ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Εγκληματολογικές και Ποινικές προσεγγίσεις της διαφθοράς, του οικονομικού και του οργανωμένου εγκλήματος

Διπλωματική Εργασία

Data laundering ως σύγχρονη εκδοχή κρατικο-εταιρικού εγκλήματος στη ψηφιακή εποχή: Η περίπτωση της κρατικής παρακολούθησης και των εμπορικών spyware.

Αδαμοπούλου Μαρίνα
ΑΜ 514419

Επιβλέπουσα καθηγήτρια Ευαγγελία Παππά

Αθήνα, Ιούνιος 2026

Data laundering ως σύγχρονη εκδοχή κρατικο-εταιρικού εγκλήματος στη ψηφιακή εποχή: Η περίπτωση της κρατικής παρακολούθησης και των εμπορικών spyware.

Επιτροπή επίβλεψης Διπλωματικής εργασίας

Επιβλέπουσα Καθηγήτρια
Παππά Ευαγγελία
Μέλος Σ.Ε.Π Ε.Α.Π

Συν-επιβλέπουσα Καθηγήτρια
Βιδάλη Σοφία
Μέλος Σ.Ε.Π Ε.Α.Π

Περίληψη

Η παρούσα διπλωματική εργασία διερευνά το ξέπλυμά δεδομένων (data laundering) ως σύγχρονη μορφή κρατικο-εταιρικού εγκλήματος στη ψηφιακή εποχή, με εμπειρικό επίκεντρο την ελληνική περίπτωση Predatorgate. Αξιοποιώντας ως κεντρικό αναλυτικό πλαίσιο τη θεωρία της εγκληματολογίας των ισχυρών και το μοντέλο κρατικο-εταιρικού εγκλήματος των Kramer και Michalowski, η εργασία αναπτύσσει τη δομική αναλογία μεταξύ data laundering και money laundering μέσω του τριμερούς μοντέλου τοποθέτησης, διαστρωμάτωσης και ενσωμάτωσης. Συμπληρωματικά, η θεωρία επιτήρησης του Φουκώ αναδεικνύει τις δημοκρατικές επιπτώσεις της κρατικής παρακολούθησης μέσω του φαινομένου του αποτρεπτικού αποτελέσματος, το οποίο επεκτείνει τη βλάβη πέραν των άμεσων θυμάτων σε ολόκληρη τη δημόσια σφαίρα.

Η εμπειρική εφαρμογή του πλαισίου αυτού στο Predatorgate αποκαλύπτει πώς και τα τρία στάδια εκδηλώθηκαν με αξιοσημείωτη σαφήνεια. Ο Ν. 4790/2021 αναλύεται ως νομοθετικά κατοχυρωμένος μηχανισμός διαστρωμάτωσης, ενώ η παράλληλη χρήση νόμιμης παρακολούθησης από την ΕΥΠ και παράνομης από το Predator κατά των ίδιων στόχων συνιστά την πιο χαρακτηριστική εκδήλωση της ενσωμάτωσης. Η καταδίκη του Φεβρουαρίου 2026, πρώτη παγκοσμίως ποινική καταδίκη στελεχών βιομηχανίας spyware, αναλύεται ταυτόχρονα ως ορόσημο και ως επιβεβαίωση της δομικής ατιμωρησίας, καθώς ο κρατικός βραχίονας παρέμεινε νομικά άθικτος. Η συγκριτική ανάλυση Ισπανίας και Ουγγαρίας επιβεβαιώνει ότι το φαινόμενο αποτελεί συστημικό πρόβλημα της Ευρωπαϊκής Ένωσης.

Η εργασία καταλήγει σε προτάσεις de lege ferenda σε τρία επίπεδα: αναθεώρηση του άρθρου 23 GDPR και δημιουργία ευρωπαϊκού μηχανισμού αδειοδότησης σε ευρωπαϊκό επίπεδο, συνταγματική αναθεώρηση του άρθρου 19 σε εθνικό επίπεδο, και ποινικοποίηση του data laundering ως αυτόνομου αδικήματος σε εγκληματολογικό επίπεδο.

Λέξεις-κλειδιά: data laundering, κρατικο-εταιρικό έγκλημα, spyware, Predatorgate, εγκληματολογία των ισχυρών

Abstract

This dissertation examines data laundering as a contemporary form of state-corporate crime in the digital age, with its empirical focus on the Greek Predatorgate scandal. Drawing on the criminology of the powerful and the state-corporate crime model of Kramer and Michalowski as its central analytical framework, the study develops the structural analogy between data laundering and money laundering through a three-stage model of placement, layering and integration. Complementarily, Foucault's theory of surveillance illuminates the democratic consequences of state surveillance through the chilling effect, which extends harm beyond immediate victims to the public sphere as a whole.

The empirical application of this framework to Predatorgate reveals how all three stages manifested with remarkable clarity. Law 4790/2021 is analyzed as a legislatively enshrined layering mechanism, while the parallel use of lawful surveillance by the EYP and unlawful Predator surveillance against the same targets constitutes the most characteristic manifestation of integration. The conviction of February 2026, the first criminal conviction of spyware industry executives anywhere in the world, is analyzed simultaneously as a landmark and as a confirmation of structural impunity, given that the state arm remained legally untouched. The comparative analysis of Spain and Hungary confirms that the phenomenon represents a systemic problem of the European Union rather than a national peculiarity.

The dissertation concludes with de lege ferenda proposals on three levels: revision of Article 23 GDPR and the creation of a European licensing mechanism at the European level, constitutional revision of Article 19 at the national level, and the criminalization of data laundering as an autonomous offense at the criminological level.

Keywords: data laundering, state-corporate crime, spyware, Predatorgate, criminology of the powerful, structural impunity

Περιεχόμενα

Συντομογραφίες & Ακρωνύμια

ΑΔΑΕ — Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
ΕΥΠ — Εθνική Υπηρεσία Πληροφοριών
ΕΔΔΑ — Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΔΕΕ — Δικαστήριο της Ευρωπαϊκής Ένωσης
ΕΕ — Ευρωπαϊκή Ένωση
ΟΗΕ — Οργανισμός Ηνωμένων Εθνών
ΗΠΑ — Ηνωμένες Πολιτείες Αμερικής
ΦΕΚ — Φύλλο Εφημερίδας της Κυβερνήσεως
ΚΕΤΥΑΚ — Κέντρο Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας
ΚΕΜΕΑ — Κέντρο Μελετών και Ανάλυσης
PEGA — Parliamentary Committee on the Use of Pegasus and Equivalent Surveillance Spyware
GDPR — General Data Protection Regulation
NSO — Niv, Shalev and Omri
NSA — National Security Agency
CIA — Central Intelligence Agency
FATF — Financial Action Task Force
SWAMI — Safeguards in a World of Ambient Intelligence
RSF — Reporters Sans Frontières
SIPRI — Stockholm International Peace Research Institute
EDPB — European Data Protection Board
ICCPR — International Covenant on Civil and Political Rights
ICIJ — International Consortium of Investigative Journalists
OLAF — Office Européen de Lutte Anti-Fraude
IPI — International Press Institute
UNHRC — United Nations Human Rights Council
ECHR — European Convention on Human Rights
CBP — Customs and Border Protection
ICE — Immigration and Customs Enforcement
IRS — Internal Revenue Service
EPRS — European Parliamentary Research Service

ΕΙΣΑΓΩΓΗ

Ο Όργουελ πολύ πριν τη σύγχρονη εντατικοποίηση των τεχνολογιών παρακολούθησης παρουσίασε μια προφητική οπτική στο «Μεγάλο Αδελφό» του λογοτεχνικού έργου του «1984». Στο φουτουριστικό έθνος Ωκεανία οι πολίτες παρακολουθούνται στα σπίτια τους από την οθόνη της τηλεόρασης. Η αστυνομία σκέψης συντονίζει την προσπάθεια παρακολούθησης ως πράκτορας ενός ολοκληρωτικού καθεστώτος. Αυτή τη δυστοπική οραματική πρόβλεψη ξεπέρασαν στη σύγχρονη εποχή οι ικανότητες των τεχνολογιών παρακολούθησης (Haggerty and Ericson , 2000, p. 605-606).

Η ταχεία εξάπλωση του διαδικτύου και της ψηφιακής τεχνολογίας εν γένει, κυρίως μετα το 1990 οδήγησε σε μετασχηματισμό του τρόπου με τον οποίο επικοινωνούμε και ανταλλάσσουμε πληροφορίες. Η ψηφιακή μεταρρύθμιση και οι καινοτομίες στις τεχνολογίες επικοινωνίας ενίσχυσαν τη συνδεσιμότητα, τη συμμετοχή και την πρόσβαση σε υπηρεσίες και ταυτόχρονα αυξήσαν τις ευκαιρίες για κρατική παρακολούθηση και παρεμβάσεις στα ανθρώπινα δικαιώματα και τις θεμελιώδεις ελευθερίες των ατόμων (Mitsilegas, 2021, p. 47). Έτσι, παράλληλα με τις ευκαιρίες που η τεχνολογία παρουσίασε ανέκυψαν και νέοι κίνδυνοι. Οι κίνδυνοι αυτοί αφορούν τη δημοκρατία, τα ανθρώπινα δικαιώματα και την προστασία προσωπικών δεδομένων, καθώς τα προγράμματα παρακολούθησης τοποθετούνται χωρίς τη γνώση του χρήστη· προκειμένου κρυφά να συλλέξουν πληροφορίες και δεδομένα, συνήθως προσωπικά και ευαίσθητα (Kaldani & Prokopets, 2022, p. 7)

Το 2013, όταν ο πρώην πράκτορας της CIA Έντουαρντ Σνόουντεν αποκάλυψε το «*Πρόγραμμα Prism*» της Εθνικής Υπηρεσίας Ασφαλείας των ΗΠΑ, ένα απεριόριστο πρόγραμμα μαζικής παρακολούθησης που πραγματοποιήθηκε όχι μόνο σε πολίτες των ΗΠΑ, αλλά και σε όλους τους χρήστες του Διαδικτύου σε όλο τον κόσμο, αρκετοί μελετητές εξέφρασαν ανησυχίες σχετικά με την εφαρμογή της συγκεκριμένης παρακολούθησης για τη συντριβή κάθε δημοκρατικού κινήματος κατά της κυβέρνησης (Krishna & Atul, 2022)

Ανάμεσα στα πιο διαδεδομένα προγράμματα ηλεκτρονικής παρακολούθησης spyware είναι και το πρόγραμμα Pegasus, το οποίο σχεδιάστηκε από την Ισραηλινή εταιρεία NSO Group για την καταπολέμηση της τρομοκρατίας και ως εργαλείο επιβολής του νόμου. Η ορθή χρήση του όμως είναι αμφιλεγόμενη λόγω της κακής χρήσης του από κυβερνήσεις, συνήθως απολυταρχικών καθεστώτων (Modderkolk, 2023). Τον Ιούλιο του 2021, μια κοινοπραξία 17 διεθνών ειδησεογραφικών οργανισμών αποκάλυψε ότι το spyware Pegasus, είχε χρησιμοποιηθεί από κυβερνήσεις σε τουλάχιστον 50 χώρες για την παρακολούθηση δημοσιογράφων, ακτιβιστών, δικηγόρων και αρχηγών κρατών (Citizen Lab, 2021). Ένα χρόνο αργότερα, η Ελλάδα βρέθηκε στο επίκεντρο ενός ανάλογου σκανδάλου, γνωστού ως Predatorgate, στο οποίο το εμπορικό spyware Predator μιας άλλης Ισραηλινής εταιρείας, της Intellexa χρησιμοποιήθηκε για την παρακολούθηση δημοσιογράφου, αρχηγού κόμματος αντιπολίτευσης, υπουργών και

στρατιωτικών αξιωματούχων, ορισμένοι εκ των οποίων ανήκαν στον κυβερνητικό χώρο. Στις 26 Φεβρουαρίου 2026, ελληνικό δικαστήριο εξέδωσε την πρώτη παγκοσμίως ποινική καταδίκη στελεχών της βιομηχανίας εμπορικών spyware στην οποία καταδικάστηκαν τέσσερις επιχειρηματίες (https://predatorgate.gr/gr/victims).

Δεν υπάρχει αμφιβολία ότι η απλή παρουσία τέτοιου spyware χωρίς κατάλληλο ρυθμιστικό πλαίσιο έχει εγείρει από μόνη της ανησυχία για το δικαίωμα κάθε ατόμου στην ιδιωτική ζωή. Τέτοια επιχειρήματα φαίνεται να είναι πιο ισχυρά υπό το φως των περιστατικών βασανιστηρίων και κράτησης με τη χρήση τεχνολογιών επιτήρησης αιχμής (Sonne and Coker 2022; Coker και Sonne 2011).

Τα γεγονότα αυτά δεν αποτελούν απλώς δημοσιογραφικές αποκαλύψεις. Από εγκληματολογική σκοπιά, συνιστούν εκδηλώσεις ενός δομικού φαινομένου, της κατάχρησης κρατικής και εταιρικής εξουσίας με σκοπό την παράνομη παρακολούθηση και τη συστηματική συγκάλυψή της. Πρόκειται για φαινόμενο που η εγκληματολογία των ισχυρών έχει χαρτογραφήσει θεωρητικά, αλλά που στη ψηφιακή εποχή αποκτά νέες, πιο επικίνδυνες διαστάσεις.

Το διαδίκτυο δεν είναι πια καταφύγιο ελευθερίας όπως στο παρελθόν, όταν αποτελούσε πεδίο ανταλλαγής πληροφοριών όπου τα κράτη δεν είχαν καμία εξουσία. Δεν είναι πλεον μόνο ένα μέσο σύνδεσης, επικοινωνίας και δικτύωσης. Όσο περισσότερο εισβάλλει στην ανθρώπινη ζωή τόσο περισσότερο συνδέεται με θέματα ασφαλείας (Modderkolk, 2023, σ. 27). Ο καινούργιος κόσμος είναι ψηφιακός. Ένας κόσμος με απεριόριστες δυνατότητες και ασαφείς κανόνες (Modderkolk, 2023, σ. 40)

Σκοπός της παρούσας εργασίας είναι να διερευνήσει πώς το data laundering εντάσσεται στο κρατικό και εταιρικό έγκλημα υπό εγκληματολογική και ποινική σκοπιά. Ειδικότερα, η εργασία επιδιώκει να φωτίσει τους μηχανισμούς συγκάλυψης, τις θεσμικές ανεπάρκειες και τις δυναμικές εξουσίας που επιτρέπουν τη νομιμοποίηση παράνομων δεδομένων στο πλαίσιο της κρατικής παρακολούθησης μέσω εμπορικών spyware.

Η εργασία βασίζεται στη θεωρία της εγκληματολογίας των ισχυρών ως κεντρικό αναλυτικό πλαίσιο. Η έννοια του data laundering ξέπλυμα δεδομένων) αναπτύσσεται μέσα από τη δομική αναλογία με το money laundering (ξέπλυμα χρήματος) (SWAMI, 2006, p. 96), αξιοποιώντας το αναλυτικό μοντέλο των τριών σταδίων, συλλογή, διαστρωμάτωση, ενσωμάτωση, προκειμένου να αποτυπωθεί ο τρόπος με τον οποίο παράνομα δεδομένα νομιμοποιούνται (FATF, 2012). Η ανάλυση των επιπτώσεων στα ανθρώπινα δικαιώματα και η νομολογία του ΕΔΔΑ χρησιμοποιούνται για να αναδειχθεί το νομικό πλαίσιο αξιολόγησης (Kaldani & Prokopets, 2022).

Έτσι, σκοπός της παρούσας εργασίας είναι να αναλυθεί πως ιδιωτικές εταιρείες σε συνεργασία με κυβερνήσεις συνεργάζονται για την παράνομη απόκτηση δεδομένων και μέσα από

διαδικασίες που ομοιάζουν με το ξέπλυμα βρώμικου χρήματος να νομιμοποιούν τα δεδομένα αυτά και να τα χρησιμοποιούν καταπατώντας βασικά ανθρώπινα δικαιώματα (SWAMI, 2006, p. 96; Kaldani & Prokopets, 2022).

Η έρευνα εξετάζει επίσης την προστασία των ανθρωπίνων δικαιωμάτων. Αυτό διαδέχεται η ανάλυση του Foucault για την πειθαρχική εξουσία της επιτήρησης. Αυτές οι προοπτικές αποτελούν τη θεωρητική βάση της εργασίας, αμφισβητώντας τη νομιμότητα των πρακτικών κρατικής επιτήρησης. Ακολουθεί μια επισκόπηση του spyware, συμπεριλαμβανομένων των τεχνικών χαρακτηριστικών και των εφαρμογών του σε κρατική χρήση. Στη συνέχεια, εξετάζει το ισχύον νομοθετικό πλαίσιο εντός της ΕΕ και εμβαθύνει στις επιπτώσεις της ψηφιακής επιτήρησης στα ανθρώπινα δικαιώματα (Saxena & Anand, 2022).

Η εργασία οργανώνεται γύρω από το ερευνητικό ερώτημα: Ποια είναι η σχέση μεταξύ data laundering και κρατικο-εταιρικού εγκλήματος, και πώς εκδηλώνεται αυτή στην ελληνική περίπτωση Predatorgate; Ποιες μηχανές συγκάλυψης, θεσμικές ανεπάρκειες και δυναμικές εξουσίας επιτρέπουν τη νομιμοποίηση παράνομα αποκτιθέντων δεδομένων και τέλος, ποιες ρυθμιστικές αλλαγές απαιτούνται σε ευρωπαϊκό και εθνικό επίπεδο για την αποτελεσματική αντιμετώπιση του data laundering ως μορφής κρατικο-εταιρικού εγκλήματος;

Η μεθοδολογία της εργασίας συνδυάζει κριτική ανάλυση βιβλιογραφίας με μελέτη περίπτωσης. Η κριτική ανάλυση της βιβλιογραφίας επιτρέπει τη συγκρότηση του θεωρητικού πλαισίου, τη σύνθεση της εγκληματολογίας του κρατικο-εταιρικού εγκλήματος, της φουκωικής θεωρίας (Foucault) και των Σπουδών Επιτήρησης (Surveillance Studies) . Η μελέτη περίπτωσης του ελληνικού Predatorgate επιτρέπει την εμπειρική εφαρμογή του θεωρητικού πλαισίου σε συγκεκριμένα, τεκμηριωμένα γεγονότα.

Ο όρος data laundering χρησιμοποιείται στην παρούσα εργασία κατ' αναλογία με το money laundering για να περιγράψει τη διαδικασία νομιμοποίησης παράνομα αποκτηθέντων δεδομένων. Αν και δεν έχει ακόμα καθιερωθεί ως αυτόνομος ακαδημαϊκός όρος, χρησιμοποιείται ήδη σε κανονιστικά και νομικά πλαίσια (SWAMI, 2006: 80; Ayoub & Goitein, 2024)

Το υλικό που αξιοποιείται περιλαμβάνει πρωτογενείς νομικές πηγές (GDPR, Κανονισμός 2021/821, ελληνική νομοθεσία), θεσμικά κείμενα (Έκθεση PEGA, εκθέσεις της ΑΔΑΕ), τεχνικές εκθέσεις (Citizen Lab, Amnesty International Security Lab), ακαδημαϊκή βιβλιογραφία από την εγκληματολογία, τη νομική και τις κοινωνικές επιστήμες, καθώς και δημοσιογραφικό υλικό διεθνών μέσων ενημέρωσης. Η επιλογή της Ελλάδας ως μελέτη περίπτωσης δεν είναι τυχαία, καθώς αποτελεί μία από τις πλέον καλά τεκμηριωμένες περιπτώσεις κρατικής χρήσης εμπορικού spyware (Predator) εντός της ΕΕ, η οποία έχει λάβει και δικαστική διάσταση (Reuters , 2026).

Η εργασία οργανώνεται σε έξι κεφάλαια. Μετά την Εισαγωγή, η οποία παρουσιάζει το ερευνητικό ερώτημα, τη μεθοδολογία και τη δομή της εργασίας, ακολουθεί το Κεφάλαιο 1 το οποίο θέτει το θεωρητικό πλαίσιο της εγκληματολογίας των ισχυρών και εξετάζει πώς η ψηφιακή

εποχή το αναδιαμορφώνει. Το **Κεφάλαιο 2** ερμηνεύει τη θεωρία του Πανοπτικού του Foucault και τη σύνδεσή του με τη ψηφιακή παρακολούθηση. Το **Κεφάλαιο 3** αποσαφηνίζει εννοιολογικά το data laundering μέσα από την αναλογία με το money laundering και αναλύει τα στάδια λειτουργίας του. Το **Κεφάλαιο 4** εξετάζει τη βιομηχανία εμπορικών spyware εστιάζοντας στην αγορά, αλυσίδα κράτος-εταιρεία-στόχος, offshore δομές και ρόλος εξαγωγικών αδειών ως μηχανισμός laundering. Το **Κεφάλαιο 5** εξετάζει το ισχύον νομικό και ρυθμιστικό πλαίσιο και καταλήγει σε προτάσεις de lege ferenda. Το **Κεφάλαιο 6** αναλύει τη μελέτη περίπτωσης του ελληνικού Predatorgate. Η εργασία ολοκληρώνεται με Συμπεράσματα που απαντούν στα ερευνητικά ερωτήματα, αναγνωρίζουν τους περιορισμούς και υποδεικνύουν κατευθύνσεις μελλοντικής έρευνας.

Το θέμα της παρούσας εργασίας είναι βαθύτατα επίκαιρο. Ζούμε σε μια εποχή όπου όλοι αναζητούν όλο και περισσότερα δεδομένα όμως ο τρόπος που τα αποκτούν δεν είναι ευδιάκριτος (Modderkolk, 2023, σ. 25). Η βιομηχανία εμπορικών spyware αναπτύσσεται με ρυθμούς που ξεπερνούν κατά πολύ τη ρυθμιστική ικανότητα των κρατών (Mildebrath, 2022, pp. 18-25). Νέες τεχνολογίες που αξιοποιούν τεχνητή νοημοσύνη καθιστούν την αορατητα της παρακολούθησης ακόμα πιο απόλυτη. Ταυτόχρονα, η παγκόσμια αντίδραση παραμένει αποσπασματική με μεμονωμένες καταδίκες, ανεπαρκείς κανονισμούς, κυβερνήσεις που αρνούνται ευθύνες (European Parliament PEGA Committee, 2023).

Η εγκληματολογική προσέγγιση που υιοθετεί η παρούσα εργασία έχει μια συγκεκριμένη αξία σε αυτό το πλαίσιο, αποδεσμεύοντας την ανάλυση από την τεχνοκρατική λογική και στρέφοντας σε ερωτήσεις που πραγματικά έχουν σημασία, ποιος επωφελείται, ποιος πλήττεται, ποιοι μηχανισμοί εξουσίας διευκολύνουν την ατιμωρησία και, τελικά, τι σημαίνει για μια κοινωνία να ζει υπό πανοπτικισμό, ακόμα και αν αυτός είναι αναδρομικός. Η εγκληματολογία των ισχυρών έχει επανειλημμένα υπογραμμίσει ότι η κοινωνική βλάβη που προκαλείται από κρατικούς και εταιρικούς δρώντες υπερβαίνει κατά πολύ εκείνη του συμβατικού εγκλήματος αλλά παραμένει συστηματικά υποαντιπροσωπευμένη στην ποινική δίωξη και στη δημόσια συζήτηση (Γεωργούλας, 2019, σ. 46). Η κρατική παρακολούθηση μέσω εμπορικών spyware αποτελεί ένα από τα πιο χαρακτηριστικά παραδείγματα αυτής της δομικής ατιμωρησίας στη ψηφιακή εποχή. Η εγκληματολογική αναγνώριση της παράνομης χρήσης λογισμικών παρακολούθησης και του data laundering ως κατηγορίας κρατικο-εταιρικού εγκλήματος και όχι απλώς ως τεχνικής ή νομικής παράβασης αποτελεί αναγκαία προϋπόθεση για την ουσιαστική αντιμετώπισή του. Αυτή είναι η συμβολή που επιδιώκει η παρούσα εργασία.

ΚΕΦΑΛΑΙΟ 1: Θεωρητικό Πλαίσιο – Κριτική Εγκληματολογία και Εξουσία

Η κατανόηση του data laundering ως σύγχρονης μορφής κρατικο-εταιρικού εγκλήματος απαιτεί αρχικά τη χαρτογράφηση του θεωρητικού πλαισίου εντός του οποίου το φαινόμενο αναλύεται. Το παρόν κεφάλαιο παρουσιάζει την εξέλιξη της εγκληματολογικής σκέψης από το έγκλημα λευκού κολλάρου στο κρατικο-εταιρικό έγκλημα, αναπτύσσει το θεωρητικό μοντέλο των Kramer και Michalowski και εξετάζει πώς η ψηφιακή εποχή αναδιαμορφώνει και επεκτείνει αυτές τις κατηγορίες.

1.1 Από το Έγκλημα Λευκού Κολλάρου στο Κρατικό Έγκλημα

Η εγκληματολογία των ισχυρών ξεκινά από τη συμβολή του Edwin Sutherland (1949), ο οποίος εισήγαγε την έννοια του «εγκλήματος λευκού κολλάρου» για να αμφισβητήσει την κρατούσα αντίληψη ότι το έγκλημα αποτελεί αποκλειστικό φαινόμενο των κατώτερων κοινωνικών στρωμάτων. Ο Sutherland κατέδειξε ότι εγκλήματα με τεράστιες κοινωνικές και οικονομικές συνέπειες τελούνται από πρόσωπα και οργανισμούς υψηλής κοινωνικής θέσης και παραμένουν συστηματικά υποαντιπροσωπευμένα στη δικαστική δίωξη και στη δημόσια ατζέντα (Sutherland, 1949). Η παρατήρηση αυτή είναι βαθύτατα πολιτική καθώς αποκαλύπτει ότι το σύστημα ποινικής δικαιοσύνης δεν είναι ουδέτερο αλλά αντανακλά τις κοινωνικές ανισότητες που καλείται υποτίθεται να ρυθμίσει. Η κυρίαρχη ιδεολογία, κοινή για την κυβέρνηση και τις επιχειρηματικές ελίτ, λειτουργεί ως επαρκές εμπόδιο για την ουσιαστική δίωξη των εγκλημάτων λευκού κολλάρου, νομιμοποιώντας κατ' ουσίαν την εγκληματικότητα των ισχυρών (Γεωργούλας, 2019, σ. 58) Η εγκληματολογία των ισχυρών αποκαλύπτει έτσι τον μονόπλευρο προσανατολισμό του ποινικού συστήματος στην τιμωρία συμπεριφορών των κατώτερων στρωμάτων και τη συστηματική παραμέληση των πολλαπλώς επιβλαβών δράσεων των ανώτερων. Ο Reiman παραλληλίζει χαρακτηριστικά το σύστημα ποινικής δικαιοσύνης με παραμορφωτικό καθρέφτη που μεγεθύνει την επικινδυνότητα της εγκληματικότητας των φτωχών, σμικρύνοντας παράλληλα εκείνη των ισχυρών (Χουλιάρας, 2019, σ. 67). Η παρατήρηση αυτή αποτέλεσε αφετηρία για μια παράδοση εγκληματολογικής σκέψης που σταδιακά επεξέτεινε την ανάλυση από τα άτομα στο ίδιο το κράτος. Η θεωρία της εγκληματικότητας των ισχυρών δεν ήρθε απλώς να καλύψει ένα κενό στην εγκληματολογική έρευνα αλλά αποτέλεσε απόρροια μιας βαθύτερης επιστημολογικής στροφής που μετέθεσε το ερευνητικό ενδιαφέρον από το άτομο στο κράτος και στον τρόπο με τον οποίο αυτό οριοθετεί και αντιμετωπίζει το εγκληματικό φαινόμενο, τόσο μέσω της νομοθετικής παραγωγής όσο και μέσω της κινητοποίησης των θεσμών αντεγκληματικής πολιτικής (Χουλιάρας, 2019, σ. 64).

