση πληροί την απαίτηση της «αναγκαιότητας σε μια δημοκρατική κοινωνία»... για παράδειγμα, εάν είναι δυνατόν να επιτευχθούν οι στόχοι με λιγότερο περιοριστικά μέσα»*[111].

Η εν λόγω επαλήθευση, μαζί με την απαίτηση να αναφέρονται οι σχετικοί λόγοι στις αποφάσεις, με τις οποίες επιτρέπεται η μυστική παρακολούθηση, αποτελούν σημαντική

---

[107] ΕΔΔΑ, 1978, *Klass και λοιποί κατά Γερμανίας*, ο.π., §52.
[108] ο.π. §161.
[109] ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*, ο.π., § 249 &
ΕΔΔΑ, 2016, *Szabo and Vissy κατά Ουγγαρίας*, ο.π. § 73.
[110] ΕΔΔΑ, 2021, *Centrum för Rättvisa κατά Σουηδίας*, § 105. Διαθέσιμη σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210078%22]}.
[111] ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*, ο.π., § 260.

εγγύηση, διασφαλίζοντας ότι τα μέτρα δεν διατάσσονται τυχαία, παράτυπα ή χωρίς την δέουσα και κατάλληλη εξέταση[112]. Ως εκ τούτου, η έγκριση και η παράταση ενός μέτρου τηλεφωνικής παρακολούθησης δεν πρέπει να είναι αβάσιμη ή «γενική» ή «διερευνητική»[113]. Η διαδικασία αδειοδότησης, για την επιβολή του μέτρου επιτήρησης, αποτελεί σημαντικό κριτήριο για την αξιολόγηση, κατά πόσον η μυστική παρακολούθηση δεν διατάσσεται τυχαία, παράνομα ή χωρίς την δέουσα και κατάλληλη εξέταση[114]. Όταν ένα σύστημα επιτρέπει στις μυστικές υπηρεσίες και την αστυνομία να παρακολουθούν άμεσα τις επικοινωνίες οποιουδήποτε πολίτη, χωρίς να απαιτείται από αυτούς να επιδείξουν άδεια παρακολούθησης στον πάροχο υπηρεσιών επικοινωνιών ή σε οποιονδήποτε άλλον, η ανάγκη για εγγυήσεις κατά της αυθαιρεσίας και της κατάχρησης φαίνεται ιδιαίτερα έντονη[115].

Εκτός από δικαστικό όργανο, που διαθέτει τις εγγυήσεις αμερόληπτης και ανεξάρτητης κρίσης, θα μπορούσε, κατά το ΕΔΔΑ, και έτερος ανεξάρτητος, από την εκτελεστική εξουσία, φορέας, να διατάξει την επιβολή του μέτρου της επιτήρησης[116].

Το ΕΔΔΑ τονίζει ακόμη, την σπουδαιότητα εποπτείας του βαθμού συμμόρφωσης προς τις επιταγές του νόμου, κατά την εφαρμογή του μέτρου, από ανεξάρτητη εποπτική Αρχή[117], καθώς οι αξίες μιας δημοκρατικής κοινωνίας πρέπει να ακολουθούνται όσο το δυνατόν πιο πιστά στις διαδικασίες εποπτείας, ώστε να μην υπερβαίνονται τα όρια της αναγκαιότητας, κατά την έννοια του άρθρου 8 της ΕΣΔΑ, ενόψει του γεγονότος, ότι η διαδικασία της παρακολούθησης λαμβάνει χώρα εν αγνοία του υποκειμένου και συνεπώς, η δυνατότητα αποτελεσματικής δικαστικής προσφυγής εκ μέρους του είναι αδύνατη[118].

Ιδιαίτερη βαρύτητα, αποδίδει το ΕΔΔΑ στο δικαίωμα ενημέρωσης του θιγόμενου προσώπου. Προφανώς η γνωστοποίηση της επιτήρησης δεν θα μπορούσε να πραγματοποιηθεί προτού παύσει η εφαρμογή της, καθώς τούτο θα αναιρούσε πλήρως τον σκοπό του μέτρου, για

---

[112] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 655.
[113] ΕΔΔΑ, 2022, *Adomaitis κατά Λιθουανίας*, § 85.
[114] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 675.
[115] ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*, ο.π., § 270
[116] ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*, ο.π., § 258.
[117] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 683.
[118] ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*, ο.π., § 233.

την εκπλήρωση του οποίου η τήρηση της μυστικότητας αποτελεί απαραίτητη προϋπόθεση. Δεν αρκεί, όμως, να έχει παύσει η ισχύς του μέτρου, αλλά επιπροσθέτως, θα πρέπει να μην υφίσταται κίνδυνος ματαίωσης του μακροπρόθεσμου σκοπού του[119]. Όπως σημειώνει το ΕΔΔΑ, το ζήτημα της επακόλουθης κοινοποίησης των μέτρων παρακολούθησης συνδέεται άρρηκτα με την αποτελεσματικότητα των ένδικων μέσων, ενώπιον των δικαστηρίων και, ως εκ τούτου, με την ύπαρξη αποτελεσματικών εγγυήσεων κατά της κατάχρησης εξουσιών παρακολούθησης[120]. Στην υπόθεση *Ekimdzhiev και λοιποί κατά Βουλγαρίας*[121], το Δικαστήριο παρατήρησε ότι στη Βουλγαρία υπήρχε απαίτηση ενημέρωσης του υποκειμένου της παρακολούθησης, μόνο εάν η παρακολούθηση διεξαγόταν παράνομα, ενώ σύμφωνα με τη νομολογία του Δικαστηρίου, η εν λόγω ενημέρωση, ελλείψει προσφυγής, χωρίς προηγούμενη ειδοποίηση, ήταν απαραίτητη σε όλες τις περιπτώσεις, μόλις αυτή μπορούσε να γίνει χωρίς να τεθεί σε κίνδυνο ο σκοπός της παρακολούθησης[122].

Ιδιαιτέρως κρίσιμη, όμως, κατά το ΕΔΔΑ, για την αξιολόγηση της νομιμότητας επιβολής του μέτρου επιτήρησης και συμβατότητας αυτής με το ενωσιακό δίκαιο παραμένει η εφαρμογή της Αρχής της αναλογικότητας, κατ' άρθρο 52 του ΧΘΔΕΕ, η οποία στην εθνική έννομη τάξη κατοχυρώνεται στο άρθρο 25 του Συντάγματος.

Η χρήση κατασκοπευτικού λογισμικού συνήθως δικαιολογείται με την επίκληση της εθνικής ασφάλειας ή σκοπών επιβολής του νόμου. Ωστόσο, φαίνεται ότι σε πολλές περιπτώσεις το κατασκοπευτικό λογισμικό χρησιμοποιείται για άλλους σκοπούς, που συχνά σχετίζονται με κομματικούς - πολιτικούς στόχους ή με την καταστολή της κοινωνικής και πολιτικής διαφωνίας. Έχει αναγνωριστεί ότι πολλά κράτη έχουν χρησιμοποιήσει την εθνική ασφάλεια ως κυνικό νομικό πρόσχημα, για να περιορίσουν την ελευθερία της έκφρασης, να νομιμοποιήσουν τα βασανιστήρια και άλλες μορφές κακομεταχείρισης και να φιμώσουν - εκφοβίσουν τις μειονότητες, τους ακτιβιστές και την πολιτική αντιπολίτευση. Ειδικότερα, υπάρχουν εκτενείς αποδείξεις ότι το Pegasus χρησιμοποιείται, για να στοχεύσει άτομα, που δεν έχουν καμία σχέση

---

[119] Ibidem, § 287.
[120] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 670.
[121] ο.π.,§ 349.
[122] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 677.

με σοβαρά εγκλήματα ή απειλές για την εθνική ασφάλεια, όπως πολιτικοί αντίπαλοι, ακτιβιστές ανθρωπίνων δικαιωμάτων, δικηγόροι και δημοσιογράφοι. Για να αποφευχθεί μια αλόγιστη χρήση της έννοιας της εθνικής ασφάλειας, η έννοια αυτή θα πρέπει να νοείται περιοριστικά και να διακρίνεται από την έννοια της εσωτερικής ασφάλειας, η οποία έχει ευρύτερο πεδίο εφαρμογής, και περιλαμβάνει την πρόληψη κινδύνων για μεμονωμένους πολίτες, και ιδίως την επιβολή του ποινικού δικαίου[123].

Το ΕΔΔΑ έχει κατ' επανάληψη επισημάνει ότι το μέτρο της επιτήρησης πρέπει να επιβάλλεται υπό συνθήκες «αυστηρής αναγκαιότητας» (strictly necessary), δηλαδή να είναι απολύτως απαραίτητο, για την προστασία των δημοκρατικών θεσμών και, ειδικότερα, για την απόκτηση ζωτικών πληροφοριών σε μια μεμονωμένη επιχείρηση. Διαφορετικά, θα υπάρξει «κατάχρηση» εκ μέρους των Αρχών[124]. Το Δικαστήριο διευκρινίζει, περαιτέρω, την απαίτηση της αυστηρής αναγκαιότητας, δηλώνοντας ότι η έννοια της, για τους σκοπούς του Άρθρου 8, σημαίνει, ότι η παρέμβαση πρέπει να αντιστοιχεί σε μια επιτακτική κοινωνική ανάγκη και, ειδικότερα, πρέπει να παραμένει ανάλογη με τον επιδιωκόμενο θεμιτό στόχο. Κατά τον καθορισμό του, κατά πόσον μια παρέμβαση ήταν «αναγκαία», το Δικαστήριο θα λάβει υπόψη Του, το περιθώριο εκτίμησης, που αφήνεται στις κρατικές αρχές, αλλά είναι καθήκον του εκάστοτε κράτους να αποδείξει την ύπαρξη μιας επιτακτικής κοινωνικής ανάγκης πίσω από την παρέμβαση.

Κατά το ΕΔΔΑ, προκειμένου να προσδιοριστεί, εάν μια συγκεκριμένη παραβίαση του άρθρου 8 της ΕΣΔΑ είναι «αναγκαία σε μια δημοκρατική κοινωνία», σταθμίζονται τα συμφέροντα του κράτους μέλους με το δικαίωμα του αιτούντος. Ο όρος «αναγκαία» σε αυτό το πλαίσιο δεν έχει την ευελιξία εκφράσεων, όπως «χρήσιμος», «εύλογος» ή «επιθυμητός», αλλά υπονοεί την ύπαρξη «πιεστικής κοινωνικής ανάγκης» για την, εν λόγω, παρέμβαση. Εναπόκειται στις εθνικές αρχές να προβούν στην αρχική αξιολόγηση της πιεστικής κοινωνικής ανάγκης σε κάθε περίπτωση· κατά συνέπεια, τους αφήνεται περιθώριο εκτίμησης. Ωστόσο, η απόφασή τους εξακολουθεί να υπόκειται σε έλεγχο από το Δικαστήριο. Ένας περιορισμός σε

[123]Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 - January 2023, «*The impact of Pegasus on fundamental rights and democratic processes*», ο.π.
[124] ΕΔΔΑ, 2016, *Szabo and Vissy κατά Ουγγαρίας*, ο.π. §§ 72 -73.

ένα δικαίωμα της Σύμβασης δεν μπορεί να θεωρηθεί «αναγκαίος σε μια δημοκρατική κοινωνία», εκτός εάν, μεταξύ άλλων, είναι ανάλογος με τον επιδιωκόμενο θεμιτό στόχο[125].

Η έννοια της αναγκαιότητας συνέχεται απόλυτα προς την Αρχή της αναλογικότητας (που συνιστά τον λεγόμενο περιορισμό των περιορισμών), σύμφωνα με την οποία το μέτρο περιορισμού του δικαιώματος, θα πρέπει να είναι αναγκαίο για την επίτευξη υπέρτερου νόμιμου σκοπού (λ.χ. δημοσίου συμφέροντος), πρόσφορο, δηλαδή κατάλληλο να επιτύχει το επιδιωκόμενο αποτέλεσμα, και το ηπιότερο, ανάμεσα σε άλλα μέτρα, δίχως να αποβαίνει δυσανάλογο.

4.2 Το φαινόμενο των μαζικών παρακολουθήσεων

Οι μαζικές (άλλως μη στοχευμένες) παρακολουθήσεις *("bulk inteceptions")* έχουν απασχολήσει ιδιαιτέρως την νομολογία του ΕΔΔΑ και του ΔΕΕ, ιδίως μετά τις αποκαλύψεις του Edward Snowden, πρώην υπαλλήλου της Υπηρεσίας Εθνικής Ασφάλειας (NSA)των Η.Π.Α. και της CIA, περί εντατικής χρήσης εργαλείων μαζικής παρακολούθησης από τις Αμερικανικές και Βρετανικές Αρχές. Η στάση τόσο του ΕΔΔΑ, όσο και του ΔΕΕ, ως προς το ζήτημα των μαζικών παρακολουθήσεων θα αναδειχθεί παρακάτω, μέσα από την θεώρηση σημαντικών υποθέσεων, οι οποίες ήχθησαν ενώπιον των Δικαστηρίων τούτων.

