ΝΟΜΙΚΗ ΣΧΟΛΗ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΤΗ ΝΟΜΙΚΗ (LLM)

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ – ΝΟΜΙΚΗ ΕΡΕΥΝΑ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ ΙΙ

Επιβλέπων Καθηγητής: Δρ. Νέστωρ Κουράκης

Θέμα: "*Ποινικό Δίκαιο και Μυστικές Υπηρεσίες: Η ποινική ευθύνη των μυστικών υπηρεσιών για παραβιάσεις της ιδιωτικότητας. Συγκριτική ανάλυση νομοθεσιων ΗΠΑ, Ηνωμένου Βασιλείου και προτάσεις βελτίωσης για την Ελλάδα*".

Λευκωσία 2025

Μεταπτυχιακός Φοιτητής
Κυριάκος Μ. Μηλιώτης
U234N0596

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ

1.1. Συνοπτική παρουσίαση 5

1.2. Μεθοδολογία και προσέγγιση 6

1.3. Διάκριση Κατασκοπείας και Παρακολούθησης 7

2. ΔΙΚΑΙΩΜΑ ΣΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ – ΑΠΟΦΑΣΕΙΣ ΕΔΔΑ 8

3. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

3.1. Μυστικές υπηρεσίες – συλλογή πληροφοριών – κατασκοπεία 10

3.2. The Brusa Agreement 1943 14

3.3. The Five Eyes Agreement 15

4. ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ

4.1. Pegasus 18

4.2. PRISM 19

4.3. ECHELON 20

4.4. Edward Snowden – Whistleblower 22

5. ΗΝΩΜΕΝΕΣ ΠΟΛΙΤΕΙΕΣ ΑΜΕΡΙΚΗΣ (ΗΠΑ)

5.1. Μυστικές Υπηρεσίες 23

5.2. Νομοθετικό πλαίσιο 25

5.3. Δικαστικές αποφάσεις 30

6. ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ (ΗΒ)

6.1. Μυστικές Υπηρεσίες 34

6.2. Νομοθετικό πλαίσιο 36

6.3. Δικαστικές αποφάσεις 41

7. ΣΥΓΚΡΙΤΙΚΗ ΑΝΑΛΥΣΗ ΗΠΑ – ΗΒ

7.1. Ομοιότητες ……43

7.2. Διαφορές ……45

8. ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΣΤΗΝ ΕΛΛΑΔΑ

8.1. Κενά και προκλήσεις στο Ελληνικό Νομικό Σύστημα ……47

8.2. Προτάσεις για αυξημένη προστασία του δικαιώματος της ιδιωτικότητας ….49

8.3. Προτάσεις για ενδεχόμενες διεθνείς συνεργασίες ……50

9. ΣΥΜΠΕΡΑΣΜΑΤΑ – ΕΠΙΛΟΓΟΣ ……51

10. ΒΙΒΛΙΟΓΡΑΦΙΑ ……55

1. ΕΙΣΑΓΩΓΗ

Το δικαίωμα στην ιδιωτικότητα αποτελεί ένα πολύ σημαντικό ανθρώπινο δικαίωμα το οποίο μεταξύ άλλων προστατεύει τους πολίτες από τις οποιεσδήποτε τυχόν αυθαίρετες παρεμβάσεις στην ιδιωτική και οικογενειακή ζωή. Η νομοθετική κατοχύρωση του εν λόγω δικαιώματος βρίσκεται σε σωρεία διεθνών και ευρωπαϊκών συμβάσεων τις οποίες έχουν κυρώσει συνολικά 167 χώρες ανά το παγκόσμιο. Πιο συγκεκριμένα, το δικαίωμα προστατεύεται, μεταξύ άλλων, από το άρθρο 12 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου[1], άρθρο 17 του Διεθνούς Συμφώνου για Αστικά και Πολιτικά Δικαιώματα[2], το άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου[3], τα άρθρα 7 και 8 του Ευρωπαϊκού Χάρτη Θεμελιωδών Δικαιωμάτων[4].

Το δικαίωμα στην ιδιωτικότητα μεταξύ άλλων προστατεύει τους ανθρώπους σε συγκεκριμένα ζητήματα όπως λόγου χάριν το σώμα τους, την οικογένεια τους, το σπίτι τους και τις επικοινωνίες τους ενώ παράλληλα περιορίζει τη συλλογή, χρήση και ανταλλαγή δεδομένων που αφορούν το άτομο που συχνά αναφέρονται ως πληροφοριακή ιδιωτικότητα[5]. Περαιτέρω, οι συμβάσεις ανθρωπίνων δικαιωμάτων οι οποίες προστατεύουν το δικαίωμα στην ιδιωτικότητα, επιβάλλουν θετική υποχρέωση στα κράτη όπως δημιουργήσουν το απαραίτητο και αναγκαίο νομικό υπόβαθρο δια την επαρκή προστασία του εν λόγω δικαιώματος έναντι παραβιάσεων ανεξαρτήτως αν οι εν λόγω παραβιάσεις γίνονται από το ίδιο το κράτος, άλλα ξένα κράτη ή/και άλλους παράγοντες[6].

Το εν λόγω δικαίωμα δεν είναι απόλυτο, υπό συγκεκριμένες προϋποθέσεις τυγχάνει περιορισμού, σε αντίθετη περίπτωση όμως κατά την οποία δεν πληρούνται οι απαραίτητες προϋποθέσεις για τον περιορισμό του δικαιώματος, τότε η οποιαδήποτε παραβίαση είναι παράνομη. Έχει λεχθεί ότι:

> «*The collection of information about an individual without his consent will always fall within the scope of Article 8. The European Court of Human Rights (ECtHR) has stated that protection of personal data is of fundamental importance to a person's enjoyment of his right to privacy (S. and Marper v. the UK, December 4, 2008). Interceptions of correspondence and telecommunications interfere with Article 8 and must meet the conditions of paragraph 2 as interpreted by the ECtHR*[7]*».*

Τα δικαστήρια, μέσα από τη νομολογία τους, έχουν αναδείξει ότι μια από τις θετικές υποχρεώσεις των κρατών έναντι των πολιτών, αναφορικά με την προστασία του δικαιώματος

---

[1] Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου (UDHR), υιοθετήθηκε με το ψήφισμα 217 A (III) της Γενικής Συνέλευσης του ΟΗΕ (10 Δεκεμβρίου 1948) art 12.

[2] Διεθνές Σύμφωνο για τα Αστικά και Πολιτικά Δικαιώματα (ICCPR), υιοθετήθηκε με ψήφισμα 2200A (XXI) της Γενικής Συνέλευσης του ΟΗΕ (16 Δεκεμβρίου 1966, τέθηκε σε ισχύ 23 Μαρτίου 1976) art 17.

[3] Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ, ECHR), υπογράφηκε στη Ρώμη στις 4 Νοεμβρίου 1950, τέθηκε σε ισχύ στις 3 Σεπτεμβρίου 1953, art 8.

[4] Ευρωπαϊκός Χάρτης Θεμελιωδών Δικαιωμάτων (ΕΧΘΔ, Charter of Fundamental Rights of European Union) [2000] EE C364/1, δεσμευτικός από τη Συνθήκη της Λισαβόνας (1 Δεκεμβρίου 2009) αρ. 7, 8.

[5] Rikke Frank Joergensen, 'Can human rights law bend mass surveillance?' (2014) 3(1) *Internet Policy Review*, https://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance acessed 13 August 2025

[6] Ibid.

[7] Ibid 3.

στην ιδιωτικότητα, είναι η σαφής και προσιτή διατύπωση της εκάστοτε ισχύουσας νομοθεσίας. Συνεπώς, οι σχετικές ρυθμίσεις οφείλουν να είναι διατυπωμένες με τρόπο κατανοητό και επαρκώς λεπτομερές, ώστε τα επηρεαζόμενα πρόσωπα να γνωρίζουν ή /και να μπορούν να αντιληφθούν πότε και με ποιον τρόπο οι μυστικές υπηρεσίες δύνανται να περιορίζουν το δικαίωμα τους στην ιδιωτική ζωή. Επιπλέον, τα κράτη έχουν την υποχρέωση να θεσπίζουν και διασφαλίζουν την ύπαρξη δικλείδων ασφαλείας, μέσω των οποίων να προβλέπεται ότι κάθε παράνομος περιορισμός του δικαιώματος θα συνεπάγεται την τιμωρία των υπαιτίων. Τέλος, τα δικαστήρια έχουν επανειλημμένως υπογραμμίσει την ανάγκη επαρκούς και αποτελεσματικής εποπτείας των μυστικών υπηρεσιών και των ενεργειών[8,9]. Το πιο πάνω επιβεβαιώνεται και από το Διεθνές Σύμφωνο για Ατομικά και Πολιτικά δικαιώματα, και συγκεκριμένα το άρθρο 17[10]. Ως προς τούτο έχει επισημανθεί ότι:

> «*Article 17 ICCPR prohibits 'arbitrary or unlawful interference with privacy, home or correspondence' and obliges all state parties to create legal frameworks for the effective protection of privacy, including adequate complaint systems and remedies for the violation of this right. […] Electronic surveillance, wire-tapping and the recording of conversations is prohibited. In addition, the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals, must be subject to appropriate state regulation and safeguards*[11]».

Συνοψίζοντας, το δικαίωμα στην ιδιωτικότητα αποτελεί έναν από τους ακρογωνιαίους λίθους της προστασίας των ανθρωπίνων δικαιωμάτων και συνιστά απαραίτητη προϋπόθεση για την ελεύθερη ανάπτυξη της προσωπικότητας και τη διασφάλιση της ανθρώπινης αξιοπρέπειας. Η καθολική αναγνώριση του τόσο σε διεθνές όσο και σε ευρωπαϊκό επίπεδο υπογραμμίζει τη σημασία του και την ανάγκη διαρκούς προστασίας απέναντι σε σύγχρονες προκλήσεις όπως η αυξανόμενη κρατική επιτήρηση και η αδιάκριτη συλλογή προσωπικών δεδομένων. Η νομολογία των διεθνών και ευρωπαϊκών δικαστηρίων έχει εδραιώσει την αρχή ότι το δικαίωμα αυτό, παρότι δεν είναι απόλυτο, μπορεί να περιορίζεται μόνο υπό αυστηρές προϋποθέσεις, με σαφή νομοθετική βάση, προβλεψιμότητα και την ύπαρξη αποτελεσματικών μηχανισμών ελέγχου. Τα κράτη επομένως, φέρουν μια διττή υποχρέωση, αφενός να προστατεύσουν το δικαίωμα αυτό από παράνομες επεμβάσεις, και αφετέρου να διασφαλίζουν μέσω θετικών μέτρων την ύπαρξη επαρκούς νομικού και θεσμικού πλαισίου που να αποτρέπει καταχρήσεις. Η ισορροπία μεταξύ προστασίας της ιδιωτικότητας και αναγκών δημόσιας ασφάλειας παραμένει μια από τις μεγαλύτερες προκλήσεις της σύγχρονης εποχής, καθιστώντας αναγκαία την ενίσχυση της διαφάνειας, της λογοδοσίας και της δημοκρατικής εποπτείας επί των μυστικών υπηρεσιών και των πρακτικών τους.

1.1. Συνοπτική παρουσίαση

Η παρούσα μελέτη διερευνά το φλέγον ζήτημα της ποινικής ευθύνης των μυστικών υπηρεσιών για παραβιάσεις του δικαιώματος της ιδιωτικότητας, αναλύοντας συγκριτικά τα

[8] Ibid.
[9] G Alex Sinha, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' (2013) 59 Loyola Law Review 923.
[10] Eliza Watt, 'The Right to Privacy and the Future of Mass Surveillance' (2017) 21(7) The International Journal of Human Rights 773.
[11] Ibid 778.

νομικά πλαίσια των ΗΠΑ, του Ηνωμένου Βασιλείου και παραθέτοντας προτάσεις βελτίωσης για την Ελλάδα. Μέσα από την ιστορική αναδρομή του φαινομένου της κατασκοπείας και της μαζικής συλλογής πληροφοριών, αναδεικνύεται η διαχρονική χρήση των μυστικών υπηρεσιών ως εργαλείο διασφάλισης της εθνικής ασφάλειας, παράλληλα με τη σταδιακή ενίσχυση των τεχνολογικών δυνατοτήτων παρακολούθησης.

Η μεθοδολογία της έρευνας βασίζεται στη συγκριτική νομική ανάλυση, με σκοπό την αξιολόγηση των διαφορετικών πλαισίων που διέπουν τη δράση των υπηρεσιών πληροφοριών και τις σχετικές εγγυήσεις προστασίας της ιδιωτικότητας. Εξετάζονται νομοθετικές πράξεις, δικαστικές αποφάσεις και διεθνείς συνθήκες, ενώ αξιοποιούνται και δευτερογενείς πηγές, όπως ακαδημαϊκά άρθρα και αναλύσεις. Η συγκριτική προσέγγιση επιτρέπει την ανάδειξη καλών πρακτικών, την εντόπιση θεσμικών κενών και την εξαγωγή συμπερασμάτων για πιθανή προσαρμογή και εφαρμογή τους στο ελληνικό νομικό περιβάλλον.

Η μελέτη εστιάζει ιδιαίτερα στην ανάλυση προηγμένων συστημάτων επιτήρησης όπως το Pegasus, το PRISM και το ECHELON, τα οποία αποδεικνύουν την εντατικοποίηση των παρακολουθήσεων σε παγκόσμιο επίπεδο και τον τρόπο με τον οποίο αυτή λαμβάνει σάρκα και οστά, συχνά χωρίς επαρκείς εγγυήσεις προστασίας της ιδιωτικής ζωής. Ιδιαίτερο βάρος δίδεται στο ρόλο του Edward Snowden ως whistleblower και στην αποκάλυψη μαζικών παραβιάσεων από τις αμερικανικές υπηρεσίες. Μέσω της ανάλυσης της σχετικής νομοθεσίας, αναδεικνύεται και η αδυναμία των θεσμικών μηχανισμών να επιβάλουν ουσιαστικό έλεγχο στις πρακτικές επιτήρησης.

Στο συγκριτικό επίπεδο εντοπίζονται κρίσιμες ομοιότητες και διαφορές μεταξύ ΗΠΑ και ΗΒ, όπως η έκταση των εξουσιών των υπηρεσιών πληροφοριών, οι δικαστικοί μηχανισμοί αδειοδότησης και η κοινοβουλευτική εποπτεία. Παρότι και τα δύο κράτη διαθέτουν θεσμικά αντίβαρα, παραμένουν σημαντικά νομοθετικά κενά, κυρίως όσον αφορά την προστασία των πολιτών και τη διεθνή συνεργασία πληροφοριών. Η ανάλυση αυτή καθίσταται ιδιαιτέρως χρήσιμη για την αξιολόγηση των αναγκών της ελληνικής έννομης τάξης.

Η εργασία ολοκληρώνεται με προτάσεις νομοθετικής και θεσμικής ενίσχυσης στην Ελλάδα, εστιάζοντας στην ανάγκη για αυξημένη διαφάνεια, αποτελεσματικό κοινοβουλευτικό έλεγχο των μυστικών υπηρεσιών και ενίσχυση των εγγυήσεων για την προστασία των προσωπικών δεδομένων. Η μελέτη συνεισφέρει ουσιαστικά στον επιστημονικό διάλογο αναφορικά με την νομική λογοδοσία των υπηρεσιών πληροφοριών και την επαναχάραξη των ορίων μεταξύ εθνικής ασφάλειας και προστασίας θεμελιωδών δικαιωμάτων στην εποχή της ψηφιακής παρακολούθησης.

1.2. Μεθοδολογία και προσέγγιση

Η παρούσα μελέτη θα βασιστεί στη συγκριτική μέθοδο σχετικά με την ανάλυση και επεξήγηση της ποινικής ευθύνης των μυστικών υπηρεσιών για παραβιάσεις της ιδιωτικότητας.

Πιο συγκεκριμένα, εξετάζονται και συγκρίνονται οι νομοθετικές ρυθμίσεις, η νομολογία και οι πρακτικές που ακολουθούνται σε ανεπτυγμένα νομικά συστήματα, ήτοι, των ΗΠΑ και ΗΒ,

οι οποίες αποτελούν δύο χώρες με μεγάλη ιστορία αναφορικά με τη χρήση μυστικών υπηρεσιών και τη συλλογή πληροφοριών.

Περαιτέρω, η συγκριτική ανάλυση εστιάζει στις ομοιότητες, τις διαφορές και τα οποιαδήποτε τυχόν νομοθετικά κενά που σχετίζονται με την ποινική ευθύνη και την προστασία της ιδιωτικότητας. Παράλληλα, η έρευνα αξιοποιεί δευτερογενείς πηγές, όπως λόγου χάριν ακαδημαϊκά άρθρα, δικαστικές αποφάσεις και διεθνείς συνθήκες.

Στο πλαίσιο αυτό, εξετάζονται και τυχόν προεκτάσεις των τεχνολογικών εξελίξεων και της χρήσης σύγχρονων εργαλείων παρακολούθησης από τις μυστικές υπηρεσίες. Απώτερος στόχος είναι η διαμόρφωση ολοκληρωμένων και τεκμηριωμένων προτάσεων σχετικά με τη βελτίωση του ελληνικού νομικού πλαισίου, δια μέσου της ενσωμάτωσης καλών πρακτικών και της άμεσης αντιμετώπισης ενδεχόμενων κενών και αδυναμιών.

1.3. Διάκριση Κατασκοπείας και Παρακολούθησης

Η κατασκοπεία και η παρακολούθηση αποτελούν δύο από τις πλέον χαρακτηριστικές πρακτικές συλλογής πληροφοριών στο πλαίσιο της εθνικής ασφάλειας και της διεθνούς πολιτικής. Παρότι συχνά χρησιμοποιούνται ως έννοιες ταυτόσημες, παρουσιάζουν ουσιώδεις διαφορές: η κατασκοπεία συνδέεται με στοχευμένες ενέργειες διείσδυσης και απόκτησης μυστικών πληροφοριών, στρατιωτικών, πολιτικών ή οικονομικών, και αποτελεί παραδοσιακά εργαλείο των κρατικών μηχανισμών πληροφοριών. Αντίθετα, η παρακολούθηση αφορά κυρίως τη συστηματική συλλογή και επεξεργασία επικοινωνιών και δεδομένων, πολλές φορές σε μαζική κλίμακα με άμεσες συνέπειες για την προστασία της ιδιωτικότητας και των θεμελιωδών δικαιωμάτων. Στον σύγχρονο ψηφιακό κόσμο, οι δύο έννοιες αλληλοσυμπλέκονται, δημιουργώντας νέες προκλήσεις τόσο για τα κράτη όσο και για το διεθνές νομικό πλαίσιο που επιχειρεί να τις ρυθμίσει.

Έχει λεχθεί ότι, η κυβερνοκατασκοπεία περιλαμβάνει σκόπιμες δραστηριότητες διείσδυσης σε υπολογιστικά συστήματα ή δίκτυα που χρησιμοποιούνται από έναν αντίπαλο, με σκοπό την απόκτηση πληροφοριών που βρίσκονται αποθηκευμένες σε αυτά ή διακινούνται μέσω αυτών των συστημάτων δικτύων. Ένα σχετικό υποσύνολο είναι η οικονομική κατασκοπεία, όπου ένα κράτος επιχειρεί να αποκτήσει μυστικά που κατέχουν ξένες εταιρείες[12]. Εξίσου σημαντική αναφορά για την κατασκοπεία βρίσκεται στο άρθρο του Darien Pun ο οποίος αναφέρει πως ο ορισμός της κατασκοπείας είναι η μη εξουσιοδοτημένη, εκ προθέσεως συλλογή πληροφοριών από τα κράτη, το οποίο περιλαμβάνει ορισμένα βασικά στοιχεία, η κατασκοπεία αναφέρεται στη συλλογή πληροφοριών, η συλλογή πληροφοριών δεν επιτρέπεται από το κράτος στόχο, η χρήση του όρου «πληροφορίες» αντί «πληροφόρηση» και τέλος αφορά αποκλειστικά δραστηριότητες που συνδέονται με κράτη, καταλήγοντας στο ότι η κυβερνοκατασκοπεία είναι απλώς η χρήση της κυβερνοτεχνολογίας για την επίτευξη των στόχων της παραδοσιακής κατασκοπείας[13].

Από την άλλη, η ηλεκτρονική παρακολούθηση υποκλέπτει επικοινωνίες μεταξύ δύο ή περισσότερων μερών. Οι υποκλοπές αυτές μπορούν να προσφέρουν εικόνα για το τι λέγεται,

[12] William C Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 *Emory LJ* 513.
[13] Darien Pun, 'Rethinking Espionage in the Modern Era' (2017) 18(1) *Chicago J Intl L* 353.

τι σχεδιάζεται και τι αναμένεται από τους αντιπάλους. Ωστόσο, επειδή πλέον μεταφέρονται τεράστιες ποσότητες επικοινωνιών μέσω του διαδικτύου, περισσότερες από όσες μπορούν οι άνθρωποι να αντιληφθούν στην ακατέργαστη μορφή τους, η παρακολούθηση συχνά οδηγεί σε επεξεργασία και αξιοποίηση μέσω αλγορίθμων ή άλλων μεθόδων αναζήτησης, οι οποίοι μπορούν να επεξεργαστούν μεγάλους όγκους συλλεγμένων δεδομένων προς επίτευξη πιο συγκεκριμένων στόχων παρακολούθησης[14].

Μια εξίσου σημαντική διαφορά μεταξύ κατασκοπείας και παρακολούθησης είναι ότι η κατασκοπεία επικεντρώνεται στη σκόπιμη, μη εξουσιοδοτημένη συλλογή πληροφοριών από κράτη, με στόχο την απόκτηση στρατηγικού πλεονεκτήματος, ενώ η παρακολούθηση συνήθως συνίσταται στην υποκλοπή επικοινωνιών για την κατανόηση όσων λέγονται, σχεδιάζονται ή αναμένονται από αντιπάλους. Η κυβερνοκατασκοπεία, αξιοποιώντας την τεχνολογία, καθιστά τη διαδικασία αυτή ευκολότερη και ασφαλέστερη, μειώνοντας σημαντικά τα κόστη και αυξάνοντας τα οφέλη, γεγονός που οδηγεί σε εκτεταμένες παραβιάσεις της ιδιωτικότητας, σε οικονομική κατασκοπεία, σε παραβίαση εμπορικών συμφωνιών, και το πιο επικίνδυνο, σε παρεμβάσεις στις κρατικές υποθέσεις από ξένα έθνη. Σε αντίθεση με το παρελθόν, όπου οι πράκτορες ρίσκαραν τη φυσική παρουσία σε ξένο έδαφος, σήμερα το διαδίκτυο και οι ψηφιακές υποδομές επιτρέπουν την άσκηση κατασκοπείας από απόσταση, δυσχεραίνοντας την απόδοση ευθύνης και την επιβολή κυρώσεων από τα κράτη-θύματα[15].

Η διάκριση μεταξύ κατασκοπείας και παρακολούθησης αναδεικνύει όχι μόνο τις διαφορετικές μεθόδους συλλογής πληροφοριών, αλλά και τις ιδιαίτερες προκλήσεις που εγείρουν στον τομέα της εθνικής ασφάλειας και της προστασίας των δικαιωμάτων. Ενώ η κατασκοπεία εστιάζει στη στοχευμένη, μυστική και μη εξουσιοδοτημένη απόκτηση στρατηγικών πληροφοριών από κράτη, η παρακολούθηση λειτουργεί ως εργαλείο ευρύτερης, συχνά μαζικής, υποκλοπής και ανάλυσης επικοινωνιών. Στο σύγχρονο ψηφιακό περιβάλλον, η κυβερνοκατασκοπεία και η ηλεκτρονική παρακολούθηση τείνουν να αλληλοεπικαλύπτονται, μετατρέποντας την τεχνολογία σε καταλύτη τόσο για την αποτελεσματικότερη συλλογή δεδομένων όσο και για την εντεινόμενη παραβίαση της ιδιωτικότητας. Το γεγονός αυτό υπογραμμίζει την ανάγκη για σαφείς ορισμούς, ισχυρό θεσμικό πλαίσιο και διεθνή συνεργασία, ώστε να διασφαλιστεί η ισορροπία ανάμεσα στην προστασία της ασφάλειας των κρατών και τον σεβασμό των θεμελιωδών δικαιωμάτων των πολιτών.

2. ΔΙΚΑΙΩΜΑ ΣΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ – ΑΠΟΦΑΣΕΙΣ ΕΔΔΑ

Το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) έχει διαδραματίσει καθοριστικό ρόλο στη διαμόρφωση των αρχών προστασίας της ιδιωτικότητας στην Ευρώπη, βασισμένο στην εν ισχύι νομοθεσία όπως αυτή αναφέρεται στην παρ.1 ανωτέρω. Μέσα από μια πλούσια νομολογία, το Δικαστήριο έχει θέσει τα όρια ανάμεσα στην κρατική παρέμβαση και το δικαίωμα του ατόμου σε μια ιδιωτική και οικογενειακή ζωή όπως κατοχυρώνεται στο άρθρο 8 της ΕΣΔΑ. Από την υπόθεση Klass έως πιο πρόσφατες αποφάσεις όπως η Big Brother Watch, το ΕΔΔΑ υπογραμμίζει διαρκώς την ανάγκη ύπαρξης επαρκών νομικών εγγυήσεων σε

[14] William C Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 *Emory LJ* 513.

[15] Darien Pun, 'Rethinking Espionage in the Modern Era' (2017) 18(1) *Chicago J Intl L* 353.

καταχρήσεις εξουσίας. Έτσι, οι αποφάσεις του αποτελούν σημείο αναφοράς για την ισορροπία ανάμεσα στην ασφάλεια και τον σεβασμό των θεμελιωδών δικαιωμάτων.

Η υπόθεση *Klass and Others v. Germany (1978)*[16], αφορούσε προσφυγή Γερμανών πολιτών κατά του νόμου «G 10 Act», ο οποίος επέτρεπε στις μυστικές υπηρεσίες να παρακολουθούν τηλεπικοινωνίες για λόγους εθνικής ασφάλειας χωρίς να ενημερώνεται ο πολίτης. Οι προσφεύγοντες υποστήριξαν ότι ακόμη και η πιθανότητα να υπόκεινται σε τέτοια μυστική παρακολούθηση συνιστούσε παραβίαση της ιδιωτικής τους ζωής. Το Δικαστήριο εξέτασε για πρώτη φορά σε βάθος τη νομιμότητα μυστικών συστημάτων παρακολούθησης και τις αναγκαίες εγγυήσεις κατά της κατάχρησης. Το Δικαστήριο, στην παρ. 36 της απόφασης του επισημαίνει ότι, όταν ένα κράτος θεσπίζει μυστική παρακολούθηση, της οποίας η ύπαρξη παραμένει άγνωστη στα πρόσωπα που ελέγχονται, με αποτέλεσμα η παρακολούθηση να μην μπορεί να αμφισβητηθεί, το άρθρο 8 θα μπορούσε σε μεγάλο βαθμό να καταστεί ανενεργό. Επιπρόσθετα το Δικαστήριο επισημαίνει ότι, σε μια τέτοια περίπτωση είναι δυνατό ένα άτομο να στερηθεί το δικαίωμα που απονέμεται από το άρθρο αυτό, χωρίς να το γνωρίζει και επομένως χωρίς να έχει τη δυνατότητα να εξασφαλίσει θεραπεία είτε σε εθνικό επίπεδο είτε ενώπιον των οργάνων της Σύμβασης[17]. Εν συνεχεία, το Δικαστήριο παρατήρησε ότι η αμφισβητούμενη νομοθεσία θέσπιζε ένα σύστημα παρακολούθησης δυνάμει του οποίου όλα τα πρόσωπα στη Γερμανική Ομοσπονδιακή Δημοκρατία μπορούν δυνητικά να έχουν την αλληλογραφία και τα τηλεπικοινωνιακά τους μέσα υπό παρακολούθηση χωρίς ποτέ να το γνωρίζουν, κάτι το οποίο επηρεάζει άμεσα όλους τους χρήστες ή δυνητικούς χρήστες των ταχυδρομικών και τηλεπικοινωνιακών υπηρεσιών στη Γερμανία[18]. Πολύ σημαντική αναφορά του Δικαστηρίου γίνετε στην παρ. 41 της απόφασης του εις την οποία επισημαίνει ότι, αν και οι τηλεφωνικές συνομιλίες δεν αναφέρονται ρητώς στην παράγραφο 1 του άρθρου 8, το Δικαστήριο θεωρεί, όπως και η Επιτροπή, ότι τέτοιες συνομιλίες εμπίπτουν στις έννοιες της «ιδιωτικής ζωής» και της «αλληλογραφίας» που αναφέρονται στη διάταξη αυτή[19]. Το Δικαστήριο κατέληξε ότι, παρόλο που η μυστική παρακολούθηση συνιστά σοβαρή παρέμβαση στο δικαίωμα της ιδιωτικότητας, μπορεί να θεωρηθεί συμβατή με το άρθρο 8 εφόσον συνοδεύεται από επαρκείς και αποτελεσματικές εγγυήσεις έναντι καταχρήσεων. Εξετάζοντας το γερμανικό σύστημα εποπτείας (δικαστική και κοινοβουλευτική), το Δικαστήριο εν τέλει έκρινε ότι οι εγγυήσεις ήταν ικανοποιητικές και, συνεπώς δεν υπήρξε παραβίαση του άρθρου 8.

Στην υπόθεση Barbulescu v. Romania (2017), το ΕΔΔΑ κατέληξε ότι υπήρξε παραβίαση του άρθρου 8 ΕΣΔΑ. Το Δικαστήριο έκρινε πως, παρότι οι εργοδότες έχουν δικαίωμα να επιβλέπουν τη χρήση των εργαλείων εργασίας, τα εθνικά δικαστήρια δεν προστάτευσαν επαρκώς το δικαίωμα του εργαζομένου στην ιδιωτική ζωή και την αλληλογραφία του. Η Ρουμανία δεν εξασφάλισε δίκαιη ισορροπία ανάμεσα στο συμφέρον του εργοδότη και στην ιδιωτικότητα του εργαζομένου, διότι η παρακολούθηση ήταν υπερβολικά παρεμβατική και χωρίς σαφείς εγγυήσεις[20]. Στην παρ. 70 της απόφασης του το Δικαστήριο εξετάζει τον όρο «ιδιωτική ζωή» επισημαίνοντας ότι αποτελεί ένα ευρύ όρο ο οποίος δεν επιδέχεται εξαντλητικό ορισμό. Το άρθρο 8 της Σύμβασης προστατεύει το δικαίωμα της προσωπικής

[16] *Case of Klass and Others v Germany* (App no 5029/71) ECHR 6 September 1978.
[17] Ibid par.36.
[18] Ibid par.37.
[19] Ibid par. 41.
[20] *Case of Bărbulescu v Romania* (App no 61496/08) ECHR 5 September 2017 (Grand Chamber)

ανάπτυξης είτε ως προς την προσωπικότητα, είτε ως προς την προσωπική αυτονομία, η οποία αποτελεί θεμελιώδη αρχή που διέπει την ερμηνεία των εγγυήσεων του άρθρου 8. Περαιτέρω το Δικαστήριο τονίζει και αναγνωρίζει ότι κάθε άτομο έχει το δικαίωμα να ζει ιδιωτικά, μακριά από ανεπιθύμητη προσοχή. Επιπλέον θεωρεί ότι θα ήταν υπερβολικά περιοριστικό να περιοριστεί η έννοια της «ιδιωτικής ζωής» σε ένα «εσωτερικό κύκλο», εντός του οποίου το άτομο μπορεί να ζει την προσωπική του ζωή όπως επιλέγει, αποκλείοντας πλήρως τον έξω κόσμο που δεν εμπίπτει σε αυτό τον κύκλο[21]. Συνεπώς, το άρθρο 8 κατοχυρώνει το δικαίωμα στην «ιδιωτική ζωή» υπό την ευρεία έννοια, που περιλαμβάνει το δικαίωμα σε μια «ιδιωτική κοινωνική ζωή», δηλαδή τη δυνατότητα του ατόμου να αναπτύσσει την κοινωνική του ταυτότητα[22]. Ιδιαίτερη αναφορά γίνετε από το Δικαστήριο στην παρ. 72 όσον αφορά την έννοια της αλληλογραφίας, σημειώνοντας ότι στη διατύπωση του άρθρου 8 η λέξη αυτή δεν συνοδεύεται από κανένα επίθετο, σε αντίθεση με τον όρο «ζωή», επισημαίνοντας παράλληλα ότι οι τηλεφωνικές επικοινωνίες καλύπτονται από τις έννοιες της «ιδιωτικής ζωής» και της «αλληλογραφίας» κατά την έννοια του άρθρου 8[23]. Συνεπώς, στην παρούσα υπόθεση το ΕΔΔΑ επιβεβαίωσε την ευρύτητα της προστασίας του άρθρου 8, καλύπτοντας τόσο την προσωπική ανάπτυξη όσο και τις κοινωνικές σχέσεις και την αλληλογραφία. Η απόφαση αυτή ενισχύει την αντίληψη ότι η ιδιωτικότητα δεν περιορίζεται σε στενό «εσωτερικό κύκλο», αλλά εκτείνεται σε κάθε πτυχή της ανθρώπινης αλληλεπίδρασης.