Το αποφασιστικό βήμα για την αναγνώριση του κράτους ως εγκληματικού δρώντα έγινε το 1989, από τον Chambliss ο οποίος εισήγαγε την έννοια του «κρατικά οργανωμένου εγκλήματος» (Chambliss, 1989). Ο Chambliss όρισε το κρατικά οργανωμένο έγκλημα ως πράξεις που τελούνται από κυβερνητικούς αξιωματούχους κατά την άσκηση των θεσμικών τους

καθηκόντων και που συνιστούν ποινικές παραβάσεις, ακόμα και αν ποτέ δεν διωχθούν ή καταδικαστούν. Εμπειρικά παραδείγματα που ανέλυσε περιελάμβαναν κρατική εμπλοκή σε διακίνηση ναρκωτικών, παρανόμους πολέμους και πολιτικές δολοφονίες, δείχνοντας ότι η εγκληματικότητα των κρατικών δρώντων δεν είναι εξαίρεση αλλά δομικό χαρακτηριστικό ορισμένων συστημάτων εξουσίας. Κρίσιμη πτυχή της ανάλυσης του Chambliss είναι η επισήμανση ότι νόμοι που αντιτίθενται στην επεκτατική λογική της αγοράς και των κρατικών συμφερόντων είναι εκ των πραγμάτων καταδικασμένοι να παραμένουν ανεφάρμοστοι, εξαιτίας της δομικής έλλειψης πολιτικής βούλησης (Chambliss, 1989, pp. 183-208). Η εγκληματικότητα των ισχυρών δεν αποτελεί παρέκκλιση από τον κανόνα αλλά συστατικό στοιχείο της λειτουργίας του ίδιου του συστήματος.

Οι Green και Ward (2004) προχώρησαν ένα βήμα παραπέρα, ορίζοντας το κρατικό έγκλημα ως «παραβίαση ανθρωπίνων δικαιωμάτων που διαπράττεται ή διευκολύνεται από κρατικούς δρώντες» (Green, & Ward, 2004, p. 3). Ο ορισμός αυτός είναι εκ προθέσεως ευρύτερος από τον νομικό ορισμό του ποινικού αδικήματος. Αναγνωρίζει ότι τα κράτη έχουν τη δυνατότητα να ορίζουν τι είναι «νόμιμο» στη δικαιοδοσία τους, και επομένως η αποκλειστική εξάρτηση από ποινικές κατηγορίες για την αναγνώριση κρατικής εγκληματικότητας οδηγεί σε δομική υποεκτίμηση του φαινομένου. Έτσι, σύμφωνα με τους Green και Ward, κρατικό έγκλημα συντελείται όταν κρατικοί δρώντες παραβιάζουν αναγνωρισμένα ανθρώπινα δικαιώματα, ανεξαρτήτως εάν η πράξη τους ορίζεται ως παράνομη από το εθνικό δίκαιο. Η προσέγγιση αυτή είναι ιδιαίτερα σημαντική για την παρούσα εργασία καθώς η χρήση εμπορικών spyware κατά δημοσιογράφων και πολιτικών αντιπάλων μπορεί να μην συνιστά τυπική ποινική παράβαση βάσει της εκάστοτε εθνικής νομοθεσίας, συνιστά όμως παραβίαση του δικαιώματος στην ιδιωτικότητα και της ελευθερίας έκφρασης, δικαιωμάτων που κατοχυρώνονται στο άρθρο 8 της ΕΣΔΑ. Κρίσιμη παράμετρος στην ανάλυση των Green και Ward είναι η έννοια της θεσμικής ατιμωρησίας. Το κράτος που παραβιάζει ανθρώπινα δικαιώματα σπάνια λογοδοτεί, διότι ελέγχει τους ίδιους τους μηχανισμούς λογοδοσίας, αναδεικνύοντας ότι η απουσία λογοδοσίας δεν είναι τυχαία αλλά δομικά παραγόμενη από τα ίδια τα συστήματα εξουσίας που τελούν το έγκλημα (Green, & Ward , 2004, pp. 2-3).

1.2 Το Μοντέλο Kramer-Michalowski

Το 1990, οι Kramer και Michalowski εισήγαγαν την έννοια του «κρατικο-εταιρικού εγκλήματος» για να περιγράψουν μια κατηγορία κοινωνικής βλάβης που προκύπτει από την αλληλεπίδραση κρατικών και εταιρικών θεσμών (Kramer & Michalowski, 2006). Η κεντρική τους θέση ήταν ότι ορισμένες από τις σοβαρότερες μορφές κοινωνικής βλάβης δεν μπορούν να ερμηνευθούν ούτε ως «κρατικό» ούτε ως «εταιρικό» έγκλημα μόνα τους. Απαιτούν ανάλυση της δομικής σύμπλευσης κρατικής εξουσίας και εταιρικής δράσης, που αμοιβαία αλληλοτροφοδοτούνται και καλύπτουν η μία την άλλη, καθώς η λειτουργία τους στο συγχρονο

καπιταλισμό είναι αλληλένδετη (Χουλιάρας,, 2019) Το βασικό στοιχείο αυτής της θεωρητικής πρότασης είναι η κατανόηση ότι καμία μοντέρνα επιχείρηση δεν μπορεί να αναπτυχθεί και να λειτουργήσει χωρίς την πολυποίκιλη στήριξη της κυβέρνησης, ενώ καμία κυβέρνηση στον σύγχρονο καπιταλισμό δεν μπορεί παρά να εξαρτάται από τις επιχειρήσεις για την παροχή αγαθών και υπηρεσιών (Γεωργούλας, 2019, σ. 48). Η αλληλεξάρτηση αυτή δεν είναι απλώς οικονομική· είναι και πολιτική, καθώς κράτος και αγορά συνδιαμορφώνουν το ρυθμιστικό πλαίσιο που υποτίθεται ότι ελέγχει τη σχέση τους.

Κεντρική στη θεωρία είναι η διάκριση δύο βασικών τύπων κρατικο-εταιρικού εγκλήματος (Kramer, Michalowski, & Kauzlarich, 2002). Το κρατικά εκκινούμενο έγκλημα (state-initiated crime) συμβαίνει όταν κρατικοί φορείς χρησιμοποιούν εταιρείες ως εκτελεστικά όργανα για τη διάπραξη εγκλημάτων που εξυπηρετούν κρατικούς σκοπούς. Όταν δηλαδή ιδιωτικές εταιρείες υπό την καθοδήγηση ή σιωπηρή έγκριση της κυβέρνησης προβαίνουν σε παρεκκλίνουσα δράση. Το κρατικά διευκολυνόμενο έγκλημα (state-facilitated crime) συμβαίνει όταν η κρατική αδράνεια, η ρυθμιστική ανεπάρκεια ή η ενεργητική κάλυψη επιτρέπουν σε εταιρείες να παραβιάζουν νόμους ή κοινωνικούς κανόνες χωρίς συνέπειες (Χουλιάρας,, 2019, σ. 78). Η διάκριση αυτή είναι αναλυτικά κρίσιμη, διότι αναγνωρίζει ότι η κρατική εμπλοκή σε εταιρικά εγκλήματα δεν απαιτεί απαραίτητα ενεργητική συμμετοχή· η παθητική διευκόλυνση μέσω σκόπιμης ρυθμιστικής αδράνειας αποτελεί εξίσου μορφή εγκληματικής ευθύνης. Η δεύτερη περίπτωση, άλλωστε, είναι μια κανονικότητα στη λειτουργία κρατών (Γεωργούλας, 2019, σ. 49). Όπως θα αναδειχθεί στο Κεφάλαιο 6, η ελληνική περίπτωση Predatorgate ενσαρκώνει και τους δύο τύπους ταυτόχρονα.

Για να ερμηνεύσουν αιτιολογικά το κρατικο-εταιρικό έγκλημα, οι Kramer και Michalowski πρότειναν ένα μοντέλο τριών αλληλεπιδρώντων παραγόντων, κανένας από τους οποίους δεν επαρκεί μόνος του (Kramer, Michalowski, & Kauzlarich, 2002). Ο πρώτος παράγοντας είναι το κίνητρο. Σε αντίθεση με εξηγήσεις που εστιάζουν στις ατομικές προθέσεις, οι Kramer και Michalowski επισημαίνουν τις θεσμικές πιέσεις που βιώνουν οι οργανισμοί, δηλαδή την ανάγκη για πολιτική εξουσία, οικονομικό κέρδος ή ανταγωνιστικό πλεονέκτημα. Στη βιομηχανία spyware το κίνητρο είναι αμοιβαίο και δομικά ενισχυόμενο, καθώς το κράτος επιδιώκει την παρακολούθηση και η εταιρεία την πώληση, δημιουργώντας μια σχέση αλληλεξάρτησης που εξυπηρετεί τα συμφέροντα και των δύο πλευρών. Σύμφωνα με τους Kauzlarich και Matthews, το κυνήγι του κέρδους μπορεί να οδηγήσει σε πολιτικές και πρακτικές επιβλαβείς για μεγάλες ομάδες πληθυσμού, ενώ οι ευκαιρίες διάπραξης πολλαπλασιάζονται από τον ελλιπή κοινωνικό έλεγχο ή από την παντελή απουσία του που πηγάζει από μια αλληλεξάρτηση ελεγκτή και ελεγχομένου (Γεωργούλας, 2019, σ. 49).

Ο δεύτερος παράγοντας είναι η ευκαιρία. Τα ρυθμιστικά κενά, η τεχνολογική πολυπλοκότητα και οι αδιαφανείς εταιρικές δομές δεν αποτελούν τυχαία χαρακτηριστικά της

αγοράς spyware, αλλά δομικές προϋποθέσεις που επιτρέπουν στην παράνομη δράση να παραμένει αόρατη και ατιμώρητη.

Ο τρίτος παράγοντας, η αποτυχία αποτελεσματικού ελέγχου, είναι ίσως ο πιο καθοριστικός. Η απλή ύπαρξη νόμων δεν επαρκεί όταν απουσιάζει η ανεξάρτητη εποπτεία, η δικαστική λογοδοσία και η κοινωνική πίεση που θα μπορούσαν να αποτρέψουν τη διάπραξη (Kramer, Michalowski, & Kauzlarich, 2002). Το τρίπτυχο αυτό δεν λειτουργεί αθροιστικά αλλά συστημικά αφού, η παρουσία και των τριών παραγόντων ταυτόχρονα παράγει μια κατάσταση όπου η παράβαση δεν είναι απλώς εφικτή αλλά κατά κάποιον τρόπο δομικά αναπόφευκτη. Η παρέκκλιση κανονικοποιείται, γίνεται ρουτίνα, και το σύστημα αναπαράγει την εγκληματικότητά του χωρίς να τη βλέπει ως εγκληματικότητα (Γεωργούλας, 2019, σ. 50).

Η ελληνική περίπτωση του Predatorgate αποτελεί χαρακτηριστικό παράδειγμα της συνύπαρξης και των τριών παραγόντων: κίνητρο από αμφότερες τις πλευρές, ευκαιρία μέσω της αδιαφανούς δομής της Intellexa, και ουσιαστική απουσία εποπτείας έως την αποκάλυψη του σκανδάλου.

1.3 Εγκληματολογία της Εξουσίας: Από το Λευκό Κολλάρο στη Θεσμική Βία

Η εγκληματολογία των ισχυρών έχει αναπτύξει μια σταδιακά διερευνώμενη τυπολογία της θεσμικής παρανομίας (Friedrichs, 2010). Στο ένα άκρο βρίσκεται το κλασικό έγκλημα λευκού κολλάρου όπως είναι η απάτη, η φοροδιαφυγή και η παράβαση της εργατικής νομοθεσίας, που παρά τις τεράστιες οικονομικές επιπτώσεις του αντιμετωπίζεται ως δευτερεύον ζήτημα σε σχέση με το «συμβατικό» έγκλημα. Στο άλλο άκρο βρίσκεται η θεσμική βία. Πράξεις κρατικών και εταιρικών δρώντων που προκαλούν σοβαρή βλάβη σε ανθρώπινα δικαιώματα, ανθρώπινη αξιοπρέπεια ή ανθρώπινη ζωή, αλλά που κρύβονται πίσω από τη ρητορική της νομιμότητας, της εθνικής ασφάλειας ή του δημοσίου συμφέροντος (Green, & Ward, 2004, pp. 2-3). Το ειδοποιό στοιχείο των εγκλημάτων αυτών συνίσταται στο γεγονός ότι οι δράστες τους διαθέτουν συντριπτικά μεγαλύτερη υλική και συμβολική δύναμη σε σύγκριση με τα θύματά τους, η οποία προκύπτει από την προνομιακή και θεσμική θέση που κατέχουν. Η ατιμωρησία δεν είναι παρά η κορυφή του παγόβουνου· η βάση του αποτελείται από ένα ευρύ σύνολο βίας και ανισότητας, επιτρέποντας τη διατύπωση της υπόθεσης ότι πίσω από την έλλειψη απάντησης του κράτους στο εγκληματικό φαινόμενο βρίσκεται παγιωμένη μια μορφή δομικής αδικίας (Χουλιάρας, 2019, σσ. 71-72).

Η συνέργεια κρατικών και εταιρικών συμφερόντων είναι συστημική καθώς κράτος και αγορά δεν λειτουργούν ανταγωνιστικά αλλά συμβιωτικά. Μοιράζονται κοινούς στόχους και ως εκ τουτου συνεργάζονται προκειμένου να δημιουργούν συνθήκες στις οποίες οι νομικοί και κοινωνικοί κανόνες υποχωρούν όταν εμποδίζουν την επίτευξη αυτών των στόχων (Kramer, Michalowski, & Kauzlarich, 2002, pp. 263-282). Ο Chambliss (1989) είχε επισημάνει ότι νόμοι

που αντιτίθενται στην επεκτατική λογική της αγοράς είναι εκ των πραγμάτων καταδικασμένοι να παραμένουν ανεφάρμοστοι, εξαιτίας της έλλειψης πολιτικής βούλησης (Chambliss, 1989, pp. 183-208). Το αποτέλεσμα είναι μια δομική κατάσταση όπου η παρανομία δεν αποτελεί παρέκκλιση από τον κανόνα αλλά συστατικό στοιχείο της λειτουργίας του συστήματος με άμεση συνέπεια την αποδυνάμωση της νομιμότητας και την εξάπλωση της διαφθοράς (Green, & Ward, 2004).

Κεντρικό χαρακτηριστικό είναι η αναγνώριση ότι οι ισχυροί έχουν τη δυνατότητα να ορίζουν τι είναι εγκληματικό και τι όχι (Rothe, & Friedrichs, 2006). Αυτή η εξουσία αυτο-ορισμού, η ικανότητα να διαμορφώνει κανείς το νομικό πλαίσιο ώστε να εξαιρεί τις δικές του πράξεις από τον ορισμό του «εγκλήματος» αποτελεί τον πιο επικίνδυνο μηχανισμό ατιμωρησίας που η εγκληματολογία των ισχυρών έχει αναγνωρίσει. Στη βιομηχανία spyware αυτός ο μηχανισμός εκδηλώνεται με ιδιαίτερη σαφήνεια. Τα κράτη που χρησιμοποιούν εργαλεία παρακολούθησης κατά των πολιτών τους είναι τα ίδια που ορίζουν τι συνιστά νόμιμη παρακολούθηση.

Η ψηφιακή εποχή δεν επεκτείνει απλώς το πεδίο εφαρμογής του κρατικο-εταιρικού εγκλήματος, αλλά το αναδιαμορφώνει ποιοτικά. Οι βασικές αλλαγές που εισάγει είναι τρείς. Πρώτον, η ψηφιακή τεχνολογία αυξάνει δραματικά τις δυνατότητες συγκάλυψης. Το κρατικο-εταιρικό έγκλημα στη φυσική του μορφή αφήνει πάντα κάποια ίχνη όπως έγγραφα, μάρτυρες, υλικές αποδείξεις. Το ψηφιακό κρατικο-εταιρικό έγκλημα και ιδίως η χρήση spyware τύπου μηδενικού κλίκ (zero-click) μπορεί να τελεστεί σχεδόν χωρίς ίχνη, καθιστώντας την απόδειξη εξαιρετικά δύσκολη (Citizen Lab, 2021). Επιπλέον, η ψηφιακή εποχή δημιουργεί νέες μορφές ιδιωτικοποίησης της κρατικής βίας (Deibert, 2020). Η ανάθεση παρακολούθησης σε εμπορικές εταιρείες όπως η NSO Group και η Intellexa επιτρέπει στο κράτος να εξωτερικεύει την ευθύνη: «δεν παρακολουθήσαμε εμείς, αγοράσαμε ένα εμπορικό προϊόν» (PEGA Committee, 2023, pp. 45-52). Αυτή η δομή αποποίησης ευθύνης είναι ακριβώς αυτό που η θεωρία state-facilitated crime περιγράφει και αυτό που το data laundering νομιμοποιεί. Τέλος, η ψηφιακή εποχή μετατρέπει τα δεδομένα σε όπλο εξουσίας με διαρκείς συνέπειες. Σε αντίθεση με παραδοσιακές μορφές κρατικής βίας, η ψηφιακή παρακολούθηση παράγει βλάβη που συνεχίζεται και μετά τη λήξη της αφού τα δεδομένα που συλλέχθηκαν παραμένουν, μπορούν να χρησιμοποιηθούν, και η γνώση ότι υπήρξαν παράγει διαρκές chilling effect στα θύματα και το ευρύτερο περιβάλλον τους.

Τα παραπάνω καθιστούν απαραίτητη την ανάπτυξη νέων εννοιολογικών εργαλείων για την ανάλυση του ψηφιακού κρατικο-εταιρικού εγκλήματος. Η έννοια του data laundering όπως παρουσιάζεται στην παρούσα εργασία αποτελεί ακριβώς μια τέτοια πρόταση. Μια εννοιολογική κατηγορία που αποτυπώνει τον ειδικό μηχανισμό με τον οποίο το ψηφιακό κρατικο-εταιρικό έγκλημα νομιμοποιεί τα αποτελέσματά του.

Συμπερασματικά, το data laundering αποτελεί ακριβώς αυτό που η θεωρία Kramer-Michalowski περιγράφει ως κρατικο-εταιρικό έγκλημα στη ψηφιακή εποχή. Η σύμπραξη κράτους και εταιρείας δεν είναι απλώς λειτουργική άλλα δομικά αναγκαία. Χωρίς την εταιρεία το κράτος δεν έχει το τεχνικό εργαλείο, χωρίς το κράτος η εταιρεία δεν έχει πελάτη. Και οι δύο επωφελούνται από τον μηχανισμό laundering. Το κράτος επιτυγχάνει τον στόχο της παρακολούθησης χωρίς νομικές συνέπειες, η εταιρεία επιτυγχάνει το οικονομικό κέρδος χωρίς ηθική ευθύνη. Η αποποίηση ευθύνης είναι ο σκοπός αυτής της συνδιαλλαγής (Kramer & Michalowski, 1990 ; Green & Ward, 2004, p 28).

ΚΕΦΑΛΑΙΟ 2: Θεωρίες Επιτήρησης

Για να κατανοηθούν οι κοινωνικές και πολιτικές επιπτώσεις της κρατικής παρακολούθησης μέσω spyware, είναι αναγκαία η προσφυγή στη φουκωική θεωρία της εξουσίας και επιτήρησης. Το παρόν κεφάλαιο παρουσιάζει το κλασικό Πανοπτικόν ως αναλυτική κατηγορία, εξετάζει την εφαρμογή και τα όριά του στη ψηφιακή παρακολούθηση και αναλύει τις εμπειρικά τεκμηριωμένες επιπτώσεις της παρακολούθησης στην ελεύθερη έκφραση και τη δημοκρατία.

2.1 Michel Foucault: εξουσία, γνώση και πειθαρχία

Η ανάλυση της σύγχρονης κρατικής παρακολούθησης και των εμπορικών spyware ως μορφών κρατικο-εταιρικού εγκλήματος προϋποθέτει ένα θεωρητικό πλαίσιο που να αποτυπώνει τις σχέσεις εξουσίας, ελέγχου και υποκειμενικότητας στην ψηφιακή εποχή. Το έργο του Michel Foucault, και ιδιαίτερα η ανάλυσή του για το Πανοπτικόν στο *Επιτήρηση και Τιμωρία* (1975), προσφέρει ένα θεωρητικό υπόβαθρο, χρήσιμο για την ανάλυση της σύγχρονης κυβερνοεπιτήρησης (Foucault, M, 2011). Παρά τη χρονική απόσταση που μας χωρίζει από τη συγγραφή του, οι θεωρητικές κατηγορίες που ανέπτυξε ο Foucault διατηρούν αξιοσημείωτη ερμηνευτική ισχύ απέναντι στα σύγχρονα φαινόμενα ψηφιακής παρακολούθησης.

Το Πανοπτικόν, ως αρχιτεκτονικό σχέδιο, εμφανίστηκε αρχικά στη σκέψη του Jeremy Bentham στα τέλη του 18ου αιώνα. Επρόκειτο για μια φυλακή με έναν κεντρικό πύργο επιτήρησης γύρω από τον οποίο βρίσκονται τα κελιά των κρατουμένων, οι οποίοι είναι ορατοί ανά πάσα στιγμή από τον πύργο, χωρίς να γνωρίζουν αν και πότε παρακολουθούνται. Η γεωμετρία αυτή δεν ήταν απλώς λειτουργική· ήταν, για τον Bentham, η τέλεια μηχανή εξουσίας (Foucault, 2011, σσ. 223-235). Ο Michel Foucault, στο «Επιτήρηση και Τιμωρία» (1975), αξιοποίησε το Πανοπτικόν ως αναλυτικό εργαλείο για να περιγράψει έναν νέο τύπο εξουσίας που χαρακτηρίζει τις σύγχρονες κοινωνίες. Για τον Foucault, το Πανοπτικόν δεν είναι απλώς ένα αρχιτεκτονικό σχέδιο. Είναι το «διάγραμμα» μιας μορφής εξουσίας που λειτουργεί μέσω της ορατότητας. Εκείνος που παρακολουθείται καθίσταται ορατός, ενώ εκείνος που παρακολουθεί παραμένει αόρατος. Αυτή η ασυμμετρία ορατότητας παράγει αυτοπειθαρχία καθώς ο κρατούμενος ρυθμίζει μόνος του τη συμπεριφορά του, ακόμα και όταν κανείς δεν τον κοιτάζει (Foucault, 2011, σσ. 223-260).

Ο Foucault υποστήριξε ότι αυτός ο τύπος εξουσίας δεν περιορίζεται στη φυλακή αλλά διαχέεται σε όλους τους σύγχρονους θεσμούς. Η συνεχής καταγραφή, ταξινόμηση και αξιολόγηση ατόμων δημιουργεί μια «κανονική» συμπεριφορά από την οποία οποιαδήποτε απόκλιση καθίσταται ορατή και επιδεκτική επέμβασης (Foucault, 2011).

Η ανάλυση Foucault για το πανοπτικον τοποθετεί την επιτήρηση στο πλαίσιο μιας διακεκριμένης θεωρίας της εξουσίας (Haggerty & Ericson, 2000, p. 607) Σε αντίθεση με την

κλασική αντίληψη της εξουσίας ως κάτι που κατέχεται και ασκείται από τα πάνω προς τα κάτω, ο Foucault περιγράφει μια μορφή εξουσίας που λειτουργεί μέσω της γνώσης και της ορατότητας. Η εξουσία δεν επιβάλλεται με τη βία αλλά παράγεται μέσω της συνεχούς παρακολούθησης, καταγραφής και ταξινόμησης των υποκειμένων. Αυτό που καθιστά το Πανοπτικόν τόσο σημαντικό αναλυτικά δεν είναι η συγκεκριμένη αρχιτεκτονική του αλλά η γενικεύσιμη αρχή που ενσαρκώνει. Συγκεκριμένα, ότι η αίσθηση της συνεχούς δυνατότητας παρακολούθησης επαρκεί για να παραχθεί υπακοή, ανεξαρτήτως του αν η παρακολούθηση πράγματι λαμβάνει χώρα (Foucault, 2011, σσ. 223-260). Ο Foucault αποκαλεί αυτή τη διαδικασία «κανονικοποίηση» καθώς, το υποκείμενο εσωτερικεύει τον κανόνα και αυτορυθμίζει τη συμπεριφορά του, καθιστώντας περιττή την ενεργό επέμβαση της εξουσίας. Είναι ακριβώς αυτή η λογική που οι Haggerty και Ericson (2000) επεκτείνουν στη σύγχρονη ψηφιακή επιτήρηση, υποστηρίζοντας ότι το σύγχρονο «surveillant assemblage» αναπαράγει και εντείνει την πανοπτική δυναμική σε κλίμακα που ο Foucault δεν μπορούσε να προβλέψει.

Η έννοια του data laundering, προσφέρει ένα ιδιαίτερα γόνιμο θεωρητικό εργαλείο για την κατανόηση των σύγχρονων μορφών κρατικής επιτήρησης (Simmons, 2009;Lyon, 2018). Το spyware δεν είναι απλώς ψηφιακό πανόπτικον. Είναι κρυφό πανόπτικον που συνδυάζει φουκωική βιοεξουσία με εταιρική ατιμωρησία, με το data laundering να είναι ο μηχανισμός που το καθιστά αόρατο και νόμιμο. Στο πανόπτικον, η αυτοπειθαρχία λειτουργεί εκ των προτέρων καθώς ο κρατούμενος γνωρίζει ότι παρακολουθείται ενώ στο spyware η αυτοπειθαρχία έρχεται εκ των υστέρων, αναδρομικά, μετα την αποκάλυψη των σκανδάλων.

Πιο συγκεκριμένα, τα λογισμικά spyware τύπου predator που επιτρέπουν πλήρη έλεγχο κινητών, ενσαρκώνουν μια μεταπειθαρχική μορφή επιτήρησης (Lyon, 2018). Τα spyware δεν λειτουργούν απλώς πειθαρχικά, υπό την έννοια παρακολουθώ για να ελέγξω, αλλά βιοπολιτικά, παρακολουθώ για να προβλέψω και να χαρτογραφήσω δίκτυα (Foucault, 2011). Σε αντίθεση με το Πανόπτικον κατά τη χρήση spyware το υποκείμενο αγνοεί ότι παρακολουθείται γεγονός που οδηγεί σε απόλυτη συγκέντρωση πληροφορίας και αδυναμία αυτοπροστασίας. Συνεπώς, το υποκείμενο οδηγείται στην αυτοπειθαρχία, ως αποτέλεσμα της δομικής επισφάλειας της ψηφιακής εποχής. Με τη χρήση τέτοιων λογισμικών και την άντληση δεδομένων χωρίς τη γνώση των υποκειμένων η εξουσία δεν χρειάζεται να περιορίσει το σώμα, αρκεί να κατέχει το πληροφοριακό αποτύπωμα. Το πανοπτικον στόχο έχει μέσω του φόβου της οπτικής επιτήρησης, καθώς οι κρατούμενοι δεν γνωρίζουν πότε παρακολουθούνται, ο κρατούμενος να αυτοπειθαρχείται. Σήμερα, η επιτήρηση συνδέεται με κάμερες παρακολούθησης, ψηφιακά δεδομένα, μέσα κοινωνικής δικτύωσης και αλγοριθμικό έλεγχο. Έτσι, η πειθαρχική εξουσία στο σήμερα λειτουργεί διαρκώς και αόρατα και βασίζεται στην επιτήρηση ως τεχνική διακυβέρνησης. Συνεπώς, η ψηφιακή επιτήρηση λειτουργεί αντίστοιχα με το πανόπτικον, όπου ο κεντρικός πύργος της φυλακής είναι τα δίκτυα, η φυλακή είναι ο κυβερνοχώρος και η άμεση επιτήρηση

αντιστοιχεί στην αλγοριθμική επεξεργασία δεδομένων. Δημιουργεί προφίλ, κατασκευάζει κατηγορίες απειλής και παράγει ύποπτα υποκείμενα μέσω δεδομένων.

