ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΔΙΑΣΦΑΛΙΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΤΗΣ ΔΗΜΟΣΙΑΣ ΑΣΦΑΛΕΙΑΣ ΜΕ ΤΗ ΣΥΓΚΛΙΣΗ ΤΗΣ ΜΗΧΑΝΙΚΗΣ ΜΑΘΗΣΗΣ ΚΑΙ ΤΗΣ ΑΝΑΛΥΤΙΚΗΣ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ: Η ΠΕΡΙΠΤΩΣΗ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΑΠΟΣΤΟΛΗΣ ΑΜΕΣΩΝ ΜΗΝΥΜΑΤΩΝ (INSTANT MESSENGERS)

Διπλωματική Εργασία

του

Χρήστου Δερβεντλή

Θεσσαλονίκη, 03/2024

Η ΔΙΑΣΦΑΛΙΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΤΗΣ ΔΗΜΟΣΙΑΣ ΑΣΦΑΛΕΙΑΣ ΜΕ ΤΗ ΣΥΓΚΛΙΣΗ ΤΗΣ ΜΗΧΑΝΙΚΗΣ ΜΑΘΗΣΗΣ ΚΑΙ ΤΗΣ ΑΝΑΛΥΤΙΚΗΣ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ: Η ΠΕΡΙΠΤΩΣΗ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΑΠΟΣΤΟΛΗΣ ΑΜΕΣΩΝ ΜΗΝΥΜΑΤΩΝ (INSTANT MESSENGERS)

Χρήστος Δερβεντλής

Πτυχίο Πολιτικής Επιστήμης, ΔΠΘ, 2018

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής:
Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/03/2024.

Ευγενία Αλεξανδροπούλου - Αιγυπτιάδου	Μαρία Μυλώση	Κωνσταντίνος Ψάννης
.....	.....	.....

Χρήστος Δερβεντλής

Περίληψη

Στην παρούσα διπλωματική εργασία, αναδεικνύεται η πτυχή της έρευνας που αφορά τη χρήση εφαρμογών αποστολής άμεσων μηνυμάτων με ισχυρή κρυπτογράφηση και την επίπτωση που έχουν στο έργο των διωκτικών αρχών. Ευρύτερα, μελετάται η δυνατότητα στάθμισης μεταξύ του δικαιώματος στην ιδιωτική ζωή και της δημόσιας ασφάλειας. Η ερευνητική προσπάθεια ξεκινά με την περιγραφή του πλαισίου ανάπτυξης της διπλωματικής εργασίας που αφορά την εξέλιξη και κατάχρηση της ισχυρής κρυπτογράφησης. Στη συνέχεια, διασαφηνίζεται η έμφαση της έρευνας μέχρι σήμερα κατά πλειοψηφία στο πεδίο της ιδιωτικότητας μέσω της μελέτης χρήσης ισχυρότερων μεθόδων κρυπτογράφησης.

Αντιλαμβανόμενοι τις δυσχέρειες που μπορεί να προκληθούν στην άσκηση καθηκόντων των διωκτικών αρχών, γίνεται εξελικτικά ξεκάθαρο πως υπάρχει ανάγκη τεχνικής λύσης η οποία θα διευκολύνει την επιβολή του νόμου, παρέχοντας παράλληλα τις απαραίτητες εγγυήσεις (τεχνικές και οργανωτικές) ώστε να μην προχωρά σε αναίτια προσβολή του δικαιώματος στην ιδιωτικότητα για τα υποκείμενα δεδομένων.

Αξιοποιώντας τις δυνατότητες της μηχανικής μάθησης και της αναλυτικής δεδομένων, η παρούσα εξερευνά την υπόθεση υιοθέτησης ενός προτύπου ασφαλείας το οποίο θα βασίζεται στην ενσωμάτωση αλγόριθμου στις εφαρμογές ανταλλαγής μηνυμάτων που θα εντοπίζει ύποπτα μοτίβα συνομιλιών, με συγκεκριμένες δικλείδες ασφαλείας υπέρ των χρηστών – ιδιαίτερα σε περιπτώσεις με περιθώρια λάθους στην αξιολόγηση ρίσκου από μεριάς του αλγόριθμου.

Η παρούσα προσπάθεια ολοκληρώνεται με στοχασμούς για περαιτέρω αξιοποίηση της υπόθεσης, στην οποία εξίσου αναλυτικά αναγνωρίζονται γκρίζες ζώνες και περιορισμοί.

Λέξεις Κλειδιά: κρυπτογράφηση, ιδιωτικότητα, ασφάλεια, μηχανική μάθηση, αναλυτική δεδομένων

Abstract

This thesis highlights the aspect of research concerning the use of instant messaging applications with strong encryption and their impact on law enforcement authorities' work. The possibility of weighing the right to privacy and public security is studied more broadly. The research effort begins with a description of the development framework of the research concerning the formulation and abuse of strong encryption. It then clarifies the emphasis of the majority of research on privacy by studying the use of stronger encryption methods.

Realizing the difficulties that may be caused in the exercise of the duties of the prosecuting authorities, it becomes evolutionarily clear that there is a need for a technical solution that will facilitate the enforcement of the law while providing the necessary guarantees (technical and organizational) so that there is no unnecessary violation of the right to privacy for data subjects.

Leveraging the capabilities of machine learning and data analytics, this research explores a possible scenario of adopting a security standard based on the integration of an algorithm into messaging applications that will detect suspicious conversational patterns, with specific safeguards in favor of users – particularly in cases with a margin of error in risk assessment on the part of the algorithm.

The present effort concludes with reflections on further development of the scenario, in which gray areas and limitations are equally recognized and analyzed.

Keywords: encryption, privacy, security, machine learning, data analytics

Ευχαριστίες

Θα ήθελα να ευχαριστήσω πρωτίστως την οικογένεια μου – τον πατέρα μου **Κωνσταντίνο**, τη μητέρα μου **Θεανώ** και τον αδερφό μου **Απόστολο**, για την κατανόηση, τις θυσίες και τη στήριξη τους καθ' όλη τη διάρκεια παρακολούθησης του ΔΠΜΣ.

Επίσης, θερμές ευχαριστίες για τη συνεργασία οφείλω στον επιβλέποντα καθηγητή μου **Κωνσταντίνο Ψάννη**, ο οποίος συνέβαλε στη διαμόρφωση της παρούσας διπλωματικής εργασίας παρέχοντας τις πολύτιμες συμβουλές του κατά την εκπόνησή της.

Τέλος, νιώθω πως χρωστώ μια από καρδιάς αναγνώριση της βοήθειας που έλαβα από τον ψυχοθεραπευτή μου, **Γιώργο**, ο οποίος αποτέλεσε σύμμαχό μου σε περιόδους που έφτανα σε τέλμα, δίνοντας μου απλόχερα τα μεθοδολογικά εργαλεία της επιστήμης του καθ' όλη τη διάρκεια συγγραφής της παρούσας.

Aut inveniam viam aut faciam.

Περιεχόμενα

1 Εισαγωγή 1

1.1 Πρόβλημα – Σημασία του θέματος 1

1.2 Σκοπός – Στόχοι – Συνεισφορά 5

1.3 Βασική Ορολογία 6

1.4 Διάρθρωση της μελέτης 10

2 Βιβλιογραφική επισκόπηση 12

2.1 Διατύπωση ερευνητικού κενού και διαμόρφωση ερευνητικής υπόθεσης: είναι δυνατή η ανάπτυξη μεθοδολογίας ώστε να εξασφαλίζεται η ιδιωτικότητα των χρηστών ενώ ταυτόχρονα θα δύνανται οι διωκτικές αρχές να εντοπίζουν περιπτώσεις υψηλού ρίσκου; 15

3 Το νομικό πλαίσιο αναφορικά με τα προσωπικά δεδομένα και τις τηλεπικοινωνίες σε ευρωπαϊκό και εθνικό επίπεδο – Βασικά σημεία 16

3.1 Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 19

3.1.1 Ο Κανονισμός Προστασίας Δεδομένων για τα ευρωπαϊκά θεσμικά όργανα (ΕΕ) 2018/1725 24

3.2 Η Οδηγία για την Προστασία Προσωπικών Δεδομένων από διωκτικές και δικαστικές Αρχές (ΕΕ) 2016/680 26

3.3 Ο Νόμος 4624/2019 και οι τροποποιήσεις του 28

3.4 Η Οδηγία για την ιδιωτικότητα στις ηλεκτρονικές επικοινωνίες (ePrivacy Directive 2002/58/ΕΚ) με την τελευταία της αναθεώρηση (2009/136/ΕΚ) 35

3.5 Εξελίξεις στο ενωσιακό νομικό πλαίσιο 38

3.5.1 Η πρόταση κανονισμού ePrivacy 38

3.5.2 Η πρόταση κανονισμού για την Τεχνητή Νοημοσύνη (EU AI Act) 40

4 Η Κρυπτογράφηση και η χρήση της στις επικοινωνίες 46

4.1 Σύγχρονες μέθοδοι κρυπτογράφησης, παρεχόμενη ασφάλεια και χρήση τους στην αγορά 49

4.1.1 Συμμετρική Κρυπτογράφηση 49

4.1.1.1 Κρυπτογράφηση Data Encryption Standard (DES) 49

4.1.1.2 Κρυπτογράφηση Advanced Encryption Standard (AES) 52

4.1.1.3 Κρυπτογράφηση Blowfish & Twofish 55

4.1.2 Ασύμμετρη Κρυπτογράφηση 56

4.1.2.1 Κρυπτογράφηση RSA 56
4.1.2.2 Κρυπτογράφηση Diffie – Hellman 58
4.1.2.3 Κρυπτογράφηση ελλειπτικών καμπυλών (ECC) 60
4.1.2.4 Κρυπτογράφηση από άκρο σε άκρο (end-to-end) 61
5 Οι αστυνομικές επιχειρήσεις στον κυβερνοχώρο 62
5.1 Νομοθετικό πλαίσιο ηλεκτρονικών παρακολουθήσεων και επισυνδέσεων – Οι Ειδικές Ανακριτικές Πράξεις 62
5.2 Οι δύο όψεις του νομίσματος: παραδείγματα παρεμπόδισης αλλά και κατάχρησης των δυνατοτήτων των Αρχών ασφαλείας μέσα από τον Τύπο 67
6 "The balancing test": Εφαρμόζοντας την αναλογικότητα με τη χρήση της τεχνολογίας – η συζήτηση για ένα νέο πρότυπο ασφαλείας με την αξιοποίηση αλγορίθμου 71
6.1 Η λειτουργία του αλγόριθμου 72
6.2 Οι εγγυήσεις για την ιδιωτικότητα των χρηστών 74
6.3 Ο αντίκτυπος στην τέλεση του αστυνομικού έργου 76
6.4 Αξιολόγηση της υπόθεσης 78
6.4.1 Τρόποι αξιοποίησης και βελτίωσης της υπόθεσης – συγκριτικά πλεονεκτήματα επί εφαρμοσμένων μοντέλων – διερεύνηση οφέλους και ωφελούμενων 78
6.4.2 Παραδοχές, ζητήματα ανοιχτά προς διερεύνηση και ανάλυση 82
6.4.3 Ο αλγόριθμος υπό το πρίσμα της πρότασης Κανονισμού EU AI Act. 87
7 Επίλογος 91
8 Βιβλιογραφία 92

Κατάλογος Εικόνων

Εικόνα: **Σελίδα:**

- Εικόνα 1: Μια τυπική διαδικασία (απο)κρυπτογράφησης **47**
- Εικόνα 2: Συμμετρική κρυπτογράφηση μηνύματος **48**
- Εικόνα 3: Ασύμμετρη κρυπτογράφηση μηνύματος **48**
- Εικόνα 4: Βήματα αλγορίθμου AES με κλειδί 128 bit. **54**
- Εικόνα 5: Επεξήγηση της λειτουργίας ανταλλαγής δημόσιου κλειδιού Diffie - Hellman κατά τον Vinck. (Προσαρμογή στην ελληνική γλώσσα) **59**
- Εικόνα 6: Παράδειγμα ελλειπτικής καμπύλης. Εντός αυτής (κόκκινο χρώμα), και με τη χρήση συνάρτησης, θα αποτυπωθούν τα σημεία που θα οδηγήσουν στην τελική δημιουργία του ζεύγους δημόσιου και ιδιωτικού κλειδιού. Πηγή: globalsign.com **61**
- Εικόνα 7: Μια σχηματική απεικόνιση των βημάτων που προτείνεται να ακολουθεί ο αλγόριθμος..... **73**
- Εικόνα 8: Εναλλακτικός τρόπος αξιοποίησης του αλγορίθμου με τη χρήση ανωνυμοποίησης..... **79**

Κατάλογος Πινάκων

- Πίνακας 1: Ελάχιστες απαιτήσεις διακίνησης συστημάτων ΤΝ με βάση το επίπεδο κινδύνου τους για τα δικαιώματα και τις ελευθερίες των ατόμων. **44**
- Πίνακας 2: Απεικόνιση ενός πίνακα state, ο οποίος περιλαμβάνει 1 byte σε κάθε του κελί και συνολικά 16 bytes (128 bit). **52**
- Πίνακας 3: Παράδειγμα state μετά την λειτουργία SubBytes. **53**
- Πίνακας 4: Παράδειγμα state μετά την λειτουργία ShiftRows. **53**

1 Εισαγωγή

1.1 Πρόβλημα – Σημασία του θέματος

Για μεγάλο μέρος του παγκόσμιου πληθυσμού, η χρήση έξυπνων κινητών τηλεφώνων είναι μέρος της καθημερινότητάς του. Από την αρχή της κυκλοφορίας τους, τα κινητά τηλέφωνα υποστήριζαν την αποστολή μηνυμάτων μεταξύ των χρηστών, αρχής γενομένης από την υπηρεσία SMS (Simple Message Service), αργότερα με τα MMS (Multimedia Messaging Service), μέχρι τη σημερινή RCS (Rich Communication Service). Παράλληλα, άλλες τεχνολογίες έκαναν την εμφάνισή τους, με σκοπό τη διευκόλυνση της επικοινωνίας των χρηστών σε ζωντανό χρόνο. Χαρακτηριστικό παράδειγμα είναι το IRC (Internet Relay Chat), το οποίο δημιουργήθηκε το 1988 από τον Φινλανδό Jarkko Oikarinen. Το IRC διευκόλυνε χιλιάδες χρήστες ανά την υφήλιο να συμμετέχουν σε συζητήσεις σχετικά με την επικαιρότητα της εποχής σε πραγματικό χρόνο και αποτέλεσε πρόγονο των σημερινών εφαρμογών άμεσης επικοινωνίας. (Scheele, 2000)

Η όλο και διευρυμένη χρήση τέτοιων εφαρμογών προσέλκυσε το ενδιαφέρον εγκληματιών του διαδικτύου, έτσι οι χρήστες υπηρεσιών instant messaging έγιναν ευάλωτοι σε μια σειρά από κινδύνους (λ.χ. η απομακρυσμένη εγκατάσταση κακόβουλου λογισμικού στο τερματικό τους), κάποιοι από τους οποίους απειλούσαν ευθέως την ιδιωτικότητα των συνομιλιών τους. (Scheele, 2000) Έτσι, παράλληλα με τους κινδύνους αναδύθηκε και η ανάγκη στεγανοποίησης των συνομιλιών των χρηστών, ειδικότερα με την αξιοποίηση της κρυπτογραφίας. Με την πάροδο των ετών, διάφορες μέθοδοι συμμετρικής και ασύμμετρης κρυπτογράφησης αξιοποιήθηκαν για την προστασία των χρηστών από κακόβουλους τρίτους. (Bhardwaj & Som, 2016) Από τον κώδικα του Καίσαρα[1] μέχρι τις σύγχρονες μεθόδους, η κρυπτογράφηση έπαιξε σημαίνοντα ρόλο στην ιδιωτικότητα, την ακεραιότητα και την πρόσβαση στο περιεχόμενο της επικοινωνίας μόνο μεταξύ του αποστολέα και του παραλήπτη – οι εφαρμογές instant messaging δε θα αποτελούσαν εξαίρεση, με τους αλγόριθμους κρυπτογράφησης να γίνονται όλο και πιο

[1] Ο κώδικας του Καίσαρα περιλαμβάνει την αντικατάσταση κάθε γράμματος ενός κειμένου με ένα άλλο το οποίο έχει σταθερή απόσταση από αυτό στο αλφάβητο. Πρόκειται για μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία.

περίπλοκοι στην προσπάθεια προστασίας του απορρήτου των επικοινωνιών. Περιπλοκότητα, που θα έφτανε στο σημείο να δυσχεραίνει το έργο των διωκτικών Αρχών.

Αυτήν την τεχνολογική εξέλιξη εκμεταλλεύτηκαν εξτρεμιστικές ομάδες σε διάφορα κράτη, καταφέρνοντας να χρησιμοποιούν κανάλια επικοινωνίας δίχως το φόβο του εντοπισμού. Είναι γνωστό πως τρομοκρατικές ομάδες όπως το Daesh χρησιμοποιούσαν την εφαρμογή Telegram ως το κύριο μέσο συντονισμού, επικοινωνίας και προπαγάνδας. (Clifford, 2020) Σα να μην έφτανε αυτό, όλο και περισσότερες εγκληματικές ομάδες (που περιλαμβάνουν αλλά δεν περιορίζονται στην τρομοκρατία), χρησιμοποιούν την ασύμμετρη κρυπτογράφηση[2] προκειμένου να σχεδιάσουν και να υλοποιήσουν τις δραστηριότητές τους. (Napoleon κ.ά., 2021) Ενδεικτική της απήχησης της κρυπτογραφίας στον κύκλο εργασιών των εγκληματιών είναι η μεθοδολογία της κοινής επιχείρησης του Αμερικανικού Ομοσπονδιακού Γραφείου Ερευνών (FBI), Αστυνομιών της EUROPOL, της Αυστραλιανής Αστυνομίας καθώς και του Αμερικανικού Οργανισμού για την Καταπολέμηση των Ναρκωτικών (DEA), οι οποίες στην ουσία διείσδυσαν σε παράνομες αγοραπωλησίες εντός του σκοτεινού διαδικτύου[3] υποκρινόμενες τη λειτουργία εταιρίας που κατασκευάζει κρυπτογραφημένες συσκευές τηλεπικοινωνίας, με στόχο την πώλησή τους σε εγκληματίες και την παρακολούθηση των επικοινωνιών τους. Η έρευνα, η οποία αποτέλεσε μια από τις μεγαλύτερες επιχειρήσεις με αντικείμενο το έγκλημα στον κυβερνοχώρο με έμφαση τις κρυπτογραφημένες επικοινωνίες, κατέληξε στον εντοπισμό και τη σύλληψη οκτακοσίων εγκληματιών ανά την υφήλιο. (EUROPOL, 2021)

Καταλαβαίνουμε, λοιπόν, πως το έργο των διωκτικών Αρχών ολοένα και δυσχεραίνει απέναντι στην τεχνολογική εξέλιξη των μεθόδων κρυπτογράφησης. Η δυσχέρεια αυτή φαίνεται ακόμη περισσότερο αν αναλογιστούμε τη μεθοδολογία

[2] Ασύμμετρη θεωρείται η κρυπτογράφηση που αντί να χρησιμοποιεί ένα «κλειδί» ώστε να κρυπτογραφείται το περιεχόμενο της επικοινωνίας, χρησιμοποιούνται δύο: ένα δημόσιο και ένα ιδιωτικό. Έτσι, επιτυγχάνεται μεγαλύτερη ασφάλεια απέναντι στην αποκρυπτογράφηση, καθώς για την τελευταία χρησιμοποιείται το ιδιωτικό κλειδί του παραλήπτη, το οποίο διαθέτει μόνον αυτός.

[3] Το μέρος του διαδικτύου που δεν είναι προσβάσιμο από κοινούς φυλλομετρητές (λ.χ. Edge, Firefox, Chrome). Χρειάζεται συγκεκριμένους φυλλομετρητές (λ.χ. Tor Browser), καθώς και γνώση των ιστοσελίδων, μιας το σκοτεινό διαδίκτυο δε χρησιμοποιεί την κατηγοριοποίηση των ιστοσελίδων μέσω των επεκτάσεων .com, gr κλπ. αλλά .onion. Λόγω της ασφάλειας που προσφέρει (μέσω των πολλαπλών ανακατευθύνσεων που καθιστούν πολύ δύσκολη την ταυτοποίηση του χρήστη), χρησιμοποιείται κατά κόρων από εγκληματικές οργανώσεις για αγοραπωλησία παράνομων προϊόντων και υπηρεσιών.