Οι αποφάσεις Klass και Barbulescu αποτελούν θεμελιώδεις σταθμούς στη νομολογία του ΕΔΔΑ για την προστασία της ιδιωτικότητας. Μέσα από αυτές, το Δικαστήριο ανέδειξε τόσο την ανάγκη ύπαρξης αποτελεσματικών εγγυήσεων απέναντι σε κρατικές παρεμβάσεις μυστικής παρακολούθησης όσο και την προστασία της ιδιωτικής ζωής και αλληλογραφίας στο εργασιακό περιβάλλον. Κοινός παρονομαστής είναι ότι το άρθρο 8 της ΕΣΔΑ ερμηνεύεται δυναμικά και ευρύτατα, διασφαλίζοντας πως η ιδιωτικότητα δεν περιορίζεται σε έναν στενό ατομικό χώρο, αλλά εκτείνεται σε όλες τις πτυχές της ανθρώπινης ζωής και αλληλεπίδρασης, αποτελώντας θεμέλιο για μια δημοκρατική κοινωνία.

3. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

3.1. Μυστικές υπηρεσίες – συλλογή πληροφοριών – κατασκοπεία

Η ανάγκη για συλλογή πληροφοριών και παρακολούθησης είναι κάτι το οποίο υπήρχε από την αρχαιότητα, καθότι, δια μέσου αυτού οι κοινωνίες διασφάλιζαν την ασφάλεια τους, πολιτική σταθερότητα και οικονομική ευημερία, όπως επίσης και την επικράτηση εναντίον των εχθρών τους εν καιρώ πολέμου. Αρχαίοι πολιτισμοί, όπως λόγου χάριν οι Έλληνες και οι Ρωμαίοι, συνήθιζαν να συλλέγουν πληροφορίες με σκοπό να αποκτήσουν στρατηγικό πλεονέκτημα στους επικείμενους πολέμους τους. Για αυτούς, η κατασκοπεία και η παρακολούθηση των εχθρών τους αποτελούσε αδήριτη ανάγκη για την αποτελεσματική στρατηγική και την πρόληψη επιθέσεων. Δια μέσου της κατασκοπείας μάθαιναν πληροφορίες όπως τα όπλα που είχαν διαθέσιμα οι αντίπαλοι τους, ο τρόπος με τον οποίο σχεδίαζαν τις επιθέσεις τους, την αριθμητική τους δύναμη και άλλα[24].

[21] Ibid par. 70.
[22] Ibid.
[23] Ibid par. 72.
[24] Konstantinos Markopoulos, 'Η κατασκοπία στην αρχαία Ελλάδα. Οι μυστικοί πράκτορες της Τροίας και οι συμβουλές για να αντιμετωπιστούν οι κατάσκοποι του εχθρού' (Μηχανή του Χρόνου, 21 February 2025) https://www.mixanitouxronou.gr/i-

Για παράδειγμα, στην αρχαία Ελλάδα υπάρχουν καταγραφές ότι κατάσκοποι των εχθρών ντύνονταν με γυναικεία ρούχα έτσι ώστε να μπουν στις πόλεις που ήθελαν να κατασκοπεύσουν μαζί με μεγάλο αριθμό άλλων γυναικών οι οποίες επέστρεφαν στην πόλη από τα χωράφια[25]. Η χρήση κατασκόπων ήταν τόσο σημαντική, που «*Ο Ξενοφώντας γράφει ότι καλό είναι 'να μεριμνούμε για ύπαρξη κατασκόπων πριν από την κήρυξη ενός πολέμου, ώστε να είναι υπήκοοι κράτους φιλικού και προς τον εχθρό και προς εμάς, καθώς και να είναι έμποροι, γιατί όλα τα κράτη όταν εισάγουν αγαθά, τα παίρνουν από φιλικά διακείμενους εμπόρους. Είναι και οι ψευδαυτόμολοι χρήσιμοι. Όμως πρέπει να είμαστε πάντα προσεκτικοί με τους κατασκόπους μας ακόμα κι αν τους έχουμε εμπιστοσύνη, γιατί όσο αξιόπιστοι κι αν είναι, δύσκολα δίνουν εγκαίρως τις πληροφορίες τους*[26]».

Επιπρόσθετα, χρήση διαφόρων ειδών κατασκόπων υφίστατο και στην Ρωμαϊκή αυτοκρατορία. Διαχωρίζονται 2 είδη κατασκόπων στην αρχαία Ρώμη, οι "exploratores" και οι «speculatores", οι πρώτοι ήταν ιππείς κατάσκοποι ενώ οι δεύτεροι ήταν αγγελιαφόροι πληροφοριών και μυστικοί πράκτορες[27]. Αφενός, οι exploratores αποστέλνονταν σε συγκεκριμένες ειδικές αποστολές, ήτοι, να εντοπίσουν την τοποθεσία των αντιπάλων και να ενημερώσουν την ηγεσία σχετικά με τις κινήσεις τους, πληροφορίες οι οποίες αξιοποιούνταν για την αποτροπή της οποιασδήποτε αιφνιδιαστικής επίθεσης, ενώ παράλληλα αξιοποιούνταν για καλύτερη και πληρέστερη προετοιμασία και υπό προϋποθέσεις για αιφνιδιαστικές επιθέσεις στους αντιπάλους τους[28]. Αφετέρου, οι speculatores, λειτουργούσαν σε μικρές ομάδες, συνήθως ομάδες δύο ατόμων, και στόχος τους ήταν η παρακολούθηση των αντιπάλων εν μέσω της νύχτας από συγκεκριμένα σημεία στις περιπτώσεις που οι στρατοί βρίσκονταν κοντά ο ένας με τον άλλο ειδικά την προηγούμενη νύχτα της επικείμενης μάχης[29]. Με την πάροδο των χρόνων, και εφόσον ο θεσμός των speculatores και exploratores έδειξε έμπρακτα ότι μπορούσε να συνεισφέρει τα μέγιστα στις στρατιωτικές επιχειρήσεις της Ρωμαϊκής αυτοκρατορίας, θεσπίστηκε ο θεσμός των frumentarii[30], η προέλευση του οποίου παραμένει μέχρι και σήμερα ασαφής. Οι άνδρες οι οποίοι απάρτιζαν τους frumentarii, ήταν λεγεωνάριοι στρατιώτες οι οποίοι ενεργούσαν ως αγγελιοφόροι μεταξύ των επαρχιακών πρωτευουσών και της Ρώμης, αλλά μπορούσαν επίσης να αναλάβουν καθήκοντα που περιλάμβαναν είσπραξη φόρων, κατασκοπεία και πολιτικές δολοφονίες[31]. Περαιτέρω, αυτοί οι στρατιώτες αποτέλεσαν το πρώτο νέο θεσμικό όργανο το οποίο δημιουργήθηκε για να κρατά τον αυτοκράτορα ενημερωμένο σχετικά με τις εξελίξεις στις επαρχίες, στην πρωτεύουσα και στην αυλή του[32].

Με την ίδια λογική, όπως και οι αρχαίοι πολιτισμοί, έτσι και οι σύγχρονες κοινωνίες έχουν την ανάγκη για κατασκοπεία και συλλογή πληροφοριών, η οποία κατά κύριο λόγο προκύπτει

---

kataskopia-stin-archaia-ellada-oi-mystikoi-praktores-tis-troias-kai-oi-symvoyles-gia-na-antimetopistoyn-oi-kataskopoi-toy-echthroy/ accessed 21 February 2025.

[25] Olga Mavrou, 'Οι κατάσκοποι στην αρχαία Ελλάδα – Ποια ήταν τα τεχνάσματα τους' (SL Press, 15 May 2023) https://slpress.gr/istorimata/oi-kataskopoi-stin-archaia-ellada-poia-itan-ta-technasmata-toys/?utm_source=chatgpt.com accessed 21 February 2025.

[26] Ibid.

[27] Rose Mary Sheldon, *Intelligence Activities in Ancient Rome* (Routledge, Taylor & Francis Group 2005) 192

[28] Ibid.

[29] Ibid.

[30] Ibid. 279

[31] Ibid.

[32] Ibid.

από την επιθυμία των κρατών και των οργανισμών τους να προστατεύσουν τα συμφέροντα τους, να διασφαλίσουν την εθνική ασφάλεια, και επίσης να αποκτήσουν στρατηγικό πλεονέκτημα έναντι των εχθρών τους. Ωστόσο, σημαντική συμβολή στην σύγχρονη κατασκοπεία, συλλογή πληροφοριών, και τις μαζικές παρακολουθήσεις έχει και η ραγδαία τεχνολογική ανάπτυξη, η παγκοσμιοποίηση και οι συνεχόμενες αλλαγές και εξελίξεις είτε στα πολιτικά δρώμενα είτε σχετικά με γεωπολιτικές συνθήκες. Η σύγχρονη κατασκοπεία και μαζική συλλογή πληροφοριών περιλαμβάνει, πέραν των παραδοσιακών τεχνικών, όπως λόγου χάριν η ανθρώπινη κατασκοπεία, αλλά και πιο σύγχρονες, μοντέρνες τεχνικές, όπως για παράδειγμα η ηλεκτρονική κατασκοπεία, συλλογή πληροφοριών και άλλα.

Επίσης, εξίσου σημαντικό σημείο αναφοράς αποτελούν και οι διάφορες εμπόλεμες συρράξεις μεταξύ των σύγχρονων κρατών, και πιο συγκεκριμένα οι δύο Παγκόσμιοι Πόλεμοι, οι οποίοι είχαν καθοριστική συμβολή στην ανάπτυξη της κατασκοπείας και συλλογής πληροφοριών. Κατά την διάρκεια των δύο αυτών πολέμων, υπήρχε μεγάλη ανάγκη για τη συλλογή στρατηγικών πληροφοριών, και επίσης την ανάπτυξη νέων τεχνολογιών. Κατά τον Α' Παγκόσμιο Πόλεμο η ανάγκη για τη συλλογή αξιόπιστων πληροφοριών οδήγησε στη δημιουργία/μετονομασία, των γνωστών σήμερα μυστικών υπηρεσιών, όπως λόγου χάριν το Βρετανικό MI5 και MI6, ενώ παράλληλα αναπτύχθηκε η κρυπτογραφία, κάτι το οποίο επέτρεπε στους χρήστες των τηλεγράφων να έχουν ασφαλέστερη και ταχύτερη επικοινωνία[33]. Κατά τον Β' Παγκόσμιο Πόλεμο, υπήρξε σημαντική ανάγκη αναφορικά με την αποκρυπτογράφηση εχθρικών επικοινωνιών, δια την καλύτερη προετοιμασία με βάση τις κινήσεις των Γερμανών, και πιο συγκεκριμένα με την αποκρυπτογράφηση του κωδικού Enigma των Ναζί[34].

Το κατασκοπευτικό σκάνδαλο του 1994, γνωστό και ως Ames spy scandal, το οποίο έλαβε χώρα μετά τη λήξη του Ψυχρού Πολέμου, αποτελεί ακόμη ένα σημαντικό γεγονός στον κατασκοπευτικό κόσμο, και τη συλλογή πληροφοριών, αναδεικνύοντας τη σημαντικότητα τους στη μεταπολεμική εποχή και παράλληλα δείχνοντας τη σημαντικότητα της συλλογής πληροφοριών από εχθρικά κράτη[35]. Ο Aldrich Ames ήταν πράκτορας της CIA, ο οποίος κατασκόπευε μυστικά για τους Ρώσους από το 1985 μέχρι και το 1994. Κατά τα 9 χρόνια κατασκοπίας του αποκάλυψε σημαντικές πληροφορίες σχετικά με διάφορους πράκτορες των ΗΠΑ τους οποίους στην πορεία η Σοβιετική Ένωση δολοφόνησε[36].

Συν τοις άλλοις, σημαντικό γεγονός άξιο προς αναφορά αποτελεί η τρομοκρατική επίθεση της 11ης Σεπτεμβρίου 2001 στις ΗΠΑ, αφού, η αδυναμία των αμερικανικών μυστικών υπηρεσιών να αποτρέψουν την επίθεση προκάλεσε σημαντικές και δραστικές αλλαγές όσο αφορά την προσέγγιση τους σε θέματα εθνικής ασφάλειας, κάτι το οποίο είχε ως αποτέλεσμα τις μαζικές παρακολουθήσεις και τη συνεχόμενη συλλογή πληροφοριών. Πιο συγκεκριμένα έχει λεχθεί ότι:

---

[33] 'Πάντα μυστική και αμφιλεγόμενη' (Το Βήμα, 24 Νοεμβρίου 2008) https://www.tovima.gr/2008/11/24/archive/panta-mystiki-kai-amfilegomeni/ accessed 22 February 2025.

[34] Γρηγόρης Κεντητός, 'Ο κωδικός Enigma των Ναζί και πώς κατάφεραν να τον σπάσουν' (Sportime, 21 February 2025) https://www.sportime.gr/must-read/o-kodikos-enigma-ton-nazi-ke-pos-kataferan-na-ton-spasoun/?utm_source=chatgpt.com accessed 22 February 2025.

[35] 'The Aldrich Ames Case' (FBI, 21 February 2025) https://www.fbi.gov/history/famous-cases/aldrich-ames accessed 22 February 2025.

[36] Ibid.

«*Before 9/11, no agency of the U.S. government systematically analyzed terrorists travel strategies. Had they done so, they could have discovered the ways in which the terrorist predecessors to al Qaeda had been systematically but detectably exploiting weaknesses in our border security since the early 1990s. […] Since 9/11, significant improvements have been made to create an integrated watchlist that makes terrorist name information available to border and law enforcement authorities. […] Internationally and in the United States, constraining terrorist travel should become a vital part of counterterrorism strategy. Better technology and training to detect terrorist travel documents are most important immediate steps to reduce America's vulnerability to clandestine entry* [37]».

«Exchanging terrorist information with other countries, consistent with privacy requirements, along with listings of lost and stolen passports, will have immediate security benefits [38]*».*

«Rice told us she understood that the FBI had tasked its 56 U.S. field offices to increase surveillance of suspected terrorists and to reach out to informants who might have information about terrorist plots[39]».

Μετά την τρομοκρατική επίθεση της 11ης Σεπτεμβρίου, η οποία ανέδειξε τις σοβαρές αδυναμίες στην προληπτική δράση των μυστικών υπηρεσιών, η ανάγκη για ενίσχυση της επιτήρησης και παρακολούθησης των τρομοκρατικών στοιχείων έγινε επιτακτική. Οι μυστικές υπηρεσίες, τόσο των ΗΠΑ όσο και διεθνώς, προχώρησαν σε σημαντικές μεταρρυθμίσεις και βελτιώσεις στις διαδικασίες ανάλυσης και καταγραφής δεδομένων με απώτερο σκοπό την αποτροπή μελλοντικών επιθέσεων. Η ανάπτυξη διασυνδεδεμένων λιστών παρακολούθησης, η ανταλλαγή πληροφοριών με άλλες χώρες και η εστίαση στην καλύτερη αναγνώριση και ανίχνευση ταξιδιωτικών εγγράφων, αποτέλεσαν θεμελιώδη βήματα στην στρατηγική εναντίον της τρομοκρατίας. Οι ενισχυμένες παρακολουθήσεις, η χρήση προηγμένων τεχνολογιών και η συστηματική συλλογή πληροφοριών απέκτησαν πλέον κεντρικό ρόλο στην παγκόσμια αντιτρομοκρατική πολιτική, συμβάλλοντας σε μια νέα εποχή παρακολούθησης και αυξημένης ασφάλειας, όπου η προστασία της εθνικής ασφάλειας τίθεται σε προτεραιότητα, συχνά με θυσία της ιδιωτικότητας.

Ένα πρόσφατο περιστατικό που αναδεικνύει τη συνεχιζόμενη παρουσία της κατασκοπείας στις σύγχρονες κοινωνίες αποτελεί η καταδίκη έξι Βούλγαρων υπηκόων, οι οποίοι διέμεναν μόνιμα στο Ηνωμένο Βασίλειο και παραδέχθηκαν ενώπιον των βρετανικών δικαστηρίων ότι κατασκόπευαν για λογαριασμό των ρωσικών μυστικών υπηρεσιών. Συγκεκριμένα, τα μέλη της ομάδας αυτής, μεταξύ των οποίων οι Katrin Ivanova, Vanya Gaberova, Tihomir Ivanchev, Bizer Dzhambazov και Ivan Stoyanov, καταδικάστηκαν βάσει των διατάξεων του βρετανικού Criminal Law Act 1977. Η υπόθεση αυτή υπογραμμίζει τη συνεχιζόμενη ύπαρξη κατασκοπευτικών δραστηριοτήτων ακόμη και σε χώρες με ισχυρές δομές ασφαλείας, όπως το Ηνωμένο Βασίλειο. Αναδεικνύει επίσης την πολυπλοκότητα των σύγχρονων κατασκοπευτικών δικτύων, τα οποία μπορούν να λειτουργούν αθόρυβα μέσα σε κοινωνίες,

[37] The 9/11 Commission, 'The 9/11 Commission Report' (Government Printing Office, 22 July 2004) https://govinfo.library.unt.edu/911/report/911Report.pdf accessed 22 February 2025, pp 383-385
[38] Ibid.
[39] Ibid. p.264

εκμεταλλευόμενα την παγκοσμιοποίηση και την τεχνολογική πρόοδο για τη συλλογή και μεταφορά πληροφοριών. Αυτό το περιστατικό αποτελεί μια υπενθύμιση της ανάγκης για συνεχή επαγρύπνηση και ενίσχυση των μηχανισμών αντικατασκοπείας, προκειμένου να προστατευθούν τα εθνικά συμφέροντα και η ασφάλεια των πολιτών[40].

Συμπερασματικά, η κατασκοπεία και η συλλογή πληροφοριών αποτελούν αναπόσπαστο κομμάτι της ανθρώπινης ιστορίας εξελισσόμενες παράλληλα με τις κοινωνίες και τις τεχνολογικές τους δυνατότητες. Από την αρχαιότητα μέχρι τη σύγχρονη εποχή, η ανάγκη για ασφάλεια, στρατηγικό πλεονέκτημα και πρόληψη απειλών οδήγησε στη συνεχή ανάπτυξη πρακτικών κατασκοπείας, προσαρμοσμένων στις εκάστοτε συνθήκες και απαιτήσεις. Η ραγδαία τεχνολογική πρόοδος, ιδιαίτερα κατά τον 20ο και 21ο αιώνα, επέτρεψε τη μετάβαση από τις παραδοσιακές μεθόδους συλλογής πληροφοριών σε σύγχρονες πρακτικές ηλεκτρονικής επιτήρησης, μαζικών παρακολουθήσεων και κρυπτογραφικών επιχειρήσεων. Οι δύο Παγκόσμιοι Πόλεμοι ανέδειξαν τη σημασία των μυστικών υπηρεσιών, ενώ ο Ψυχρός Πόλεμος και τα μετέπειτα σκάνδαλα, όπως αυτό του Ames, κατέδειξαν το συνεχή ανταγωνισμό μεταξύ κρατών στον τομέα της πληροφόρησης. Ιδιαίτερα μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001, η κατασκοπεία και η παρακολούθηση απέκτησαν ακόμα πιο κεντρικό ρόλο στις πολιτικές εθνικής ασφάλειας, με έμφαση στη μαζική συλλογή δεδομένων και τη διακρατική συνεργασία για την καταπολέμηση της τρομοκρατίας. Ωστόσο, η εντατικοποίηση αυτών των πρακτικών, έχει εγείρει σοβαρές ανησυχίες σχετικά με τα όρια μεταξύ ασφάλειας και προστασίας της ιδιωτικής ζωής. Συνεπώς, η σύγχρονη κατασκοπεία και οι παρακολουθήσεις αποτελούν μια διττή πραγματικότητα, αφού αφενός είναι απαραίτητες για την πρόληψη απειλών και τη διατήρηση της σταθερότητας, αφετέρου όμως μπορούν να οδηγήσουν σε καταχρήσεις εξουσίας και περιορισμό ατομικών δικαιωμάτων. Η διαρκής αναζήτηση ισορροπίας μεταξύ εθνικής ασφάλειας και προστασίας των προσωπικών δεδομένων, ιδιωτικότητας, καθίσταται πιο κρίσιμη από ποτέ, καθώς οι τεχνολογικές εξελίξεις συνεχίζουν να επαναπροσδιορίζουν το τοπίο της παγκόσμιας πληροφόρησης και επιτήρησης.

3.2. The Brusa Agreement 1943

Στις 17 Μαΐου 1943, κατά τη διάρκεια του Β' Παγκόσμιου Πόλεμου, υπογράφηκε μεταξύ του War Department των ΗΠΑ και τις Βρετανικής Κυβέρνησης Code and Cipher School, μυστική συμφωνία για συγκεκριμένου είδους συλλογής μυστικών πληροφοριών, γνωστή και ως The Brusa Agreement[41]. Η ανάγκη του ΗΒ για το ανθρώπινο δυναμικό των ΗΠΑ, καθώς και της εντυπωσιακής βιομηχανικής ικανότητας και τεχνογνωσίας για την άμεση κάλυψη της ζήτησης για πρόσθετες μηχανές αποκωδικοποίησης Enigma είχαν ως αποτέλεσμα τη σύναψη της ως άνω συμφωνίας[42].

Σε γράμμα ημ. 10 Ιουνίου 1943, το οποίο αποστέλλετε προς τον Chief of Staff των ΗΠΑ, και εις το οποίο επισυνάπτεται αντίγραφο της ως άνω συμφωνίας, στην δεύτερη παράγραφο αναφέρετε ότι:

---

[40] 'Six arrested for operating a Russian spy ring in UK' (*UK Defence Journal*, March 10, 2025) https://ukdefencejournal.org.uk/six-arrested-for-operating-a-russian-spy-ring-in-uk/ accessed 22 February 2025.

[41] 'Special Intelligence Report, 10 June 1943' (US Department of Defense, 10 June 1943) https://media.defense.gov/2021/Jul/15/2002763671/-1/-1/0/SPEC_INT_10JUN43.PDF accessed 22 February 2025.

[42] Stephen Budiansky, *Code Warriors, NSA's Codebrakers and the Secret Intelligence War Against the Soviet Union,* page 44

«*2. This agreement covers the production, exchange and dissemination of all special intelligence derived by cryptanalysis of the communications of the military and air forces of the Axis powers, including their secret service*[43]».

Η εν λόγω συμφωνία αφορούσε τη μυστική συλλογή πληροφοριών από τις Δυνάμεις του Άξονα, Γερμανία, Ιταλία και Ιαπωνία, και ανταλλαγή αυτών μεταξύ ΗΠΑ και ΗΒ[44]. Πιο συγκεκριμένα, σύμφωνα με τις παραγράφους (2) και (3) της συμφωνίας, οι ΗΠΑ είχαν αναλάβει τη συλλογή πληροφοριών από την Ιαπωνία, ενώ το ΗΒ από τις Γερμανία και Ιταλία[45], πληροφορίες οι οποίες στη συνέχεια ανταλλάσσονταν μεταξύ των δύο κρατών. Η συγκεκριμένη συμφωνία, έπρεπε να διατηρηθεί απολύτως μυστική από τα εμπλεκόμενα κράτη, καθότι τυχόν διάρρευση πληροφοριών προς τον εχθρό να επηρέαζε δυσμενώς τις επιχειρήσεις των κρατών και την προσπάθεια τους να επικρατήσουν του μαινόμενου πόλεμου[46]. Ως προς τούτο, αναφέρετε ρητώς στη συμφωνία ότι:

«*4) When ULTRA information is to be used by the Commander of an Army or an Air Force as a basis for action to be taken by a subordinate command, the information must be translated, when passed to the subordinate command, into terms of an operational order, so worded that if captured or intercepted by the enemy the origin of the information could not be tracked back to the ULTRA source, e.g., orders must never contain the precise time, date or place of an enemy operation revealed by ULTRA […]*[47]».

Συμπερασματικά, η ως άνω συμφωνία αποτέλεσε μια από τις σημαντικότερες συμφωνίες για την ανταλλαγή μυστικών πληροφοριών κατά τη διάρκεια του Β' Παγκόσμιου Πόλεμου. Επικεντρώθηκε στην κρυπτοανάλυση των επικοινωνιών των Δυνάμεων του Άξονα, περιλαμβανομένων των Γερμανών, Ιταλών και Ιαπώνων, και στη μυστική ανταλλαγή αυτών των πληροφοριών μεταξύ ΗΠΑ και ΗΒ. Η συμφωνία αυτή διασφάλισε την αποτελεσματικότητα των στρατηγικών επιθέσεων και επιχειρήσεων των δύο χωρών, μέσω της συλλογής και ανάλυσης κωδικοποιημένων μηνυμάτων, καθώς και της προστασίας αυτών των πληροφοριών από τυχόν διαρροές. Ιδιαίτερη έμφαση δόθηκε στην απόλυτη μυστικότητα των πληροφοριών, όπως αποδεικνύεται από τις διατάξεις που όριζαν ότι οι πληροφορίες δεν πρέπει να ενσωματώνονται σε επιχειρησιακές εντολές με τρόπο που να οδηγούν στον εντοπισμό της προέλευσης τους από τον εχθρό. Τέλος, η συμφωνία BRUSA, όχι μόνο ενίσχυσε τη στρατηγική συνεργασία μεταξύ των δύο μεγάλων δυνάμεων, αλλά αποτέλεσε και το θεμέλιο για τη μακροχρόνια συμμαχία στην κατασκοπεία και την ανταλλαγή πληροφοριών, η οποία θα συνεχιστεί και μετά τη λήξη του πολέμου, με τη δημιουργία της συμφωνίας UKUSA και τη σύσταση του δικτύου Five Eyes.

3.3. The Five Eyes Agreement

[43] 'Special Intelligence Report, 10 June 1943' (US Department of Defense, 10 June 1943) https://media.defense.gov/2021/Jul/15/2002763671/-1/-1/0/SPEC_INT_10JUN43.PDF accessed 22 February 2025. p. 1, para. 2

[44] Ibid. 3 [11] - [13]

[45] Ibid. 2 [2] – [3]

[46] Ibid. 1- [3]

[47] Ibid. 10 [4]

Με το τέλος του Β' Παγκοσμίου Πολέμου, τα κράτη τα οποία υπέγραψαν την Brusa Agreement (ανωτέρω) ήταν αναγκασμένα να επανεκτιμήσουν την ανάγκη για μια τέτοια συνεργασία, όπου εν τέλει κατέληξαν να μετατρέψουν τη συνεργασία της πολεμικής περιόδου σε μια μεταπολεμική συμμαχία[48]. Αυτή η συμμαχία, γνωστή και ως Five Eyes Agreement υπογράφηκε στις 5 Μαρτίου 1946, η οποία υπογράφηκε με γνώμονα τη συνεργασία σε εθνική βάση μεταξύ ΗΒ και ΗΠΑ, αντιθέτως με ότι συνέβαινε κατά τη διάρκεια της πολεμικής περιόδου, δηλαδή, τις συμφωνίες σε επίπεδο επιμέρους τμημάτων με ξεχωριστές συμφωνίες για το στρατό και το ναυτικό[49]. Η συμφωνία Five Eyes αποτελεί παράλληλα μακροχρόνια και εξαιρετικά σημαντική συνεργασία στον τομέα της ανταλλαγής πληροφοριών μεταξύ πέντε αγγλόφωνων χωρών, ήτοι, των ΗΠΑ, του ΗΒ, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας. Η εν λόγω συνεργασία βασίζεται στην ανταλλαγή στρατηγικών πληροφοριών και σημάτων (signals intelligence – SIGINT), και εξελίχθηκε σε ένα ισχυρό δίκτυο παρακολούθησης και ανάλυσης δεδομένων για τη διασφάλιση της εθνικής ασφάλειας και την καταπολέμηση της τρομοκρατίας, του εγκλήματος και άλλων απειλών σε διεθνές επίπεδο.

Η FEA υπογράφηκε μεταξύ του State Army Navy Communication Intelligence Board (STANCIB) το οποίο αντιπροσώπευε το U.S. State, Navy, and War Department and all other U.S. Communication Intelligence Authorities και του London Signal Intelligence (SIGINT) Board, το οποίο αντιπροσώπευε το Foreign Office, Admirality, War Office, Air Ministry και όλη την υπόλοιπη Βρετανική αυτοκρατορία[50]. Σκοπός της συμφωνίας ήταν να διέπει τις σχέσεις των πιο πάνω κρατών σε ζητήματα τα οποία αφορούσαν την επικοινωνία και ανταλλαγή μυστικών πληροφοριών.

Το άρθρο 3 της συμφωνίας καθορίζει τον τρόπο συλλογής και ανταλλαγής πληροφοριών μεταξύ των δύο χωρών, όπως επίσης και το είδος των πληροφοριών που θα συλλέγονται και ανταλλάσσονται, ήτοι, στρατιωτικής, πολιτικής και οικονομικής φύσης. Επίσης, περιλάμβανε τη συλλογή και ανάλυση επικοινωνιακής κίνησης, την απόκτηση εξοπλισμού και πληροφοριών για επικοινωνιακές δομές, καθώς και την κρυπτανάλυση, αποκρυπτογράφηση και μετάφραση ξένων μηνυμάτων. Η συγκεκριμένη συνεργασία θεμελίωσε ένα διακρατικό δίκτυο πληροφοριών, ενισχύοντας με αυτό τον τρόπο τη στρατηγική παρακολούθηση και την ασφάλεια μέσω κοινών επιχειρησιακών δυνατοτήτων[51].