Η χρήση των spyware σε πολιτικά πρόσωπα και δημοσιογράφους υπονομεύει το κράτος δικαίου και διαβρώνει την ιδιωτικότητα ως όρο ελευθερίας. Έτσι η επιτήρηση μετατρέπεται σε μηχανισμό πολιτικής κυριαρχίας μέσω της πληροφορίας. Το σύγχρονο πανόπτικον, τα λογισμικά παρακολούθησης, μπορούν να θεωρηθούν συνέχεια της πειθαρχικής λογικής της επιτήρησης. Η μεταπειθαρχική μορφή της επιτήρησης ταυτίζεται με τη μετάβαση σε ψηφιακή κοινωνία ελέγχου (Lyon, 2018).

Η σύγχρονη βιβλιογραφία έχει αναδείξει τις ισχυρές ομοιότητες μεταξύ του φουκωικού Πανόπτικου και της ψηφιακής παρακολούθησης (Lyon, D, 2007, pp. 57-72)[1]. Η βασική ομοιότητα είναι δομική αφού και στις δύο περιπτώσεις, εκείνος που παρακολουθεί παραμένει αόρατος ενώ εκείνος που παρακολουθείται εκτίθεται. Το κράτος που χρησιμοποιεί spyware γνωρίζει τα πάντα για τον στόχο ενώ ο στόχος αγνοεί τελείως ότι παρακολουθείται. Αυτή η ριζική ασυμμετρία γνώσης είναι η σύγχρονη εκδοχή του πανοπτικού βλέμματος.

Επιπλέον, η ψηφιακή παρακολούθηση όπως και το Πανόπτικον, δεν χρειάζεται να είναι συνεχής για να είναι αποτελεσματική. Αρκεί η γνώση ότι είναι δυνατή. Όταν ένας δημοσιογράφος μαθαίνει ότι άλλοι δημοσιογράφοι παρακολουθούνται, αρχίζει να συμπεριφέρεται σαν να παρακολουθείται και ο ίδιος, όπως συμβαίνει ακριβώς στη πανοπτική αυτοπειθαρχία που περιέγραφε ο Foucault (Penney, 2016, p. 167 ; PEN America , 2013)

Υπάρχουν όμως και σημαντικές διαφορές που η εγκληματολογική ανάλυση οφείλει να αναγνωρίσει. Το Πανοπτικόν του Bentham είναι ορατό στον κρατούμενο καθώς αυτός βλέπει τον κεντρικό πύργο, γνωρίζει ότι υπάρχει φύλακας, κατανοεί τη δομή της εξουσίας. Αυτή ακριβώς η ορατότητα της αρχιτεκτονικής παράγει την αυτοπειθαρχία (Kaldani & Prokopets, 2022, p. 8).[2] Αντίθετα, το spyware είναι εξ ορισμού αόρατο κατά τη διάρκεια της λειτουργίας του. Το θύμα δεν γνωρίζει ότι παρακολουθείται και άρα δεν αυτοπειθαρχείται κατά τη διάρκεια της παρακολούθησης.

Το αποτέλεσμα όμως αλλάζει μετά την αποκάλυψη, όταν δηλαδή σκάνδαλα όπως το Predatorgate γίνονται δημόσια γνωστά. Εμπειρικές μελέτες έχουν τεκμηριώσει ότι η γνώση ότι η παρακολούθηση υπήρξε ή μπορεί να υπάρχει, παράγει μετρήσιμο chilling effect με αποτέλεσμα την αυτολογοκρισία, αποφυγή ευαίσθητων επικοινωνιών, μείωση δημοσιογραφικής έρευνας (Deibert, 2020, pp. 96-98). Η πανοπτική αυτοπειθαρχία δεν απαιτεί πλέον αρχιτεκτονικό πύργο.

[1] Ο Lyon υποστηρίζει ότι το φουκωικό Πανοπτικόν παραμένει το πιο επιδραστικό θεωρητικό εργαλείο για την ανάλυση της παρακολούθησης, αλλά χρειάζεται επικαιροποίηση για να αποτυπώσει τη δικτυακή, αποκεντρωμένη φύση της ψηφιακής επιτήρησης

[2] Οι συγγραφείς αναφέρονται ρητά στη φουκωική λογική της επιτήρησης για να περιγράψουν τον τρόπο με τον οποίο το Pegasus παράγει «συνθήκες συνεχούς υποτέλειας» στα θύματά του.

Αρκεί η γνώση ότι η παρακολούθηση είναι τεχνικά δυνατή και πολιτικά εφικτή (Penney, 2016, pp. 155-165 ; Stoycheff, 2016, pp. 304-308)

Από εγκληματολογική σκοπιά, η σύνδεση αυτή είναι κρίσιμη για δύο λόγους. Αναδεικνύει ότι η κοινωνική βλάβη του spyware δεν περιορίζεται στα άμεσα θύματα αλλά επεκτείνεται σε κάθε πολίτη, δημοσιογράφο ή ακτιβιστή που μαθαίνει για την ύπαρξή του και αλλάζει συμπεριφορά. Επιπλέον, και πιο σημαντικό για την παρούσα εργασία, η πανοπτική λογική εξηγεί γιατί το data laundering είναι τόσο επικίνδυνο. Όσο η παρακολούθηση παραμένει αδιαφανής, όσο τα δεδομένα «ξεπλένονται» και η καταγωγή τους αποκρύπτεται, τόσο η κοινωνική βλάβη συνεχίζεται χωρίς τη γνώση εκείνων που την υφίστανται (Bauman, & Lyon, 2013, p. 67).

Τέλος, η ψηφιακή παρακολούθηση μέσω spyware είναι πολυεπίπεδη. Κράτη, εταιρείες, μεσάζοντες (intermediaries) κανένας δεν είναι «ο φύλακας στον πύργο» (Mathiesen, 1997, pp. 215-220). Το Πανοπτικόν παρακολουθεί δεκάδες κρατούμενους. Τα σύγχρονα spyware έχουν χρησιμοποιηθεί σε χιλιάδες στόχους παγκοσμίως και επηρεάζουν εκατομμύρια τρίτους.

2.2 Chilling effect και επιπτώσεις

Η φουκωική θεωρία της αυτοπειθαρχίας βρίσκει εμπειρική επιβεβαίωση στην ανεπτυγμένη βιβλιογραφία για το λεγόμενο «chilling effect», δηλαδή την αποτρεπτική επίδραση που η γνώση παρακολούθησης ασκεί στην ελεύθερη έκφραση και συμπεριφορά (Deibert, 2020, pp. 93-100).[3]

Σε μια θεμελιώδη μελέτη, ο Penney (2016) τεκμηρίωσε εμπειρικά ότι μετά τις αποκαλύψεις Snowden (2013) για μαζική παρακολούθηση της NSA, οι αναζητήσεις στη Wikipedia για θέματα που χαρακτηρίστηκαν «ευαίσθητα» μειώθηκαν κατά περίπου 20% σε σύγκριση με χώρες εκτός της αμερικανικής επικράτειας (Penney, 2016). Η μελέτη της Stoycheff (2016) ενίσχυσε αυτά τα ευρήματα, δείχνοντας ότι άτομα που πιστεύουν ότι παρακολουθούνται είναι σημαντικά λιγότερο πιθανό να εκφράσουν μειοψηφικές απόψεις ακόμα και ανώνυμα στο διαδίκτυο (Stoycheff, 2016).

Αυτά τα ευρήματα έχουν άμεση σχέση με την ελληνική περίπτωση. Το chilling effect δεν αφορά μόνο τα άμεσα θύματα παρακολούθησης, αφορά κάθε δημοσιογράφο, ακτιβιστή ή πολίτη που μαθαίνει για την ύπαρξη του Predator και αρχίζει να αυτολογοκρίνεται (Bauman, & Lyon, 2013).[4] Η σύνθεση της φουκωικής θεωρίας με τα εμπειρικά δεδομένα για το chilling effect οδηγεί σε μια σοβαρή εγκληματολογική και πολιτική διαπίστωση ότι η κρατική παρακολούθηση μέσω spyware δεν προκαλεί μόνο ατομική βλάβη στα θύματά της αλλά απειλεί τη δημόσια σφαίρα στο

[3] Ο Deibert περιγράφει πώς η γνώση ότι κάποιος παρακολουθείται ή ότι μπορεί να παρακολουθείται , αλλάζει τη συμπεριφορά ακόμα και εκείνων που δεν έχουν κάνει τίποτα παράνομο

[4] Οι συγγραφείς εξετάζουν πώς ο φόβος παρακολούθησης γίνεται αυτοτροφοδοτούμενος: η αβεβαιότητα για το αν κάποιος παρακολουθείται είναι από μόνη της αρκετή για να αλλάξει συμπεριφορά.

σύνολό της. Δημοσιογράφοι που δεν μπορούν να επικοινωνούν ασφαλώς με τις πηγές τους, αντιπολίτευση που αδυνατεί να συντονιστεί χωρίς φόβο παρακολούθησης, πληροφοριοδότες που αποθαρρύνονται, δεν αποτελούν ατομικές παρενέργειες αλλά συστηματικές επιθέσεις στη δημοκρατική λειτουργία (IPI, 2023). Η πτώση της Ελλάδας στον δείκτη ελευθερίας Τύπου της RSF, από την 70η θέση το 2021 στην 107η το 2023, αποτελεί μετρήσιμη ένδειξη αυτής της διαδικασίας (Reporters Without Borders, 2023).

Εντός του θεωρητικού πλαισίου της παρούσας εργασίας, αυτή η διαπίστωση συνδέεται άμεσα με το data laundering καθώς η νομιμοποίηση παράνομων δεδομένων δεν επιτρέπει μόνο την τέλεση εγκλημάτων χωρίς συνέπειες. Επιτρέπει τη διαρκή άσκηση εξουσίας μέσω του φόβου που η αποκάλυψη των εγκλημάτων παράγει. Το ψηφιακό Πανοπτικόν, σε αντίθεση με το αρχιτεκτονικό πρότυπο του Bentham, δεν χρειάζεται να λειτουργεί συνεχώς για να είναι αποτελεσματικό. Αρκεί να έχει λειτουργήσει μια φορά και να γίνει γνωστό. Οι κοινωνίες κινδυνεύουν να καταλήξουν, αν δεν προστατευθούν αποτελεσματικά τα θεμελιώδη δικαιώματα, σε δυστοπίες τύπου Πανόπτικον (Παπανικολάου, 2025, σ. 643).

Το παράδειγμα του predatorgate δείχνει πως τα παρανόμως κτηθέντα δεδομένα μέσω κατασκοπευτικών λογισμικών ακόμα και αν αποτελούν προϊόν παράνομης παρακολούθησης μπορούν να ενσωματώνονται σε επίσημες διαδικασίες ή να χρησιμοποιούνται χωρίς πλήρη διαφάνεια συμβάλλοντας στην αποδυνάμωση της προστασίας της ιδιωτικότητας και των δημοκρατικών εγγυήσεων (Χονδρογιάννης , 2023)

ΚΕΦΑΛΑΙΟ 3: Data Laundering: Εννοιολογική Αποσαφήνιση και Αναλυτικό Πλαίσιο

Η έννοια του data laundering αποτελεί τον εννοιολογικό πυρήνα της παρούσας εργασίας. Το παρόν κεφάλαιο αποσαφηνίζει τον ορισμό και την προέλευση της έννοιας, αναπτύσσει τη δομική αναλογία με το money laundering, αναλύει τα τρία στάδια λειτουργίας του, και εξετάζει τα νομικά και ηθικά κενά που καθιστούν το φαινόμενο δυσχερώς αντιμετωπίσιμο.

3.1 Ορισμός και λειτουργία του data laundering

Ο όρος «data laundering», «ξέπλυμα δεδομένων», αναφέρεται στη διαδικασία μέσω της οποίας δεδομένα που αποκτήθηκαν παράνομα, αντιδεοντολογικά ή χωρίς νόμιμη βάση εισέρχονται σε νόμιμες ροές πληροφοριών, με τρόπο που αποκρύπτει την παράνομη καταγωγή τους και νομιμοποιεί τη χρήση τους κατά τη μέθοδο που το Money laundering λειτουργεί (SWAMI, 2006, pp. 96,136; FATF, 2012). Η λογική αυτή εντοπίζεται και στην έννοια του «surveillance laundering», όπου κράτη ή υπηρεσίες «ξεπλένουν» παράνομη παρακολούθηση δρομολογώντας τη μέσω τρίτων χωρών ή ιδιωτικών φορέων με χαλαρότερο νομικό πλαίσιο, ώστε τα δεδομένα να επανεμφανίζονται ως νόμιμα (Harper, Ellis, & Tucker, 2021, pp. 185-186)

Η πρώτη χρήση του ορισμού έγινε το 2006 (swami) και εξηγούσε την αγορά παράνομων δεδομένων από εμπορικές εταιρείες. Το φαινόμενο ορίστηκε ως η διαδικασία μέσω της οποίας παράνομη προέλευση προσωπικών δεδομένων αποκρύπτεται μέσω πλήθους συναλλαγών ώστε τα δεδομένα να εμφανίζονται νόμιμα ακριβώς όπως συμβαίνει στο ξέπλυμα χρήματος (SWAMI, 2006, pp. 96,138). Ως εννοιολογική κατηγορία, το data laundering δεν έχει ακόμη αποκρυσταλλωθεί στην ακαδημαϊκή βιβλιογραφία με ενιαίο τρόπο. Ωστόσο, η διαδικασία που περιγράφει είναι αναγνωρίσιμη σε πολλαπλά πλαίσια όπως στην εμπορική εκμετάλλευση δεδομένων που συλλέχθηκαν για άλλον σκοπό (Lyon, 2001), στη χρήση δεδομένων αποκτηθέντων από παράνομες υποκλοπές σε δικαστικές διαδικασίες (Panzavolta, & Maes, 2022), και στην κρατική αξιοποίηση δεδομένων που αποκτήθηκαν μέσω εμπορικών spyware εκτός νόμιμου πλαισίου.

3.2 Νομιμοποίηση παράνομων ροών δεδομένων

Η αναλογία με το money laundering δεν είναι απλώς ρητορική. Είναι δομική και αναλυτικά παραγωγική. Το money laundering, όπως ορίζεται από τον FATF, είναι η διαδικασία μέσω της οποίας εγκληματικά έσοδα μετατρέπονται σε φαινομενικά νόμιμα περιουσιακά στοιχεία (FATF, 2012). Η παράλληλη διαδικασία στο data laundering αφορά τα δεδομένα παράνομης προέλευσης που μετατρέπονται σε φαινομενικά νόμιμη πληροφορία, αξιοποιήσιμη από κρατικούς και εταιρικούς δρώντες χωρίς νομικές συνέπειες(SWAMI, 2006, p. 138).

Η αναλογία λειτουργεί σε τρία επίπεδα. Στο επίπεδο της λειτουργίας και τα δύο φαινόμενα μετατρέπουν κάτι παράνομο σε φαινομενικά νόμιμο μέσω διαδοχικών σταδίων απόκρυψης. Στο επίπεδο της δομής και τα δύο αξιοποιούν νόμιμες δομές όπως χρηματοπιστωτικά ιδρύματα ή νόμιμες εξαιρέσεις για να αποκρύψουν την παράνομη καταγωγή. Στο επίπεδο της ατιμωρησίας και τα δύο ωφελούνται από τη δυσκολία απόδειξης αφού στο money laundering αποκρύπτεται η προέλευση χρημάτων και στο data laundering αποκρύπτεται η προέλευση πληροφοριών.

Αυτή η αναλογία με το money laundering δεν είναι μόνο εννοιολογική αλλά είναι και εγκληματολογικά παραγωγική καθώς αναδεικνύει γιατί το data laundering συνιστά κρατικο-εταιρικό και όχι απλώς κρατικό έγκλημα. Όπως στο money laundering, η νομιμοποίηση παράνομων εσόδων απαιτεί τη διαμεσολάβηση νόμιμων χρηματοπιστωτικών δομών τραπεζών, εταιρειών, ιδρυμάτων, ομοίως, το data laundering απαιτεί τη διαμεσολάβηση νόμιμων εταιρικών και θεσμικών δομών όπως οι εξαγωγικές άδειες, οι εξωχώριες εταιρείες ή η εξαίρεση εθνικής ασφάλειας. Χωρίς αυτές τις δομές, τα παράνομα δεδομένα δεν μπορούν να «ξεπλυθούν» και το έγκλημα παραμένει ορατό. Ο ρόλος λοιπόν της εταιρείας δεν είναι απλώς εκτελεστικός, είναι δομικά απαραίτητος για την ατιμωρησία του κράτους (SWAMI, 2006 ; Columbia Law Review, 2022).

Η δομική αναλογία με το money laundering αποκτά πλήρες εμπειρικό περιεχόμενο όταν εξεταστεί η συγκεκριμένη αλληλουχία σταδίων μέσω των οποίων τα παράνομα δεδομένα μετατρέπονται σε αξιοποιήσιμη πληροφορία. Όπως ακριβώς το money laundering δεν νοείται ως ενιαία πράξη αλλά ως διαδικασία με διακριτά στάδια, έτσι και το data laundering αποκαλύπτει την εγκληματολογική του σημασία μόνο μέσα από την ανάλυση κάθε σταδίου χωριστά.

Το πρώτο στάδιο αντιστοιχεί στη «τοποθέτηση»(placement) του money laundering κατα την οποία η παράνομη «ύλη» εισάγεται στο σύστημα. Στο data laundering, αυτό είναι η παράνομη συλλογή δεδομένων μέσω spyware, παράνομων υποκλοπών ή συλλογής χωρίς νόμιμη βάση. Η τεχνολογία zero-click του Pegasus και του Predator καθιστά αυτό το στάδιο εξαιρετικά δυσαπόδεικτο. Η μόλυνση της συσκευής αφήνει ελάχιστα τεχνικά ίχνη, και ακόμα λιγότερα ίχνη διαθέσιμα σε μη εξειδικευμένους ερευνητές (Amnesty International Security Lab, 2021). [5]

Το δεύτερο στάδιο, η «διαστρωμάτωση»(layering), είναι το πιο εξελιγμένο και αποτελεί το κλειδί της επιτυχίας του data laundering. Αντιστοιχεί στη διαστρωμάτωση του Money laundering. Τα παράνομα δεδομένα περνούν μέσα από πολλαπλά θεσμικά, νομικά και τεχνολογικά φίλτρα που αποκόπτουν τη σύνδεσή τους με την παράνομη καταγωγή τους.

Στην ελληνική περίπτωση, η διαστρωμάτωση επιτεύχθηκε μέσω τριών παράλληλων μηχανισμών: α) της επίκλησης της εξαίρεσης «εθνικής ασφάλειας» που απαλλάσσει από τις

[5] Η τεχνική ανάλυση επιβεβαιώνει ότι τα zero-click exploits αφήνουν ελάχιστα έως μηδενικά ίχνη γεγονός που καθιστά αδύνατη την απόδειξη της συλλογής εκτός εξειδικευμένης εγκληματολογικής ανάλυσης.

υποχρεώσεις GDPR, β) των πολυεπίπεδων εταιρικών δομών της Intellexa που καθιστούσαν αδύνατη την αναγνώριση του τελικού ωφελούμενου, και γ) των νόμιμων εξαγωγικών αδειών που παρείχαν το νομικό κάλυμμα για την εμπορία του spyware (European Parliament PEGA Committee, 2023).[6]

Ένα ακόμα παράδειγμα που αποδεικνύει ότι το κράτος δεν τελεί το έγκλημα άμεσα αλλά χρησιμοποιεί ιδιωτικές εταιρείες ως τρίτους για να παρακάμψει τις νομικές εγγυήσεις είναι η αγορά δεδομένων από data brokers (Ayoub, & Goitein, 2024) . Η χρήση των data brokers αποδεικνύει ότι το data laundering είναι δομικό χαρακτηριστικό της σύγχρονης κρατικής παρακολούθησης παγκοσμίως και όχι μόνο ελληνικό φαινόμενο. Το παράδειγμα αυτό προέρχεται από τις ΗΠΑ, όπου κυβερνητικές υπηρεσίες όπως η CBP, η ICE και η IRS αγόραζαν δεδομένα τοποθεσίας πολιτών απευθείας από ιδιωτικές εταιρείες (data brokers), παρακάμπτοντας έτσι την απαίτηση δικαστικού εντάλματος που επέβαλε η απόφαση Carpenter v. United States (2018). Η λογική αυτή αποκαλύπτει πως ό,τι δεν μπορεί να αποκτηθεί νόμιμα μέσω δικαστικής εντολής, αποκτάται μέσω της ανοιχτής αγοράς, μετατρέποντας μια παράκαμψη συνταγματικών εγγυήσεων σε τυπικά νόμιμη εμπορική συναλλαγή. Αυτή η πρακτική αποτελεί εφαρμογή του σταδίου layering του data laundering όπου τα δεδομένα αλλάζουν χέρια μέσω ενδιάμεσων εταιρειών, αποκτώντας φαινομενική νομιμότητα, ενώ η κρατική παρακολούθηση συνεχίζεται χωρίς δικαστικό έλεγχο (Columbia Law Review, 2022)

Το τρίτο στάδιο, «ενσωμάτωση» (integration), είναι το πιο δύσκολο να αποδειχθεί αλλά και το πιο επικίνδυνο. Τα δεδομένα επανεντάσσονται στο νόμιμο σύστημα ως αξιόπιστες πληροφορίες, αξιοποιούμενες για λήψη αποφάσεων, πολιτικές κινήσεις ή νομικές διαδικασίες χωρίς να αμφισβητείται η καταγωγή τους. Αυτό είναι το στάδιο για το οποίο η αποδεικτική δυσκολία είναι μέγιστη. Πώς αποδεικνύεται ότι μια πολιτική απόφαση ή μια δικαστική κατηγορία βασίστηκε σε πληροφορίες που αποκτήθηκαν παράνομα;

Ένα από τα κεντρικά ζητήματα για την εγκληματολογική αξιολόγηση του data laundering είναι η ταυτοποίηση των θυμάτων. Σε πρώτη ανάγνωση, φαίνεται να πρόκειται για «έγκλημα χωρίς θύμα». Η πληροφορία «ξεπλένεται» αθόρυβα, χωρίς άμεσα ορατή βλάβη σε συγκεκριμένα πρόσωπα (Green, & Ward, 2004, p. 3).[7] Ωστόσο, αυτή η εντύπωση είναι παραπλανητική. Τα θύματα του data laundering είναι πολλαπλά και διαστρωματωμένα. Στο άμεσο επίπεδο βρίσκονται τα πρόσωπα των οποίων τα δεδομένα συλλέχθηκαν παράνομα όπως δημοσιογράφοι, πολιτικοί, ακτιβιστές. Στο ευρύτερο επίπεδο βρίσκονται όλοι εκείνοι που αλλάζουν συμπεριφορά λόγω chilling effect. Άτομα δηλαδή, που ποτέ δεν υπήρξαν στόχοι αλλά υφίστανται τις επιπτώσεις. Στο συλλογικό επίπεδο βρίσκεται η ίδια η δημοκρατία, ο θεσμός που υπονομεύεται

[6]Η έκθεση PEGA διαπιστώνει ρητά ότι οι εξαγωγικές άδειες λειτουργούν de facto ως μηχανισμός νομιμοποίησης εργαλείων που χρησιμοποιούνται για παράνομη παρακολούθηση.

[7] Η απουσία αναγνωρίσιμου θύματος — ή η διάχυση της βλάβης σε τόσο ευρύ πληθυσμό ώστε να μην αναγνωρίζεται εύκολα — αποτελεί χαρακτηριστικό γνώρισμα των εγκλημάτων ισχυρών δρώντων.

όταν η ελεύθερη έκφραση, ο ανεξάρτητος Τύπος και η πολιτική αντιπολίτευση καθίστανται αντικείμενα κρατικής παρακολούθησης. (Kaldani & Prokopets, 2022, pp. 20-28)[8]

3.3 Νομικά και Ηθικά Κενά στη Ρύθμιση της Κυβερνοεπιτήρησης

Το πιο θεμελιώδες νομικό κενό είναι η απουσία ρητής ποινικοποίησης της νομιμοποίησης παράνομα αποκτηθέντων δεδομένων επιτήρησης ως αυτόνομου αδικήματος. Σε αντίθεση με το money laundering, για το οποίο υπάρχει εκτεταμένο διεθνές και ευρωπαϊκό κανονιστικό πλαίσιο, δεν υπάρχει αντίστοιχο πλαίσιο που να απαγορεύει ρητά τη διαδικασία μέσω της οποίας παράνομα δεδομένα επιτήρησης εισέρχονται σε νόμιμες ροές πληροφοριών και αξιοποιούνται χωρίς έλεγχο της προέλευσής τους (SWAMI, 2006, σ. 96).

Επιπροσθέτως, είναι η εξαίρεση εθνικής ασφάλειας του GDPR (άρθρο 23), η οποία λειτουργεί ως νομικά κωδικοποιημένη δυνατότητα διαστρωμάτωσης. Το κράτος μπορεί να επικαλεστεί «εθνική ασφάλεια» για να αποκλείσει κάθε έλεγχο της νομιμότητας της συλλογής δεδομένων, χωρίς ανεξάρτητη δικαστική εποπτεία (European Data Protection Board (EDPB)., 2021, σ. 8). Τέλος, είναι ο Κανονισμός Διπλής Χρήσης (2021/821). Παρά τη νέα κατηγορία «κυβερνο-επιτήρησης», οι εξαγωγικές άδειες χορηγούνται εθνικά χωρίς ευρωπαϊκή εναρμόνιση, επιτρέποντας το arbitrage δικαιοδοσίας (European Parliament Committee of Inquiry (PEGA), 2023).

Πέραν των νομικών κενών, υπάρχουν και ηθικά κενά που η εγκληματολογία οφείλει να αναλύσει. Το κεντρικό ηθικό ζήτημα είναι η απουσία συγκατάθεσης καθώς τα δεδομένα συλλέγονται, επεξεργάζονται και αξιοποιούνται χωρίς τη γνώση ή συναίνεση των υποκειμένων τους. Στο πλαίσιο της καντιανής ηθικής, αυτό συνιστά ακριβώς εκείνη τη μορφή παραβίασης που ο Καντ θεωρούσε πιο θεμελιώδη, τη μεταχείριση ανθρώπινου προσώπου αποκλειστικά ως μέσου για την επίτευξη άλλων σκοπών (Rentmeester, 2022).

Το δεύτερο ηθικό κενό είναι η ασυμμετρία γνώσης και εξουσίας. Το κράτος γνωρίζει τα πάντα για τον πολίτη, ενώ ο πολίτης αγνοεί τι γνωρίζει το κράτος για αυτόν. Αυτή η ασυμμετρία, που το data laundering συντηρεί και ενισχύει, αντιτίθεται στη δημοκρατική αρχή της διαφάνειας και λογοδοσίας (Braman, & Lynch, 2014).

[8] Οι συγγραφείς επισημαίνουν την απουσία αποτελεσματικών ένδικων μέσων για θύματα παρακολούθησης ως δομικό κενό του ευρωπαϊκού νομικού πλαισίου.

ΚΕΦΑΛΑΙΟ 4 : Η Βιομηχανία Εμπορικού Spyware ως υποδομή επιτήρησης

Η εγκληματολογική ανάλυση του data laundering απαιτεί την κατανόηση της συγκεκριμένης βιομηχανίας που το παράγει. Το παρόν κεφάλαιο χαρτογραφεί τη βιομηχανία εμπορικών spyware, την αγορά, τους κύριους δρώντες, τη λειτουργική αλυσίδα κράτος-εταιρεία-στόχος, και τους μηχανισμούς όπως εξαγωγικές άδειες, μεσάζοντες και εξωχώριες δομές που καθιστούν δυνατή τη λειτουργία της εκτός αποτελεσματικής ρύθμισης (Deibert, 2020).

4.1 Αγορά spyware και μοντέλα λειτουργίας

Η αγορά εμπορικών spyware αποτελεί το δομικό υπόβαθρο εντός του οποίου το data laundering καθίσταται εφικτό. Χωρίς την ύπαρξη νόμιμης αγοράς που να προσδίδει εμπορική υπόσταση στα εργαλεία παρακολούθησης, η διαδικασία νομιμοποίησης παράνομα αποκτηθέντων δεδομένων δεν θα μπορούσε να ξεκινήσει.