επιχειρήσεων σαν και αυτή που περιγράφτηκε παραπάνω, κατά την οποία οι Αρχές χρειάστηκε να επιστρατεύσουν εκτός από τεχνικές λύσεις και μεθόδους της κοινωνικής μηχανικής[4] προκειμένου να μπορέσουν να εντοπίσουν την εγκληματική δραστηριότητα «εκ των έσω». Παρόλο που οι υπηρεσίες πληροφοριών και οι αστυνομικές Αρχές ανά τον κόσμο στελεχώνονται από τα ικανότερα μυαλά στον τομέα της πληροφορικής, η διαλεύκανση εγκλημάτων και η πρόληψή τους γίνεται ολοένα και δυσκολότερη όσο οι εγκληματίες χρησιμοποιούν την κρυπτογράφηση για τους σκοπούς τους.

Από την άλλη, δε θα πρέπει να πέσουμε στην παγίδα του συμβιβασμού εξ ολοκλήρου της ιδιωτικότητας μας θέτοντας την κρυπτογραφία εκτός του τομέα των επικοινωνιών, καθώς τα οφέλη της τελευταίας, εκτός από την ιδιωτικότητα, συμβάλλουν και στην ασφάλεια των προσωπικών μας δεδομένων έναντι κακόβουλων τρίτων. Δε θα πρέπει να ξεχνάμε πως η ιδιωτικότητα αναγνωρίζεται ως δικαίωμα το οποίο χαίρει ιδιαίτερης προστασίας τόσο στην ελληνική όσο και στην ευρωπαϊκή έννομη τάξη. Ενδεικτικά (διότι θα ακολουθήσει ανάλυση στο κεφάλαιο 3), τα βασικά νομοθετήματα που περιλαμβάνουν την προστασία της ιδιωτικής ζωής στις προβλέψεις τους είναι σε εθνικό επίπεδο:

- Το Σύνταγμα της Ελλάδος (Άρθρα 9, 9^{A}, 19) (Βουλή των Ελλήνων, 2019),
- Ο νόμος 4624/2019[5], όπως τροποποιήθηκε από τον νόμο 5002/2022 και εμπλουτίστηκε σε θέματα άρσης του απορρήτου για λόγους εθνικής ασφάλειας,
- Ο νόμος 3471/2006[6], ο οποίος ενσωματώνει την ευρωπαϊκή Οδηγία 2002/58/ΕΚ και εξειδικεύει το καθεστώς της επεξεργασίας των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών,
- Ο νόμος 3674/2008, που ενισχύει το πλαίσιο διασφάλισης του απορρήτου των τηλεφωνικών και ηλεκτρονικών επικοινωνιών,

[4] Πρόκειται για την (κυρίως) προφορική χειραγώγηση, κατά την οποία ο θύτης παρουσιάζει μια ψεύτικη ταυτότητα (με τη στενή και την ευρύτερη έννοια) στο θύμα με σκοπό την απόσπαση πληροφοριών. Χαρακτηριστικό παράδειγμα είναι η τηλεφωνική εξαπάτηση.

[5] Σχετικά με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις., 2019

[6] Σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

- Άλλα νομοθετήματα, οδηγίες και αποφάσεις των αρμόδιων Ανεξάρτητων Αρχών (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων και Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών) τα οποία εξειδικεύουν τις διατάξεις της κύριας νομοθεσίας σε θέματα ερμηνείας της και υιοθέτησης τεχνικών και οργανωτικών μέσων από τους παρόχους υπηρεσιών επικοινωνών για τη διασφάλιση του απορρήτου και της νομιμότητας της επεξεργασίας των προσωπικών δεδομένων.

Σε επίπεδο Ευρωπαϊκής Ένωσης, έχουμε να κάνουμε κυρίως με Οδηγίες και Κανονισμούς που αφορούν την επεξεργασία προσωπικών δεδομένων και την εξασφάλιση του απορρήτου των επικοινωνιών, με τα βασικά (σε ισχύ) νομοθετήματα να είναι:

- Ο Γενικός Κανονισμός Προστασίας Δεδομένων - ΓΚΠΔ (Κανονισμός ΕΕ 2016/679) όπως τροποποιήθηκε από τα διορθωτικά έγγραφα που δημοσιεύθηκαν στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης[7], ως γενικότερος κανόνας δικαίου με αυτόματη ισχύ σε όλα τα κράτη-μέλη της Ε.Ε. χωρίς την υποχρέωση ενσωμάτωσης στο εθνικό δίκαιο,
- Ο Κανονισμός (ΕΕ) 2018/1725 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, κατά τα πρότυπα του ΓΚΠΔ.
- Η Οδηγία (ΕΕ) 2016/680 για την προστασία των προσωπικών δεδομένων από τις διωκτικές και δικαστικές αρχές στο πλαίσιο άσκησης των αρμοδιοτήτων τους – με την Οδηγία να ενσωματώνεται στην εθνική νομοθεσία με το Ν. 4624/2019,
- Η Οδηγία 2002/58/ΕΚ για την προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, όπως ισχύει με την τελευταία αναθεώρησή της[8] και έχει ενσωματωθεί στην ελληνική έννομη τάξη με το Ν. 4070/2012, ο οποίος με τη σειρά του τροποποιήθηκε με το Ν. 4727/2020.
- Άλλες Οδηγίες σχετικά με τα πρότυπα υπηρεσιών και δικτύων, καθώς και γνωμοδοτήσεις και αποφάσεις του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, του ευρωπαϊκού οργανισμού που έχει ως βασικό ρόλο την εξασφάλιση της συνεκτικής ερμηνείας και εφαρμογής της ενωσιακής νομοθεσίας στα κράτη-μέλη.

[7] Διαθέσιμα στο σύνδεσμο http://data.europa.eu/eli/reg/2016/679/2016-05-04 (πρόσβαση 27/1/2023)

[8] Με την Οδηγία 2009/136/ΕΚ, διαθέσιμη στο σύνδεσμο http://data.europa.eu/eli/dir/2009/136/2020-12-21 (πρόσβαση 27/1/2023)

Σαφώς, δεν θα μπορούσε να παραληφθεί η αναφορά στη Σύμβαση 108 του Συμβουλίου της Ευρώπης, όπως έχει τροποποιηθεί από το σχετικό πρωτόκολλο, καθώς πρόκειται για το πρώτο ιστορικά δεσμευτικό κείμενο στον ευρωπαϊκό χώρο που δημιουργεί ένα πλαίσιο προστασίας για τα (αρχικά ευαίσθητα) προσωπικά δεδομένα των πολιτών.

Παρατηρούμε, λοιπόν, πως οι Αρχές βρίσκονται μεταξύ δύο πυρών: καλούνται να δείξουν τη μέγιστη αποτελεσματικότητα όσον αφορά την πρόληψη και την πάταξη του εγκλήματος χωρίς ωστόσο να έχουν στη διάθεσή τους τα μέσα που βρίσκονται στα χέρια των εγκληματιών, ενώ ταυτόχρονα – σε αντίθεση με τους φορείς του εγκλήματος – καλούνται να σεβαστούν τα νομοθετήματα που προστατεύουν το δικαίωμα στην ιδιωτικότητα. Και ενώ επί της αρχής ορθώς πράττουν, επί του πρακτέου δημιουργούνται εμπόδια και καθυστερήσεις στην άσκηση των καθηκόντων τους που σε ορισμένες περιπτώσεις ενδέχεται να κοστίσουν ανθρώπινες ζωές.

1.2 Σκοπός – Στόχοι – Συνεισφορά

Υπάρχει άραγε η δυνατότητα παράκαμψης των παραπάνω εμποδίων με τεχνικά μέσα, τα οποία παράλληλα να μην προσβάλλουν το δικαίωμα των υποκειμένων στην ιδιωτική τους ζωή και στο απόρρητο της επικοινωνίας τους; Μπορούν να αναπτυχθούν τεχνικές λύσεις με την αξιοποίηση της τεχνητής νοημοσύνης και της αναλυτικής δεδομένων ώστε οι διωκτικές Αρχές να «λύσουν τα χέρια τους» αλλά με την υιοθέτηση τέτοιων δικλείδων που δεν θα παραβιάζεται ένα από τα σημαντικότερα δικαιώματα της σύγχρονης κοινωνίας;

Σκοπός της παρούσας ερευνητικής προσπάθειας είναι να αναδείξει, εκτός από τη χρησιμότητα, και τις δυσλειτουργίες που μπορεί να δημιουργήσει η ανάπτυξη και η εκτεταμένη χρήση της κρυπτογραφίας χωρίς την ανάλογη διεργασία για την διατήρηση της επιχειρησιακής ικανότητας των Αρχών, συμβάλλοντας στο διάλογο μεταξύ των ενδιαφερομένων μερών. Το εγχειρίδιο που διαβάζετε επικεντρώνεται στις εφαρμογές αποστολής άμεσων μηνυμάτων (instant messengers), όμως τα περισσότερα από τα χαρακτηριστικά που θα περιγραφτούν στις επόμενες σελίδες μπορούν να βρουν εφαρμογή σε οποιοδήποτε μέσο χρησιμοποιεί την κρυπτογράφηση για την προστασία του περιεχομένου των επικοινωνιών.

Θα ήταν απολύτως ατελέσφορη η συγγραφή της παρούσας αν δεν υπήρχε προσδοκώμενη συνεισφορά στην επιστημονική κοινότητα και στην Κοινωνία της

Πληροφορίας. Η συνεισφορά αυτή συνίσταται στην υπόθεση ενός μοντέλου αναγνώρισης μοτίβων συνομιλιών υψηλού ρίσκου, σεβόμενοι απόλυτα το απόρρητο της επικοινωνίας των χρηστών – ιδιαίτερα όσων δεν εμπλέκονται σε ενδεχόμενη εγκληματική δραστηριότητα, το οποίο θα επιτρέπει στις Αρχές την αποτελεσματικότερη αποτρεπτική δράση τους σε σχεδιαζόμενα εγκλήματα. Απώτερος στόχος της πρακτικής εφαρμογής της παρούσας υπόθεσης είναι η μείωση (αν όχι η εξάλειψη) των θυμάτων εγκλημάτων στα τα οποία αξιοποιείται η αποστολή μηνυμάτων για το συντονισμό τους, και η υιοθέτηση των κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε η προτεινόμενη μεθοδολογία να παραμένει εντός των ορίων της νομοθεσίας, προστατεύοντας στο μέγιστο βαθμό τους χρήστες των υπηρεσιών επικοινωνιών.

1.3 Βασική Ορολογία

Οι παρακάτω όροι θεωρούνται θεμελιώδεις για την κατανόηση σε βάθος της παρούσας εργασίας. Πέραν αυτών, οποιαδήποτε ορολογία χρήζει επεξήγησης, αυτή θα δίνεται με τη μορφή υποσημείωσης.

- **End-to-end encryption**: Κρυπτογράφηση από άκρο σε άκρο. Μέθοδος κρυπτογράφησης μέσω της οποίας κατά την αποστολή ενός μηνύματος, το κλειδί αποκρυπτογράφησης αποθηκεύεται τοπικά στην τερματική συσκευή και όχι στους εξυπηρετητές του παρόχου.
- **GDPR**: Ο Κανονισμός (ΕΕ) 2016/679 ή αλλιώς Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ).
- **Instant messenger**: εφαρμογή αποστολής άμεσων μηνυμάτων η οποία κυρίως εγκαθίσταται στις έξυπνες συσκευές και χρησιμοποιεί αλγόριθμους κρυπτογράφησης για την προστασία του περιεχομένου της επικοινωνίας.
- **ISP (Internet Service Provider)**: Πάροχος Υπηρεσιών Διαδικτύου. Ο φορέας (συνήθως κερδοσκοπικού χαρακτήρα) που παρέχει στους πελάτες του υπηρεσίες που σχετίζονται με την πρόσβαση και την αξιοποίηση του διαδικτύου, συνήθως έναντι αντιτίμου.
- **RCS: Rich Communication Service**. Νέο πρωτόκολλο επικοινωνίας το οποίο αποτελεί εξέλιξη του SMS/MMS, προσθέτοντας περισσότερες δυνατότητες στην επικοινωνία, όπως η αποστολή αρχείων, οι κλήσεις, η χρήση χαρτών εκτός του μηνύματος κ.ά.

- **SSL: Secure Sockets Layer**. Πρωτόκολλο ασφαλείας για την εξασφάλιση και την πιστοποίηση της ασφαλούς – κρυπτογραφημένης σύνδεσης μεταξύ εξυπηρετητών και των τελικών εφαρμογών client, όπως π.χ. τους φυλλομετρητές.
- **TLS: Transport Layer Security**. Πρωτόκολλο ασφαλείας για την κρυπτογράφηση της επικοινωνίας κατά τη μεταφορά πληροφοριών σε υπηρεσίες επικοινωνών, όπως email. Αντικατέστησε το SSL λόγω της μεγαλύτερης ασφάλειας που προσφέρει και της μικρότερης πολυπλοκότητάς του σε σχέση με αυτό.
- **Αλγόριθμος**: σειρά βημάτων (μέθοδος) για την επίλυση ενός προβλήματος, με πεπερασμένο, αιτιοκρατικό και αποτελεσματικό χαρακτήρα, που υλοποιείται σε πρόγραμμα ηλεκτρονικού υπολογιστή. (Γεωργιάδης κ.ά., 2016)
- **Αναλυτική δεδομένων**: ανάλυση μεγάλου όγκου δεδομένων με σκοπό την εξαγωγή μοτίβων και συμπερασμάτων.
- **Ανωνυμοποίηση**: η διαδικασία κατά την οποία τα δεδομένα «δεν σχετίζονται πλέον με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο», «έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί»[9]
- **Απλά προσωπικά δεδομένα**: ή αλλιώς «δεδομένα προσωπικού χαρακτήρα κατά τον ΓΚΠΔ είναι «κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου»
- **Βιομετρικά δεδομένα**: σύμφωνα με τον ΓΚΠΔ, τα βιομετρικά δεδομένα είναι «δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα»

[9] Αιτιολογική σκέψη 26 Γενικού Κανονισμού Προστασίας Δεδομένων.

- **Εκτελών την επεξεργασία δεδομένων**: Ορίζεται από τον ΓΚΠΔ ως «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας»
- **Εξωτερικά στοιχεία επικοινωνίας (μεταδεδομένα)**: Στον τομέα των τηλεπικοινωνιών, μεταδεδομένα (ή αλλιώς εξωτερικά στοιχεία επικοινωνίας) ονομάζονται οι πληροφορίες πέραν του περιεχομένου της επικοινωνίας, οι οποίες της προσδίδουν συγκεκριμένα χαρακτηριστικά. Παραδείγματα μεταδεδομένων είναι ο αποστολέας και ο παραλήπτης, το είδος της επικοινωνίας, η διάρκεια της επικοινωνίας και οι γεωγραφικές συντεταγμένες των τερματικών από τις οποίες έγινε η επικοινωνία.
- **Ευαίσθητα προσωπικά δεδομένα**: πληροφορίες που το υποκείμενο δεδομένων (ήτοι το φυσικό πρόσωπο που φέρει τα προσωπικά δεδομένα) ενδέχεται να μην επιθυμεί την ευρεία γνωστοποίησή τους, η οποία με τη σειρά της ίσως ενέχει δυσμενή αντίκτυπο στα δικαιώματα και τις ελευθερίες του. Τα ευαίσθητα προσωπικά δεδομένα ονομάζονται αλλιώς και «ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα» και απαριθμούνται στο άρθρο 9 ΓΚΠΔ.
- **Ευρωπαϊκή οδηγία**: Νομική πράξη η οποία ανήκει στο παράγωγο δίκαιο της Ευρωπαϊκής Ένωσης και ορίζεται από το άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης. Η βασική της διαφορά με τον Κανονισμό είναι πως σε αντίθεση με τον τελευταίο, η Οδηγία πρέπει να μεταφερθεί στο εθνικό δίκαιο των κρατών-μελών για να τεθεί σε ισχύ, καθώς εστιάζει στο επιδιωκόμενο αποτέλεσμα, η επίτευξη του οποίου επαφίεται στο κάθε κράτος-μέλος.
- **Ευρωπαϊκός κανονισμός**: Νομική πράξη στην ευρωπαϊκή έννομη τάξη η οποία έχει γενική ισχύ στο σύνολό της, δεσμεύει στις περισσότερες περιπτώσεις όλα τα κράτη-μέλη και ισχύει σε αυτά άμεσα. Οι ευρωπαϊκοί κανονισμοί ορίζονται στο άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).
- **Κρυπτογραφία**: μέρος της επιστημονικής περιοχής της κρυπτολογίας (μαζί με την κρυπτανάλυση) (Μαυρίδης, 2016a). Πρόκειται για επιστημονικό πεδίο με βασικό αντικείμενο την μελέτη τεχνικών απόκρυψης του περιεχομένου ενός μηνύματος από μη εξουσιοδοτημένες οντότητες, κυρίως μέσω της χρήσης αλγορίθμων.
- **Μηχανική μάθηση**: Υποπεδίο του τομέα της τεχνητής νοημοσύνης. Πρόκειται για τη δυνατότητα ενός συστήματος να βελτιώνει την απόδοσή του όταν εκτελεί μια

εργασία, χωρίς να χρειάζεται να προγραμματιστεί από την αρχή, μέσω της δημιουργίας μοντέλων ή μοτίβων από ένα σύνολο δεδομένων. (Γεωργούλη, 2015)

- **Νομική βάση**: Η νομική αιτιολόγηση πάνω στην οποία βασίζεται η επεξεργασία δεδομένων, εξασφαλίζοντας πως είναι σύννομη.
- **Στεγανογραφία**: η πρακτική της απόκρυψης της ύπαρξης ενός μηνύματος, κρύβοντάς το μέσα σε ένα φαινομενικά απροστάτευτο μέρος της επικοινωνίας μεταξύ αποστολέα και παραλήπτη. Η βασική διαφορά μεταξύ στενογραφίας και κρυπτογραφίας είναι ότι η τελευταία πραγματεύεται την παρεμπόδιση της πρόσβασης στο περιεχόμενο ενός μηνύματος ενώ η πρώτη την απόκρυψη του ίδιου του μηνύματος, το οποίο δεν είναι απαραίτητα κρυπτογραφημένο. (Μαυρίδης, 2016b)
- **Συγκατάθεση**: στον Γενικό Κανονισμό Προστασίας Δεδομένων[10], η συγκατάθεση ενός φυσικού προσώπου ορίζεται ως «κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν»
- **Συνθετικά δεδομένα**: τεχνητά δεδομένα, η παραγωγή των οποίον είναι αποτέλεσμα επεξεργασίας πρωτότυπων δεδομένων μέσω ενός μοντέλου που είναι εκπαιδευμένο να αναπαράγει τη δομή και τα χαρακτηριστικά των πρωτότυπων. Στόχος για τη χρήση τους είναι η μείωση του ρίσκου που συνεπάγεται η επεξεργασία προσωπικών δεδομένων, διατηρώντας ταυτόχρονα την ίδια αξία όταν υπόκεινται σε στατιστική ανάλυση.(EDPS, 2023)
- **Τεχνητή νοημοσύνη**: Τομέας της Επιστήμης των Υπολογιστών με βασικό αντικείμενο τη σχεδίαση και την υλοποίηση υπολογιστικών συστημάτων με την ικανότητα μίμησης ανθρώπινων γνωστικών ικανοτήτων να μιμηθούν τις ανθρώπινες γνωστικές ικανότητες, όπως η επίλυση προβλημάτων, η αντίληψη και κατανόηση εικόνων, η μάθηση, η εξαγωγή συμπερασμάτων, η κατανόηση φυσικής γλώσσας, και άλλων. (Βλαχάβας κ.ά., 2020)

[10] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ, 2016)

- **Τρίτο μέρος (third party)**: Ο Γενικός Κανονισμός Προστασίας Δεδομένων το περιγράφει ως «οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα»
- **Υπεύθυνος επεξεργασίας δεδομένων**: Κατά τον Κανονισμό (ΕΕ) 2016/679, είναι «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους»
- **Υποκείμενο δεδομένων**: Ένα ταυτοποιήσιμο φυσικό πρόσωπο, το οποίο σύμφωνα με τον ΓΚΠΔ είναι «εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου»
- **Ψευδωνυμοποίηση**: κατά τον Κανονισμό (ΕΕ) 2016/679, είναι «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο»

1.4 Διάρθρωση της μελέτης

Η παρούσα μελέτη ξεκινάει από την προσέγγιση του προβλήματος που αποτελεί το εναρκτήριο λάκτισμα. Περιγράφεται η σημασία του, και πώς προσδοκάται να συμβάλλει η διπλωματική εργασία στον επιστημονικό διάλογο και την κοινωνία.