Στην υπόθεση *Big Brother Watch και λοιποί κατά Ην. Βασιλείου,* το ΕΔΔΑ, κατά την αρχική του κρίση (συνεδριάσαν σε Τμήμα Ελάσσονος Συνθέσεως), υιοθέτησε μια πιο φιλελεύθερη προσέγγιση, σύμφωνα με την οποία οι κυβερνήσεις μπορούν να εφαρμόζουν εργαλεία μαζικών παρακολουθήσεων, χωρίς να παραβιάζουν τις διατάξεις της ΕΣΔΑ, καθώς η απόφαση για την διενέργεια μαζικής παρακολούθησης, με σκοπό τον εντοπισμό αγνώστων απειλών (unknown threats) για την εθνική ασφάλεια, εμπίπτει στο ευρύ περιθώριο εκτίμησης, που διαθέτουν τα κράτη, κατά την επιλογή του καλύτερου δυνατού τρόπου επίτευξης του θεμιτού στόχου της προστασίας της εθνικής ασφάλειας. Με την σκέψη αυτή, το ΕΔΔΑ επανέλαβε την κρίση, που είχε διαμορφώσει στην υπόθεση *Weber and Saravia κατά Γερμανίας*[126], σύμφωνα με την οποία, προκειμένου η εφαρμογή μαζικών παρακολουθήσεων να κριθεί νόμιμη, θα πρέπει να

[125] European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, ο.π., § 34.
[126] Διαθέσιμη σε: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-76586%22]}.

πληρούνται έξι (6) ελάχιστες απαιτήσεις (γνωστές ως «*έξι εγγυήσεις Weber*»), κατά τις οποίες, το εθνικό δίκαιο οφείλει να καθορίζει: α) τη φύση των αδικημάτων, που μπορούν να οδηγήσουν σε εντολή παρακολούθησης, β) έναν ορισμό των κατηγοριών ατόμων, που υπόκεινται σε παρακολούθηση των επικοινωνιών τους, γ) ένα όριο στη διάρκεια της παρακολούθησης, δ) τη διαδικασία, που πρέπει να ακολουθείται για την εξέταση, τη χρήση και την αποθήκευση των δεδομένων που λαμβάνονται, ε) τις προφυλάξεις, που πρέπει να λαμβάνονται κατά την κοινοποίηση των δεδομένων σε άλλα μέρη και στ) τις περιστάσεις, υπό τις οποίες τα υποκλαπέντα δεδομένα μπορούν ή πρέπει να διαγραφούν ή να καταστραφούν. Έτσι το Τμήμα του ΕΔΔΑ, κατέληξε ότι, μολονότι η επιβολή ενός συστήματος μαζικών παρακολουθήσεων δεν αποτελούσε per se παράβαση της ΕΣΔΑ, εντούτοις, διαπίστωσε ότι η ανεξάρτητη εποπτεία της διαδικασίας παρακολούθησης ήταν ανεπαρκής, καθώς και ότι δεν υπήρχαν επαρκείς εγγυήσεις, για την επιλογή των σχετικών δεδομένων επικοινωνίας, παρόλο που τα δεδομένα αυτά θα μπορούσαν να αποκαλύψουν πολλά για τις συνήθειες και τις επαφές ενός ατόμου. Οι ελλείψεις αυτές, κατά το Δικαστήριο, δεν ανταποκρίνονται στις απαιτήσεις της «ποιότητας του νόμου» και δεν μπορούσαν να δικαιολογήσουν παρέμβαση, που «ήταν αναγκαία σε μια δημοκρατική κοινωνία». Περαιτέρω, σημείωσε ότι το δίκαιο της Ευρωπαϊκής Ένωσης απαιτεί το καθεστώς, που επιτρέπει την πρόσβαση σε δεδομένα, που κατέχουν οι πάροχοι υπηρεσιών επικοινωνιών, πρέπει να περιορίζεται με το σκοπό της καταπολέμησης του "σοβαρού εγκλήματος" και η πρόσβαση σε πληροφορίες να υπόκειται σε προηγούμενη εξέταση από δικαστήριο ή ανεξάρτητο διοικητικό όργανο. Το δίκαιο, όμως, του Ην. Βασιλείου, προέβλεπε τέτοιο σύστημα παρακολούθησης, το οποίο δεν περιλάμβανε τις, εν λόγω, διασφαλίσεις.

Το Τμήμα Μείζονος Συνθέσεως του ΕΔΔΑ, το οποίο απεφάνθη οριστικώς, συμφώνησε σε μεγάλο βαθμό με την προηγηθείσα κρίση του Τμήματος Ελάσσονος Συνθέσεως και προσέθεσε ακόμη δύο απαιτήσεις (στις προηγούμενες έξι (6)): α) την εποπτεία της εφαρμογής μέτρων παρακολούθησης και β) την γνωστοποίηση της επιβολής τους, καθώς και των διαθέσιμων ενδίκων μέσων.

Σύμφωνα με το ΕΔΔΑ[127], ο κίνδυνος κατάχρησης των συστημάτων μαζικής παρακολούθησης είναι ορατός, γι' αυτό και προκειμένου να ελαχιστοποιηθεί, η διαδικασία θα πρέπει να υπόκειται σε διασφαλίσεις από άκρο σε άκρο, που σημαίνει ότι, σε εθνικό επίπεδο, θα πρέπει να γίνεται αξιολόγηση σε κάθε στάδιο της διαδικασίας της αναγκαιότητας και της αναλογικότητας των μέτρων, που λαμβάνονται, ότι η μαζική παρακολούθηση θα πρέπει να υπόκειται σε ανεξάρτητη άδεια εξ αρχής, όταν ορίζονται το αντικείμενο και το πεδίο εφαρμογής της επιχείρησης και ότι η επιχείρηση θα πρέπει να υπόκειται σε εποπτεία και ανεξάρτητη, εκ των υστέρων, αναθεώρηση[128].

Το γεγονός, ωστόσο, ότι το ΕΔΔΑ, θέτοντας οκτώ (8) συνολικά απαιτήσεις, αποδίδει ιδιαίτερη έμφαση στην διαδικασία της μαζικής παρακολούθησης και τις εγγυήσεις κατά της κατάχρησης, που παρέχει το εθνικό δίκαιο, ώστε να καθορίσει, αν το σύστημά της, είναι συμβατό με την ΕΣΔΑ, δεν αποτελεί σαφή προσέγγιση, αν οι ανωτέρω απαιτήσεις είναι υποχρεωτικές. Οι Δικαστές Lemmens, Vehabović και Bošnjak υποστήριξαν ότι τα νέα κριτήρια δεν χρησιμεύουν σαφώς ως «αυτοτελή ελάχιστα πρότυπα», ούτε «ορίζουν ελάχιστες εγγυήσεις» στο εσωτερικό δίκαιο, παραλείποντας να προβλέψουν «οποιαδήποτε σαφή ουσιαστική προστασία ενός ατόμου από δυσανάλογες παρεμβάσεις» στα δικαιώματά του[129].

Η χαλαρή και διαδικαστική προσέγγιση της πλειοψηφίας των Δικαστών στην υπόθεση *Big Brother Watch* ενισχύει το «αναπόφευκτο» της μαζικής παρακολούθησης, μη αμφισβητώντας την αποτελεσματικότητα ή την αναλογικότητα των γενικών καθεστώτων παρακολούθησης και υποθέτοντας, μάλλον, την αναγκαιότητα και την αποτελεσματικότητά τους για τη διασφάλιση της εθνικής ασφάλειας[130].

Το ΕΔΔΑ, φαίνεται να ελαστικοποιεί τα κριτήριά του, αρκούμενο για την επιβολή του μέτρου των μαζικών παρακολουθήσεων, στην επίκληση της έννοιας των «απροσδιόριστων απειλών» για την εθνική ασφάλεια. Δημιουργείται, όμως, εύλογα, εννοιολογική ασάφεια ως

---

[127] Ας σημειωθεί ότι, εκτός από την απόφαση *Big Brother Watch και λοιποί κατά Ην. Βασιλείου*, και στην απόφαση *Centrum för Rättvisa κατά Σουηδίας* , το ΕΔΔΑ, κατέληξε σε παρόμοια κρίση.

[128]ΕΔΔΑ, 2021, *Big Brother Watch και λοιποί κατά Ην. Βασιλείου*, ο.π. § 350.

[129] ΕΔΔΑ, 2021, *Big Brother Watch και λοιποί κατά Ην. Βασιλείου*, ο.π. §§ 13-14 of JOINT PARTLY CONCURRING OPINION OF JUDGES LEMMENS, VEHABOVIĆ AND BOŠNJAK.

[130] «*Big Brother Watch and Others v. the United Kingdom*», 28.2.2022, Cambridge University Press. Διαθέσιμο σε: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/big-brother-watch-and-others-v-the-united-kingdom/024BF9DDDFA0C882358B052845230352.

προς τον όρο των «απροσδιόριστων απειλών», η οποία (ασάφεια) συνιστά χαλάρωση του κριτηρίου της ύπαρξης εύλογων υποψιών[131], ως προϋπόθεση για την επιβολή μέτρων τηλεφωνικής παρακολούθησης. Αυτό μπορεί να αναγνωσθεί και ως υποχώρηση του ΕΔΔΑ υπέρ της επιχειρησιακής αποτελεσματικότητας των διοικητικών μηχανισμών πρόληψης κατ' επίκληση της ανάγκης για έγκαιρη συλλογή κρίσιμων πληροφοριών, προς αποτροπή εγκληματικών ενεργειών, η οποία υποχώρηση, όμως, εγείρει προβληματισμό, σε σχέση με τα minima του κράτους δικαίου[132].

Το ΕΔΔΑ, τονίζοντας ότι τα προηγμένα τεχνολογικά μέσα, έχουν χρησιμοποιηθεί από τρομοκράτες και εγκληματίες, προκειμένου να αποφύγουν τον εντοπισμό τους, επιχειρηματολογώντας για την αποτελεσματικότητα του μέτρου και επαινώντας την προληπτική του λειτουργία, παρείδε το γεγονός ότι τα συστήματα επιτήρησης, μπορούν να χρησιμοποιηθούν από κρατικές Αρχές, όχι μόνο για τον εντοπισμό τρομοκρατών και εγκληματιών, αλλά και για την παρακολούθηση των ατόμων, εν γένει, με τον βαθμό κινδύνου καταχρήσεων υψηλό. Το δόγμα του «περιθωρίου εκτίμησης», επιπροσθέτως, δεν δύναται να υπερκαλύψει την εφαρμογή της Αρχής της αναλογικότητας και την στάθμιση μεταξύ ατομικών δικαιωμάτων και συλλογικών σκοπών[133]. Όπως έχει παρατηρηθεί, η κρίση του ΕΔΔΑ στις υποθέσεις *Big Brother Watch και λοιποί κατά Ην. Βασιλείου* και *Centrum för Rättvisa κατά Σουηδίας*, υποδηλώνει την τάση της κοινωνίας να κινείται προς ένα «παγκόσμιο πανοπτικό», επιβεβαιώνοντας λέξη προς λέξη το σενάριο που περιέγραψε ο Foucault. Η θέση του ΕΔΔΑ και στις δύο, ως άνω, υποθέσεις, σε περίπτωση, που οι δικαστές προτιμήσουν την αποτελεσματικότητα από την ακεραιότητα και μειώσουν το όριο των απαιτήσεων, για την προστασία της ιδιωτικής ζωής, θα μπορούσε κάλλιστα να αποβεί μοιραία[134].

---

131 ΕΔΔΑ, 2009, *Iordachi και λοιποί κατά Μολδαβίας*, § 51. Διαθέσιμη σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-91245%22]}.