Τα spyware αποτελούν μια κατηγορία λογισμικών τα οποία μπορούν να εγκατασταθούν χωρίς τη γνώση του χρήστη και ιδιοκτήτη του υπολογιστή ή τηλεφώνου. Λειτουργούν πίσω από τα υπόλοιπα λογισμικά αντιγράφοντας και υποκλέπτοντας δεδομένα που ενδιαφέρουν τρίτους όπως κωδικούς, αρχεία, αρχεία πιστωτικών καρτών και άλλα τραπεζικά δεδομένα, συνομιλίες, email και άλλα δεδομένα τα οποία μπορεί να ενδιαφέρουν τον διαχειριστή του spyware προγράμματος. Τα δεδομένα αυτά συγκεντρώνονται σε μια προσωρινή μνήμη και αποστέλλονται μέσω διαδικτύου σε άλλο υπολογιστή. Επηρεάζει ελάχιστα τη λειτουργία των συσκευών και γι αυτό είναι δύσκολο να εντοπιστεί. Σε αντίθεση με τους ιούς δεν έχει τη δυνατότητα να εξαπλώνεται αυτόματα αλλά αντιθέτως χρειάζεται την ενέργεια του χρήστη για να εγκατασταθεί.

Τα τελευταία χρόνια καθώς μεγάλες εταιρείες τεχνολογίας όπως η Apple επένδυσαν σημαντικά στην κρυπτογράφηση και την ασφάλεια οι κυβερνήσεις βρέθηκαν σε αδυναμία να παρακολουθούν τις επικοινωνίες μέσω των παραδοσιακών κερκόπορτων (backdoors) στα συστήματα. Αυτό δημιούργησε μια νέα αγορά όπου χάκερ αναζητούν εκμεταλλεύσιμες ευπάθειες και εταιρείες τις μετατρέπουν σε εμπορικά εργαλεία παρακολούθησης που πωλούνται σε κυβερνήσεις (Deibert, 2020) (Citizen Lab, 2021).

Ο μεγαλύτερος παράγοντας στην αγορά αυτή είναι η NSO Group με το spyware Pegasus το οποίο μπορεί να υποκλέψει συνομιλίες, αρχεία και να ενεργοποιήσει κάμερα και μικρόφωνο εν αγνοία του χρήστη, μέσω zero clicks, καθιστώντας την ανίχνευση σχεδόν αδύνατη (Παπανικολάου, 2025, σ. 9).

Το Pegasus δεν αποτελεί μεμονωμένο φαινόμενο. Η αγορά τεχνολογιών επιτήρησης περιλαμβάνει δεκάδες εταιρείες (FinFisher/Gamma International, Amesys, Trovicor, Blue Coat, Sandvine) οι οποίες εδρεύουν κυρίως σε δυτικές χώρες αλλά πωλούν σε αυταρχικά καθεστώτα. Χαρακτηριστική είναι η περίπτωση της Αιγύπτου κατά την ανατροπή του Μουμπάρακ όπου η

βρετανική Gamma International παρείχε το Fin Spy για παρακολούθηση ακτιβιστών (Timm, 2012).

Τα τελευταία χρόνια κινεζικές εταιρείες επιτήρησης έχουν επεκτείνει την παρουσία τους σε Αφρική και Ασία εξάγοντας μοντέλα παρακολούθησης τόσο σε αυταρχικά όσο και σε φιλελεύθερα κράτη. Η UNCHR έχει αναγνωρίσει τη χρήση εμπορικών τεχνολογιών κυβερνοεπιτήρησης ως παγκόσμιο ζήτημα ανθρωπίνων δικαιωμάτων (Feldstein, 2019)

Οι διαβεβαιώσεις των κατασκευαστριών εταιρειών περί αποκλειστικού προορισμού των προϊόντων τους για την καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας έχουν στη πράξη διαψευστεί (Παπανικολάου, 2025, σ. 9) Αντιθέτως, λειτουργούν ως πανοπτικοί μηχανισμοί απόλυτου ελέγχου της τηλεφωνικής συσκευής καθώς αποκτούν πρόσβαση τόσο στο λειτουργικό σύστημα της όσο και στις χρησιμοποιούμενες εφαρμογές. Παρεισφρέουν αποσπώντας το σύνολο των δεδομένων και πληροφοριών που είναι αποθηκευμένα στη συσκευή (Παπανικολάου, 2025, σ. 9)

Η NSO Group, ισρηλινή εταιρεία, αποτελεί τον πιο γνωστό και καλύτερα τεκμηριωμένο παράγοντα της βιομηχανίας εμπορικών spyware. Το προϊόν της, Pegasus, είναι ένα spyware πλήρους πρόσβασης που εγκαθίσταται σε συσκευές iOS και Android χωρίς αλληλεπίδραση του χρήστη (zero-click) εκμεταλλευόμενο ευπάθειες zero-day (Marczak, 2018). Μόλις εγκατασταθεί, παρέχει πλήρη πρόσβαση σε κλήσεις, μηνύματα, email, κάμερα, μικρόφωνο, δεδομένα τοποθεσίας και κωδικούς πρόσβασης, ακόμα και σε κρυπτογραφημένες επικοινωνίες (Citizen Lab, 2021).

Το Pegasus Project (2021) αποκάλυψε ότι το Pegasus είχε χρησιμοποιηθεί σε τουλάχιστον 50 χώρες, με στόχους που περιλάμβαναν 189 δημοσιογράφους, 85 ακτιβιστές ανθρωπίνων δικαιωμάτων, 65 επιχειρηματίες και 600 πολιτικούς, συμπεριλαμβανομένων αρχηγών κρατών και κυβερνήσεων (Citizen Lab, 2021).

Στις 18 Ιουλίου 2021, αποκαλύφθηκε από την Amnesty International and Forbidden Stories ότι αρκετές χιλιάδες πολιτικοί ηγέτες, εργαζόμενοι στα ανθρώπινα δικαιώματα και δημοσιογράφοι, βρίσκονται υπό την ευρεία παρακολούθηση των Niv, Shalev και Omri Group (NSO Group) χρησιμοποιώντας το λογισμικό κατασκοπείας Pegasus στα κινητά τους τηλέφωνα (Khan, 2022). Ο Όμιλος NSO αρνήθηκε εντελώς οποιαδήποτε παράνομη χρήση του λογισμικού του, υποστηρίζοντας ότι η εταιρεία παρέχει τέτοιο λογισμικό υποκλοπής spyware «μόνο σε κυβερνητικές υπηρεσίες πληροφοριών και επιβολής του νόμου» με στόχο τον περιορισμό τρομοκρατικών δραστηριοτήτων ή άλλων σοβαρών αδικημάτων. Η σύμβαση χρήσης του Pegasus δεν προβλέπει κανέναν μηχανισμό προστασίας ανθρωπίνων δικαιωμάτων. Σε περίπτωση παραβίασης των όρων της, ο Όμιλος NSO δικαιούται μόνο αστικά ένδικα μέσα όπως διακοπή της σύμβασης, αποζημίωση ή ένταξη στη μαύρη λίστα, χωρίς καμία πρόβλεψη για τα θύματα της παράνομης παρακολούθησης (Khan, 2022). Συνεπώς, η αρχιτεκτονική της σύμβασης εξασφαλίζει

ότι η ευθύνη παραμένει αόρατη. Ενόψει αυτής της δομικής ατιμωρησίας, εμπειρογνώμονες του ΟΗΕ για τα Ανθρώπινα Δικαιώματα κάλεσαν σε «παγκόσμιο μορατόριουμ» στην πώληση και χρήση spyware «απειλητικού για τη ζωή», έως ότου αναπτυχθεί επαρκές ρυθμιστικό πλαίσιο (Saxena, & Anand, 2022)

Η Intellexa αποτελεί τον δεύτερο μεγάλο παράγοντα της βιομηχανίας και το άμεσα σχετικό με την ελληνική υπόθεση. Ιδρύθηκε από τον Ισραηλινό πρώην αξιωματούχο της Mossad Tal Dilian, αρχικά με έδρα την Ελλάδα και στη συνέχεια με πολύπλοκη πολυεδαφική δομή (Citizen Lab, 2021). Το προϊόν της, Predator, παρουσιάζει παρόμοιες δυνατότητες με το Pegasus όπως zero-click μόλυνση, πλήρης πρόσβαση σε συσκευή, παρακολούθηση επικοινωνιών και δεδομένων τοποθεσίας σε πραγματικό χρόνο.

Πέραν αυτών των δύο κυρίαρχων παραγόντων, η βιομηχανία περιλαμβάνει δεκάδες μικρότερες εταιρείες FinFisher (Γερμανία), Hacking Team (Ιταλία), Candiru (Ισραήλ) που συγκροτούν ένα παγκόσμιο οικοσύστημα εμπορικής παρακολούθησης με εκτιμώμενο τζίρο δισεκατομμυρίων ευρώ ετησίως (European Parliament PEGA Committee, 2023).

4.2 Η Αλυσίδα Κράτος-Εταιρεία-Στόχος

Η λειτουργία της βιομηχανίας spyware οργανώνεται γύρω από μια τυπική αλυσίδα που ο Kaldani και ο Prokopets (2022) έχουν αναλύσει συστηματικά. (Kaldani & Prokopets, 2022, pp. 5-8) Η αλυσίδα έχει τέσσερις κρίκους. Ο πρώτος κρίκος είναι ο κατασκευαστής (NSO, Intellexa) ο οποίος αναπτύσσει και συντηρεί το spyware, ανακαλύπτει ευπάθειες μηδενικής ημέρας (zero-day vulnerabilities) παρέχει τεχνική υποστήριξη. Ο δεύτερος κρίκος είναι το κράτος-πελάτης που αγοράζει το σύστημα, συνήθως μέσω εθνικής υπηρεσίας πληροφοριών ή αστυνομίας, με επίκληση «νόμιμης παρακολούθησης». Ο τρίτος κρίκος είναι η υποδομή ανάπτυξης δηλαδή διακομιστές (servers), ονόματα τομέα (domains), δίκτυα διανομής που αποκρύπτουν την πραγματική ταυτότητα του χειριστή. Ο τέταρτος κρίκος είναι ο στόχος, το πρόσωπο του οποίου η συσκευή μολύνεται, χωρίς γνώση και χωρίς τη δυνατότητα αντίδρασης.

Εγκληματολογικά, η σημασία αυτής της αλυσίδας είναι ότι κάθε κρίκος μπορεί να αποποιηθεί την ευθύνη για τον επόμενο. Ο κατασκευαστής ισχυρίζεται ότι πουλά μόνο σε «νόμιμες κυβερνήσεις» για «νόμιμη χρήση». Το κράτος-πελάτης ισχυρίζεται ότι χρησιμοποιεί νόμιμο εμπορικό προϊόν. Η υποδομή ανάπτυξης είναι αόρατη. Ο στόχος δεν γνωρίζει τίποτα. Αυτή η αλυσίδα αποποίησης ευθύνης είναι ακριβώς αυτό που οι Kramer και Michalowski περιέγραψαν ως «state-facilitated crime» (Kramer, & Michalowski, 2006).

Προς τεκμηρίωση του, ενδεικτικό παράδειγμα αποτελεί η αποποίηση ευθύνης από την NSO Group η οποία ενώ διατηρεί πλήρη έλεγχο της τεχνικής υποδομής της Pegasus ισχυρίστηκε ότι δεν χειρίζεται και δεν έχει ορατότητα στη χρήση του συστήματος από τους πελάτες. Αυτή η άρνηση λειτουργικής ευθύνης αποτελεί δομικό στοιχείο της αλυσίδας αποποίησης ευθύνης

(Berthelet, 2022). Η αποποίηση ευθύνης δεν αποτελεί ιδιαιτερότητα της NSO Group αλλά δομικό χαρακτηριστικό ολόκληρης της βιομηχανίας spyware. Τα τελευταία δεδομένα, κατά τη συγγραφή της παρούσας εργασίας, από την ελληνική περίπτωση επιβεβαιώνουν αυτή την ανάλυση. Σε δηλώσεις του, ο καταδικασθέντας ιδρυτής της Intellexa Tal Dillian επιβεβαίωσε την ύπαρξη συμφωνητικού συνεργασίας με την ΕΥΠ το 2020 καθώς και ηλεκτρονικής αλληλογραφίας της Intellexa με Έλληνες κρατικούς υπαλλήλους που αφορούσαν τεχνικά ζητήματα και παρεμβάσεις στο σύστημα Predator (Ζαφειρόπουλος, 2026).

4.3 Τεχνολογία Διπλής Χρήσης και Εξαγωγικές Άδειες

Οι εξαγωγικές άδειες αντιστοιχούν στο πρώτο στάδιο του data laundering, τη τοποθέτηση (placement). Η τεχνολογία παρακολούθησης αποκτά επίσημη κρατική έγκριση που της προσδίδει νομιμοποιητική βαρύτητα πριν καν χρησιμοποιηθεί, με αποτέλεσμα η μελλοντική κατάχρηση να καθίσταται νομικά σχεδόν αναπόδεικτη.

Η εξαγωγική άδεια αποτελεί τον πιο εξελιγμένο μηχανισμό ξεπλύματος της βιομηχανίας spyware. Πρόκειται για επίσημη κρατική έγκριση που επιτρέπει σε μια εταιρεία να πωλήσει τεχνολογία δύο χρήσεων, δηλαδή τεχνολογία με δυνατότητα τόσο νόμιμης όσο και επιβλαβούς χρήσης, σε αλλοδαπό αγοραστή. Η λογική της είναι αρχικά αμυντική, το κράτος ελέγχει ποιος αποκτά ευαίσθητες τεχνολογίες ώστε να μην καταλήξουν σε εχθρικά καθεστώτα. Στην πράξη όμως, στη βιομηχανία spyware λειτουργεί αντεστραμμένα. Η χορήγηση της άδειας από κρατικό φορέα μετατρέπει ένα εργαλείο που μπορεί να χρησιμοποιηθεί για παράνομη παρακολούθηση σε «νόμιμο εξαγώγιμο προϊόν», δίνοντάς του έναν μανδύα νομιμότητας που δεν αντικατοπτρίζει την πραγματική χρήση του (Bromley, & Maletta, 2024).

Αυτό είναι ακριβώς το ανάλογο της τοποθέτησης στο money laundering. Όπως ο εγκληματίας εισάγει βρώμικο χρήμα στο χρηματοπιστωτικό σύστημα για να αποκτήσει νόμιμη υπόσταση, έτσι και ο παραγωγός spyware εισάγει το προϊόν του στο διεθνές εμπόριο μέσω μιας επίσημης κρατικής διαδικασίας που του προσδίδει νομιμοποιητική βαρύτητα. Από τη στιγμή που χορηγηθεί η άδεια, η όποια μελλοντική κατάχρηση καθίσταται πολύ δυσκολότερο να αποδοθεί νομικά στον παραγωγό.

Ο Κανονισμός Διπλής Χρήσης 2021/821 εισήγαγε νέα κατηγορία «κυβερνο-επιτήρησης» και ρήτρα catch-all που επιτρέπει θεωρητικά τον έλεγχο εξαγωγής ακόμα και προϊόντων εκτός καταλόγου. Στην πράξη όμως, όπως διαπιστώνει το SIPRI (2024), η ρήτρα αυτή παραμένει σχεδόν αναξιοποίητη (Bromley, & Maletta, 2024). Τα κράτη-μέλη χορηγούν άδειες εθνικά, χωρίς ευρωπαϊκή εναρμόνιση, και συχνά με βάση οικονομικά ή διπλωματικά κριτήρια αντί για κριτήρια ανθρωπίνων δικαιωμάτων. Η δυαδικότητα που κατασκευάζεται από τον όρο υπονομεύει τις διασφαλίσεις των ανθρωπίνων δικαιωμάτων στον έλεγχο των εξαγωγών spyware. Η διπλή χρήση έχει τις ρίζες της στη διάκριση μεταξύ «ειρηνικών» και «μη ειρηνικών» ή «πολιτικών» και

«στρατιωτικών» χρήσεων η οποία σταδιακά συνδέθηκε με μια ευρύτερη διχοτόμηση μεταξύ «νόμιμων» και «αθέμιτων» σκοπών. Το αφήγημα των ειδών διπλής χρήσης χρησίμευε ιστορικά όχι μόνο για να διατυπώσει τους κινδύνους που ενέχουν ορισμένες τεχνολογίες και να υποδείξει το σκεπτικό για τον έλεγχο των εξαγωγών τους, αλλά και για να δικαιολογήσει το εμπόριο τους. Η προσφυγή των φορέων της ΕΕ στη διπλή χρήση κλίνει τη συζήτηση της ΕΕ για τον έλεγχο των εξαγωγών κατασκοπευτικού λογισμικού προς εμπορικά συμφέροντα και κρατικοκεντρικά ζητήματα ασφάλειας έναντι των ανθρωπίνων δικαιωμάτων. Συνεπώς, η πλαισίωση του spyware ως διπλής χρήσης δημιουργεί μια εννοιολογικά ελαττωματική, παραπλανητική και κενή δυαδικότητα που εμποδίζει τις προσπάθειες περιορισμού των εξαγωγών spyware με βάση τους κινδύνους για τα ανθρώπινα δικαιώματα (Riecke, 2023).

4.4 Μεσάζοντες και Εξωχώριες Δομές: Η Αρχιτεκτονική της Αδιαφάνειας

Οι μεσάζοντες (intermediaries) αποτελούν τον κεντρικό μηχανισμό του δεύτερου σταδίου του data laundering, του layering. Ο ρόλος τους δεν είναι εμπορικός αλλά δομικά αναγκαίος για την αποκοπή της αλυσίδας ευθύνης μεταξύ κατασκευαστή και κράτους-πελάτη.

Στη βιομηχανία spyware σπάνια ο κατασκευαστής πουλά απευθείας στο κράτος-πελάτη. Ανάμεσά τους παρεμβάλλεται συνήθως ένας ή περισσότεροι μεσάζοντες, οι μεσάζοντες, που αναλαμβάνουν τη διαπραγμάτευση και την τεχνική ολοκλήρωση της συμφωνίας. Ο πραγματικός τους ρόλος δεν είναι τεχνικός αλλά νομικός, ώστε να δημιουργήσουν απόσταση μεταξύ του εργαλείου και της χρήσης του. Η λογική είναι απλή. Όταν αποκαλύπτεται κακή χρήση, ο κατασκευαστής ισχυρίζεται ότι πούλησε σε έναν νόμιμο μεσάζοντα και δεν είχε τρόπο να γνωρίζει πού κατέληξε τελικά το προϊόν του. Ο μεσάζοντας, από την πλευρά του, ισχυρίζεται ότι απλώς διευκόλυνε μια εμπορική συναλλαγή. Και το κράτος-πελάτης επικαλείται εθνική ασφάλεια για να αρνηθεί κάθε σχόλιο. Το αποτέλεσμα είναι μια αλυσίδα αμοιβαίας αποποίησης ευθύνης που έχει τεκμηριωθεί διεξοδικά στην περίπτωση της Intellexa (Citizen Lab, 2021)

Εάν οι εξαγωγικές άδειες συνιστούν τη τοποθέτηση του data laundering, οι εξωχώριες δομές της Intellexa αποτελούν την πιο εξελιγμένη έκφραση του layering. Η κατανομή σε πολλές δικαιοδοσίες διασφαλίζει ότι κανένας εποπτικός φορέας δεν αποκτά πλήρη εικόνα και επομένως δεν μπορεί να αποδείξει την παράνομη αλυσίδα.

Η εταιρεία Intellexa αποτελεί χαρακτηριστικό παράδειγμα της χρήσης εξωχώριων δομών για τη δημιουργία αδιαφάνειας (Citizen Lab, 2023). Η εταιρική δομή της κατά την περίοδο 2018-2022 περιελάμβανε μητρική εταιρεία με έδρα τις Βρετανικές Παρθένες Νήσους, λειτουργικές εταιρείες στην Ελλάδα (Cytrox Holdings) και Βόρεια Μακεδονία (Cytrox AD), εταιρεία πωλήσεων στην Ιρλανδία, και εταιρεία τεχνικής υποστήριξης στην Κύπρο (PEGA Committee, 2023, pp. 45-52).

Κάθε επίπεδό αυτής της δομής εξυπηρετούσε έναν συγκεκριμένο σκοπό. Η κατανομή σε πολλές δικαιοδοσίες διασφάλιζε ότι κανένας εθνικός εποπτικός φορέας δεν μπορούσε να έχει πλήρη εικόνα του συνόλου, η νομική αδιαφάνεια ήταν ενσωματωμένη στην ίδια την αρχιτεκτονική της εταιρείας (Citizen Lab, 2021). Παράλληλα, η πολυεδαφική παρουσία επέτρεπε το εξαγωγικό arbitrage καθώς η εταιρεία μπορούσε να επιλέγει κάθε φορά από ποια χώρα θα χορηγηθεί η εξαγωγική άδεια, σταθμίζοντας ποια δικαιοδοσία προσέφερε τις λιγότερες αντιστάσεις (PEGA Committee, 2023, σσ. 45-52). Τέλος, η δρομολόγηση των κερδών μέσω εταιρειών χαμηλής φορολόγησης ολοκλήρωνε μια εικόνα που θυμίζει λιγότερο εμπορική επιχείρηση και περισσότερο σκόπιμα σχεδιασμένο σύστημα αδιαφάνειας.

4.5 Η Βιομηχανία Spyware ως Κρατικο-Εταιρικό Έγκλημα

Η συνολική εικόνα που προκύπτει από την ανάλυση της βιομηχανίας spyware επιβεβαιώνει τη θεωρητική πρόβλεψη των Kramer και Michalowski πως το τρίπτυχο κίνητρο-ευκαιρία-έλλειψη ελέγχου δεν συντρέχει τυχαία αλλά δομικά, αποτελώντας συστατικό στοιχείο της λειτουργίας του κλάδου (Kramer, Michalowski, & Kauzlarich, 2002)

Το κίνητρο είναι αμοιβαίο και αυτοτροφοδοτούμενο. Για τις εταιρείες, η αγορά spyware προσφέρει εξαιρετικά κερδοφόρες συμβάσεις με κρατικούς πελάτες που διαθέτουν σχεδόν απεριόριστους προϋπολογισμούς ασφαλείας. Για τα κράτη-πελάτες, η απόκτηση spyware ικανοποιεί την ανάγκη για πολιτικό έλεγχο, παρακολούθηση αντιπάλων και καταστολή διαφωνίας, στόχοι που συχνά δεν μπορούν να επιτευχθούν μέσω νόμιμων εγχώριων διαδικασιών (Green, & Ward, 2004, pp. 28-30). Αυτή η σύμπλευση συμφερόντων δημιουργεί αυτό που ο Deibert (2020) αποκαλεί «cyber mercenary ecosystem» δηλαδή ένα οικοσύστημα όπου κράτος και αγορά συναντώνται σε ένα σημείο που κανένας δεν θέλει να ονομαστεί «παράνομο» (Deibert, 2020).

Η ευκαιρία παρέχεται από συστοιχία δομικών παραγόντων που αναλύθηκαν στα προηγούμενα κεφάλαια. Τα τεχνολογικά κενά, οι ευπάθειες μηδενικής μέρας (zero-day vulnerabilities) που αγοράζονται στη μαύρη αγορά, επιτρέπουν τη διείσδυση χωρίς ανιχνεύσιμα ίχνη. Τα ρυθμιστικά κενά, όπως η εξαίρεση εθνικής ασφάλειας του GDPR, η αδυναμία εναρμόνισης του Κανονισμού Διπλής Χρήσης, δημιουργούν νομικές γκρίζες ζώνες που η βιομηχανία εκμεταλλεύεται συστηματικά. Οι εξωχώριες εταιρικές δομές, όπως αυτή της Intellexa, ολοκληρώνουν την αρχιτεκτονική της αδιαφάνειας, διασφαλίζοντας ότι κανένας εθνικός εποπτικός φορέας δεν μπορεί να έχει πλήρη εικόνα (Citizen Lab, 2021;European Parliament PEGA Committee, 2023)

Η έλλειψη αποτελεσματικού ελέγχου είναι ίσως η πιο κρίσιμη διάσταση, καθώς δεν πρόκειται για απλή αποτυχία των θεσμών αλλά για δομικά παραγόμενη ατιμωρησία. Οι Green και Ward (2004) είχαν επισημάνει ότι τα κράτη που διαπράττουν παραβιάσεις ανθρωπίνων

δικαιωμάτων σπάνια λογοδοτούν, διότι ελέγχουν τους ίδιους τους μηχανισμούς λογοδοσίας (Green, & Ward, 2004). Στην περίπτωση του spyware, συντρέχουν τα παρακάτω: οι εποπτικές αρχές είναι πολιτικά εκτεθειμένες, καθώς στις περισσότερες χώρες οι υπηρεσίες πληροφοριών υπάγονται απευθείας στην εκτελεστική εξουσία (PEGA Committee, 2023). Επίσης, οι δικαστικές αρχές αποκλείονται συχνά μέσω της επίκλησης εθνικής ασφάλειας, που λειτουργεί ως νομικά κωδικοποιημένο εμπόδιο στον δικαστικό έλεγχο (Riecke, 2023). Τέλος, και πιο σημαντικό εγκληματολογικά, τα θύματα συνήθως αγνοούν ότι είναι θύματα, χαρακτηριστικό που καθιστά το spyware ριζικά διαφορετικό από κάθε άλλη μορφή κρατικής βίας που είχε αναλύσει η εγκληματολογία έως τώρα (Citizen Lab, 2021;Amnesty International & Forbidden Stories , 2021).