Εξίσου σημαντικές είναι και οι πρόνοιες του άρθρου 5, εις το οποίο ρητά αναφέρετε ότι αμφότερα τα μέρη θα θεωρούν την συμφωνία ως αποκλείουσα οποιαδήποτε ενέργεια με τρίτα μέρη, με τον όρο τρίτα μέρη εννοώντας όλα τα άτομα ή τις αρχές πλην εκείνων των ΗΠΑ, Βρετανικής Αυτοκρατορίας και Βρετανικών Κτήσεων, σε οποιοδήποτε θέμα σχετικό με τις υπηρεσίες επικοινωνιακής κατασκοπείας[52]. Η εν λόγω ρητή πρόνοια φανερώνει την πρόθεση των μερών όπως δεσμευτούν να μην εμπλακούν σε συνεργασία με τρίτες χώρες, ενισχύοντας με αυτό τον τρόπο ένα κλειστό δίκτυο πληροφοριών, περιορίζοντας τη διαρροή ευαίσθητων δεδομένων και παράλληλα αναδεικνύοντας τη σημασία της αποκλειστικότητας

[48] Jérôme Mellon, *The UKUSA Agreement of 1948* (27 November 2001) http://www.europarl.eu.int/committees/echelon_home.htm accessed 18 March 2025.
[49] Ibid.
[50] 'British-U.S. Communication Intelligence Agreement' (5 March 1946) https://www.gchq.gov.uk/feature/ukusa-agreement accessed 22 February 2025. p. 3, para. (1)
[51] Ibid. 3
[52] Ibid. 4-5 [5]

στη διαχείριση πληροφοριών μεταξύ των συμβαλλομένων κρατών σχετικά με την ελεγχόμενη δομή των μυστικών υπηρεσιών στο αγγλοσαξονικό πλαίσιο. Ενδεικτική είναι και η παράγραφος (α) του πιο πάνω άρθρου η οποία αναφέρει:

> «*It will be contrary to this agreement to reveal its existence to any third party whatever*[53]».

Με την πάροδο των χρόνων, η συμμαχία Five Eyes μεγάλωσε καθότι συμπεριλήφθηκαν σε αυτή και άλλα κράτη τα οποία συνείσφεραν και συνεχίζουν να συνεισφέρουν στην ανταλλαγή ευαίσθητων πληροφοριών, αυξάνοντας τον αριθμό των κρατών σε 15. Η κυριότερη έμφαση της συμφωνίας ήταν η κατανομή των αρμοδιοτήτων μεταξύ των μερών, έτσι, οι ΗΠΑ είναι υπεύθυνες για τη συλλογή σημάτων στη Λατινική Αμερική, στο μεγαλύτερο μέρος της Ασίας, τη Ρωσία και την Βόρεια Κίνα, το ΗΒ είναι υπεύθυνο για την πρώην Σοβιετική Ένωση, δυτικά των Ουραλίων την Αφρική και άλλα[54].

Η συμφωνία Five Eyes, η οποία ξεκίνησε ως μια στρατηγική συνεργασία για την ανταλλαγή πληροφοριών και την παρακολούθηση επικοινωνιών μεταξύ πέντε αγγλόφωνων κρατών, έχει εξελιχθεί σε έναν από τους πιο ισχυρούς μηχανισμούς πληροφοριακής συνεργασίας στον κόσμο. Η συμφωνία αυτή δεν περιορίστηκε μόνο στη στρατιωτική ή πολιτική παρακολούθηση, αλλά διεύρυνε τον σκοπό της στην προστασία της εθνικής ασφάλειας και την καταπολέμηση της τρομοκρατίας και του εγκλήματος, επηρεάζοντας το διεθνές πεδίο ασφάλειας. Μέσα από την αυστηρή δομή της και την έντονη μυστικότητα η συμφωνία αυτή δημιούργησε ένα κλειστό δίκτυο συνεργασίας, περιορίζοντας τη διαρροή ευαίσθητων πληροφοριών και ενισχύοντας τις στρατηγικές παρακολούθησης. Καθώς η συμμαχία επεκτάθηκε με την προσθήκη νέων κρατών, η σημασία της Five Eyes συνεχίζει να αυξάνεται, αποδεικνύοντας τη διαρκή αναγκαιότητα και αποτελεσματικότητα της διεθνούς συνεργασίας για την ασφάλεια των κρατών και την καταπολέμηση των σύγχρονων απειλών.

4. ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ

Οι μαζικές παρακολουθήσεις από τις μυστικές υπηρεσίες έχουν εξελιχθεί διαχρονικά, αφού στα παλαιότερα χρόνια γίνονταν με διαφορετικούς τρόπους, όπως λόγου χάριν την φυσική παρακολούθηση, την συλλογή επιστολών και άλλα, πρακτικές οι οποίες απαιτούσαν έντονη ανθρώπινη εμπλοκή και χρόνο. Με την τεχνολογική ανάπτυξη όμως, το τοπίο των παρακολουθήσεων έχει αλλάξει ριζικά. Πλέον, προηγμένα προγράμματα και εργαλεία, επιτρέπουν στις μυστικές υπηρεσίες την μαζική συλλογή, αποθήκευση και ανάλυση δεδομένων δια μέσου ηλεκτρονικών επικοινωνιών, διαδικτυακής δραστηριότητας, ακόμα και από συσκευές οι οποίες χρησιμοποιούνται καθημερινά. Από χειροκίνητες μεθόδους, οι μυστικές υπηρεσίες έχουν περάσει πλέον σε αυτοματοποιημένα συστήματα παρακολούθησης, τα οποία αξιοποιούν τεχνολογίες όπως λόγου χάριν η τεχνητή νοημοσύνη και οι αλγόριθμοι. Τα κατασκοπευτικά λογισμικά τα οποία έχουν δημιουργηθεί, έχουν ως σκοπό τη συλλογή πληροφοριών κάποιου ατόμου, χωρίς το συγκεκριμένο άτομο να έχει δώσει τη συγκατάθεση του. Μεταξύ άλλων, τα κατασκοπευτικά λογισμικά μπορούν να

[53] Ibid. 5 [a]

[54] Jérôme Mellon, *The UKUSA Agreement of 1948* (27 November 2001) http://www.europarl.eu.int/committees/echelon_home.htm accessed 18 March 2025.

κλέβουν προσωπικές πληροφορίες, να εμφανίζουν ανεπιθύμητες διαφημίσεις ακόμα και να παρακολουθούν τις οποιεσδήποτε διαδικτυακές δραστηριότητες των χρηστών[55].

Η συγκεκριμένη μετάβαση, όχι μόνο διεύρυνε τις δυνατότητες παρακολούθησης, αλλά ανέδειξε και νέες προκλήσεις για την προστασία της ιδιωτικότητας. Πιο κάτω, θα εξεταστούν μερικά από τα πιο γνωστά σύγχρονα προγράμματα που χρησιμοποιούνται για την υλοποίηση αυτών των πρακτικών.

4.1. Pegasus

Ένα πολύ γνωστό σύστημα παρακολούθησης είναι το Pegasus, γνωστό και ως PEGA, το οποίο έχει τη δυνατότητα να παραβιάζει κινητές συσκευές.

> «*Το Pegasus έχει πλήρη και απεριόριστη πρόσβαση στην παραβιασθείσα συσκευή: μπορεί να εξάγει όλα τα δεδομένα που περιέχονται στη συσκευή (αρχική εξαγωγή δεδομένων), να παρακολουθεί όλες τις δραστηριότητες που εκτελούνται μέσω αυτής (παθητική επιτήρηση) και ενδεχομένως να παρεμβαίνει στο περιεχόμενο της συσκευής για τη συλλογή περαιτέρω δεδομένων (ενεργή επιτήρηση) και ενδεχομένως να παρεμβαίνει στο περιεχόμενο της συσκευής και στα μηνύματα που αποστέλλονται από αυτήν (χειραγώγηση). Μπορεί να εγκατασταθεί χωρίς καμία ενέργεια από τα ενδιαφερόμενα άτομα και δεν θα αφήσει κανένα ίχνος λειτουργίας του (ή πολύ λίγα ίχνη)[56]*».

Το σύστημα παρακολούθησης Pegasus, διαθέτει τρία πολύ σημαντικά χαρακτηριστικά, πρώτο, έχει τη δυνατότητα να αποκτήσει πλήρη πρόσβαση σε οποιαδήποτε συσκευή στοχεύει, δεύτερο, μπορεί να πραγματοποιεί επιθέσεις χωρίς κλικ, δηλαδή, μπορεί να εγκατασταθεί σε μια συσκευή χωρίς το επηρεαζόμενο άτομο να κάνει την οποιαδήποτε ενέργεια είτε κλικ σε κάποια ειδοποίηση είτε σε μήνυμα[57], και τρίτο, μπορεί να μην αφήσει καθόλου ίχνη πίσω του ή/και στην περίπτωση που αφήσει ίχνη αυτά είναι ελάχιστα[58], τα οποία θα επεξηγηθούν αναλυτικότερα στις επόμενες παραγράφους.

Αρχικά, αναφορικά με το πρώτο χαρακτηριστικό του εν λόγω λογισμικού, το Pegasus μπορεί να συλλέγει δεδομένα με κάποιους συγκεκριμένους τρόπους. Πρώτο, μπορεί να συλλέγει όλες τις πληροφορίες οι οποίες να είναι ήδη διαθέσιμες στη συσκευή που στοχεύει όταν γίνετε η εγκατάσταση του συγκεκριμένου λογισμικού, και πιο συγκεκριμένα, έχει τη δυνατότητα να συλλέγει όλα τα αρχεία μηνυμάτων, επαφών, ιστορικό κλήσεων, αρχείων ημερολογίου, μηνυμάτων ηλεκτρονικού ταχυδρομείου, και ιστορικού περιήγησης. Εν συνεχεία, έχει τη δυνατότητα να συλλέγει δεδομένα σχετικά με νέα αρχεία που γίνονται διαθέσιμα στη συσκευή, και τέλος, μπορεί ανά πάσα στιγμή να κάνει χρήση των λειτουργιών της συσκευής, όπως λόγου χάριν, η εξεύρεση της θέσης της συσκευής με τη χρήση του GPS, να καταγράφει φωνητικές κλήσεις, ακόμη και να αποθηκεύει στιγμιότυπα οθόνης[59].

---

[55] European Parliament, *Ο αντίκτυπος του Pegasus στα θεμελιώδη δικαιώματα και τις δημοκρατικές διαδικασίες στην Ευρωπαϊκή Ένωση* (Study PE 739.870, 2023) 14.
[56] Ibid 7.
[57] Ibid 26.
[58] Ibid 24.
[59] Ibid 24-25.

Επιπρόσθετα, το συγκεκριμένο κατασκοπευτικό λογισμικό έχει τη δυνατότητα να χειραγωγεί το περιεχόμενο των παραβιασμένων συσκευών, ήτοι, μπορεί να συμμετέχει σε «ενεργή επιτήρηση», για παράδειγμα να δώσει εντολή στο μικρόφωνο και τη κάμερα της συσκευής προκειμένου να καταγράψουν πληροφορίες από το περιβάλλον[60].

Επιπρόσθετα:

> «*Επιπλέον, ο έλεγχος μιας συσκευής από το Pegasus θα μπορούσε κατ' αρχήν να χρησιμοποιηθεί για την υλοποίηση πολλαπλών παράνομων σκοπών: για την τροποποίηση του περιεχομένου της συσκευής, τη δημιουργία και αποθήκευση πλαστών μηνυμάτων ή άλλων εγγράφων· για την αποστολή ψεύτικων μηνυμάτων, υποδυόμενο τον κάτοχο της συσκευής, για την απόκτηση πρόσβασης στα ψηφιακά ή υλικά περιουσιακά στοιχεία του ιδιοκτήτη και ενδεχομένως την εκτέλεση συναλλαγών στο όνομα του ιδιοκτήτη, ή για την τοποθέτηση ψευδών αποδεικτικών στοιχείων για εγκλήματα ή άλλες παράνομες δραστηριότητες στη συσκευή*[61]».

Επίσης, είναι σημαντικό να αναφερθεί ότι:

> «*[…] Έχει δηλώσει ότι έχει πουλήσει το Pegasus σε 60 κυβερνητικές υπηρεσίες σε 40 χώρες. […] το κατασκοπευτικό λογισμικό Pegasus έχει χρησιμοποιηθεί ευρέως από κυβερνήσεις σε όλο τον κόσμο για να στοχεύσει ακτιβιστές ανθρωπίνων δικαιωμάτων, προσωπικότητες της αντιπολίτευσης, δικηγόρους, δικαστές και ξένους ηγέτες*[62]».

Εν κατακλείδι, το σύστημα παρακολούθησης Pegasus αποτελεί ένα από τα πιο εξελιγμένα και επικίνδυνα εργαλεία κατασκοπείας, με την ικανότητα να παραβιάζει προσωπικές συσκευές χωρίς τη γνώση του κατόχου τους και να συλλέγει ευαίσθητα δεδομένα με ακρίβεια και αποτελεσματικότητα. Η δυνατότητα του να επιτίθεται χωρίς την ανάγκη αλληλεπίδρασης από τον χρήστη, καθώς και η ικανότητα του να μην αφήνει ίχνη παρακολούθησης, καθιστούν τον Pegasus εξαιρετικά δύσκολο να ανιχνευθεί και να αντιμετωπιστεί. Η χρήση του από κυβερνήσεις και οργανισμούς σε παγκόσμιο επίπεδο, για την παρακολούθηση ακτιβιστών, πολιτικών αντιπάλων και άλλων στόχων, εγείρει σοβαρά ζητήματα για την ιδιωτικότητα, τα ανθρώπινα δικαιώματα και την κυβερνοασφάλεια. Το Pegasus, με τις δυνατότητες του για ενεργή και παθητική επιτήρηση, δεν αποτελεί μόνο ένα εργαλείο παρακολούθησης, αλλά και μια απειλή για την προσωπική ελευθερία, καθώς η εκμετάλλευση του μπορεί να οδηγήσει σε καταστρατήγηση της εμπιστοσύνης των πολιτών προς τις κυβερνητικές αρχές και τις θεσμικές δομές που έχουν την ευθύνη για την προστασία των προσωπικών δεδομένων.

4.2. Prism

Το λογισμικό PRISM, επίσης γνωστό και ως SIGAD US-984XN[63], αποτελεί ένα εξελιγμένο πρόγραμμα ηλεκτρονικής επιτήρησης, το οποίο δημιουργήθηκε από την Υπηρεσία Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών Αμερικής (NSA) περί το 2007. Τα αρχικά του σημαίνουν «Planning Tool for Resource Integration, Synchronization, and Management» και σχεδιάστηκε για να συλλέγει και

[60] Ibid 28.
[61] Ibid.
[62] Ibid.
[63] Kate Hawkins, *What is the PRISM Program? NSA, Edward Snowden and Government Surveillance in 2025* (31 July 2024).

επεξεργάζεται ξένες πληροφορίες οι οποίες περνούν από αμερικανικούς διακομιστές[64]. Ως ηλεκτρονικό πρόγραμμα επιτήρησης, το PRISM δεν αποτελεί κατασκοπευτικό λογισμικό υπό την στενή έννοια του όρου, όπως λόγου χάριν το Pegasus.

Κυριότερος σκοπός του λογισμικού είναι η συλλογή δεδομένων από μεγάλες τεχνολογικές εταιρείες, όπως λόγου χάριν, η Google, η Apple, το Facebook, η Microsoft[65] και άλλα. Μέσω του συγκεκριμένου λογισμικού, η NSA έχει τη δυνατότητα πλέον να αποκτά πρόσβαση σε όλων των ειδών τις ηλεκτρονικές επικοινωνίες, όπως λόγου χάριν emails, μηνύματα, βιντεοκλήσεις, και αποθηκευμένα αρχεία, χωρίς να απαιτείται το οποιοδήποτε ατομικό ένταλμα[66], όπως ένταλμα έρευνας ή παρακολούθησης το οποίο εκδίδεται από τις αστυνομικές αρχές για ένα συγκεκριμένο άτομο.

Το «σκάνδαλο PRISM» αποκαλύφθηκε τον Ιούνιο του 2013, όταν οι εφημερίδες The Washington Post και The Guardian δημοσίευσαν μια μυστική εντολή η οποία απαιτούσε από την εταιρεία τηλεφωνίας Verizon να παρέχει στην NSA πληροφορίες για όλες τις εσωτερικές και διεθνείς κλήσεις των ΗΠΑ, σε συνεχιζόμενη βάση. Στις 6 Ιουνίου, οι δύο εφημερίδες αποκάλυψαν την ύπαρξη του προγράμματος PRISM της NSA, το οποίο αποκτούσε δεδομένα από κορυφαίες αμερικανικές εταιρείες διαδικτύου. Το πρόγραμμα αυτό βασιζόταν στις εξουσίες του νόμου FISA Amendment του 2008. Το σκάνδαλο αποκάλυψε διάφορα προγράμματα παρακολούθησης και η αποκάλυψη αυτών έγινε με τη βοήθεια τεσσάρων δημοσιογράφων, των Barton Gellman, Laura Poitras, Jacob Appelbaum και Glenn Greenwald[67].

Το PRISM νομικά στηρίζεται στο το SEC. 702 – Foreign Intelligence Surveillance Act 2008[68], το οποίο άρθρο φέρει τίτλο «*Procedures for Targeting certain persons outside the United States other than United States Persons*». Το συγκεκριμένο άρθρο δίδει το δικαίωμα στο Γενικό Εισαγγελέα όπως επίσης και στον Διευθυντή της Εθνικής Υπηρεσίας Πληροφοριών να στοχεύουν άτομα τα οποία διαμένουν εκτός των ΗΠΑ με στόχο την απόσπαση και συλλογή πληροφοριών[69].

Η ανάλυση του λογισμικού PRISM καταδεικνύει με σαφήνεια το πώς η τεχνολογία μπορεί να χρησιμοποιηθεί από κρατικούς φορείς για σκοπούς επιτήρησης, συχνά υπερβαίνοντας τα παραδοσιακά όρια της ιδιωτικότητας και των θεμελιωδών δικαιωμάτων. Η λειτουργία του προγράμματος υπό την αιγίδα της NSA και η νομική του θεμελίωση στο άρθρο 702 του νόμου FISA Amendment Act του 2008 εγείρουν σοβαρούς προβληματισμούς σχετικά με την ισορροπία μεταξύ εθνικής ασφάλειας και ατομικών ελευθεριών. Η αποκάλυψη του σκανδάλου το 2013 σηματοδότησε ένα σημείο καμπής στη δημόσια συζήτηση γύρω από την κυβερνητική διαφάνεια, την προστασία των προσωπικών δεδομένων και τη λογοδοσία των υπηρεσιών πληροφοριών. Εν κατακλείδι, το PRISM αποτελεί χαρακτηριστικό παράδειγμα των προκλήσεων που προκύπτουν όταν η εθνική ασφάλεια έρχεται σε σύγκρουση με το κράτος δικαίου και τα ανθρώπινα δικαιώματα σε μια εποχή ψηφιακής παγκοσμιοποίησης.

4.3. ECHELON

Το σύστημα ECHELON αποτελεί ένα από τα πιο χαρακτηριστικά και αμφιλεγόμενα παραδείγματα διεθνούς μηχανισμού μαζικής παρακολούθησης. Αναπτύχθηκε και

[64] Kate Hawkins, '*What Is the PRISM Program? NSA Surveillance Tool 2025*' (Cloudwards.net, 31 July 2024) https://www.cloudwards.net/what-is-the-prism-program-nsa-surveillance-tool-2025/ accessed 21 March 2025.
[65] NSA Prism program taps into user data of Apple, Google and others' *The Guardian* (6 June 2013)
[66] 'The NSA's PRISM Program and the New EU Privacy Regulation' (2017) *American University Business Law Review*
[67] European Parliament, *The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights* (2013).
[68] Foreign Intelligence Surveillance Act 2008
[69] Ibid s 702 (a).

διαχειρίζεται από τις ΗΠΑ, σε συνεργασία με συμμαχικές δυτικές δυνάμεις, και έχει ως κύριο στόχο την υποκλοπή τηλεπικοινωνιών και ηλεκτρονικών επικοινωνιών ακόμη και από φιλικές προς τις ΗΠΑ χώρες. Η ύπαρξη του συστήματος ξεκίνησε να συζητείται δημόσια στα μέσα της δεκαετίας του 1990, όταν δημοσιογραφικά ρεπορτάζ και φήμες υποδείκνυαν τη λειτουργία ενός παγκόσμιου δικτύου υποκλοπών. Το 1998 η Επιτροπή STOA του Ευρωπαϊκού Κοινοβουλίου, μέσω της μελέτης με τίτλο «Αξιολόγηση Τεχνολογιών Πολιτικού Ελέγχου», αναγνώρισε για πρώτη φορά, έστω και με ημιεπίσημο τρόπο, την ύπαρξη του ECHELON. Η εν λόγω μελέτη αποτέλεσε την απαρχή της πολιτικής ενασχόλησης της Ευρωπαϊκής Ένωσης με το ζήτημα των παρακολουθήσεων και ανέδειξε τις σημαντικές επιπτώσεις που μπορεί να έχουν τέτοιου είδους προγράμματα στην προστασία της ιδιωτικότητας ακόμα και σε δημοκρατικά κράτη[70]. Πολύ σημαντικό απόσπασμα από την μελέτη της ως άνω Επιτροπής αποτελεί το πιο κάτω:

> «*The Echelon system forms part of the UKUSA system but unlike many of the electronic spy systems developed during the cold war, Echelon is designed for primarily non-military targets: governments, organisations and businesses in virtually every country. The Echelon system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex*[71,72]».

Μέσα από διάφορες έρευνες έχει διαπιστωθεί ότι το σύστημα ECHELON χρησιμοποιήθηκε όχι μόνο για στρατιωτικούς ή αντικατασκοπευτικούς σκοπούς, αλλά και για τη διενέργεια βιομηχανικής κατασκοπείας. Ενδεικτική είναι η περίπτωση του 1994, όταν η NSA φέρεται να παρακολουθούσε τηλεφωνικές συνομιλίες μεταξύ της εταιρείας Thompson CSF και της κυβέρνησης της Βραζιλίας, αναφορικά με συμβόλαιο εγκατάστασης συστημάτων επιτήρησης στον Αμαζόνιο. Υπήρχαν ισχυρισμοί ότι η συγκεκριμένη υπόθεση συνδεόταν με χρηματισμούς και μίζες. Τελικά, το συμβόλαιο κατακυρώθηκε σε αμερικανική εταιρεία, η οποία φέρεται να είχε άμεση σχέση με το δίκτυο ECHELON[73].

Συμπερασματικά, το σύστημα ECHELON αποτελεί ένα χαρακτηριστικό παράδειγμα του πώς η τεχνολογία μπορεί να χρησιμοποιηθεί για την άσκηση υπερκρατικής ισχύος εις βάρος βασικών ανθρωπίνων δικαιωμάτων, όπως είναι η ιδιωτικότητα και η ελευθερία της επικοινωνίας. Παρά την απουσία πλήρους διαφάνειας και επίσημων παραδοχών από τις εμπλεκόμενες κυβερνήσεις, η μελέτη και η δράση της ΕΕ, ιδίως μέσω της STOA και της Προσωρινής Επιτροπής του Ευρωπαϊκού Κοινοβουλίου, ανέδειξαν όχι μόνο την τεχνική ικανότητα και την εμβέλεια του συστήματος, αλλά και τις πολλαπλές νομικές και ηθικές του προεκτάσεις. Η περίπτωση του ECHELON αποτυπώνει την ανάγκη για ισχυρότερους μηχανισμούς δημοκρατικής εποπτείας στις μυστικές υπηρεσίες, καθώς και για αποτελεσματικό νομικό πλαίσιο που θα διασφαλίζει την προστασία των θεμελιωδών δικαιωμάτων των πολιτών έναντι αυθαίρετων πρακτικών παρακολούθησης. Η πολιτική διάσταση του ζητήματος παραμένει ανοιχτή και επίκαιρη, ιδίως υπό το φως των πρόσφατων

---

[70] Franco Piodi and Iolanda Mombelli, *The Echelon Affair* (European Parliament, November 2014) https://historicalarchives.europarl.europa.eu/files/live/sites/historicalarchive/files/03_PUBLICATIONS/03_European-Parliament/01_Documents/the-echelon-affair-en.pdf accessed 2 April 2025.

[71] Ibid.

[72] Steven Wright, *An Appraisal of Technologies of Political Control – Interim Study, Working Document for the STOA Panel, European Parliament, Directorate General for Research* PE 166.499/Int.St. (Luxembourg, 19 January 1998).

[73] Piodi and Mombelli, 'The Echelon Affair', 11.

αποκαλύψεων σχετικά με τη μαζική επιτήρηση και την ευαλωτότητα της ιδιωτικής ζωής στην ψηφιακή εποχή.

4.4. Edward Snowden – Whistleblower

Ο Edward Snowden, αποτελεί μια από τις πλέον αμφιλεγόμενες και εμβληματικές προσωπικότητες του 21ου αιώνα στον τομέα της προστασίας της ιδιωτικότητας και της πληροφόρησης. Πρώην υπάλληλος της CIA και εξωτερικός συνεργάτης της NSA, έγινε διεθνώς γνωστός το 2013 όταν διέρρευσε απόρρητα έγγραφα, περί το 1,5 εκατομμύριο έγγραφα[74], που αποκάλυπταν τη λειτουργία ευρείας κλίμακας προγραμμάτων παρακολούθησης από τις αμερικανικές μυστικές υπηρεσίες. Οι αποκαλύψεις αυτές έφεραν στο φως τη συστηματική και ανεξέλεγκτη συλλογή προσωπικών δεδομένων πολιτών, τόσο εντός όσο και εκτός των ΗΠΑ, πυροδοτώντας έντονες αντιδράσεις διεθνώς και αναζωπυρώνοντας τον διάλογο σχετικά με την ισορροπία μεταξύ εθνικής ασφάλειας και προστασίας θεμελιωδών δικαιωμάτων.

Αρχικά, ο Snowden χρησιμοποίησε ηλεκτρονικά εργαλεία για τη μαζική λήψη απόρρητων αρχείων από τα δίκτυα και τους διακομιστές της NSA[75]. Στη συνέχεια, άρχισε να χρησιμοποιεί τα προνόμια που είχε ως διαχειριστής συστημάτων έτσι ώστε να πραγματοποιεί αναζήτηση σε μονάδες προσωπικών δικτύων άλλων υπαλλήλων της NSA και να αντιγράφει όσα βρήκε στις μονάδες δίσκου τους. Επίσης, επιστράτευσε συναδέλφους του για να τον βοηθήσουν ζητώντας από αρκετούς να του παρέχουν τα διαπιστευτήρια τους προκειμένου να αποκτήσει πληροφορίες στις οποίες θα μπορούσαν να έχουν αυτοί πρόσβαση και όχι ο ίδιος[76]. Περαιτέρω, σύμφωνα με το βιβλίο Beyond Snowden: Privacy Mass Surveillance, and the Struggle to Reform the NSA, ο Edward Snowden, ως τεχνικός υπάλληλος αποσπασμένος στην NSA στη Χαβάη, απέκτησε πρόσβαση σε απόρρητα αρχεία μέσω της θέσης του. Εκμεταλλεύτηκε τα προνόμια που είχε στα συστήματα της Υπηρεσίας και συγκέντρωσε χιλιάδες έγγραφα σχετικά με προγράμματα μαζικής επιτήρησης. Τα εν λόγω αρχεία τα μετέφερε σε φορητές μνήμες (USB drives), παρακάμπτοντας τις τυπικές διαδικασίες ασφάλειας, και στη συνέχεια τα διέρρευσε σε δημοσιογράφους, γεγονός που αποκάλυψε το εύρος των πρακτικών παρακολούθησης της NSA[77].

Περί τις αρχές Δεκεμβρίου 2012, ο Snowden επιχείρησε για πρώτη φορά να επικοινωνήσει με τον δημοσιογράφο Glenn Greenwald χρησιμοποιώντας το ψευδώνυμο «Cincinnatus», με σκοπό να του αποστείλει διάφορα από τα απόρρητα έγγραφα τα οποία είχε στην κατοχή του και αφορούσαν τις μαζικές παρακολουθήσεις και διάφορες κατ' ισχυρισμό παράνομες δραστηριότητες από την NSA[78]. Στις 06 Ιουνίου 2013, ο εν λόγω δημοσιογράφος προχώρησε με τη δημοσίευση του άρθρου του με τίτλο «*NSA collecting phone records of millions of Verizon customers daily*», στην εφημερίδα The Guardian, εις το οποίο αναφέρει ότι η Verizon

[74] House Permanent Select Committee on Intelligence**,** *HPSCI Snowden Review: Declassified* (September 2016) https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf i, accessed 2 April 2025.
[75] Ibid 10.
[76] Ibid 11.
[77] Timothy H Edgar, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA* (Brookings Institution Press 2017).
[78] House Permanent Select Committee on Intelligence, HPSCI Snowden Review 14.

δυνάμει διατάγματος ήταν υποχρεωμένη να παρέχει σε καθημερινή βάση πληροφορίες στην NSA σχετικά με όλες τις τηλεφωνικές επικοινωνίες που υπήρχαν στα συστήματα της[79].

Ορισμένα άλλα από τα στοιχεία που αποκάλυψε σχετίζονταν με την περίοδο 2001-2006, κατά την οποία πρόεδρος των ΗΠΑ ήταν ο George W. Bush. Σύμφωνα με τον Snowden, ο τότε πρόεδρος φέρεται να είχε εγκρίνει τη συλλογή δεδομένων από την NSA για το σύνολο του αμερικανικού πληθυσμού, στο πλαίσιο μιας ευρύτερης στρατηγικής για την ενίσχυση των δυνατοτήτων των υπηρεσιών πληροφοριών να εντοπίζουν τρομοκρατικά δίκτυα μέσω της ανάλυσης τηλεφωνικών αριθμών και επικοινωνιών προσώπων ύποπτων για σχέσεις με την τρομοκρατία[80].

Περαιτέρω, ο Snowden μέσα από τις αποκαλύψεις του, ήταν το πρώτο άτομο που έφερε στην επιφάνεια το κατασκοπευτικό λογισμικό PRISM, το πρόγραμμα Boundless Informant έδειξε ότι η Microsoft είχε παραδώσει πρόσβαση στην NSA σε κρυπτογραφημένα μηνύματα, έφερε στο φως πληροφορίες οι οποίες έδειχναν ότι τόσο οι Αμερικάνοι όσοι και οι Βρετανοί κατασκόπευαν ξένους ηγέτες και διπλωμάτες κατά τη σύνοδο του 2009 στο Λονδίνο, απέδειξε την τοποθέτηση κοριών στο υπουργείο εξωτερικών της Νοτίου Αφρικής, ανέδειξε την συμμετοχή του Skype στο κατασκοπευτικό λογισμικό PRISM, επίσης αποκάλυψε τη μαζική παρακολούθηση από την Βρετανική υπηρεσία GCHQ, επιπρόσθετα φανέρωσε ότι γίνονται συστηματικές παρακολουθήσεις και συλλογή δεδομένων από διάφορες χώρες όπως λόγου χάριν η Γερμανία, Γαλλία, Βραζιλία και άλλα[81]. Είναι εμφανές λοιπόν ότι οι απόρρητες πληροφορίες που αποκάλυψε ο Snowden, αποδεικνύουν την ύπαρξη ενός παγκόσμιου συστήματος μαζικών παρακολουθήσεων, το οποίο έχει ως στόχο όλους, παραβιάζοντας με αυτό τον τρόπο βασικά ανθρώπινα δικαιώματα.