132 Παπανικολάου Α. (2020), «*Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: Επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*», Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης, σελ. 14. Διαθέσιμο στο: https://www.constitutionalism.gr/2020-07-papanikolaou-aporito-epikinonias/. [Ημ. Πρόσβασης 14.7.2025]

133 Rusinova V. (2019), *"A European perspective on Privacy and mass Surveillance at the Crossroads"*, Basic Research Porgram, Working Papers, Series: Law, WP BRP 87/LAW/2019, σελ. 16-17. Διαθέσιμο σε: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347711. [Ημ. Πρόσβασης 13.8.2025]

134 Ibidem, σελ. 20.

Στην υπόθεση *Szabo and Vissy κατά Ουγγαρίας*, το ΕΔΔΑ έκρινε ότι η νομοθεσία της Ουγγαρίας, που προέβλεπε την ίδρυση Αντιτρομοκρατικής Υπηρεσίας, με αρμοδιότητα τη συλλογή μυστικών πληροφοριών και συγκεκριμένα, τις κρυφές κατ' οίκον έρευνες και την παρακολούθηση με μαγνητοσκόπηση, το άνοιγμα των επιστολών και πακέτων, καθώς και τον έλεγχο και την καταγραφή του περιεχομένου των ηλεκτρονικών ή ψηφιακών επικοινωνιών, χωρίς τη συγκατάθεση του υποκειμένου, παραβιάζει τη διάταξη του άρθρου 8 της ΕΣΔΑ, με την οποία προστατεύεται η ιδιωτική και οικογενειακή ζωή και η αλληλογραφία του ατόμου. Και τούτο, διότι η, εν λόγω, νομοθεσία δεν προέβλεπε επαρκείς εγγυήσεις, για την αποφυγή καταχρήσεων, ενόψει του, ότι στο πλαίσιο αυτό εντάσσονται όλοι οι πολίτες της Ουγγαρίας και είναι δυνατή η υποκλοπή τεράστιου όγκου δεδομένων, αφορώντων ακόμα και πρόσωπα, που δεν περιλαμβάνονται στην αρχική έρευνα. Περαιτέρω, το Δικαστήριο επεσήμανε την σπουδαιότητα δικαστικής εποπτείας της διαδικασίας επιτήρησης και ιδίως την ανάγκη προηγούμενης δικαστικής άδειας, που διατάσσει το μέτρο, καθώς η εποπτεία από ένα πολιτικό πρόσωπο, μέλος της εκτελεστικής εξουσίας, δεν παρέχει εγγυήσεις αμεροληψίας και ανεξαρτησίας. Περαιτέρω, το Δικαστήριο δέχτηκε ότι θα μπορούσαν να προκύψουν καταστάσεις εξαιρετικά επείγουσας ανάγκης, στις οποίες η απαίτηση για προηγούμενο δικαστικό έλεγχο θα ενείχε τον κίνδυνο απώλειας πολύτιμου χρόνου. Τόνισε, ωστόσο, ότι σε τέτοιες περιπτώσεις, οποιαδήποτε μέτρα παρακολούθησης, που έχουν εγκριθεί εκ των προτέρων από μη δικαστική αρχή, έπρεπε να υπόκεινται σε δικαστικό έλεγχο μετά το πέρας της διαδικασίας. Το Δικαστήριο σημείωσε, ακόμη, ότι, βάσει του ουγγρικού νόμου, η εκτελεστική εξουσία ήταν υποχρεωμένη να λογοδοτεί γενικά για τέτοιες επιχειρήσεις σε κοινοβουλευτική επιτροπή. Ωστόσο, δεν πείστηκε, ότι αυτή η διαδικασία υποβολής εκθέσεων, η οποία δεν παρουσιαζόταν δημόσια, ήταν σε θέση να ελέγχει αποτελεσματικά την λειτουργία των οργάνων παρακολούθησης. Επιπλέον, η εσωτερική νομοθεσία δεν προέβλεπε μηχανισμό δικαστικού ελέγχου, που θα μπορούσε να ενεργοποιηθεί από όσους υπόκεινται σε μυστική παρακολούθηση, καθώς η διαδικασία υποβολής καταγγελιών δεν προέβλεπε κανενός είδους μεταγενέστερη κοινοποίηση των μέτρων παρακολούθησης στους πολίτες που υπόκεινται σε αυτά. Επιπλέον, οι καταγγελίες τύγχαναν διερεύνησης από τον Υπουργό Εσωτερικών, η κρίση του οποίου δεν παρείχε εχέγγυα ανεξαρτησίας.

Αξιοσημείωτη, τέλος, χαρακτηρίζεται η κρίση του ΕΔΔΑ, στην υπόθεση *Zakharov κατά Ρωσίας*, όπου κατά το Δικαστήριο, μολονότι δεν απεδείχθη ότι ο προσφεύγων είχε γίνει στόχος παρακολούθησης από τις Ρωσικές Αρχές, και μόνο η πρόβλεψη του εθνικού νόμου, σύμφωνα με την οποία ο προσφεύγων (εκδότης και πρόεδρος ΜΚΟ), διέτρεχε κίνδυνο να υποβληθεί σε καθεστώς παρακολούθησης, αρκούσε για την δυνατότητα αμφισβήτησης της νομιμότητας του μέτρου, ενώπιον του Δικαστηρίου, ιδίως στην περίπτωση, που το εθνικό δίκαιο δεν προβλέπει αποτελεσματική δικαστική προστασία και η ανησυχία κατάχρησης της δυνατότητας επιτήρησης είναι διάχυτη.

Καθίσταται σαφές, ότι οι μαζικές παρακολουθήσεις, αποτελούν πλέον σημαντικό εργαλείο, των κρατικών Αρχών για την πρόληψη και καταστολή της τρομοκρατίας και του οργανωμένου εγκλήματος, εν γένει. Στην παγίωση της θέσης αυτής συνέβαλε σε μεγάλο βαθμό το κύμα τρομοκρατικών επιθέσεων, με τις οποίες ήρθε αντιμέτωπη η Ευρώπη και οι Η.Π.Α., ήδη από τις Αρχές της δεκαετίας του 2000. Ωστόσο, οι αποκαλύψεις Snowden, για το μέγεθος των προγραμμάτων μαζικής παρακολούθησης από κρατικές μυστικές υπηρεσίες, έθεσαν στο τραπέζι την ανάγκη οριοθέτησης της χρήσης των συστημάτων αυτών, υπό τον κίνδυνο κατάχρησης και αυθαιρεσιών, που προσβάλλουν θεμελιώδη δικαιώματα των ανθρώπων.

5. ΣΥΓΧΡΟΝΕΣ ΠΡΟΚΛΗΣΕΙΣ

5.1 Η περίπτωση των υποκλοπών στην Ελλάδα[135, 136]

Το ζήτημα της νομιμότητας της χρήσης λογισμικών κατασκοπείας κατέστη πιο επίκαιρο από ποτέ στην εγχώρια έννομη τάξη, όταν, τον Ιούλιο του 2022, ο αρχηγός (και τότε Ευρωβουλευτής) αντιπολιτευόμενου κόμματος, Ν. Ανδρουλάκης, υπέβαλε ενώπιον της Εισαγγελίας του Αρείου Πάγου, μηνυτήρια αναφορά για απόπειρα παγίδευσης του κινητού του τηλεφώνου με το παράνομο λογισμικό Predator, η οποία διαπιστώθηκε κατόπιν ελέγχου της τηλεφωνικής του συσκευής από την Υπηρεσία Ψηφιακής Ασφάλειας του Ευρωπαϊκού Κοινοβουλίου (CERT-EU). Είχε προηγηθεί η περίπτωση του δημοσιογράφου κ. Κουκάκη, το κινητό τηλέφωνο του οποίου είχε επίσης μολυνθεί από το κακόβουλο λογισμικό Predator και παρακολουθούνταν για διάστημα αρκετών μηνών, σύμφωνα με σχετική έκθεση του Διεπιστημονικού Εργαστηρίου Citizen Lab του Πανεπιστημίου του Τορόντο. Μετά την καταγγελία του ανωτέρω πολιτικού αρχηγού, αποκαλύφθηκε ότι η ΕΥΠ φέρεται να είχε στοχεύσει δύο δικούς της υπαλλήλους με κατασκοπευτικό λογισμικό. Ακολούθησε η αποκάλυψη από τα ελληνικά μέσα ενημέρωσης μιας λίστας με 33 στόχους του Predator, όλοι εκ των οποίων ήταν προσωπικότητες υψηλού προφίλ. Η λίστα - η οποία ούτε επιβεβαιώθηκε, ούτε διαψεύστηκε από την κυβέρνηση ή από τους παρακολουθούμενους - περιλαμβάνει ονόματα προσώπων, από τον χώρο της πολιτικής, των επιχειρήσεων και των μέσων μαζικής ενημέρωσης.

Η ελληνική κυβέρνηση παραδέχτηκε, ότι η ΕΥΠ πράγματι παρακολουθούσε τους κ. κ. Ανδρουλάκη και Κουκάκη, αλλά αρνήθηκε ότι είχε χρησιμοποιήσει ή αγοράσει ποτέ το λογισμικό Predator. Επιπλέον, κατά τη διάρκεια αυτής της περιόδου, ήρθαν στο φως και άλλες

---

[135] *«Τι δήλωσε ο Ν. Ανδρουλάκης για την παρακολούθηση του τηλεφώνου του και τη μήνυση που κατέθεσε»* (26.7.2022). Διαθέσιμο σε: https://www.inewsgr.com/421/ti-dilose-o-nandroulakis-gia-tin-parakolouthisi-tou-tilefonou-tou-kai-ti-minysi-pou-katethese.htm.[Ημ. Πρόσβασης 8.8.2025]

[136] Έκθεση Ευρωπαϊκού Κοινοβουλίου για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA). Διαθέσιμη σε: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html#_section1. [Ημ. Πρόσβασης 8.8.2025]

περιπτώσεις παρακολούθησης δημοσιογράφων από την ΕΥΠ, χωρίς ωστόσο μέχρι σήμερα, οι επίσημοι λόγοι για την παρακολούθηση να έχουν αποκαλυφθεί.

Ο Πρωθυπουργός, μάλιστα, δήλωσε διφορούμενα, ότι η παρακολούθηση του Ν. Ανδρουλάκη ήταν «νόμιμη», αλλά «πολιτικά απαράδεκτη». Δεν έκανε καμία αναφορά στην παρακολούθηση του Κουκάκη, ούτε στις άλλες φερόμενες υποθέσεις. Ισχυρίστηκε, ακόμη, ότι δεν γνώριζε την παρακολούθηση, αλλά, αν γνώριζε, δεν θα την είχε επιτρέψει. Σύμφωνα με την επίσημη δήλωση του κυβερνητικού εκπροσώπου, μόλις ο Πρωθυπουργός έλαβε γνώση της «νόμιμης παρακολούθησης» του πολιτικού του αντιπάλου, έγιναν προσπάθειες εκ μέρους της Κυβέρνησης, ώστε να ενημερωθεί πλήρως ο κ. Ανδρουλάκης κατ' ιδίαν για τους λόγους, που κρύβονταν πίσω από αυτήν.

Τόσο η ΕΥΠ, όσο και η Κυβέρνηση αρνήθηκαν κατηγορηματικά ότι το Predator έχει αγοραστεί ή χρησιμοποιηθεί ποτέ από τις Ελληνικές Αρχές. Ελλείψει οποιωνδήποτε αποδεικτικών στοιχείων σχετικά με την ταυτότητα του αγοραστή και του χρήστη του Predator, δεν μπορεί να διαπιστωθεί με βεβαιότητα, εάν ή πώς η Κυβέρνηση ή άλλος φορέας απέκτησε το Predator. Ο αρχικός ισχυρισμός της Κυβέρνησης ότι μη κρατικός φορέας, δηλαδή ιδιώτης, ήταν υπεύθυνος για τις υποκλοπές (και τις απόπειρες αυτών) κατά των κ. κ. Κουκάκη και Ανδρουλάκη, παραμένει αναπόδεικτος και δεν μπορεί να δικαιολογηθεί από την επιλογή των στόχων.

Η έρευνα της ΑΔΑΕ, που ακολούθησε της καταγγελίας του κ. Ανδρουλάκη, επιβεβαίωσε ότι το κινητό του τηλέφωνο είχε αποτελέσει αντικείμενο επιτήρησης από την ΕΥΠ. Μετά τα ευρήματα αυτά, ο Διοικητής της ΕΥΠ και ο Γ.Γ. του Πρωθυπουργού, υπό την ευθύνη του οποίου είχε υπαχθεί η λειτουργία της ΕΥΠ, παραιτήθηκαν. Ο Διοικητής της ΕΥΠ, μάλιστα, δήλωσε ότι η παρακολούθηση του κ. Ανδρουλάκη ξεκίνησε κατόπιν αιτήματος ξένων Αρχών - και πιο συγκεκριμένα των Υπηρεσιών Πληροφοριών της Αρμενίας και της Ουκρανίας - ενόψει της συμμετοχής του κ. Ανδρουλάκη στην Επιτροπή Διεθνούς Εμπορίου του Ευρωπαϊκού Κοινοβουλίου, η οποία ασχολείται με τις εμπορικές σχέσεις μεταξύ ΕΕ και Κίνας, ισχυρισμό τον οποίο τόσο η Ουκρανία, όσο και η Αρμενία έχουν αρνηθεί.

Ακολούθησαν κι άλλες καταγγελίες εκ μέρους δημοσιογράφων, ότι είχαν στοχοποιηθεί από την ΕΥΠ, οι οποίες, εν τέλει, επιβεβαιώθηκαν από έρευνες της ΑΔΑΕ. Διαπιστώθηκε ακόμη, ότι και ο Αρχηγός των Ελληνικών Ενόπλων Δυνάμεων, ένας εν ενεργεία υπουργός,

αρκετοί αξιωματικοί που ασχολούνται με υποθέσεις όπλων και ένας πρώην σύμβουλος εθνικής ασφάλειας, είχαν, επίσης, τεθεί υπό παρακολούθηση από την ΕΥΠ.