Αυτή η τριπλή αδυναμία ελέγχου παράγει αυτό που μπορεί να χαρακτηριστεί ως «δομική ατιμωρησία» δηλαδή μια κατάσταση όπου η ατιμωρησία δεν είναι απλώς αποτέλεσμα αδράνειας αλλά είναι ενσωματωμένη στην ίδια την αρχιτεκτονική του συστήματος. Το data laundering αποτελεί τον μηχανισμό που συντηρεί αυτή την ατιμωρησία. Εφόσον τα δεδομένα που αποκτήθηκαν παράνομα «καθαρίζονται» και ενσωματώνονται σε επίσημες διαδικασίες, η αλυσίδα ευθύνης θολώνει. Όπως θα αναδειχθεί στο επόμενο κεφάλαιο μέσω της ελληνικής περίπτωσης, αυτή η τριπλή αδυναμία ελέγχου παράγει δομική ατιμωρησία που δεν είναι αποτέλεσμα αδράνειας αλλά είναι ενσωματωμένη στην ίδια την αρχιτεκτονική του συστήματος (Green, & Ward, 2004)

ΚΕΦΑΛΑΙΟ 5: Νομικό και Ρυθμιστικό Πλαίσιο

Το απόρρητο των τηλεπικοινωνιών το οποίο πλήττεται από τα λογισμικά παρακολούθησης, αποτελεί δίπολο ελευθερίας και ασφάλειας, αφενός ιδιωτικότητας και αφετέρου πρόσβασης του κράτους στο σύνολο των αναγκαίων πληροφοριών για λόγους δημόσιας και εθνικής ασφάλειας. Η υπεράσπιση του δικαίωματος στην ιδιωτικότητα είναι συνδεδεμένο με την αξία του ανθρώπου (Παπανικολάου, 2025, σ. 642). Στο τελευταίο κείμενο του ΧΘΔ αναφέρεται στο άρθρο 6 από κοινού το δικαίωμα στην ελευθερία και την ασφάλεια. (Παπανικολάου, 2025, σ. 2) Το σκάνδαλο των παρακολουθήσεων μέσω spyware υπήρξε στην πράξη η επιβεβαίωση της κρισιμότητας του δικαιώματος. Η υπόθεση του predatorgate δεν αποτελεί μεμονωμένο φαινόμενο και πρωτοτυπία. Ήδη από το 1993 ο καθ. Τσακυράκης διαπίστωνε ότι «δεν θα ήταν υπερβολή να καθιερωθεί στην πράξη ένα περίεργο δικαίωμα, το δικαίωμα στις υποκλοπές των τηλεφωνικών συνδιαλέξεων» (Τσακυράκης, 1993, σ. 995)

Ο κίνδυνος, για το δικαίωμα στην ιδιωτικότητα, που παράγεται από την ανάπτυξη των νέων τεχνολογιών είναι σημαντικά αυξημένος και απαιτεί συνεχή επικαιροποίηση του θεσμικού πλαισίου, καθώς η τεχνολογική πρόοδος αποτελεί υποκειμενική συνθήκη της πολιτειακής λειτουργίας (Παπανικολάου, 2025, σσ. 2-5). Το ευρωπαϊκό νομικό πλαίσιο αδυνατεί να ακολουθήσει αυτή την εξέλιξη. Ζητούμενο είναι η προσαρμογή των εγγυήσεων που περιβάλλουν το δικαίωμα στην ιδιωτικότητα και το απόρρητο των τηλεπικοινωνιών, στις ειδικότερες κάθε φορά απαιτήσεις και τα χαρακτηριστικά των διαφορετικών μέσω και τρόπων επικοινωνίας. (Παπανικολάου, 2025, σ. 7)

Η λανθασμένη χρήση λογισμικών παρακολούθησης συνδέεται συχνά με παραβιάσεις των ανθρωπίνων δικαιωμάτων, οφειλόμενη και στο κατακερματισμένο ρυθμιστικό πλαίσιο (Kaldani & Prokopets, 2022, pp. 30-38). Η έρευνα σχετικά με τους ρυθμιστικούς μηχανισμούς είναι απαραίτητη προκειμένου να προληφθούν επιπλέον επιβλαβείς συνέπειες στα ανθρώπινα δικαιώματα, τη δημοκρατία και το κράτος δικαίου που προκαλούνται από αυτές τις τεχνολογίες παρακολούθησης. Αυτές οι τεχνολογίες αναδύονται ταχύτερα από τους ρυθμιστικούς φορείς, τους μηχανισμούς ελέγχου ή τα νομικά πλαίσια που τις διέπουν. Αυτό σημαίνει ότι το ευρωπαϊκό νομικό πλαίσιο δεν είναι έτοιμο για αυτό που είναι τεχνολογικά εφικτό (European Parliament PEGA Committee, 2023, pp. 18-25). Συνεπώς, τα κράτη μπορούν να διεξάγουν παράνομη παρακολούθηση χωρίς τον φόβο νομικών συνεπειών. Εκτός από την παραβίαση των ανθρωπίνων δικαιωμάτων υπονομεύεται επίσης η δημοκρατία, οι δημοκρατικοί θεσμοί και το κράτος δικαίου. Για τους παραπάνω λόγους είναι απαραίτητη η δημιουργία ισχυρού νομικού πλαισίου και αποτελεσματικών μηχανισμών εποπτείας για τη μείωση των κινδύνων που συνδέονται με τις τεχνολογίες επιτήρησης (Saxena, & Anand, 2022). Επιπλέον, σημαντική είναι και η συνεργασία μεταξύ κυβερνήσεων, διεθνών οργανισμών και της κοινωνίας των πολιτών. Αντί να απαγορεύουν πλήρως το κατασκοπευτικό λογισμικό, τα κράτη μέλη της ΕΕ θα πρέπει να πληρούν

συγκεκριμένες απαιτήσεις, όπως η αποτελεσματική δικαστική έγκριση, η διαφάνεια, η ανεξάρτητη εποπτεία και να διασφαλίζουν ότι η χρήση του αποτελεί πάντα έσχατη λύση.

Συμπερασματικά, δεν υπάρχει αμφιβολία ότι η απλή παρουσία τέτοιου spyware χωρίς κατάλληλο ρυθμιστικό πλαίσιο εγείρει από μόνη της ανησυχία για το δικαίωμα κάθε ατόμου στην ιδιωτική ζωή (Tushar &Atul, 2022).

5.1 Θεμελιώδη δικαιώματα και επιτήρηση

Οι επιπτώσεις στα ανθρώπινα δικαιώματα που αναλύονται στην παρούσα ενότητα δεν είναι ανεξάρτητες από τον μηχανισμό data laundering. Αντίθετα, είναι άμεση συνέπειά του, εφόσον η παράνομη παρακολούθηση «ξεπλένεται» και η προέλευσή της αποκρύπτεται, τα θύματα στερούνται κάθε δυνατότητας έννομης προστασίας, με αποτέλεσμα η βλάβη να παραμένει αόρατη και αδιόρθωτη.

Η εκτεταμένη παρακολούθηση επηρεάζει την ιδιωτικότητα των ανθρώπων, την προστασία των δεδομένων και άλλα ατομικά δικαιώματα όπως τα δικαιώματα της ελευθερίας του λόγου, της συνάθροισης και του συνεταιρίζεσθε, καθώς και τους δημοκρατικούς θεσμούς της κοινωνίας (Kaldani & Prokopets, 2022, p. 19). Η επιρροή δύναται να αφορά ακόμα και την πολιτική συμμετοχή καθώς, οι πολίτες που παρακολουθούνται μπορεί να αισθάνονται υποχρεωμένοι να απέχουν από την εμπλοκή σε αλληλεπιδράσεις πολιτικού περιεχομένου, από το να εκφράζουν ειλικρινά τις απόψεις τους και από το να συνδέονται με άλλους για πολιτικούς σκοπούς. Αυτό επηρεάζει την ποιότητα της δημοκρατικής δημόσιας σφαίρας, η οποία τελικά βασίζεται στην εισροή και τις αντιδράσεις των πολιτών. Πιο συγκεκριμένα, το κακόβουλο λογισμικό παρακολούθησης επηρεάζει άτομα όπως δημοσιογράφους, πολιτικούς και ακτιβιστές που έχουν ειδικό ρόλο στη δημόσια σφαίρα. Η παρακολούθηση τέτοιων ατόμων δημιουργεί χώρο για καταπίεση, χειραγώγηση, εκβιασμό, παραποίηση και δυσφήμιση. Γι’ αυτό και χρησιμοποιείται πολύ πιο συχνά από απολυταρχικά καθεστώτα. Η ίδια η εκλογική διαδικασία μπορεί να επηρεαστεί, όταν οι συλλεχθείσες πληροφορίες, ενδεχομένως χειραγωγημένες, χρησιμοποιούνται για τη διεξαγωγή εκστρατειών δυσφήμισης κατά στοχευμένων υποψηφίων ή για την ανάληψη άλλων ενεργειών που επηρεάζουν τις πιθανότητες επιτυχίας τους στις εκλογές (European Parliament , 2022). Αυτή η δυνατότητα εξουσίας πάνω σε πολιτικούς αποκαλύφθηκε και από την υπόθεση Σνόουντεν για τις παρακολουθήσεις της NSA (Greenwald, 2014) Ο ίδιος ο φόβος της παρακολούθησης μπορεί να ωθήσει τους ανθρώπους να αποφύγουν να θέσουν υποψηφιότητα ή να διεξάγουν αποτελεσματική εκστρατεία (European Parliament , 2022). Ο Επίτροπος Ανθρωπίνων Δικαιωμάτων του Συμβουλίου της Ευρώπης προειδοποίησε ότι, πέρα από τις επιπτώσεις του στην ιδιωτική ζωή, «το κατασκοπευτικό λογισμικό έχει αποτρεπτικό αποτέλεσμα σε άλλα ανθρώπινα δικαιώματα και θεμελιώδεις ελευθερίες» καθώς μπορεί να

«δημιουργήσει ένα κλίμα αυτολογοκρισίας και φόβου». Αυτό εμποδίζει τα άτομα να ασκήσουν την ελευθερία της έκφρασης και να συμμετάσχουν στη δημόσια, πολιτική ζωή (Riecke, 2023).

Οι επεμβατικές τεχνολογίες παρακολούθησης έχουν ένα ψυχολογικό αποτρεπτικό αποτέλεσμα και σε άλλα ανθρώπινα δικαιώματα και θεμελιώδεις ελευθερίες και όχι μόνο στο δικαίωμα στην ιδιωτικότητα και στην ελευθερία της έκφρασης. Για παράδειγμα, το δικαίωμα στην υγεία μπορεί επίσης να επηρεαστεί από τις ψηφιακές πρακτικές παρακολούθησης, καθώς τα άτομα μπορεί να απέχουν από το να μοιράζονται ευαίσθητα δεδομένα υγείας με επαγγελματίες υγείας, φοβούμενα ότι η εμπιστευτικότητα μπορεί να παραβιαστεί. Η ελευθερία της θρησκείας μπορεί επίσης να επηρεαστεί, ειδικά εάν η σφραγίδα της εξομολόγησης και η προνομιακή επικοινωνία με θρησκευτικούς λειτουργούς υποκλέπτονται. Η στοχευμένη ή μαζική παρακολούθηση δημιουργεί επίσης ένα κλίμα αυτολογοκρισίας. Φοβούμενοι ότι κάθε ενέργεια και κίνηση βρίσκονται υπό παρακολούθηση, οι άνθρωποι θα είναι λιγότερο πιθανό να επικοινωνούν για συγκεκριμένα θέματα διαδικτυακά ή εκτός διαδικτύου. Το αποτρεπτικό αποτέλεσμα της παρακολούθησης μπορεί επίσης να οδηγήσει σε κοινωνική απομόνωση (Kaldani & Prokopets, 2022, p. 19). Η συσσώρευση του τεράστιου όγκου πληροφοριών που έχουν συλλεγεί από τα μέσα επικοινωνίας και καταλήγουν στη διάθεση είτε του κράτους είτε ιδιωτών γεννά τον κίνδυνο εκβιασμών (Παπανικολάου, 2025, σ. 642). Συνολικά, η κατάχρηση spyware αποτελεί υπαρξιακή απειλή για τη δημοκρατία και το κράτος δικαίου (Riecke, 2023).

Συμπερασματικά, η παραβίαση του ιδιωτικού χώρου των πολιτών τους οδηγεί στον φόβο, την καχυποψία και την αυτολογοκρισία. Κάτω από αυτές τις συνθήκες δεν δημιουργούνται οι πολίτες τους οποίους χρειάζεται μια δημοκρατική κοινωνία. Συνεπώς η διασφάλιση του δικαιώματος είναι απαραίτητος όρος για την προστασία θεμελιωδών συνταγματικών ατομικών δικαιωμάτων και ελευθεριών, όπως η ελεύθερη ανάπτυξη της προσωπικότητας, η ελευθερία έκφρασης, η δημοσιογραφική ελευθερία κα, η προστασία δηλαδή του κράτους δικαίου και της ίδιας της δημοκρατίας (Παπανικολάου, 2025, σ. 643).

5.2 General Data Protection Regulation (GDPR) και όρια εφαρμογής

Το άρθρο 23 του GDPR δεν αποτελεί απλώς νομικό κενό. Αποτελεί το κατεξοχήν νομικό εργαλείο που καθιστά εφικτό το δεύτερο στάδιο του data laundering, το layering. Η δυνατότητα επίκλησης εθνικής ασφάλειας χωρίς ανεξάρτητη εποπτεία λειτουργεί ως θεσμικά κωδικοποιημένος μηχανισμός απόκρυψης της παράνομης προέλευσης δεδομένων.

Ο GDPR αποτελεί το θεμελιώδες ευρωπαϊκό εργαλείο προστασίας προσωπικών δεδομένων αλλά περιέχει ένα δομικό κενό που η βιομηχανία spyware αξιοποιεί άμεσα, την εξαίρεση εθνικής ασφάλειας του άρθρου 23 (Regulation (EU) 2016/679 (GDPR), άρθρο 23.).[9] Η

[9] Η διάταξη επιτρέπει στα κράτη-μέλη να περιορίζουν τα δικαιώματα υποκειμένων δεδομένων «για λόγους εθνικής ασφάλειας», χωρίς να ορίζει ρητά τα όρια αυτής της εξαίρεσης.

εξαίρεση επιτρέπει στα κράτη-μέλη να παρεκκλίνουν από τις βασικές αρχές του GDPR συμπεριλαμβανομένης της διαφάνειας, της ενημέρωσης του υποκειμένου και της δικαστικής προσβολής, με απλή επίκληση εθνικής ασφάλειας.

Η έννοια της εθνικής ασφάλειας συνιστά αόριστη και γενική νομική έννοια, και ως εκ τούτου επιδεικτική καταχρηστικών εφαρμογών, αλλά όχι υπέρτατο αγαθό όπως συμβαίνει σε αυταρχικά και δικτατορικά καθεστώτα. Οι έννοιες εθνική ασφάλεια και δημόσια τάξη μπορεί να τέμνονται αλλά δεν ταυτίζονται Σε μια δημοκρατική κοινωνία η εθνική ασφάλεια απαιτείται για να εξασφαλίζει την ελευθερία, δηλαδή την ομαλή λειτουργία του κράτους και την πλήρη απόλαυση των ατομικών και κοινωνικών δικαιωμάτων από τους πολίτες (Παπανικολάου, 2025, σσ. 649-650).

Η νομολογία του ΔΕΕ έχει προσπαθήσει να θέσει όρια στη χρήση αυτής της εξαίρεσης (ΔΕΕ, 2020) Ωστόσο, το πρόβλημα παραμένει δομικό. Η κρίση περί «εθνικής ασφάλειας» γίνεται εθνικά, χωρίς ευρωπαϊκή εποπτεία, και συχνά χωρίς ανεξάρτητη δικαστική αξιολόγηση. Ο αυξημένος κίνδυνος κατάχρησης μπορεί να αντισταθμιστεί μόνο από κατάλληλους εποπτικούς μηχανισμούς ως θεσμικό αντίβαρο. Τέτοια θεσμικά αντίβαρα είναι οι ανεξάρτητες αρχές αλλά και η θέσπιση αιτιολόγησης από τις εισαγγελικές αρχές, της απόφασης περί άρσης του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας (Παπανικολάου, 2025, σ. 650). Η μη εφαρμογή των παραπάνω καθιστούν το άρθρο 23 GDPR τον πιο αδύναμο κρίκο του ευρωπαϊκού πλαισίου προστασίας δεδομένων.

Η Οδηγία ePrivacy (2002/58/ΕΚ) ρυθμίζει την εμπιστευτικότητα των ηλεκτρονικών επικοινωνιών και αποτελεί το lex specialis απέναντι στον GDPR για τον τομέα αυτό (ΕΔΑΔ, 2015).[10] Το άρθρο 15 της Οδηγίας επιτρέπει στα κράτη-μέλη να παρεκκλίνουν από την αρχή εμπιστευτικότητας για λόγους εθνικής ασφάλειας, δημόσιας ασφάλειας ή δίωξης ποινικών αδικημάτων, δημιουργώντας ένα ευρύ παράθυρο που εθνικές νομοθεσίες έχουν αξιοποιήσει εκτεταμένα (ΕΔΑΔ, 2016)[11]

Η νομολογία του ΕΔΔΑ έχει θέσει αυστηρά κριτήρια για τη νόμιμη παρακολούθηση: νομική βάση, αναγκαιότητα σε δημοκρατική κοινωνία, αναλογικότητα και ανεξάρτητη εποπτεία (Directive 2002/58/EC (ePrivacy Directive), άρθρο 15).[12] Τα κριτήρια αυτά, παγιωμένα στις αποφάσεις Zakharov (2015) και Szabó (2016), που αναφέρθηκαν παραπάνω δεν έχουν ενσωματωθεί επαρκώς στις εθνικές νομοθεσίες κρατών-μελών της ΕΕ, συμπεριλαμβανομένης της ελληνικής (Kaldani & Prokopets, 2022, σσ. 30-38)

[10] Το ΕΔΔΑ έθεσε για πρώτη φορά αυστηρές απαιτήσεις για τη νομιμότητα κρατικής παρακολούθησης: νομική βάση, αναγκαιότητα, αναλογικότητα και ανεξάρτητη εποπτεία.

[11] Ιδιαίτερα σχετική για την ελληνική υπόθεση είναι η κρίση για τη «δικαστική εξαίρεση» σε υποθέσεις εθνικής ασφάλειας.

[12] Η διάταξη επιτρέπει στα κράτη-μέλη να παρεκκλίνουν από την εμπιστευτικότητα επικοινωνιών για λόγους εθνικής ασφάλειας, δημόσιας ασφάλειας ή δίωξης ποινικών αδικημάτων.

Η εγκληματολογική ανάλυση που προηγήθηκε συνιστά τη βάση για την αξιολόγηση του ισχύοντος νομικού πλαισίου και τη διατύπωση προτάσεων βελτίωσης. Το παρόν κεφάλαιο εξετάζει το κανονιστικό πλαίσιο σε ευρωπαϊκό, διεθνές και εθνικό, αναδεικνύει τα δομικά του κενά και καταλήγει σε προτάσεις de lege ferenda.

Οι περισσότερες διεθνείς συμβάσεις και νομοθεσίες για την ιδιωτική ζωή διαμορφώθηκαν πριν τη δεκαετία του 1980, εποχή κατά την οποία τεχνολογίες spyware ήταν αδύνατο να προβλεφθούν. Αυτό καθιστά το υφιστάμενο νομικό πλαίσιο ανεπαρκές για τις σύγχρονες ψηφιακές απειλές. Συνεπώς, η απουσία ενός ενιαίου, καθολικά αποδεκτού ορισμού της ιδιωτικής ζωής, σε συνδυασμό με τη ραγδαία τεχνολογική πρόοδο, καθιστά αναγκαία την αναθεώρησή του ώστε να συμπεριλαμβάνει το δικαίωμα κάθε ατόμου να ελέγχει την πρόσβαση στα προσωπικά του δεδομένα. Έχουν ήδη γίνει σημαντικά βήματα όπως ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ που αναγνωρίζει χωριστά την προστασία δεδομένων, ενώ το ΕΔΔΑ και η υπόθεση Schrems έχουν θέσει σαφή όρια στη μαζική πρόσβαση σε ηλεκτρονικές επικοινωνίες (Saxena, & Anand, 2022).

Το δικαίωμα στην ιδιωτική ζωή είναι ένα παγκοσμίως αναγνωρισμένο δικαίωμα, ενσωματωμένο σε πολλά εθνικά νομοθετικά δίκαια. Στο αρθ 17 του Διεθνούς Συμφώνου για τα Ατομικά και πολιτικά δικαιώματα (ICCPR 1966) τα συμβαλλόμενα μέρη υποχρεούνται να διασφαλίζουν τα ατομικά και πολιτικά δικαιώματα των ανθρώπων. Πιο συγκεκριμένα κανείς δεν μπορεί να υποβληθεί σε αυθαίρετες ή παράνομες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία και καθένας έχει δικαίωμα στην προστασία από τέτοιες παρεμβάσεις (αρθ 17 International Coventation Civil and Political Rights, 1966). Ομοίως στο αρθρ 12 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου. Το 1988 το πεδίο εφαρμογής του δικαιώματος στην ιδιωτική ζωή επεκτάθηκε με την υιοθέτηση του Γενικού σχολίου 16 για το αρθρ 17 του ICCPR στην αρχή της αναγνώρισης των ανησυχιών για την παρακολούθηση στον κυβερνοχώρο (Krishna & Atul, 2022)

Και στην νομολογία της ΕΕ εντοπίζεται επίσης μια παρεμφερής προσέγγιση. Το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (ΕΔΔΑ) στην πρόσφατη υπόθεση Schrems κατά επιτρόπου προστασίας δεδομένων κρίθηκε ότι ακόμα και η νομοθεσία που επιτρέπει στις κυβερνητικές αρχές μια γενικευμένη βάση για το περιεχόμενων των ηλεκτρονικών υπηρεσιών, παραβιάζει τη βασική συνιστώσα του δικαιώματος στην ιδιωτική ζωή που το αρθρ 7 του χάρτη των θεμελιωδών δικαιωμάτων της ΕΕ εγγυάται (Krishna & Atul, 2022). Εν κατακλείδι το δικαίωμα ενός ατόμου στην ιδιωτική ζωή είναι μια εγγενή νομική αρχή σε διεθνές και εθνικό επίπεδο.

5.3 Ευρωπαϊκό και διεθνές Ρυθμιστικό Πλαίσιο

Το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων έχει αναπτύξει εκτεταμένη νομολογία σχετικά με την παρακολούθηση και το άρθρο 8 της ΕΣΔΑ, η οποία είναι άμεσα συναφής με την περίπτωση του Predator.

Η θεμελιώδης αρχή που διατρέχει τη νομολογία του ΕΔΔΑ είναι ότι κάθε παρακολούθηση από κρατικούς φορείς πρέπει να πληροί τρεις σωρευτικές προϋποθέσεις: να προβλέπεται από νόμο, να είναι αναγκαία σε δημοκρατική κοινωνία και να είναι αναλογική προς τον επιδιωκόμενο σκοπό. Οι προϋποθέσεις αυτές διατυπώθηκαν αρχικά στην υπόθεση Klass κατά Γερμανίας (1978), όπου το Δικαστήριο αναγνώρισε για πρώτη φορά ότι η μυστική παρακολούθηση συνιστά σοβαρή απειλή για τα δικαιώματα που κατοχυρώνει η ΕΣΔΑ, και ότι τα κράτη οφείλουν να διαθέτουν επαρκείς εγγυήσεις κατά της αυθαιρεσίας (ΕΔΔΑ, 1978).

Η σημαντικότερη απόφαση για την ψηφιακή εποχή είναι η Big Brother Watch κατά Ηνωμένου Βασιλείου (2021), με την οποία το ΕΔΔΑ έκρινε ότι το καθεστώς μαζικής παρακολούθησης που εφάρμοζε το Ηνωμένο Βασίλειο παραβίαζε το άρθρο 8 της ΕΣΔΑ, καθώς δεν προέβλεπε επαρκείς εγγυήσεις επιλογής, εξέτασης και χρήσης των παρακολουθούμενων δεδομένων. Η απόφαση αυτή είναι ιδιαίτερα σημαντική για την παρούσα εργασία διότι το Δικαστήριο υπογράμμισε ότι η απουσία εκ των υστέρων ενημέρωσης των θυμάτων, ακριβώς αυτό που κατήργησε ο Ν. 4790/2021 στην Ελλάδα, αποτελεί καθαυτή παραβίαση της Σύμβασης (ΕΔΔΑ, 2021). Στην απόφαση αυτή αποκρυσταλλώνονται οι θέσεις του ΕΔΔΑ, ως προς τις προϋποθέσεις νόμιμης χρήσης συστημάτων παρακολούθησης. Η απόφαση αυτή πραγματεύεται κρίσιμα νομικά ζητήματα ως προς την οριοθέτηση περιορισμών ως προς τη χρήση αυτών των τεχνολογιών. Το σπουδαιότερο με την απόφαση είναι ο αντίκτυπος στο πολιτικό πεδίο καθώς απαιτείται η ισορροπημένη συναίρεση ασφάλειας και ελευθερίας. Σύμφωνα με την απόφαση του ΕΔΔΑ εξαιτίας του πλήθους και της πολυπλοκότητας των απειλών στην ασφάλεια στη σύγχρονη κοινωνία, η χρήση των επίμαχων συστημάτων δεν αντίκειται στη Σύμβαση αλλά εξειδίκευσε τις προϋποθέσεις για τη χρήση τους ώστε να είναι σύμφωνη με το αρθρο 8 του ΕΣΔΑ. Προϋποθέσεις οι οποίες δεν πληρούνταν στην επίμαχη υπόθεση. Ουσιαστικά το δικαστήριο κανονικοποιεί με την απόφαση του τη χρήση αυτών των μέσων ως αποδεκτών στο πεδίο της εθνικής ασφάλειας. Καταληκτικά, η συμβατότητα των μαζικών παρακολουθήσεων με το άρθρο 8 ΕΣΔΑ προϋποθέτει εγγυήσεις για την αναλογικότητα και νομιμότητα των μέτρων οι οποίες πρέπει να αξιολογούνται σε κάθε στάδιο της διαδικασίας. Σημαντικό στην παρούσα απόφαση είναι η απαίτηση εποπτείας από ανεξάρτητο όργανο αλλά και η απαίτηση χρήσης λέξεων κλειδιών-αναζήτησης ώστε να γίνεται εστίαση μόνο στα δεδομένα που συνδέονται με τον σκοπό. Η δεύτερη απαίτηση προστατεύει την αδιάκριτη προσπέλαση στα δεδομένα που δεν συνδέονται με το σκοπό (Παπανικολάου, 2025, σσ. 253-254). Επίσης, σημαντική από την υπόθεση αυτή είναι η διατύπωση ότι οι μαζικές παρακολουθήσεις είναι εξ ορισμού μη στοχευμένες και άρα δεν

απαιτείται «εύλογη υποψία». Η απαίτηση « εύλογης υποψίας» την οποία οι ενάγοντες ζήτησαν ως προϋπόθεση παρακολούθησης περιορίζεται στις περιπτώσεις στοχευμένης παρακολούθησης (Παπανικολάου, 2025, σ. 256).

Εξίσου σημαντική είναι η Zakharov κατά Ρωσίας (2015), στην οποία το ΕΔΔΑ διαπίστωσε παραβίαση του άρθρου 8 λόγω της απουσίας ανεξάρτητης εποπτείας των μυστικών υπηρεσιών. Το Δικαστήριο έκρινε ότι η υπαγωγή των υπηρεσιών πληροφοριών στην εκτελεστική εξουσία χωρίς ανεξάρτητο δικαστικό έλεγχο δεν συνάδει με τις απαιτήσεις της Σύμβασης, πρόβλημα που εντοπίζεται με ιδιαίτερη οξύτητα στην ελληνική περίπτωση (ΕΔΔΑ, 2015).

Τέλος, η Szabó και Vissy κατά Ουγγαρίας (2016) αποτελεί την πιο άμεσα συναφή απόφαση με τη βιομηχανία spyware, καθώς το ΕΔΔΑ εξέτασε για πρώτη φορά καθεστώς στοχευμένης παρακολούθησης που επέτρεπε την υποκλοπή ηλεκτρονικών επικοινωνιών χωρίς προηγούμενη δικαστική εξουσιοδότηση. Το Δικαστήριο έκρινε ότι η δυνατότητα παρακολούθησης «οποιουδήποτε» με μόνη βάση την επίκληση εθνικής ασφάλειας παραβιάζει κατάφωρα το άρθρο 8 (ΕΔΔΑ, 2016).

Συνολικά, η νομολογία του ΕΔΔΑ θέτει ένα σαφές κανονιστικό πλαίσιο το οποίο η χρήση του Predator στο Predatorgate παραβιάζει συστηματικά, με την απουσία νομικής βάσης για τη χρήση εμπορικού spyware, απουσία ανεξάρτητης εποπτείας, και κατάργηση του δικαιώματος εκ των υστέρων ενημέρωσης των θυμάτων. Επιπλέον, απαιτεί να τηρούνται αυστηροί διαδικαστικοί εγγυητικοί κανόνες όταν επιχειρείται από κράτος μέλος του Συμβουλίου της Ευρώπης κάποιος περιορισμός στο δικαίωμα. Ο ΕΔΔΑ λοιπόν, απαιτεί να υπάρχει εθνικός ποιοτικός νόμος, το θεσπιζόμενο μέτρο να είναι πράγματι αναγκαίο και να μην υπερβαίνει ότι μπορεί να είναι ανεκτό βάσει της σύγχρονης αντίληψης περι φιλελεύθερης δημοκρατίας (Παπανικολάου, 2025, σ. 648).

Σχετικά με τις μαζικές παρακολουθήσεις για την προστασία της εθνικής ασφάλειας το ΕΔΔΑ απαιτεί επαρκή και αποτελεσματικά εχέγγυα για την αποτροπή ενδεχόμενων καταχρήσεων. Επιμένει στην αναζήτηση σημείου ισορροπίας μεταξύ των οριζόντιων παρακολουθήσεων και του ιδιωτικού βίου. Οι γενικευμένες παρακολουθήσεις κατατάσσονται από τον ΕΔΔΑ στην κορυφή της κλίμακας των τεχνολογικών κινδύνων που παράγονται σε βάρος του δικαιώματος στον ιδιωτικό βίο. Συνεπώς, οι κανονιστικές πρόνοιες για την χρήση και αξιοποίηση των ευρημάτων από τις παρακολουθήσεις πρέπει να υπόκεινται σε δικαιοδοτικό έλεγχο ως προς τη συμβατότητα τους με την ΕΣΔΑ (Παπανικολάου, 2025, σσ. 246-247).