Ο Edward Snowden, με τις αποκαλύψεις του, ανέδειξε τις σκοτεινές πτυχές της λειτουργίας των κρατικών μηχανισμών ασφαλείας στην ψηφιακή εποχή και προκάλεσε παγκόσμια αναστάτωση στον τομέα της ιδιωτικότητας και των ανθρωπίνων δικαιωμάτων. Ενώ κάποιοι τον θεωρούν ήρωα και υπερασπιστή της διαφάνειας και των ελευθεριών, άλλοι τον αντιμετωπίζουν ως προδότη που έθεσε σε κίνδυνο την εθνική ασφάλεια. Ανεξαρτήτως της εκτίμησης για τις πράξεις του, το έργο του Snowden αποτέλεσε την αφετηρία για την ενίσχυση της συζήτησης σχετικά με τα όρια της κρατικής επιτήρησης, την ανάγκη για δημοκρατική λογοδοσία των μυστικών υπηρεσιών και την προστασία της ιδιωτικής ζωής σε ένα ολοένα και πιο συνδεδεμένο τεχνολογικό περιβάλλον. Η υπόθεση αποτελεί εμβληματικό παράδειγμα whistleblowing στη σύγχρονη εποχή και καταδεικνύει τη λεπτή γραμμή ανάμεσα στην ασφάλεια και την ελευθερία.

5. ΗΝΩΜΕΝΕΣ ΠΟΛΙΤΕΙΕΣ ΑΜΕΡΙΚΗΣ – ΗΠΑ

5.1. Μυστικές Υπηρεσίες

[79] Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' *The Guardian* (6 June 2013) https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order accessed 5 April 2025.

[80] Constitutional Rights Foundation, 'Edward Snowden, the NSA, and Mass Surveillance' (BRIA 31:3, Spring 2016) https://www.crf-usa.org accessed 2 April 2025.

[81] Skytales Blog, 'Τι μας αποκάλυψε μέχρι σήμερα ο Snowden;' (Skytales, 6 June 2013) https://skytal.es/blog/index.html?p=381 accessed 5 April 2025.

Οι μυστικές υπηρεσίες των ΗΠΑ αποτελούν ένα από τους πιο οργανωμένους και πολυεπίπεδους μηχανισμούς συλλογής και ανάλυσης πληροφοριών παγκοσμίως. Στο επίκεντρο του συστήματος αυτού βρίσκονται κυρίως η Κεντρική Υπηρεσία Πληροφοριών (Central Intelligence Agency – CIA) και η Εθνική Υπηρεσία Ασφαλείας (National Security Agency – NSA), δύο οργανισμοί με διαφορετικό πεδίο δράσης αλλά κοινό στόχο, την προστασία της εθνικής ασφάλειας των ΗΠΑ.

Η CIA ιδρύθηκε το 1947 με την ψήφιση του National Security Act, ως διάδοχος του Γραφείου Στρατηγικών Υπηρεσιών που είχε λειτουργήσει κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου. Η αποστολή της CIA επικεντρώνεται κυρίως στη συλλογή και ανάλυση πληροφοριών από το εξωτερικό, στη διενέργεια μυστικών επιχειρήσεων με απώτερο σκοπό την προστασία της εθνικής ασφάλειας. Από την ίδρυση της μέχρι και το 1953, η υπηρεσία είχε πλέον καθιερωθεί και η αξία της είχε αναγνωριστεί από όλους[82].

Από την άλλη, η NSA, η οποία ιδρύθηκε στις 4 Νοεμβρίου το 1952[83], είναι υπεύθυνη για την κρυπτογραφική και επικοινωνιακή ευφυΐα και ασφάλεια[84]. Περαιτέρω, η αποστολή του οργανισμού περιλαμβάνει την προστασία και διαμόρφωση κωδικών κρυπτογράφησης και άλλης κρυπτολογίας για τον στρατό των ΗΠΑ και άλλες διάφορες κυβερνητικές υπηρεσίες, όπως επίσης και την παρακολούθηση, ανάλυση και επίλυση κωδικοποιημένων μεταδόσεων με ηλεκτρονικά ή άλλα μέσα. Η δημιουργία της NSA ήταν αποκύημα των δραστηριοτήτων των επικοινωνιών των στρατιωτικών μονάδων των ΗΠΑ κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου. Επιπρόσθετα, ακόμη ένας λόγος σχετικός με τη δημιουργία της NSA αποτελούσε η πεποίθηση ότι ο ξεχωριστός χαρακτήρας της συλλογής πληροφοριών δικαιολογούσε τη δημιουργία μιας οργάνωσης η οποία θα ήταν διαφορετική από τις ένοπλες δυνάμεις και τις άλλες υπηρεσίες πληροφοριών[85].

Εκτός από αυτούς τους δύο οργανισμούς, το δίκτυο των αμερικανικών υπηρεσιών πληροφοριών περιλαμβάνει και άλλες σημαντικές υπηρεσίες όπως η Defence Intelligence Agency (DIA)[86], η Federal Bureau of Investigation (FBI)[87] που δρα κυρίως εντός των ΗΠΑ, και η Office of the Director of National Intelligence (ODNI)[88] που ιδρύθηκε το 2004 για να συντονίζει το σύνολο της Κοινότητας Πληροφοριών, και άλλες.

Συνοψίζοντας, το πλέγμα των αμερικανικών μυστικών υπηρεσιών αποτελεί ένα σύνθετο και τεχνολογικά προηγμένο μηχανισμό συλλογής, ανάλυσης και διαχείρισης πληροφοριών με διακριτούς αλλά συμπληρωματικούς ρόλους. Η CIA και η NSA, ως οι δύο κυρίαρχοι πυλώνες του δικτύου αυτού, καλύπτουν το φάσμα των επιχειρήσεων τόσο στο εξωτερικό όσο και στον τομέα της ψηφιακής επιτήρησης, ενώ οργανισμοί όπως η DIA, το FBI και η ODNI ενισχύουν τη συνεργασία και το συντονισμό σε εθνικό και διεθνές επίπεδο. Αν και οι υπηρεσίες αυτές έχουν συμβάλει καθοριστικά στην ενίσχυση της εθνικής ασφάλειας των ΗΠΑ, η δράση τους

[82] Central Intelligence Agency, 'History of CIA' https://www.cia.gov/legacy/cia-history/ accessed 5 April 2025.
[83] National Security Agency, 'The Early History of NSA' (National Security Agency) https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/early_history_nsa.pdf accessed 5 April 2025
[84] Encyclopaedia Britannica, 'National Security Agency' https://www.britannica.com/topic/National-Security-Agency accessed 5 April 2025
[85] Ibid.
[86] Defense Intelligence Agency, 'Home' https://www.dia.mil/ accessed 5 April 2025
[87] Federal Bureau of Investigation, 'Welcome to fbi.gov' https://www.fbi.gov/ accessed 5 April 2025
[88] Office of the Director of National Intelligence, 'Home' https://www.dni.gov/ accessed 5 April 2025

έχει επανειλημμένα προκαλέσει έντονες συζητήσεις για την ισορροπία μεταξύ κρατικής ασφάλειας και σεβασμού των πολιτικών και ατομικών δικαιωμάτων. Η μελέτη και η κατανόηση της λειτουργίας τους καθίσταται απαραίτητη προκειμένου να αξιολογηθεί ο ρόλος τους στο σύγχρονο παγκόσμιο γεωπολιτικό περιβάλλον, καθώς και οι επιπτώσεις τους στην προστασία της ιδιωτικότητας και των θεμελιωδών ελευθεριών.

5.2. Νομοθετικό πλαίσιο

Το νομοθετικό πλαίσιο που διέπει τη λειτουργία των μυστικών υπηρεσιών στις ΗΠΑ αποτελεί έναν από τους πλέον σύνθετους τομείς του δικαίου. Από τη μια πλευρά η ανάγκη για εθνική ασφάλεια και η πρόληψη απειλών, όπως η τρομοκρατία και η κατασκοπεία επιβάλλουν τη λειτουργία ισχυρών και αποτελεσματικών υπηρεσιών πληροφοριών. Από την άλλη, το κράτος δικαίου και η προστασία των θεμελιωδών δικαιωμάτων με έμφαση στην ιδιωτικότητα και την ελευθερία των πολιτών δημιουργούν την ανάγκη για αυστηρή νομοθετική ρύθμιση και αποτελεσματικό δημοκρατικό έλεγχο. Στις ΗΠΑ το νομικό καθεστώς που ρυθμίζει τις δραστηριότητες των μυστικών υπηρεσιών έχει διαμορφωθεί διαχρονικά μέσα από έναν συνδυασμό νόμων, προεδρικών διαταγμάτων, δικαστικών αποφάσεων και εσωτερικών κανονισμών. Ιδιαίτερο βάρος δίνεται σε θεσμικά αντίβαρα, όπως λόγου χάριν η εποπτεία του Κογκρέσου, οι διαδικασίες αδειοδότησης για παρακολουθήσεις από ειδικά δικαστήρια καθώς και η δράση ανεξάρτητων οργάνων.

Έχει αναπτυχθεί η θέση ότι:

> «*[…] But the general principle under which American law operates is that surveillance is legal unless forbidden. Perhaps out of fear that surveillance might be used to suppress dissent, American law contains some limited protections against government surveillance of purely political activity. […] NSLs are statutory authorizations by which the FBI can obtain information about people from their telephone companies, internet service providers, banks, credit agencies, and other institutions with which those people have a relationship. NSLs are covert and come with a gag order that prohibits the recipient of the letter from disclosing its existence, even to the person whose secrets have been told to the government. […] these provisions allow the FBI to access a wide variety of information about people, including historical and transactional information relating to telephone calls and emails, financial information, and consumer credit information. […] the FBI must merely certify in writing that the request is 'relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities*[89]».

Η Τέταρτη Τροπολογία του Συντάγματος των ΗΠΑ (Fourth Amendment) αποτελεί μια από τις θεμελιώδεις διατάξεις προστασίας των ατομικών ελευθεριών, καθώς κατοχυρώνει το δικαίωμα των πολιτών στην ιδιωτικότητα και τους προφυλάσσει από παράνομες έρευνες, συλλήψεις, κατασχέσεις χωρίς ένταλμα ή εύλογη αιτία. Αποτελεί βασικό πυλώνα του δικαίου περί προστασίας της ιδιωτικής ζωής και περιορίζει τις αυθαίρετες επεμβάσεις της κρατικής εξουσίας στον ιδιωτικό βίο[90].

[89] Neil M Richards, 'The Dangers of Surveillance' (2013) 126(7) Harvard Law Review 1934.
[90] William C Heffernan, *The Fourth Amendment: Origins and Interpretations* (Carolina Academic Press 2022).

Μέσα από τη συνεχή ερμηνευτική της προσέγγιση, όπως αυτή αποτυπώνεται σε σημαντικές αποφάσεις του Ανωτάτου Δικαστηρίου, η Τροπολογία αυτή αποδεικνύει την εξελικτική της φύση. Δικαστικές αποφάσεις όπως η *Katz v. United States (1967)*[91] και η *Carpenter v. United States (2018)*[92] δεν εφαρμόζουν απλώς το γράμμα του Συντάγματος, αλλά επεκτείνουν την έννοια της εύλογης προσδοκίας ιδιωτικότητας προσαρμοσμένη στις σύγχρονες συνθήκες, αναδεικνύοντας πως το δίκαιο δύναται να προσαρμοστεί στις τεχνολογικές εξελίξεις και τις κοινωνικές ανάγκες. Μέσω αυτών των ερμηνειών, η Τέταρτη Τροπολογία αποκτά δυναμική διάσταση, καθιστώντας σαφές ότι η προστασία της ιδιωτικότητας δεν είναι στατική, αλλά μετασχηματίζεται και εξελίσσεται βάσει των απαιτήσεων της εποχής[93]. Η προστασία της ιδιωτικότητας, αν και δεν κατοχυρώνεται ρητά από την Τέταρτη Τροπολογία, έχει αναγνωριστεί μέσα από τη νομολογία. Στην υπόθεση *Boyd v. United States*[94], το Δικαστήριο, για πρώτη φορά, συνέδεσε την Τέταρτη Τροπολογία με την έννοια της ιδιωτικότητας, υπογραμμίζοντας το απόλυτο δικαίωμα των ατόμων στην προστασία των προσωπικών και γραπτών τους επικοινωνιών[95].

Το National Security Act, παρέχει σημαντικές εγγυήσεις για την προστασία των πολιτών των ΗΠΑ από αυθαίρετες παρακολουθήσεις και τη συλλογή πληροφοριών κατά τη διάρκεια δραστηριοτήτων που προστατεύονται από την Πρώτη Τροπολογία του Συντάγματος των ΗΠΑ. Ειδικότερα, το άρθρο 105 C[96] σχετίζεται άμεσα με την απαγόρευση αυθαίρετης παρακολούθησης, διασφαλίζοντας τον σεβασμό των θεμελιωδών δικαιωμάτων. Επιπλέον, το άρθρο SEC.511[97] επιβάλλει θετική υποχρέωση στον Διευθυντή του National Intelligence να υποβάλλει ετήσια έκθεση, στην οποία πρέπει να περιλαμβάνονται λεπτομερώς τυχόν παραβιάσεις της νομοθεσίας που σχετίζονται με τις δραστηριότητες πληροφοριών από μέλη του προσωπικού. Το μέτρο αυτό ενισχύει τη λογοδοσία και συμβάλλει στη διατήρηση της διαφάνειας εντός της κοινότητας πληροφοριών.

Ανάλογης σημασίας είναι και το άρθρο SEC 501[98], το οποίο θεσμοθετεί την υποχρέωση του προέδρου των ΗΠΑ να διασφαλίζει ότι οι αρμόδιες κοινοβουλευτικές επιτροπές ενημερώνονται πλήρως και εγκαίρως για τις προγραμματισμένες δραστηριότητες συλλογής πληροφοριών. Επίσης, η παράγραφος (b) του σχετικού άρθρου επιτάσσει την άμεση ενημέρωση του Κογκρέσου σε περίπτωση παράνομων δραστηριοτήτων συλλογής πληροφοριών, καθώς και την αναφορά των διορθωτικών ενεργειών που έχουν ληφθεί ή πρόκειται να ληφθούν[99]. Η συγκεκριμένη πρόβλεψη ενισχύει τη θεσμική διαφάνεια και τη λογοδοσία των εκτελεστικών οργάνων έναντι της νομοθετικής εξουσίας, εξισορροπώντας την ανάγκη για μυστικότητα με την αρχή της δημοκρατικής εποπτείας. Ωστόσο, το άρθρο δεν προβλέπει την υποχρέωση λήψης συγκατάθεσης από το Κογκρέσο για την έναρξη μελλοντικών επιχειρήσεων πληροφοριών, στοιχείο το οποίο διατηρεί την επιχειρησιακή ευελιξία της εκτελεστικής εξουσίας.

---

[91] *Katz v United States*, 389 US 347 (1967).
[92] *Carpenter v United States*, 138 S Ct 2206 (2018).
[93] US Const amend IV, in *Fourth Amendment—Search and Seizure* (US Government Publishing Office 2021)
[94] Boyd v. United States, 116 U.S. 616, 626-627 (1886)
[95] Stanislava Nedeva, 'Intelligence Services' Unaccountability for Human Rights Violations' (2020) 20(1) International Comparative Law Review 43.
[96] National Security Act of 1947, Pub L No 80–253, 61 Stat 496, as amended through P.L. 118–159 (23 December 2024), art 105 C.
[97] Ibid s 511 (C).
[98] Ibid s 501.
[99] Ibid s 501 (b).

Συναφές είναι και το άρθρο SEC 513[100] το οποίο καθιερώνει την υποχρέωση του Διευθυντή της Εθνικής Υπηρεσίας Πληροφοριών να υποβάλλει ετήσια έκθεση προς τις επιτροπές πληροφοριών του Κογκρέσου, με πλήρη καταγραφή των εσωτερικών δραστηριοτήτων που διεξάγονται από κάθε οργανισμό της κοινότητας πληροφοριών. Για κάθε επιμέρους δραστηριότητα απαιτείται σαφής αναφορά της νομικής εξουσιοδότησης που τη δικαιολογεί, εξασφαλίζοντας έτσι θεσμική διαφάνεια και νομιμοποίηση των επιχειρησιακών δράσεων.

Εξίσου σημαντικό είναι και το SEC 510[101], που καθιερώνει την υποχρέωση του Γενικού Συμβουλίου κάθε υπηρεσίας πληροφοριών να ενημερώνει γραπτώς τις επιτροπές του Κογκρέσου για κάθε σημαντική νομική ερμηνεία του Συντάγματος των ΗΠΑ, εφόσον αυτή επηρεάζει τις δραστηριότητες της αντίστοιχης υπηρεσίας. Η εν λόγω πρόνοια διασφαλίζει ότι οι υπηρεσίες πληροφοριών δεν προβαίνουν σε αυθαίρετες ερμηνείες του νομικού πλαισίου χωρίς θεσμική επίβλεψη, ενισχύοντας τον έλεγχο και τη διαφάνεια στο νομικό πεδίο των επιχειρήσεων πληροφοριών.

Ιδιαίτερης σημασίας στον τομέα των παρακολουθήσεων και της μαζικής συλλογής πληροφοριών είναι το Foreign Intelligence Surveillance Act of 1978 (FISA) as amended in 2008[102]. Το εν λόγω νομοθέτημα αποτελεί το κυριότερο νομικό πλαίσιο που ρυθμίζει τις εξουσίες των αμερικανικών υπηρεσιών πληροφοριών όσον αφορά τη συλλογή δεδομένων.

Ειδικότερα το Section 702[103] επιτρέπει την παρακολούθηση χωρίς ένταλμα αλλοδαπών προσώπων εκτός ΗΠΑ, υπό την προϋπόθεση ότι τηρούνται οι προβλεπόμενες διαδικασίες στόχευσης και ελαχιστοποίησης, καθώς και ότι η διαδικασία συμμορφώνεται με την Τέταρτη Τροπολογία του Συντάγματος των ΗΠΑ. Αντίστοιχα, τα Section 703 & 704[104] καθορίζουν τις προϋποθέσεις υπό τις οποίες μπορεί να πραγματοποιηθεί νομίμως παρακολούθηση Αμερικανών πολιτών στο εξωτερικό.

Το Section 707[105] προβλέπει την υποχρεωτική εξαμηνιαία ενημέρωση του Κογκρέσου από το Γενικό Εισαγγελέα σχετικά με την εφαρμογή των διατάξεων του νόμου, ενισχύοντας τον κοινοβουλευτικό έλεγχο. Το Section 706[106] επιβάλλει περιορισμούς στη χρήση των πληροφοριών που έχουν αποκτηθεί μέσω των εν λόγω παρακολουθήσεων, επιτρέποντας την αξιοποίηση τους μόνο υπό συγκεκριμένες και περιορισμένες προϋποθέσεις.

Συνοψίζοντας, το FISA Amendments Act του 2008 παρέχει το βασικό νομικό έρεισμα για τη διεξαγωγή μαζικών παρακολουθήσεων από τις αμερικανικές υπηρεσίες πληροφοριών χωρίς την ανάγκη δικαστικής εντολής, εφόσον τηρούνται οι εγγυήσεις στόχευσης και προστασίας της ιδιωτικότητας. Αν και προβλέπεται θεσμικός και εν μέρει δικαστικός έλεγχος των σχετικών διαδικασιών, το νομοθετικό πλαίσιο δεν προβλέπει ρητά ποινικές κυρώσεις για

[100] Ibid s 513.
[101] Ibid s 510.
[102] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub L No 110–261, 122 Stat 2436 (codified in part at 50 USC §1801 et seq).
[103] Ibid s 702.
[104] Ibid s 703 & 704.
[105] Ibid s 707.
[106] Ibid s 706.

παράνομες παρακολουθήσεις, περιορίζοντας την ευθύνη των υπηρεσιών κυρίως στο διοικητικό επίπεδο.

Ο Patriot Act[107], ο οποίος θεσπίστηκε στις ΗΠΑ αμέσως μετά τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001, αποτελεί ένα από τα πλέον αμφιλεγόμενα νομοθετήματα στον τομέα της εθνικής ασφάλειας. Στόχος του ήταν η ενίσχυση των εργαλείων, των διωκτικών και πληροφοριακών υπηρεσιών για την πρόληψη της τρομοκρατίας μέσω της διεύρυνσης των εξουσιών επιτήρησης, συλλογής δεδομένων και διασταύρωσης πληροφοριών. Το εν λόγω νομοθέτημα ενίσχυσε σε μεγάλο βαθμό τις εξουσίες των μυστικών υπηρεσιών όσο αφορά την υποκλοπή, κοινοποίηση και χρήση ιδιωτικών τηλεπικοινωνιών[108].

Αρχικά, σύμφωνα με τις πρόνοιες του Sec 103[109], προκειμένου οι υπηρεσίες των ΗΠΑ να έχουν την δυνατότητα να αντιμετωπίσουν την τρομοκρατία, αυξήθηκε σημαντικά η χρηματοδότηση τους για την ολοκλήρωση των επιχειρήσεων τους.

Περαιτέρω, το Sec 201[110] τροποποιεί το Section 2516 (1) του Title 18, United States Code[111]. Με την εν λόγω τροποποίηση, συμπεριλαμβάνονται και άλλα αδικήματα κάτω από τις πρόνοιες του Section 2516, δίδοντας την δυνατότητα στο FBI να δύναται να ζητήσει από δικαστή την έκδοση διατάγματος για την παρακολούθηση προσώπου το οποίο φέρεται να έχει διαπράξει ή συμμετέχει στη διάπραξη ποινικών αδικημάτων ή/και τρομοκρατίας. Γενικότερα, το USA Patriot Act του 2001 παρέχει διάφορες μεταρρυθμίσεις και τροποποιήσεις οι οποίες αφορούν κατά κύριο λόγο το United States Code.

Εν συνεχεία, αρκετά σημαντικό είναι το υπό αναφορά United States Code[112] το οποίο αποτελεί το κυριότερο νομοθέτημα όσο αφορά το ποινικό δίκαιο στην Ομοσπονδία των ΗΠΑ, και πιο συγκεκριμένα οι παραγράφοι 2510-2523, καθότι αυτές ενασχολούνται με την παρακολούθηση επικοινωνιών. Η παράγραφος 2511[113], αφενός απαγορεύει ρητά την σκόπιμη υποκλοπή ή ακόμα και την προτροπή άλλου προσώπου στην υποκλοπή τηλεπικοινωνιακών ή προφορικών ή ηλεκτρονικών επικοινωνιών, με την χρήση συσκευών και ρητά αναφέρει στην παράγραφο (1) ότι τιμωρείτε αυστηρά, αφετέρου όμως βάσει της παραγράφου (2) επιτρέπει σε χειριστές τηλεφωνικών κέντρων ή αστυνομικών ή τον αντιπρόσωπο ενός πάροχου ενσύρματης ηλεκτρονικής υπηρεσίας επικοινωνιών να υποκλέπτει, αποκαλύπτει ή χρησιμοποιεί αυτή την επικοινωνία κατά την κανονική πορεία της απασχόλησης του. Συνεχίζοντας, η παράγραφος (ii) επιτρέπει την υποκλοπή τηλεπικοινωνιακών, προφορικών ή ηλεκτρονικών επικοινωνιών σε άτομα που δύνανται από το νόμο να προβαίνουν σε τέτοιες ενέργειες, νοουμένου ότι υπάρχει δικαστική απόφαση ή έγγραφη πιστοποίηση από πρόσωπο το οποίο προσδιορίζεται στο άρθρο 2518(7) του τίτλου 18 ή από το Γενικό Εισαγγελέα των ΗΠΑ ότι δεν απαιτείται ένταλμα ή δικαστική εντολή βάσει

[107] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT) Act of 2001, Pub L No 107–56, 115 Stat 272.
[108] Committee on Civil Liberties, Justice and Home Affairs, *US Legal Instruments for Access and Electronic Surveillance of EU Citizens: Background Note* (European Parliament 2013)
[109] *USA PATRIOT Act 2001*, Pub L No 107–56, 115 Stat 272, s 103.
[110] Ibid s 201.
[111] 18 USC § 2516(1) (authorising specified officials to apply for wiretap orders in investigations of certain offences).
[112] 18 USC ch 119, pt I (Wire and Electronic Communications Interception and Interception of Oral Communications).
[113] Ibid 2511.

του νόμου, ότι έχουν τηρηθεί όλες οι νομοθετικές απαιτήσεις και ότι η συγκεκριμένη υποκλοπή είναι αναγκαία.

Περαιτέρω, ο USA Freedom Act 2015[114], αποτελεί ακόμη ένα πολύ σημαντικό νομοθέτημα δια τους σκοπούς της παρούσας μελέτης, καθότι ψηφίστηκε ως απάντηση στις αποκαλύψεις για τις μαζικές παρακολουθήσεις της NSA, επιφέροντας σημαντικές μεταρρυθμίσεις στο πρόγραμμα συλλογής δεδομένων. Ο νόμος, κατάργησε τη μαζική και αδιάκριτη συλλογή τηλεφωνικών μεταδεδομένων από την κυβέρνηση, μεταφέροντας την ευθύνη φύλαξης στους παρόχους επικοινωνίας, οι οποίοι υποχρεούνται να τα διατηρούν και να τα παρέχουν μόνο ύστερα από δικαστική εντολή. Παράλληλα, ενίσχυσε τον έλεγχο του FISC (Foreign Intelligence Surveillance Court), προβλέποντας τη συμμετοχή ανεξάρτητων «φίλων του δικαστηρίου» για σκοπούς ενίσχυσης της διαφάνειας. Πιο συγκεκριμένα, το SEC. 103 – Prohibition on Bulk Collection of Tangible Things[115], εις την οποία γίνεται ρητή αναφορά ότι αποτελεί απαραίτητη προϋπόθεση η έκδοση διατάγματος για τη συλλογή πληροφοριών. Περαιτέρω το SEC 201[116] απαγορεύει πλέον ρητά τη μαζική συλλογή πληροφοριών.

Ρητές πρόνοιες ως προς την ποινική ευθύνη ατόμων τα οποία εμπλέκονται σε ηλεκτρονική επιτήρηση/παρακολούθηση βρίσκονται και στο 50 USC par. 1809 (Criminal Sanctions under the Foreign Intelligence Surveillance Act)[117]. Δια μέσου του ως άνω καθορίζεται ως αδίκημα οποιαδήποτε πράξη ατόμου που σχετίζεται με την ηλεκτρονική επιτήρηση, η οποία ηλεκτρονική επιτήρηση δυνάμει των παρ. 1801 (f) (1), (2), (3) και (4)[118] καθορίζεται ως απόκτηση μέσω ηλεκτρονικής, μηχανικής ή άλλης συσκευής παρακολούθησης, του περιεχομένου οποιασδήποτε τηλεφωνικής ή ραδιοφωνικής επικοινωνίας από πρόσωπο το οποίο βρίσκεται στις ΗΠΑ εφόσον το περιεχόμενο αυτό αποκτάται με σκοπό την στοχοποίηση του εν λόγω προσώπου κάτω από συνθήκες κατά τις οποίες το άτομο αυτό έχει εύλογη προσδοκία ιδιωτικότητας και θα απαιτείτο ένταλμα για σκοπούς επιβολής του νόμου, ή όταν γίνεται για τη λήψη του περιεχομένου της επικοινωνίας προς ή από πρόσωπο εντός των ΗΠΑ χωρίς τη συγκατάθεση οποιουδήποτε από τα εμπλεκόμενα μέρη, ή υπό συνθήκες κατά τις οποίες το άτομο έχει εύλογη προσδοκία ιδιωτικότητας και θα απαιτείτο ένταλμα για σκοπούς επιβολής του νόμου, και εφόσον τόσο ο αποστολέας όσο και όλοι οι αποδέκτες βρίσκονται εντός των ΗΠΑ. Εξαιρετικά σημαντική είναι η παρ. (d) εις την οποία προβλέπεται ότι υφίσταται αδίκημα βάση των προνοιών της διάταξης παρ. 1809 εφόσον το πρόσωπο που διέπραξε το αδίκημα ήταν αξιωματούχος ή υπάλληλος των ΗΠΑ κατά τον χρόνο τέλεσης του αδικήματος. Επομένως, είναι ενδεικτικό των πιο πάνω ότι, με τις πρόνοιες του 50 U.S. Code, όσο αφορά τις εγχώριες παρακολουθήσεις στις ΗΠΑ, αποτελεί βασικό κριτήριο η λήψη δικαστικής απόφασης και εντάλματος προκειμένου να είναι εφικτή η ηλεκτρονική παρακολούθηση από μέλη της κυβέρνησης, κατά συνέπεια των υπηρεσιών πληροφοριών, και σε περίπτωση παραβίασης αυτών των διατάξεων προβλέπονται αυστηρές ποινές.

Η πρακτική των μαζικών παρακολουθήσεων από υπηρεσίες όπως η NSA επηρεάζει άμεσα το δικαίωμα στην ιδιωτικότητα, ιδίως όταν η συλλογή δεδομένων γίνεται χωρίς σαφή και

[114] USA FREEDOM Act of 2015, Pub L No 114–23, 129 Stat 268.
[115] Ibid s 103.
[116] Ibid s 201.
[117] 50 USC § 1809 (Criminal sanctions under the Foreign Intelligence Surveillance Act) https://www.law.cornell.edu/uscode/text/50/1809.
[118] 50 USC § 1801 (Definitions under the Foreign Intelligence Surveillance Act) https://www.law.cornell.edu/uscode/text/50/1801.

προηγούμενη δικαστική έγκριση. Η αποκάλυψη του προγράμματος PRISM έδειξε ότι η παρακολούθηση δεν περιοριζόταν σε στοχευμένα άτομα αλλά περιλάμβανε μαζική απόκτηση δεδομένων επικοινωνίας, χωρίς επαρκή φίλτρα ή εποπτεία. Αν και το νομικό πλαίσιο όπως το FISA προβλέπει ορισμένες δικαστικές διαδικασίες, οι εξαιρέσεις που παρέχονται στην εθνική ασφάλεια υπονομεύουν την ουσιαστική προστασία της ιδιωτικότητας. Το δικαίωμα αυτό θίγεται τόσο σε επίπεδο αμερικανών πολιτών όσο και σε μη αμερικανούς που ενδέχεται να βρίσκονται στο επίκεντρο διεθνούς επιτήρησης. Ο περιορισμένος ρόλος του FISA Court και η έλλειψη πρόσβασης των πολιτών σε ένδικα μέσα, έχουν προκαλέσει ευρεία κριτική για έλλειψη αναλογικότητας και διαφάνειας. Συνεπώς, απαιτείται αυστηρότερη νομοθετική ρύθμιση και ουσιαστική δικαστική εποπτεία, ώστε να διασφαλίζεται η ισορροπία μεταξύ ασφάλειας και σεβασμού των ατομικών ελευθεριών.

Αξίζει επίσης να σημειωθεί ότι, στο διεθνές δίκαιο επικρατεί η άποψη ότι η ποινική δίωξη πράξεων κατασκοπείας δεν συνιστά αντικείμενο διεθνούς ποινικής ευθύνης, αλλά παραμένει κυρίως ζήτημα εθνικού δικαίου που εγείρεται από το επηρεαζόμενο κράτος. Όπως σημειώνει ο Dieter Fleck, η κατασκοπεία δεν έχει τυποποιηθεί ως διεθνές έγκλημα, και η αντιμετώπιση της εναπόκειται στην κρατική κυριαρχία και στις ανάγκες προστασίας της εθνικής ασφάλειας μέσω της εσωτερικής νομοθεσίας των ενίοτε διπλωματικών πρακτικών[119].