Ας σημειωθεί ότι η Εθνική Αρχή Διαφάνειας (ΕΑΔ), έχουσα αρμοδιότητα πρόληψης, εντοπισμού και διαχείρισης ενεργειών απάτης και διαφθοράς από δημόσιους και ιδιωτικούς φορείς, διεξήγαγε έλεγχο, σχετικά με την φερόμενη αγορά του λογισμικού Predator, από την Ελληνική Κυβέρνηση και την ΕΥΠ. Το παράδοξο είναι ότι η έκθεση, που συνέταξε η ΕΑΔ, εστάλη στην ΕΥΠ (οι ενέργειες της οποίας είχαν αποτελέσει αντικείμενο ελέγχου!!!) προς έγκριση. Εν τέλει, σύμφωνα με το πόρισμα της ΕΑΔ, ούτε η ΕΥΠ, ούτε η Κυβέρνηση είχαν προμηθευτεί ή χρησιμοποιήσει το λογισμικό Predator ή οποιοδήποτε άλλο λογισμικό κατασκοπείας.

Κι ενώ οι αποκαλύψεις για σωρεία παρακολουθήσεων στη χώρα μας, πήραν τη μορφή χιονοστιβάδας, ο κ. Ανδρουλάκης υπέβαλε, ενώπιον του ΣτΕ αίτηση ακυρώσεως κατά της πράξης του Προέδρου της ΑΔΑΕ, δυνάμει της οποίας απερρίφθη το αίτημά του να του γνωστοποιηθούν, κατ' εφαρμογή των διατάξεων των παρ. 4 και 9 του άρθρου 5 του, τότε ισχύοντος αναφορικά με την άρση του επικοινωνιακού απορρήτου, Ν. 2225/1994, η εισαγγελική διάταξη και ο πλήρης φάκελος με το υλικό, που είχε συλλεγεί, μετά την επιβολή σε βάρος του τού μέτρου της άρσης απορρήτου των επικοινωνιών του. Με την υπ' αριθ. 465/2024 απόφασή της[137], η Ολομέλεια του Ανωτάτου Ακυρωτικού, απεφάνθη ότι «*η ενημέρωση του θιγόμενου προσώπου, μετά τη λήξη του μέτρου, και υπό την προϋπόθεση, ότι δεν διακυβεύεται πλέον ο σκοπός για τον οποίο αυτό επιβλήθηκε, αποτελεί απαραίτητο θεσμικό αντίβαρο, στο πλαίσιο του κράτους δικαίου, έναντι του ευρύτατου, κατά ανωτέρω, περιθωρίου εκτίμησης, που διαθέτουν οι κρατικές αρχές να προβαίνουν σε άρση του απορρήτου της επικοινωνίας των πολιτών, όταν ιδιαίτερα σοβαροί λόγοι το επιβάλλουν. Τούτο διότι, σύμφωνα με τις διατάξεις της οδηγίας 2002/58/ΕΚ, όπως ερμηνεύθηκαν από τη νομολογία του ΔΕΕ, η πλήρης απαγόρευση της, εκ των υστέρων, ενημέρωσης του θιγόμενου για την επιβολή του μέτρου της άρσης του απορρήτου για λόγους εθνικής ασφάλειας, ακόμη και όταν δεν υφίσταται πλέον διακινδύνευση του σκοπού για τον οποίο επιβλήθηκε το μέτρο, συνιστά υπέρμετρο και αδικαιολόγητο περιορισμό του απαραβίαστου της επικοινωνίας*»

[137] ΟλΣτΕ 465/2024, ΤΝΠ ΝΟΜΟΣ.

Περαιτέρω, η Ολομέλεια του ΣτΕ, κήρυξε αντισυνταγματική και κατ' επέκταση ανίσχυρη την διάταξη του άρθρου 87 του Ν. 4790/2021, σύμφωνα με την οποία, στην περίπτωση επιβολής του μέτρου άρσης του απορρήτου των επικοινωνιών, για λόγους εθνικής ασφάλειας, προβλέφθηκε η πλήρης απαγόρευση της δυνατότητας ενημέρωσης του θιγόμενου, μετά τη λήξη του μέτρου, ακόμη και όταν δεν υφίσταται διακινδύνευση των σκοπών, που οδήγησαν στην επιβολή του. Η, εν λόγω, νομοθετική πρόβλεψη, αποτελεί υπέρμετρο περιορισμό του απαραβίαστου της επικοινωνίας, που δεν δικαιολογείται στο πλαίσιο της λειτουργίας του Κράτους Δικαίου, και, συνεπώς, αντίκειται στα άρθρα 19 παρ. 1 του Συντάγματος, 5 παρ. 1 και 15 παρ. 1 της οδηγίας 2002/58/ΕΚ, 7, 8 και 11 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και 8 της ΕΣΔΑ. Κατά το Δικαστήριο, για να είναι ορθή και πλήρης η ενημέρωση, θα πρέπει να περιλαμβάνει και «*το αιτιολογικό της επιβολής του μέτρου της άρσης των επικοινωνιών, ώστε (ο θιγόμενος) να έχει τη δυνατότητα αποτελεσματικής δικαστικής προστασίας*». Η διευκρίνιση αυτή θα μπορούσε να θεωρηθεί ότι απαιτεί η ενημέρωση να εξηγεί, για ποιο λόγο ένα πρόσωπο τέθηκε υπό παρακολούθηση και μάλιστα όχι γενικά, ώστε να είναι δυνατός ο δικαστικός έλεγχος[138]

Το Δικαστήριο επεσήμανε, μεταξύ άλλων, ότι ο νέος Ν. 5002/2022, που τέθηκε σε ισχύ, μετά τις καταγγελίες του αιτούντος πολιτικού αρχηγού, δεν τυγχάνει εφαρμοστέος σε εκκρεμή αιτήματα γνωστοποίησης στον θιγόμενο, του μέτρου άρσης του απορρήτου των επικοινωνιών του, ληφθέντος υπό προηγούμενο νομοθετικό καθεστώς.

Κατόπιν των ανωτέρω, η Ολομέλεια του Δικαστηρίου, κάνοντας εν μέρει δεκτή την αίτηση του κ. Ανδρουλάκη, ακύρωσε ως μη νόμιμη (στηριζόμενη σε αντισυνταγματική διάταξη νόμου) την προσβαλλόμενη με αυτήν πράξη του Προέδρου της ΑΔΑΕ, με την οποία απορρίφθηκε το αίτημα περί γνωστοποίησης του μέτρου της άρσης του απορρήτου των επικοινωνιών του, αναπέμποντας την υπόθεση στην ΑΔΑΕ, για νέα νομική κρίση, σύμφωνα με τις διατάξεις του Ν. 2225/1994.

Η απόφαση της Ολομέλειας του ΣτΕ, παρά το γεγονός, ότι χαρακτηρίστηκε ιστορική από τους νομικούς κύκλους, αποτελούσα νίκη για το Κράτος Δικαίου και τους δημοκρατικούς

---

[138] Μποτόπουλος Κ. (2024), «*Συμβούλιο της Επικρατείας και «απόφαση Ανδρουλάκη»*», Syntagmawatch. Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/symvoulio-ths-epikrateias-kai-apofasi-androulaki/. [Ημ. Πρόσβασης 14.8.2025]

θεσμούς, που είχαν υποστεί σοβαρότατο πλήγμα, στην πραγματικότητα απεδείχθη αλυσιτελής. Και τούτο διότι, προκειμένου η ΑΔΑΕ να ενημερώσει τον θιγόμενο, για την επιβολή σε βάρος του της άρσης του απορρήτου, θα πρέπει να έχει στη διάθεσή της το σχετικό υλικό, το οποίο η ΕΥΠ μέχρι στιγμής δεν έχει χορηγήσει στην ΑΔΑΕ, επιδεικνύοντας απροθυμία συνεργασίας. Δημοσιεύματα μάλιστα στον Τύπο, έκαναν λόγο για «εκ παραδρομής καταστροφή» του σχετικού φακέλου![139]Αποτέλεσμα, ο αποδεδειγμένα θιγείς, πολιτικός αρχηγός, να μην έχει ενημερωθεί ακόμη, για τους λόγους, εξαιτίας των οποίων οι τηλεφωνικές του επικοινωνίες στοχοποιήθηκαν από την ΕΥΠ.

5.2 Οι προκλήσεις που θέτουν τα λογισμικά παρακολούθησης για την έννομη τάξη και τα πορίσματα της Έκθεσης PEGA

Με αφορμή πληθώρα περιστατικών παραβιάσεων του δικαίου της Ε.Ε., μέσω της καταχρηστικής εφαρμογής λογισμικών κατασκοπίας σε αρκετά κράτη μέλη, η αρμόδια Εξεταστική Επιτροπή του Ευρωπαϊκού Κοινοβουλίου για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA), στην έκθεσή της[140], κατόπιν πολύμηνης έρευνας, διαπίστωσε ότι τα λογισμικά κατασκοπείας αποτέλεσαν αντικείμενο κατάχρησης πολλών ευρωπαϊκών Κυβερνήσεων, με στόχο τον εκφοβισμό της αντιπολίτευσης, τη φίμωση των επικριτικών μέσων ενημέρωσης και τη χειραγώγηση των εκλογών. Εκτός από την Ουγγαρία και την Πολωνία, όπου το νομικό πλαίσιο για την προστασία του απορρήτου των επικοινωνιών, χαρακτηρίζεται εξαιρετικά ελλιπές και η χρήση λογισμικών κατασκοπείας αποτελεί μέρος μιας γενικότερης στρατηγικής για τον περιορισμό της ελευθερίας των ΜΜΕ, η Επιτροπή εξέφρασε σοβαρές ανησυχίες, ότι στην Ελλάδα τα λογισμικά κατασκοπείας, αν και δεν συνιστούν μέρος μιας αυταρχικής πολιτικής, εντούτοις έχουν χρησιμοποιηθεί για πολιτικά και οικονομικά οφέλη[141].

---

[139] Κοντιάδης Ξ. (2024), *«Η απόφαση Ανδρουλάκη του ΣτΕ, η ΕΥΠ και ο ρόλος της ΑΔΑΕ»*, Syntagmawatch. Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/h-apofasi-androulaki-tou-ste/. [Ημ. Πρόσβασης 14.8.2025]

[140] ο.π. Έκθεση Ευρωπαϊκού Κοινοβουλίου για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA).

[141] Δελτίο Τύπου Ευρωπαϊκού Κοινοβουλίου (8.5.2023), *«Κατασκοπευτικά λογισμικά: ανησυχία για τη δημοκρατία και κάλεσμα για μεταρρυθμίσεις»*. Διαθέσιμο στο: https://www.europarl.europa.eu/news/el/press-room/20230505IPR84901/kataskopeutika-logismika-anisuchia-gia-ti-dimokratia-kalesma-gia-metarruthmiseis. [Ημ. Πρόσβασης 13.6.2025]

Τα πορίσματα της σχετικής έρευνας, που διεξήγαγε η αρμόδια Εξεταστική Επιτροπή του Ευρωπαϊκού Κοινοβουλίου, για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA) και αποτυπώθηκαν στην έκθεσή της, είναι πλέον ανησυχητικά.

Κατά τα διαλαμβανόμενα για τη χώρα μας, κατόπιν επίσκεψης της Εξεταστικής Επιτροπής: «*Θα πρέπει να θεσπιστούν όλες οι απαραίτητες εγγυήσεις και οι μεταρρυθμίσεις να βελτιώσουν τη διαφάνεια και να διασφαλίσουν την κατάλληλη δικαστική εποπτεία της χρήσης των λογισμικών παρακολούθησης. Η επίσκεψη επιβεβαίωσε επίσης ότι απαιτούνται σαφείς κανόνες για τον περιορισμό της χρήσης της εθνικής ασφάλειας ως βάσης παρακολούθησης, τη διασφάλιση της ορθής δικαστικής εποπτείας και την εγγύηση ενός υγιούς, πλουραλιστικού περιβάλλοντος μέσων ενημέρωσης.*»[142]

Όπως, περαιτέρω, επισημαίνεται στην έκθεση, «*Ο αριθμός των εξουσιοδοτημένων τηλεφωνικών παρακολουθήσεων έχει αυξηθεί σημαντικά με την πάροδο των ετών. Από 4.871 το 2015, σε 11.680 το 2019 και σε 15.475 το 2021. Επί του παρόντος, περίπου 60 αιτήματα πρέπει να διεκπεραιώνονται κάθε μέρα, μέχρι πρόσφατα από έναν μόνο εισαγγελέα. Επιπλέον, οι διατάξεις της ΕΥΠ, που αίρουν το απόρρητο των επικοινωνιών των πολιτών για λόγους εθνικής ασφάλειας, δεν αναφέρουν το όνομα του ενδιαφερομένου ή τον λόγο άρσης του απορρήτου. Περιορίζονται στον αριθμό τηλεφώνου και στην επίκληση λόγων εθνικής ασφάλειας.*[143]»

Παρατηρήθηκε ακόμη, ότι παρά την επικαιροποίηση, με Πράξη Νομοθετικού Περιεχομένου, του Νόμου 3649/2008, αναφορικά με την λειτουργία της ΕΥΠ και την προσθήκη σχετικής νομοθετικής πρόβλεψης, σύμφωνα με την οποία απαιτείται γνωμοδότηση της Μόνιμης Επιτροπής Θεσμών και Διαφάνειας για τον διορισμό του Διοικητή της ΕΥΠ, καθώς το κυβερνόν κόμμα κατείχε την απόλυτη πλειοψηφία της ανωτέρω Επιτροπής, ουσιαστικά η ΕΥΠ εξακολουθούσε να βρίσκεται υπό την εποπτεία της Ελληνικής Κυβέρνησης και του ίδιου του Πρωθυπουργού[144].