Έπειτα, περνάμε σε μια βιβλιογραφική επισκόπηση της τελευταίας πενταετίας, η οποία επικεντρώνεται στην τάση της επιστημονικής κοινότητας να ενισχύει την ιδιωτικότητα των χρηστών με τεχνικά μέσα, χωρίς παράλληλη υποστήριξη του αστυνομικού έργου που επηρεάζεται. Η επισκόπηση αυτή θα μας οδηγήσει στο ερευνητικό κενό το οποίο θα κληθούμε να συζητήσουμε παρακάτω: μπορούμε να ισορροπήσουμε μεταξύ ιδιωτικότητας και δημόσιας ασφάλειας χρησιμοποιώντας την τεχνητή νοημοσύνη και τα μεγάλα δεδομένα στο έργο των διωκτικών Αρχών;

Οι τελευταίες, όμως, δε λειτουργούν εκτός νόμου. Υπάρχουν διαδικασίες που ακολουθούνται, οι οποίες μεν συνδέονται με καθυστερήσεις αλλά βασίζονται στο υπάρχον νομοθετικό πλαίσιο ώστε να εξασφαλίζεται η αρχή της αναλογικότητας στο έργο τους. Σε αυτό το νομικό πλαίσιο θα αναφερθούμε στο τρίτο μέρος της παρούσας, αναλύοντας τα κύρια σημεία των βασικών νομοθετημάτων αναφορικά με την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας τόσο στον ελλαδικό όσο και στον ευρωπαϊκό χώρο. Σε αυτό το σημείο θα στοιχειοθετήσουμε και τις ζυμώσεις που γίνονται, κυρίως σε επίπεδο Ε.Ε., για μελλοντικά νομοθετήματα.

Για να κατανοήσουμε τη δυσκολία που αντιμετωπίζουν οι Αρχές στην άσκηση των καθηκόντων τους, κρίνεται αναγκαίο να περιγράψουμε τις βασικές μεθόδους κρυπτογράφησης που χρησιμοποιούνται ευρέως στην αγορά, τη χρήση τους στην καθημερινότητα των καταναλωτών, καθώς και το επίπεδο παρεχόμενης ασφάλειας τόσο από τις διωκτικές Αρχές, όσο και από κακόβουλους τρίτους.

Μεγάλο ενδιαφέρον παρουσιάζει το επιχειρησιακό κομμάτι των Αρχών στο διαδίκτυο. Έτσι, στο πέμπτο κεφάλαιο θα πραγματευτούμε το (κυρίως ελληνικό) νομοθετικό πλαίσιο αποκλειστικά στον τομέα των ηλεκτρονικών παρακολουθήσεων και επισυνδέσεων (μέρος του οποίου έχει συζητηθεί επιγραμματικά στο τρίτο κεφάλαιο), θα αναφέρουμε τους τρόπους με τις οποίες οι Αρχές παρακολουθούν εγκληματικές οντότητες – ο Τύπος θα φανεί ιδιαίτερα χρήσιμος σε αυτό το σημείο, ενώ για λόγους δεοντολογίας και διαφάνειας, δε θα παραλειφθεί η αναφορά σε περιπτώσεις κατάχρησης των δυνατοτήτων των Αρχών, ζήτημα στο οποίο παίζει καίριο ρόλο ο ανθρώπινος παράγοντας, τον οποίο επιδιώκουμε μέσω του αλγόριθμου που θα προταθεί να μειώσουμε στο απολύτως απαραίτητο επίπεδο.

Όλοι αυτοί οι προβληματισμοί, τα γεγονότα και οι προσεγγίσεις, φέρνουν ως λογική συνέπεια την προσπάθεια εξισορρόπησης της δημόσιας ασφάλειας με την ιδιωτικότητα, μέσα από την υπόθεση για ένα πρότυπο ασφαλείας που θα λειτουργεί στις

εφαρμογές αποστολής άμεσων μηνυμάτων μέσω της χρήσης αλγορίθμου. Στην έκτη ενότητα της παρούσας διπλωματικής εργασίας περιγράφονται αναλυτικά τα βήματα του αλγορίθμου, ενώ παράλληλα προτείνονται τεχνικές και οργανωτικές εγγυήσεις που θα λειτουργούν προς όφελος της ιδιωτικότητας των χρηστών. Εξετάζεται ο αντίκτυπος που μπορεί να έχει η χρήση ενός τέτοιου αλγορίθμου στο αστυνομικό έργο (λ.χ. τι πόροι ενδεχομένως να χρειάζονται από τις Αρχές σε χρόνο, λογισμικό και ανθρώπινο δυναμικό), ενώ επιχειρείται και η αξιολόγηση της υπόθεσης μέσα από μια πιο κριτική ματιά, μέσω παραδοχών και ανοιχτών ζητημάτων προς περαιτέρω βελτίωση και διερεύνηση. Η αξιολόγηση του αλγορίθμου ολοκληρώνεται με μια πρώιμη κατάταξή του στο σύστημα που περιγράφεται στην πρόταση ευρωπαϊκού κανονισμού για την τεχνητή νοημοσύνη – EU AI Act, η οποία βρίσκεται στο στάδιο της διαβούλευσης.

Η έρευνα κλείνει με μια γενικότερη αξιολόγηση της προσπάθειας και των δυνατοτήτων των τεχνολογιών αιχμής στην πρόληψη και καταστολή του εγκλήματος μέσω του κυβερνοχώρου.

2 Βιβλιογραφική επισκόπηση

Στο δημόσιο ακαδημαϊκό και ερευνητικό βίο, το ζήτημα της ασφάλειας της ιδιωτικής ζωής και των επικοινωνιών έχει αναλυθεί σε διάφορους τομείς και από πολλούς δρώντες. Οι κυριότερες πτυχές του συναντώνται στον ακαδημαϊκό χώρο, σε έρευνες - εκδόσεις της Κοινωνίας των Πολιτών και των επιχειρήσεων, σε εκθέσεις και δημοσιεύσεις θεσμικών φορέων, σε αναλύσεις που αναπτύσσονται σε δικαστικές αποφάσεις και φυσικά στον δημοσιευμένο Τύπο.

Ο ακαδημαϊκός διάλογος σε αυτήν την προβληματική έχει μακρά ιστορία, με τις αρχικές συνεισφορές να ξεκινάνε λίγο μετά τα μέσα του 20ού αιώνα. Σε τεχνικό επίπεδο, οι βάσεις τέθηκαν από τους εμπνευστές των αλγορίθμων κρυπτογράφησης, οι οποίοι παρουσίασαν νέους τρόπους προστασίας του απορρήτου. Η δομή Feistel (1974) αποτέλεσε την πρώτη ευρέως χρησιμοποιούμενη πρόταση στην κρυπτογράφηση δεδομένων με μορφή δέσμης. Η πρόταση αυτή θα χρησιμοποιούνταν κατά την προτυποποίηση του Data Encryption Standard και αργότερα στους νέους αλγόριθμους Advanced Encryption Standard (National Institute of Standards and Technology, 2023a) και Blowfish (Schneier, 1994). Στους αλγόριθμους ροής, την αρχή έκαναν οι Diffie και Hellman (1976) περιγράφοντας για πρώτη φορά την κρυπτογράφηση δημόσιου κλειδιού, σε έναν

αλγόριθμο που θα ενισχύονταν αργότερα από τις ιδιότητες των ελλειπτικών καμπυλών (Koblitz, 1987; Miller, 1986). Η μεθοδολογία που ανέπτυξαν οι Diffie – Hellman, θα χρησιμοποιούνταν αργότερα και στον αλγόριθμο RSA (Rivest κ.ά., 1978), επεκτείνοντας τη χρήση της κρυπτογράφησης δημόσιου κλειδιού σε εφαρμογές αυθεντικοποίησης και ψηφιακής υπογραφής. Ο RSA απολαμβάνει ευρεία χρήση μέχρι και σήμερα και θεωρείται εις εκ των ασφαλέστερων αλγορίθμων.

Βέβαια, οι παραπάνω αλγόριθμοι τύγχαναν και κριτικής, καθώς όσο αναπτύσσονταν η τεχνολογία, άρχισαν να εμφανίζονται στην επιφάνεια τους ευπάθειες. Οι Bhardwaj και Som (2016) περιγράφουν τα τρωτά σημεία των κρυπτογραφικών συστημάτων που οδήγησαν διαχρονικά στην ανάπτυξη ισχυρότερων, ενώ αντίστοιχη σύγκριση περιγράφεται και για τους ευρύτερα γνωστούς αλγορίθμους DES, AES & Blowfish (Chinnasamy & Kailasam, 2023). Όσον αφορά την ανταλλαγή κλειδιών κατά Diffie – Hellman, έχει και αυτή την κριτική της, η οποία περιγράφεται στο έργο των Adrian κ.ά. (2015).

Το ζήτημα όμως προσεγγίστηκε και σε θεωρητικό – κοινωνιολογικό επίπεδο, με τη βιβλιογραφία να είναι πλούσια όσον αφορά την ιδιωτικότητα (συμπεριλαμβανομένης στις ηλεκτρονικές επικοινωνίες), τόσο από πλευράς κατάχρησης και καταστρατήγησης της, όσο και με τα ρίσκα που συνδέονται με αυτή. Ιδιαίτερα, όσον αφορά την προληπτική αστυνόμευση, η αποτελεσματικότητα της αλγοριθμικής ενσωμάτωσης έχει υπάρξει αντικείμενο ανάλυσης, με μελέτες περίπτωσης την Ολλανδία (Oosterloo & Schie, 2018; Strikwerda, 2021; Schuilenburg & Soudijn, 2023) αλλά και τις ΗΠΑ (Brayne, 2017; Carleton κ.ά., 2020; Brayne & Christin, 2021; Gaddis, 2022). Αντίστοιχη βιβλιογραφική μελέτη με επιπλέον εγχώρια δεδομένα γίνεται και από τον Γκόλνα (2022). Επίσης, ενδιαφέρον παρουσιάζει το έργο των Hussein & Abdulameer (2022), οι οποίοι προτείνουν τη χρήση νευρωνικών δικτύων βαθιάς μάθησης για την πρόβλεψη τριών χαρακτηριστικών εγκλημάτων: τον τύπο, την ώρα και το μέρος που πρόκειται να συμβούν.

Όσον αφορά τη χρήση εφαρμογών ανταλλαγής άμεσων μηνυμάτων από άτομα στο φάσμα του θρησκευτικού εξτρεμισμού, μεγάλο ενδιαφέρον μπορούμε να βρούμε στην έκθεση του Clifford εκ μέρους του International Centre for the Study of Radicalisation (2020), στην οποία παρατηρείται ένα μοτίβο προτίμησης εφαρμογών που χρησιμοποιούν ισχυρή κρυπτογράφηση και εγγυώνται την ανωνυμία με επιπλέον τεχνικά μέτρα – μια πολύ δημοφιλής εξ αυτών είναι η εφαρμογή Telegram. Βέβαια, παρόλο που η χρήση ισχυρής κρυπτογράφησης είναι διαδεδομένη ανάμεσα σε τρομοκρατικές ομάδες, συνεχίζει

να θεωρείται απαραίτητη, με τα οφέλη της για την πλειονότητα των χρηστών να υπερτερούν των πιθανών κινδύνων της, σύμφωνα με τη σχετική έκθεση της διεθνούς οργάνωσης Privacy International (2022).

Λαμβάνοντας υπόψη πως στο εσωτερικό μας δίκαιο το δικαίωμα στην ιδιωτικότητα δεν είναι απόλυτο αλλά υπό συγκεκριμένες προϋποθέσεις ο νόμος προβλέπει την παραβίασή του από τις αρχές (βλ. Κεφάλαιο 5), σχετική ανάλυση για την άρση του απορρήτου των επικοινωνιών έχουν κάνει μεταξύ άλλων οι Δαλακούρας (2019), Καρανικόλα (2022), Κορίζης (2022), Ναζίρης (2023) και Παπαδημητράκης (2023). Οι δημοσιεύσεις των παραπάνω λήφθηκαν υπόψη κατά τη συγγραφή της παρούσης.

Σημαντική συμβολή στην θέση του τεχνολογικού διαλόγου στο εδώ και στο τώρα έπαιξαν οι τεκμηριώσεις επιχειρήσεων (κυρίως στον κλάδο της πληροφορικής), οι οποίες ενσωματώνουν την ακαδημαϊκή γνώση σε προϊόντα και υπηρεσίες διαθέσιμα για το ευρύ κοινό. Εταιρίες όπως το WhatsApp (όμιλος Meta) (2023), το Viber (όμιλος Rakuten) (χ.χ.) και το Telegram (χ.χ.) έχουν δημοσιευμένες εκδόσεις στις οποίες επεξηγούν τη μεθοδολογία κρυπτογράφησης (και τους ενδεχόμενους περιορισμούς της εντός της πλατφόρμας), ώστε οι χρήστες να γνωρίζουν σε ποιο βαθμό και με ποια μέσα προστατεύεται το απόρρητο των επικοινωνιών τους.

Σε επίπεδο χάραξης πολιτικής, θεσμικοί φορείς συμβάλλουν στη ρύθμιση του πεδίου, δημοσιεύοντας τις προτεραιότητες τους επί θεμάτων που το αφορούν ή εκδίδοντας μελέτες, κατευθυντήριες οδηγίες και εκθέσεις αναφορικά με αυτό. Πέραν των φορέων νομοθέτησης σε ενωσιακό και εθνικό επίπεδο, δύο βασικοί ευρωπαϊκοί φορείς με επιδραστικό έργο στην προστασία της ιδιωτικότητας είναι ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB). Στην παρούσα εργασία λήφθηκαν υπόψη οι εκθέσεις του ENISA για τα πρωτόκολλα κρυπτογράφησης (2014), την ιδιωτικότητα εκ σχεδιασμού κατά τη χρήση μεγάλων δεδομένων (2015), τις τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs) (2017), την αξιοπιστία και την ασφάλεια στις ηλεκτρονικές επικοινωνίες (2019b) και τις τεχνικές ψευδωνυμοποίησης (2019a). Επίσης, από την πλευρά του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, λήφθηκε ιδιαίτερα υπόψη η Γνώμη 05/2014 (πρώην Ομάδας Εργασίας Άρθρου 29) σχετικά με τις τεχνικές ανωνυμοποίησης (2014).

Ιδιαίτερο ενδιαφέρον υπάρχει και στην απονομή δικαιοσύνης, καθώς δικαστικές αποφάσεις έχουν εξίσου επηρεάσει τον ακαδημαϊκό νομικό διάλογο, αναλύοντας ζητήματα της ιδιωτικότητας και της προστασίας προσωπικών δεδομένων, ορισμένες φορές

ακυρώνοντας ολόκληρα νομοθετήματα. Ιδιαίτερα για τα ζητήματα που εξετάσουμε στην παρούσα ερευνητική προσπάθεια, αξίζει να αναφερθούμε σε δύο: πρώτον, στην υπόθεση «Big Brother Watch και Άλλοι κατά Ηνωμένου Βασιλείου» στο Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΣτΕ), όπου το ΕΔΔΑ κατέληξε πως μέρος του προγράμματος μαζικής παρακολούθησης του Ηνωμένου Βασιλείου ήταν παράνομο και ασύμβατο με την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (*Big Brother Watch and Others v. The United Kingdom*, 2018) και δεύτερον, στην απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης για τις συνδικαθείσες υποθέσεις C-293/12 και C-594/12, η οποία επί της ουσίας ακύρωσε την ευρωπαϊκή Οδηγία 2006/24/ΕΚ[11].

Τέλος, όλα τα παραπάνω παίρνουν τη διάσταση που τους αρμόζει στη δημόσια σφαίρα μέσω δημοσιεύσεων από τον Τύπο, στις οποίες προσφέρεται και αξιολόγηση των εξελίξεων προσθέτοντας ακόμη μια συμβολή στη δημόσια προβολή του τομέα. Μεγάλη σημασία αποκτούν τα ρεπορτάζ της ερευνητικής δημοσιογραφίας, η οποία έχει αποκαλύψει αρκετές περιπτώσεις κατάχρησης εξουσίας από την πλευρά των Αρχών Επιβολής του Νόμου (ΑΕΝ) ή από πολιτικά πρόσωπα, αναγκάζοντας την νομοθετική εξουσία σε νέα νομοθετήματα για την προστασία των πολιτών. Δύο σημαντικές υποθέσεις που αξιοποιήθηκαν (μεταξύ άλλων) στην παρούσα εργασία είναι το πρόγραμμα μαζικών παρακολουθήσεων PRISM της αμερικανικής Εθνικής Υπηρεσίας Ασφαλείας (NSA), το οποίο δημοσιεύτηκε από τον Edward Snowden μέσω του διαδικτυακού τόπου WikiLeaks (‘Edward Snowden’, 2013; *WikiLeaks*, χ.χ.) και η υπόθεση παρακολουθήσεων από την Εθνική Υπηρεσία Πληροφοριών, όπως καλύφθηκε από το ελληνικό δίκτυο ρεπόρτερ ερευνητικής δημοσιογραφίας Reporters United (Λεοντόπουλος & Χονδρόγιαννος, 2023)

2.1 Διατύπωση ερευνητικού κενού και διαμόρφωση ερευνητικής υπόθεσης: είναι δυνατή η ανάπτυξη μεθοδολογίας ώστε να εξασφαλίζεται

[11] *Συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12: Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 8ης Απριλίου 2014 [αιτήσεις του High Court of Ireland, Verfassungsgerichtshof (Ιρλανδία — Αυστρία) για την έκδοση προδικαστικής αποφάσεως] — Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl κ.λπ. (C-594/12) κατά Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Siochána, Ireland and the Attorney General (Ηλεκτρονικές επικοινωνίες — Οδηγία 2006/24/ΕΚ — Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών — Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο της παροχής τέτοιων υπηρεσιών — Κύρος — Άρθρα 7, 8 και 11 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης)*, 2014

η ιδιωτικότητα των χρηστών ενώ ταυτόχρονα θα δύνανται οι διωκτικές αρχές να εντοπίζουν περιπτώσεις υψηλού ρίσκου;

Από τα παραπάνω, φαίνεται πως το ζήτημα της προστασίας της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες έχει εξεταστεί από διάφορες σκοπιές: έχει υπάρξει εκτενέστατη έρευνα πάνω στο πώς μπορούν οι επικοινωνίες των χρηστών να προστατεύονται από κακόβουλους τρίτους (συμπεριλαμβανομένων των διωκτικών Αρχών), ενώ έχουν επίσης ερευνηθεί οι περιπτώσεις κατάχρησης εξουσίας από τις τελευταίες. Έχουν επίσης αναλυθεί περιπτώσεις χρήσης της τεχνητής νοημοσύνης και της αναλυτικής δεδομένων για την επιδίωξη της προληπτικής αστυνόμευσης, κυρίως σε επίπεδο αποτελεσμάτων αλλά όχι απαραίτητα στο στάδιο του σχεδιασμού τους. Στο μέγιστο δυνατό της έρευνας για την παρούσα, βρέθηκε μόνο μια αντίστοιχη πρόταση που αξιοποιεί νευρωνικά δίκτυα βαθιάς μάθησης, η οποία όμως βασίζεται σε στατιστικά δεδομένα, με τις όποιες αποκλείσεις που αυτά μπορεί να έχουν.