Η αλλαγή πρέπει να είναι ταυτόχρονη σε διεθνές και εθνικό επίπεδο, επηρεάζοντας δικαστήρια, νομοθέτες και εταιρείες, ώστε το δικαίωμα στην ιδιωτική ζωή να ανταποκρίνεται στις απαιτήσεις της ψηφιακής εποχής παγκόσμια. Επειδή οι φορείς του επίσημου κοινωνικού ελέγχου είναι μέρος του προβλήματος και όχι η λύση του, η αντιμετώπιση του φαινομένου

απαιτεί δράσεις σε υπερεθνικό επίπεδο που θα σπάσουν το μείγμα απάθειας, παραπληροφόρησης και αποσιώπησης που αποτελεί γόνιμο έδαφος για την ανάπτυξή του (Γεωργούλας, 2019, σ. 59)

Το πεδίο εφαρμογής του ΔΣΑΠΔ, όπως ορίζεται στο άρθρο 2 παράγραφος 1, εκτείνεται σε όλα τα πρόσωπα που βρίσκονται «εντός της επικράτειας και υπόκεινται στη δικαιοδοσία» των υπογραφόντων κρατών. Το ζήτημα τίθεται σχετικά με τον καθορισμό της κρατικής δικαιοδοσίας σε θέματα επιτήρησης στον κυβερνοχώρο. Εδώ, το κύριο ερώτημα είναι αν καλύπτει τα άτομα που δεν ζουν στην επικράτεια του κράτους. Εάν όχι, τότε θα σήμαινε απλώς ότι τα κράτη δεν είναι υποχρεωμένα σε σχέση με άτομα που μπορεί να μην διαμένουν στην επικράτεια του κράτους αλλά βρίσκονται, στην πραγματικότητα, υπό τον «έλεγχο της δικαιοδοσίας του». Ακόμη και οι εθνικές νομοθεσίες σε πολλά ανεπτυγμένα έθνη κάνουν διάκριση μεταξύ της εσωτερικής και της εξωεδαφικής εποπτείας τους όσον αφορά την υποχρέωση που προκύπτει από μια τέτοια συμπεριφορά

Το παραδοσιακό κριτήριο του φυσικού ελέγχου αποδεικνύεται ανεπαρκές στην ψηφιακή εποχή. Εργαλεία όπως το Pegasus μπορούν να παρακολουθούν εξ αποστάσεως οποιονδήποτε, ανεξαρτήτως τοποθεσίας, επιτρέποντας στα κράτη να καταστρατηγούν εύκολα τις υποχρεώσεις τους. Ενδεικτική είναι η υπόθεση Jaloud κατά Ολλανδίας, όπου το ΕΔΔΑ αναγνώρισε εξωεδαφική δικαιοδοσία χωρίς φυσικό έλεγχο του θύματος, θέτοντας προηγούμενο που μπορεί να εφαρμοστεί και στην κυβερνοεπιτήρηση.

Διατυπώνονται πολλαπλές προτάσεις αντιμετώπισης αυτου του θέματος, εστιάζοντας στον «έλεγχο της επικοινωνίας» και όχι στον φυσικό έλεγχο. Η Nyst υποστηρίζει ότι η υποχρέωση ενεργοποιείται μόλις τα δεδομένα υποκλαπούν κάτω από την επικράτεια ενός κράτους (Nyst, 2013), ενώ ο Milanovic διακρίνει μεταξύ της αρνητικής υποχρέωσης (μη παρέμβαση) και της θετικής υποχρέωσης (ενεργή προστασία) του κράτους (Milanovic, 2016).

Το μοντέλο αυτό εξασφαλίζει ισότιμη προστασία ανεξαρτήτως εθνικότητας ή τοποθεσίας, και καλύπτει ακόμη και περιπτώσεις όπου κυβερνήσεις συνεργάζονται με ιδιωτικές εταιρείες επιτήρησης, όπως ο Όμιλος NSO. Την προσέγγιση αυτή ενστερνίζεται και η Γενική Συνέλευση του ΟΗΕ με το ψήφισμα 68/167, καλώντας τα κράτη να αναθεωρήσουν τις πρακτικές μαζικής παρακολούθησης ώστε να διασφαλιστεί η πλήρης συμμόρφωση με το διεθνές δίκαιο ανθρωπίνων δικαιωμάτων (Krishna & Atul, 2022)

5.4 Η Έκθεση PEGA και οι Συστάσεις της

Η Έκθεση PEGA (Μάιος 2023) αποτελεί το πιο ολοκληρωμένο θεσμικό κείμενο για τη ρύθμιση της βιομηχανίας spyware εντός της ΕΕ και το σημαντικότερο θεσμικό ορόσημο για την κατανόηση του φαινομένου. Η επιτροπή PEGA συστάθηκε τον Απρίλιο του 2022, ύστερα από τις αποκαλύψεις του Pegasus Project (2021) και τις επακόλουθες αποκαλύψεις για τη χρήση εμπορικών spyware κατά πολιτικών, δημοσιογράφων και ακτιβιστών σε κράτη μέλη της ΕΕ.

Έπειτα από δεκατετράμηνη έρευνα μέσω ακροάσεων θυμάτων παρακολούθησης, τεχνικών εμπειρογνωμόνων και εκπροσώπων κυβερνήσεων και εταιρειών του κλάδου κατέληξε σε μια έκθεση που για πρώτη φορά σε ευρωπαϊκό θεσμικό επίπεδο αναγνώρισε τη συστημική φύση του προβλήματος (PEGA Committee, 2023)

Οι κύριες συστάσεις της περιελάμβαναν την απαγόρευση χρήσης spyware κατά ευρωβουλευτών, δημοσιογράφων και ακτιβιστών αναγνωρίζοντας ότι η στόχευση αυτών των κατηγοριών δεν αποτελεί απλώς ατομική παραβίαση αλλά επίθεση στη δημοκρατική λειτουργία. Επιπλέον, τη σύσταση ανεξάρτητης ευρωπαϊκής αρχής τεχνικής έρευνας, ικανής να ανιχνεύει μολύνσεις από εμπορικά spyware ανεξάρτητα από τις εθνικές αρχές, δεδομένου ότι η Επιτροπή διαπίστωσε ότι τα περισσότερα κράτη-μέλη στερούνται τεχνικής ικανότητας να το πράξουν μόνα τους. Ακόμα συστήνει την αναθεώρηση της εξαίρεσης εθνικής ασφάλειας του άρθρου 23 GDPR, η οποία, όπως αναλύθηκε στο Κεφάλαιο 3, αποτελεί τον κεντρικό νομικό μηχανισμό του layering στη διαδικασία του data laundering. Τέλος, συστήνει την ευρωπαϊκή εναρμόνιση των εξαγωγικών αδειών κυβερνο-επιτήρησης, ώστε να παύσει η εθνική χορήγηση αδειών με βάση οικονομικά και διπλωματικά κριτήρια αντί για κριτήρια ανθρωπίνων δικαιωμάτων (PEGA Committee, 2023, pp. 100-115)

Ιδιαίτερης σημασίας για την παρούσα εργασία είναι η διαπίστωση της Επιτροπής PEGA ότι η αποτυχία λογοδοσίας στις υποθέσεις spyware δεν οφείλεται σε έλλειψη νομικού πλαισίου αλλά σε συστηματική αδυναμία εφαρμογής του. Η Επιτροπή εντόπισε τρία δομικά εμπόδια, την κατάχρηση της εξαίρεσης εθνικής ασφάλειας ως ασπίδα αδιαφάνειας, την απουσία ανεξάρτητης δικαστικής εποπτείας των υπηρεσιών πληροφοριών, και την αδυναμία των θυμάτων να αποδείξουν τη μόλυνση χωρίς εξειδικευμένη τεχνική υποστήριξη. Και τα τρία αυτά εμπόδια αντιστοιχούν ακριβώς στα στάδια του data laundering που η παρούσα εργασία ανέλυσε: το placement μέσω των εξαγωγικών αδειών, το layering μέσω της εξαίρεσης εθνικής ασφάλειας, και το integration μέσω της χρήσης δεδομένων σε επίσημες διαδικασίες χωρίς αμφισβήτηση της προέλευσής τους (PEGA Committee, 2023).

Ωστόσο, οι συστάσεις PEGA παραμένουν μη δεσμευτικές. Ουδεμία νομοθετική πρωτοβουλία ακολούθησε σε επίπεδο ΕΕ, αποδεικνύοντας ότι η πολιτική βούληση, ιδιαίτερα των κρατών-μελών που εμπλέκονται, αποτελεί το κυριότερο εμπόδιο, αποκαλύπτοντας μια βαθύτερη αντίφαση, ότι η ΕΕ διαθέτει το θεσμικό πλαίσιο για να διαγνώσει το πρόβλημα αλλά όχι την πολιτική βούληση να το αντιμετωπίσει. Η αντίφαση αυτή δεν είναι τυχαία. Τα κράτη-μέλη που εμπλέκονται στα σκάνδαλα spyware, μεταξύ των οποίων η Ελλάδα, η Ισπανία και η Ουγγαρία, είναι τα ίδια που θα έπρεπε να συναινέσουν σε δεσμευτική ευρωπαϊκή ρύθμιση. Η αρχή της ομόφωνης απόφασης στο Συμβούλιο σε θέματα εθνικής ασφάλειας μετατρέπεται έτσι σε δομικό εμπόδιο μεταρρύθμισης καθώς, κάθε εμπλεκόμενο κράτος-μέλος έχει de facto δικαίωμα αρνησικυρίας. Από εγκληματολογική σκοπιά, η αδυναμία εφαρμογής των συστάσεων PEGA

επιβεβαιώνει αυτό που οι Green και Ward (2004) περιέγραψαν ως δομική ατιμωρησία. Τα κράτη που τελούν το έγκλημα ελέγχουν τους ίδιους τους μηχανισμούς στους οποίους θα έπρεπε να λογοδοτούν, αναπαράγοντας έτσι συστημικά την ατιμωρησία που η θεωρία του κρατικο-εταιρικού εγκλήματος έχει αναγνωρίσει ως κεντρικό χαρακτηριστικό του φαινομένου. (Green, P. & Ward, T. , 2004)

5.5 Το Ελληνικό Ρυθμιστκό Πλαίσιο

Το ελληνικό εθνικό πλαίσιο αποτελεί χαρακτηριστικό παράδειγμα της τρίτης διάστασης του data laundering, του integration. Ο Ν. 4790/2021, απαγορεύοντας στην ΑΔΑΕ να ενημερώνει εκ των υστέρων τα θύματα, δεν αποτελεί απλώς παράβαση δικαιώματος. Αποτελεί νομοθετικά κατοχυρωμένο μηχανισμό που εξασφαλίζει ότι τα παράνομα δεδομένα θα παραμείνουν ενσωματωμένα στο σύστημα χωρίς ποτέ να αμφισβητηθεί η προέλευσή τους.

Παρότι στο Σύνταγμα του 1844 περιλαμβανόταν διάταξη σχετική με το απόρρητο των επικοινωνιών, διάταξη η οποία επαναλήφθηκε και στα επόμενα Συντάγματα με την προσθήκη επιπλέον ρύθμισης η οποία περιλάμβανε εκτός από το απόρρητο των επιστολών και το απόρρητο των τηλεγραφημάτων και τηλεφωνημάτων, γεγονότα όπως πόλεμοι, εμφύλιοι και δικτατορίες δεν επέτρεψαν την αποτελεσματική προστασία του δικαιώματος. Έμφαση, μέχρι τη Μεταπολίτευση, δινόταν η προστασία του κράτους από κινδύνους και όχι η προστασία των δικαιωμάτων των πολιτών. Στο αρθρο 19 του Συντάγματος διατυπώνεται πλήρως τι αποτελεί αντικείμενο της προστασίας του.

Το ελληνικό νομοθετικό πλαίσιο για την παρακολούθηση διαμορφώνεται κυρίως από δύο νόμους: τον Ν. 2225/1994 για την προστασία του απορρήτου επικοινωνιών και τον Ν. 3115/2003 που ίδρυσε την ΑΔΑΕ. Το πλαίσιο αυτό παρουσιάζει τρία θεμελιώδη κενά.

Παρότι προστατεύεται συνταγματικά το απαραβίαστο δικαίωμα, στην ίδια διάταξη το άρθρο 19 του Συντάγματος εξαιρεί ρητά την εθνική ασφάλεια ή την διακρίβωση πολύ σοβαρών εγκλημάτων από τις εγγυήσεις απορρήτου, χωρίς να απαιτεί ανεξάρτητη δικαστική έγκριση για κάθε παρακολούθηση. Η έννοια της εθνικής ασφάλειας έχει ιδιαίτερο νομικό και πολιτικό χαρακτήρα και είναι αρκετά αόριστη. Η προστασία της εξασφαλίζει την ύπαρξη και λειτουργία των κρατών, την ομαλή συμβίωση της κοινωνίας και τις συνθήκες που κάθε άτομο μπορεί να αναπτύσσει την προσωπικότητα του. Επειδή όμως, αυτές οι έννοιες είναι ασαφείς και γενικές υπάρχει ο κίνδυνος να χρησιμοποιηθούν αυθαίρετα αφήνοντας περιθώριο στις αρχές να αποφασίζουν κατά περίπτωση πως θα τις εφαρμόσουν (Παπανικολάου, 2025, σ. 13) Η οριοθέτηση του δικαιώματος κατά την επιβολή περιορισμών για λόγους εθνικής ασφάλειας διέρχεται από την κρίση των οργάνων της ποινικής δικαιοσύνης ενώ οι όροι και η διαδικασία επιβολής του μέτρου υπόκεινται στον έλεγχο της ανεξάρτητης αρχής (ΑΔΑΕ) (Παπανικολάου,

2025, σ. 12). Η ΑΔΑΕ έχει εποπτικές αρμοδιότητες αλλά δεν έχει πρόσβαση σε υποθέσεις που χαρακτηρίζονται «απόρρητες» για λόγους εθνικής ασφάλειας.

Τα περισσότερα κράτη ασχολήθηκαν με την ψηφιακή επιτήρηση για την προώθηση της λεγόμενης εθνικής τους ασφάλειας. Είναι αμφίβολο εάν μια τέτοια συμπεριφορά μπορεί να θεωρηθεί εγγενής κρατική δραστηριότητα που περιορίζεται μόνο στο κράτος (Zuboff, S., 2019). Η κρατική συμμετοχή δίνει στην πράξη της παρακολούθησης κάποιο είδος δικαιολογημένης νομιμότητας, που υποστηρίζεται από λόγους όπως η αντιμετώπιση τρομοκρατικών ενεργειών ή άλλων άκρως εγκληματικών ενεργειών. Διαφορετικά, αυτή η παρακολούθηση στον κυβερνοχώρο είναι από μόνη της εκ πρώτης όψεως παράνομη

Στην Ελλάδα οι περισσότερες αποφάσεις του απορρήτου γίνονται για λόγους προστασίας της εθνικής ασφάλειας. Σημαντικό είναι να εξεταστεί εάν η διαδικασία έχει επαρκείς εγγυήσεις και εάν είναι σύμφωνες με όσα προβλέπει το Σύνταγμα. Σημαντικό είναι επίσης να οριστεί τί σημαίνει εθνική ασφάλεια καθώς το πώς ερμηνεύεται επηρεάζεται από αξιακές και πολιτικές επιλογές. Χαρακτηριστική έιναι η τοποθέτηση του Μ Γλέζου το ΄86 κατά την τοποθέτηση του για το άρθρο 48 του Συντάγματος ότι « όλοι όσοι κατέλυσαν το δημοκρατικό πολίτευμα είχαν ως προμετωπίδα το πρόσχημα της εθνικής ασφάλειας» (Παπανικολάου, 2025, σ. 16)

Τέλος, και πιο κρίσιμο κενό είναι η πλήρης απουσία ειδικής νομοθεσίας για την αγορά, χρήση και εξαγωγή εμπορικών spyware από κρατικούς φορείς. Αυτό σημαίνει ότι η απόκτηση του Predator από ελληνικές αρχές δεν παραβίαζε κανένα ρητό νομοθετικό απαγορευτικό, κενό που η Intellexa εκμεταλλεύτηκε συστηματικά και που η έκθεση PEGA (2023) χαρακτήρισε ως κεντρικό παράγοντα της δομικής ατιμωρησίας στην ελληνική περίπτωση (European Parliament PEGA Committee, 2023).

5.6 Προτάσεις De Lege Ferenda

Για την νομολογιακή αντιμετώπιση των παρακολουθήσεων μέσω λογισμικών spyware που μάλιστα σε πολλές επιβεβαιωμένες υποθέσεις αφορά μαζικές παρακολουθήσεις, ως συστημικής πηγής διακινδύνευσης του επικοινωνιακού απορρήτου, επιβάλλεται ο επαναπροσδιορισμός του δικαστικού ελέγχου (Παπανικολάου, 2025, σ. 250). Με βάση την ανάλυση που προηγήθηκε, διατυπώνονται οι ακόλουθες προτάσεις de lege ferenda σε τρία επίπεδα.

Σε Ευρωπαϊκό Επίπεδο είναι αναγκαία η αναθεώρηση του άρθρου 23 GDPR ώστε να απαιτεί ανεξάρτητη δικαστική ή ρυθμιστική εποπτεία ως προϋπόθεση για κάθε επίκληση εξαίρεσης εθνικής ασφάλειας. Η εξαίρεση δεν πρέπει να αποτελεί «ασπίδα» αλλά εξαίρεση αυστηρώς ελεγχόμενη. Επιπλέον, απαραίτητη είναι και η ευρωπαϊκή εναρμόνιση των εξαγωγικών αδειών κυβερνο-επιτήρησης: αντί για εθνική χορήγηση, θέσπιση κεντρικού ευρωπαϊκού μηχανισμού αδειοδότησης με κριτήρια ανθρωπίνων δικαιωμάτων. Η ρήτρα catch-all του

Κανονισμού 2021/821 πρέπει να εφαρμόζεται υποχρεωτικά. Ακόμα, η σύσταση ανεξάρτητης ευρωπαϊκής τεχνικής αρχής για τη διερεύνηση υποθέσεων spyware εντός ΕΕ, ανάλογη με την OLAF για τις οικονομικές απάτες. Κατα την επικαιροποίηση μεθοδολογικά των ελέγχων που ασκούνται από τον ΕΣΔΑ σε συνάρτηση με την τεχνολογικά εξελιγμένη φύση των περιστατικών επι των οποίων εφαρμόζονται οι κανόνες, απαιτείται κατανόηση των πραγματολογικών δεδομένων που αφορούν τεχνολογίες αιχμής. Η νομική επιστήμη δεν μπορεί να είναι αυτάρκης αλλά είναι απαραίτητη μια διεπιστημονική προσέγγιση και ευρύτερες συνέργειες για την οριστικοποίηση νομικών λύσεων (Παπανικολάου, 2025, σ. 248).

Σε εθνικό επίπεδο το κυριότερο νομικό κενό εντοπίζεται στο άρθρο 19 του Συντάγματος, το οποίο, όπως αναλύθηκε στο Κεφάλαιο 5, επιτρέπει παρακολουθήσεις εθνικής ασφάλειας χωρίς δικαστική εποπτεία και χωρίς πρόσβαση της ΑΔΑΕ στις «απόρρητες» υποθέσεις. Η συνταγματική αναθεώρηση πρέπει να καθιερώσει υποχρεωτική δικαστική έγκριση για κάθε παρακολούθηση ανεξαρτήτως επίκλησης εθνικής ασφάλειας, με πλήρη πρόσβαση της ΑΔΑΕ σε όλες τις υποθέσεις. Η εμπειρία του Predatorgate κατέδειξε ότι η εξαίρεση εθνικής ασφάλειας χωρίς ανεξάρτητη εποπτεία δεν αποτελεί νόμιμη παρέκκλιση αλλά θεσμικά κατοχυρωμένο μηχανισμό ατιμωρησίας. Επιπλέον, απαιτείται ειδική νομοθεσία που να ρυθμίζει την αγορά και χρήση εμπορικών spyware από κρατικούς φορείς, με υποχρεωτική έγκριση από ανεξάρτητο φορέα, δημόσια αναφορά χρήσης και αυστηρές ποινικές κυρώσεις για παράνομη χρήση. Η απουσία τέτοιας νομοθεσίας δεν είναι απλώς νομοτεχνικό κενό αποτελεί, όπως η παρούσα εργασία ανέδειξε, δομική προϋπόθεση για τη λειτουργία του data laundering σε εθνικό επίπεδο.

Εγκληματολογικά, η πιο άμεση απάντηση στο αναλυτικό πρόβλημα που η παρούσα εργασία ανέδειξε είναι η ποινικοποίηση του data laundering ως αυτόνομου αδικήματος. Εφόσον ο μηχανισμός λειτουργεί διαμέσου τριών σταδίων που κανένα υφιστάμενο νομικό πλαίσιο δεν αντιμετωπίζει συνολικά, μόνο η θέσπιση αδικήματος που να καλύπτει και τα τρία στάδια μπορεί να κλείσει το κανονιστικό κενό. Η πιο φιλόδοξη αλλά και πιο αναγκαία πρόταση de lege ferenda είναι η ρητή ποινικοποίηση του data laundering ως αυτόνομου αδικήματος, σε αντιστοιχία με το money laundering. Ένα τέτοιο αδίκημα θα έπρεπε να περιλαμβάνει την εν γνώσει χρήση δεδομένων παράνομης προέλευσης σε δικαστικές ή διοικητικές διαδικασίες, την απόκρυψη της παράνομης προέλευσης δεδομένων μέσω θεσμικών μηχανισμών· και την οργανωμένη διευκόλυνση αυτών των πράξεων από εταιρικούς δρώντες.

ΚΕΦΑΛΑΙΟ 6: Κυβερνοεπιτήρηση στην Ελλάδα

6.1 Η υπόθεση Predator στην Ελλάδα

Η ελληνική περίπτωση δεν αναλύεται εδώ απλώς ως σκάνδαλο παρακολούθησης αλλά ως εμπειρική επιβεβαίωση των τριών σταδίων του data laundering. Η τοποθέτηση (placement) εκδηλώνεται μέσω των εξαγωγικών αδειών και της νόμιμης αγοράς του Predator. Η διαστρωμάτωση (layering) πραγματοποιείται μέσω του Ν. 4790/2021 και της επίκλησης εθνικής ασφάλειας. Χρησιμοποιήθηκε ενδιάμεση εταιρεία προκειμένου να κρυφτεί η προέλευση, offshore εταιρείες ώστε να μην αποκαλυφθεί ποιος παρήγγειλε τις παρακολουθήσεις και η κυβέρνηση αρνήθηκε κάθε εμπλοκή. Η ενσωμάτωση (integration) συντελείται μέσω της χρήσης των δεδομένων σε παράλληλες παρακολουθήσεις με την ΕΥΠ χωρίς ποτέ να ελεγχθεί η προέλευσή τους προκειμένου να αποκτήσουν νομιμοφάνεια.

Το ελληνικό σκάνδαλο Predatorgate αποτελεί το πρωτεύον εμπειρικό υλικό της παρούσας εργασίας. Εφαρμόζει in vivo το θεωρητικό πλαίσιο που αναπτύχθηκε στα προηγούμενα κεφάλαια: κρατικο-εταιρικό έγκλημα, data laundering, ψηφιακό πανοπτικόν. Ταυτόχρονα, αποτελεί ιστορικά μοναδική περίπτωση, η πρώτη παγκοσμίως ποινική καταδίκη στελεχών εμπορικής εταιρείας spyware.

Τον Μάρτιο του 2022, ο δημοσιογράφος Θανάσης Κουκάκης αποκάλυψε δημοσίως ότι είχε πέσει θύμα παρακολούθησης τόσο από την ΕΥΠ όσο και από το spyware Predator (Koukakis, 2022; Τριανταφύλλου, 2026). Τους επόμενους μήνες αποκαλύφθηκε ότι μεταξύ των στόχων συγκαταλεγόταν ο αρχηγός της αξιωματικής αντιπολίτευσης Νίκος Ανδρουλάκης, ευρωβουλευτής και πρόεδρος του ΠΑΣΟΚ, γεγονός που έθεσε άμεσα ζητήματα δημοκρατικής λειτουργίας.

Στην υπόθεση αυτή, η κρατική εμπλοκή λειτούργησε σε δύο παράλληλα επίπεδα, όπως ακριβώς περιγράφει η θεωρία Kramer-Michalowski, δηλαδή τη state-initiated και state-facilitated διπλή μορφή (Kramer, & Michalowski, 2006, pp. 15-22). Ως state facilitated καθώς το κράτος παρείχε το νομικό πλαίσιο το οποίο επέτρεψε τη λειτουργία της Intellexa, αδράνησε εποπτικά και εμπόδισε τη διερεύνηση (European Parliament PEGA Committee, 2023, pp. 45-52). Ως state initiated καθώς, αν και δεν εχει μέχρι σήμερα αποδειχτεί δικαστικά, υπάρχουν ισχυρές ενδείξεις κρατικής εμπλοκής, λόγω της χρονικής σύμπτωσης των παρακολουθήσεων κοινών στόχων μεταξύ predator και ΕΥΠ (Mildebrath, 2022, pp. 1-2) αλλά και εξαιτίας της δήλωσης σε δημοσιογράφο του καταδικασθέντα για την υπόθεση Ταλ Ντίλιαν ότι η εταιρεία του παρέχει υπηρεσίες μόνο σε κυβερνήσεις και υπηρεσίες υποβολής του νόμου (Αναγνωστοπούλου, 2026)) γεγονός που αποκλείει εκ των πραγμάτων μη κρατικό χειριστή. Ο ίδιος αποκάλυψε ότι η αρχιτεκτονική του λογισμικού είναι σχεδιασμένη ώστε η εταιρεία να μην γνωρίζει τους στόχους και τις επιχειρήσεις, καθώς «οι εθνικές υπηρεσίες καθορίζουν τους στόχους και εκτελούν την

επιχείρηση χωρίς τη γνώση μας» (predatorgate.gr, 2026). Αυτή η δήλωση είναι εγκληματολογικά κρίσιμη αφού αποκαλύπτει ότι η αποσύνδεση γνώσης μεταξύ εταιρείας και κράτους δεν είναι τυχαία αλλά σκόπιμα ενσωματωμένη στην αρχιτεκτονική του συστήματος, αποτελώντας έτσι τον πιο εξελιγμένο μηχανισμό διαστρωμάτωσης του data laundering. Η εικόνα της κρατικής εμπλοκής συμπληρώνεται από δημοσιογραφικές αποκαλύψεις που τεκμηριώνουν ότι η Intellexa είχε ενταχθεί σε κοινοπραξία η οποία υπέγραψε συμφωνητικό συνεργασίας με το ΚΕΤΥΑΚ της ΕΥΠ, ενώ ο επικεφαλής της είχε σειρά επαφών με πολιτικά πρόσωπα που του υπέδειξαν τη χρηματοδότηση μέσω ΚΕΜΕΑ (predatorgate.gr, 2026). Πρόκειται για ακριβώς αυτό που οι Green και Ward (2004) περιγράφουν ως θεσμική διευκόλυνση καθώς το κράτος δεν ανέχεται απλώς την εταιρεία αλλά την εντάσσει ενεργά στις δομές του.