---

[142] Εξεταστική Επιτροπή του Ευρωπαϊκού Κοινοβουλίου για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA) (2022), σκέψη 134.
[143] Ibidem, σκέψη 167.
[144] Ibidem, σκέψη 170.

Σημειώνεται, μεταξύ άλλων, ότι όταν το 2021 η ΑΔΑΕ ενημέρωσε την ΕΥΠ σχετικά με το δικαίωμα γνωστοποίησης στον δημοσιογράφο κ. Κουκάκη, ότι είχε γίνει αντικείμενο παρακολούθησης, η κυβέρνηση υπέβαλε αμέσως τροπολογία[145], δυνάμει της οποίας καταργήθηκε η αρμοδιότητα της ΑΔΑΕ να ενημερώνει τους πολίτες, για την άρση του απορρήτου των επικοινωνιών, όταν αυτή έχει διαταχθεί για λόγους εθνικής ασφάλειας, μετά την παύση της ισχύος του μέτρου και εφόσον δεν υφίσταται κίνδυνος ματαίωσης του σκοπού του μέτρου. Αυτό στερεί εκ των πραγμάτων τον θιγόμενο από το δικαίωμά του στην ενημέρωση. Η τροπολογία, μάλιστα, εισήχθη με εντελώς «αντικανονικό» τρόπο και με την προσθήκη σε ένα άσχετο νομοσχέδιο, αναφορικά με τα μέτρα πρόληψης της πανδημίας COVID-19.[146]

Αξιολογώντας, μάλιστα, η αρμόδια Εξεταστική Επιτροπή τον Ν. 5002/2022, έκρινε ότι: «*…ο νόμος εισάγει αρκετές διατάξεις που αποδυναμώνουν τις εγγυήσεις, τον έλεγχο και τη λογοδοσία. Όπως ορίζεται στο Άρθρο 4, παράγραφος 7, οποιοδήποτε αίτημα ατόμων για πληροφορίες σχετικά με το εάν έχουν υποβληθεί σε παρακολούθηση για λόγους εθνικής ασφάλειας θα εξετάζεται από τριμελή επιτροπή που αποτελείται από τον διευθυντή της ΕΥΠ, τον εισαγγελέα της ΕΥΠ και τον επικεφαλής της ΑΔΑΕ. Αυτό σημαίνει ότι* ***η πλειοψηφία ανήκει σε εκείνους που διέταξαν (διευθυντή της ΕΥΠ) και ενέκριναν (εισαγγελέα) την παρακολούθηση εξαρχής.*** *Επιπλέον, καθιστά πρακτικά αδύνατο για τα άτομα που βρίσκονται υπό παρακολούθηση για λόγους εθνικής ασφάλειας να ενημερωθούν κατάλληλα εκ των υστέρων, καθώς ο νόμος ορίζει ότι μπορούν να υποβάλουν σχετικό αίτημα μόνο τρία χρόνια μετά τη λήξη της παρακολούθησης. Αυτό είναι ασυμβίβαστο με τη σχετική νομολογία του Ευρωπαϊκού Δικαστηρίου και τον Ευρωπαϊκό Χάρτη των Δικαιωμάτων του Ανθρώπου και δεν προβλέπει θεσμικούς ελέγχους και ισορροπίες για τη διασφάλιση της ορθής λειτουργίας των κρατικών εξουσιών. Η ΑΔΑΕ έχει εκφράσει τη διαφωνία της με το τριμελές όργανο. Μέχρι σήμερα, δεν υπάρχει λειτουργικό πλαίσιο για το τριμελές όργανο, πράγμα που σημαίνει ότι εκ των πραγμάτων δεν λειτουργεί. Επιπλέον, ο νέος νόμος ποινικοποιεί τη χρήση κατασκοπευτικού λογισμικού από ιδιώτες ή ιδιωτικές εταιρείες και για πρώτη φορά καθιστά νόμιμη την αγορά κατασκοπευτικού λογισμικού από τις δημόσιες αρχές,*

---

[145] Άρ. 87 Ν. 4790/2021 (ΦΕΚ Α' 48/31.3.2021. Διαθέσιμος σε: https://search.et.gr/el/search-legislation/?legislationNumber=4790&selectYear=2021.)

[146] Εξεταστική Επιτροπή του Ευρωπαϊκού Κοινοβουλίου για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA) (2022), ο.π., σκέψη 174.

εξουσιοδοτώντας την κυβέρνηση να θεσπίσει τη διαδικασία μέσω Προεδρικού Διατάγματος. Δεν υπάρχει πρόβλεψη για δικαστική εποπτεία της χρήσης κατασκοπευτικού λογισμικού ή για υπεργολαβία υποκλοπών σε ιδιωτικούς φορείς[147].

Η προμήθεια κατασκοπευτικού λογισμικού από ιδιωτικούς φορείς είναι παράνομη μόνο, εάν το, εν λόγω, λογισμικό περιλαμβάνεται σε ενδεικτικό κατάλογο «απαγορευμένου κατασκοπευτικού λογισμικού», που ενημερώνεται από τον Αρχηγό της ΕΥΠ κάθε έξι μήνες. (Ο νόμος) *Εξουσιοδοτεί την ΕΥΠ να αποκτά κατασκοπευτικό λογισμικό νόμιμα, καθώς τα κρίσιμα σχετικά ζητήματα θα αντιμετωπίζονται αποκλειστικά μέσω παράγωγης νομοθεσίας (δηλαδή Προεδρικού Διατάγματος). Συνεπώς, μια ενημερωμένη έκδοση του υπάρχοντος λογισμικού κατασκοπείας θα θεωρείται νόμιμη μέχρι να συμπεριληφθεί στον προαναφερθέντα κατάλογο.* ***Ο ορισμός της «εθνικής ασφάλειας» στον νόμο είναι εξαιρετικά ευρύς και ασαφής, επομένως έρχεται σε αντίθεση με το Άρθρο 19, παράγραφος 1 του Συντάγματος, το οποίο απαιτεί στενή ερμηνεία.*** *Η ΑΔΑΕ παρεμποδίζεται περαιτέρω στις προσπάθειές της να ασκήσει τον συνταγματικά ορισμένο ρόλο της στον έλεγχο της διαδικασίας αποχαρακτηρισμού.* ***Ο ρόλος της ανεξάρτητης αρχής που έπαιξε καθοριστικό ρόλο στην αποκάλυψη του σκανδάλου παρακολούθησης υποβαθμίζεται στον νέο νόμο, παρά τις σχετικές συνταγματικές εγγυήσεις***[148]***.***

Προς δυσάρεστη επιβεβαίωση της ανησυχίας, που είχε προκύψει, για την ελευθερία του Τύπου στη χώρα μας, η αρμόδια Εξεταστική Επιτροπή, διαπίστωσε ότι η Ελλάδα κατατάσσεται τελευταία από όλες τις χώρες της ΕΕ, στον Παγκόσμιο Δείκτη Ελευθερίας του Τύπου, αναφερόμενη σε συγκεκριμένα περιστατικά προσπάθειας φίμωσης δημοσιογράφων, με παρακολουθήσεις των συνομιλιών τους, εκφοβισμό και απειλές, που σε μία περίπτωση κατέληξαν στη δολοφονία δημοσιογράφου, η οποία μέχρι και σήμερα παραμένει ανεξιχνίαστη[149].

Η Έκθεση της αρμόδιας Εξεταστικής Επιτροπής αναφέρεται μεταξύ άλλων και στην υπ' αριθ. 1/2023 Γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου, κ. Ι. Ντογιάκου, σύμφωνα με την οποία η ΑΔΑΕ στερείται της εξουσίας να διεξάγει έρευνες στα αρχεία τηλεπικοινωνιακών παρόχων. Η Γνωμοδότηση συνοδεύτηκε από έμμεσες «απειλές» προς τα μέλη της ΑΑΔΕ και

[147] Ibidem, σκέψη 176.
[148] Ibidem, σκέψη 177.
[149] Ibidem, σκέψη 179.

κάθε άλλο σχετιζόμενο πρόσωπο, περί επιβολής ποινικών κυρώσεων, σε περίπτωση μη συμμόρφωσης προς το περιεχόμενο της, εν λόγω, Γνωμοδοτήσεως[150], η οποία προκάλεσε πληθώρα αντιδράσεων στους νομικούς κύκλους, ως παραβιάζουσα εξόφθαλμα την ευθέως εκ του Συντάγματος εκπορευόμενη ανεξαρτησία της ΑΔΑΕ, και με δεδομένο ότι η γενική αρμοδιότητα του Εισαγγελέα του Αρείου Πάγου να γνωμοδοτεί επί «νομικών ζητημάτων γενικού ενδιαφέροντος», ουδόλως εκτείνεται μέχρι του σημείου να διατυπώνει γνώμη επί της ερμηνείας και εφαρμογής διατάξεων, που αφορούν τις συνταγματικές αρμοδιότητες της ΑΔΑΕ, απευθύνοντας σε αυτήν κατευθυντήριες οδηγίες και απειλώντας μάλιστα με πρωτοφανή τρόπο τα μέλη της με βαρύτατες ποινικές κυρώσεις, αν ασκήσουν τις αρμοδιότητες τους με τρόπο διαφορετικό από τον, από αυτόν, υιοθετούμενο[151].

Η αρμόδια Εξεταστική Επιτροπή σημειώνει ότι και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), συνάντησε αρκετά εμπόδια στο έργο της και ειδικότερα σε έρευνα που πραγματοποίησε στα γραφεία εταιρείας που δραστηριοποιούνταν στο πεδίο της πληροφορικής και φαίνεται να είχε άμεση ανάμιξη στην υπόθεση των υποκλοπών με την διάθεση του κακόβουλου λογισμικού Predator, η εταιρεία επέδειξε απροθυμία συνεργασίας, μην παρέχοντας τις αναγκαίες πληροφορίες, συμπεριφορά για την οποία της επεβλήθη από την ανωτέρω Ανεξάρτητη Αρχή, πρόστιμο 50.000 Ευρώ[152].

Καταλήγοντας η αρμόδια Εξεταστική Επιτροπή, στα συμπεράσματά της, για την χρήση λογισμικών κατασκοπείας, επισημαίνει ότι: «*Υπάρχουν μοτίβα που υποδηλώνουν ότι η ελληνική κυβέρνηση επιτρέπει τη χρήση spyware εναντίον δημοσιογράφων, πολιτικών και επιχειρηματιών. Επιτρέπει επίσης την εξαγωγή spyware σε χώρες με χαμηλό ιστορικό ανθρωπίνων δικαιωμάτων και παρέχει ένα κέντρο εκπαίδευσης για πράκτορες χωρών εκτός ΕΕ, που θέλουν να μάθουν για το spyware. Παρόλο που η χρήση spyware είναι παράνομη στην Ελλάδα, η έρευνα για την προέλευση των επιθέσεων spyware κέρδισε δυναμική μόνο το καλοκαίρι του 2022. Σύμφωνα με πληροφορίες,*

---

[150] Ibidem, σκέψη 188.

[151] Ράμμος Χ. (2023), «*Δήλωση του Προέδρου της ΑΔΑΕ για τη Γνωμοδότηση 1/10879/10.01.2023 του Εισαγγελέως του Αρείου Πάγου κ. Ισίδωρου Ντογιάκου*», Syntagmawatch. Διαθέσιμο στο: https://www.syntagmawatch.gr/trending-issues/dilosi-tou-proedrou-ths-adae-xrhstou-rammou-gia-th-gnwmodothsh-1-10879-10-01-2023/. [Ημ. Πρόσβασης 12.8.2025]

[152] Εξεταστική Επιτροπή του Ευρωπαϊκού Κοινοβουλίου για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA) (2022), ο.π., σκέψεις 198-199.