Έτσι, βρισκόμαστε μπροστά σε ένα ερευνητικό τέλμα: υπάρχει τρόπος να αξιοποιηθούν πρωτογενείς πηγές δεδομένων για τον εντοπισμό μελλοντικών εγκλημάτων, με τρόπο ακριβέστερο από ό,τι σήμερα και ανεξάρτητο από τα στατιστικά δεδομένα και τους όποιους αστάθμητους παράγοντες; Και αν ναι, υπάρχει η δυνατότητα αυτή η μέθοδος να αξιοποιηθεί με τη λιγότερη δυνατή επέμβαση στην ιδιωτική σφαίρα των πολιτών ώστε να επιτευχθεί η στάθμιση του δικαιώματος της ιδιωτικότητας και του αγαθού της δημόσιας ασφάλειας; Αφού αναλύσουμε το νομικό και τεχνικό πλαίσιο που οριοθετεί το ερευνητικό μας πεδίο, θα καταπιαστούμε με μια δυνητική υπόθεση προς αυτήν την κατεύθυνση μαζί με μια εναλλακτική της. Έπειτα, θα την αξιολογήσουμε υπό το πρίσμα των πιθανών της ρίσκων και των νέων νομοθετικών πρωτοβουλιών της Ε.Ε.

3 Το νομικό πλαίσιο αναφορικά με τα προσωπικά δεδομένα και τις τηλεπικοινωνίες σε ευρωπαϊκό και εθνικό επίπεδο – Βασικά σημεία

Το ζήτημα της προστασίας της ιδιωτικότητας των πολιτών στην Ευρώπη απέκτησε σάρκα και οστά για πρώτη φορά με την υπογραφή της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) το 1950 (Council of Europe, 1950), στο κείμενο της οποίας εκφραζόταν ρητά το δικαίωμα του κάθε ανθρώπου στην ιδιωτική και οικογενειακή

ζωή του, όπως επίσης και στο απόρρητο της αλληλογραφίας του.[12] Φυσικά, πάντα με βάση την αρχή της αναλογικότητας, το δικαίωμα αυτό δεν είναι απόλυτο, κάτι που επίσης αναφέρεται στο ίδιο άρθρο της ΕΣΔΑ.

Καθώς η τεχνολογική εξέλιξη αναπτυσσόταν τις επόμενες δεκαετίες, από τη δεκαετία του 1980, η προβληματική ενός πλαισίου προστασίας των προσωπικών δεδομένων των υποκειμένων από την αυτοματοποιημένη επεξεργασία τους απασχόλησε σοβαρά τον ευρωπαϊκό χώρο. Ήταν, λοιπόν, φυσικό επακόλουθο η υπογραφή της Σύμβασης 108 του Συμβουλίου της Ευρώπης[13]. (Council of Europe, 1981) Σαφώς, η ανάγκη προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας, όπως και των επί μέρους εκφάνσεών της (λ.χ. το οικογενειακό άσυλο) δεν ήταν καινούρια, και εμφανίζεται σε διάφορες διακηρύξεις, συστάσεις και συναφή έγγραφα διεθνών οργανισμών.[14] Η Σύμβαση 108, όμως, αποτέλεσε το πρώτο έγγραφο εστιασμένο στα προσωπικά δεδομένα με νομικά δεσμευτικό χαρακτήρα για τα συμβαλλόμενα μέρη, όπως επίσης έθεσε τις βάσεις για τη δομή και την προσέγγιση της μέλλουσας νομοθετικής διαδικασίας στον τομέα. Στόχος της Σύμβασης 108 ήταν εξ αρχής να εξασφαλίσει πως ο τρόπος επεξεργασίας των δεδομένων των ατόμων γίνεται με τρόπο που σέβεται το δικαίωμα στην ιδιωτικότητα τους (ιδιαίτερα όσον αφορά τα ευαίσθητα προσωπικά δεδομένα), όπως επίσης και η εναρμόνιση του τρόπου χειρισμού και προστασίας των δεδομένων αυτών για διευκολυνθούν οι διασυνοριακές ροές δεδομένων μεταξύ των κρατών-μερών. Η Σύμβαση 108 επικαιροποιήθηκε το 2018 με την υιοθέτηση του διορθωτικού πρωτοκόλλου, με σκοπό την εναρμόνισή της στις νέες τεχνολογικές τάσεις και εξελίξεις. Μέχρι σήμερα, 55 (πενήντα πέντε) κράτη είναι συμβαλλόμενα μέρη, συμπεριλαμβανομένης και της Ουρουγουάης, ως το πρώτο μη ευρωπαϊκό κράτος. (Council of Europe, 2021)

Περιορίζοντας το εδαφικό εύρος στην προστασία της ιδιωτικότητας, δε θα μπορούσαμε να παραλείψουμε τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής

[12] Άρθρο 8: «Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής»

[13] «Για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων.»

[14] Χαρακτηριστικό παράδειγμα αποτελεί το Άρθρο 12 της Οικουμενικής Διακήρυξης Ανθρωπίνων Δικαιωμάτων του Οργανισμού Ηνωμένων Εθνών, το οποίο ορίζει πως «Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.» (Περιφερειακό Κέντρο Πληροφόρησης του ΟΗΕ, 2019)

Ένωσης[15], ο οποίος τέθηκε σε ισχύ το 2009 με την υπογραφή της Συνθήκης της Λισαβόνας. Στο άρθρο 8, ο Χάρτης προβλέπει το δικαίωμα των ατόμων στην προστασία των προσωπικών τους δεδομένων, όπως επίσης ορίζει και τον έλεγχο της εφαρμογής των κανόνων που διέπουν την επεξεργασία προσωπικών πληροφοριών από ανεξάρτητη αρχή. Το εν λόγω άρθρο βασίστηκε στις διατυπώσεις της Συνθήκης για την Ευρωπαϊκή Ένωση, και πιο συγκεκριμένα στο άρθρο 286 (το οποίο αντικαταστάθηκε από το Άρθρο 16 ΣΛΕΕ[16]), ενώ η (πλέον καταργηθείσα) Οδηγία 95/46/ΕΚ και το άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου αποτέλεσαν επίσης πηγές του.(FRA, 2015)

Η ευρωπαϊκή ολοκλήρωση μέσω της διεύρυνσης και κυρίως της εμβάθυνσης, και η παράλληλη τεχνολογική εξέλιξη, ανέδειξαν την ανάγκη για ένα ομοιόμορφο κανονιστικό πλαίσιο στον τομέα της προστασίας και διακίνησης προσωπικών δεδομένων στην Ένωση. Έτσι, η μέχρι προσφάτως ισχύουσα Οδηγία 95/46/ΕΚ αντικαθίσταται το 2016 από τον Γενικό Κανονισμό Προστασίας Δεδομένων - ΓΚΠΔ, με σκοπό την αποτελεσματικότερη και εναρμονισμένη εφαρμογή των κανόνων δικαίου στην ενιαία αγορά.[17] Παρόλο που αποτέλεσε τη βάση του ΓΚΠΔ, η Οδηγία 95/45/ΕΚ κρίθηκε ως ανελαστική και ανεπαρκής απέναντι στις νέες τεχνολογικές δυνατότητες για την επεξεργασία δεδομένων.

Τηρώντας την αρχή πως ο ειδικός κανόνας υπερισχύει του γενικού («lex specialis derogat legi generali»), το 2002 τίθεται σε εφαρμογή η Οδηγία 2002/58/ΕΚ (ή αλλιώς ePrivacy Directive) η οποία εξειδίκευε την τότε «γενικότερη» οδηγία στην προβληματική της επεξεργασίας των προσωπικών δεδομένων και της προστασίας τους στο πλαίσιο των ηλεκτρονικών επικοινωνιών.[18] Η εν λόγω Οδηγία υιοθετήθηκε στην προσπάθεια

[15] Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, 2016

[16] Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης - ΜΕΡΟΣ ΠΡΩΤΟ - ΟΙ ΑΡΧΕΣ - ΤΙΤΛΟΣ ΙΙ - ΔΙΑΤΑΞΕΙΣ ΓΕΝΙΚΗΣ ΕΦΑΡΜΟΓΗΣ - Άρθρο 16 (πρώην άρθρο 286 της ΣΕΚ), 2016, διαθέσιμο στο σύνδεσμο http://data.europa.eu/eli/treaty/tfeu_2016/art_16/oj [Πρόσβαση 10/12/2023]

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance, 2016)

[18] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, 2002)

εξειδίκευσης γενικότερων προβλέψεων, μιας και τη δεκαετία του 2000 οι ηλεκτρονικές επικοινωνίες εξαπλώθηκαν με ραγδαίο ρυθμό, ενώ νέες τεχνολογίες (λ.χ. τα cookies) έκαναν την εμφάνισή τους. Το νομοθέτημα επικαιροποιήθηκε το 2009, όπου πήρε τη σημερινή του μορφή[19]. Συνεχίζοντας την τάση της μετατροπής υφιστάμενων Οδηγιών σε Κανονισμούς, η Οδηγία ePrivacy βρίσκεται τα τελευταία χρόνια σε διαδικασία αναθεώρησης και μετατροπής της σε Κανονισμό, με αιτιολογικό αντίστοιχο της δημιουργίας του Γενικού Κανονισμού Προστασίας Δεδομένων, όμως παρόλες τις καινοτομίες της, η πρωτοβουλία αυτή δεν έχει ολοκληρωθεί μέχρι στιγμής.

Τη στιγμή που γράφονται αυτές οι γραμμές, η Ευρωπαϊκή Ένωση έχει στρέψει το βλέμμα της στον τομέα της τεχνητής νοημοσύνης, και σε μια προσπάθεια ρύθμισης των αλγοριθμικών συστημάτων βρίσκεται υπό ανάπτυξη το κείμενο για έναν ευρωπαϊκό κανονισμό ΤΝ (EU AI Act), σκοπός του οποίου θα είναι η ταξινόμηση των αλγορίθμων σε κατηγορίες ρίσκου (και αντίστοιχων περιορισμών) ανάλογα με το σκοπό που επιτελούν.

Αντίστοιχα νομοθετήματα που αφορούν την προστασία προσωπικών δεδομένων σε διάφορους τομείς έχουν επίσης τεθεί σε ισχύ, είτε με τη μορφή Οδηγιών είτε Κανονισμών, ενώ όπου απαιτούνταν, αυτά ενσωματώθηκαν και στο ελληνικό δίκαιο. Στις επόμενες ενότητες γίνεται μια προσπάθεια στοιχειοθέτησης αυτών των νομοθετημάτων ως προς τον σκοπό τους, τις συνθήκες που οδήγησαν στην υιοθέτησή τους αλλά και τις βασικές προβλέψεις τους.

3.1 Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679

Βασικά στοιχεία και εφαρμογή

Ο Γενικός Κανονισμός Προστασίας Δεδομένων[20] (εφεξής ΓΚΠΔ ή Γενικός Κανονισμός ή Κανονισμός) είναι το νομοθετικό εργαλείο που ρυθμίζει ζητήματα που

[19] Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 , για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), 2009

[20] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα

αφορούν την επεξεργασία δεδομένων φυσικών προσώπων που βρίσκονται στην ΕΕ και τον ΕΟΧ, με ή χωρίς αυτοματοποιημένο τρόπο. Τέθηκε σε εφαρμογή την 25η Μαΐου 2016 και αντικατέστησε την Οδηγία 45/96/ΕΚ, επιτυγχάνοντας ένα ενιαίο καθεστώς νομικής προστασίας των δεδομένων προσωπικού χαρακτήρα των υποκειμένων εντός της Ένωσης. Η εφαρμογή του ΓΚΠΔ προσδιορίζεται μέσω δύο βασικών κριτηρίων – πεδίων: το ουσιαστικό και το εδαφικό.

Όσον αφορά το πρώτο[21], ο Κανονισμός εφαρμόζεται σε περιπτώσεις που τα προσωπικά δεδομένα «[…] περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης» και η επεξεργασία τους γίνεται είτε μη αυτοματοποιημένα, είτε μερικώς ή ολικώς αυτοματοποιημένα. Αξίζει να παρατηρήσουμε πως σε σχέση με την αντικατασταθείσα Οδηγία 95/46/ΕΚ, ο Κανονισμός υιοθετεί μια πιο συμπεριληπτική και τεχνολογικά ουδέτερη στάση, αναφερόμενος σε «σύστημα αρχειοθέτησης» παντός τύπου, μη ορίζοντας αν αυτό είναι αποκλειστικά έγχαρτο. Ξεκαθαρίζει πως στο πεδίο εφαρμογής του δεν περιλαμβάνονται οικιακές δραστηριότητες φυσικών προσώπων (λ.χ. οι φωτογραφίες που μπορεί να συλλέγει κάποιο άτομο για το οικογενειακό του άλμπουμ), δραστηριότητες εκτός του πεδίου εφαρμογής του ενωσιακού δικαίου, ενώ παραπέμπει σε άλλες νομοθετικές πράξεις όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα από θεσμικούς φορείς της Ευρωπαϊκής Ένωσης[22] και αυτή που λαμβάνει χώρα στο πλαίσιο λειτουργίας των Αρχών «[…] για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων […]».

Πέραν του ουσιαστικού πεδίου εφαρμογής, το οποίο αφορούσε τη φύση των πράξεων που ρυθμίζονται από τον Κανονισμό, υπάρχει και το αντίστοιχο εδαφικό κριτήριο[23], το οποίο περιγράφει τα φυσικά και νομικά πρόσωπα που υπόκεινται στις

και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ, 2016)

[21] Άρθρο 2 ΓΚΠΔ.

[22] Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ., 2018)

[23] Άρθρο 3 ΓΚΠΔ.

διατάξεις του με βάση την περιοχή δραστηριοποίησής τους. Έτσι, είναι υποχρεωμένοι σε συμμόρφωση με τον Γενικό Κανονισμό υπεύθυνοι και εκτελούντες επεξεργασία που:

- Είτε είναι εγκατεστημένοι στην Ένωση,
- Είτε δεν είναι εγκατεστημένοι στην Ένωση
    - αλλά προσφέρουν αγαθά και υπηρεσίες σε άτομα που βρίσκονται στην Ένωση,
    - ή παρακολουθούν συμπεριφορά ατόμων που λαμβάνει χώρα εντός της Ένωσης,
    - ή βρίσκονται σε τόπο που εφαρμόζεται το δίκαιο κάποιου κράτους – μέλους της ΕΕ.

Με τη νέα διατύπωση του εδαφικού κριτηρίου, επιτυγχάνεται μια ευρύτερη και πιο ξεκάθαρη περιγραφή των οντοτήτων που υπόκεινται στον Κανονισμό, με την παράλληλη κατάργηση της υποχρέωσης των υπεύθυνων επεξεργασίας στον ορισμό αντιπροσώπου σε κάθε κράτος – μέλος από το οποίο διέρχονται προσωπικά δεδομένα.

Διάρθρωση του ΓΚΠΔ και βασικά σημεία

Ο Κανονισμός αποτελείται από 173 (εκατόν εβδομήντα τρεις) αιτιολογικές σκέψεις, οι οποίες καταλήγουν σε 99 (ενενήντα εννέα) άρθρα, τα οποία με τη σειρά τους ταξινομούνται σε 11 (έντεκα) κεφάλαια. Για την πληρέστερη κατανόηση του νομοθετήματος, στις επόμενες παραγράφους θα δούμε αναλυτικότερα τη θεματολογία των κεφαλαίων, καθώς και τα βασικά σημεία/προβλέψεις/άρθρα που περιλαμβάνονται σε αυτά:

Αρχικά, στα **πρώτα** 4 (τέσσερα) άρθρα του Κανονισμού περιγράφονται οι στόχοι του, τα πεδία εφαρμογής που αναλύθηκαν πιο πάνω καθώς και ορισμοί που θα χρησιμοποιηθούν παρακάτω. Στο άρθρο 4 ορίζονται -μεταξύ άλλων- έννοιες όπως «δεδομένα προσωπικού χαρακτήρα», «επεξεργασία» καθώς και οι ιδιότητες του «υποκειμένου δεδομένων», του «υπεύθυνου» και του «εκτελούντος» την επεξεργασία.

Το **δεύτερο** κεφάλαιο του Κανονισμού (άρθρα 5-11) περιγράφει τις συνθήκες υπό τις οποίες η επεξεργασία προσωπικών δεδομένων θεωρείται νόμιμη. Ο σεβασμός των βασικών αρχών επεξεργασίας, η εύρεση νομικής βάσης που να την αιτιολογεί, καθώς και οι επιπλέον προϋποθέσεις εφόσον αυτή βασίζεται στη συγκατάθεση, αναλύονται σε αυτό το κεφάλαιο. Ιδιαίτερο ενδιαφέρον παρουσιάζει το άρθρο 9, το οποίο ορίζει τα ευαίσθητα

προσωπικά δεδομένα και το άρθρο 10 που επιβάλλει τους όρους επεξεργασίας δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα.

Στο **τρίτο** κεφάλαιο (άρθρα 12-23) αναφέρονται οι ελάχιστες προϋποθέσεις για την επίτευξη επαρκούς ενημέρωσης προς το υποκείμενο δεδομένων, και παράλληλα απαριθμούνται τα δικαιώματα των υποκειμένων (άρθρα 15 – 22) που τους δίνουν τον έλεγχο πάνω στις πληροφορίες τους, καθώς και οι προϋποθέσεις περιορισμού τους (άρθρο 23).

Ποιος όμως είναι αυτός που επεξεργάζεται τα προσωπικά δεδομένα κάθε φορά; Τι συμβαίνει όταν η επεξεργασία δεν γίνεται για σκοπούς που έχει θέσει ο ίδιος αλλά στο όνομα άλλου; Και ποια η σχέση και οι υποχρεώσεις όσων επεξεργάζονται προσωπικά δεδομένα που απορρέουν από αυτή τη δραστηριότητα; Αυτά τα ζητήματα αποσαφηνίζονται στο **τέταρτο** κεφάλαιο (άρθρα 24-43) του κειμένου, όπου αναλύονται οι έννοιες του υπεύθυνου και του εκτελούντος επεξεργασία.

Αναγνωρίζοντας πως οι ευρωπαίοι κάτοικοι μοιράζονται τα δεδομένα τους όχι μόνο με ευρωπαϊκές επιχειρήσεις, ειδικά μέσω του διαδικτύου, το **πέμπτο** κεφάλαιο του ΓΚΠΔ (άρθρα 44-50) πραγματεύεται τις διαβιβάσεις πληροφοριών ατόμων που βρίσκονται στην Ένωση προς τρίτες χώρες και διεθνείς οργανισμούς. Στόχος των προβλέψεων είναι η παροχή νομικών και κατ' επέκταση τεχνικών εγγυήσεων, ώστε τα υποκείμενα να απολαμβάνουν τον ίδιο έλεγχο και το ίδιο επίπεδο προστασίας των δεδομένων τους στην τρίτη χώρα, όπως και εντός της ΕΕ.

Η λειτουργία και εφαρμογή όλων των παραπάνω θα πρέπει να ελέγχεται και από μια Ανεξάρτητη Εποπτική Αρχή (εφεξής Αρχή) στα κράτη – μέλη της Ένωσης. Έτσι, το **έκτο** κεφάλαιο (άρθρα 51-59) επανιδρύει το θεσμό των εθνικών Εποπτικών Αρχών, ξεκαθαρίζει το ανεξάρτητο καθεστώς τους, και παράλληλα περιγράφει τις αρμοδιότητες που αυτές έχουν είτε εντός της επικράτειας τους είτε σε περίπτωση που λειτουργούν ως Επικεφαλής Εποπτικές Αρχές στο πλαίσιο συνεργασίας με ομόλογους φορείς άλλων κρατών – μελών.

Στον τομέα της συνεργασίας μεταξύ των Αρχών, της συνεκτικής ερμηνείας του Κανονισμού αλλά και της επίλυσης διαφορών που μπορεί να προκύψουν μεταξύ Αρχών κρατών-μελών, ο ΓΚΠΔ περιλαμβάνει προβλέψεις που αφορούν λ.χ. την αμοιβαία συνδρομή και τις κοινές επιχειρήσεις των Αρχών στο **έβδομο** κεφάλαιο (άρθρα 60-76). Συν τοις άλλοις, στο ίδιο κεφάλαιο ιδρύεται το Ευρωπαϊκό Συμβούλιο Προστασίας

Δεδομένων[24] (εφεξής Συμβούλιο Προστασίας Δεδομένων ή ΕΣΠΔ ή EDPB) και περιγράφεται ο «μηχανισμός συνεκτικότητας», η διαδικασία κατά την οποία το ΕΣΠΔ εκδίδει γνώμες μη δεσμευτικού ή δεσμευτικού χαρακτήρα και φροντίζει για την ομοιόμορφη εφαρμογή του Κανονισμού στα κράτη-μέλη.