Εν κατακλείδι, το νομοθετικό πλαίσιο των ΗΠΑ γύρω από τις μυστικές υπηρεσίες και τη μαζική παρακολούθηση αντανακλά την πολυπλοκότητα της ισορροπίας μεταξύ εθνικής ασφάλειας και ατομικών ελευθεριών. Αν και παρέχεται ένα εκτεταμένο θεσμικό σύστημα ελέγχου, με σημαντικές εγγυήσεις όπως λόγου χάριν η Τέταρτη Τροπολογία και οι νομοθετικές προβλέψεις του FISA και του National Security Act, δεν παύει να παρατηρείται μια σταθερή τάση ενίσχυσης των εξουσιών των υπηρεσιών πληροφοριών ιδίως μετά την 11η Σεπτεμβρίου. Οι τροποποιήσεις του FISA το 2008, η ψήφιση του Patriot Act και η πρακτική εφαρμογή τους, συχνά θολώνουν τα όρια νομιμότητας και λογοδοσίας. Παρά τις προσπάθειες διατήρησης του ελέγχου και της λογοδοσίας, η πραγματικότητα δείχνει ότι η ιδιωτικότητα υποχωρεί συχνά μπροστά στην επιταγή της ασφάλειας. Το νομικό σύστημα των ΗΠΑ παρέχει πολύτιμο υλικό για την κατανόηση των σύγχρονων προκλήσεων στο πεδίο της επιτήρησης, λειτουργώντας ως υπόδειγμα αλλά και ως παράδειγμα προς αποφυγή για άλλες έννομες τάξεις.

5.3. Δικαστικές Αποφάσεις

Οι δικαστικές αποφάσεις στις ΗΠΑ σχετικά με τις μαζικές παρακολουθήσεις και την ιδιωτικότητα βρίσκονται στο επίκεντρο ενός διαρκώς εξελισσόμενου νομικού και κοινωνικού διαλόγου. Καθώς η τεχνολογία προοδεύει με ταχύτατους ρυθμούς και οι δυνατότητες συλλογής και επεξεργασίας δεδομένων επεκτείνονται, ανακύπτουν κρίσιμα ερωτήματα γύρω από την ισορροπία μεταξύ εθνικής ασφάλειας και προστασίας των ατομικών δικαιωμάτων. Τα δικαστήρια καλούνται συχνά να καθορίσουν τα όρια των κυβερνητικών εξουσιών, ερμηνεύοντας το Σύνταγμα υπό το φως νέων τεχνολογικών πραγματικοτήτων. Σε αυτό το πλαίσιο, οι αποφάσεις τους διαμορφώνουν όχι μόνο το νομικό τοπίο των ΗΠΑ, αλλά

[119] Dieter Fleck, Individual and State Responsibility for Intelligence Gathering, 28 MICH. J. INT'L L. 687 (2007). Available at: https://repository.law.umich.edu/mjil/vol28/iss3/9 511.

επηρεάζουν και τον τρόπο με τον οποίο αντιλαμβανόμαστε τη σχέση μεταξύ του πολίτη και του κράτους στη σύγχρονη ψηφιακή εποχή.

Αρκετά σημαντική είναι η υπόθεση *Klayman v Obama*[120], η οποία αφορούσε τη μαζική συλλογή δεδομένων τηλεφωνικών επικοινωνιών από την NSA ακόμη και ατόμων για τα οποία δεν υπήρχε τεκμηριωμένος λόγος παρακολούθησης. Εξαιρετικά σημαντικό για την υπό κρίση υπόθεση αποτελεί το κάτωθι απόσπασμα από την απόφαση του δικαστηρίου:

> «*Since May 2006, the government has relied on this provision to operate a program that has come to be called 'bulk data collection', namely, the collection, in bulk, of call records produced by telephone companies containing 'telephony metadata'- the telephone numbers dialed (incoming and outgoing), times, and durations of calls […].*[121]».

Σύμφωνα με το δικαστήριο, απαραίτητη προϋπόθεση για την πρόσβαση από την NSA σε αυτά τα δεδομένα αποτελούσε η ύπαρξη «*reasonable articulable suspicion*», ότι συγκεκριμένος αριθμός συσχετιζόταν άμεσα με τρομοκρατικές οργανώσεις. Στην παρούσα υπόθεση οι Ενάγοντες ισχυρίστηκαν ότι υπήρξε σοβαρή παραβίαση των δικαιωμάτων τους δυνάμει της Τέταρτης Τροπολογίας του Συντάγματος των ΗΠΑ και ζητούσαν όπως διακοπεί το πρόγραμμα μαζικής συλλογής δεδομένων και αποζημιώσεις. Ωστόσο, το δικαστήριο παρά τους ισχυρισμούς των Εναγόντων έκρινε ότι, προκειμένου να υπάρχει αγώγιμο δικαίωμα, οι Ενάγοντες πρέπει να αποδείξουν ότι τα δεδομένα τους συλλέχθηκαν από την κυβέρνηση.

Αρκετά σημαντικό σημείο στην υπό κρίση υπόθεση αφορά η αναφορά του δικαστηρίου στην περιορισμένη αποκάλυψη που δύναται να αιτηθούν οι Ενάγοντες σε παρόμοιες υποθέσεις, η οποία δυνατό να τους βοηθήσει και ενισχύσει την υπόθεση τους, αφετέρου όμως υπάρχει η απροθυμία του κράτους να παρέχει την εν λόγο περιορισμένη αποκάλυψη έτσι ώστε να προστατευθούν οι υπηρεσίες αναφέροντας επι λέξει «*Plaintiffs must realize that secrecy is yet another form of regulation, prescribing not 'what the citizen may do' but instead 'what the citizen may know' […]*[122]». Προκειμένου να ενισχύσει αυτή τη θέση του, το δικαστήριο ενδεικτικά αναφέρει ότι ακόμη ένας λόγος που δεν προχωρεί στην περιορισμένη αποκάλυψη επαφίεται στο ότι η άκρα μυστικότητα περιορίζει την κριτική και τη συζήτηση.

Ακόμη μια εξίσου σημαντική υπόθεση είναι η *ACLU v. Clapper*[123]. Στην συγκεκριμένη υπόθεση η Αμερικανική Ένωση Πολιτικών Ελευθεριών (ACLU) προσέφυγε ενώπιον του Δευτεροβάθμιου Ομοσπονδιακού Εφετείου, αμφισβητώντας τη νομιμότητα του προγράμματος συλλογής τηλεφωνικών μεταδεδομένων από την NSA, το οποίο διεξαγόταν βάσει του Section 215 του USA Patriot Act. Η αγωγή βασίστηκε στις αποκαλύψεις του Edward Snowden το 2013, οι οποίες αποκάλυψαν ότι η κυβέρνηση σύλλεγε μαζικά και αδιάκριτα δεδομένα τηλεπικοινωνιών από παρόχους όπως η Verizon, χωρίς να παρέχει εύλογη υπόνοια ή ένταλμα για κάθε επιμέρους πολίτη. Αν και σε πρώτο βαθμό το δικαστήριο απέρριψε την αγωγή, το Εφετείο αναγνώρισε ότι η ερμηνεία του Section 215 από την κυβέρνηση υπερέβαινε το νομοθετικό του πλαίσιο και ότι η μαζική συλλογή δεδομένων δεν ήταν

[120] *Klayman v Obama*, 800 F3d 559 (DC Cir 2015).
[121] Ibid 2.
[122] Ibid 5.
[123] *ACLU v Clapper*, 785 F3d 787 (2d Cir 2015).

σύμφωνη με τη βούληση του Κογκρέσου, ούτε μπορούσε να θεωρηθεί σχετική με κάποια έρευνα. Παρότι το δικαστήριο απέφυγε να αποφανθεί ευθέως περί αντισυνταγματικότητας της Τέταρτης Τροπολογίας, αναγνώρισε την αντιστοιχία μεταξύ θεσμικού πλαισίου και πρακτικής. Η υπόθεση δεν κατέληξε σε ποινικές ευθύνες για τα στελέχη των υπηρεσιών, ανέδειξε ωστόσο τα όρια της θεσμικής λογοδοσίας και επιτάχυνε την κατάργηση του επίμαχου προγράμματος μέσω της θέσπισης του USA Freedom Act το 2015, εισάγοντας αυστηρότερα κριτήρια για τη συλλογή τηλεπικοινωνιακών δεδομένων.

Στην ως άνω υπόθεση ειδική αναφορά γίνετε από το δικαστήριο σχετικά με την παράγραφο 215 του Patriot Act, προχωρώντας σε μια σύντομη ιστορική αναδρομή όσο αφορά τη λειτουργία του εν λόγω άρθρου, την εξελικτική του πορεία αναφέροντας συγκεκριμένα ότι αρχικά οι πάροχοι τηλεφωνικών υπηρεσιών παρείχαν στον διευθυντή του FBI μετά από σχετική εξουσιοδότηση από το δικαστήριο FISC τηλεφωνικά μεταδεδομένα τα οποία αφορούσαν επιχειρήσεις. Εν συνεχεία, με τις διάφορες τροποποιήσεις στον πιο πάνω αναφερόμενο νόμο, προστέθηκαν οι λέξεις «*any tangible things*», εξαλείφοντας τους οποιουσδήποτε περιορισμούς και παράλληλα παρέχοντας στις μυστικές υπηρεσίες τη δυνατότητα να λαμβάνουν τηλεφωνικά μεταδεδομένα τα οποία δεν αφορούν μόνο επιχειρήσεις[124]. Επιπρόσθετα, εξίσου σημαντική είναι η αναφορά στην απόφαση του δικαστηρίου όσο αφορά το FISC δικαστήριο, δια το οποίο αναφέρει ρητά τον τρόπο λειτουργίας του, λέγοντας ότι οι αιτήσεις προς το δικαστήριο γίνονται ex parte (μονομερώς χωρίς ειδοποίηση προς το άλλο διάδικο μέρος), πίσω από κλειστές πόρτες και οι στόχοι της συλλογής δεδομένων δεν τυγχάνουν εκπροσώπησης από δικηγόρο[125].

Περαιτέρω, η υπόθεση *ACLU v. NSA (2006)*[126] αποτέλεσε μια από τις κυριότερες νομικές προκλήσεις κατά της αμερικανικής κυβέρνησης για το πρόγραμμα Terrorist Surveillance Program, το οποίο υλοποιήθηκε από την NSA μετά την 11η Σεπτεμβρίου. Η Αμερικανική Ένωση Πολιτικών Ελευθεριών, προσέφυγε κατά της κυβέρνησης Bush, καταγγέλλοντας τη μαζική και εξωθεσμική παρακολούθηση τηλεφωνικών και ηλεκτρονικών επικοινωνιών χωρίς ουδεμία δικαστική άδεια, κατά παράβαση του Foreign Surveillance Act, και της Τέταρτης Τροπολογίας του Συντάγματος. Το Δικαστήριο αποφάσισε ότι το εν λόγω πρόγραμμα παραβιάζει την Τέταρτη Τροπολογία και το FISA, καθώς στερείται νομικής βάσης και θεσμικής εποπτείας. Αν και η απόφαση ανετράπη σε δεύτερο βαθμό για λόγους έλλειψης έννομου συμφέροντος, η υπόθεση ανέδειξε σημαντικά ζητήματα σχετικά με τη συνταγματικότητα των κυβερνητικών προγραμμάτων παρακολούθησης, τη διακριτική ευχέρεια των μυστικών υπηρεσιών και την απουσία ποινικής λογοδοσίας για παραβιάσεις των δικαιωμάτων των πολιτών. Παρά την έλλειψη ουσιαστικών συνεπειών για τα εμπλεκόμενα στελέχη της κυβέρνησης ή των υπηρεσιών, η υπόθεση συνέβαλε στην έναρξη δημοσίου και νομικού διάλογου για τα όρια της εθνικής ασφάλειας και της ιδιωτικότητας στο πλαίσιο της αντιτρομοκρατικής πολιτικής των ΗΠΑ. Ως εκ των ως άνω, γίνετε άμεσα αντιληπτό δια μέσου της υπό κρίση απόφασης ότι, αφενός δεν οδήγησε σε οποιαδήποτε ποινική κύρωση, αφετέρου όμως ανέδειξε σε σημαντικό βαθμό την απουσία ελέγχου των υπηρεσιών πληροφοριών και την αδυναμία απόδοσης ευθύνης.

[124] Ibid 11.
[125] Ibid 8 [14-42] cv, SACK, Circuit Judge.
[126] *ACLU v NSA*, 493 F3d 644 (6th Cir 2007).

Οι ως άνω αναφερθείσες υποθέσεις, αποτελούν τρεις θεμελιώδεις σταθμούς στη νομική αξιολόγηση των μαζικών παρακολουθήσεων από τις μυστικές υπηρεσίες των ΗΠΑ, αναδεικνύοντας τις βαθιές προκλήσεις που ανακύπτουν στην προσπάθεια εξισορρόπησης της εθνικής ασφάλειας με τα ατομικά δικαιώματα. Σε όλες τις υποθέσεις καταγράφεται η εφαρμογή μαζικών, αδιάκριτων και εξωδικαστικών πρακτικών παρακολούθησης, είτε μέσω τηλεφωνικών μεταδεδομένων, είτε μέσω ηλεκτρονικών επικοινωνιών χωρίς ένταλμα, οι οποίες πραγματοποιούνταν από την NSA με τη στήριξη προγραμμάτων όπως το FISA, TSP και ο Patriot Act. Κοινός παρονομαστής είναι η προσφυγή των πολιτών και οργανώσεων επικαλούμενοι παραβίαση της Τέταρτης Τροπολογίας, η οποία κατοχυρώνει την προστασία από παράνομες έρευνες και κατασχέσεις.

Ωστόσο, παρά τις σοβαρές διαπιστώσεις περί υπέρβασης των νομικών ορίων και λειτουργίας των υπηρεσιών εκτός του θεσμικού πλαισίου, καμία από τις υποθέσεις δεν κατέληξε σε επιβολή ποινικών ευθυνών προς τις αρμόδιες αρχές ή τα φυσικά πρόσωπα που ενέκριναν ή υλοποίησαν τα προγράμματα παρακολούθησης. Η αδυναμία αναγνώρισης έννομου συμφέροντος από τα δικαστήρια (λόγω έλλειψης απόδειξης προσωπικής ζημιάς) υπογραμμίζει την πρακτική δυσκολία ελέγχου των μυστικών υπηρεσιών μέσω των κλασικών ένδικων βοηθημάτων. Παράλληλα, η επίκληση της κρατικής μυστικότητας περιορίζει τη δυνατότητα πρόσβασης των εναγόντων σε κρίσιμα στοιχεία, συντηρώντας ένα καθεστώς υπερπροστασίας της εκτελεστικής εξουσίας.

Προς υποστήριξη της ως άνω παρατήρησης, έχει λεχθεί ότι:

> «*The difficulty with reliance on such rules is that Nardone is not sweeping in reach and each case requires an examination of the particular facts. Subjecting intelligence activities to advance legal review for potential criminal activities, and producing the resulting legal opinions in coordination with the Department of Justice, is time consuming, inefficient, and unfair to those intelligence officers at risk of being targets of criminal investigations. It is unlikely that such officers would ultimately be convicted for actions they believed to be officially authorized. For one reason, they would not possess the required mens rea, or criminal intent, in almost every situation*[127]».

Περαιτέρω, ιδιαίτερη σημασία έχει το Executive Order 12,333 του 1981, και ειδικότερα το μέρος 1.7, το οποίο διευκρινίζει ότι η μυστικότητα υπό την οποία λειτουργούν οι υπηρεσίες πληροφοριών δεν συνιστά μόνιμη ασπίδα για όλες τις πράξεις τους. Βάσει της εν λόγω διάταξης, οι υπηρεσίες πληροφοριών υποχρεούνται να αναφέρουν τυχόν παραβιάσεις ποινικών νόμων που διαπράττονται από πράκτορες, κατασκόπους, υπαλλήλους ή οποιοδήποτε άλλο πρόσωπο ενεργεί υπό τις οδηγίες τους, σύμφωνα με κατευθυντήριες γραμμές που έχουν εκπονηθεί από τον Γενικό Εισαγγελέα και την αρμόδια υπηρεσία[128].

Η παραπάνω ρύθμιση καταδεικνύει ότι η αρχή της νομιμότητας ισχύει και στον χώρο των μυστικών υπηρεσιών, αποκλείοντας την ύπαρξη απόλυτης ασυλίας. Συναφώς, έχει υποστηριχθεί ότι το ποινικό δίκαιο μπορεί να λειτουργήσει ως όριο ακόμη και για τις ενέργειες του Προέδρου των ΗΠΑ. Αν και είναι σπάνιο να καταλογιστεί ποινική ευθύνη σε

[127] Paul J Manget, 'Intelligence and the Criminal Law in the United States' (2006) 19 (2) International Journal of Intelligence and Counterintelligence 431.
[128] Ibid 433.

υπαλλήλους που δρουν καλή τη πίστει εντός των ορίων της νομιμότητας, η ίδια διαδικασία μιας ποινικής έρευνας μπορεί να αποβεί ιδιαιτέρως επιβαρυντική, τόσο για τα εμπλεκόμενα πρόσωπα όσο και για τις ίδιες τις υπηρεσίες, με συνέπειες που μπορεί να διαρκέσουν έτη[129]. Επιπλέον, έχει επισημανθεί ότι η εμφάνιση στοιχείων περί τέλεσης εγκλήματος από πρόσωπα του χώρου της εθνικής ασφάλειας και της συλλογής πληροφοριών μπορεί να οδηγήσει σε απότομη διακοπή ακόμη και νόμιμων και κρίσιμων επιχειρήσεων συλλογής πληροφοριών[130].

Κρίσιμη είναι και η υπόθεση *USA v. Moalin*[131], εις την οποία κάποιος Σομαλός μετανάστης στις ΗΠΑ κατηγορήθηκε μαζί με άλλα άτομα για παροχή υποστήριξης σε τρομοκρατική οργάνωση. Η δίωξη του βασίστηκε κατά κύριο λόγο σε αποδείξεις που συγκεντρώθηκαν, μεταξύ άλλων, από το μαζικό πρόγραμμα τηλεφωνικής μεταδεδομένης παρακολούθησης της NSA. Το πρόγραμμα αυτό, συγκέντρωνε χωρίς ένταλμα πληροφορίες για τηλεφωνικές κλήσεις εκατομμυρίων Αμερικανών πολιτών, παραβιάζοντας κατά συνέπεια τη FISA.

Το δικαστήριο, έκρινε ότι το εν λόγω πρόγραμμα συλλογής τηλεφωνικών μεταδεδομένων της NSA ήταν παράνομο και ενδεχομένως αντισυνταγματικό, καθώς παραβίασε τις προβλέψεις της FISA. Συγκεκριμένα, το δικαστήριο διαπίστωσε ότι το πρόγραμμα παραβίασε το άρθρο 50 U.S.C Par. 1861, το οποίο προϋποθέτει συγκεκριμένες και τεκμηριωμένες ενδείξεις ότι τα δεδομένα σχετίζονται με τρομοκρατική δραστηριότητα, κάτι το οποίο δεν ίσχυε στην περίπτωση της γενικευμένης συλλογής.

Συνολικά, η εν λόγω απόφαση αποτελεί σημαντικό νομικό προηγούμενο που αναγνωρίζει πως ακόμη και υπηρεσίες εθνικής ασφάλειας υπόκεινται στο κράτος δικαίου, και πως η παράνομη συλλογή δεδομένων μπορεί να έχει συνέπειες τόσο νομικές όσο και ποινικές, εφόσον αποδειχθεί πρόθεση και παραβίαση της FISA.

Εν κατακλείδι, οι υποθέσεις αποκαλύπτουν τη διαδικασία εσωτερικής επιτήρησης μέσω του FISA το οποίο όμως λειτουργεί χωρίς διαφάνεια, χωρίς συμμετοχή ή εκπροσώπηση του θιγόμενου προσώπου και με περιορισμένο ουσιαστικό έλεγχο της κυβερνητικής δράσης. Αν και η υπόθεση Clapper (ανωτέρω) οδήγησε στη ψήφιση του USA Freedom Act 2015, ο οποίος περιόρισε το νομικό έρεισμα για τις μαζικές παρακολουθήσεις, το ζήτημα της ουσιαστικής λογοδοσίας και της ποινικής ευθύνης των μυστικών υπηρεσιών παραμένει ανοιχτό. Οι αποφάσεις αυτές επιβεβαιώνουν ότι οι μυστικές υπηρεσίες στις ΗΠΑ λειτουργούν σε ένα καθεστώς μεταθεσμικής αυτονομίας, όπου οι δικλείδες ασφαλείας δεν αρκούν πάντοτε για την προστασία των θεμελιωδών ελευθεριών. Κατοχυρώνεται επίσης μέσα από τις πιο πάνω αναφερθείσες υποθέσεις ότι η εθνική ασφάλεια και η προστασία του κράτους έναντι της τρομοκρατίας και του οργανωμένου εγκλήματος υποσκιάζει την ανάγκη για την προστασία του δικαιώματος της ιδιωτικότητας.

6. Ηνωμένο Βασίλειο

6.1. Μυστικές Υπηρεσίες

[129] Ibid.
[130] Ibid 434.
[131] *United States v Moalin*, 973 F3d 977 (9th Cir 2020).

Οι μυστικές υπηρεσίες του ΗΒ διαδραματίζουν ένα καθοριστικό ρόλο στη διασφάλιση της εθνικής ασφάλειας και στην αντιμετώπιση απειλών τόσο στο εσωτερικό όσο και στο εξωτερικό της χώρας. Οι βρετανικές υπηρεσίες ασφαλείας βασίζονται κυρίως σε τρεις βασικούς οργανισμούς, την MI5 (Security Service) η οποία είναι αρμόδια για την εσωτερική ασφάλεια, την MI6 (Secret Intelligence Service) η οποία είναι υπεύθυνη για τη συλλογή πληροφοριών στο εξωτερικό, και την GCHQ (Government Communications Headquarters) η οποία εξειδικεύεται στην ηλεκτρονική παρακολούθηση και την κυβερνοασφάλεια. Οι υπηρεσίες αυτές λειτουργούν υπό την εποπτεία της κυβέρνησης και συντονίζονται από την Μεικτή Επιτροπή Πληροφοριών (Joint Intelligence Committee), παρέχοντας κρίσιμες πληροφορίες για την πρόληψη τρομοκρατικών ενεργειών, την αντιμετώπιση απειλών στον κυβερνοχώρο και την υποστήριξη της εξωτερικής πολιτικής του ΗΒ.

Η MI5 ξεκίνησε να υπάρχει ως υπηρεσία πληροφοριών από το 1909, υπήρξε από τότε μέχρι και σήμερα σε διάφορες μορφές μέχρι να καταλήξει όπως είναι σήμερα. Η αρχική της ονομασία ήταν Secret Service Bureau, και ο οργανισμός ιδρύθηκε από τον Captain Vernon Kell, διαδραματίζοντας μεγάλο ρόλο στη σύλληψη πολλών πρακτόρων της Γερμανίας που βρίσκονταν στο Ηνωμένο Βασίλειο κατά τη διάρκεια του Πρώτου Παγκοσμίου Πολέμου[132]. Προτεραιότητα για την MI5 ήταν κατά τα έτη 1990-2000 οι διάφορες τρομοκρατικές απειλές από τη Βόρεια Ιρλανδία και κράτη όπως η Λιβύη του Συνταγματάρχη Καντάφι[133]. Πλέον, η MI5 ενασχολείται με κίνδυνους οι οποίοι στόχο έχουν να πλήξουν το ΗΒ εσωτερικά, όπως λόγου χάριν διάφορες τρομοκρατικές επιθέσεις από ισλαμιστές και άλλα.

Αντίθετα με την MI5, η οποία δραστηριοποιείται εντός του ΗΒ, η MI6 είναι επιφορτισμένη με τη συλλογή πληροφοριών στο εξωτερικό, παρέχοντας στην κυβέρνηση μια παγκόσμια επιχειρησιακή δυνατότητα που στοχεύει στην προστασία της εθνικής ασφάλειας και την ενίσχυση της οικονομικής ευημερίας της χώρας[134]. Η MI6 ιδρύθηκε παράλληλα με την MI5 ως παράρτημα του Secret Service Bureau με κυριότερο στόχο τη διεξαγωγή εξωτερικών επιχειρήσεων πληροφοριών[135]. Η δράση της MI6 καλύπτεται από υψηλό επίπεδο μυστικότητας και οι λεπτομέρειες για τις επιχειρήσεις της παραμένουν αυστηρά απόρρητες. Είναι γνωστό ωστόσο ότι συνέβαλε σημαντικά στην ασφάλεια των Ολυμπιακών Αγώνων του Λονδίνου το 2012, αναλαμβάνοντας την πρόληψη ενδεχόμενων τρομοκρατικών επιθέσεων και άλλων απειλών κατά τη διάρκεια της διοργάνωσης[136].

Η GCHQ – Government Communication Headquarters, αποτελεί την αρμόδια υπηρεσία του ΗΒ για την ηλεκτρονική επιτήρηση, την κυβερνοασφάλεια και την κρυπτογράφηση, διαδραματίζοντας κεντρικό ρόλο στην εθνική ασφάλεια μέσω της αξιοποίησης προηγμένων τεχνολογιών και μεθόδων συλλογής πληροφοριών[137]. Οι κυριότεροι τομείς δραστηριοποίησης περιλαμβάνουν την καταπολέμηση της τρομοκρατίας, την αποτροπή

[132] Security Service (MI5), 'MI5's Early Years' (MI5) https://www.mi5.gov.uk/history/mi5s-early-years accessed 3 June 2025.
[133] Security Service (MI5), 'MI5 in the 1990s and 2000s' (MI5) https://www.mi5.gov.uk/history/mi5-in-the-1990s-and-2000s accessed 3 June 2025.
[134] UK Government, 'About the Secret Intelligence Service (MI6)' (GOV.UK, undated) https://www.gov.uk/government/organisations/secret-intelligence-service/about accessed 3 June 2025.
[135] Secret Intelligence Service (MI6), 'Our History' (SIS, undated) https://www.sis.gov.uk/about-us/our-history accessed 3 June 2025.
[136] Ibid.

[137] Government Communications Headquarters (GCHQ), 'Overview' (GCHQ, undated) https://www.gchq.gov.uk/section/mission/overview accessed 3 June 2025.

κυβερνοεπιθέσεων, την αντιμετώπιση απειλών από εχθρικά κράτη, καθώς και την υποστήριξη ερευνών για σοβαρό και οργανωμένο έγκλημα, ενώ παράλληλα παρέχει ουσιαστική στήριξη στην εθνική άμυνα, προστατεύοντας το ανθρώπινο δυναμικό και την κρίσιμη υποδομή του Υπουργείου Άμυνας[138]. Η λειτουργία της GCHQ διέπεται από αυστηρό νομικό πλαίσιο και εποπτεύεται από ανεξάρτητους φορείς, προκειμένου να διασφαλίζεται η νομιμότητα και αναλογικότητα των δραστηριοτήτων της. Μέσα από ένα εύρος τεχνικών, όπως λόγου χάριν η παρακολούθηση επικοινωνιών και η επεξεργασία ψηφιακών δεδομένων, η GCHQ συλλέγει και αναλύει πληροφορίες υψηλής στρατηγικής αξίας. Τα ευρήματα αυτά αξιοποιούνται για την παραγωγή αναλυτικών εκθέσεων που υποστηρίζουν τη λήψη αποφάσεων από την κυβέρνηση, με σκοπό την πρόληψη και διαχείριση κρίσεων που δύνανται να απειλήσουν την ασφάλεια και τα συμφέροντα του ΗΒ[139].

Ιδιαίτερα κρίσιμο ρόλο στο σύστημα εποπτείας των βρετανικών υπηρεσιών πληροφοριών διαδραματίζει η Intelligence and Security Committee of Parliament, η οποία ιδρύθηκε δυνάμει του Intelligence Services Act 1994 και ενισχύθηκε θεσμικά με το Justice and Security Act 2013[140]. Η ISC αποτελεί ανεξάρτητη, διακομματική επιτροπή του Κοινοβουλίου εφόσον αποτελείται από εννέα μέλη τα οποία προέρχονται από το Κοινοβούλιο. Κυριότερος ρόλος της είναι η εποπτεία στις πολιτικές, τις δαπάνες, τη διοίκηση και τις επιχειρήσεις των MI5, MI6, GCHQ, της Στρατιωτικής Υπηρεσίας Πληροφοριών (Defence Intelligence), της Εθνικής Δύναμης Κυβερνοασφάλειας (National Cyber Force), της Κοινής Οργάνωσης Πληροφοριών (Joint Intelligence Organisation), της Γραμματείας Εθνικής Ασφάλειας (National Security Secretariat – NSS) και της Ομάδας Εσωτερικής Ασφάλειας (Homeland Security Group)[141]. Μέσω της πιο πάνω αναφερθείσας δομής, επιδιώκεται η ισορροπία μεταξύ της ανάγκης προστασίας της εθνικής ασφάλειας και της δημοκρατικής λογοδοσίας, διασφαλίζοντας ότι οι υπηρεσίες πληροφοριών λειτουργούν εντός των ορίων της νομιμότητας και υπό την επίβλεψη της εκλεγμένης αντιπροσωπείας του λαού.

Συνοψίζοντας, οι μυστικές υπηρεσίες πληροφοριών του ΗΒ αποτελούν ένα εξειδικευμένο και πολυεπίπεδο σύστημα διαχείρισης κινδύνων που στοχεύει στην προστασία της εθνικής ασφάλειας, τόσο στο εσωτερικό όσο και στο διεθνές πεδίο. Μέσω της συντονισμένης δράσης των MI5, MI6 και GCHQ και υπό την εποπτεία ανεξάρτητων θεσμών όπως η ISC, επιδιώκεται η αποτελεσματική πρόληψη απειλών, η ενίσχυση της στρατηγικής ασφάλειας και η διασφάλιση της λειτουργίας των υπηρεσιών εντός των πλαισίων της δημοκρατικής λογοδοσίας και του κράτους δικαίου.

6.2. Νομοθετικό πλαίσιο

Το νομοθετικό πλαίσιο του ΗΒ που ρυθμίζει τις μαζικές παρακολουθήσεις και την προστασία των ατομικών δικαιωμάτων αντικατοπτρίζει τη συνεχή προσπάθεια του κράτους να ανταποκριθεί στις απαιτήσεις της εθνικής ασφάλειας, χωρίς να παραβλέπει τις θεμελιώδεις ελευθερίες των πολιτών. Μέσα από μια σειρά νομοθετημάτων, όπως και μηχανισμών εποπτείας και λογοδοσίας, το ΗΒ επιδιώκει να οριοθετήσει τις εξουσίες των κρατικών

[138] Ibid.
[139] Ibid.
[140] Intelligence and Security Committee of Parliament, 'Home – ISC' (ISC, undated) https://isc.independent.gov.uk/ accessed 3 June 2025.
[141] Ibid.

υπηρεσιών πληροφόρησης και να διασφαλίσει τη συμμόρφωση με τις αρχές της αναλογικότητας, της νομιμότητας και του σεβασμού της ιδιωτικής ζωής. Η νομοθεσία αυτή εξελίσσεται διαρκώς, καθώς καλείται να αντιμετωπίσει τις προκλήσεις της τεχνολογικής προόδου και των νέων μορφών απειλών, ενώ παράλληλα υπόκειται σε αυστηρό δικαστικό και δημόσιο έλεγχο ως προς τη συμβατότητα της με τα ανθρώπινα δικαιώματα.