η κομματική πλειοψηφία χρησιμοποιείται για την προώθηση συγκεκριμένων συμφερόντων και όχι του γενικού συμφέροντος, ιδίως με τον διορισμό συνεργατών και πιστών σε βασικές θέσεις όπως η ΕΥΠ, η ΕΑΔ (Εθνική Αρχή Διαφάνειας) και η Krikel (μια εταιρεία που ειδικεύεται σε ηλεκτρονικά συστήματα ασφαλείας). Η ανώτατη πολιτική ηγεσία της χώρας χρησιμοποιεί spyware ως εργαλείο πολιτικής εξουσίας και ελέγχου, σε ορισμένες περιπτώσεις παράλληλα ή μετά από νόμιμη παρακολούθηση. Η Ελλάδα διαθέτει ένα αρκετά ισχυρό νομικό πλαίσιο κατ' αρχήν. Ωστόσο, ***οι νομοθετικές τροποποιήσεις έχουν αποδυναμώσει κρίσιμες διασφαλίσεις και οι πολιτικοί διορισμοί σε βασικές θέσεις αποτελούν εμπόδιο στον έλεγχο και τη λογοδοσία****. Οι μηχανισμοί ελέγχου ex ante και ex post έχουν αποδυναμωθεί σκόπιμα και η διαφάνεια και η λογοδοσία αποφεύγονται. Οι επικριτικοί δημοσιογράφοι ή αξιωματούχοι, που καταπολεμούν τη διαφθορά και την απάτη έρχονται αντιμέτωποι με εκφοβισμό και παρεμπόδιση. Συνολικά, το σύστημα διασφαλίσεων και εποπτείας της επιτήρησης είναι ανεπαρκές, για την προστασία των πολιτών από την κατάχρηση από κρατικές υπηρεσίες και ιδιωτικούς φορείς. Πρέπει να γίνουν περισσότερα για την αντιμετώπιση αυτού του προβλήματος. Επιπλέον, το πρόσχημα της «εθνικής ασφάλειας» προβάλλεται ως δικαιολογία για την παρακολούθηση τηλεφωνικών κλήσεων ατόμων.*

Η κατασκοπεία για πολιτικούς λόγους δεν είναι κάτι καινούργιο στην Ελλάδα, αλλά οι νέες τεχνολογίες κατασκοπείας καθιστούν την παράνομη επιτήρηση πολύ πιο εύκολη, ιδίως σε ένα πλαίσιο σοβαρά εξασθενημένων διασφαλίσεων. Σε αντίθεση με άλλες περιπτώσεις, όπως η Πολωνία, η κατάχρηση κατασκοπείας δεν φαίνεται να αποτελεί μέρος μιας ολοκληρωμένης ανταρχικής στρατηγικής, αλλά μάλλον ένα εργαλείο, που χρησιμοποιείται σε ad hoc βάση για πολιτικό και οικονομικό κέρδος. ***Ωστόσο, διαβρώνει εξίσου τη Δημοκρατία και το Κράτος Δικαίου και αφήνει άφθονο περιθώριο για διαφθορά, όταν αυτές οι ταραγμένες εποχές απαιτούν αξιόπιστη και υπεύθυνη ηγεσία****»*[153]

[153] Ibidem., σκέψεις 238-239.

5.3 Η Σύσταση του Ευρωπαϊκού Κοινοβουλίου[154]

Κατόπιν των ανωτέρω πορισμάτων το Ευρωπαϊκό Κοινοβούλιο προχώρησε στην έκδοση Σύστασης προς τα κράτη μέλη, στα οποία είχε διαπιστωθεί παράνομη χρήση λογισμικών κατασκοπείας (μεταξύ των οποίων και η χώρα μας).

Μεταξύ άλλων, η Ελλάδα εκλήθη να λάβει άμεσα μέτρα ως αντίβαρο της κατάχρησης λογισμικών κατασκοπείας. Ενδεικτικά των μέτρων αυτών: η διασφάλιση της δυνατότητας των αρχών να διερευνούν ελεύθερα και ανεμπόδιστα την βασιμότητα όλων των καταγγελιών περί χρήσης spyware, ιδίως ο σεβασμός του θεσμικού ρόλου της ΑΔΑΕ, ως ανεξάρτητης αρχής, παρέχοντάς της τα εχέγγυα, για την πρόσβασή της σε πληροφορίες και την ακώλυτη συνεργασία της με δημόσιους και ιδιωτικούς φορείς, η δημιουργία ηλεκτρονικού αρχείου της ΑΔΑΕ, η απαγόρευση εξαγωγής λογισμικών κατασκοπείας, κατά τρόπο που δεν συνάδει με την ευρωπαϊκή έννομη τάξη, η εξασφάλιση της ανεξαρτησίας της ΕΑΔ, αλλά και του Δικαστικού Σώματος, που επιλαμβάνεται της διαδικασίας άρσης του απορρήτου των επικοινωνιών, η πλήρης διαλεύκανση του σκανδάλου των παρακολουθήσεων πολιτικών προσώπων, δημοσιογράφων και κρατικών αξιωματούχων και η απεμπλοκή της ΕΥΠ από τον έλεγχο του Πρωθυπουργού.

Το Ευρωπαϊκό Κοινοβούλιο, τονίζει την ανάγκη καθορισμού κοινών προτύπων στην ΕΕ για τη ρύθμιση της χρήσης κατασκοπευτικού λογισμικού από τους φορείς των κρατών μελών, με βάση τα πρότυπα που ορίζονται από το ΔΕΕ και το ΕΔΔΑ.

Σύμφωνα με τα προτεινόμενα πρότυπα: Η χρήση κατασκοπευτικού λογισμικού πρέπει να επιτρέπεται μόνο σε εξαιρετικές και ειδικές περιπτώσεις, προκειμένου να προστατευτεί η εθνική ασφάλεια, και πρέπει να υπόκειται σε αποτελεσματική, δεσμευτική και ουσιαστική εκ των προτέρων δικαστική άδεια από αμερόληπτη και ανεξάρτητη Δικαστική Αρχή ή άλλον ανεξάρτητο δημοκρατικό φορέα επίβλεψης, η οποία θα έχει πρόσβαση σε όλες τις σχετικές πληροφορίες και θα αποδεικνύει την αναγκαιότητα και την αναλογικότητα του προβλεπόμενου μέτρου. Ομοίως, η άδεια για τη χρήση κατασκοπευτικού λογισμικού μπορεί να

---

[154] Σύσταση του Ευρωπαϊκού Κοινοβουλίου της 15ης Ιουνίου 2023 προς το Συμβούλιο και την Επιτροπή σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (2023/2500(RSP)), ό.π.

χορηγείται μόνο σε εξαιρετικές περιπτώσεις, σε σχέση με έρευνες για περιορισμένο και κλειστό κατάλογο επ' ακριβώς ορισμένων σοβαρών εγκλημάτων, που συνιστούν πραγματική απειλή για την εθνική ασφάλεια, το δε κατασκοπευτικό λογισμικό μπορεί να χρησιμοποιείται μόνο για πρόσωπα για τα οποία υπάρχουν επαρκείς ενδείξεις, ότι έχουν διαπράξει ή σχεδιάζουν να διαπράξουν τέτοια σοβαρά ποινικά αδικήματα

Περαιτέρω, η εφαρμογή λογισμικού κατασκοπείας θα πρέπει να περιορίζεται χρονικά, στο αναγκαίο, για την επίτευξη του σκοπού, μέτρο, ενώ η παράτασή της να καθορίζεται επίσης με ακρίβεια, κατόπιν προηγούμενης δικαστικής άδειας.

Ιδιαίτερη προσοχή απαιτείται, κατά την χρήση λογισμικών κατασκοπείας σε συγκεκριμένες κατηγορίες προσώπων, όπως πολιτικοί, δημοσιογράφοι, δικηγόροι, στρατιωτικοί, στις οποίες η επιτήρηση θα πρέπει να λαμβάνει χώρα, μόνον όταν συντρέχουν σοβαρές ενδείξεις συμμετοχής τους σε εγκληματικές δραστηριότητες ή προκύπτουν ζητήματα εθνικής ασφάλειας.

Προς περιορισμό του κινδύνου κατάχρησης των λογισμικών κατασκοπείας, σκόπιμη θα ήταν η δημοσίευση, τουλάχιστον, του αριθμού των αιτήσεων επιτήρησης, που εγκρίνονται και απορρίπτονται, καθώς και του είδους και του σκοπού της έρευνας, και η καταχώρηση ανώνυμα κάθε έρευνας σε εθνικό μητρώο με μοναδικό αναγνωριστικό κωδικό.

Ακόμη, εξαιρετικά σημαντική για την προστασία του κράτους δικαίου είναι η ελεύθερη άσκηση του δικαιώματος γνωστοποίησης της επιβολής του μέτρου της επιτήρησης (και όλων των στοιχείων που σχετίζονται με αυτό, λ.χ. ο λόγος και η διάρκεια της εφαρμογής του μέτρου, τα δεδομένα που συνελέγησαν, για ποιον σκοπό χρησιμοποιήθηκαν και αν διεγράφησαν, κλπ.) στο στοχοποιημένο πρόσωπο, μετά το πέρας της παρακολούθησης και εφόσον δεν διακυβεύεται ο σκοπός του μέτρου.

Η εθνική έννομη τάξη θα πρέπει, επιπλέον, να εξασφαλίσει την δυνατότητα άσκησης ενός ουσιαστικού και αποτελεσματικού ενδίκου μέσου, για τα άτομα που ισχυρίζονται ότι επηρεάζονται αρνητικά από την παρακολούθηση, καθώς και την ταχεία, ενδελεχή και αμερόληπτη έρευνα από ανεξάρτητο εποπτικό φορέα της σχετικής καταγγελίας.

Κατά τη διάρκεια της παρακολούθησης, οι Αρχές θα πρέπει να διαγράφουν όλα τα δεδομένα, που δεν είναι συναφή με την εξουσιοδοτημένη έρευνα, ενώ μετά την ολοκλήρωση της επιτήρησης και της έρευνας, για την οποία χορηγήθηκε η άδεια, οι Αρχές θα πρέπει να

διαγράφουν τα δεδομένα, καθώς και κάθε σχετικό έγγραφο, όπως σημειώσεις που ελήφθησαν κατά τη διάρκεια της εν λόγω περιόδου, και η διαγραφή αυτή πρέπει να καταγράφεται και να είναι ελέγξιμη.

Θα πρέπει, επιπλέον, να θεσπιστούν ελάχιστα πρότυπα δικαιωμάτων των ατόμων κατά τις ποινικές διαδικασίες, σχετικά με το παραδεκτό των αποδεικτικών στοιχείων, που συλλέγονται με τη βοήθεια κατασκοπευτικού λογισμικού.

Τέλος, στο λογισμικό παρακολούθησης θα πρέπει να συμπεριληφθεί ιχνηθέτης, ώστε οι εποπτικοί φορείς να είναι σε θέση να προσδιορίζουν σαφώς εκείνον που το χρησιμοποιεί, σε περίπτωση υπόνοιας κατάχρησης.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Ολοκληρώνοντας την παρούσα μελέτη και κατόπιν όσων ανωτέρω εκτίθενται, καθίσταται αντιληπτό, ότι η προστασία των θεμελιωδών δικαιωμάτων, σε έναν διαρκώς και με ταχύτατους ρυθμούς μεταβαλλόμενο ψηφιακό κόσμο, αποτελεί πρόκληση.

Οι κυβερνήσεις, σε συνεργασία με κρατικές αρχές και ιδιώτες, χρησιμοποιούν πλέον ευρέως συστήματα επιτήρησης, ακόμη και σε μαζική κλίμακα, όχι μόνο για την πάταξη του οργανωμένου εγκλήματος και την προάσπιση της εθνικής ασφάλειας, όπως ευαγγελίζονται, αλλά και για την ικανοποίηση αθέμιτων συμφερόντων: για την εξόντωση πολιτικών αντιπάλων, για την φίμωση της αντίθετης γνώμης, ακόμη και για την συγκάλυψη αξιόποινων πράξεων.

Η δικαιολογημένη ανησυχία, για την χρήση λογισμικών κατασκοπείας, εντοπίζεται, όχι μόνον στην ισχυρή επεμβατικότητα των μεθόδων παρακολούθησης, αλλά κατ' αρχάς στην εκτός κανονιστικού πλαισίου και απολύτως ανεξέλεγκτη δράση των επίδοξων εισβολέων[155].

Το γεγονός, μάλιστα, ότι τα κατασκοπευτικά λογισμικά, δεν διαθέτουν απλώς ισχυρή διεισδυτική δράση, αλλά τα περισσότερα από αυτά δεν καταλείπουν κανένα απολύτως ίχνος, καθώς δεν περιλαμβάνουν by design ρυθμίσεις, που να εγγυώνται τη διατήρηση του ιστορικού της δραστηριότητάς τους (διάρκεια, δεδομένα, κλπ), δυσχεραίνει έτι περαιτέρω το έργο των Εποπτικών Αρχών, προκειμένου να διαπιστώσουν τις συνθήκες εφαρμογής του μέτρου και να εκτιμήσουν την συμβατότητά του, σύμφωνα με τις επιταγές του Νόμου.