Το δικαίωμα αναφοράς στις Αρχές και η δικαστική προσφυγή των ατόμων είναι μέρος του νομικού πολιτισμού της Ευρωπαϊκής Ένωσης, και ο Κανονισμός δε θα μπορούσε παρά να συμπεριλάβει προβλέψεις επί του θέματος στο **όγδοο** κεφάλαιο (άρθρα 77-84). Σε αυτό γίνεται ρητή αναφορά στα δικαιώματα του υποκειμένου για καταγγελία προς την εποπτική Αρχή, για δικαστική προσφυγή κατά υπευθύνου/εκτελούντος επεξεργασία(ς), αλλά και για τη δυνατότητα εκπροσώπησής του από μη κερδοσκοπικούς φορείς με σχετική δραστηριότητα.

Το **ένατο** κεφάλαιο (άρθρα 85-91) θέτει δικλείδες ασφαλείας όσον αφορά ειδικές πράξεις επεξεργασίας που σχετίζονται με τη στάθμιση δικαιωμάτων στο πλαίσιο της ελευθερίας της έκφρασης, της πρόσβασης των πολιτών σε επίσημα έγγραφα, των εργασιακών σχέσεων, της αρχειοθέτησης για σκοπούς επιστημονικής έρευνας κ.ά, ώστε να προληφθεί κατά το δυνατόν παρανόηση του πνεύματος του νόμου και κατάχρησή του.

Στο **δέκατο** κεφάλαιο (άρθρα 92-93) δίνονται διευκρινίσεις αναφορικά με διάφορες διαδικασίες και πρωτοβουλίες για τις οποίες έχει εξουσιοδοτηθεί η Ευρωπαϊκή Επιτροπή στο κείμενο του Κανονισμού, ενώ το ενδέκατο και τελευταίο κεφάλαιο (άρθρα 94-99) περιλαμβάνει κάποιες τελικές διατάξεις που αφορούν τη σχέση του Γενικού Κανονισμού Προστασίας Δεδομένων με παλαιότερη ή/και άλλη σχετιζόμενη νομοθεσία.

Παραπάνω περιεγράφηκαν τα κύρια χαρακτηριστικά και τα βασικά σημεία του Γενικού Κανονισμού Προστασίας Δεδομένων, ο οποίος έχει εφαρμογή στο σύνολο των φυσικών και νομικών προσώπων που πληρούν το ουσιαστικό και το εδαφικό πεδίο εφαρμογής. Μια από τις περιπτώσεις που αποτελεί εξαίρεση και δεν καλύπτεται από αυτά, είναι η επεξεργασία προσωπικών δεδομένων από «τα θεσμικά όργανα, τους φορείς τις υπηρεσίες και τους οργανισμούς της Ευρωπαϊκής Ένωσης»[25]. Οι εν λόγω φορείς δεσμεύονται από τον Κανονισμό (ΕΕ) 2018/1725[26], ο οποίος τέθηκε σε ισχύ –

[24] Ουσιαστικά πρόκειται για αναβάθμιση μέσω νομικής μορφής της πρώην άτυπης ομάδας εργασίας του Άρθρου 29 της Οδηγίας 95/46/ΕΚ. (Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, 2018)

[25] Άρθρο 2 παρ. 3 ΓΚΠΔ

[26] Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού

αναθεωρώντας τον αρχικό Κανονισμό (ΕΚ) 45/2001[27] - για αυτόν ακριβώς το σκοπό και παρουσιάζεται στην επόμενη ενότητα.

3.1.1 Ο Κανονισμός Προστασίας Δεδομένων για τα ευρωπαϊκά θεσμικά όργανα (ΕΕ) 2018/1725

Δύο χρόνια μετά την έναρξη ισχύος του Γενικού Κανονισμού Προστασίας Δεδομένων, δημοσιεύτηκε και ο Κανονισμός Προστασίας Δεδομένων για τα ευρωπαϊκά θεσμικά όργανα, φορείς και υπηρεσίες (ΕΕ) 2018/1725 (εφεξής EUDPR ή ΚΠΔΕΕ), ο οποίος αυστηροποιεί το πλαίσιο προστασίας των προσωπικών δεδομένων στις δραστηριότητες των θεσμικών οργάνων, καταργεί τον προηγούμενο Κανονισμό (ΕΚ) 45/2001 και την απόφαση 1247/2002/ΕΚ σχετικά με τα καθήκοντα του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (εφεξής Επόπτη ή ΕΕΠΔ ή EDPS), εναρμονίζει τους δύο κανονισμούς προστασίας δεδομένων (ΓΚΠΔ και ΚΠΔΕΕ), εναρμονίζεται με την Οδηγία για την επιβολή του Νόμου (ΕΕ) 2016/680 (θα αναλυθεί παρακάτω), και θέτει το πλαίσιο επεξεργασίας των «επιχειρησιακών δεδομένων προσωπικού χαρακτήρα» (ήτοι προσωπικά δεδομένα στα οποίαν γίνεται επεξεργασία στο πλαίσιο εκτέλεσης καθηκόντων για την επιβολή του Νόμου).

Ως επί το πλείστον, ο ΚΠΔΕΕ ακολουθεί τις ίδιες αρχές επεξεργασίας, προσφέρει τα ίδια δικαιώματα στα υποκείμενα και επιβάλλει τις ίδιες υποχρεώσεις στους Υπεύθυνους και Εκτελούντες επεξεργασία(ς) με τον ΓΚΠΔ. (Ευρωπαϊκή Ένωση, 2018) Λόγω του ιδιαίτερου και πιο στοχευμένου πεδίου του, όμως, προχωράει στις εξής καινοτομίες[28], με στόχο οι πολίτες να απολαμβάνουν κατά την επικοινωνία τους με τα ευρωπαϊκά θεσμικά όργανα το ίδιο επίπεδο προστασίας και δικαιωμάτων όπως με τον ΓΚΠΔ:

- Όπως συμβαίνει και στο Γενικό Κανονισμό, ο ΚΠΔΕΕ θέτει πολύ ξεκάθαρα την αρχή της λογοδοσίας και της απόδειξης συμμόρφωσης από

χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ., 2018)

[27] Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών, 2000

[28] *Deloitte's View on the Implementation of Regulation (EU) 2018/1725 - GDPR for European Union Institutions | Deloitte Belgium | Risk Services | cyber@EU*, 2019

πλευράς των Υπεύθυνων και των Εκτελούντων επεξεργασία(ς). Στόχος του δεν είναι το αίσθημα λογοδοσίας να βασίζεται μόνο λόγω φόβου κυρώσεων, αλλά η ουσιαστική δημιουργία κουλτούρας εντός του φορέα, η οποία θα υποστηρίζεται από τα κατάλληλα τεχνικά και οργανωτικά μέτρα.

- Παρόμοια με τον ΓΚΠΔ, έτσι και μέσω του Επόπτη εκφράζεται πως δεν αρκεί μόνο να ακολουθείται ο νόμος, αλλά θα πρέπει να είναι δυνατή και η επίδειξη αυτής της συμμόρφωσης. Έτσι, πρέπει να υπάρχει από την πλευρά των ευρωπαϊκών φορέων η ανάλογη τεκμηρίωση μέσω αρχείου δραστηριοτήτων επεξεργασίας σε ένα κεντρικό, δημόσια προσβάσιμο μητρώο.[29] Το μέτρο αυτό έρχεται ως συνέχεια του προηγούμενου μηχανισμού ειδοποίησης του Υπεύθυνου Προστασίας Δεδομένων που προβλεπόταν στον Κανονισμό (ΕΚ) 45/2001, ενώ η νέα του μορφή έρχεται ως συνέπεια της γενικότερης προσέγγισης του ΓΚΠΔ και του ΚΠΔΕΕ για αυτορρύθμιση των Υπευθύνων και των Εκτελούντων επεξεργασία(ς).
- Μια ακόμη βασική διαφορά με τον αντικατασταθέντα κανονισμό είναι πως ο νέος ΚΠΔΕΕ προωθεί τη συλλογιστική του ρίσκου, εκφράζοντας πως θα πρέπει να λαμβάνεται πάντα υπόψη ο αντίκτυπος που προκαλεί η εκάστοτε επεξεργασία στα υποκείμενα. Για παράδειγμα, ο Υπεύθυνος Επεξεργασίας θα πρέπει να λάβει υπόψη του παράγοντες όπως τη φύση, το πεδίο, το σκοπό και την έκταση της επεξεργασίας ώστε να προσδιορίσει αν μπορεί αυτή να προσβάλει τα δικαιώματα και τις ελευθερίες των ατόμων.
- Μια νέα υποχρέωση που εισάγεται για τους ευρωπαϊκούς φορείς είναι η ενημέρωση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σε περίπτωση διαρροής δεδομένων που μπορεί να οδηγήσει σε υψηλό ρίσκο για τα υποκείμενα δεδομένων. Ο Υπεύθυνος επεξεργασίας είναι υποχρεωμένος να προχωρήσει σε γνωστοποίηση του περιστατικού το αργότερο εντός 72 ωρών από τη στιγμή που θα λάβει γνώση της διαρροής.
- Τέλος, αξίζει να σημειωθεί πως ο ΚΠΔΕΕ αφιερώνει ένα ολόκληρο κεφάλαιο απαριθμώντας συγκεκριμένους κανόνες για τους ευρωπαϊκούς φορείς που έχουν στην κατοχή τους επιχειρησιακά προσωπικά δεδομένα στο πλαίσιο επιβολής του νόμου. Όσον αφορά την Ευρωπόλ και την

[29] Άρθρο 31 ΚΠΔΕΕ

Ευρωπαϊκή Εισαγγελία, ο ΚΠΔΕΕ βρίσκει εφαρμογή μόνο στα προσωπικά δεδομένα που υπόκεινται σε επεξεργασία για διοικητικούς λόγους και όχι στο πλαίσιο επιχειρήσεων και υποθέσεων, καθώς ο τρόπος χειρισμού αυτών των δεδομένων περιγράφεται στις διατάξεις της νομοθεσίας που ιδρύει αυτούς τους φορείς.

Βέβαια, εφόσον αναφερθήκαμε στους φορείς επιβολής του Νόμου, έχει ενδιαφέρον να δούμε πώς και εκείνοι οφείλουν να χειρίζονται τα προσωπικά δεδομένα στο πλαίσιο της αρμοδιότητάς τους. Στην επόμενη ενότητα εστιάζουμε στην Οδηγία (ΕΕ) 2016/680, η οποία αφορά την προστασία δεδομένων προσωπικού χαρακτήρα από τις διωκτικές και δικαστικές Αρχές.

3.2 Η Οδηγία για την Προστασία Προσωπικών Δεδομένων από διωκτικές και δικαστικές Αρχές (ΕΕ) 2016/680

Η Οδηγία (ΕΕ) 2016/680[30] (εφεξής Οδηγία ή/και LED ή/και Οδηγία επιβολής του Νόμου) έρχεται ως το τρίτο νομοθετικό κείμενο που επικαιροποιεί το ενωσιακό πλαίσιο προστασίας προσωπικών δεδομένων – το πρώτο είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) και το δεύτερο ο ΚΠΔΕΕ. Η ισχύς της ξεκίνησε την 5η Μαΐου 2016, με τα κράτη μέλη να πρέπει να την ενσωματώσουν στο εθνικό τους δίκαιο μέσα σε δύο χρόνια.

Η εν λόγω Οδηγία ως ειδικός νόμος στοχεύει στην εναρμόνιση του τρόπου χειρισμού των προσωπικών δεδομένων των εμπλεκόμενων σε ποινικές διαδικασίες στα πρότυπα του Γενικού Κανονισμού Προστασίας Δεδομένων, λαμβάνοντας υπόψη την ιδιαίτερη φύση του αντικειμένου και των πράξεων επεξεργασίας που αυτό περιλαμβάνει. Επίσης, θέτει ένα συγκεκριμένο και οριοθετημένο πλαίσιο πρακτικών ώστε να καθιστά εφικτή τη συνεργασία μεταξύ των κρατών – μελών στον τομέα της ποινικής δικαιοσύνης για την πρόληψη απειλών όπως η τρομοκρατία, ενισχύοντας την εμπιστοσύνη μεταξύ τους στο χειρισμό των προσωπικών δεδομένων, μιας και οι πρακτικές εφαρμόζονται ομοιόμορφα στην Ευρωπαϊκή Ένωση και τη ζώνη Σένγκεν.

[30] Πλήρης ονομασία: «Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου»

Όσον αφορά τη δομή της, είναι παρόμοια με αυτή του ΓΚΠΔ, με τα βασικά σημεία και τις ιδιαιτερότητές της να περιγράφονται παρακάτω:

- Σε αντίθεση με τον ΓΚΠΔ, ως υποκείμενα δεδομένων νοούνται τα άτομα που εμπλέκονται σε κάποια ποινική διαδικασία, είτε ως καταδικασμένοι, ως κατηγορούμενοι, ως ύποπτοι, ως θύματα, ως μάρτυρες, είτε ως εμπειρογνώμονες, με την οδηγία να ορίζει πως πρέπει να λαμβάνεται υπόψη η ιδιότητα του ατόμου κατά την επεξεργασία των δεδομένων του.[31]
- Προβλέπονται σαφείς και συγκεκριμένες αρχές επεξεργασίας των προσωπικών δεδομένων των υποκειμένων από τους υπεύθυνους και τους εκτελούντες επεξεργασία(ς), συμπεριλαμβανομένης της νομιμότητας αυτής και των σκοπών της, της αναλογικότητας των δεδομένων που συλλέγονται ως προς τον σκοπό, της επικαιροποίησης και ακρίβειας των δεδομένων κατά την επεξεργασία τους, της διατήρησής τους μόνο για το διάστημα που απαιτούν οι διαδικασίες που οδήγησαν στην επεξεργασία, καθώς και της επαρκούς προστασίας τους μέσω τεχνικών και οργανωτικών μέτρων, ιδιαίτερα μέσω κρυπτογράφησης και ψευδωνυμοποίησης.
- Ιδιαίτερη μνεία γίνεται στις επιπλέον εγγυήσεις που πρέπει να εφαρμόζονται όταν προσωπικά δεδομένα υποβάλλονται σε αυτοματοποιημένη επεξεργασία δεδομένων[32], ώστε να παρεμποδιστεί η μη εξουσιοδοτημένη πρόσβαση σε αυτά και η αλλοίωσή τους από κακόβουλους τρίτους – ορισμένες από αυτές τις εγγυήσεις περιλαμβάνουν την απαγόρευση μη εξουσιοδοτημένης πρόσβασης με τεχνικό τρόπο και την καταγραφή ιστορικού επεξεργασίας μέσω των αρχείων συστήματος (log files).
- Όπως προβλέπεται στον Γενικό Κανονισμό Προστασίας Δεδομένων, έτσι και εδώ τα υποκείμενα απολαμβάνουν δικαιώματα αναφορικά με τις πληροφορίες τους, με το δικαίωμα στην πλήρη ενημέρωση να έχει δεσπόζουσα θέση στις υποχρεώσεις των Αρχών. Επίσης, σταθμίζοντας το δημόσιο συμφέρον και τα συμφέροντα του υποκειμένου, υπό προϋποθέσεις προβλέπεται η παροχή του δικαιώματος διόρθωσης, διαγραφής, και περιορισμού της επεξεργασίας.

Στην Ελλάδα, ο Γενικός Κανονισμός Προστασίας Δεδομένων (κυρίως τα στοιχεία που αφήνουν περιθώριο ελιγμού στα κράτη-μέλη) και η Οδηγία LED ενσωματώθηκαν στο

[31] Άρθρο 6 της Οδηγίας.

[32] Άρθρο 29 της Οδηγίας.

εθνικό μας δίκαιο μέσω του Ν. 4624/2019. Ο νόμος αυτός αναθεωρήθηκε με τον Ν. 5002/2022[33], ενώ ορισμένα σημεία που είχαν να κάνουν με την εθνική εποπτική Αρχή επικαιροποιήθηκαν σε «λοιπές και επείγουσες» διατάξεις του Ν.5043/2023.[34]

3.3 Ο Νόμος 4624/2019 και οι τροποποιήσεις του

Παρόλο που οι ευρωπαϊκοί κανονισμοί είναι άμεσα εφαρμοστέοι στα κράτη – μέλη και δε χρειάζεται νομοθέτηση σε εθνικό επίπεδο, εντούτοις ο Γενικός Κανονισμός Προστασίας Δεδομένων διατηρεί κάποια στοιχεία οδηγίας ή αλλιώς «ρήτρες ευελιξίας» (Γριβοκωστόπουλος, 2021), επιτρέποντας την εξειδίκευση ορισμένων ζητημάτων με βάση τις δυνατότητες, την κουλτούρα και την προσέγγιση που επιθυμεί το εκάστοτε κράτος – μέλος.

Έτσι, μετά από αλλεπάλληλες καθυστερήσεις και χειρισμούς που θα μπορούσαν να εγείρουν λιγότερες απορίες[35] το 2019 ψηφίζεται στη χώρα μας ο Νόμος 4624/2019 (εφεξής εθνική νομοθεσία), ο οποίος έχει διττή χρησιμότητα: από τη μία, εξειδικεύει ζητήματα που ο ΓΚΠΔ αφήνει στην ευχέρεια της κάθε έννομης τάξης και από την άλλη, ενσωματώνει στο ελληνικό δίκαιο την Οδηγία 690/2016. Παρακάτω θα αναφέρουμε τα σημεία όπου η εθνική νομοθεσία εξειδικεύει τον Κανονισμό, καθώς και τις βασικές της προβλέψεις όσον αφορά την ενσωμάτωση της Οδηγίας LED.

Η εθνική νομοθεσία, στον τομέα της εξειδίκευσης των γενικών κανόνων προστασίας δεδομένων, προσφέρει από τη μια πλευρά καινοτομίες, και από την άλλη αστοχίες που οφείλονται κυρίως στην επιρροή του γερμανικού δικαίου στο σχετικό νομοσχέδιο. Αυτό φαίνεται από την αρχή του Νόμου, μιας και στις προβλέψεις του κάνει διάκριση μεταξύ ιδιωτικών και δημόσιων φορέων. Παρόλο που η απόφαση αυτή πλέει εντός των ορίων που έχει θέσει ο ΓΚΠΔ και η προσέγγιση είναι εμπνευσμένη από ένα δίκαιο αρκετά ωριμότερο στον τομέα των προσωπικών δεδομένων, εντούτοις εγείρονται (και δικαίως) ερωτήματα σχετικά με την αμερόληπτη μεταχείριση των υπευθύνων

[33] (Ν. 5002/2022: Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών., 2022)

[34] Ν. 5043/2023: Ρυθμίσεις σχετικά με τους Οργανισμούς Τοπικής Αυτοδιοίκησης α’ και β’ βαθμού - Διατάξεις για την ευζωία των ζώων συντροφιάς - Διατάξεις για το ανθρώπινο δυναμικό του δημοσίου τομέα - Λοιπές ρυθμίσεις του Υπουργείου Εσωτερικών και άλλες επείγουσες διατάξεις, 2023

[35] Γριβοκωστόπουλος, Ι. (2021). Κριτική ανάλυση του Ν. 4624/2019. Επιθεώρηση Δικαίου Πληροφορικής, 2(1), Article 1. https://doi.org/10.26262/infolawj.v2i1.8231, σελίδα 3.

επεξεργασίας από τον νόμο, ανεξάρτητα από το νομικό καθεστώς τους. Δυστυχώς, στην εθνική νομοθεσία, οι δημόσιοι φορείς αντιμετωπίζονται ελαστικότερα από τους ιδιωτικούς όσον αφορά τις υποχρεώσεις και την επιβολή προστίμων.