Ωστόσο, το πιο αποκαλυπτικό στοιχείο για τη δομική ατιμωρησία δεν είναι η ίδια η παρακολούθηση αλλά η αντίδραση του συστήματος στην αποκάλυψή της. Είναι τεκμηριωμένο στην υπόθεση του Κουκάκη πως υπήρχε μια συγκεκριμένη λογική στην οποία η ΕΥΠ ξεκίνησε τη παρακολούθηση, καταγράφοντας απλές συνομιλίες και μηνύματα όμως όταν η νόμιμη επισύνδεση δεν αρκούσε πλέον, η παρακολούθηση συνεχίστηκε με τη χρήση του predator, το οποίο είχε τη δυνατότητα να βλέπει ακόμα και μέσα από την κάμερα του κινητού τη προσωπική ζωή του θύματος. Και ενώ αυτό συνέβη στο 30% των περιπτώσεων ο αντιεισαγγελέας του Αρείου Πάγου υποστήριξε πως δεν υπήρχε συντονισμός νομιμότητας παρανομίας (Τριανταφύλλου, 2026 σελ 84-85). Επίσης, αντί να ζητήσει από την ΑΔΑΕ στοιχεία για τις νόμιμες επισυνδέσεις επικοινωνιών που γίνονταν για λόγους εθνικής ασφάλειας[13], ο Άρειος Πάγος τα ζήτησε από την ελεγχόμενη ΕΥΠ. Στο πόρισμα του συμπέρανε πως δεν υπήρχε κανένα κοινό κέντρο μεταξύ Predator και ΕΥΠ με αποτέλεσμα το σκέλος της υπόθεσης που αφορούσε την ΕΥΠ να μπει στο αρχείο και να παραπεμφθούν μόνο τέσσερις ιδιώτες με πλημμελληματικού χαρακτήρα κατηγορίες (Τριανταφύλλου, 2026 σελ.87-88). Αργότερα, ο Εισαγγελέας του Αρείου Πάγου έκρινε ότι τα νέα στοιχεία που προέκυψαν μετά την καταδίκη δεν δικαιολογούν επανεξέταση της υπόθεσης, ενώ κρίσιμο είναι επίσης οτι ο Εισαγγελέας είναι ο ίδιος που είχε εγκρίνει με την υπογραφή του την παρακολούθηση του δημοσιογράφου Κουκάκη (predatorgate.gr, 2026). Αυτή η σύμπτωση δεν είναι απλώς διαδικαστικό πρόβλημα. Αποτελεί εμπειρική επιβεβαίωση της κεντρικής θέσης των Green και Ward ότι τα κράτη που διαπράττουν παραβιάσεις ανθρωπίνων δικαιωμάτων σπάνια λογοδοτούν διότι ελέγχουν τους ίδιους τους μηχανισμούς λογοδοσίας (Green, & Ward, 2004, pp 2-3). Το ερώτημα ποιος έδωσε την εντολή παρακολούθησης παραμένει αναπάντητο όχι επειδή τα στοιχεία απουσιάζουν, αλλά επειδή η θεσμική αρχιτεκτονική είναι σχεδιασμένη ώστε να μην μπορεί να απαντηθεί.

Η ΕΥΠ παρακολουθούσε στόχους με εισαγγελικές εντολές, παρακολούθηση που νομικοί εμπειρογνώμονες χαρακτήρισαν παράνομη ως προς τον σκοπό της (Mildebrath, 2022, p. 2).

[13] Η ΑΔΑΕ μπορεί να εντοπίσει παρακολουθήσεις ερευνώντας τηλεπικοινωνιακούς παρόχους

Παράλληλα, το Citizen Lab τεκμηρίωσε τη χρήση του εμπορικού Predator κατά των ίδιων στόχων, χρήση που, ανεξαρτήτως του χειριστή της, δεν υπόκειτο σε οποιαδήποτε εποπτεία από την ΑΔΑΕ, καθώς η αρμοδιότητά της περιορίζεται στις νόμιμες παρακολουθήσεις και όχι στη χρήση εμπορικών spyware. (Citizen Lab, 2021)

Πιο συγκεκριμένα η ελληνική υπόθεση αποτελεί ιδανική μελέτη περίπτωσης καθώς αφενός αποκαλύπτει τη συσχέτιση ιδιωτικού τομέα με θεσμικούς φορείς μέσω της παράλληλης χρήσης νόμιμης παρακολούθησης από την ΕΥΠ και παράνομης από το predator, κατά των ίδιων στόχων και αφετέρου εξαιτίας της συστηματικής θεσμικής απόκρυψης που ακολούθησε. Ο νόμος 4790/2021 τροποποίησε το αρθρ 5 του Ν 2225/1994 απαγορεύοντας στην ΑΔΑΕ να ενημερώνει εκ των υστέρων τα υποκείμενα παρακολούθησης για λόγους εθνικής ασφάλειας στερώντας τους έτσι κάθε δυνατότητα έννομης προστασίας. Η θεσμική αυτή απόκρυψη συνδυαστικά με την άρνηση της κυβέρνησης να αποκαλύψει τον αγοραστή του predator, συνιστά το στάδιο layering του data laundering. Ουσιαστικά τα παράνομα δεδομένα προστατεύονται από κάθε έλεγχο μέσω της επίκλησης εθνικής ασφάλειας ως νομικής ασπίδας.

Ο Ν4790/2021 που απαγόρευσε στην ΑΔΑΕ να ενημερώνει εκ των υστέρων τα θύματα παρακολούθησης για λόγους εθνικής ασφάλειας (ΦΕΚ Α' 145/2021) αλλά και το οτι οι εκπρόσωποι των εμπλεκόμενων θεσμών στις κοινοβουλευτικές επιτροπές αποκάλυψαν ελάχιστες πληροφορίες (Mildebrath, H., 2022, p. 2) δηλώνει την προσπάθεια θεσμικής απόκρυψης που αποτέλεσε αναπόσπαστο μέρος του σκανδάλου. Η κυβέρνηση αρνήθηκε αρχικά κάθε γνώση για την ύπαρξη του Predator στην Ελλάδα και ο διοικητής της ΕΥΠ αντικαταστάθηκε (European Parliament PEGA Committee, 2023)

6.2 Θύματα και επιπτώσεις στα δικαιώματα

Τα τεκμηριωμένα θύματα περιλαμβάνουν τρεις κατηγορίες: δημοσιογράφους (Κουκάκης), πολιτικά πρόσωπα (Ανδρουλάκης και άλλα μέλη αντιπολίτευσης) και κρατικά στελέχη και επιχειρηματίες, γεγονός που αναδεικνύει τη διάχυτη φύση της παρακολούθησης.

Πέραν των άμεσων θυμάτων, η υπόθεση παρήγαγε ευρύτερο chilling effect, όπως τεκμηριώνεται από τις μελέτες Penney (2016) και Stoycheff (2016) που αναλύθηκαν στο Κεφάλαιο 2 (Penney, 2016 ; Stoycheff, 2016). Η πτώση της Ελλάδας στον δείκτη RSF[14] από την 70η στην 107η θέση αποτελεί μετρήσιμη ένδειξη αυτής της βλάβης. Οι συνέπειες για την ελευθερία του Τύπου ήταν άμεσες και μετρήσιμες. Συγκεκριμένα, η Ελλάδα κατρακύλησε από τη 70η στη 107η–108η θέση του δείκτη ελευθερίας Τύπου της RSF, καταλαμβάνοντας την τελευταία θέση μεταξύ χωρών-μελών της ΕΕ. Η κατακόρυφη πτώση της Ελλάδας στον δείκτη της RSF συνέπεσε χρονικά με τις αποκαλύψεις του Predatorgate και αποδίδεται από την ίδια την

[14] Διεθνής μη κυβερνητική οργάνωση με έδρα το Παρίσι που υπερασπίζεται την ελευθερία του Τύπου και εκδίδει ετησίως τον Παγκόσμιο Δείκτη Ελευθερίας Τύπου για 180 χώρες.

οργάνωση εν μέρει στο κλίμα φόβου που δημιούργησαν οι αποκαλύψεις παρακολούθησης (Reporters Without Borders, 2023). Αν και δεν υπάρχει στην Ελλάδα συστηματική εμπειρική έρευνα αντίστοιχη εκείνης των Penney (2016) και Stoycheff (2016) που θα τεκμηρίωνε ποσοτικά το chilling effect του Predatorgate, τα παραπάνω στοιχεία συνάδουν με τη θεωρητική πρόβλεψη του πανοπτικισμού, ότι η αποκάλυψη της παρακολούθησης παράγει αυτοπειθαρχία ακόμα και χωρίς συνεχιζόμενη ενεργή επιτήρηση.

Η χρήση του Predator στο πλαίσιο του Predatorgate συνιστά παραβίαση του δικαιώματος στην ιδιωτικότητα σε τρία διακριτά επίπεδα, καθένα από τα οποία αντιστοιχεί σε διαφορετική διάσταση της προσβολής του δικαιώματος.

Το πρώτο επίπεδο αφορά την έκταση της παραβίασης. Το spyware δεν περιορίζεται στα δεδομένα του στόχου αλλά αποκτά πρόσβαση και στα δεδομένα τρίτων προσώπων που επικοινωνούν μαζί του, οικογένειας, συναδέλφων, δημοσιογραφικών πηγών, χωρίς αυτοί να έχουν υπάρξει ποτέ στόχοι παρακολούθησης (Kaldani & Prokopets, 2022). Αυτό σημαίνει ότι η παραβίαση διαχέεται αόρατα στο ευρύτερο κοινωνικό περιβάλλον του θύματος. Οι αποκαλύψεις του Edward Snowden (συνεργάτης της NSA) αποκάλυψαν και επιβεβαίωσαν ότι οι επιχειρήσεις των μυστικών υπηρεσιών του 21^{ου} αιώνα για την προστασία της «εθνικής ασφάλειας» περιλαμβάνουν παρακολουθήσεις μεγάλης κλίμακας με ζητούμενο τη συλλογή μεγάλου όγκου δεομένων. Οι εξατομικευμένες παρακολουθήσεις συνιστούν μέρος των δράσεων όμως, η αδυναμία των υπηρεσιών για σαφή προσδιορισμό των γεγονότων που συνιστούν απειλή για την εθνική ασφάλεια, ενεργοποιεί μηχανισμούς πολλαπλασιαστικής προβλεπτικής δυνατότητας (Παπανικολάου, 2025, σσ. 241-243) Συνεπώς, παρατηρείται πλέον μια μετάβαση από την ανθρωποκεντρική επιτήρηση στην τεχνοκατευθυνόμενη σάρωση και την καθολική αποθησαύριση συνομιλιών και δεδομένων για την συγκέντρωση big data, χρήσιμων ή μη, για τρέχουσα ή μελλοντική χρήση (Παπανικολάου, 2025, σ. 243)

Το δεύτερο επίπεδο αφορά την αορατότητα. Η μόλυνση γίνεται χωρίς γνώση του θύματος, χωρίς δυνατότητα ανίχνευσης και χωρίς κανένα προηγούμενο σημάδι παραβίασης, αφαιρώντας κάθε δυνατότητα άμυνας ή έννομης προστασίας εκ των προτέρων (Cisco Talos, 2023). Η τεχνολογία zero-click, που δεν απαιτεί καμία ενέργεια από τον χρήστη για την εγκατάστασή της, καθιστά τον στόχο ανυπεράσπιστο.

Το τρίτο επίπεδο αφορά το βάθος της εισβολής. Το Predator αποκτά πρόσβαση σε κατηγορίες δεδομένων που απολαμβάνουν αυξημένη νομική προστασία όπως είναι τα δεδομένα υγείας, σεξουαλικής ζωής, πολιτικών πεποιθήσεων και θρησκευτικών απόψεων, σύμφωνα με το άρθρο 9 του GDPR και το άρθρο 8 της ΕΣΔΑ. Επιπλέον, παρέχει απομακρυσμένη και απεριόριστη πρόσβαση στις κινητές συσκευές κλήσεις, μηνύματα, φωτογραφίες, κωδικούς, τοποθεσία, παρακάμπτοντας κάθε κρυπτογράφηση (Kaldani & Prokopets, 2022; Amnesty International Security Lab, 2023)

Συνολικά, η χρήση κατασκοπευτικών λογισμικών όπως το Predator δεν αφορά παραβίαση διαδικαστικών κανόνων αλλά την πλήρη κατάλυση της ιδιωτικής σφαίρας του στόχου, αυτό που ο Solove (2008) αποκαλεί «πρόβλημα συσσώρευσης δεδομένων» (aggregation problem). Ο Solove (2008) ανέπτυξε την έννοια του «πρόβλημα συσσώρευσης δεδομένων» για να περιγράψει ένα φαινόμενο που η παραδοσιακή θεωρία ιδιωτικότητας αδυνατούσε να συλλάβει, ότι η συνδυαστική συλλογή δεδομένων που φαίνονται αθώα μεμονωμένα παράγει μια γνώση για το άτομο που υπερβαίνει κατά πολύ το άθροισμα των μερών της. Η συνδυαστική επεξεργασία δεδομένων όπως το ονομα, η διεύθυνση, η εργασία δημιουργεί ένα «ψηφιακό προφίλ» που αποκαλύπτει διαστάσεις της ζωής του ατόμου που το ίδιο δεν έχει επιλέξει να αποκαλύψει σε κανέναν (Solove, D.J. , 2008, pp. 101-114).

Στην περίπτωση του Predator, το πρόβλημα συσσώρευσης δεδομένων εκδηλώνεται με ιδιαίτερη ένταση. Το spyware δεν συλλέγει απλώς μια κατηγορία δεδομένων αλλά αποκτά ταυτόχρονη πρόσβαση σε επικοινωνίες, τοποθεσία, φωτογραφίες, κωδικούς, επαφές και ημερολόγια, δηλαδή στο σύνολο της ψηφιακής ύπαρξης του στόχου. Το αποτέλεσμα δεν είναι απλώς παραβίαση δεδομένων αλλά πλήρης χαρτογράφηση της ιδιωτικής ζωής, των σχέσεων και των προθέσεων του θύματος (Cisco Talos, 2023; Amnesty International Security Lab, 2023).

Οι Kaldani και Prokopets (2022) τεκμηριώνουν ότι η χρήση του Pegasus δεν απαιτεί συνεργασία με τις εταιρείες τηλεπικοινωνιών, και μπορεί εύκολα να παρακάμψει την κρυπτογράφηση και οποιοδήποτε εμπόδιο εισάγεται από τις πολύπλοκες επικοινωνίες παγκοσμίως. Επιτρέπει την παρακολούθηση των κλήσεων σε πραγματικό χρόνο. Παρέχει απομακρυσμένη, μυστική και απεριόριστη πρόσβαση στις κινητές συσκευές του στόχου και, συνεπώς, στις σχέσεις τους, στις εικονικές ταυτότητες, στην τοποθεσία, στις τηλεφωνικές κλήσεις, στα γραπτά και φωνητικά μηνύματα, στα emails, στις φωτογραφίες, στα βίντεο και σε άλλα αρχεία, στις επαφές, στους κωδικούς πρόσβασης, στις περιβαλλοντικές παρακολουθήσεις, στα σχέδια και στις δραστηριότητες που αποκαλύπτουν τις πιο ευαίσθητες πληροφορίες και υπονομεύει τα πρότυπα και τις προσεγγίσεις που έχουν θεσπιστεί από το Ευρωπαϊκό Δικαστήριο στη εκτεταμένη νομολογία του σχετικά με τη στοχευμένη παρακολούθηση επικοινωνιών και την αδιάκριτη/μαζική παρακολούθηση δεδομένων επικοινωνία (Kaldani & Prokopets, 2022). Η συνολική αυτή εικόνα αναδεικνύει ότι η χρήση κατασκοπευτικών λογισμικών όπως το Predator δεν αφορά απλώς παραβίαση διαδικαστικών κανόνων αλλά αφορά την ολοκληρωτική κατάρρευση της ιδιωτικής σφαίρας του στόχου.

6.3 Θεσμικές Αντιδράσεις

Η θεσμική αντίδραση στο Predatorgate αποκάλυψε με ιδιαίτερη σαφήνεια τους μηχανισμούς της δομικής ατιμωρησίας που αναλύθηκαν στο προηγούμενο κεφάλαιο. Σε κάθε

επίπεδο ελέγχου, διοικητικό, κοινοβουλευτικό και ευρωπαϊκό, η αντίδραση των θεσμών ήταν είτε ανεπαρκής είτε δομικά αδύνατη.

Η ΑΔΑΕ, ως ο κατ' αρχήν αρμόδιος φορέας, εξέδωσε αποφάσεις που διαπίστωναν παραβιάσεις, αλλά αντιμετώπισε τρία δομικά εμπόδια που καθιστούσαν την παρέμβασή της ουσιαστικά άνευ αποτελέσματος. Πρώτον, δεν είχε πρόσβαση στα δεδομένα της ΕΥΠ, η οποία υπαγόταν απευθείας στην εκτελεστική εξουσία. Δεύτερον, η αρμοδιότητά της δεν εκτεινόταν στα εμπορικά spyware, δημιουργώντας ένα κανονιστικό κενό που η Intellexa εκμεταλλεύτηκε συστηματικά. Τρίτον, ο πρόεδρός της αντικαταστάθηκε κατά τη διάρκεια της κρίσης, γεγονός που έθεσε υπό αμφισβήτηση την ανεξαρτησία της αρχής (European Parliament PEGA Committee, 2023).

Η κοινοβουλευτική διερεύνηση απέδωσε εξίσου περιορισμένα αποτελέσματα. Η κυβερνητική πλειοψηφία απέτρεψε τη σύσταση εξεταστικής επιτροπής, ενώ η επίκληση της «εθνικής ασφάλειας» λειτούργησε ως νομικό εμπόδιο στην πρόσβαση κρίσιμων εγγράφων. Η ψηφοφορία δυσπιστίας της 27ης Ιανουαρίου 2023 απορρίφθηκε με 156 έναντι 143 ψήφων, με τη ΝΔ να διατηρεί την κοινοβουλευτική της πλειοψηφία (Reuters , 2023)

Η πιο ουσιαστική θεσμική αντίδραση ήρθε από το Ευρωπαϊκό Κοινοβούλιο. Η Επιτροπή PEGA εξέδωσε τον Μάιο του 2023 την τελική της έκθεση, διαπιστώνοντας για την ελληνική περίπτωση σοβαρή παραβίαση δημοκρατικών αξιών, ανεπαρκή θεσμική αντίδραση και ανάγκη ενίσχυσης της ΑΔΑΕ και νομικής ρύθμισης της αγοράς spyware. Η έκθεση υπογράμμισε ότι το παράνομο κατασκοπευτικό λογισμικό χρησιμοποιήθηκε σε περιβάλλον όπου νομοθετικές τροποποιήσεις, και ιδίως ο Ν. 4790/2021, είχαν αποδυναμώσει τα θεμέλια της προστασίας του απορρήτου, αυξάνοντας τον κίνδυνο παράνομης παρακολούθησης χωρίς επαρκή δικαστική εποπτεία. Επιπλέον, η PEGA διαπίστωσε ότι η Ελλάδα επέτρεψε την εξαγωγή του λογισμικού σε χώρες με αμφιλεγόμενο ιστορικό σεβασμού των ανθρωπίνων δικαιωμάτων, αναδεικνύοντας τη διάσταση του εξαγωγικού arbitrage (European Parliament PEGA Committee, 2023).

Συνολικά, η PEGA κατέληξε ότι η κατάσταση στην Ελλάδα δεν αποτελεί απλώς παράβαση ανθρωπίνων δικαιωμάτων αλλά συστηματικό ζήτημα δημοκρατικών εγγυήσεων, με σοβαρές επιπτώσεις στην ιδιωτικότητα, τη δημοσιογραφική ελευθερία και την ελευθερία της έκφρασης (Chondrogiannos, 2023) Το εύρημα αυτό επιβεβαιώνει τη θεωρητική πρόβλεψη των Green και Ward (2004) ότι η ατιμωρησία δεν είναι τυχαία αλλά δομικά παραγόμενη από τα ίδια τα συστήματα εξουσίας που τελούν το έγκλημα (Green, & Ward, 2004).

6.4 Δικαστικές εξελίξεις και ζητήματα λογοδοσίας

Στις 26 Φεβρουαρίου 2026, το Μονομελές Πλημμελειοδικείο Αθηνών εξέδωσε απόφαση ιστορικής σημασίας καθώς, για πρώτη φορά παγκοσμίως, στελέχη εμπορικής εταιρείας spyware καταδικάστηκαν ποινικά για παραβίαση του απορρήτου των επικοινωνιών, παραβίαση της

προστασίας δεδομένων προσωπικού χαρακτήρα και παράνομη πρόσβαση σε πληροφοριακά συστήματα (ICIJ , 2026). Καταδικάστηκαν ο Tal Dilian, ιδρυτής της Intellexa και πρώην αξιωματικός ισραηλινών μυστικών υπηρεσιών, η Sara Hamou, επιχειρηματική εταίρος του, ο Felix Bitzios, μέτοχος της Intellexa, και ο Γιάννης Λαβράνος, ιδιοκτήτης της Kriel, της εταιρείας μέσω της οποίας φέρεται να αποκτήθηκε το Predator. Η ποινή ανήλθε σε 126 χρόνια και 8 μήνες για τον καθένα, αναστέλλεται όμως μέχρι την εκδίκαση της έφεσης που ήδη ασκήθηκε.

Από εγκληματολογική σκοπιά, η απόφαση είναι ταυτόχρονα σημαντική και αποκαλυπτικά ελλιπής. Σημαντική, διότι αποτελεί το πρώτο διεθνές προηγούμενο ποινικής ευθύνης για στελέχη βιομηχανίας spyware, επιβεβαιώνοντας ότι η επίκληση «νόμιμης εμπορικής δραστηριότητας» δεν αποτελεί ανυπέρβλητο ασπίδα ατιμωρησίας. Όπως χαρακτηριστικά σχολίασε ο Scott-Railton του Citizen Lab, «αυτό δείχνει ότι όταν τα πραγματικά στοιχεία των επιχειρηματικών μοντέλων εταιρειών spyware παρουσιαστούν ενώπιον δίκαιου δικαστή, οι συνέπειες θα ακολουθήσουν» (ICIJ, 2026).

Ωστόσο, η καταδίκη παραμένει δομικά ελλιπής για τρεις λόγους που αναδεικνύουν με σαφήνεια τους μηχανισμούς της δομικής ατιμωρησίας. Η δίκη περιορίστηκε σε πλημμελήματα, αποκλείοντας τα βαρύτερα αδικήματα κατασκοπείας. Επιπλέον, ο εισαγγελέας ζήτησε μεν τη διερεύνηση της εμπλοκής κρατικών φορέων, η ΕΥΠ όμως είχε ήδη απαλλαγεί από τον Άρειο Πάγο το 2024. Τέλος και πιο κρίσιμο εγκληματολογικά, τιμωρήθηκε ο εταιρικός βραχίονας ενώ ο κρατικός βραχίονας, δηλαδή εκείνος που φαίνεται ότι παρήγγειλε, χρηματοδότησε και χρησιμοποίησε το spyware, παραμένει νομικά άθικτος.

Η καταδίκη αποκαλύπτει επίσης την κεντρική λειτουργία του data laundering. Εφόσον η αλυσίδα μεσαζόντων (intermediaries) έχει επιτυχώς αποσυνδέσει την ευθύνη, το σύστημα δικαιοσύνης δυσκολεύεται να ανιχνεύσει τον εντολέα ακόμα και όταν θέλει να το κάνει. Η μερική λογοδοσία δεν αναιρεί τη δομική ατιμωρησία αλλά την επιβεβαιώνει. Αυτό αποκαλύπτει την κεντρική αδυναμία και τη πραγματική χρησιμότητα του μηχανισμού data laundering καθώς όπως περιγράφει η θεωρία των Kramer-Michalowski, το σύστημα τιμώρησε τον εκτελεστή προστατεύοντας τον εντολέα (Kramer, Michalowski, & Kauzlarich, 2002, pp. 263-282)

6.5 Άλλα Ευρωπαικά Παραδείγματα: Ισπανία (Catalangate) και Ουγγαρία

Οι αντίστοιχες ευρωπαϊκές περιπτώσεις επιβεβαιώνουν ότι το ψηφιακό κρατικο-εταιρικό έγκλημα αποτελεί δομικό και όχι εξαιρετικό φαινόμενο εντός της ΕΕ. Στην Ισπανία, τον Απρίλιο του 2022, το Citizen Lab αποκάλυψε παρακολούθηση τουλάχιστον 65 προσώπων από την Καταλανική πολιτική και κοινωνία με τεχνολογία Pegasus και Candiru. Μεταξύ τους ο Carles Puigdemont, τέσσερις διαδοχικοί πρόεδροι της Καταλονίας, ευρωβουλευτές, νομικοί σύμβουλοι του ανεξαρτησιακού κινήματος και μέλη οργανώσεων της κοινωνίας των πολιτών (Citizen Lab , 2022)

Η ισπανική κυβέρνηση αναγνώρισε εν μέρει τις παρακολουθήσεις επικαλούμενη «νόμιμη κρατική ασφάλεια», χωρίς ωστόσο να παράσχει καμία ανεξάρτητη δικαστική εποπτεία ή λογοδοσία (PEGA Committee, 2023). Η δομή είναι πανομοιότυπη με την ελληνική: κράτος-πελάτης, εμπορικό spyware και επίκληση εθνικής ασφάλειας λειτουργούν ως ασπίδα ατιμωρησίας. Η ουσιαστική διαφορά έγκειται στη στόχευσης καθώς στην Ισπανία η παρακολούθηση ήταν συγκεντρωμένη σε ένα συγκεκριμένο πολιτικό κίνημα, ενώ στην Ελλάδα ήταν διάχυτη, καλύπτοντας δημοσιογράφους, πολιτικούς αντιπάλους, στρατιωτικούς αξιωματούχους και επιχειρηματίες

Η ουγγρική περίπτωση αποτελεί την πιο ακραία εκδοχή κατάχρησης spyware εντός της ΕΕ, καθώς η χρήση του Pegasus δεν φαίνεται να αποτέλεσε εξαίρεση αλλά συστηματική κυβερνητική πρακτική. Σύμφωνα με τα ευρήματα του Pegasus Project και την έκθεση PEGA (2023), μεταξύ των στόχων συγκαταλέγονταν δημοσιογράφοι ανεξάρτητων μέσων ενημέρωσης, ακτιβιστές και πολιτικοί της αντιπολίτευσης (Amnesty International & Forbidden Stories , 2021). Χαρακτηριστικό της ουγγρικής περίπτωσης είναι η στάση της κυβέρνησης Orbán. Σε αντίθεση με άλλες κυβερνήσεις που αρνήθηκαν ή υποβάθμισαν τις κατηγορίες, η Ουγγαρία επέλεξε την ουσιαστική αδιαφορία, επικαλούμενη κυριαρχικό δικαίωμα για εθνική ασφάλεια χωρίς να παράσχει καμία εξήγηση ή να επιτρέψει ανεξάρτητη διερεύνηση (PEGA, 2023). Η στάση αυτή αποτελεί εμπειρική επιβεβαίωση της θέσης των Green και Ward (2004) ότι τα κράτη που διαπράττουν παραβιάσεις ανθρωπίνων δικαιωμάτων σπάνια λογοδοτούν, διότι ελέγχουν τους ίδιους τους μηχανισμούς λογοδοσίας (Green, & Ward, 2004)

Η συγκριτική ανάλυση των περιπτώσεων Ελλάδας, Ισπανίας και Ουγγαρίας αναδεικνύει ένα σύνολο κοινών δομικών χαρακτηριστικών που επιβεβαιώνουν ότι το ψηφιακό κρατικο-εταιρικό έγκλημα δεν αποτελεί εθνικό φαινόμενο αλλά συστημικό πρόβλημα της ΕΕ (PEGA, 2023). Σε όλες τις περιπτώσεις οι στόχοι ανήκουν στις ίδιες κατηγορίες(δημοσιογράφοι ανεξάρτητων μέσων, πολιτικοί της αντιπολίτευσης και ακτιβιστές) δηλαδή ακριβώς εκείνοι που ασκούν κοινωνικό έλεγχο στην εξουσία. Η επίκληση εθνικής ασφάλειας λειτούργησε παντού ως νομικά κωδικοποιημένη ασπίδα αδιαφάνειας, αποτρέποντας κάθε ανεξάρτητη διερεύνηση, ενώ η χρήση εμπορικών εταιρειών επέτρεψε στα κράτη να εξωτερικεύουν την ευθύνη επικαλούμενα ότι απλώς απέκτησαν ένα νόμιμο εμπορικό προϊόν. Η θεσμική αντίδραση σε εθνικό επίπεδο υπήρξε σε όλες τις περιπτώσεις ανεπαρκής, είτε λόγω πολιτικής εξάρτησης των εποπτικών αρχών είτε λόγω νομικών κενών που απέτρεπαν τη διερεύνηση.