Το ήδη ισχύον στη χώρα μας κανονιστικό πλαίσιο κρίνεται σε κάθε περίπτωση ανεπαρκές. Η θέσπιση του Ν. 5002/2022, αξιολογείται οπωσδήποτε θετικά, ανταποκρινόμενη στην επιτακτική ανάγκη αναδιαμόρφωσης του προϋφιστάμενου κανονιστικού πλαισίου, το οποίο σε καμία περίπτωση δεν μπορούσε να συμβαδίσει με τις σύγχρονες τεχνολογικές εξελίξεις. Ωστόσο, πολλές από τις διατάξεις του νέου Νόμου, όχι μόνο δεν προβλέπουν δικλείδες ασφαλείας, για την επιβολή μέτρων επιτήρησης των επικοινωνιών, τουναντίον επιτρέπουν στην κρατική εξουσία να επεμβαίνει αυθαίρετα στον ιδιωτικό βίο των ανθρώπων. Η απουσία ρυθμιστικού πλαισίου, για την χρήση λογισμικών κατασκοπείας, θα μπορούσε

[155] Παπανικολάου (2022), ο.π.

ενδεχομένως να θεραπευθεί, τουλάχιστον, αν ο Νόμος προέβλεπε ορισμένα εχέγγυα, ως προς τη διαδικασία άρσης του επικοινωνιακού απορρήτου, όπως ενδεικτικά: α) η αιτιολόγηση της εισαγγελικής διάταξης, που επιτρέπει την εφαρμογή του μέτρου, ώστε να μπορεί να ελεγχθεί η στάθμιση εκ μέρους του εισαγγελικού λειτουργού των αντικρουόμενων εννόμων αγαθών και η τήρηση της Αρχής της αναλογικότητας, β) στην περίπτωση της άρσης του απορρήτου, για λόγους εθνικής ασφάλειας, η γνωστοποίηση στον θιγόμενο της επιβολής του μέτρου αμέσως μόλις παύσει η ισχύς του μέτρου (και όχι τρία χρόνια μετά!) και εφόσον δεν υφίσταται κίνδυνος ματαίωσης του σκοπού του, γ) η παροχή άδειας, για την γνωστοποίηση του μέτρου από ανεξάρτητο όργανο, και όχι από πρόσωπα (εν προκειμένω δύο εισαγγελικούς λειτουργούς), που έχουν ήδη εκφράσει τη θέση τους σε προγενέστερο στάδιο της διαδικασίας άρσης του απορρήτου, δ) η, κατά το δυνατόν, πιο συσταλτική ερμηνεία των αόριστων εννοιών της εθνικής ασφάλειας και των ιδιαιτέρως σοβαρών εγκλημάτων, προς περιορισμό του κινδύνου κατάχρησης εκ μέρους της εκτελεστικής εξουσίας, ε) η ενίσχυση του ρόλου της ΑΔΑΕ και η διασφάλιση της ανεμπόδιστης δράσης της, όπως αυτή προβλέπεται στο Σύνταγμα.

Ως προς τον θεσμικό ρόλο της ΑΔΑΕ, σκόπιμο είναι να επισημανθεί, ότι υφίστανται μέχρι και σήμερα σημαντικά οργανωτικά και διαδικαστικά ελλείματα, τα οποία υποβαθμίζουν την δράση της, δημιουργώντας εύλογες ανησυχίες, κατά πόσον αυτή μπορεί, εν τοις πράγμασι, να λειτουργήσει ως αντίβαρο στην ανέλεγκτη, όπως αποδεικνύεται, δικαστική κρίση. Ενδεικτικό, είναι το γεγονός ότι η ΑΔΑΕ, παρά την ύπαρξη σχετικής νομοθετικής πρόβλεψης, μόλις το 2021, δυνάμει της διάταξης του άρθρου 36 του Ν. 4786/2021, αλλά και δυνάμει των άρθρων 4 και 8 του Ν. 5002/2022, δεν διαθέτει μέχρι σήμερα ψηφιοποιημένο αρχείο των εισαγγελικών διατάξεων, που διατάσσουν την άρση του απορρήτου, έλλειμμα το οποίο εξακολουθεί να υποκαθίσταται, μέσω της συνδρομής των τηλεπικοινωνιακών παρόχων, στα αρχεία των οποίων προστρέχει για τον αναγκαίο έλεγχο η ΑΔΑΕ, κάθε φορά που της υποβάλλεται αίτημα γνωστοποίησης. Έτσι η ΑΔΑΕ δεν είναι σε θέση να επαληθεύσει την ακρίβεια των πληροφορίων, που αντλεί από τα αρχεία των παρόχων, τους οποίους, σημειωτέον, εποπτεύει, σύμφωνα με τη διάταξη της παρ. 1 του άρθρου 6 του Ν. 3115/2003, με συνέπεια να τίθεται ζήτημα αξιοπιστίας, όταν η άσκηση της εξουσίας του εποπτεύοντος οργάνου «εξαρτάται» από τον ελεγχόμενο.

Η προσπάθεια του Έλληνα νομοθέτη να εντάξει τη χρήση των κατασκοπευτικών λογισμικών εντός νομοθετικού πλαισίου, με την εισαγωγή συγκεκριμένων διατάξεων (άρθρα 10 -14 Ν. 5002/2022), μέχρι στιγμής αποδεικνύεται μάλλον προσχηματική και ανεπιτυχής, καθώς, όπως ήδη εκτέθηκε, το Π.Δ., δυνάμει του οποίου θα καθορίζονταν οι προϋποθέσεις σύναψης συμβάσεων εκ μέρους κρατικών δομών για την προμήθεια λογισμικών κατασκοπείας, δεν έχει ακόμη εκδοθεί!

Το γεγονός μάλιστα, ότι τρία (3) σχεδόν έτη μετά το ξέσπασμα του σκανδάλου των υποκλοπών στη χώρα μας (κατόπιν δε και της δικαστικής κρίσης του Ανωτάτου Ακυρωτικού περί αντισυνταγματικότητας της νομοθετικής διάταξης που καταργούσε την δυνατότητα ενημέρωσης του υποκειμένου, επί άρσης του απορρήτου για λόγους εθνικής ασφάλειας), πρόσωπα που εθίγησαν από την χρήση λογισμικών κατασκοπείας, δεν έχουν έως σήμερα λάβει σαφή απάντηση, για ποιόν λόγο στοχοποιήθηκαν, είναι ιδιαίτερα αποθαρρυντικό για την λειτουργία των θεσμών και γεννά εύλογες ανησυχίες για το επίπεδο του Κράτους Δικαίου στη Χώρα μας.

Επί του παρόντος και όσο ακόμη δεν υφίσταται συνεκτικό κανονιστικό πλαίσιο οι θέσεις του ΕΔΔΑ και του ΔΕΕ, αναφορικά με τα κριτήρια και τις προϋποθέσεις περιορισμού του δικαιώματος στο επικοινωνιακό απόρρητο, όπως αυτές διαμορφώνονται από την πλούσια Νομολογία του, μπορούν να αποτελέσουν ασφαλείς κατευθυντήριες γραμμές, για την αποτελεσματική προστασία των θεμελιωδών δικαιωμάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλιογραφία

Αλιβιζάτος Ν. (1987), «*Η συνταγματική θέση των ενόπλων δυνάμεων, Ι. Η αρχή του πολιτικού ελέγχου*», Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή.

Βενιζέλος Ε. (2022), «*Δικαστικός έλεγχος της συνταγματικότητας των νόμων και ερμηνεία του Συντάγματος – Μαθήματα Εμβάθυνσης στο Συνταγματικό Δίκαιο*», Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη.

Δαγτόγλου Π. (2012), «*Συνταγματικό Δίκαιο, Ατομικά Δικαιώματα*», Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη.

Μάνεσης Α. (1981), «*Ατομικές Ελευθερίες*», Εκδοτικός Οίκος Σάκκουλα.

Μάνεσης Α. (1982), «*Συνταγματικά Δικαιώματα, τόμ. α' Ατομικές Ελευθερίες*» (πανεπιστημιακές παραδόσεις), δ' έκδοση

Μανωλεδάκης Ι. (2005), «*Το απόρρητο του ιδιωτικού βίου και η έλλογη ποινική προστασία του*», ΠοινΔικ.

Μαυρίας Κ. (1982), «*Το συνταγματικό δικαίωμα ιδιωτικού βίου*», Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή.

Παντελής Α. (2018), «*Εγχειρίδιο Συνταγματικού Δικαίου*», 4η έκδοση, Εκδοτικός Οίκος Λιβάνη, Αθήνα.

Παπαδόπουλος Ν. (2017), «*Ερμηνεία Άρθρου 19 Σ.*», σε Φ. Σπυρόπουλο/Ξ. Κοντιάδη/Χ. Ανθόπουλο/ Γ. Γεραπετρίτη, «*Σύνταγμα, Κατ' άρθρο ερμηνεία*», Εκδόσεις Σάκκουλας, Αθήνα – Θεσσαλονίκη.

Ράμμος Χ. (2024), «*Η Αρχή Διασφαλίσεως του Απορρήτου των Επικοινωνιών (ΑΔΑΕ): Ένα θεσμικό αντίβαρο για την προστασία της πιο ευαίσθητης πτυχής του ιδιωτικού βίου, στο πλαίσιο του 5ου ετήσιου forum του Κέντρου του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης για τον Ευρωπαϊκό Νομικό Πολιτισμό, 7 και 8 Δεκεμβρίου 2023*», στο βιβλίο «*Η ιδιωτικότητα στην ψηφιακή εποχή*». Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα.

Τασσόπουλος Γ. (2006): «Η κοινωνία και το Σύνταγμα στην Ελλάδα – Μεταξύ πολιτικού ενθουσιασμού και ευπρέπειας», Εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη.

Τσίρης Π. (2002), «*Η συνταγματική κατοχύρωση του δικαιώματος του απορρήτου των επικοινωνιών*», Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή.

Τσόλιας Γ. (2013) «*Απόρρητο Ηλεκτρονικών Επικοινωνιών Ι - Συνταγματικό πλαίσιο προστασίας του απορρήτου στον τομέα των τηλεπικοινωνιών*», Ειδικοί Ποινικοί Νόμοι, Εκδόσεις Π.Ν. Σάκκουλα, Αθήνα.

Χρυσόγονος Κ. /Βλαχόπουλος Σ. (2017), «*Ατομικά και Κοινωνικά Δικαιώματα*», 4η αναθεωρημένη έκδοση, Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα.

Ηλεκτρονική Βιβλιογραφία - Αρθογραφία

Birchall M. (2025), *"What is spyware? How to detect it and protect yourself"*, Norton. Διαθέσιμο σε: https://us.norton.com/blog/malware/spyware.

Marczak B., Scott-Railton J., McKune S., Razzak A.B., Deibert R., (18.9.2018), *"HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries"*, Citizen Lab. Διαθέσιμο σε https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Reimer J. (2007), «*The tricky issue of spyware with a badge: meet 'policeware'*» Διαθέσιμο σε: https://arstechnica.com/information-technology/2007/07/will-security-firms-avoid-detecting-government-spyware/.

Rusinova V. (2019), *"A European perspective on Privacy and mass Surveillance at the Crossroads"*, Basic Research Porgram, Working Papers, Series: Law, WP BRP 87/LAW/2019. Διαθέσιμο σε: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347711.

Βενιζέλος Ε. (2025), «*Το Ελληνικό Σύνταγμα*», τόμ. 1, Sakkoulas – Online.gr.

Καράτσαλος Γ. (2023), «*Προσβολές εννόμων αγαθών σε ψηφιακό περιβάλλον και ποινική αντιμετώπισή τους*», Εθνική Σχολή Δικαστών (ΕΣΔΙ). Διαθέσιμο στο:

https://www.esdi.gr/wp-content/uploads/2023/seminars/02/psifiaki_oikonomia/karatsalos_2023.pdf

Μαντζούφας Π. (21.9.2024), *«Το συνταγματικό πλαίσιο του δικαιώματος επικοινωνίας και οι προϋποθέσεις άρσης του απορρήτου για λόγους εθνικής ασφάλειας»*, Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης. Διαθέσιμο στο: https://www.constitutionalism.gr/to-sintagmatiko-plaisio-tou-dikaiomatos-epikoinonias/.

Παναγοπούλου Φ. (2023): *«Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 19»* Σε Βλαχόπουλο Σπ., Κοντιάδη Ξ., Τασόπουλο Γ. (επιμ.), Syntagmawatch. Διαθέσιμο στο: https://www.syntagmawatch.gr/my-constitution/arthro-19/.

Παναγοπούλου Φ. (2023): *«Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 9»* Σε Βλαχόπουλο Σπ., Κοντιάδη Ξ., Τασόπουλο Γ. (επιμ.), Syntagmawatch. Διαθέσιμο στο: https://www.syntagmawatch.gr/wp-content/uploads/2023/02/%CE%86%CF%81%CE%B8%CF%81%CE%BF-9-me-cover.pdf.