Ακόμη ένα ζήτημα που διαφοροποιεί την εθνική νομοθεσία από τον ΓΚΠΔ και απασχολεί το νομικό κόσμο, είναι το ζήτημα της εποπτείας πράξεων επεξεργασίας που αφορούν ζητήματα "εθνικής ασφάλειας"[36]. Τέτοιου είδους πράξεις επεξεργασίας που περιλαμβάνουν διαβαθμισμένες πληροφορίες δεν εμπίπτουν (συνειδητά από το νομοθέτη) στην δικαιοδοσία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής Εποπτική Αρχή ή ΑΠΔΠΧ). Η προηγούμενη εθνική νομοθεσία δεν περιλάμβανε παρόμοια ρύθμιση, οπότε το νέο καθεστώς θέτει πιο ξεκάθαρα όρια στις ευθύνες και τις αρμοδιότητες της Εποπτικής Αρχής. Ταυτόχρονα, όμως, δημιουργεί ένα νομικό κενό το οποίο όφειλε να διαχειριστεί μέσω της σύστασης αντίστοιχου σώματος εποπτείας. Αυτή η παράλειψη στην εθνική νομοθεσία αφήνει διάτρητο το νομικό μας πλαίσιο στον τομέα, καθώς νομοθετήματα που βρίσκονται ψηλά στην ιεραρχία δικαίου εγγυώνται την εποπτεία της τήρησης των κανόνων προστασίας προσωπικών δεδομένων χωρίς συγκεκριμένες εξαιρέσεις[37].

Παρόλο που οι πράξεις επεξεργασίας δεδομένων από τις αρχές επιβολής του Νόμου δεν εμπίπτουν στον ΓΚΠΔ (εκτός από αυτές που γίνονται για διοικητικούς σκοπούς), ας μη λησμονούμε ότι ο Ν. 4624/2019 ενσωματώνει και την Οδηγία LED, που σημαίνει ότι ως νομοθετικό εργαλείο περιλαμβάνει στους κόλπους του και αυτές τις περιπτώσεις. Και, συνδέοντας την περίπτωση των ζητημάτων «εθνικής ασφάλειας» με αυτή, αξίζει να σημειώσουμε πως εκτός της αρμοδιότητας της ΑΠΔΠΧ βρίσκονται και οι πράξεις επεξεργασίας προσωπικών δεδομένων που γίνονται από τα δικαστήρια και τις εισαγγελικές αρχές όταν αυτές λαμβάνουν χώρα στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας[38]. Η εξαίρεση αυτή, σύμφωνα με το νομοθέτη[39], προβλέπεται ώστε να εξασφαλιστεί ο ανεξάρτητος χαρακτήρας της δικαιοσύνης αλλά και να προληφθεί ενδεχόμενη προσβολή της αρχής της διάκρισης των εξουσιών. Παρόλο που και ο ΓΚΠΔ και η Οδηγία LED τάσσονται υπέρ της εποπτείας/ευαισθητοποίησης των πράξεων επεξεργασίας εσωτερικά εντός του δικαστικού συστήματος ώστε να μην τίθεται εν

[36] Ένας όρος που από μόνος του ενέχει ένα επίπεδο ασάφειας και εξετάζεται κάθε φορά ad hoc.

[37] Βλ. Άρθρο 9^{A}Σ και άρθρο 8 παρ. 3 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ.

[38] Δυνάμει του άρθρου 45 παρ. 2 της Οδηγίας LED.

[39] Βλ. Αιτιολογική σκέψη 80 της Οδηγίας LED και 20 του Γενικού Κανονισμού

αμφιβόλω η δυνατότητα του υποκειμένου να ασκήσει τα δικαιώματά του, ο εθνικός νομοθέτης δεν προέβλεψε κάτι τέτοιο στις διατάξεις του Ν. 4624/2019, επεκτείνοντας το κενό που θέτει τα υποκείμενα εκτεθειμένα απέναντι σε πράξεις επεξεργασίας των δεδομένων τους από φορείς επιβολής του νόμου.

Αφήνοντας το πεδίο των δικαστικών και εισαγγελικών Αρχών, αξίζει να αναφέρουμε πως ο Ν. 4624/2019, ενεργώντας εντός του περιθωρίου που του προσφέρει ο Γενικός Κανονισμός, ορίζει ως κατώτατο όριο για την εγκυρότητα της συγκατάθεσης του ανηλίκου σε περιπτώσεις αξιοποίησης υπηρεσιών της κοινωνίας της πληροφορίας, την ηλικία των 15 ετών[40]. Σε περίπτωση μικρότερης ηλικίας από την πλευρά του ανήλικου, η συγκατάθεση μπορεί να είναι έγκυρη μόνο μετά από τη σύμφωνη γνώμη του ατόμου που ασκεί τη γονική μέριμνα. Και ενώ οι προβλέψεις αυτές φαίνονται ορθές, τίθεται ένα εύλογο ζήτημα στο οποίο δυστυχώς ούτε η ευρωπαϊκή ούτε η εθνική νομοθεσία έχουν καταφέρει να απαντήσουν επαρκώς: πώς αποδεικνύεται με αδιάβλητο τρόπο ότι το άτομο που έχει συγκατατεθεί πληροί όντως τις προϋποθέσεις για έγκυρη συγκατάθεση κατά περίπτωση; Παρόλο που στο πνεύμα του ΓΚΠΔ εννοείται η υποχρέωση των υπευθύνων επεξεργασίας στην επαλήθευση της ηλικίας των υποκειμένων, ούτε ο Κανονισμός, ούτε ο εθνικός νομοθέτης προέβλεψαν πώς αυτό μπορεί να γίνει επί του πρακτέου, σεβόμενοι παράλληλα και άλλες βασικές αρχές επεξεργασίας (λ.χ. της αναλογικότητας ή της ελαχιστοποίησης δεδομένων).

Δε θα μπορούσε να μη δοθεί ευελιξία στα κράτη, όσον αφορά τη θέσπιση κανόνων που αφορούν τα δεδομένα ειδικών κατηγοριών. Ο εθνικός νομοθέτης, αφουγκραζόμενος[41] τη Σύμβαση του Συμβουλίου της Ευρώπης για τα Ανθρώπινα Δικαιώματα και τη Βιοϊατρική[42] και τις θέσεις άλλων οργανισμών[43], όρισε ρητά πως τα ανθρώπινα γενετικά δεδομένα δεν θα μπορούν να υπόκεινται σε επεξεργασία για λόγους ασφάλισης υγείας και ζωής[44]. Βέβαια, σε αυτό το σημείο κρίνεται καίριο να γίνει η εξής διευκρίνιση: ενώ τα

[40] Βλ. Άρθρο 21 Ν. 4624/2019.

[41] Σύμφωνα με τη σχετική αιτιολογική έκθεση που συνοδεύει το νομοσχέδιο.

[42] Όπως κυρώθηκε με τον Ν. 2619/1998: Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ανθρωπίνων δικαιωμάτων και της αξιοπρέπειας του ατόμου σε σχέση με τις εφαρμογές της βιολογίας και της ιατρικής: Σύμβαση για τα ανθρώπινα Δικαιώματα και τη Βιοϊατρική, 1998

[43] Όπως για παράδειγμα της UNESCO μέσω της Οικουμενικής Διακήρυξης για τα Γενετικά Δεδομένα (UNESCO, 2003).

[44] Βλ. Άρθρο 23 Ν. 4624/2019.

γενετικά δεδομένα δεν μπορούν να χρησιμοποιηθούν σε καμία περίπτωση για τον προσδιορισμό ρίσκου στον τομέα της ασφάλισης, δεν παρέχεται η ίδια προστασία στα βιομετρικά δεδομένα και τα δεδομένα υγείας του ατόμου. Συνεπώς, οι πάροχοι ασφαλιστικών προϊόντων δύνανται να θέτουν σχετικά ερωτήματα στους υποψήφιους και ήδη ασφαλισμένους για να προσδιοριστεί ο κίνδυνος και το ύψος των ασφαλίστρων.

Στο άρθρο 88 ΓΚΠΔ διαβάζουμε ακόμη μία ρήτρα ευελιξίας προς τα κράτη-μέλη, αυτή τη φορά όσον αφορά την επεξεργασία προσωπικών πληροφοριών στο πλαίσιο των εργασιακών σχέσεων. Ο εθνικός νομοθέτης, βασιζόμενος σε αυτή, εξειδικεύει αυτές τις περιπτώσεις επεξεργασίας μέσω του άρθρου 27. Εν συντομία, σε αυτό αναφέρεται πως τα δεδομένα των εργαζομένων θα πρέπει να υπόκεινται σε επεξεργασία μόνο για σκοπούς που αφορούν τη σύναψη ή την εκτέλεση της σύμβασης εργασίας, ενώ τίθενται τα κριτήρια σύμφωνα με τα οποία μπορεί κατ' εξαίρεση να θεωρηθεί έγκυρη η συγκατάθεση του εργαζομένου. Επίσης, στο άρθρο υπενθυμίζονται οι προϋποθέσεις για την επεξεργασία ειδικών κατηγοριών δεδομένων και ξεκαθαρίζεται πως δεδομένα που απορρέουν από κλειστά κυκλώματα οπτικής καταγραφής των χώρων εργασίας δεν μπορούν να χρησιμοποιηθούν για αξιολόγηση της αποδοτικότητας των εργαζομένων, παρά μόνον για την προστασία ατόμων και αγαθών.

Επιπρόσθετα, παρατηρούμε πως στο αμέσως επόμενο άρθρο (28) του Ν. 4624/2019, ο νομοθέτης επιχειρεί να οριοθετήσει την επεξεργασία προσωπικών δεδομένων η οποία γίνεται στο πλαίσιο της δημοσιογραφικής έρευνας και της ακαδημαϊκής και καλλιτεχνικής έκφρασης γενικότερα, θέτοντας τις προϋποθέσεις ώστε να σταθμίζονται κατά το εφικτό καλύτερα το δικαίωμα στην ελευθερία της έκφρασης και το δικαίωμα στην προστασία της ιδιωτικής ζωής των ατόμων.[45]

Ένα ακόμα ζήτημα το οποίο έχρηζε πρόβλεψης είναι η ικανοποίηση του δικαιώματος των πολιτών για την πρόσβαση σε επίσημα έγγραφα. Ο Γενικός Κανονισμός αναφέρει[46] πως επί της αρχής η κοινοποίηση τέτοιων εγγράφων επιτρέπεται εφόσον αυτά σχετίζονται με την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον, όμως η στάθμιση των δικαιωμάτων (που και στον ΓΚΠΔ και στο εθνικό μας δίκαιο έχουν την ίδια βαρύτητα, χωρίς να υφίσταται μεταξύ τους σχέση γενικής-ειδικής διάταξης) δύναται να επιτευχθεί σε επίπεδο κρατών-μελών. Αξιοποιώντας αυτή τη δυνατότητα, ο εθνικός νομοθέτης μας

[45] Απαντώντας στις απαιτήσεις που θέτει το άρθρο 85 ΓΚΠΔ.

[46] Βλ. Άρθρο 86 ΓΚΠΔ.

παραπέμπει στις υφιστάμενες σχετικές διατάξεις οι οποίες συνεχίζουν να εφαρμόζονται ανεξάρτητα από την παρουσία προσωπικών δεδομένων στα έγγραφα που υπόκεινται στο πεδίο τους.[47]

Η τελευταία πρόβλεψη που αφήνει περιθώριο ελιγμού στα κράτη-μέλη αφορά τις κυρώσεις και την επιβολή διορθωτικών μέτρων. Συγκεκριμένα, στο άρθρο 83 παράγραφος 7 του Γενικού Κανονισμού, ορίζεται πως μέσω εθνικής νομοθεσίας δύναται να θεσμοθετηθεί διαφοροποίηση (ή ακόμα και εξαίρεση) στα διοικητικά πρόστιμα που θα εφαρμόζονται στους φορείς του δημοσίου τομέα. Σε αυτό το σημείο, ο νομοθέτης επέλεξε επί της αρχής να μην εξαιρέσει τους δημόσιους φορείς από την επιβολή προστίμων σε περίπτωση σοβαρής παραβίασης της νομοθεσίας, όμως όρισε πως το ανώτατο ποσό επιβολής προστίμου σε δημόσιο φορέα δεν μπορεί να ξεπερνά τα 10.000.000 ευρώ – πρακτικά το ήμισυ του ποσού που μπορεί να επιβληθεί ως πρόστιμο σε έναν φορέα του ιδιωτικού τομέα. Έτσι, παρατηρούμε πως δημιουργείται ένα σύστημα αξιολόγησης παραβιάσεων δύο ταχυτήτων, σαφώς με ωφελούμενους τους δημόσιους φορείς. Η προσέγγιση αυτή, παρόλο που τυπικά εδράζεται εντός των προβλέψεων του Κανονισμού, βρίσκεται οριακά εντός του πνεύματος του τελευταίου, καθώς δημιουργεί λανθασμένα την εντύπωση πως μια παραβίαση από δημόσιο φορέα είναι κατά βάση ήσσονος σημασίας, ενώ στον ΓΚΠΔ το βάρος της απαξίας ορίζεται με κριτήριο την παραβίαση και όχι τον φορέα που την προκάλεσε.

Μέχρι τη στιγμή που γράφονται αυτές οι γραμμές, ο Ν. 4624/2019 έχει τροποποιηθεί από τρεις νεότερους νόμους. Παρακάτω θα δούμε (με χρονολογική σειρά) ποιοι είναι αυτοί και πώς μετέβαλαν τις αρχικές διατάξεις:

- **Ν. 4829/2021**[48]: Οι αλλαγές προσανατολίζονταν στις πρακτικές για την κάλυψη των υπηρεσιακών αναγκών της ΑΠΔΠΧ, καθώς καταργήθηκε η παρ. 6 του άρθρου 18 για τη «Γραμματεία της Αρχής». Καμιά διαφοροποίηση όσον αφορά το ουσιαστικό πεδίο του νόμου.
- **Ν. 5002/2022**[49]:

[47] Συγκεκριμένα, πρόκειται για το άρθρο 5 του Κώδικα Διοικητικής Διαδικασίας και το άρθρο 22 του Κώδικα Οργανισμού Δικαστηρίων και Κατάστασης Δικαστικών Λειτουργών (βλ. Άρθρο 42 Ν. 4624/2019).

[48] Ν. 4829/2021: Ενίσχυση διαφάνειας και λογοδοσίας σε θεσμικούς φορείς της Πολιτείας, αποκατάσταση της ακεραιότητας του Ενιαίου Συστήματος Κινητικότητας και λοιπές διατάξεις., 2021

[49] Ν. 5002/2022: Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών., 2022

- Γίνεται υποχρεωτική η γνωστοποίηση προς την ΑΠΔΠΧ του ονοματεπώνυμου και των στοιχείων επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων (εφεξής ΥΠΔ ή DPO), και καταργείται η ρήτρα περί μη γνωστοποίησης σε περιπτώσεις καθήκοντος εχεμύθειας ή για λόγους εθνικής ασφάλειας.[50]
- Διευκρινίζεται το ουσιαστικό πεδίο εφαρμογής των διατάξεων που αφορούν την ενσωμάτωση της Οδηγίας LED, καθώς πλέον αναφέρεται ρητά πως οι πράξεις επεξεργασίας προσωπικών δεδομένων από τις Αρχές επιβολής του νόμου που δεν γίνονται στο πλαίσιο των δικαιοδοτικών ή ποινικών τους αρμοδιοτήτων, δε ρυθμίζονται από τις διατάξεις που ενσωματώνουν την Οδηγία αλλά από τον ΓΚΠΔ και τις διατάξεις του Ν.4624/2019 που τον εξειδικεύουν.[51]
- Ο όρος «δημόσια αρχή» αντικαθίσταται από τον όρο «αρμόδια αρχή», ενώ η τελευταία ορίζεται είτε ως δημόσια αρχή είτε ως ιδιωτικός φορέας στον οποίο έχει ανατεθεί εξουσία δημόσιας αρχής.[52]
- Προστίθεται διάταξη η οποία ενσωματώνει το άρθρο 8 της Οδηγίας LED και επισημαίνει τις συνθήκες που εγγυώνται τη νομιμότητα της επεξεργασίας των προσωπικών δεδομένων από τις Αρχές επιβολής του νόμου.[53]
- Γίνεται πιο αναλυτική, συγκεκριμένη και αυστηρή η διάταξη που κατευθύνει την επεξεργασία ειδικών κατηγοριών δεδομένων.[54]
- Η διάταξη που περιγράφει τις προϋποθέσεις για την εγκυρότητα της συγκατάθεσης του υποκειμένου γίνεται αναλυτικότερη και χωρίς τους «αστερίσκους» που υπήρχαν στο αρχικό κείμενό της όσον αφορά το περιεχόμενο της ενημέρωσης προς το υποκείμενο.[55]
- Επιλέγεται η προσέγγιση “opt-in” όσον αφορά την αυτοματοποιημένη επεξεργασία και την κατάρτιση προφίλ, η οποία πλέον επί της αρχής

[50] Βλ. Παρ. 5 άρθ. 6 Ν.4624/2019

[51] Βλ. Παρ. 3 άρθ. 43 Ν.4624/2019

[52] Βλ. Άρθ. 44 Ν.4624/2019

[53] Βλ. Άρθ. 45Α Ν.4624/2019

[54] Βλ. Άρθ. 46 Ν.4624/2019

[55] Βλ. Άρθ. 49 Ν.4624/2019

απαγορεύεται. Περιγράφονται (πλέον) με τη μορφή εξαίρεσης οι περιπτώσεις που μπορεί να επιτραπεί, με παράλληλη αναφορά σε εγγυήσεις και δικαιώματα, φορέας των οποίων είναι το υποκείμενο και το προστατεύουν από αναιτιολόγητα και δυσμενή έννομα αποτελέσματα.[56] Στο ίδιο αυστηρό πλαίσιο, απαγορεύεται πλέον ρητά η χρήση ειδικών κατηγοριών δεδομένων σε αυτοματοποιημένη επεξεργασία/κατάρτιση προφίλ, ενώ για τις περιπτώσεις που (κατ' εξαίρεση) αυτή γίνει, προστίθεται ρήτρα νομιμότητας (δηλ. πρόβλεψη αυτής από την εθνική ή ευρωπαϊκή νομοθεσία).[57]

- Προβλέπονται συγκεκριμένες προϋποθέσεις που οι Αρχές επιβολής του νόμου καλούνται να λάβουν υπόψη τους κατά την (επαν)εξέταση της περιόδου διατήρησης των προσωπικών δεδομένων, ενώ προβλέπεται και η υποχρέωση της τήρησης της αρχής της ελαχιστοποίησης της περιόδου αποθήκευσης «εκ σχεδιασμού» και «από προεπιλογή» στα συστήματα επεξεργασίας που χρησιμοποιούνται.[58]
- Προστέθηκε το άρθρο 84Α, το οποίο αναφέρεται στις περιπτώσεις δημοσιοποίησης δεδομένων προσωπικού χαρακτήρα από εισαγγελικές αρχές και περιγράφει αναλυτικά το περιεχόμενο, τις προϋποθέσεις, τις προβλεπόμενες εγγυήσεις που πρέπει να περιλαμβάνει η σχετική διάταξη σύμφωνα με την αρχή της αναλογικότητας, τις διαδικασίες και τη διάρκεια της δημοσιοποίησης των δεδομένων του δράστη.

- **Ν. 5043/2023**[59]: Καταργεί την 6η παράγραφο του άρθρου 11 περί (αστικής) ευθύνης των μελών της ΑΠΔΠΧ έναντι τρίτων και του Ελληνικού Δημοσίου για πράξεις ή παραλείψεις από δόλο ή αμέλεια.[60]

[56] Βλ. Παρ. 1 άρθ. 52 Ν.4624/2019

[57] Βλ. Παρ. 2 άρθ. 52 Ν.4624/2019

[58] Βλ. Άρθ. 73 Ν.4624/2019

[59] Ν. 5043/2023: Ρυθμίσεις σχετικά με τους Οργανισμούς Τοπικής Αυτοδιοίκησης α' και β' βαθμού - Διατάξεις για την ευζωία των ζώων συντροφιάς - Διατάξεις για το ανθρώπινο δυναμικό του δημοσίου τομέα - Λοιπές ρυθμίσεις του Υπουργείου Εσωτερικών και άλλες επείγουσες διατάξεις, 2023

[60] Βλ. Εδάφ. γ' παρ. 2 άρθ. 123 Ν.5043/2023

Πέραν όμως του βασικού (και γενικού) νομοθετικού πλαισίου περί προστασίας προσωπικών δεδομένων και ιδιωτικότητας σε ευρωπαϊκό και εθνικό επίπεδο, υπάρχει και το αντίστοιχο ειδικό που αφορά συγκεκριμένα τον τομέα των ηλεκτρονικών επικοινωνιών.

Παρακάτω θα δούμε τις βασικές προβλέψεις της ευρωπαϊκής Οδηγίας 2002/58/ΕΚ, όπως αυτή τροποποιήθηκε, ενσωματώθηκε στο ελληνικό δίκαιο και ισχύει μέχρι σήμερα.