Το πιο κρίσιμο εγκληματολογικά εύρημα είναι ότι ακόμα και στην ελληνική περίπτωση, που αποτελεί το μοναδικό παράδειγμα ποινικής καταδίκης παγκοσμίως, ο κρατικός βραχίονας παρέμεινε νομικά άθικτος. Αυτό επιβεβαιώνει ότι η μερική λογοδοσία δεν αναιρεί τη δομική ατιμωρησία αλλά αποτελεί την πιο χαρακτηριστική έκφρασή της. Το σύστημα μπορεί να τιμωρήσει τον εκτελεστή ακριβώς επειδή έτσι προστατεύει τον εντολέα (Green, & Ward, 2004).

Συμπεράσματα

Η παρούσα εργασία ανέλαβε να διερευνήσει πώς το data laundering εντάσσεται στο κρατικο-εταιρικό έγκλημα, ένα ερώτημα που όμως η εγκληματολογία δεν είχε ακόμα διατυπώσει με συστηματικό τρόπο, και πώς αυτή η σχέση εκδηλώνεται εμπειρικά στην ελληνική περίπτωση Predatorgate. Τα ευρήματα της ανάλυσης επιτρέπουν πλέον να δοθεί συστηματική απάντηση και στα τρία ερευνητικά ερωτήματα που τέθηκαν στην Εισαγωγή.

Ως προς το πρώτο ερευνητικό ερώτημα, η εργασία κατέδειξε ότι η σχέση data laundering και κρατικο-εταιρικού εγκλήματος δεν είναι τυχαία αλλά δομικά αναγκαία. Το data laundering δεν είναι απλώς ένα εργαλείο που οι κρατικοί και εταιρικοί δρώντες χρησιμοποιούν ευκαιριακά. Είναι ο μηχανισμός που καθιστά δυνατή την ύπαρξη του κρατικο-εταιρικού εγκλήματος στη ψηφιακή εποχή, αποκρύπτοντας την παράνομη καταγωγή των δεδομένων και νομιμοποιώντας τη χρήση τους. Χωρίς τον μηχανισμό data laundering, η αλυσίδα κράτος-εταιρεία-στόχος που ανέλυσε η εργασία δεν θα μπορούσε να λειτουργήσει καθώς η παράνομη παρακολούθηση θα παρέμενε ορατή, η ευθύνη θα ήταν αποδοτέα και η ατιμωρησία δεν θα μπορούσε να παραχθεί δομικά. Το τρίπτυχο placement-layering-integration που δανείστηκε η εργασία από τη θεωρία του money laundering αποδείχθηκε αναλυτικά παραγωγικό εφόσον κάθε στάδιο αντιστοιχεί σε συγκεκριμένους μηχανισμούς που η βιομηχανία spyware έχει αναπτύξει με αξιοσημείωτη επιδεξιότητα. Το placement πραγματοποιείται μέσω της νόμιμης αγοράς του spyware και των εξαγωγικών αδειών που του προσδίδουν επίσημη κρατική υπόσταση. Το layering επιτυγχάνεται μέσω της επίκλησης εθνικής ασφάλειας, των offshore εταιρικών δομών και των μεαζόντων (intermediaries) που αποκόπτουν την αλυσίδα ευθύνης. Το integration συντελείται μέσω της ενσωμάτωσης των παράνομα αποκτηθέντων δεδομένων σε επίσημες διαδικασίες, νομικές, διοικητικές και πολιτικές, χωρίς ποτέ να αμφισβητηθεί η προέλευσή τους. Η ελληνική περίπτωση Predatorgate επιβεβαίωσε εμπειρικά αυτή τη δομή. Και τα τρία στάδια εκδηλώθηκαν με αξιοσημείωτη σαφήνεια, από τις εξαγωγικές άδειες του Predator έως τον Ν. 4790/2021 που νομοθετικά κατοχύρωσε το layering, και από τη χρήση δεδομένων σε παράλληλες παρακολουθήσεις ΕΥΠ-Predator έως την αδυναμία απόδοσης ευθύνης μετά την αποκάλυψη.

Ως προς το δεύτερο ερευνητικό ερώτημα, η εργασία ανέδειξε τρεις κατηγορίες μηχανισμών που επιτρέπουν τη νομιμοποίηση παράνομα αποκτηθέντων δεδομένων. Η πρώτη κατηγορία είναι οι θεσμικές ανεπάρκειες, δηλαδή τα νομικά κενά που δεν είναι τυχαία αλλά δομικά παραγόμενα. Η εξαίρεση εθνικής ασφάλειας του άρθρου 23 GDPR, η απουσία ευρωπαϊκής εναρμόνισης των εξαγωγικών αδειών, η ανεπάρκεια του ελληνικού άρθρου 19 Συντάγματος και η πλήρης απουσία ειδικής νομοθεσίας για εμπορικά spyware δεν αποτελούν αποτυχίες του συστήματος. Αποτελούν τις δομικές προϋποθέσεις που επιτρέπουν στο σύστημα να λειτουργεί όπως λειτουργεί. Η δεύτερη κατηγορία είναι οι μηχανισμοί συγκάλυψης, δηλαδή η αρχιτεκτονική αδιαφάνειας που η βιομηχανία spyware έχει αναπτύξει: οι εξωχώριες δομές της

Intellexa, η αλυσίδα μεσαζόντων, η τεχνολογία zero-click που δεν αφήνει ίχνη, και η σκόπιμη αποσύνδεση γνώσης μεταξύ εταιρείας και κράτους-πελάτη όπως ο ίδιος ο Dilian αποκάλυψε. Η τρίτη κατηγορία είναι οι δυναμικές εξουσίας, δηλαδή η ικανότητα των ισχυρών να ορίζουν τι είναι νόμιμο και τι όχι. Τα κράτη που χρησιμοποιούν spyware είναι τα ίδια που χορηγούν εξαγωγικές άδειες, ορίζουν τις εξαιρέσεις εθνικής ασφάλειας, ελέγχουν τις εισαγγελικές αρχές και αποφασίζουν αν θα επανεξεταστεί μια υπόθεση. Αυτή η εξουσία αυτο-ορισμού που η εγκληματολογία των ισχυρών έχει αναγνωρίσει ως τον πιο επικίνδυνο μηχανισμό ατιμωρησίας εκδηλώθηκε στο Predatorgate με εξαιρετική σαφήνεια. Ο ίδιος Εισαγγελέας που είχε εγκρίνει την παρακολούθηση του Κουκάκη ήταν αυτός που αποφάσισε να μην επανεξεταστεί η υπόθεση μετά την καταδίκη.

Ως προς το τρίτο ερευνητικό ερώτημα, η εργασία κατέδειξε ότι οι αναγκαίες ρυθμιστικές αλλαγές πρέπει να λειτουργήσουν σε τρία επίπεδα ταυτόχρονα, διαφορετικά η μεταρρύθμιση σε ένα επίπεδο παρακάμπτεται από τα κενά στα άλλα. Σε ευρωπαϊκό επίπεδο, η αναθεώρηση του άρθρου 23 GDPR ώστε να απαιτεί ανεξάρτητη εποπτεία για κάθε επίκληση εθνικής ασφάλειας αποτελεί την πιο επείγουσα μεταρρύθμιση, καθώς αυτή η εξαίρεση λειτουργεί ως ο κεντρικός νομικός μηχανισμός του layering σε ολόκληρη την ΕΕ. Εξίσου αναγκαία είναι η δημιουργία κεντρικού ευρωπαϊκού μηχανισμού αδειοδότησης εξαγωγών κυβερνο-επιτήρησης με κριτήρια ανθρωπίνων δικαιωμάτων και η σύσταση ανεξάρτητης ευρωπαϊκής τεχνικής αρχής ανίχνευσης spyware, ανάλογης με την OLAF. Σε εθνικό επίπεδο, η συνταγματική αναθεώρηση του άρθρου 19 ώστε να απαιτεί δικαστική έγκριση για κάθε παρακολούθηση ανεξαρτήτως επίκλησης εθνικής ασφάλειας, η πλήρης πρόσβαση της ΑΔΑΕ σε όλες τις υποθέσεις και η θέσπιση ειδικής νομοθεσίας για εμπορικά spyware αποτελούν αναγκαίες αλλά όχι επαρκείς προϋποθέσεις. Σε εγκληματολογικό επίπεδο, η πιο πρωτότυπη πρόταση που η εργασία αναδεικνύει είναι η ρητή ποινικοποίηση του data laundering ως αυτόνομου αδικήματος σε αντιστοιχία με το money laundering, που θα καλύπτει και τα τρία στάδια της διαδικασίας, τη συλλογή, την απόκρυψη και τη νομιμοποίηση.

Πέραν των τριών ερευνητικών ερωτημάτων, η εργασία ανέδειξε δύο ευρύτερα εγκληματολογικά ευρήματα που έχουν σημασία πέραν της συγκεκριμένης υπόθεσης. Το πρώτο αφορά τη φύση της δομικής ατιμωρησίας στη ψηφιακή εποχή. Η καταδίκη του Φεβρουαρίου 2026 αποτελεί ιστορικό ορόσημο, αλλά ταυτόχρονα αποκαλυπτικά ελλιπής επιβεβαίωση της θεωρητικής πρόβλεψης των Green και Ward καθώς το σύστημα τιμώρησε τον εκτελεστή ακριβώς επειδή έτσι προστατεύει τον εντολέα. Η μερική λογοδοσία δεν αναιρεί τη δομική ατιμωρησία αλλά αποτελεί την πιο χαρακτηριστική έκφρασή της. Ο κρατικός βραχίονας παρέμεινε νομικά άθικτος όχι επειδή τα στοιχεία απουσιάζουν αλλά επειδή η θεσμική αρχιτεκτονική είναι σχεδιασμένη ώστε να μην μπορεί να αποδειχθεί. Το δεύτερο εύρημα αφορά τη διεύρυνση της κοινωνικής βλάβης πέραν των άμεσων θυμάτων. Μέσα από τη φουκωική ανάλυση του chilling

effect αποδείχθηκε ότι η βλάβη του spyware δεν περιορίζεται σε εκείνους που παρακολουθήθηκαν. Εκτείνεται σε κάθε δημοσιογράφο που αυτολογοκρίνεται, σε κάθε ακτιβιστή που αποφεύγει ευαίσθητες επικοινωνίες, σε κάθε πολίτη που γνωρίζει ότι η παρακολούθηση είναι τεχνικά δυνατή και πολιτικά εφικτή. Η πτώση της Ελλάδας από την 70η στην 107η θέση του δείκτη ελευθερίας Τύπου RSF αποτελεί μετρήσιμη ένδειξη αυτής της διάχυτης βλάβης που κανένα ποινικό δίκαιο δεν μπορεί ακόμα να συλλάβει.

Η εργασία αναγνωρίζει τους περιορισμούς της. Η έννοια του data laundering παραμένει εννοιολογικά υπό ανάπτυξη και η χρήση της κατ' αναλογία με το money laundering, αν και αναλυτικά παραγωγική, χρειάζεται περαιτέρω εμπειρική τεκμηρίωση σε διαφορετικές εθνικές περιπτώσεις. Επιπλέον, η αδυναμία δικαστικής απόδειξης της κρατικής εμπλοκής στο Predatorgate σημαίνει ότι ο χαρακτηρισμός της υπόθεσης ως state-initiated παραμένει, από αυστηρά νομική σκοπιά, υπό αίρεση, αν και εγκληματολογικά οι ενδείξεις είναι ισχυρές. Τέλος, η συγκριτική ανάλυση των περιπτώσεων Ισπανίας και Ουγγαρίας παρέμεινε σχετικά συνοπτική λόγω των ορίων της έκτασης της εργασίας.

Κατευθύνσεις για μελλοντική έρευνα προκύπτουν από τα ίδια τα ευρήματα. Η συστηματική εμπειρική τεκμηρίωση του chilling effect στην ελληνική περίπτωση μέσω ποσοτικής έρευνας, ανάλογης με τις μελέτες Penney και Stoycheff, θα ενίσχυε σημαντικά το επιχείρημα για τη διάχυτη κοινωνική βλάβη του spyware. Η συγκριτική μελέτη των μηχανισμών data laundering σε πολλαπλές ευρωπαϊκές χώρες θα επέτρεπε τη διαμόρφωση ενός πιο γενικεύσιμου αναλυτικού πλαισίου. Τέλος, η παρακολούθηση των εξελίξεων στην ελληνική υπόθεση, καθώς η διαδικασία της έφεσης βρίσκεται σε εξέλιξη και τα νέα στοιχεία που ανακοίνωσε ο Dilian τον Ιούνιο του 2026 δεν έχουν ακόμα αξιολογηθεί δικαστικά, θα προσφέρει νέο εμπειρικό υλικό για την εγκληματολογική ανάλυση της δομικής ατιμωρησίας.

Η εγκληματολογία των ισχυρών έχει επανειλημμένα υπογραμμίσει ότι η κοινωνική βλάβη που προκαλείται από κρατικούς και εταιρικούς δρώντες υπερβαίνει κατά πολύ εκείνη του συμβατικού εγκλήματος αλλά παραμένει συστηματικά υποεκπροσωπημένη στην ποινική δίωξη και στη δημόσια συζήτηση. Η κρατική παρακολούθηση μέσω εμπορικών spyware αποτελεί ένα από τα πιο χαρακτηριστικά παραδείγματα αυτής της δομικής ατιμωρησίας στη ψηφιακή εποχή. Η εγκληματολογική αναγνώριση του data laundering ως κατηγορίας κρατικο-εταιρικού εγκλήματος και όχι απλώς ως τεχνικής ή νομικής παράβασης αποτελεί αναγκαία προϋπόθεση για την ουσιαστική αντιμετώπισή του. Αυτή ήταν η συμβολή που επιδίωξε η παρούσα εργασία.

Βιβλιογραφία

Ξενόγλωσση Βιβλιογραφία

European Parliament PEGA Committee. (2023). Report on the use of Pegasus and equivalent surveillance and spyware . Strasbourg: European Parliament

Koukakis, T. . (2022). Πώς ανακάλυψα ότι με παρακολουθούσε η ΕΥΠ και το Predator. . Inside Story.

Milanovic, Marko. (2016). UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR. Ανάκτηση από www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr

Amnesty International & Forbidden Stories . (2021). The Pegasus Project. Amnesty Tech.

Amnesty International. (2023). Hungary: Government use of Pegasus. London: London.

Amnesty International Security Lab. (2021). Forensic Methodology Report: How to Catch NSO Group's Pegasus. Amnesty International. London: Amnesty International.

Amnesty International Security Lab. (2023). Predator Files. Amnesty International.

Ayoub, E. & Goitein, E. (2024). Closing the Data Broker Loophole. Brennan Center for Justice, NYU School of Law. New York: Brennan Center for Justice, NYU School of Law. Ανάκτηση από https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole

Bauman, Z. & Lyon, D. (2013). Liquid Surveillance: A Conversation. . Cambridge: Polity Press.

Berthelet, P. . (2022). Europe's PegasusGate: Countering Spyware Abuse. Brussels: European Parliament Research Service.

Braman, S. & Lynch, S. (2014). Information Asymmetry and Power in a Surveillance Society. Government Information Quarterly, 30(S1), S9–S17. ScienceDirect. *Information and Organization*, σσ. 214-235.

Bromley, M. & Maletta, G. (2024). Making the Most of the EU Catch-All Control on Cyber-Surveillance Exports. Stockholm International Peace Research Institute. Ανάκτηση από https://www.sipri.org/commentary/topical-backgrounder/2024/making-most-eu-catch-all-control-cyber-surveillance-exports

Chambliss,W.J. (1989). State-Organized Crime. *Criminology*, 183-208.

Chondrogiannos, T. (2023, 5 30). *gowatch*. Ανάκτηση από https://govwatch.gr/en/finds/ekthesi-tis-epitropis-pega-gia-paranomes-parakoloythiseis-stin-ellada

Cisco Talos. (2023). Mercenary Mayhem: A Technical Analysis of Intellexa's PREDATOR Spyware. Cisco Talos. Ανάκτηση από https://blog.talosintelligence.com/mercenary-intellexa-predator/

Citizen Lab . (2022, Απριλίου 18). CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru. University of Toronto.

Citizen Lab. (2021). *Pegasus Project: Technical Analysis. .*

Citizen Lab. (2021). Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. University of Toronto. Ανάκτηση από https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Citizen Lab. (2023). *Predator in the Wires: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Bid. University of Toronto.* Toronto: University of Toronto.

Columbia Law Review. (2022). Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades the Fourth Amendment. Columbia Law Review, . *122(3)*. Columbia Law Review.

Deibert, R. (2020). Reset: Reclaiming the Internet for Civil Society. 88-95. Toronto: Anansi Press.

European Data Protection Board (EDPB). (2021). Guidelines 10/2020 on Restrictions under Article 23 GDPR (Version 2.0, 13 Οκτωβρίου 2021). Ανάκτηση από https://www.edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf

European Parliament . (2022). The impact of Pegasus on fundamental rights and democratic processes (PE 740.514). Strasbourg: European Parliament.

European Parliament Committee of Inquiry (PEGA). (2023). Report on the Investigation of Alleged Contraventions in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (A9-0189/2023). Rapporteur: Sophie in 't V. PEGA. Ανάκτηση από https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

European Parliament PEGA Committee. (2023). European Parliament PEGA Committee (2023). Report on the use of Pegasus and equivalent surveillance and spyware. 18-25. Strasbourg: European Parliament. Ανάκτηση από https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html#_section1

FATF. (2012). International Standards on Combating Money Laundering. . Paris: FATF/OECD. Ανάκτηση 2026

Feldstein, S. . (2019, Σεπτέμβριος). The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace, Working Paper, , DC: Carnegie Endowment for International Peace. Washington: DC: Carnegie Endowment for International Peace.

Foucault, M. (2011). *Επιτήρηση και Τιμωρία: Η Γέννηση της Φυλακής*. . Αθήνα: Πλέθρον.

Friedrichs, D.O. (2010). Trusted Criminals: White Collar Crime in Contemporary Society . Belmont: Wadsworth.

Green, P. & Ward, T. . (2004). State Crime: Governments, Violence and Corruption. . London: Pluto Press.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* . New York: Metropolitan Books .

Harper, D.J., Ellis, D. & Tucker, I. (2021). Covert Aspects of Surveillance and the Ethical Issues They Raise. Στο *Ethical Issues in Covert, Security and Surveillance Research* (Τόμ. 8, σσ. 177-197). Emerald. doi:https://doi.org/10.1108/S2398-601820210000008012

https://predatorgate.gr/gr/victims. (χ.χ.).

https://securitylab.amnesty.org/case-study-the-pegasus-project/. (χ.χ.).

ICIJ . (2026). Greek Court Convicts Intellexa Founder Tal Dilian. International Consortium of Investigative Journalists.

IPI. (2023). Greece: Media freedom concerns deepen amid surveillance scandal. . Vienna: International Press Institute.

Kaldani, T., & Prokopets, Z. (2022). Pegasus spyware and its implications on human rights (DGI(2022)04). Ανάκτηση από https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8.

Kevin D. Haggerty and Richard V. Ericson. (2000, December). The surveillant assemblage. *British Journal of Sociology pp. 605–622, 4*(51), σσ. 605-622. doi:DOI: 10.1080/00071310020015280

Khan, A. (2022). Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism. Laws, 11(6), 85. MDPI. *11, 6*. Laws . doi: https://doi.org/10.3390/laws11060085

Kramer, R.C.& Michalowski RJ. (2006). State-Corporate Crime: WrongdoIng at the Intersection of Business and Government. New Brunwick: Rutgers University Press.

Kramer, R.C., Michalowski, R.J. & Kauzlarich, D. (2002). The Origins and Development of the Concept and Theory of State-Corporate Crime. Crime & Delinquency, 48(2),. *2, 48*, 263-282. Crime & Delinquency.

Krishna, T., & Atul, A. (2022, 11 23). *Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism.* doi:https://doi.org/10.3390/laws11060085

Lyon, D. (2007). Surveillance Studies: An Overview. 57-72. Cambridge:: Polity Press.

Lyon, D. . (2001). Surveillance Society: Monitoring Everyday Life. . Open University Press.

Lyon, D. (2018). The culture of surveillance watching as a way of life. *Cambridge polity press*.

Marczak, B. (2018). Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab Research Report No. 113. . *Citizen Lab Research Report No. 113.* . Toronto: University of Toronto.

Mathiesen, T. (1997). The Viewer Society: Michel Foucault's Panopticon Revisited. . *1(2)*, 215-234. Theoretical Criminology.

Mildebrath, H. (2022). Europe's PegasusGate. EPRS, PE 729.397· PEGA Committee (2023). EPRS. Ανάκτηση από https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf

Mildebrath, H. (2022). Greece's Predatorgate: The latest chapter in Europe's spyware scandal? . EPRS.

Mitsilegas, V. (2021). War on Terror: The Case for a Global Privay Regime,European, Transatlantic and Global Perspectives. Στο N. V. Valsamis Mitsilegas, *Surveillance and Privacy in the Digital Age.* Hart Publishing.

Modderkolk, H. (2023). *Γίνεται πόλεμος αλλα κανείς δεν τον βλέπει.* Εκδόσεις Αλεξάνδρεια.

Nyst, Carly. (2013). Interface Based Jurisdiction Over Violations of the Right to Privacy. EJIL. Ανάκτηση από www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-toprivacy/

Panzavolta, M. & Maes, E. (2022). Exclusion of Evidence in Times of Mass Surveillance. *International Journal of Evidence & Proof*. Sage Journals.

PEGA Committee. (2023). Final Report, A9-0189/2023 . PEGA Committee.

PEN America . (2013). Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor. New York: PEN American Center.

Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *(31)*, 117-182. Berkeley Technology Law Journal. Ανάκτηση από https://btlj.org/data/articles2016/vol31/31_1/0117_0182_Penney_ChillingEffects_WEB.pdf

predatorgate.gr. (2026, Μαρτίου 24). Ανάκτηση από https://predatorgate.gr/gr.

Rentmeester, C. (2022). Kant's Ethics in the Age of Online Surveillance. Chapter 9. Στο C. &. Rentmeester, *Digital Ethics and Power* (σσ. 187-204). Bellin College Press. Ανάκτηση 4 13, 2026, από https://www.diva-portal.org/smash/get/diva2:1746832/FULLTEXT01.pdf

Reporters Without Borders. (2023). World Press Freedom Index 2023. . Paris: RSF.

Reuters . (2023, Ιανουαρίου 27). Greek Government Wins No-Confidence Vote Over Wiretapping Scandal. Reuters .

Reuters . (2026, 2 26). Greek court convicts four in Predator spyware case. . Reuters.

Riecke, L. (2023). Unmasking the Term 'Dual Use' in EU Spyware Export Control. Στο *European Journal of International Law* (3 εκδ., Τόμ. 34, σσ. 697-720). European Journal of International Law. doi:https://doi.org/10.1093/ejil/chad039

Rothe, D.L. & Friedrichs, D.O. (2006). The State of the Criminology of Crimes of the State. . *1, 33*, 147-161. Social Justice,.

Saxena, P. & Anand, A. (2022). Pegasus Project: Re-Questioning the Legality of the Cyber-Surveillance Mechanism. Laws, 11(6), 85. doi:https://doi.org/10.3390/laws11060085

Simmons, J. (2009). Buying You" The Governments Use Of Third Parties to Launder Data about the People. *SSRN working Paper*.

Solove, D.J. . (2008). Understanding Privacy. Cambridge: Harvard University Press.

Stoycheff, E. (2016). Under Surveillance. . *93(2)*, 296-311. Journalism & Mass Communication Quarterly.

Sutherland, E.H. (1949). White Collar Crime. . New York: Dryden Press.

SWAMI. (2006). Safeguards in a World of Ambient Intelligence: Deliverable D2 — Dark Scenarios. European Commission Sixth Framework Programme.

Timm, T. (2012). Spy Tech Companies & Their Authoritarian Customers: Part I — FinFisher and Amesys. https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfishe. Electronic Frontier Foundation. Ανάκτηση από https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys

UNHRC . (2019). Special Rapporteur on Freedom of Opinion and Expression, Surveillance and Human Rights. UN Human Rights Council.

Zuboff, S. (2019). The Age of Surveillance Capitalism. New York: PublicAffairs, σελ. 8–15. 8-15. New York: PublicAffairs,.

Ελληνόγλωσση Βιβλιογραφία

Αναγνωστοπούλου, Δ. (2026, 03 12). Mega Stories: «Βόμβα» από καταδικασθέντα για το Predator — «Συνεργαζόμαστε μόνο με κυβερνήσεις». Mega TV. Ανάκτηση από https://www.megatv.com/2026/03/13/mega-stories-vomva-apo-katadikasthenta-gia-to-predator-synergazomaste-mono-me-kyverniseis/

Γεωργούλας, Σ. (2019). Απο το έγκλημα του λευκού κολαρου στο κρατικό εταιρικό έγκλημα. Στο *Εγκλήματα των ισχυρών-Διαφθορά, οικονομικό και οργανωμένο έγκλημαα* (σσ. 41-61). Αθήνα: ΕΑΠ.

ΔΕΕ. (2020, 6 16). Data Protection Commissioner κατά Facebook Ireland (Schrems II). ΔΕΕ.

ΕΔΑΔ. (2015, 12 4). Zakharov κατά Ρωσίας, αριθ. προσφ. 47143/06 . §§ 229-234. ΕΔΑΔ.

ΕΔΑΔ. (2016, 1 12). Szabó και Vissy κατά Ουγγαρίας, αριθ. προσφ. 37138/14. § 73. ΕΔΑΔ.

ΕΔΔΑ. (1978). Klass κατά Γερμανίας (1978), αρ. προσφυγής 5029/71. ΕΔΔΑ,.

ΕΔΔΑ. (2015). Zakharov κατά Ρωσίας (2015), αρ. προσφυγής 47143/06. ΕΔΔΑ.

ΕΔΔΑ. (2021). Big Brother Watch κατά Ηνωμένου Βασιλείου (2021), αρ. προσφυγής 58170/13. ΕΔΔΑ.

Ελληνική Δημοκρατία. (2021, Μαρτίου 25). Νόμος 4790/2021: Εκσυγχρονισμός του πλαισίου λειτουργίας της Εθνικής Υπηρεσίας Πληροφοριών. Τεύχος Α', αρ. 48,. *(Α)*. Αθήνα: Φύλλο Εφημερίδας της Κυβερνήσεως.

Παπανικολάου, Α. (2025). *Επικοινωνιακό απόρρητο και εθνική ασφάλεια.* Αθήνα: Εκδόσεις Σάκκουλα.

Τσακυράκης, Σ. (1993). *Το απόρρητο της επικοινωνίας-απόλυτα απαραβίαστο ή ευχή της έννομης τάξης*. Νομικό Βήμα.

Τριανταφύλλου, Ε. (2026). *ΤΟ ΡΕΠΟΡΤΑΖ.* Αθήνα: Αντίποδες

Χονδρογιάννης , Θ. (2023, 05 30). EU's PEGA Committee report on illegal surveillance in Greece. govwatch. Ανάκτηση 4 9, 2026, από https://govwatch.gr/en/finds/ekthesi-tis-epitropis-pega-gia-paranomes-parakoloythiseis-stin-ellada/

Χουλιάρας,, Α. (2019). ' Εγκληματικότητα των ισχυρών: Εγκληματολογική θεωρία και ποινική προβληματική. Στο Κ. Ν. Βιδάλη Σ. (Επιμ.), *Εγκλήματα των ισχυρών. Διαφθορά , οικονομικό και οργανωμένο έγκλημα* (σσ. 63-85). Αθήνα: Εκδόσεις Ε.Α.Π.