Παπανικολάου Α. (2020), *«Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: Επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα»*, Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης. Διαθέσιμο στο: https://www.constitutionalism.gr/2020-07-papanikolaou-aporito-epikinonias/.

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

Τασόπουλος Γ. (2023): *«Σύνταγμα, Ερμηνεία κατ' άρθρο, Άρθρο 14»* Σε Βλαχόπουλο Σπ., Κοντιάδη Ξ., Τασόπουλο Γ. (επιμ.), Syntagmawatch. Διαθέσιμο στο: https://www.syntagmawatch.gr/my-constitution/arthro-14/.

Χελιουδάκης Λ. (2019): *«Διατήρηση Μεταδεδομένων Ηλεκτρονικών Επικοινωνιών: Το ευρωπαϊκό φάντασμα που θέλει να πάρει ξανά σάρκα και οστά»*, Homo

Digitalis. Διαθέσιμο στο: https://homodigitalis.gr/posts/4048/#1534226687868-199cba6f-d67a

Δημοσιεύσεις - Ιστότοποι

«*Big Brother Watch and Others v. the United Kingdom*», 28.2.2022, Cambridge University Press. Διαθέσιμο σε: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/big-brother-watch-and-others-v-the-united-kingdom/024BF9DDDFA0C882358B052845230352.

«*Europe's PegasusGate – Countering spyware abuse*», Μελέτη του Ευρωπαϊκού Κοινοβουλίου (2022). Διαθέσιμη σε: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729397.

«*The ePrivacy Regulation proposal has been withdrawn, but the fight for your privacy is far from over*», 19.2.2025. Διαθέσιμο στο: https://edri.org/our-work/the-eprivacy-regulation-proposal-has-been-withdrawn-but-the-fight-for-your-privacy-is-far-from-over/.

«*Συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες*», Γ/ΕΞ/1525/25.2.2020 Δελτίο Τύπου της ΑΠΔΠΧ. Διαθέσιμο σε: https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythynon-epexergasias-dedomenon-me-tin-eidiki.

«*Τι δήλωσε ο Ν. Ανδρουλάκης για την παρακολούθηση του τηλεφώνου του και τη μήνυση που κατέθεσε» (26.7.2022). Διαθέσιμο σε: https://www.inewsgr.com/421/ti-dilose-o-nandroulakis-gia-tin-parakolouthisi-tou-tilefonou-tou-kai-ti-minysi-pou-katethese.htm*.

«*Τι είναι το Spyware στην Κυβερνοασφάλεια;*» Διαθέσιμο σε: https://www.geeksforgeeks.org/ethical-hacking/what-is-spyware-in-cyber-security/.

European Court of Human Rights (updated version 28.2.2025), *"Guide on Article 8 of the European Convention on Human Rights"*, Διαθέσιμο στο: : https://ks.echr.coe.int/web/echr-ks/article-8.

Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.514 - January 2023, «*The impact of Pegasus on fundamental rights and democratic processes*». Διαθέσιμο σε:

https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf.

Spyware, CISA. Διαθέσιμο σε: https://www.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf.

Vogiatzoglou P. (2019), «*Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity*». European Journal of Law and Technology, Vol 10, Issue 1, 2019.

What is spyware, Fortinet. Διαθέσιμο σε: https://www.fortinet.com/resources/cyberglossary/spyware.

ΑΠΔΠΧ (3.7.2001), *Υπ' αριθ. 92/2001 Απόφαση σχετικά με την τηλεοπτική εκπομπή με την ονομασία «Μεγάλος Αδερφός» (Big Brother).* Διαθέσιμη στο: https://www.dpa.gr/el/enimerwtiko/prakseisArxis/arheio-tileoptikis-paragogis-big-brother.

Δελτίο Τύπου Ευρωπαϊκού Κοινοβουλίου (8.5.2023), «*Κατασκοπευτικά λογισμικά: ανησυχία για τη δημοκρατία και κάλεσμα για μεταρρυθμίσεις*». Διαθέσιμο στο: https://www.europarl.europa.eu/news/el/press-room/20230505IPR84901/kataskopeutika-logismika-anisuchia-gia-ti-dimokratia-kalesma-gia-metarruthmiseis.

Έκθεση Ευρωπαϊκού Κοινοβουλίου για την διερεύνηση της χρήσης του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (PEGA), Διαθέσιμη στο: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html#_section1.

Ευρωπαϊκή Επιτροπή, Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, COM(2017)010 final. Διαθέσιμος στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52017PC0010.

Κοντιάδης Ξ. (2024), «*Η απόφαση Ανδρουλάκη του ΣτΕ, η ΕΥΠ και ο ρόλος της ΑΔΑΕ*», Syntagmawatch. Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/h-apofasi-androulaki-tou-ste/.

Μποτόπουλος Κ. (2024), *«Συμβούλιο της Επικρατείας και «απόφαση Ανδρουλάκη»*, Syntagmawatch. Διαθέσιμο σε: https://www.syntagmawatch.gr/trending-issues/symvoulio-ths-epikrateias-kai-apofasi-androulaki/.

ΟΛΑΔΑΕ (2022), *«Παρατηρήσεις της Ολομέλειας της ΑΔΑΕ επί του νομοσχεδίου για την διαδικασία άρσης του απορρήτου των επικοινωνιών, την κυβερνοασφάλεια και την προστασία των προσωπικών δεδομένων»*, Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης, σελ. 2. Διαθέσιμο στο: https://www.constitutionalism.gr/paratiriseis-tis-olomeleias-tis-adae-epi-tou-nomosxediou-gia-tin-arsi-tou-aporitoy-ton-sinomilion/.

Ράμμος Χ. (2023), *«Δήλωση του Προέδρου της ΑΔΑΕ για τη Γνωμοδότηση 1/10879/10.01.2023 του Εισαγγελέως του Αρείου Πάγου κ. Ισίδωρου Ντογιάκου»*, Syntagmawatch. Διαθέσιμο στο: https://www.syntagmawatch.gr/trending-issues/dilosi-tou-proedrou-ths-adae-xrhstou-rammou-gia-th-gnwmodothsh-1-10879-10-01-2023/.

Σύσταση του Ευρωπαϊκού Κοινοβουλίου της 15ης Ιουνίου 2023 προς το Συμβούλιο και την Επιτροπή σχετικά με τη διερεύνηση εικαζόμενων παραβάσεων και περιστατικών κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης (2023/2500(RSP)). Διαθέσιμη σε: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EL.html.

Νομοθεσία

Σύνταγμα της Ελλάδος, ΦΕΚ Α' 211/24.12.2019. Διαθέσιμο σε: https://search.et.gr/el/fek/?fekId=605083.

Ν. 2225/1994, ΦΕΚ Α' 121/20.7.1994. Διαθέσιμος σε: https://search.et.gr/el/search-legislation/?legislationNumber=2225&selectYear=1994.

Ν. 3115/2003, ΦΕΚ Α' 47/27.2.2003. Διαθέσιμος σε: https://search.et.gr/el/search-legislation/?legislationNumber=3115&selectYear=2003.

Π.Δ. 47/2005 ΦΕΚ Α' 64/10.3.2005. Διαθέσιμο στο: https://search.et.gr/el/search-legislation/?legislationNumber=47&selectYear=2005.

Ν. 3471/2006, ΦΕΚ Α' 133/28.6.2006. Διαθέσιμος σε: https://search.et.gr/el/fek/?fekId=334206.

Ν. 4070/2012, ΦΕΚ Α' 82/10.4.2012. Διαθέσιμος σε: https://search.et.gr/el/fek/?fekId=473837.

Ν. 4622/2019, ΦΕΚ Α' 133/7.8.2019. Διαθέσιμος σε: https://search.et.gr/el/search-legislation/?legislationNumber=4622&selectYear=2019.

Ν. 4624/2019, ΦΕΚ Α' 137/29.8.2019. Διαθέσιμος σε: https://search.et.gr/el/search-legislation/?legislationNumber=4624&selectYear=2019.

Ν. 4790/2021, ΦΕΚ Α' 48/31.3.2021. Διαθέσιμος σε: https://search.et.gr/el/search-legislation/?legislationNumber=4790&selectYear=2021.

Ν. 5002/2022, ΦΕΚ Α' 228/ 9.12.2022. Διαθέσιμος σε: https://search.et.gr/el/fek/?fekId=554496.

ΕΣΔΑ

Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (ΔΣΑΠΔ)

ΧΘΔΕΕ

Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμος σε: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&qid=1694157262478.

Κανονισμός (ΕΕ) 2024/1083 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Απριλίου 2024, για τη θέσπιση κοινού πλαισίου για τις υπηρεσίες μέσων ενημέρωσης στην εσωτερική αγορά και την τροποποίηση της οδηγίας 2010/13/ΕΕ (Ευρωπαϊκός Νόμος για την Ελευθερία των Μέσων Ενημέρωσης). Διαθέσιμος σε: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1083.

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). Διαθέσιμη σε: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex:32002L0058.

Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, 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 και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. Διαθέσιμη σε: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32016L0680.

Υπ' αριθ. 205/2013 Απόφαση της ΑΔΑΕ (ΦΕΚ Β' 1742/15.7.2013). Διαθέσιμη σε: https://adae.gov.gr/images/nomothetiko-plaisio/Kanonismos_FEK_1742_B_15_07_2013_asfaleia_akeraiotita__ADAE_205_2013_01.pdf.

Νομολογία - Γνωμοδοτήσεις

Γνωμ 9/2009 ΕισΑΠ

Γνωμ 12/2009 ΕισΑΠ

Γνωμ 9/2011 ΕισΑΠ

Γνωμ 1/2023 ΕισΑΠ

ΑΠ 1/2001

ΑΠ 42/2004

ΑΠ 1421/2010

ΟλΑΠ 1/2017

ΑΠ 916/2019

ΑΠ 1014/2020

ΟλΑΠ 4/2024

ΟλΑΠ 5/2024

ΑΠ 587/2025

ΣτΕ 715/2013

ΣτΕ 1091/2015

ΣτΕ 1593/2016

ΣτΕ 3473/2017

ΟλΣτΕ 465/2024

ΣυμβΠλημμΑθ 613/2016

ΜΠλΣαμ 634/2012

ΕΔΔΑ, 1976, *Engel και λοιποί κατά Κάτω Χωρών*. Διαθέσιμη στο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57479%22]}.

ΕΔΔΑ, 1978, *Klass και λοιποί κατά Γερμανίας*. Διαθέσιμη στο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}.

ΕΔΔΑ, 1990, *Groppera Radio Ag και λοιποί κατά Ελβετίας*. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22ENG%22],%22appno%22:[%2210890/84%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-57623%22]}.

ΕΔΔΑ, 2001, *P.G. and J.H. κατά Ην. Βασιλείου*. Διαθέσιμη στο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59665%22]}.

ΕΔΔΑ, 2006, *Weber and Saravia κατά Γερμανίας*. Διαθέσιμη σε: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-76586%22]}.

ΕΔΔΑ, 2009, *Zolotukhin κατά Ρωσίας*. Διαθέσιμη στο: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-91222%22]}.

ΕΔΔΑ, 2009, *Iordachi και λοιποί κατά Μολδαβίας*. Διαθέσιμη σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-91245%22]}.

ΕΔΔΑ, 2010, *Kennedy κατά Ην. Βασιλείου*. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-98473%22]}.

ΕΔΔΑ, 2015, *Zakharov κατά Ρωσίας*. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22appno%22:[%2247143/06%22],%22itemid%22:[%22001-159324%22]}.

ΕΔΔΑ, 2016, *Szabo and Vissy κατά Ουγγαρίας*. Διαθέσιμο σε: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}.

ΕΔΔΑ, 2021, *Big Brother Watch και λοιποί κατά Ην. Βασιλείου*. Διαθέσιμη στο: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}.

ΕΔΔΑ, 2021, *Centrum för Rättvisa κατά Σουηδίας*. Διαθέσιμη σε: *https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210078%22]}*.

ΕΔΔΑ, 2022, *Ekimdzhiev κατά Βουλγαρίας*. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-214673%22]}.

ΕΔΔΑ, 2022, *Adomaitis κατά Λιθουανίας*. Διαθέσιμο σε: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-215168%22]}.

ΔΕΕ, Υπόθεση *Digital Rights Ireland Ltd* (C-293/12). Διαθέσιμη στο: https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EL.

ΔΕΕ, Υπόθεση *Tele 2 Sverige και Watson* (C-203/15 & C-698/2015). Διαθέσιμη στο: https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EL.

ΔΕΕ Υπόθεση *La Quadrature du Net* (C-511/18 & C-512/18).

ΔΕΕ Υπόθεση *HYA κ.λπ.* (C-349/21). Διαθέσιμη στο: https://curia.europa.eu/juris/document/document.jsf?docid=270504&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EL&cid=7351394.