3.4 Η Οδηγία για την ιδιωτικότητα στις ηλεκτρονικές επικοινωνίες (ePrivacy Directive 2002/58/ΕΚ) με την τελευταία της αναθεώρηση (2009/136/ΕΚ)

Ολοκληρώνοντας την ανάλυση του Γενικού Κανονισμού Προστασίας Δεδομένων και του Ν.4624/2019 ως νομοθετήματα γενικής εφαρμογής (lex generalis), αξίζει να εξετάσουμε (όχι τόσο λεπτομερώς αυτή τη φορά) την Οδηγία 2002/58/ΕΚ[61] (εφεξής οδηγία για την ιδιωτικότητα στις ηλεκτρονικές επικοινωνίες ή ePrivacy Directive) , ως νομοθέτημα ειδικού ενδιαφέροντος (lex specialis).

Αντικείμενο της εν λόγω Οδηγίας είναι η θέσπιση κανόνων που αφορούν τον τρόπο χειρισμού των προσωπικών δεδομένων που υπόκεινται σε επεξεργασία στο πλαίσιο των ηλεκτρονικών επικοινωνιών μέσω των δημόσιων[62] δικτύων. Το νομοθέτημα απευθύνεται στους παρόχους των υπηρεσιών ηλεκτρονικών επικοινωνιών, οριοθετώντας το μέτρο μέχρι το οποίο μπορεί να φτάσει η παρέμβασή τους στα δεδομένα των τελικών χρηστών όπως επίσης τις υποχρεώσεις τους και τις εγγυήσεις που οφείλουν να εφαρμόζουν οι πάροχοι προκειμένου να διασφαλιστεί το απόρρητο, η ακεραιότητα και η διαθεσιμότητα των δεδομένων. Επίσης, στην ePrivacy Directive περιγράφεται ο μηχανισμός εποπτείας της Οδηγίας μέσω των εθνικών εποπτικών αρχών, της συνεργασίας των εμπλεκόμενων θεσμών και της εναρμόνισης τεχνικών προδιαγραφών για την πληρέστερη εφαρμογή του νόμου.

[61] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, 2002)

[62] Με τον όρο «δημόσιων» νοείται το δίκτυο ή/και υπηρεσία που είναι εμπορικά διαθέσιμη στο ευρύ κοινό, και δε θα πρέπει να συγχέεται με τον όρο «δημόσιο αγαθό».

Το πλήρες κείμενο της Οδηγίας αποτελείται από είκοσι ένα (21) άρθρα, ενώ τα ζητήματα με τα οποία καταπιάνεται προς ρύθμιση στη σημερινή της μορφή[63] θα μπορούσαν να συνοψιστούν ως εξής:

- Αρχικά, τίθεται το ουσιαστικό πεδίο εφαρμογής της Οδηγίας, το οποίο αφορά μόνο περιπτώσεις επεξεργασίας που γίνονται στο πλαίσιο χρήσης υπηρεσιών επικοινωνιών μέσω δημόσιων δικτύων στην ΕΕ.[64]
- Στη συνέχεια, δίνεται ιδιαίτερη έμφαση στην υποχρέωση των παρόχων να εκτελούν την επεξεργασία των προσωπικών δεδομένων (ήτοι το περιεχόμενο της επικοινωνίας και τα δεδομένα κίνησης και θέσης) με τη δέουσα ασφάλεια μέσω βασικών αρχών και υιοθετώντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα, ενώ περιγράφεται το πώς αναμένεται να κινηθούν σε περίπτωση περιστατικού παραβίασης των δεδομένων.[65]
- Διασφαλίζεται το πλαίσιο εντός του οποίου οι επικοινωνίες λειτουργούν με απόρρητο χαρακτήρα, ενώ προβλέπεται και η επιτρεπόμενη χρήση των δεδομένων κίνησης (ή αλλιώς «μεταδεδομένων») που συνοδεύουν την εκάστοτε επικοινωνία.[66]
- Περιγράφεται ρητά το δικαίωμα των συνδρομητών στη λήψη μη αναλυτικών λογαριασμών ώστε να αυξηθεί το επίπεδο προστασίας της ιδιωτικότητας των συνδιαλεγόμενων. Στο ίδιο κλίμα ρυθμίζεται και η δυνατότητα απόκρυψης ταυτότητας στις κλήσεις, με τις ανάλογες εξαιρέσεις της.[67]
- Η Οδηγία θέτει αυστηρές προϋποθέσεις επεξεργασίας των δεδομένων θέσης των τερματικών συσκευών (ανωνυμοποιημένα ή μετά από έγκυρη συγκατάθεση).[68]
- Ρυθμίζεται η δυνατότητα (μη) αναγραφής των στοιχείων των συνδρομητών στους δημόσια προσβάσιμους τηλεφωνικούς καταλόγους.[69]

[63] Η παρούσα Οδηγία έχει τροποποιηθεί από δύο νεότερες Οδηγίες, βλ. παρακάτω στην ίδια ενότητα.

[64] Βλ. Άρθ. 1-3 της Οδηγίας 2002/58/ΕΚ

[65] Βλ. Άρθ. 4 της Οδηγίας 2002/58/ΕΚ

[66] Βλ. Άρθ. 5-6 της Οδηγίας 2002/58/ΕΚ

[67] Βλ. Άρθ. 7-8 και 10 της Οδηγίας 2002/58/ΕΚ

[68] Βλ. Άρθ. 9 της Οδηγίας 2002/58/ΕΚ

[69] Βλ. Άρθ. 12 της Οδηγίας 2002/58/ΕΚ

- Περιορίζεται η δυνατότητα κλήσεων ή αποστολής μηνυμάτων για εμπορική προώθηση μέσω αυτόματων συστημάτων (εκτός ορισμένων εξαιρέσεων που ορίζει ο νόμος), η οποία μπορεί να λαμβάνει χώρα είτε με την προηγούμενη συγκατάθεση των συνδρομητών, είτε δίνοντας τη δυνατότητα στους τελευταίους να αντιτίθενται στη λήψη τέτοιας επικοινωνίας.[70]
- Απαγορεύτηκε η επιβολή ειδικών τεχνικών χαρακτηριστικών από τα κράτη-μέλη στον εξοπλισμό που εμπλέκεται στις τηλεπικοινωνίες, τα οποία ενδεχομένως να παρεμπόδιζαν την ελεύθερη διακίνηση των συσκευών στην ενιαία αγορά.[71]

Η Οδηγία 2002/58/ΕΚ τροποποιήθηκε δύο φορές, την πρώτη φορά με την (πλέον καταργηθείσα) Οδηγία 2006/24/ΕΚ[72] και τη δεύτερη φορά με την Οδηγία 2009/136/ΕΚ[73], ενώ ενσωματώθηκε στην ελληνική έννομη τάξη με το Ν. 3471/2006[74].

---

[70] Βλ. Άρθ. 13 της Οδηγίας 2002/58/ΕΚ. Σε αυτό το άρθρο βασίστηκε και το αντίστοιχο άρθρο 11 του Ν. 3471/2006, στο οποίο αντλεί τη νομική του βάση το γνωστό «Μητρώο 11» των παρόχων τηλεπικοινωνιών στην Ελλάδα.

[71] Βλ. Άρθ. 14 της Οδηγίας 2002/58/ΕΚ

[72] Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ, 2006, η οποία το 2014 καταργήθηκε με απόφαση του ΔΕΕ στις συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12.

[73] Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 , για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ, 2009). Η τροποποίηση με το μεγαλύτερο ενδιαφέρον που επέφερε η εν λόγω Οδηγία υφίσταται στην παρ. 3 άρθ. 5 της Οδηγίας ePrivacy, καθώς εγκαθιδρύει μια στροφή στην προσέγγιση της εγκατάστασης των cookies στις τερματικές συσκευές των χρηστών: ενώ στην αρχή ακολουθούνταν η πρακτική "opt-out" σε περίπτωση που ο χρήστης ήθελε να εναντιωθεί μετά την εγκατάσταση αυτών των αρχείων, με την αναθεώρηση απαιτείται η εγκατάσταση των cookies να γίνεται μετά από την ρητή και ενημερωμένη συγκατάθεση του χρήστη του τερματικού εξοπλισμού ("opt-in").

[74] Ν. 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997, 2006

3.5 Εξελίξεις στο ενωσιακό νομικό πλαίσιο

Έχοντας ολοκληρώσει την αναφορά μας και στην Οδηγία 2002/58/ΕΚ (ePrivacy Directive), παρατηρούμε πως όσο προχωράει η ευρωπαϊκή ενοποίηση μέσω της εμβάθυνσης, τόσο προτιμάται το μοντέλο ευρωπαϊκής νομοθέτησης μέσω Κανονισμών (έστω και με ρήτρες ευελιξίας) αντί για τις Οδηγίες. Ο κύριος λόγος που συμβαίνει αυτό είναι διότι μέσω αυτών επιτυγχάνεται ένα άμεσο, ομοιόμορφο και συνεκτικό πλαίσιο ρύθμισης ζητημάτων που υπό άλλες συνθήκες θα άφηνε περιθώρια διαφοροποίησης μεταξύ των κρατών-μελών, σε σημείο που η εναρμόνιση των επιχειρήσεων με παρουσία σε περισσότερες ευρωπαϊκές χώρες θα καθίσταντο δυσεπίλυτος γρίφος. Για τις επιχειρήσεις, οι Κανονισμοί προσφέρουν συγκεκριμένες, σταθερές και ξεκάθαρες νομικές απαιτήσεις εναρμόνισης. Λαμβάνοντας, λοιπόν, υπόψη την εύρυθμη λειτουργία της ενιαίας αγοράς, την ευρωπαϊκή ολοκλήρωση αλλά και την εκθετική εξέλιξη της τεχνολογίας, η Ευρωπαϊκή Επιτροπή εργάζεται πάνω σε δύο νομοθετικές πρωτοβουλίες που αφορούν την επεξεργασία προσωπικών δεδομένων των ευρωπαίων πολιτών:

- Την επικαιροποίηση και μετατροπή της ePrivacy από Οδηγία σε καθολικά δεσμευτικό Κανονισμό, και
- Την δημιουργία ενός Κανονισμού που θα οριοθετεί τις εφαρμογές που χρησιμοποιούν τις δυνατότητες της τεχνητής νοημοσύνης (εφεξής ΤΝ ή AI).

3.5.1 Η πρόταση κανονισμού ePrivacy

Η αναβάθμιση της Οδηγίας 2002/58/ΕΚ σε Κανονισμό e-Privacy δεν είναι κάτι νέο. Για την ακρίβεια, η νομοθετική πρωτοβουλία από την Ευρωπαϊκή Επιτροπή (εφεξής και Επιτροπή ή Κομισιόν ή ΕC) ξεκίνησε το 2017, αρχής γενομένης κατά τη διάρκεια της μαλτέζικης προεδρίας του Συμβουλίου της Ευρωπαϊκής Ένωσης. Τον Ιανουάριο του 2017, η Κομισιόν παρουσίασε μια πρόταση κανονισμού, η οποία (όπως και ο Γενικός Κανονισμός Προστασίας Δεδομένων) θα αποτελούσε μέρος της γενικότερης προσπάθειας της Ένωσης για επικαιροποίηση των κανόνων προστασίας δεδομένων καθιστώντας τους σύγχρονους και τεχνολογικά ουδέτερους.

Η πρόταση, λοιπόν, αφορούσε έναν Κανονισμό για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες[75]. Η αρχική στόχευση του νομοθετήματος ήταν να ανεβάσει το επίπεδο της ασφάλειας και της εμπιστοσύνης που νιώθουν οι χρήστες ηλεκτρονικών υπηρεσιών, ενώ παράλληλα να αυξήσει τη συνεκτικότητα του νομικού πλαισίου στην αλληλεπίδραση με τον ΓΚΠΔ. Το αρχικό κείμενο που προτάθηκε από την Επιτροπή[76], περιλαμβάνει στους κόλπους του τα μέσα ηλεκτρονικών επικοινωνιών που δεν εντάσσονταν στο ουσιαστικό πεδίο της Οδηγίας (π.χ. πάροχοι υπηρεσιών φωνής μέσω διαδικτύου - VoIP, οι ανταλλαγές άμεσων μηνυμάτων και e-mails μέσω διαδικτύου κ.ά.). Επίσης, αλλάζει η προσέγγιση για τη διαχείριση των cookies, προτείνοντας την κατηγοριοποίησή τους ανάλογα με τους σκοπούς επεξεργασίας και της επεμβατικότητας τους και τη διαχείρισή τους κεντρικά μέσω του φυλλομετρητή. Επιπλέον, αυξάνει το επίπεδο διαφάνειας προς τον τελικό χρήστη όσον αφορά τη μη ζητηθείσα επικοινωνία, δίνοντας ιδιαίτερη βάση στο δικαίωμα αντίταξης του τελευταίου. Τέλος, μια ακόμη καινοτομία είναι πως λαμβάνεται υπόψη η συνεχής ανάπτυξη του διαδικτύου των πραγμάτων (Internet of Things – IoT), οπότε και η ανταλλαγή δεδομένων μεταξύ συσκευών εντάσσεται εντός των απαιτήσεων που θέτει η πρόταση Κανονισμού.

Δυστυχώς, αν και η πρόταση Κανονισμού έχει τύχει επεξεργασίας κατά τη διάρκεια διαδοχικών προεδριών του Συμβουλίου της ΕΕ[77], η τελευταία ενημέρωση που κατέδειξε πρόοδο στη νομοθετική διαδικασία δημοσιεύτηκε στις αρχές του 2021[78] οπότε και οι πρέσβεις της Επιτροπής των Μόνιμων Αντιπροσώπων του Συμβουλίου Υπουργών της ΕΕ ενέκριναν μια κοινή θέση, η οποία θα συζητούνταν από το Συμβούλιο και το Ευρωκοινοβούλιο κατά τη διαπραγμάτευση των διατάξεων του τελικού κειμένου του

[75] Πρόταση - Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), 2017

[76] Διαθέσιμο στο σύνδεσμο https://t.ly/E1ANT (πρόσβαση 20/10/2023)

[77] Για την ακρίβεια της μαλτέζικης, της εσθονικής, της βουλγαρικής, της αυστριακής, της ρουμανικής, της φινλανδικής, της κροατικής, της γερμανικής και της πορτογαλικής (έως και το 2021), Πηγή: (*List of Presidencies of the Council of the European Union*, 2023), διαθέσιμο στο σύνδεσμο https://t.ly/26mPk (Πρόσβαση 28/10/2023)

[78] Σύμφωνα με σχετικό Δελτίο Τύπου, (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2021), διαθέσιμο στη διεύθυνση https://t.ly/CBfcr (Πρόσβαση 28/10/2023)

Κανονισμού ePrivacy. Από το 2021 η νομοθετική πρωτοβουλία της Επιτροπής βρίσκεται στο στάδιο του τριμερούς διαλόγου μεταξύ Επιτροπής, Συμβουλίου και Ευρωκοινοβουλίου, ενώ αναμένεται να ακολουθήσει η «πρώτη ανάγνωση», σύμφωνα με τη συνήθη νομοθετική διαδικασία.[79]

3.5.2 Η πρόταση κανονισμού για την Τεχνητή Νοημοσύνη (EU AI Act)

Τα τελευταία χρόνια, η αγορά προϊόντων λογισμικού άρχισε να περιλαμβάνει προϊόντα (εφαρμογές και προγράμματα) τα οποία εμπεριείχαν κάποιο είδος τεχνητής νοημοσύνης («ΤΝ» ή «AI»). Από ένα απλό chatbot[80] μέχρι εφαρμογές που μπορούν να δημιουργήσουν deepfakes[81], η τεχνητή νοημοσύνη άρχισε να διεισδύει όλο και περισσότερο στους παραγωγικούς κλάδους και στην καθημερινότητα όλων, άλλες φορές με επωφελή και άλλες με επιζήμια αποτελέσματα. Θέλοντας να βάλει μια τάξη στο τοπίο που δημιουργούνταν, μετά από διαβουλεύσεις με εμπλεκόμενα μέρη και φορείς, η Κομισιόν συνέστησε το 2018 μια ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη[82] (εφεξής «Ομάδα για την ΤΝ» ή «AI HLEG»), με στόχο την παροχή συμβουλευτικής όσον αφορά την χάραξη πολιτικής για την ΤΝ. Η Ομάδα για την ΤΝ συνέταξε ορισμένες κατευθυντήριες γραμμές δεοντολογίας για την αξιοπιστία της ΤΝ[83], οι οποίες βασίζονταν γύρω από 7 (επτά) θεμελιώδεις και εξίσου σημαντικές απαιτήσεις:

1) **Ανθρώπινη παρέμβαση και εποπτεία:** οι χρήστες θα πρέπει να έχουν τη δυνατότητα να λαμβάνουν αυτόνομες, τεκμηριωμένες και ελεύθερες

[79] Περισσότερα για τη συνήθη νομοθετική διαδικασία είναι διαθέσιμα στο σύνδεσμο https://t.ly/ag9ue (Πρόσβαση 28/10/2023)

[80] Τα chatbot είναι μικροεφαρμογές διεπαφής σε μορφή διαλόγου chat, μέσω των οποίων ο τελικός χρήστης μπορεί να βρει πληροφορίες ή να εκτελέσει εντολές για μια υπηρεσία καθοδηγούμενος από τα βήματα που του εμφανίζει το chatbot. Η λογική αυτών των μικροεφαρμογών θέλει το χρήστη να αλληλοεπιδρά με την υπηρεσία με τρόπο απλό και ενστικτώδη, μιμούμενος τον τρόπο διαλόγου με άλλους ανθρώπους μέσω εφαρμογών ανταλλαγής μηνυμάτων.

[81] Τα deepfakes ορίζονται ως αρχεία πολυμέσων (εικόνα, βίντεο, ήχος) στα οποία χρησιμοποιείται η εικόνα ή/και η φωνή ενός πραγματικού ανθρώπου, όμως η επεξεργασία γίνεται με τέτοιο τρόπο ώστε στο τελικό αποτέλεσμα το άτομο το οποίο εικονίζεται φαίνεται να δηλώνει ή/και να κάνει πράγματα ψευδή. Σκοπός των deepfakes είναι να παραπλανήσουν και να πείσουν τον αποδέκτη με τη χρήση εντελώς αναληθών «τεκμηρίων».

[82] Περισσότερες πληροφορίες για την Ομάδα (ή αλλιώς AI HLEG) είναι διαθέσιμες στο σύνδεσμο https://t.ly/pnX8X (Πρόσβαση 29/10/2023)

[83] Διαθέσιμες και στα ελληνικά στο σύνδεσμο https://t.ly/rmPyD (Πρόσβαση 29/10/2023)

αποφάσεις κατά την αλληλεπίδρασή τους με συστήματα ΤΝ, ενώ θα πρέπει να υπάρχει και η δυνατότητα εποπτείας ώστε τα τελευταία να ελέγχονται για ενδεχόμενες δυσμενείς επιπτώσεις σε αυτή τη δυνατότητα.