Το Security Service Act 1989[142] καθιερώνει την MI5 και ορίζει τις αρμοδιότητες της. Εις το άρθρο 1 (2) καθορίζεται με σαφή τρόπο ότι ο σκοπός λειτουργίας της υπηρεσίας πληροφοριών είναι η προστασία της εθνικής ασφάλειας, και πιο συγκεκριμένα από απειλές όπως κατασκοπεία, τρομοκρατία και δολιοφθορά, από δραστηριότητες πρακτόρων ξένων δυνάμεων, και επίσης σύμφωνα με το άρθρο 1 (3) καθιερώνεται στις δράσεις της υπηρεσίας η διασφάλιση της οικονομικής ευημερίας του ΗΒ από απειλές οι οποίες προέρχονται από ενέργειες ή προθέσεις ατόμων εκτός των Βρετανικών Νήσων[143]. Περαιτέρω, σε τροποποιήσεις που έγιναν στον νόμο περί το 2000, το άρθρο 2 (2) καθορίζει πως ο υπεύθυνος της υπηρεσίας πληροφοριών πρέπει να διασφαλίζει ότι θα συλλέγονται πληροφορίες οι οποίες σχετίζονται με τις λειτουργίες της υπηρεσίας και αποσκοπούν στην πρόληψη και καταπολέμηση σοβαρών εγκλημάτων, ότι η υπηρεσία δεν θα προβαίνει σε πράξεις οι οποίες να προωθούν τα συμφέροντα οποιουδήποτε πολιτικού κόμματος και άλλα[144].

Το Intelligence Services Act 1994[145] καθιερώνει νομικά την MI6 και GCHQ, και παράλληλα καθορίζει τις εξουσίες τους όσο αφορά τη συλλογή πληροφοριών. Το άρθρο 1 καθορίζει ότι οι αρμοδιότητες της υπηρεσίας πληροφοριών θα είναι η απόκτηση και παροχή πληροφοριών σχετικά με τις ενέργειες ή/και προθέσεις προσώπων που βρίσκονται εκτός των Βρετανικών Νήσων, και οι εν λόγω αρμοδιότητες της δύνανται να ασκηθούν μόνο προς το συμφέρον της εθνικής ασφάλειας, της οικονομικής ευημερίας του ΗΒ και προς υποστήριξη της πρόληψης και ανίχνευσης σοβαρών εγκλημάτων[146]. Επιπλέον, παρόμοιες πρόνοιες με το Security Service Act αναφέρονται και στην παράγραφο 2 του Intelligence Service Act σχετικά με την μη συλλογή πληροφοριών οι οποίες δεν είναι αναγκαίες για την εκτέλεση των εργασιών της υπηρεσίας πληροφοριών, ενώ παράλληλα δυνάμει της παραγράφου 4 του άρθρου 2 επιβάλλεται η θετική υποχρέωση στην υπεύθυνο της υπηρεσίας πληροφοριών όπως ετοιμάζει και παραδίδει ετήσια έκθεση στον Πρωθυπουργό και στον Υπουργό Εξωτερικών σχετικά με ζητήματα που αφορούν το έργο της[147], κάτι το οποίο πρακτικά συνεισφέρει στον επαρκή έλεγχο και λογοδοσία των υπηρεσιών διασφαλίζοντας παράλληλα μια δημοκρατική κοινωνία και προστατεύοντας τα ανθρώπινα δικαιώματα. Ιδιαίτερα σημαντικές είναι οι πρόνοιες του άρθρου 5 οι οποίες αφορούν την έκδοση ενταλμάτων. Πιο συγκεκριμένα, το εν λόγω άρθρο επιβάλλει τη θετική υποχρέωση όπως προτού γίνει είσοδος σε κάποιο ακίνητο ή σε ασύρματη τηλεγραφία ληφθεί ένταλμα από τον Υπουργό, μετά από αίτηση της υπηρεσίας πληροφοριών, εις το οποίο να εξουσιοδοτεί την υπηρεσία για τη λήψη των αναγκαίων μέτρων όπως αυτά θα περιγράφονται στο ένταλμα για την εκτέλεση των σκοπών της. Επιπρόσθετα, αποτελεί απαραίτητη προϋπόθεση για την έκδοση του εν λόγω εντάλματος η ισορροπία μεταξύ της πράξης που πρόκειται να ληφθεί με το αποτέλεσμα που

[142] Security Service Act 1989 (UK) c 5.
[143] Ibid s 1(2), (3).
[144] Ibid s 2 (2) (a)- (b).
[145] Intelligence Services Act 1994 (UK) c 13.
[146] Ibid ss 1-2.
[147] Ibid s 2 (4).

επιδιώκεται και εξετάζεται κατά πόσο τα μέτρα που πρόκειται να ληφθούν μπορούσαν να εκπληρωθούν με οποιοδήποτε άλλο τρόπο[148].

Το Regulation of Investigatory Powers Act[149], ίσως ο πιο σημαντικός νόμος για παρακολουθήσεις και υποκλοπές στο ΗΒ, θεσπίστηκε για να ρυθμίζει τις εξουσίες παρακολούθησης των δημοσίων αρχών, διασφαλίζοντας ότι η συλλογή πληροφοριών (μέσω υποκλοπών, επιτήρησης και μυστικών πληροφοριοδοτών) γίνεται νόμιμα, αναλογικά και με σεβασμό στα δικαιώματα ιδιωτικότητας των πολιτών. Πιο συγκεκριμένα, το άρθρο 1 του νόμου ρυθμίζει την έννοια της παράνομης και εξουσιοδοτημένης υποκλοπής επικοινωνιών, προβλέποντας ότι συνιστά ποινικό αδίκημα η εκ προθέσεως και χωρίς νόμιμη εξουσιοδότηση παρεμβολή ή υποκλοπή επικοινωνιών εντός της επικράτειας του ΗΒ, είτε μέσω ταχυδρομείου είτε μέσω δημόσιου τηλεπικοινωνιακού συστήματος[150]. Επιπλέον, η παράγραφος 7 του ίδιου άρθρου, προβλέπει τις ποινικές κυρώσεις για τα πρόσωπα που κριθούν ένοχα για την τέλεση της εν λόγω παράνομης πράξης επιβάλλοντας ποινές φυλάκισης οι οποίες δεν ξεπερνούν τα δύο (2) χρόνια ή/και επιβολή προστίμου[151]. Το άρθρο 2 του νόμου προβαίνει σε εκτενή ανάλυση και επεξήγηση διάφορων όρων μεταξύ των οποίων η υποκλοπή, το ιδιωτικό δίκτυο τηλεπικοινωνιών και άλλα, προσδιορίζοντας με αυτό τον τρόπο τη σημασία των λέξεων και τη χρήση τους εντός του νομοθετήματος[152]. Περαιτέρω, ειδική αναφορά γίνεται στο άρθρο 5 όσο αφορά την έκδοση εντάλματος εξουσιοδοτώντας λειτουργούς των υπηρεσιών να προβαίνουν σε υποκλοπές όπως λόγου χάριν, υποκλοπή επιστολών δια μέσου ταχυδρομείου, τη συμμόρφωση με οποιαδήποτε διεθνή σύμβαση και παροχή βοήθειας υποκλοπής πληροφοριών με οποιοδήποτε τρόπο αυτές ζητηθούν και άλλα[153]. Εν συνεχεία, ιδιαίτερα σημαντικές είναι οι παραγράφοι (2) και (3) του άρθρου 5, καθότι καθορίζουν με σαφήνεια ότι ο Υπουργός δύναται να αρνηθεί την έκδοση τέτοιου εντάλματος στην περίπτωση που κρίνει ότι η ενέργεια που εγκρίνεται με το ένταλμα είναι δυσανάλογη προς αυτό που επιδιώκεται να επιτευχθεί[154], και επιπρόσθετα ότι πρέπει να τηρούνται σημαντικές προϋποθέσεις για την επιτυχία έκδοσης ενός τέτοιου εντάλματος, ήτοι, να αποβλέπει στην προστασία της δημόσιας ασφάλειας, για την πρόληψη και ανίχνευση σοβαρών εγκλημάτων, για την προστασία της οικονομίας του ΗΒ, και για οποιοδήποτε άλλο λόγο ο Υπουργός κρίνει ότι είναι ισοδύναμες με εκείνες υπό τις οποίες κανονικά θα εξέδιδε ένταλμα δυνάμει των προηγούμενων παραγράφων και της εφαρμογής διατάξεων οποιασδήποτε διεθνούς συμφωνίας αμοιβαίας συνδρομής[155].

Επιπρόσθετα, ο νόμος καθορίζει ακόμη μια προϋπόθεση για την έκδοση των εν λόγω ενταλμάτων, πιο συγκεκριμένα, αν οι πληροφορίες που επιζητείται όπως αποκτηθούν, μπορούν να αποκτηθούν με οποιοδήποτε άλλο μέσο ή/και τρόπο[156]. Συν τοις άλλοις, ο νόμος καθορίζει ποια άτομα ή/και εκπρόσωποι τους δύνανται να προχωρήσουν σε αίτηση για έκδοση αυτών των ενταλμάτων[157], όπως επίσης και από ποιους πρέπει να υπογράφεται[158].

[148] Ibid s 5.
[149] Regulation of Investigatory Powers Act 2000 (UK) c 23.
[150] Ibid s1.
[151] Ibid s 1 (7).
[152] Ibid s 2.
[153] Ibid s 5.
[154] Ibid s 5 (2).
[155] Ibid s 5 (3).
[156] Ibid s 5 (4).
[157] Ibid s 6.
[158] Ibid s 7.

Σύμφωνα με το άρθρο 8, το ένταλμα για υποκλοπή πρέπει απαραίτητα να αναφέρει προς ποιο άτομο απευθύνεται ή/και ένα ενιαίο σύνολο εγκαταστάσεων ως οι εγκαταστάσεις στις οποίες πρόκειται να πραγματοποιηθεί η υποκλοπή στην οποία αφορά και πρέπει να περιγράφονται οι επικοινωνίες των οποίων η υποκλοπή εγκρίνεται ή απαιτείται από το ένταλμα, και να περιλαμβάνονται διευθύνσεις, αριθμοί, συσκευές και άλλοι παράγοντες που πρόκειται να χρησιμοποιηθούν για τον εντοπισμό των επικοινωνιών που πρόκειται να υποκλαπούν[159]. Περαιτέρω, το άρθρο 9 καθορίζει την περίοδο λήξης ενός εντάλματος και επίσης παρέχει τη δυνατότητα στις υπηρεσίες πληροφοριών όπως προχωρήσουν σε ανανέωση του εντάλματος[160]. Δυνάμει των άρθρων 55, 57, 58 και 59, υπάρχουν πρόνοιες σχετικά με τα άτομα που διαχειρίζονται τα ευαίσθητα δεδομένα (άρθρο 55), διορίζεται επικεφαλής ο οποίος φέρει ως αρμοδιότητα την επίβλεψη του Υπουργού για τις αρμοδιότητες του οι οποίες εμπίπτουν στα άρθρα 1-11 (άρθρο 57), επιβάλλεται η θετική υποχρέωση προς όλα τα εμπλεκόμενα μέρη όπως ενημερώνουν και αποκαλύπτουν τις πληροφορίες που χρειάζεται δια την εκτέλεση των εργασιών του δυνάμει του άρθρου 57 (άρθρο 58), και διορίζεται επίτροπος υπηρεσιών πληροφοριών του οποίου οι αρμοδιότητες, μεταξύ άλλων, είναι η επίβλεψη του Υπουργού κατά την ενάσκηση των εξουσιών του όπως αυτές του παρέχονται δυνάμει του Intelligence Services Act 1994[161]. Είναι επομένως αντιληπτό ότι το ως άνω αναφερθέν νομοθέτημα, καλύπτει πλήρως και με σαφήνεια όλες τις παραμέτρους οι οποίες αφορούν την υποκλοπή δεδομένων και παρακολουθήσεις.

Σε πιο γενικό πλαίσιο, ο RIPA 2000, αποτελεί βασικό νομοθέτημα του ΗΒ το οποίο ρυθμίζει τις εξουσίες παρακολούθησης των δημόσιων αρχών στο πλαίσιο της εθνικής ασφάλειας και της πρόληψης σοβαρών εγκλημάτων. Ο νόμος καθορίζει τις νόμιμες διαδικασίες για την υποκλοπή επικοινωνιών, την επιτήρηση, την χρήση μυστικών πληροφοριοδοτών και τη συλλογή δεδομένων επικοινωνίας, θέτοντας παράλληλα περιορισμούς, άρθρα 5, 6 15 και 23, και μηχανισμούς εποπτείας, άρθρα 55, 57, 58 και 59, για την προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής των πολιτών. Η έκδοση ενταλμάτων παρακολούθησης επιτρέπεται μόνο κατόπιν αίτησης στις εξουσιοδοτημένες αρχές, με αυστηρές προϋποθέσεις αναγκαιότητας, αναλογικότητας και σκοπού, ενώ οι πράξεις αυτές υπόκεινται σε ανεξάρτητο έλεγχο από αρμόδιο Επίτροπο και δικαστικά όργανα. Επιπλέον, ο νόμος προβλέπει ότι άτομα που πραγματοποιούν παρακολουθήσεις χωρίς νόμιμη εξουσιοδότηση διαπράττουν ποινικό αδίκημα και υπόκεινται σε ποινικές κυρώσεις όπως αυτές ορίζονται μεταξύ άλλων και στο άρθρο 1.

Ο Νόμος Investigatory Powers Act 2016[162] αποτελεί ένα εκτενές και σύγχρονο νομοθέτημα του ΗΒ, το οποίο εκσυγχρονίζει παλαιότερες διατάξεις που αφορούν την κρατική παρακολούθηση, όπως λόγου χάριν τις διατάξεις του RIPA 2000 (ανωτέρω). Σε ένα γενικό πλαίσιο ο νόμος καθορίζει τις προϋποθέσεις και την νομική βάση για την υποκλοπή επικοινωνιών, τη συλλογή δεδομένων επικοινωνίας, την παρείσδυση σε συσκευές καθώς και την επεξεργασία μαζικών δεδομένων από τις μυστικές υπηρεσίες. Σημαντική εισαγωγή από αυτό το νομοθέτημα αποτελεί το νέο μέτρο προστασίας από αυθαίρετες ή/και παράνομες παρακολουθήσεις με τον συνδυασμό έγκρισης από κυβερνητικό υπουργό και από ανεξάρτητο δικαστή για την έκδοση ενταλμάτων. Περαιτέρω, προβλέπει αυστηρούς

[159] Ibid s 8.
[160] Ibid s 9.
[161] Ibid ss 55, 57- 59.
[162] Investigatory Powers Act 2016 (UK) c 25.

μηχανισμούς εποπτείας και ποινικές κυρώσεις για παράνομη χρήση ή αποκάλυψη των εξουσιών αυτών. Ιδιαίτερη έμφαση δίδεται στην προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, με λεπτομερείς διατάξεις για διαφάνεια και λογοδοσία.

Ιδιαίτερα σημαντικό και σχετικό είναι το Μέρος 6 του Νόμου με τίτλο «Bulk Warrants» το οποίο ρυθμίζει και καλύπτει όλες τις εξουσίες που σχετίζονται με την μαζική συλλογή πληροφοριών από τις υπηρεσίες πληροφοριών του ΗΒ. Το άρθρο 136[163] του νόμου καθορίζει τα εντάλματα μαζικής υποκλοπής, δηλαδή, τη συλλογή μεγάλου όγκου επικοινωνιών. Καθορίζει επίσης ότι τέτοιο ένταλμα μπορεί να εκδοθεί μόνο υπό προϋποθέσεις, πρώτο την υποκλοπή επικοινωνιών που σχετίζονται με το εξωτερικό και την απόκτηση δευτερογενών δεδομένων από τις εν λόγω επικοινωνίες, και δεύτερο εξουσιοδοτεί και απαιτεί από το πρόσωπο στο οποίο απευθύνεται να διασφαλίσει μέσω οποιασδήποτε ενέργειας περιγράφεται στο ένταλμα, την υποκλοπή κατά τη διάρκεια της μετάδοσης τους μέσω τηλεπικοινωνιακού συστήματος επικοινωνιών, την απόκτηση δευτερογενών δεδομένων από επικοινωνίες που μεταδίδονται μέσω του εν λόγω συστήματος και άλλα. Επιπλέον, στην παράγραφο (5) του εν λόγω άρθρου γίνεται αναφορά σε επιπρόσθετες εξουσίες που κατέχει το άτομο το οποίο εκτελεί το ένταλμα δίδοντας του την εξουσία να υποκλέπτει επικοινωνίες οι οποίες δεν αναφέρονται στο ένταλμα. Σύμφωνα με τον νόμο, τα εντάλματα για μαζικές παρακολουθήσεις πρέπει να τηρούν συγκεκριμένες προϋποθέσεις, σχετικό είναι το άρθρο 142[164]. Ορισμένες από τις προϋποθέσεις που καθορίζονται από το άρθρο είναι αρχικά ότι το ένταλμα πρέπει συγκεκριμένα να αναφέρει ότι είναι ένταλμα μαζικής υποκλοπής, πρέπει να απευθύνεται προς τον υπεύθυνο της υπηρεσίας πληροφοριών εκ μέρους του οποίου το ένταλμα εκδόθηκε, πρέπει επίσης να προσδιορίζει τους επιχειρησιακούς σκοπούς για τους οποίους οποιοδήποτε υποκλαπέν περιεχόμενο ή δευτερογενή δεδομένα που αποκτώνται δυνάμει του εντάλματος επιτρέπεται να επιλέγονται προς εξέταση και άλλα. Μεταξύ άλλων, ο νόμος καθορίζει τη διάρκεια των ενταλμάτων (άρθρο 143), την ανανέωση τους (άρθρο 144), οποιεσδήποτε τροποποιήσεις σε αυτά (άρθρο 145), οποιεσδήποτε σημαντικές και ουσιώδεις τροποποιήσεις (άρθρα 146 και 147), την ακύρωση των ενταλμάτων (άρθρο 148), την εκτέλεση των ενταλμάτων (άρθρο 149), παρέχει ασφαλιστικές δικλείδες όσο αφορά τη διατήρηση και γνωστοποίηση υλικού (άρθρο 150), και επίσης παρέχει εγγυήσεις σχετικά με την εξέταση του υλικού (άρθρο 152).

Επιπρόσθετα, ο νόμος καθορίζει αδικήματα τα οποία δυνατό να διαπραχθούν, ήτοι, άρθρο 155 αδίκημα παραβίασης των εγγυήσεων που σχετίζονται με την εξέταση του υλικού, το άρθρο 174 καθορίζει το αδίκημα μη εξουσιοδοτημένης γνωστοποίησης, και το άρθρο 11 το οποίο καθορίζει το αδίκημα για την παράνομη απόκτηση δεδομένων επικοινωνιών.

Οι νομοθετικές διατάξεις του ΗΒ, αν και παρουσιάζονται αναλυτικότερες από εκείνες των ΗΠΑ, εγείρουν παρόμοιες ανησυχίες ως προς το δικαίωμα της ιδιωτικότητας. Η μαζική παρακολούθηση επικοινωνιών από την GCHQ, όπως αποκαλύφθηκε στις υποθέσεις *Liberty v GCHQ* και *Big Brother Watch*, προκάλεσε τον προβληματισμό του ΕΔΔΑ, το οποίο έκρινε ότι υπήρξε παραβίαση του άρθρου 8 της ΕΣΔΑ. Παρά το θεσμικό πλαίσιο του Investigatory Powers Act 2016, η έλλειψη προηγούμενης ανεξάρτητης δικαστικής εποπτείας και η δυνατότητα έκδοσης ενταλμάτων μαζικής υποκλοπής καθιστούν ασαφή τα όρια της προστασίας της ιδιωτικής ζωής. Η ύπαρξη μηχανισμών εποπτείας όπως η Intelligence and

[163] Ibid s 136.
[164] Ibid s 142.

Security Committee δεν επαρκεί για την πλήρη εξισορρόπηση μεταξύ κρατικής ισχύος και θεμελιωδών δικαιωμάτων. Για την ουσιαστική προστασία της ιδιωτικότητας απαιτείται ενίσχυση της διαφάνειας, περιορισμός των εντολών γενικής ισχύος και πρόβλεψη ατομικής προσφυγής ή ειδοποίησης του θιγόμενου όταν παρέλθει το κρίσιμο διάστημα.

Εν κατακλείδι, το νομοθετικό πλαίσιο του ΗΒ για τις μυστικές υπηρεσίες και τις παρακολουθήσεις αντικατοπτρίζει την προσπάθεια του κράτους να εξισορροπήσει την ανάγκη προστασίας της εθνικής ασφάλειας με την κατοχύρωση θεμελιωδών δικαιωμάτων. Μέσα από μια σειρά διατάξεων, οι οποίες θεμελιώνουν τη λειτουργία των υπηρεσιών πληροφοριών, ρυθμίζουν τη συλλογή και χρήση δεδομένων και προβλέπουν ποινικές κυρώσεις για καταχρηστικές πρακτικές, διαμορφώνεται ένα σύστημα που τελεί υπό δημοκρατική εποπτεία και επιδιώκει να ανταποκρίνεται στις προκλήσεις της εποχής. Η διαρκής προσαρμογή της νομοθεσίας στις τεχνολογικές εξελίξεις και στις διεθνείς απαιτήσεις αναδεικνύει τη σημασία του κράτους δικαίου ακόμη και στο πεδίο της κρατικής ασφάλειας και της μυστικότητας.

6.3. Δικαστικές αποφάσεις

Οι δικαστικές αποφάσεις στο ΗΒ σχετικά με τις μαζικές παρακολουθήσεις και την προστασία των ατομικών δικαιωμάτων αποτελούν βασικό πυλώνα στη διαμόρφωση του νομικού πλαισίου που διέπει τη δράση των κρατικών υπηρεσιών ασφαλείας. Τα δικαστήρια καλούνται να σταθμίσουν σύνθετα ζητήματα που ανακύπτουν από τη χρήση σύγχρονων τεχνολογιών επιτήρησης και να ερμηνεύσουν τη συμβατότητα των σχετικών πρακτικών με τις αρχές του κράτους δικαίου και τις διεθνείς υποχρεώσεις του ΗΒ στον τομέα των ανθρωπίνων δικαιωμάτων. Μέσα από τις αποφάσεις τους, αναδεικνύουν τα όρια της κρατικής εξουσίας, ενισχύουν τη λογοδοσία και συμβάλλουν στη διασφάλιση μιας ισορροπημένης προσέγγισης ανάμεσα στην ασφάλεια και την ελευθερία, ιδιαίτερα στο πλαίσιο των ταχέως μεταβαλλόμενων ψηφιακών συνθηκών.

Η υπόθεση *Big Brother Watch and Others v. The United Kingdom*[165] ενώπιον του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) αφορούσε τη νομιμότητα των μαζικών παρακολουθήσεων που πραγματοποιούσαν οι βρετανικές υπηρεσίες πληροφοριών όπως αποκαλύφθηκε μετά τις διαρροές του Edward Snowden. Οι προσφεύγοντες, μεταξύ των οποίων και δημοσιογράφοι, μη κυβερνητικές οργανώσεις και ακτιβιστές, ισχυρίστηκαν ότι τα μέτρα παρακολούθησης παραβίαζαν το άρθρο 8 (σεβασμός της ιδιωτικής ζωής) και το άρθρο 10 (ελευθερία έκφρασης) της ΕΣΔΑ καθότι οι υπηρεσίες του ΗΒ είχαν λάβει παράνομα πληροφορίες από παροχείς τηλεφωνικών υπηρεσιών όπως επίσης και από ξένες υπηρεσίες πληροφοριών[166]. Συγκεκριμένα, το δικαστήριο εξέτασε τρεις διαφορετικούς μηχανισμούς, την ευρεία υποκλοπή επικοινωνιών, την απόκτηση μεταδεδομένων από παρόχους υπηρεσιών και την ανταλλαγή πληροφοριών με ξένες υπηρεσίες πληροφοριών.

Το ΕΔΔΑ διαπίστωσε ότι οι πρακτικές των βρετανικών μυστικών υπηρεσιών παραβίαζαν θεμελιώδη δικαιώματα. Το νομικό πλαίσιο που διέπει τη μαζική υποκλοπή κρίθηκε ελλιπές,

[165] *Big Brother Watch and Others v United Kingdom* (2021) App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).
[166] Lorna Woods, Anna George and Maria Smyth, 'Big Brother Watch and Others v the United Kingdom: Mass Surveillance and the Right to Privacy' (2019) 20 Human Rights Law Review 1.

αφού δεν προέβλεπε επαρκή εγγυητικά μέτρα, όπως ανεξάρτητη και προηγούμενη δικαστική εποπτεία ή σαφή κριτήρια για την επιλογή των επικοινωνιών που θα παρακολουθούνταν. Έτσι, το δικαστήριο έκρινε ότι υπήρξε παραβίαση του άρθρου 8 ΕΣΔΑ. Επιπλέον, όσο αφορά την στοχοποίηση δημοσιογράφων, κρίθηκε ότι παραβιάστηκε και το άρθρο 10, αφού δεν υπήρχε ειδική προστασία των δημοσιογραφικών πηγών και της ελευθερίας της έκφρασης. Το δικαστήριο τόνισε ότι ακόμη και όταν πρόκειται για λόγους εθνικής ασφάλειας, η μαζική παρακολούθηση πρέπει να διέπεται από αυστηρούς και σαφείς κανόνες, ώστε να αποφεύγεται η αυθαιρεσία. Αν και η απόφαση δεν επέβαλε ποινικές κυρώσεις κατά προσώπων ή οργανισμών, το δικαστήριο αναγνώρισε τη θεσμική ευθύνη του κράτους και των υπηρεσιών πληροφοριών να εξασφαλίζουν πλήρη λογοδοσία και διαφάνεια στο πλαίσιο τέτοιων παρεμβάσεων.

Η απόφαση της UK Supreme Court στην υπόθεση *R (Privacy International) v Investigatory Powers Tribunal and others*[167] αποτελεί μια από τις πιο σημαντικές αποφάσεις του HB που σχετίζονται με τη λειτουργία των μυστικών υπηρεσιών, τις μαζικές παρακολουθήσεις και το ζήτημα της δικαστικής εποπτείας. Η υπόθεση αφορά τη δυνατότητα των πολιτών και οργανώσεων να αμφισβητούν ενώπιον των δικαστηρίων τις αποφάσεις του Investigatory Powers Tribunal («IPT»), του ειδικού δικαστηρίου που εξετάζει καταγγελίες για παράνομες δραστηριότητες των υπηρεσιών πληροφοριών. Το Δικαστήριο στην απόφαση του έκρινε ότι το άρθρο 67 (8) του RIPA δεν αποκλείει την εποπτεία του IPT από ανώτατα δικαστήρια. Κατέστη σαφές ότι τα δικαστήρια διατηρούν τη δικαιοδοσία τους να εξετάζουν αν το IPT υπερέβη τα όρια της δικαιοδοσίας του. Αυτή η προσέγγιση του δικαστηρίου ενισχύει με σημαντικό τρόπο την λογοδοσία των μυστικών υπηρεσιών και παράλληλα ενισχύει την προστασία της ιδιωτικότητας και των ανθρωπίνων δικαιωμάτων. Επιπρόσθετα, η υπόθεση αυτή ενισχύει την ιδέα ότι καμία υπηρεσία ασφαλείας δεν είναι υπεράνω του νόμου, ακόμη και όταν λειτουργεί υπό το καθεστώς απορρήτου. Περαιτέρω, τονίζεται ο ρόλος των δικαστηρίων στη διασφάλιση της νομιμότητας και των πρακτικών των υπηρεσιών ασφαλείας, ιδιαίτερα σε περιπτώσεις που αφορούν παραβιάσεις της ιδιωτικής ζωής μέσω μαζικών παρακολουθήσεων. Καταληκτικά, η εν λόγω υπόθεση έχει θεμελιώδη σημασία για την προστασία των ανθρωπίνων δικαιωμάτων έναντι των μυστικών υπηρεσιών. Αναδεικνύει ότι η δικαστική ανεξαρτησία και ο έλεγχος της εκτελεστικής εξουσίας παραμένουν ακρογωνιαίοι λίθοι του κράτους δικαίου, ακόμη και στο πεδίο πληροφοριών και της εθνικής ασφάλειας.

Η υπόθεση *Liberty v GCHQ*[168] ενώπιον του IPT αφορά προσφυγές διαφόρων οργανώσεων ανθρωπίνων δικαιωμάτων κατά των υπηρεσιών πληροφοριών του HB, σχετικά με παραβιάσεις του δικαιώματος στην ιδιωτικότητα όπως αυτό κατοχυρώνεται στο άρθρο 8 της ΕΣΔΑ. Η υπόθεση εστίασε στη μαζική παρακολούθηση ηλεκτρονικών επικοινωνιών με τη συνεργασία των Βρετανικών υπηρεσιών πληροφοριών με τις ΗΠΑ μέσω των προγραμμάτων επιτήρησης Prism και Upstream. Στην υπό κρίση υπόθεση η GCHQ υπερέβη τα χρονικά όρια διατήρησης των δεδομένων, κάτι για το οποίο υπήρχαν ρητές πρόνοιες από τις εσωτερικές πολιτικές της, παραβίαση που τελικά αποφασίστηκε ότι αποτελούσε παραβίαση του άρθρου 8 της ΕΣΔΑ. Περαιτέρω, η διαδικασία που ακολουθήθηκε για την εξέταση των υποκλαπεισών επικοινωνιών δεν ακολουθήθηκε σωστά, κάτι το οποίο αποτελούσε ξανά παραβίαση του άρθρου 8 της ΕΣΔΑ. Αφενός το δικαστήριο δεν επέβαλε τις οποιεσδήποτε κυρώσεις, διέταξε ωστόσο τη διαγραφή των δεδομένων και τη λήψη διορθωτικών μέτρων καθώς και την

[167] *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22, [2020] AC 491.
[168] *Liberty and Others v GCHQ and Others* [2015] UKIPTrib 13_77-H_2.

υποβολή σχετικής αναφοράς προς τον Πρωθυπουργό όπως αναφέρεται στο νόμο. Η εν λόγω απόφαση είναι ιδιαίτερα σημαντική καθότι αναδεικνύει την κρίσιμη ανάγκη ύπαρξης διαφανών και αυστηρών διαδικασιών για τις μαζικές παρακολουθήσεις από τις υπηρεσίες πληροφοριών, την ευθύνη των υπηρεσιών ακόμη και για τεχνικές παραβιάσεις όταν αυτές αφορούν θεμελιώδη δικαιώματα όπως το δικαίωμα στην ιδιωτική ζωή, και την δυσκολία απόδοσης ποινικής ευθύνης σε πράκτορες ή φορείς, καθώς στην προκειμένη περίπτωση οι παραβιάσεις αντιμετωπίστηκαν ως διοικητικές και όχι ως ποινικές.

Ολοκληρώνοντας την ανάλυση των δικαστικών αποφάσεων του Ηνωμένου Βασιλείου σχετικά με τις μαζικές παρακολουθήσεις και την προστασία της ιδιωτικότητας, καθίσταται σαφές ότι η νομολογία διαδραματίζει έναν κρίσιμο ρόλο στον έλεγχο των κρατικών πρακτικών επιτήρησης και στη διαφύλαξη των θεμελιωδών δικαιωμάτων των πολιτών. Μέσα από αποφάσεις όπως *Big Brother Watch, Privacy International* και *Liberty v. GCHQ*, τα εθνικά και διεθνή δικαστήρια ανέδειξαν επανειλημμένα τις σοβαρές προκλήσεις που ανακύπτουν από την αδιαφανή δράση των μυστικών υπηρεσιών, επισημαίνοντας νομικά κενά, την έλλειψη επαρκών εγγυήσεων και την ανάγκη για αυστηρότερη λογοδοσία. Οι αποφάσεις αυτές υπογραμμίζουν τη σημασία ύπαρξης ενός επαρκούς και σαφώς καθορισμένου νομικού πλαισίου που να διασφαλίζει την προηγούμενη και ανεξάρτητη δικαστική εποπτεία, την προστασία των δημοσιογραφικών πηγών, καθώς και τη διαφάνεια των διαδικασιών συλλογής και επεξεργασίας πληροφοριών. Ταυτόχρονα, η νομολογία αναδεικνύει τον θεσμικό ρόλο των δικαστηρίων ως ελεγκτών της εκτελεστικής εξουσίας, ακόμη και όταν αυτή επικαλείται λόγους εθνικής ασφάλειας. Ενώ δεν αναγνωρίζεται συστηματικά ποινική ευθύνη σε μεμονωμένους πράκτορες ή υπηρεσίες, καταγράφεται σαφώς η θεσμική ευθύνη του κράτους και η υποχρέωση συμμόρφωσης με τις αρχές του κράτους δικαίου και της ΕΣΔΑ. Ουσιαστικά, το σύνολο της νομολογίας συνθέτει ένα προοδευτικό νομικό αφήγημα, το οποίο θέτει τα θεμέλια για μελλοντικές θεσμικές βελτιώσεις, ενισχύει το αίτημα για λογοδοσία και επιβεβαιώνει ότι ακόμη και σε ζητήματα εθνικής ασφάλειας, τα ανθρώπινα δικαιώματα δεν μπορούν να τεθούν σε δεύτερη μοίρα.

7. Συγκριτική ανάλυση ΗΠΑ - ΗΒ

7.1. Ομοιότητες

Η συγκριτική θεώρηση των νομικών συστημάτων των ΗΠΑ και του ΗΒ αποκαλύπτει σημαντικές ομοιότητες ως προς την αντιμετώπιση των ζητημάτων που σχετίζονται με τις μαζικές παρακολουθήσεις και την προστασία της ιδιωτικότητας. Και στα δύο κράτη, το νομικό πλαίσιο διαμορφώνεται από την ανάγκη να αντιμετωπιστούν σύγχρονες απειλές ασφαλείας, με τρόπο που να συνάδει με τις θεμελιώδεις αρχές του κράτους δικαίου. Επιπλέον, τόσο οι ΗΠΑ όσο και το ΗΒ στηρίζονται σε ισχυρά δικαστικά σώματα, τα οποία επιτελούν κρίσιμο ρόλο στον έλεγχο της συνταγματικότητας και της νομιμότητας των κυβερνητικών πρακτικών επιτήρησης. Παρά τις επιμέρους διαφορές σε επίπεδο δομής και νομοθετικής προσέγγισης, και οι δύο έννομες τάξεις υιοθετούν παρόμοιους προβληματισμούς και επιδιώκουν μια ισορροπημένη σύνθεση μεταξύ ασφάλειας και προστασίας των ατομικών δικαιωμάτων.

Τόσο στο ΗΒ όσο και στις ΗΠΑ, οι υπηρεσίες πληροφοριών κατέχουν κεντρικό ρόλο στη διασφάλιση της εθνικής ασφάλειας, ιδιαίτερα μετά τα γεγονότα της 11ης Σεπτεμβρίου. Και

στις δύο έννομες τάξεις, παρατηρείται συστηματική χρήση τεχνολογικά εξελιγμένων μεθόδων μαζικής επιτήρησης, μέσω των οποίων συλλέγονται τεράστιοι όγκοι πληροφοριών με σκοπό την πρόληψη τρομοκρατικών ενεργειών και άλλων απειλών. Στις ΗΠΑ, χαρακτηριστικό παράδειγμα αποτελεί η δράση της Εθνικής Υπηρεσίας Ασφαλείας (NSA) μέσω του προγράμματος PRISM, το οποίο αποκαλύφθηκε δημόσια μετά τις διαρροές του Edward Snowden (ανωτέρω). Αντίστοιχα, στο ΗΒ, η GCHQ αποτελεί τον βασικό οργανισμό ηλεκτρονικής επιτήρησης, αρμόδιο για την κυβερνοασφάλεια και την παρακολούθηση επικοινωνιών με ανάλογη προσέγγιση στον τομέα της συλλογής πληροφοριών.

Μια ακόμη αξιοσημείωτη ομοιότητα αφορά τη συνεργασία μεταξύ των δύο χωρών στον τομέα των πληροφοριών. Οι υπηρεσίες πληροφοριών των ΗΠΑ και του ΗΒ έχουν ιστορικά διαμορφώσει σχέσεις ανταλλαγής δεδομένων, γεγονός που αναδείχθηκε, μεταξύ άλλων, στην υπόθεση *Liberty v GCHQ*, όπου έγινε ρητή αναφορά στη συνεργασία με την NSA μέσω των προγραμμάτων Prism και Upstream. Η διασυνοριακή αυτή συνεργασία, αν και ενισχύει την επιχειρηματική αποτελεσματικότητα, ταυτόχρονα δημιουργεί σημαντικές προκλήσεις ως προς την προστασία των θεμελιωδών δικαιωμάτων των πολιτών.

Επιπρόσθετη ομοιότητα εντοπίζεται στη δομή και λειτουργία των νομικών συστημάτων των δύο χωρών, τα οποία βασίζονται στο common law. Και στις δύο έννομες τάξεις, ο ρόλος των δικαστικών αποφάσεων είναι ιδιαίτερα σημαντικός, καθώς ερμηνεύουν και διαμορφώνουν την εφαρμογή του νόμου ειδικά σε τομείς που σχετίζονται με την εθνική ασφάλεια και την προστασία των θεμελιωδών δικαιωμάτων. Οι υποθέσεις *USA v Moalin, Big Brother Watch, Privacy International* και *Liberty v GCHQ*, όπως παρουσιάζονται στην εργασία, αποτελούν παραδείγματα της ενεργούς συμμετοχής των δικαστηρίων στον έλεγχο της δράσης των υπηρεσιών πληροφοριών, αναδεικνύοντας την κοινή θεσμική αρχή ότι ακόμη και οι μυστικές υπηρεσίες υπόκεινται σε δικαστική εποπτεία και δεν βρίσκονται υπεράνω του νόμου.

Ανάλογες ομοιότητες εντοπίζονται στο ίδιο το νομοθετικό πλαίσιο που ρυθμίζει τις αρμοδιότητες και τα όρια των υπηρεσιών πληροφοριών. Στις ΗΠΑ, η Foreign Intelligence Surveillance Act (FISA) και ο USA Patriot Act, όπως εξελίχθηκαν με την ψήφιση του USA Freedom Act, προσδιορίζουν τους όρους υπό τους οποίους επιτρέπονται οι παρακολουθήσεις, προβλέποντας διαδικασίες για την έκδοση ενταλμάτων από το ειδικό δικαστήριο FISC. Αντίστοιχα, στο ΗΒ οι νόμοι Security Service Act 1989, Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000 και Investigatory Powers Act 2016, προβλέπουν αντίστοιχες διαδικασίες για την έκδοση ενταλμάτων από αρμόδιους υπουργούς ή δικαστικά όργανα, περιλαμβάνοντας και αυστηρούς όρους αναγκαιότητας, αναλογικότητας και σκοπού. Και στις δύο χώρες παρατηρείται κοινή τάση ενίσχυσης των μηχανισμών εποπτείας, με τη δημιουργία ανεξάρτητων επιτροπών, όπως η Privacy and Civil Liberties Oversight Board στις ΗΠΑ και η Intelligence and Security Committee of Parliament στο ΗΒ, επιβεβαιώνοντας τη συγκλίνουσα κατεύθυνση των δύο κρατών προς τη θεσμική λογοδοσία, στο πλαίσιο των δημοκρατικών αρχών του κράτους δικαίου.

Η συγκριτική προσέγγιση των συστημάτων του ΗΒ και των ΗΠΑ αναδεικνύει μια κοινή φιλοσοφία ως προς την ανάγκη προστασίας της εθνικής ασφάλειας μέσα από προηγμένα τεχνολογικά μέσα παρακολούθησης, χωρίς όμως να παραβλέπετε η θεσμική υποχρέωση σεβασμού των θεμελιωδών δικαιωμάτων. Παρά τις γεωγραφικές και διοικητικές διαφορές, οι δύο χώρες επιδιώκουν τη διατήρηση μιας ισορροπίας ανάμεσα στην κρατική ασφάλεια

και την ιδιωτικότητα, μέσω θεσμικά κατοχυρωμένων εγγυήσεων. Το κοινό υπόβαθρο του common law, η θεσμοθέτηση ειδικών οργάνων εποπτείας και οι εξελίξεις στη νομολογία επιβεβαιώνουν ότι τόσο οι ΗΠΑ όσο και το ΗΒ κινούνται σε μια παράλληλη κατεύθυνση προς ένα μοντέλο κρατικής επιτήρησης που φιλοδοξεί να παραμείνει εντός των ορίων της συνταγματικής και διεθνούς νομιμότητας.

7.2. Διαφορές

Παρά τις σημαντικές ομοιότητες, το νομικό και θεσμικό πλαίσιο των ΗΠΑ και του ΗΒ παρουσιάζει και ορισμένες κρίσιμες διαφορές, τόσο ως προς την ένταση των παρεμβάσεων στην ιδιωτικότητα όσο και στον τρόπο λογοδοσίας των υπηρεσιών πληροφοριών. Μια ουσιώδης διαφορά έγκειται στο ότι το αμερικανικό σύστημα στηρίζεται σε ένα ιδιαίτερα εξειδικευμένο δικαστήριο, το FISC, το οποίο λειτουργεί με μυστικές και μονομερείς διαδικασίες, χωρίς ουσιαστική δυνατότητα αντίκρουσης εκ μέρους των πολιτών. Αντιθέτως, στο ΗΒ, μολονότι το IPT είναι εξίσου ειδική δικαιοδοσία, η απόφαση στην υπόθεση *Privacy International* κατέστησε σαφές ότι υπόκειται σε δικαστικό έλεγχο από τα ανώτατα δικαστήρια ενισχύοντας το πλέγμα δημοκρατικής λογοδοσίας.

Μια ακόμη διαφορά εντοπίζεται στο βαθμό επισημοποίησης των παραβιάσεων της κρατικής ευθύνης. Στην υπόθεση *USA v Moalin*, το εφετείο αναγνώρισε ότι η NSA ενήργησε κατά παράβαση της FISA, ωστόσο δεν επέβαλε ποινικές κυρώσεις ούτε προσδιόρισε θεσμικά ποιος φέρει ατομική ευθύνη. Από την άλλη πλευρά, στο ΗΒ, η απόφαση στην *Big Brother Watch v UK* του ΕΔΔΑ, διαπίστωσε θεσμική ευθύνη του κράτους, καθώς κρίθηκε ότι το σύνολο του νομικού πλαισίου για τις μαζικές παρακολουθήσεις στερούνταν επαρκών εγγυήσεων και προσέβαλε τα άρθρα 8 και 10 ΕΣΔΑ. Παράλληλα στην υπόθεση *Liberty v GCHQ*, έγινε αποδεκτό ότι η παραβίαση της νομοθεσίας από την υπηρεσία GCHQ, έστω και τεχνικής φύσεως, επιφέρει υποχρέωση διορθωτικών ενεργειών, χωρίς όμως να προβλέπεται ποινική ευθύνη των εμπλεκομένων. Αντίθετα, στις ΗΠΑ, η FISA και ο USA Patriot Act, περιλαμβάνουν ρητές ποινικές και αστικές κυρώσεις για μη εξουσιοδοτημένες παρακολουθήσεις, αν και σπανίως εφαρμόζονται στην πράξη.

Μια ακόμη σημαντική διαφορά εντοπίζεται στο νομοθετικό επίπεδο και τη ρυθμιστική ακρίβεια των διατάξεων που διέπουν την έκδοση και εκτέλεση ενταλμάτων παρακολούθησης. Το ΗΒ, ιδιαίτερα μετά την ψήφιση του Investigatory Powers Act 2016, έχει διαμορφώσει ένα ιδιαίτερα αναλυτικό και εκτενές νομοθετικό πλαίσιο που προβλέπει με σαφήνεια τα είδη των ενταλμάτων, τις ακριβείς προϋποθέσεις έκδοσης, τη διαδικασία ελέγχου από υπουργό και ανεξάρτητο δικαστή, και τις δικλείδες διαφάνειας και αναλογικότητας, καθώς και ποινικές κυρώσεις για μη εξουσιοδοτημένη δράση. Αντιθέτως, η αμερικανική νομοθεσία, αν και περιλαμβάνει σημαντικά νομοθετήματα όπως η FISA, και οι τροποποιήσεις της μέσω του USA Patriot Act, παρουσιάζει μικρότερη διαφάνεια και περιορισμένη δικαστική συμμετοχή ως προς την εποπτεία. Η έκδοση ενταλμάτων από την FISC, χωρίς την παρουσία αντιδίκου ή ανεξάρτητης αρχής για την υπεράσπιση των δικαιωμάτων των πολιτών, καθιστά την πρακτική λογοδοσία σημαντικά ασθενέστερη. Παράλληλα, η FISA δεν περιλαμβάνει λεπτομερές κανονιστικό πλαίσιο για την προστασία προσωπικών δεδομένων σε κάθε στάδιο της διαδικασίας όπως προβλέπεται στο IPA 2016, ενώ η έννοια των bulk powers παραμένει νομικά αμφιλεγόμενη στις ΗΠΑ σε σχέση με το ΗΒ όπου ρυθμίζεται ρητά.

Περαιτέρω, το συνταγματικό υπόβαθρο διαφέρει ουσιωδώς, εφόσον αφενός οι ΗΠΑ βασίζονται στην Τέταρτη Τροπολογία του Συντάγματος που προστατεύει από παράνομες έρευνες και κατασχέσεις, παρέχοντας άμεση συνταγματική βάση για την αμφισβήτηση μαζικών παρακολουθήσεων. Αφετέρου, το ΗΒ δεν διαθέτει γραπτό σύνταγμα και αντλεί την προστασία των θεμελιωδών δικαιωμάτων κυρίως από το Human Rights Act 1998[169] και την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ).

Μια επιπλέον και κρίσιμη διαφορά μεταξύ των δύο έννομων τάξεων αφορά τη σχετική βαρύτητα που αποδίδεται στην προστασία της ιδιωτικότητας και των θεμελιωδών δικαιωμάτων. Το ΗΒ ως μέλος του Συμβουλίου της Ευρώπης και με πλήρη ενσωμάτωση της ΕΣΔΑ μέσω του Human Rights Act οφείλει να συμμορφώνεται με τις αποφάσεις του ΕΔΔΑ. Η συμμόρφωση αυτή ασκεί ισχυρή πίεση στο κράτος να διασφαλίζει υψηλό επίπεδο θεσμικής λογοδοσίας και σεβασμού των δικαιωμάτων, ακόμη και όταν πρόκειται για λόγους εθνικής ασφάλειας. Αντίθετα, στις ΗΠΑ, όπου το νομικό πλαίσιο αντλεί κυρίως έρεισμα από τη συνταγματική Τέταρτη Τροπολογία και από εξειδικευμένες νομοθεσίες, η προστασία της ιδιωτικότητας φαίνεται συχνά να υποχωρεί έναντι των προτεραιοτήτων της εθνικής ασφάλειας, ενώ η δικαστική εποπτεία εφαρμόζεται πιο περιορισμένα, κυρίως μέσω μυστικών διαδικασιών του FISA Court.

Τέλος, αξιοσημείωτη διαφορά παρατηρείται στον τρόπο προσέγγισης της διαφάνειας και της δημοσιοποίησης των πληροφοριών. Το ΗΒ φαίνεται να επιδεικνύει μεγαλύτερη πρόθεση δημοσιοποίησης των αποφάσεων των αρμόδιων οργάνων και επιτροπών εποπτείας, γεγονός που επιβεβαιώνεται τόσο από την ISC όσο και από την νομοθετική απαίτηση υποβολής ετήσιων εκθέσεων. Αντιθέτως, στις ΗΠΑ, πολλές από τις κρίσιμες πληροφορίες παραμένουν ταξινομημένες, και σημαντικές αποκαλύψεις προέρχονται κυρίως από διαρροές, όπως αυτή του Edward Snowden που αποκάλυψε τα προγράμματα Prism και Upstream.

Συνοψίζοντας, οι διαφορές ανάμεσα στις ΗΠΑ και το ΗΒ σε ό,τι αφορά τις μαζικές παρακολουθήσεις και την προστασία της ιδιωτικότητας εντοπίζονται όχι μόνο στο θεσμικό και νομοθετικό επίπεδο, αλλά και στον τρόπο αντίληψης και εφαρμογής των δημοκρατικών εγγυήσεων. Το ΗΒ εμφανίζεται πιο δεσμευμένο σε ένα πολυεπίπεδο σύστημα προστασίας με έντονη παρουσία κοινοβουλευτικής εποπτείας και νομολογιακού ελέγχου, κυρίως λόγω της ενσωμάτωσης της ΕΣΔΑ. Αντίθετα το αμερικανικό σύστημα στηρίζεται σε ένα πιο εσωστρεφές μοντέλο στο οποίο η προστασία των δικαιωμάτων των πολιτών υποχωρεί έναντι των αναγκών εθνικής ασφάλειας ιδίως όταν απουσιάζει η δυνατότητα ουσιαστικής συμμετοχής ή αμφισβήτησης των πολιτών στις διαδικασίες παρακολούθησης. Οι εν λόγω διαφοροποιήσεις αναδεικνύουν τις εναλλακτικές προσεγγίσεις που μπορούν να υιοθετήσουν τα δημοκρατικά κράτη για την επίτευξη ισορροπίας μεταξύ ασφάλειας και ελευθερίας, προσφέροντας πολύτιμα διδάγματα για τον επαναπροσδιορισμό της προστασίας της ιδιωτικότητας στο σύγχρονο ψηφιακό περιβάλλον.

8. Προτάσεις βελτίωσης στην Ελλάδα

[169] Human Rights Act 1998 (UK) c 42.

8.1. Κενά και προκλήσεις στο Ελληνικό νομικό σύστημα

Στην Ελλάδα, η νομοθετική προσέγγιση στο ζήτημα της παρακολούθησης και της δράσης των υπηρεσιών πληροφοριών παραμένει κατακερματισμένη και λιγότερο ανεπτυγμένη συγκριτικά με άλλα ευρωπαϊκά ή διεθνή πρότυπα, όπως αυτά του ΗΒ και των ΗΠΑ. Παρότι το Σύνταγμα (άρθρο 19 παρ. 1)[170] αναγνωρίζει το απόρρητο των επικοινωνιών ως απαραβίαστο, επιτρέπει την κατ' εξαίρεση άρση του αποκλειστικά για λόγους εθνικής ασφάλειας ή για τη διακρίβωση σοβαρών εγκλημάτων, βάσει του νόμου και με δικαστική συνδρομή.

Στην Ελλάδα, η βασική υπηρεσία πληροφοριών είναι η Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ), η οποία θεσμοθετήθηκε με τον Νόμο 3649/2008[171]. Η ΕΥΠ υπαγόταν διοικητικά στον Υπουργό Εσωτερικών, ενώ με την ψήφιση του Νόμου 4622/2019[172] και πιο συγκεκριμένα το άρθρο 21 (4), πλέον υπάγεται στην Προεδρία της Κυβέρνησης και αποτελεί το κύριο όργανο συλλογής και ανάλυσης πληροφοριών για την πρόληψη και αντιμετώπιση απειλών κατά τις εθνικής ασφάλειας με την άσκηση των σχετικών αρμοδιοτήτων να διέπεται από νομοθετικά προβλεπόμενες εγγυήσεις. Ωστόσο, μέχρι σήμερα δεν υφίσταται ειδικό νομοθετικό πλαίσιο που να προβλέπει ρητά τη δυνατότητα ή τα όρια των μαζικών παρακολουθήσεων, ενώ σημαντικά ζητήματα ανακύπτουν και από την απουσία πλήρους δικαστικής εποπτείας και ενημέρωσης του θιγόμενου πολίτη. Το σκάνδαλο των υποκλοπών μέσω του λογισμικού Predator το 2022, ανέδειξε με έντονο τρόπο τα θεσμικά και νομικά κενά, φέρνοντας στο προσκήνιο την ανάγκη για ενίσχυση της διαφάνειας, της λογοδοσίας και της προστασίας θεμελιωδών δικαιωμάτων στο πλαίσιο της εθνικής ασφάλειας.

Η ΕΥΠ έχει τη δυνατότητα να αιτείται την άρση του απορρήτου επικοινωνιών, κατόπιν εισαγγελικής έγκρισης για λόγους εθνικής ασφάλειας. Η διαδικασία αυτή, αν και προβλέπεται στο υφιστάμενο νομικό πλαίσιο, στερείται επαρκούς δικαστικής εποπτείας και διαφάνειας, γεγονός που έχει προκαλέσει έντονο προβληματισμό στη νομική θεωρία και την κοινή γνώμη, ιδιαίτερα μετά τα πρόσφατα περιστατικά παρακολουθήσεων δημοσίων προσώπων. Παρότι η ΕΥΠ αποτελεί τη μοναδική θεσμοθετημένη υπηρεσία πληροφοριών στην Ελλάδα, το υπάρχον θεσμικό πλαίσιο δεν παρέχει εξειδικευμένες προβλέψεις για πιο σύνθετες μορφές επιτήρησης, όπως η μαζική ή προληπτική παρακολούθηση, ενώ η λογοδοσία και η ανεξάρτητη εποπτεία παραμένουν ανεπαρκώς διασφαλισμένες.

Ο Νόμος υπ' αριθμ. 5002/2022[173] αποτέλεσε την πρώτη συστηματική νομοθετική απάντηση της ελληνικής Πολιτείας στις ανησυχίες που προέκυψαν μετά το σκάνδαλο των παρακολουθήσεων με κακόβουλο λογισμικό, όπως το Predator. Κυριότεροι σκοποί του ως άνω νόμου σύμφωνα με τις πρόνοιες του άρθρου 1 είναι η θωράκιση και ο εκσυγχρονισμός της διαδικασίας άρσης του απορρήτου των επικοινωνιών σύμφωνα με το Σύνταγμα, η βελτίωση της δράσης της ΕΥΠ, η προστασία του απορρήτου των επικοινωνιών από διάφορα λογισμικά παρακολούθησης, η αναβάθμιση του επιπέδου κυβερνοασφάλειας στην Ελλάδα και η πιο αποτελεσματική προστασία των φυσικών προσώπων έναντι της επεξεργασίας

[170] Σύνταγμα της Ελλάδας, αρ. 19 § 1.
[171] Νόμος 3649/2008 «Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις» (ΦΕΚ Α 39, 3 Μαρτίου 2008).
[172] Νόμος 4622/2019 «Επιτελικό Κράτος: οργάνωση, λειτουργία και διαφάνεια της Κυβέρνησης, των κυβερνητικών οργάνων και της κεντρικής δημόσιας διοίκησης» (ΦΕΚ Α 133/7.8.2019).
[173] Νόμος 5002/2022 (Α' 228/09.12.2022) «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών».

δεδομένων προσωπικού χαρακτήρα. Περαιτέρω, ο Νόμος τροποποίησε βασικές διατάξεις του Ν. 2225/1994[174] και του Ν. 3649/2008 και εισήγαγε αυστηρότερο πλαίσιο για την άρση του απορρήτου των επικοινωνιών, ιδίως όταν αυτή σχετίζεται με λόγους εθνικής ασφάλειας. Μεταξύ άλλων, καθιερώθηκε η υποχρέωση διπλής θεσμικής έγκρισης για διενέργεια παρακολούθησης, τόσο από τον εισαγγελέα Εφετών όσο και από ειδική τριμελή επιτροπή[175].

Εισήχθη επίσης πρόβλεψη δια της οποίας δίδεται η δυνατότητα στο θιγόμενο πρόσωπο να λάβει γνώση για την επιβολή του περιοριστικού μέτρου, μετά πάροδο τριών ετών από την παύση της ισχύος της διάταξης άρσης, και εφόσον δεν διακυβεύεται ο σκοπός για τον οποίο αυτή διατάχθηκε[176]. Επιπρόσθετα, ολόκληρο το νομοθέτημα κάνει λόγο για σημαντικές πτυχές της διαχείρισης υλικού σε άρσεις για λόγους εθνικής ασφάλειας (άρθρο 5), περιπτώσεις κατά τις οποίες είναι επιτρεπτή η άρση του απορρήτου (άρθρο 6), τη διαδικασία άρσης απορρήτου (άρθρο 8), καθορίζει το αδίκημα για παραβίαση του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας προβλέποντας ποινή φυλάκισης μέχρι και 10 έτη κάτι το οποίο δείχνει τη σοβαρότητα της παραβίασης (άρθρο 10), και γενικότερα αποτελεί ένα πλήρες νομοθέτημα το οποίο αναφέρεται με σαφήνεια σε όλα τα σχετιζόμενα ζητήματα προσφέροντας με αυτό τον τρόπο νομοθετική προστασία στους πολίτες και στο δικαίωμα τους στην ιδιωτικότητα.

Εξαιρετικά σημαντική για τον Ελληνικό νομικό διάλογο είναι η υπόθεση *Athanasios Koukakis v. Greece*[177]. Ο προσφεύγον, Θανάσης Κουκάκης, είναι Έλληνας δημοσιογράφος που εργάζεται σε οικονομικά ρεπορτάζ. Η προσφυγή του αφορά την παρακολούθηση των τηλεπικοινωνιών του τόσο μέσω κρατικής άρσης του απορρήτου για λόγους εθνικής ασφάλειας όσο και μέσω κακόβουλου λογισμικού. Ο προσφεύγον υποστήριξε ότι οι ελληνικές αρχές παραβίασαν το άρθρο 8 της ΕΣΔΑ το οποίο κατοχυρώνει το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής λόγω του τρόπου με τον οποίο εφαρμόστηκε το εθνικό νομικό πλαίσιο και της αδυναμίας του να προσβάλει δικαστικά τη διαδικασία παρακολούθησης. Η αποδοχή της προσφυγής του προσφεύγον από το ΕΔΔΑ, καθώς και η απόφαση του Δικαστηρίου να αποστείλει πρόταση φιλικού διακανονισμού τόσο στον προσφεύγοντα όσο και την Ελληνική κυβέρνηση, συνιστούν ενδείξεις πως το Δικαστήριο διέκρινε σοβαρά ζητήματα ως προς τη συμμόρφωση της ελληνικής έννομης τάξης με τις επιταγές της ΕΣΔΑ. Το γεγονός ότι η υπόθεση κρίθηκε παραδεκτή και προωθήθηκε σε ουσιαστική εξέταση υποδηλώνει ότι το ΕΔΔΑ ενδέχεται να διαπίστωσε εκ πρώτης όψεως παραβίαση του άρθρου 8 της Σύμβασης, δηλαδή του δικαιώματος στον σεβασμό της ιδιωτικής ζωής και της επικοινωνίας. Παρόλο που η υπόθεση απορρίφθηκε από το ΕΔΔΑ λόγω της φερόμενης αποκάλυψης πληροφοριών από τον ίδιο τον προσφεύγοντα, γεγονός που, σύμφωνα με το Δικαστήριο παραβίασε τις αρχές της εμπιστευτικότητας της διαδικασίας διακανονισμού, το ουσιαστικό ζήτημα της υπόθεσης παραμένει ανοιχτό. Η απόφαση του Δικαστηρίου να διακόψει την εξέταση της υπόθεσης βασίστηκε σε διαδικαστικό λόγο και όχι σε ουσιαστική αξιολόγηση της καταγγελίας περί παραβίασης του άρθρου 8 ΕΣΔΑ. Κατά συνέπεια, δεν είναι δυνατό να εξαχθεί ασφαλές συμπέρασμα ως προς το ποια θα ήταν η ουσία της κρίσης του Δικαστηρίου επί των θεμάτων που εγείρονται, εάν η υπόθεση είχε

[174] Νόμος 2225/1994, «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α 121, 20 Ιουλίου 1994).
[175] Νόμος 5002/2022 (Α' 228/09.12.2022) «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών», άρθρο 4 (2)
[176] Ibid s 4 (7)
[177] *Athanasios Koukakis v Greece*, App no 37659/22 (ECtHR, 11 June 2024).

εξεταστεί πλήρως. Η παραδοχή της προσφυγής και η έναρξη διαδικασίας φιλικού διακανονισμού, κατέδειξαν ότι το Δικαστήριο θεώρησε ότι υπήρχε τουλάχιστον σε πρώτο στάδιο, βάση για ενδεχόμενη παραβίαση των δικαιωμάτων του προσφεύγοντος. Συνεπώς, αν και η υπόθεση δεν κατέληξε σε απόφαση επί της ουσίας, παραμένει μεταίωρο το ζήτημα του κατά πόσον η ελληνική έννομη τάξη παρείχε επαρκείς εγγυήσεις προστασίας της ιδιωτικότητας, γεγονός που υπογραμμίζει τη σημασία της υπόθεσης ως προς την ανάδειξη των συστημικών προβλημάτων του υφιστάμενου θεσμικού πλαισίου.

Πολύ σημαντικό για σκοπούς της παρούσας μελέτης αποτελεί το γεγονός ότι η ΕΣΔΑ κυρώθηκε από την Ελλάδα στις 28 Μαρτίου 1953 και τέθηκε σε ισχύ για τη χώρα στις 3 Σεπτεμβρίου του ίδιου έτους. Η κύρωση της ΕΣΔΑ αποτέλεσε ένα κρίσιμο βήμα για την ενσωμάτωση των ευρωπαϊκών προτύπων προστασίας των θεμελιωδών δικαιωμάτων στο ελληνικό νομικό σύστημα. Με την κύρωση αυτή, η Ελλάδα ανέλαβε τη διεθνή υποχρέωση να προστατεύει τα κατοχυρωμένα από τη Σύμβαση δικαιώματα και ελευθερίες, διασφαλίζοντας αυξημένο επίπεδο προστασίας για τους πολίτες έναντι αυθαίρετων κρατικών παρεμβάσεων. Οι διατάξεις της ΕΣΔΑ, και ιδίως το άρθρο 8 περί σεβασμού ιδιωτικής και οικογενειακής ζωής έχουν αποκτήσει υπερνομοθετική ισχύ και δεσμεύουν τόσο τη νομοθετική όσο και την εκτελεστική εξουσία, λειτουργώντας ως αναγκαίο όριο στη λήψη και εφαρμογή μέτρων επιτήρησης και παρακολούθησης.

Η ελληνική έννομη τάξη, παρά την αναγνώριση της σημασίας της εθνικής ασφάλειας και την ύπαρξη θεσμοθετημένων υπηρεσιών πληροφοριών, εξακολουθεί να παρουσιάζει σοβαρά κενά και προκλήσεις όσο αφορά τη ρύθμιση της παρακολούθησης και την προστασία των θεμελιωδών δικαιωμάτων. Το νομικό πλαίσιο παραμένει κατακερματισμένο και ανεπαρκώς προσαρμοσμένο στις σύγχρονες μορφές επιτήρησης, ενώ η απουσία ρητής πρόβλεψης για μαζικές παρακολουθήσεις, ο περιορισμένος βαθμός δικαστικής εποπτείας και η έλλειψη ουσιαστικής λογοδοσίας αναδεικνύουν την ανάγκη για ουσιαστικές θεσμικές μεταρρυθμίσεις. Το σκάνδαλο των υποκλοπών του 2022 αποτέλεσε χαρακτηριστική απόδειξη των αδυναμιών του συστήματος και ώθησε προς την ψήφιση του Ν. 5002/2022. Ωστόσο η αποτελεσματικότητα του νόμου αυτού, όπως και η συμμόρφωση του εθνικού πλαισίου με τις επιταγές της ΕΣΔΑ, θα κριθεί στην πράξη, απαιτώντας συνεχή εγρήγορση, ενίσχυση της διαφάνειας και θέσπιση ουσιαστικών μηχανισμών προστασίας των δικαιωμάτων του ανθρώπου στο πεδίο της εθνικής ασφάλειας.

8.2. Προτάσεις για αυξημένη προστασία του δικαιώματος της ιδιωτικότητας

Η ανάγκη προστασίας του δικαιώματος στην ιδιωτική ζωή καθίσταται ολοένα και πιο επιτακτική, ιδίως σε περιβάλλοντα αυξημένης χρήσης τεχνολογικών μέσων επιτήρησης από κρατικές υπηρεσίες. Στην Ελλάδα, το νομοθετικό και θεσμικό πλαίσιο παρά τις πρόσφατες τροποποιήσεις, εξακολουθεί να παρουσιάζει σημαντικά κενά. Ως εκ τούτου, κρίνεται αναγκαία η υιοθέτηση μιας σειράς στοχευμένων προτάσεων, με σκοπό την ενίσχυση της λογοδοσίας, της δικαστικής εποπτείας και των εγγυήσεων του πολίτη έναντι κρατικών παρεμβάσεων.

Σε νομοθετικό επίπεδο, επιβάλλεται η θέσπιση ειδικού νόμου που να ρυθμίζει ρητώς και λεπτομερώς τη δυνατότητα άσκησης μαζικών ή προληπτικών παρακολουθήσεων από τις αρμόδιες υπηρεσίες. Το ισχύον πλαίσιο δεν περιλαμβάνει τέτοια πρόβλεψη, γεγονός που

δημιουργεί πεδία αυθαιρεσίας. Ο νέος νόμος θα πρέπει να ορίζει με σαφήνεια τους σκοπούς, τις προϋποθέσεις, τις διαδικασίες έκδοσης ενταλμάτων, και τα δικαιώματα των πολιτών, σε συμμόρφωση με την αρχή της αναλογικότητας και με πρόβλεψη προηγούμενης δικαστικής εποπτείας.

Περαιτέρω, παροτρύνεται η αναθεώρηση του Ν. 5002/2022, ιδίως σε σημεία που περιορίζουν υπερβολικά την ενημέρωση των πολιτών που αποτέλεσαν αντικείμενο παρακολούθησης για λόγους εθνικής ασφάλειας. Η διατήρηση μόνιμης άγνοιας του παρακολουθούμενου ατόμου πλήττει την αρχή της διαφάνειας και της δικαστικής προστασίας. Επομένως, κρίνεται απαραίτητο να προβλεφθεί υπό προϋποθέσεις, η ενημέρωση του θιγόμενου προσώπου μετά τη λήξη της παρακολούθησης. Επιπλέον, πρέπει να ενισχυθούν οι ποινικές και αποζημιωτικές συνέπειες σε περιπτώσεις καταχρηστικής ή παράνομης χρήσης παρακολουθητικών μέσων. Σε θεσμικό επίπεδο, δύναται να προταθεί η ίδρυση ανεξάρτητου εποπτικού φορέα, κατά το πρότυπο της Intelligence and Security Committee of Parliament στο ΗΒ. Ένα τέτοιο όργανο, με διακομματική σύνθεση και πρόσβαση σε διαβαθμισμένο υλικό, θα μπορούσε να ενισχύσει τη λογοδοσία των υπηρεσιών πληροφοριών και να επιβλέπει τη νομιμότητα των πράξεων τους σε τακτική βάση.

Ταυτόχρονα, πρέπει να ενισχυθεί η επιχειρησιακή ικανότητα της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, ώστε να επιτελεί πιο ουσιαστικά τον ελεγκτικό της ρόλο. Η ενίσχυση αυτή πρέπει να περιλαμβάνει την πρόσβαση της σε τεχνικά εργαλεία, την ανεξαρτησία της από την εκτελεστική εξουσία και την ενίσχυση της υποχρέωσης συνεργασίας όλων των κρατικών οργάνων μαζί της.

Τέλος, σε επίπεδο κοινωνικής και διοικητικής συνείδησης, απαιτείται η ενσωμάτωση της προστασίας της ιδιωτικότητας ως πυλώνα του κράτους δικαίου. Οι φορείς της διοίκησης, ιδίως οι δικαστές, οι εισαγγελείς και οι δημόσιοι υπάλληλοι, πρέπει να εκπαιδεύονται συστηματικά για την εφαρμογή της ΕΣΔΑ και των συνταγματικών εγγυήσεων. Παράλληλα, πρέπει να θεσμοθετηθούν μηχανισμοί πληροφόρησης και προσφυγής για τους πολίτες, ώστε να γνωρίζουν τα δικαιώματα τους και να έχουν πρόσβαση σε ένδικα βοηθήματα.

Η προστασία του δικαιώματος στην ιδιωτική ζωή συνιστά θεμέλιο της συνταγματικής τάξης και προϋπόθεση για τη λειτουργία μιας πραγματικής δημοκρατίας. Οι προτάσεις που παρατίθενται δεν επιδιώκουν την απόλυτη κατάργηση των πρακτικών επιτήρησης αλλά την υπαγωγή τους σε θεσμικά αντίβαρα, διαφάνεια και αυστηρούς ελέγχους, ώστε να αποφεύγεται η κατάχρηση και να διασφαλίζεται ο σεβασμός των θεμελιωδών ελευθεριών. Η ισορροπία μεταξύ ασφάλειας και ελευθερίας δεν μπορεί να επιτευθχεί χωρίς την ύπαρξη σαφούς, διαφανούς και λειτουργικού πλαισίου. Η Ελλάδα, ιδίως μετά τα γεγονότα των τελευταίων ετών, καλείται να προχωρήσει σε ουσιαστικές μεταρρυθμίσεις που να ανταποκρίνονται στις απαιτήσεις της ΕΣΔΑ, της ευρωπαϊκής νομολογίας και των διεθνών εξελίξεων, και να αποκαταστήσει την εμπιστοσύνη των πολιτών στους θεσμούς.

8.3. Προτάσεις για ενδεχόμενες διεθνείς συνεργασίες

Η αντιμετώπιση των σύγχρονων προκλήσεων στον τομέα της εθνικής ασφάλειας και της προστασίας της ιδιωτικότητας δεν μπορεί να επιτευχθεί αποκλειστικά σε εθνικό επίπεδο. Η διασυνοριακή φύση των απειλών, όπως η διεθνής τρομοκρατία, το κυβερνοέγκλημα και οι

υβριδικές απειλές, επιβάλλουν την ενίσχυση της διεθνούς συνεργασίας, τόσο σε θεσμικό όσο και σε επιχειρησιακό επίπεδο. Η Ελλάδα οφείλει να αξιοποιήσει την συμμετοχή της σε διεθνείς οργανισμούς και σχήματα, ώστε να ενισχύσει τις δυνατότητες της για πρόληψη, καταστολή και λογοδοσία στον τομέα των πληροφοριών και των παρακολουθήσεων.

Καταρχάς, κρίνεται σκόπιμη η εμβάθυνση της συνεργασίας με τις ευρωπαϊκές αρχές όπως την Europol και τον EU Intelligence and Situation Centre. Η συμμετοχή σε κοινά ευρωπαϊκά προγράμματα ανταλλαγής πληροφοριών, εκπαίδευσης προσωπικού και ανάλυσης απειλών θα μπορούσε να ενισχύσει την τεχνική και αναλυτική ικανότητα της ελληνικής ΕΥΠ, διασφαλίζοντας παράλληλα την τήρηση των ευρωπαϊκών προτύπων προστασίας των θεμελιωδών δικαιωμάτων. Επιπλέον, η συμμετοχή σε ευρωπαϊκούς μηχανισμούς ελέγχου όπως το European Data Protection Board, μπορεί να ενισχύσει τη συμμόρφωση της Ελλάδας με τις απαιτήσεις της ΕΣΔΑ και του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ.

Εξίσου σημαντική είναι η ενίσχυση της συνεργασίας με κράτη που διαθέτουν ανεπτυγμένο νομικό και θεσμικό πλαίσιο για τη δράση των υπηρεσιών πληροφοριών, όπως το ΗΒ. Η Ελλάδα θα μπορούσε να επωφεληθεί από τεχνική βοήθεια, μεταφορά τεχνογνωσίας και καλές πρακτικές σε θέματα θεσμικής εποπτείας, λογοδοσίας και προστασίας της ιδιωτικότητας. Η εμπειρία της βρετανικής Intelligence and Security Committee of Parliament θα μπορούσε να αξιοποιηθεί για τη δημιουργία αντίστοιχων μηχανισμών κοινοβουλευτικής ή ανεξάρτητης εποπτείας στην Ελλάδα.

Σε παγκόσμιο επίπεδο η Ελλάδα οφείλει να τηρεί και να ενισχύει τις υποχρεώσεις της που απορρέουν από διεθνείς συνθήκες, όπως η Σύμβαση του ΟΗΕ για τα Ατομικά και Πολιτικά Δικαιώματα, και να συμμετέχει ενεργά στους μηχανισμούς ελέγχου και αξιολόγησης που προκύπτουν από αυτές. Παράλληλα, η ανάπτυξη διμερών συνεργασιών με άλλα κράτη, στο πλαίσιο ανταλλαγής πληροφοριών με σεβασμό στα δικαιώματα, μπορεί να ενισχύσει την αποτελεσματικότητα των υπηρεσιών πληροφοριών, αρκεί να προβλέπονται αυστηρές ρήτρες για την προστασία της ιδιωτικότητας και να υφίστανται εσωτερικοί μηχανισμοί ελέγχου.

Τέλος, η Ελλάδα πρέπει να αναλάβει πρωτοβουλίες για την προώθηση ενός ευρύτερου ευρωπαϊκού ή διεθνούς πλαισίου που να καθορίζει ελάχιστες εγγυήσεις για τη νόμιμη χρήση τεχνολογιών επιτήρησης και την προστασία των θεμελιωδών δικαιωμάτων. Η απουσία κοινών διεθνών κανόνων επιτρέπει την ασύδοτη χρήση τεχνολογικών εργαλείων, όπως τα λογισμικά τύπου Predator, υπονομεύοντας την εμπιστοσύνη των πολιτών στους δημοκρατικούς θεσμούς.

Η ενίσχυση της διεθνούς συνεργασίας με όρους νομιμότητας, διαφάνειας και σεβασμού των δικαιωμάτων μπορεί να αποτελέσει βασικό πυλώνα για την προστασία της ιδιωτικότητας σε μια εποχή συνεχών και πολυδιάστατων απειλών. Μέσα από στοχευμένες στρατηγικές σύμπραξης, η Ελλάδα μπορεί να αποκτήσει τα απαραίτητα εχέγγυα για να συνδυάσει την εθνική ασφάλεια με τον σεβασμό των θεμελιωδών ελευθεριών.

9. Συμπεράσματα – Επίλογος

Η παρούσα εργασία ανέδειξε με συστηματικό και συγκριτικό τρόπο τα βασικά νομικά, θεσμικά και πρακτικά ζητήματα που σχετίζονται με την ποινική ευθύνη των μυστικών υπηρεσιών για παραβιάσεις της ιδιωτικότητας, εστιάζοντας ειδικά στις έννοιες της λογοδοσίας, της δικαστικής εποπτείας και της προστασίας των θεμελιωδών δικαιωμάτων στο πλαίσιο των σύγχρονων πρακτικών επιτήρησης. Μέσα από την ανάλυση των νομοθετικών πλαισίων και της νομολογίας των ΗΠΑ, ΗΒ και της Ελλάδας αναδείχθηκε η πολυπλοκότητα του θέματος και η ανάγκη εξισορρόπησης δύο κρίσιμων αρχών, της προστασίας της εθνικής ασφάλειας και της διασφάλισης του δικαιώματος στην ιδιωτική ζωή.

Η συζήτηση γύρω από τις μαζικές παρακολουθήσεις και την επιτήρηση των πολιτών στο παρελθόν συχνά χαρακτηριζόταν ως υπερβολική ή και ως θεωρία συνωμοσίας, ιδίως όταν γινόταν λόγος για πλήρη παρακολούθηση ψηφιακών επικοινωνιών από κρατικές υπηρεσίες. Ωστόσο, η εμφάνιση και η τεκμηριωμένη χρήση προηγμένων κατασκοπευτικών λογισμικών όπως το Pegasus, έχουν διαλύσει κάθε αμφιβολία και έχουν επιβεβαιώσει ότι οι πρακτικές αυτές συνιστούν μια απτή και ανησυχητική πραγματικότητα. Η εργασία ανέδειξε πως αυτά τα λογισμικά, τα οποία δίνουν τη δυνατότητα πλήρους ελέγχου των επικοινωνιών, πρόσβασης σε αρχεία, κάμερες και μικρόφωνα, χρησιμοποιήθηκαν όχι μόνο από αυταρχικά καθεστώτα, αλλά και στο πλαίσιο δημοκρατικών κρατών. Η διαπίστωση αυτή δεν επιβεβαιώνει απλώς τις ανησυχίες για την κατάχρηση εξουσίας από τις κρατικές υπηρεσίες πληροφοριών, αλλά καταδεικνύει και την επείγουσα ανάγκη για ενίσχυση του θεσμικού πλαισίου προστασίας της ιδιωτικότητας.

Στις ΗΠΑ, η δράση των υπηρεσιών πληροφοριών (NSA, CIA, FBI) διέπεται από ένα σύνολο θεσμικών και νομοθετικών κειμένων, με πιο χαρακτηριστικά το Foreign Intelligence Surveillance Act (FISA) Και τον Patriot Act. Οι υπηρεσίες έχουν ευρείες εξουσίες για μυστική παρακολούθηση, ενώ η δικαστική εποπτεία μέσω του FISA Court έχει συχνά ασκηθεί κεκλεισμένων των θυρών, με περιορισμένη διαφάνεια. Η νομολογία, όπως στην υπόθεση *ACLU v Clapper*, έδειξε ότι οι μαζικές παρακολουθήσεις μπορεί να οδηγήσουν σε παραβιάσεις της Τέταρτης Τροπολογίας του Συντάγματος, όμως οι κρατικοί μηχανισμοί παραμένουν προσανατολισμένοι στην ενίσχυση της επιχειρησιακής αποτελεσματικότητας των υπηρεσιών.

Αντίστοιχα, στο ΗΒ, το νομικό πλαίσιο για τις υπηρεσίες MI5, MI6 και GCHQ έχει αναπτυχθεί πιο συστηματικά, με τις σημαντικότερες νομοθεσίες να περιλαμβάνουν τον Security Service Act 1989, Intelligence Services Act 1994, Regulation of Investigatory Powers Act 2000, και τον Investigatory Powers Act 2016. Η ύπαρξη αναλυτικών και εξειδικευμένων ρυθμίσεων, ιδίως στο ζήτημα της έκδοσης ενταλμάτων, της δικαστικής εποπτείας και των μηχανισμών διαφάνειας, προσφέρει ένα πιο διαρθρωμένο νομικό περιβάλλον. Ωστόσο, η νομολογία του ΕΔΔΑ (*Big Brother Watch and Others v UK*) και οι εσωτερικές αποφάσεις του Investigatory Powers Tribunal ανέδειξαν ότι ακόμη και αυτό το προηγμένο θεσμικό πλαίσιο μπορεί να οδηγήσει σε παραβιάσεις των άρθρων 8 και 10 της ΕΣΔΑ, λόγω της μαζικής και αδιαφανούς φύσης των παρακολουθήσεων.

Η Ελλάδα, σε σύγκριση με τα ανωτέρω, εμφανίζεται πιο αδύναμη θεσμικά και νομοθετικά. Η ΕΥΠ αποτελεί τη μοναδική θεσμοθετημένη υπηρεσία πληροφοριών, ενώ μέχρι πρότινος λειτουργούσε με περιορισμένη θεσμική εποπτεία. Οι νόμοι 3649/2008, 2225/1994 και 5002/2022 ρυθμίζουν τη δράση της, με τον τελευταίο να επιχειρεί για πρώτη φορά να εισάγει

ένα αυστηρότερο πλαίσιο, ειδικά σε σχέση με την άρση του απορρήτου και τη χρήση κακόβουλων λογισμικών. Παρόλα αυτά, οι αδυναμίες παραμένουν έντονες, κυρίως λόγω της απουσίας πλήρους και ανεξάρτητης δικαστικής εποπτείας, της μη υποχρεωτικής ενημέρωσης των πολιτών που παρακολουθούνται και της γενικότερης έλλειψης διαφάνειας και λογοδοσίας.

Η συγκριτική ανάλυση κατέδειξε τόσο ομοιότητες όσο και θεμελιώδεις διαφορές. Από τη μια, και τα τρία κράτη μοιράζονται κοινές πρακτικές εμπλοκής των υπηρεσιών πληροφοριών σε δραστηριότητες παρακολούθησης, στο όνομα της εθνικής ασφάλειας. Επιπλέον, σε όλα τα συστήματα αναγνωρίζεται η ανάγκη θεσμικών εγγυήσεων και προβλέπεται κάποια μορφή δικαστικής εποπτείας ή ανεξάρτητης επιτροπή. Από την άλλη, η Ελλάδα παρουσιάζει σημαντικά υστερήματα σε επίπεδο εξειδικευμένης νομοθεσίας, ανεξάρτητης λογοδοσίας και θεσμικής κουλτούρας ελέγχου των υπηρεσιών ασφαλείας.

Η ΕΣΔΑ λειτουργεί ως κρίσιμο υπερεθνικό εργαλείο, δεδομένου ότι τα κράτη συμμορφώνονται με τις προβλέψεις της, ιδίως ως προς το άρθρο 8 για την προστασία της ιδιωτικής ζωής. Ιδιαίτερα για την Ελλάδα που κύρωσε τη Σύμβαση ήδη από το 1953, η δεσμευτική της ισχύς καθιστά αναγκαία την αναμόρφωση του εθνικού πλαισίου προς την κατεύθυνση της διασφάλισης πλήρους συμβατότητας με τις υποχρεώσεις της.

Τέλος, η εργασία προτείνει συγκεκριμένα μέτρα για τη βελτίωση της προστασίας της ιδιωτικότητας, όπως η ενίσχυση της δικαστικής εποπτείας, καθιέρωση υποχρεωτικής ενημέρωσης των θιγόμενων προσώπων, θεσμοθέτηση ανεξάρτητης αρχής ελέγχου, και υιοθέτηση διακρατικών συνεργασιών για την αντιμετώπιση απειλών που ξεπερνούν τα εθνικά σύνορα. Η αναβάθμιση της λογοδοσίας και της διαφάνειας στον τομέα της εθνικής ασφάλειας δεν αποτελεί απλώς νομική υποχρέωση αλλά θεμελιώδη εγγύηση για τη διατήρηση της δημοκρατίας και του κράτους δικαίου σε μια εποχή αυξημένων τεχνολογικών προκλήσεων.

Η προστασία της ιδιωτικότητας απέναντι στις σύγχρονες πρακτικές μαζικής επιτήρησης δεν μπορεί να θεωρείται πολυτέλεια ή εμπόδιο στην εθνική ασφάλεια. Αντιθέτως, αποτελεί αναγκαία προϋπόθεση για την ύπαρξη ελεύθερων και δημοκρατικών κοινωνιών. Η παρούσα εργασία ανέδειξε ότι μόνο μέσω ενός ισχυρού θεσμικού πλαισίου, που βασίζεται στη διαφάνεια, τη λογοδοσία και τον αυστηρό έλεγχο των κρατικών μηχανισμών, μπορεί να επιτευχθεί η απαιτούμενη ισορροπία μεταξύ προστασίας των δικαιωμάτων και διαφύλαξης της ασφάλειας. Η πρόκληση των επόμενων ετών δεν είναι απλώς νομική ή τεχνική, είναι πρωτίστως πολιτική και ηθική, η επαναβεβαίωση της αξίας του ατόμου απέναντι στη δύναμη του κράτους.

UNIVERSITY of NICOSIA

ΒΙΒΛΙΟΓΡΑΦΙΑ

Πίνακας Υποθέσεων:

- *ACLU v Clapper* 785 F3d 787 (2d Cir 2015).
- *ACLU v NSA* 493 F3d 644 (6th Cir 2007).
- *Athanasios Koukakis v Greece* App no 37659/22 (ECtHR, 11 June 2024).
- *Bărbulescu v Romania* (App no 61496/08) ECHR, Grand Chamber, 5 September 2017
- *Big Brother Watch and Others v United Kingdom* (2021) App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).
- Boyd v. United States, 116 U.S. 616, 626-627 (1886)
- *Carpenter v United States* 138 S Ct 2206 (2018).
- *Katz v United States* 389 US 347 (1967).
- *Klayman v Obama* 800 F3d 559 (DC Cir 2015).
- *Klass and Others v Germany* (App no 5029/71) ECHR, 6 September 1978.
- *Liberty and Others v GCHQ and Others* [2015] UKIPTrib 13_77-H_2.
- *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22, [2020] AC 491.
- *United States v Moalin* 973 F3d 977 (9th Cir 2020).

Ξένη Νομοθεσία:

- British-U.S. Communication Intelligence Agreement' (5 March 1946) https://www.gchq.gov.uk/feature/ukusa-agreement
- Espionage Act of 1917, First Amendment Encyclopedia https://firstamendment.mtsu.edu/article/espionage-act-of-1917/
- Foreign Intelligence Surveillance Act 2008, §702 et seq (US).
- Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub L No 110–261, 122 Stat 2436 (codified in part at 50 USC §1801 et seq)
- Human Rights Act 1998 (UK) c 42

- Intelligence Services Act 1994 (UK) c 13

- Investigatory Powers Act 2016 (UK) c 25

- National Security Act of 1947, Pub L No 80–253, 61 Stat 496, as amended through P.L. 118–159 (23 December 2024) art 105 C

- Official Secrets Act 1889 (UK), as amended

- Regulation of Investigatory Powers Act 2000 (UK) c 23

- Security Service Act 1989 (UK).

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act 2001, Pub L No 107–56, 115 Stat 272

- US Constitution amend IV, in *Fourth Amendment—Search and Seizure* (US Government Publishing Office, 2021).

- *USA FREEDOM Act of 2015*, Pub L No 114–23, 129 Stat 268.

- 18 USC § 2516(1) (authorising specified officials to apply for wiretap orders in investigations of certain offences).

- 50 USC §1801 (Definitions under FISA) https://www.law.cornell.edu/uscode/text/50/1801

- 50 USC §1809 (Criminal sanctions under FISA) https://www.law.cornell.edu/uscode/text/50/1809

- Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου (UDHR), ΓΑ Ψήφισμα 217 Α (III) (10 Δεκεμβρίου 1948).

- Διεθνές Σύμφωνο για τα Αστικά και Πολιτικά Δικαιώματα (ICCPR), ΓΑ Ψήφισμα 2200Α (XXI) (16 Δεκεμβρίου 1966, σε ισχύ από 23 Μαρτίου 1976).

- Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ, ECHR), 4 Νοεμβρίου 1950, σε ισχύ από 3 Σεπτεμβρίου 1953.

- Ευρωπαϊκός Χάρτης Θεμελιωδών Δικαιωμάτων (ΕΧΘΔ, Charter of Fundamental Rights of the European Union) [2000] ΕΕ C364/1, δεσμευτικός από 1 Δεκεμβρίου 2009.

Ελληνική Νομοθεσία

- Σύνταγμα της Ελλάδας (ισχύον από 1975, όπως ισχύει μετά την αναθεώρηση του 2019).

- Νόμος 2225/1994, «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α 121, 20 Ιουλίου 1994).

- Νόμος 3649/2008, «Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις» (ΦΕΚ Α 39, 3 Μαρτίου 2008).

- Νόμος 4622/2019, «Επιτελικό Κράτος: οργάνωση, λειτουργία και διαφάνεια της Κυβέρνησης, των κυβερνητικών οργάνων και της κεντρικής δημόσιας διοίκησης» (ΦΕΚ Α 133, 7 Αυγούστου 2019).

- Νόμος 5002/2022, «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών» (ΦΕΚ Α 228, 9 Δεκεμβρίου 2022).

Βιβλία:

- Chesterman S, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (OUP 2011).

- Heffernan WC, *The Fourth Amendment: Origins and Interpretations* (Carolina Academic Press 2022).

- G Babiniotis, *Λεξικό της Νέας Ελληνικής Γλώσσας* (Κέντρο Λεξικολογίας 2022).

- Edgar T H, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA* (Brookings Institution Press 2017).

- Friedewald M and others (eds), *Surveillance, Privacy and Security: Citizens' Perspectives* (Routledge 2017)

- Ober J, *Mass and Elite in Democratic Athens: Rhetoric, Ideology, and the Power of the People* (Princeton UP 1989).

Επιστημονικά Άρθρα:

- Banks WC, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 *Emory Law Journal* 513.

- Bartlett G and Everett M, *The Official Secrets Acts and Official Secrecy* (Briefing Paper CBP07422, House of Commons Library, 2 May 2017) https://www.parliament.uk/commons-library

- European Parliament, *Ο αντίκτυπος του Pegasus στα θεμελιώδη δικαιώματα και τις δημοκρατικές διαδικασίες στην Ευρωπαϊκή Ένωση* (Μελέτη PE 739.870, 2023)

- European Parliament, *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights* (2013) https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/510024/IPOL-LIBE_ET(2013)510024_EN.pdf

- Eliza Watt (2017) 'The right to privacy and the future of mass Surveillance', The International Journal of Human Rights, 21:7, 773-799, DOI: 10.1080/13642987.2017.1298091

- Fleck D, 'Individual and State Responsibility for Intelligence Gathering' (2018) 39(3) Michigan Journal of International Law 511.

- Manget P J, 'Intelligence and the Criminal Law in the United States' (2006) 19(2) International Journal of Intelligence and CounterIntelligence 208.

- Pun D, 'Rethinking Espionage in the Modern Era' (2017) 18(1) *Chicago Journal of International Law* 353.

- Sinha G A, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' (2013) 59 Loyola Law Review 861.

- Mellon J, *The UKUSA Agreement of 1948* (27 November 2001) http://www.europarl.eu.int/committees/echelon_home.htm

- Nedeva S, 'Intelligence Services' Unaccountability for Human Rights Violations' (2020) 20(1) International Comparative Law Review 43.

- Joergensen RF, 'Can human rights law bend mass surveillance?' (2014) 3(1) *Internet Policy Review* https://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance Acessed 14 August 2025

- Piodi F and Mombelli I, *The Echelon Affair* (European Parliament, November 2014) https://www.europarl.europa.eu/committees/en/echelon-home

- Richards N M, 'The Dangers of Surveillance' (2013) 126(7) Harvard Law Review 1934.

- The 9/11 Commission, *The 9/11 Commission Report* (Government Printing Office, 22 July 2004) https://govinfo.library.unt.edu/911/report/911Report.pdf

- Wright S, *An Appraisal of Technologies of Political Control – Interim Study* (European Parliament, Directorate General for Research PE 166.499/Int.St., 19 January 1998)

- Woods L, George A and Smyth M, 'Big Brother Watch and Others v the United Kingdom: Mass Surveillance and the Right to Privacy' (2019) 20 Human Rights Law Review 1.

Δημοσιεύματα Εφημερίδων:

- Greenwald G, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' *The Guardian* (6 June 2013) https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

- Hawkins K, 'What is the PRISM Program? NSA, Edward Snowden and Government Surveillance in 2025' (Cloudwards, 31 July 2024) https://www.cloudwards.net/what-is-the-prism-program-nsa-surveillance-tool-2025/

- Μαύρου Ο., «Οι κατάσκοποι στην αρχαία Ελλάδα – Ποια ήταν τα τεχνάσματα τους» *SL Press*, 15 Μαΐου 2023, https://slpress.gr/istorimata/oi-kataskopoi-stin-archaia-ellada-poia-itan-ta-technasmata-toys/

- Μαρκόπουλος Κ, «*Η κατασκοπία στην αρχαία Ελλάδα. Οι μυστικοί πράκτορες της Τροίας και οι συμβουλές για να αντιμετωπιστούν οι κατάσκοποι του εχθρού*», Μηχανή του Χρόνου, 21 Φεβρουαρίου 2025 https://www.mixanitouxronou.gr/i-kataskopia-stin-archaia-ellada-oi-mystikoi-praktores-tis-troias-kai-oi-symvoyles-gia-na-antimetopistoyn-oi-kataskopoi-toy-echthroy/

- NSA Prism program taps into user data of Apple, Google and others' *The Guardian* (6 June 2013) https://www.theguardian.com/world/2013/jun/06/nsa-prism-program-data-mining

- «Πάντα μυστική και αμφιλεγόμενη» *Το Βήμα*, 24 Νοεμβρίου 2008, https://www.tovima.gr/2008/11/24/archive/panta-mystiki-kai-amfilegomeni/

- 'Six arrested for operating a Russian spy ring in UK' *UK Defence Journal* (10 March 2025) https://ukdefencejournal.org.uk/six-arrested-for-operating-a-russian-spy-ring-in-uk/

- Κεντητός Γ, «Ο κωδικός Enigma των Ναζί και πώς κατάφεραν να τον σπάσουν» *Sportime*, 21 Φεβρουαρίου 2025 https://www.sportime.gr/must-read/o-kodikos-enigma-ton-nazi-ke-pos-kataferan-na-ton-spasoun/

Άλλες Διαδικτυακές Πηγές:

- CIA, 'History of CIA' https://www.cia.gov/legacy/cia-history/

- Committee on Civil Liberties, Justice and Home Affairs, *US Legal Instruments for Access and Electronic Surveillance of EU Citizens: Background Note* (European Parliament, 2013)

- Constitutional Rights Foundation, 'Edward Snowden, the NSA, and Mass Surveillance' (BRIA 31:3, Spring 2016) https://www.crf-usa.org

- Defense Intelligence Agency, 'Home' https://www.dia.mil/

- Encyclopaedia Britannica, 'National Security Agency' https://www.britannica.com/topic/National-Security-Agency

- FBI, 'The Aldrich Ames Case' (21 February 2025) https://www.fbi.gov/history/famous-cases/aldrich-ames

- FBI, 'Welcome to fbi.gov' https://www.fbi.gov/

- GCHQ, 'Overview' https://www.gchq.gov.uk/section/mission/overview

- Government Communications Headquarters (GCHQ), 'Overview' (*GCHQ*, undated) https://www.gchq.gov.uk/section/mission/overview
-

- House Permanent Select Committee on Intelligence, *HPSCI Snowden Review: Declassified* (September 2016) https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf

- Intelligence and Security Committee of Parliament, 'Home – ISC' https://isc.independent.gov.uk/

- MI5, 'MI5 in the 1990s and 2000s' https://www.mi5.gov.uk/history/mi5-in-the-1990s-and-2000s

- MI5, 'MI5's Early Years' https://www.mi5.gov.uk/history/mi5s-early-years

- National Security Agency, 'The Early History of NSA' https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/early_history_nsa.pdf

- ODNI, 'Home' https://www.dni.gov/

- SIS (MI6), 'Our History' https://www.sis.gov.uk/about-us/our-history

- 'Six arrested for operating a Russian spy ring in UK' (*UK Defence Journal*, 10 March 2025) https://ukdefencejournal.org.uk/six-arrested-for-operating-a-russian-spy-ring-in-uk/

- Skytales Blog, 'Τι μας αποκάλυψε μέχρι σήμερα ο Snowden;' (6 June 2013) https://skytal.es/blog/index.html?p=381

- Special Intelligence Report, 10 June 1943' (US Department of Defense, 10 June 1943) https://media.defense.gov/2021/Jul/15/2002763671/-1/-1/0/SPEC_INT_10JUN43.PDF

- The NSA's PRISM Program and the New EU Privacy Regulation' (2017) *American University Business Law Review* https://digitalcommons.wcl.american.edu/aublr/vol6/iss3/3/

- UK Government, 'About the Secret Intelligence Service (MI6)' https://www.gov.uk/government/organisations/secret-intelligence-service/about