2) **Τεχνική στιβαρότητα και ασφάλεια:** τα συστήματα ΤΝ θα πρέπει να σχεδιάζονται με τέτοιο τρόπο ώστε να προλαμβάνονται οι βλάβες και οι τεχνικοί κίνδυνοι που μπορεί να αντιμετωπίσουν, είτε λόγω τεχνικών αστοχιών, ανακριβειών είτε λόγω επιθέσεων από κακόβουλους τρίτους.
3) **Ιδιωτική ζωή και διακυβέρνηση δεδομένων:** κατά τον κύκλο ζωής τους, τα συστήματα ΤΝ θα πρέπει να σέβονται την ιδιωτικότητα των χρηστών και να επιτυγχάνουν τη συνεχή ακρίβεια και ακεραιότητα των δεδομένων που επεξεργάζονται, η οποία συμπαρασύρει και την ποιότητα αυτών. Επιπλέον, θα πρέπει η πρόσβαση σε προσωπικά δεδομένα εντός του συστήματος ΤΝ να διέπεται από πρωτόκολλα ώστε να εξασφαλίζεται η μικρότερη δυνατή έκθεση των δεδομένων εντός και εκτός του οργανισμού.
4) **Διαφάνεια:** ο τρόπος λειτουργίας, τα μοντέλα, τα σύνολα αποφάσεων που παίρνονται και τα δεδομένα που επεξεργάζεται ένα σύστημα ΤΝ θα πρέπει να μπορούν να εξηγηθούν. Επίσης, οι χρήστες που έρχονται σε επαφή με ένα τέτοιο σύστημα θα πρέπει να ενημερώνονται πως πρόκειται για αυτοματοποιημένο μέσο και όχι για συνομιλία με άνθρωπο.
5) **Πολυμορφία, απαγόρευση των διακρίσεων και δικαιοσύνη:** τα συστήματα ΤΝ θα πρέπει να σχεδιάζονται με τρόπο που δεν θα επιτρέπει την αθέμιτη μεροληψία λόγω λανθασμένων μοντέλων επεξεργασίας και διακυβέρνησης δεδομένων. Επίσης, θα πρέπει να μπορούν να είναι προσβάσιμα στους τελικούς χρήστες ανεξάρτητα από την ηλικία, το φύλο ή άλλα χαρακτηριστικά τους, δίνοντας ιδιαίτερη έμφαση στην προσβασιμότητα των ευάλωτων κοινωνικών ομάδων.
6) **Κοινωνική και περιβαλλοντική ευημερία:** τα συστήματα ΤΝ θα πρέπει να εξετάζονται ως προς τις επιπτώσεις τους στις κοινωνικές σχέσεις των ανθρώπων, στη δημοκρατία και γενικότερα στην κοινωνία, ώστε να εφαρμόζονται με τρόπο που τις βελτιώνει και δεν τις βλάπτει. Επίσης, ο σχεδιασμός, η εγκατάσταση και υλοποίηση ενός συστήματος ΤΝ δεν θα πρέπει να γίνεται εις βάρος του περιβάλλοντος, αλλά με τρόπο φιλικό προς αυτό.

7) **Λογοδοσία:** η αποτελεσματικότητα των συστημάτων ΤΝ θα πρέπει να μπορεί να αποδειχθεί σε κάθε φάση της υλοποίησής τους, ενώ δεδομένα που αφορούν τις εσωτερικές και εξωτερικές αξιολογήσεις τους, τις ενδεχόμενες αρνητικές επιπτώσεις τους καθώς και τα μέτρα για την ελαχιστοποίηση τους θα πρέπει να είναι διαθέσιμα – και πολλές φορές να υπόκεινται σε ανεξάρτητο έλεγχο.

Οι προτάσεις της Ομάδας για την ΤΝ συνοδεύονταν και από ένα πρότυπο αξιολόγησης, το οποίο μπορούν να χρησιμοποιήσουν οι φορείς που αναπτύσσουν συστήματα AI ώστε να εξασφαλίσουν τη συμμόρφωση του προϊόντος τους με τους κανόνες δεοντολογίας. Όλα τα παραπάνω εφαρμόζονται εθελοντικά από τους φορείς ανάπτυξης εργαλείων ΤΝ.

Δεδομένου ότι τα χρόνια που ακολούθησαν το 2018, ήρθαν στο προσκήνιο ευκαιρίες αξιοποίησης αλλά κυρίως και περιπτώσεις κατάχρησης της τεχνητής νοημοσύνης[84], η Ευρωπαϊκή Επιτροπή, λαμβάνοντας υπόψη τις παραπάνω κατευθυντήριες γραμμές και μετά από διαβούλευση με τους ενδιαφερόμενους φορείς, δημοσιεύει στις 22 Απριλίου 2021 την Πρόταση Κανονισμού για την Τεχνητή Νοημοσύνη (εφεξής και «EU AI Act»)[85]. Όπως και σε κάθε Κανονισμό, έτσι και εδώ βασικός στόχος είναι η υιοθέτηση ενός ενιαίου ρυθμιστικού πλαισίου, ιδιαίτερα λαμβάνοντας υπόψη το γεγονός πως η επιβολή αντίστοιχης νομοθεσίας σε κάθε κράτος – μέλος ξεχωριστά σε μια αγορά που από τη φύση της δε γνωρίζει σύνορα, θα δημιουργούσε περισσότερα προβλήματα από όσα θα έλυνε.

Προτείνοντας, λοιπόν, τον εν λόγω Κανονισμό, η Επιτροπή επιχειρεί να διασφαλίσει πως όλα τα συστήματα ΤΝ που διατίθενται εντός της ενιαίας αγοράς είναι ασφαλή απέναντι στους πολίτες, σέβονται τα ατομικά και κοινωνικά τους δικαιώματα και δεν έρχονται σε αντίθεση με τις αξίες της ΕΕ. Επίσης, η ύπαρξη συγκεκριμένου πλαισίου αναμένεται να ενισχύσει το αίσθημα ασφάλειας τόσο των ευρωπαίων πολιτών, όσο και των επιχειρήσεων, συνδράμοντας στην περαιτέρω ανάπτυξη καινοτόμων και ασφαλών εργαλείων.

---

[84] Πολύ ενδιαφέρουσα είναι και η μελέτη των (Ciancaglini κ.ά., 2020) αναφορικά με τη χρήση και τις περιπτώσεις κατάχρησης της τεχνητής νοημοσύνης.

[85] Για το πλήρες κείμενο, βλ. Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την Τεχνητή Νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης, 2021, διαθέσιμη στο https://shorturl.at/iwELZ (Πρόσβαση 27/12/2023)

Προσπαθώντας να είναι τεχνολογικά ουδέτερη και ταυτόχρονα όσο ευέλικτη απαιτείται, η πρόταση της Κομισιόν ακολουθεί μια προσέγγιση βασισμένη στο επίπεδο ρίσκου που μπορεί να δημιουργούν τα διαφορετικά συστήματα ΤΝ. Παρακάτω βλέπουμε (με τη μορφή πίνακα) την κατηγοριοποίησή τους, καθώς και τις απαιτήσεις που θα πρέπει να πληρούνται για να διακινηθεί νόμιμα το εκάστοτε προϊόν:

Χαρακτηρισμός συστήματος ΤΝ με βάση το ρίσκο του	**Ελάχιστες απαιτήσεις διακίνησης σύμφωνα με την αρχική Πρόταση Κανονισμού EU AI Act**
Απαράδεκτου κινδύνου[86]	Απαγόρευση διακίνησης
Υψηλού κινδύνου[87]	- Ένταξη σε σύστημα διαχείρισης κινδύνου[88] - Πρακτικές διακυβέρνησης και διαχείρισης δεδομένων[89] - Κατάρτιση τεχνικού φακέλου[90] - Ύπαρξη «αρχείων καταγραφής» ώστε να προσφέρεται η δυνατότητα ιχνηλασιμότητας της επεξεργασίας[91] - Διαφάνεια απέναντι στους χρήστες για τον τρόπο λειτουργίας τους[92] - Δυνατότητα εποπτείας από άνθρωπο κατά τη χρήση τους[93] - Ανθεκτικότητα απέναντι σε σφάλματα ή ανθρώπινες αστοχίες και απόπειρες κακόβουλων τρίτων δια πρόσβαση, αλλοίωση και καταστροφή δεδομένων[94]

[86] Βλ. Άρθρο 5 της Πρότασης Κανονισμού EU AI Act.

[87] Βλ. Άρθρο 6 της Πρότασης Κανονισμού EU AI Act.

[88] Βλ. Άρθρο 9 της Πρότασης Κανονισμού EU AI Act.

[89] Βλ. Άρθρο 10 της Πρότασης Κανονισμού EU AI Act.

[90] Βλ. Άρθρο 11 της Πρότασης Κανονισμού EU AI Act.

[91] Βλ. Άρθρο 12 της Πρότασης Κανονισμού EU AI Act.

[92] Βλ. Άρθρο 13 της Πρότασης Κανονισμού EU AI Act.

[93] Βλ. Άρθρο 14 της Πρότασης Κανονισμού EU AI Act.

[94] Βλ. Άρθρο 15 της Πρότασης Κανονισμού EU AI Act.

	- Λειτουργία συστήματος διαχείρισης ποιότητας για τη συνεχή παρακολούθηση και τεκμηρίωση της συμμόρφωσης[95]
Συστήματα ΤΝ γενικού σκοπού και δημιουργικής ΤΝ	Υποχρεώσεις διαφάνειας και προαιρετική συμμόρφωση με κανόνες δεοντολογίας, εκτός εάν πρόκειται για συστήματα με υψηλό αντίκτυπο[96]
Συστήματα ΤΝ περιορισμένου ρίσκου	Υποχρεώσεις διαφάνειας και προαιρετική συμμόρφωση με κανόνες δεοντολογίας (Madiega, 2023)
Συστήματα ΤΝ ελάχιστου ρίσκου	Προαιρετική συμμόρφωση με κανόνες δεοντολογίας (Madiega, 2023)

Πίνακας 1: Ελάχιστες απαιτήσεις διακίνησης συστημάτων ΤΝ με βάση το επίπεδο κινδύνου τους για τα δικαιώματα και τις ελευθερίες των ατόμων.

Η αρχική πρόταση της Κομισιόν πρότεινε συγκεκριμένες πρακτικές[97] να ενταχτούν στη λίστα των συστημάτων ΤΝ με «απαράδεκτο» επίπεδο κινδύνου. Μετά από διαπραγματεύσεις με το Ευρωκοινοβούλιο και το Συμβούλιο, η τελική λίστα πρακτικών που θεωρούνται «απαράδεκτες» και άρα απαγορευμένες, είναι η παρακάτω (European Parliament, 2023):

1) Συστήματα βιομετρικής κατηγοριοποίησης που επεξεργάζονται ειδικές κατηγορίες δεδομένων (π.χ. σεξουαλικός προσανατολισμός, θρησκευτικές και πολιτικές πεποιθήσεις κλπ.)[98],
2) Ανεξέλεγκτη συλλογή εικόνων προσώπου μετά από σάρωση τοποθεσιών στο διαδίκτυο ή υλικού καμερών κλειστού κυκλώματος για τη δημιουργία βάσεων δεδομένων με σκοπό την αναγνώριση προσώπων,
3) Χρήση συστημάτων για την αναγνώριση συναισθημάτων στον εργασιακό ή εκπαιδευτικό χώρο,

[95] Βλ. Άρθρο 17 της Πρότασης Κανονισμού EU AI Act.

[96] Βλ. Άρθρο 69 της Πρότασης Κανονισμού EU AI Act και σχετικό ενημερωτικό έγγραφο της υπηρεσίας Κοινοβουλευτικής Έρευνας του Ευρωπαϊκού Κοινοβουλίου (2023).

[97] Βλ. Άρθρο 5 της Πρότασης Κανονισμού EU AI Act.

[98] Βλ. Άρθρο 9 του Γενικού Κανονισμού Προστασίας Δεδομένων.

4) Εφαρμογή κοινωνικής βαθμολόγησης με βάση τη συμπεριφορά ή τα χαρακτηριστικά των ατόμων,
5) Χειραγώγηση ανθρώπινων συμπεριφορών με σκοπό την παράκαμψη της ελεύθερης βούλησης με τη χρήση συστημάτων ΤΝ,
6) Εκμετάλλευση ιδιαίτερων χαρακτηριστικών ή/και ευπαθειών ατόμων μέσω της ΤΝ.

Πέραν των απαγορευμένων πρακτικών, οι συννομοθέτες συμφώνησαν και σε μια σειρά εγγυήσεων ώστε να αυστηροποιηθούν οι προϋποθέσεις εξαιρέσεων για τη χρήση συστημάτων βιομετρικής ταυτοποίησης σε δημόσιους χώρους για σκοπούς επιβολής του νόμου. Όσον αφορά τα συστήματα «υψηλού κινδύνου», μια εξέλιξη της διαπραγμάτευσης είναι η εισαγωγή της υποχρεωτικής «εκτίμησης αντικτύπου θεμελιωδών δικαιωμάτων», όπως επίσης και το δικαίωμα των πολιτών στην υποβολή παραπόνων σχετικά με συστήματα ΤΝ και στη λήψη αιτιολογημένων απαντήσεων σχετικά με τον τρόπο λειτουργίας τους όταν αυτός επηρεάζει τα δικαιώματα και τις ελευθερίες τους. Τέλος, όσον αφορά τα συστήματα ΤΝ «γενικού σκοπού», συμφωνήθηκε πως και αυτά θα πρέπει να ανταποκρίνονται τουλάχιστον στις απαιτήσεις διαφάνειας και πως οι κανόνες δεοντολογίας μπορούν να θεωρούνται ως το εργαλείο εναρμόνισης έως ότου η ΕΕ υιοθετήσει συγκεκριμένες προδιαγραφές για αυτά.

Αξίζει να σημειώσουμε, πως παρόλο που το EU AI Act σχετίζεται με τον Γενικό Κανονισμό Προστασίας Δεδομένων ως ειδική νομοθεσία («lex specialis»), τα πρόστιμα που προβλέπονται σε περίπτωση παραβίασής του είναι αρκετά υψηλότερα σε σχέση με τον ΓΚΠΔ, για την ακρίβεια από 35 εκατομμύρια ευρώ ή 7% του παγκόσμιου τζίρου έως 7,5 εκατομμύρια ευρώ ή 1,5% του τζίρου, ανάλογα με τη σοβαρότητα της παραβίασης και το μέγεθος του οργανισμού στον οποίο επιβάλλεται η κύρωση.[99]

Μέχρι και την ώρα που γράφονται αυτές οι γραμμές, η πρόταση Κανονισμού EU AI Act βρίσκεται στο στάδιο ολοκλήρωσης της πρώτης ανάγνωσης της συνήθους νομοθετικής διαδικασίας, με το Ευρωκοινοβούλιο και το Συμβούλιο να έχουν καταλήξει σε πολιτική συμφωνία. Αναμένεται η επίσημη ψήφιση του τελικού κειμένου του

[99] Βλ. Άρθρο 71 της Πρότασης Κανονισμού EU AI Act, στην οποία αρχικά τα πρόστιμα ήταν χαμηλότερα, ήτοι έως 30 εκατομμύρια ευρώ ή μέχρι 6% του παγκόσμιου κύκλου εργασιών αλλά τα χαμηλότερα πρόστιμα ήταν υψηλότερα από τα τελικώς συμφωνηθέντα, δηλαδή έως 20 εκατομμύρια ευρώ ή μέχρι 4% του κύκλου εργασιών και έως 10 εκατομμύρια ευρώ ή μέχρι 2% του συνολικού κύκλου εργασιών.

Κανονισμού από το καθένα από τα δύο θεσμικά όργανα ώστε ο Κανονισμός να γίνει και επίσημα μέρος της ευρωπαϊκής νομοθεσίας. (European Parliament, 2023)

Καταλήγοντας, θα ήταν παράλειψη να μην αναφερθεί πως όσα περιεγράφηκαν παραπάνω οδήγησαν και στην υιοθέτηση της ελληνικής νομοθεσίας για την ανάπτυξη της τεχνητής νοημοσύνης με τη θέση σε ισχύ του Ν. 4961/2022[100]. Είναι σαφώς ευτυχές η ύπαρξη του στην ελληνική έννομη τάξη όμως η ανάλυση του στην παρούσα διπλωματική δεν κρίνεται αναγκαία, αφενός διότι το EU AI Act βρίσκεται στην τελική ευθεία ψήφισης, οπότε και η εθνική νομοθεσία θα χρειαστεί ενδεχομένως να επικαιροποιηθεί, αφετέρου μιας και η προσέγγιση του Έλληνα νομοθέτη ακολουθεί σε μεγάλο βαθμό τις προτάσεις της ομάδας υψηλού επιπέδου για την ΤΝ, όπως αυτές περιγράφονται στον αντίστοιχο κώδικα δεοντολογίας.

4 Η Κρυπτογράφηση και η χρήση της στις επικοινωνίες

Όταν χρησιμοποιούμε τον όρο κρυπτογράφηση, αναφερόμαστε σε μια επιμέρους επιστημονική θεματική της κρυπτολογίας. Η τελευταία πραγματεύεται ευρύτερα τη μυστικότητα του προφορικού και του γραπτού λόγου, μέσω της κρυπτογράφησης, της στεγανογραφίας και της κρυπτανάλυσης (Μαυρίδης, 2016a). Αφενός, στόχος της κρυπτογραφίας είναι η «μετατροπή των δεδομένων με τέτοιο τρόπο ώστε να καθίσταται αδύνατη η ανάγνωση και ερμηνεία του μεταδιδόμενου κρυπτογραφημένου μηνύματος» μέσω της χρήσης ενός (ή και παραπάνω) μυστικού κλειδιού (Μαυρίδης, 2016a) και αφετέρου η κρυπτανάλυση προσπαθεί να αποκωδικοποιήσει το κλειδί που χρησιμοποιείται κατά την κρυπτογράφηση μιας επικοινωνίας και κατ' επέκταση το περιεχόμενό της.

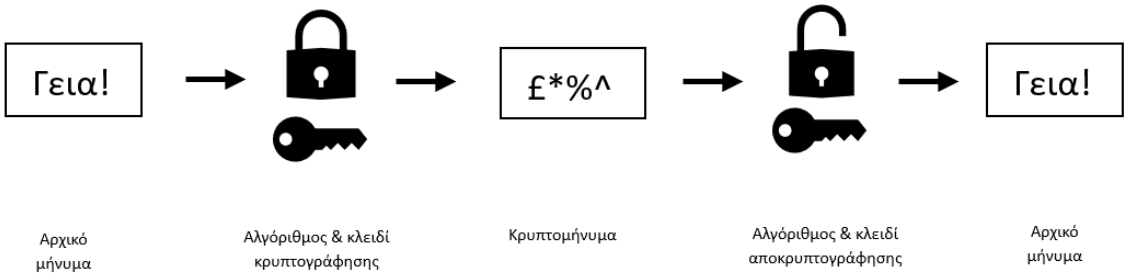
Σε αυτό το σημείο θα πρέπει να διαχωρίσουμε την κρυπτανάλυση από την αποκρυπτογράφηση, διότι παρόλο που και οι δύο αφορούν την αποκωδικοποίηση ενός κρυπτογραφημένου μηνύματος (αγγλ. cipher), στην αποκρυπτογράφηση η ανάκτηση της αρχικής επικοινωνίας γίνεται από εξουσιοδοτημένο δρώντα, ενώ στην κρυπτανάλυση αναφερόμαστε σε παραβίαση της επικοινωνίας (Μαυρίδης, 2016a). Τέλος, με τον όρο στεγανογραφία εννοούμε την πρακτική της απόκρυψης ενός μηνύματος μέσα σε μια

[100] Βλ. Άρθρα 3 έως και 14 του Ν. 4961/2022: Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις, 2022

φαινομενικά μη κρυπτογραφημένη επικοινωνία. Σκοπός της στεγανογραφίας είναι να αποκρύψει όχι μόνο το περιεχόμενο ενός μηνύματος αλλά και την ίδια την ύπαρξη του – αυτό αποτελεί και τη βασική της διαφορά από την κρυπτογραφία (Μαυρίδης, 2016a).

Σε αυτήν την ενότητα, το ενδιαφέρον μας θα εστιαστεί κυρίως στην κρυπτογράφηση και λιγότερο στην κρυπτανάλυση, ενώ η στεγανογραφία δε θα μας απασχολήσει καθόλου. Η χρησιμότητα της κρυπτογράφησης έχει εντοπιστεί εδώ και χιλιάδες χρόνια, ενώ διάφορες μέθοδοι της για την εγγύηση της μυστικότητας των επικοινωνιών έχουν βρει εφαρμογή σε περιστάσεις που την απαιτούσαν όπως π.χ. πόλεμοι (Μαυρίδης, 2016a). Σήμερα, η κρυπτογράφηση είναι θεμελιώδες χαρακτηριστικό των πληροφοριακών συστημάτων, καθώς είναι ένα μέσο για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας[101] των δεδομένων πάνω στα οποία χρησιμοποιείται.

Ο τρόπος που κρυπτογραφείται ένα σύνολο δεδομένων εξαρτάται από τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται (βλ. ενότητα 4.1) και μπορεί να διαφέρει ανάλογα την περίσταση. Σε γενικές γραμμές, αν λάβουμε υπόψη πως σε ένα κρυπτογραφικό σύστημα απαιτούνται το αρχικό μήνυμα, ο αλγόριθμος (απο)κρυπτογράφησης με το κλειδί του και το κρυπτομήνυμα, μια απλή διαδικασία κρυπτογράφησης θα έμοιαζε ως εξής:

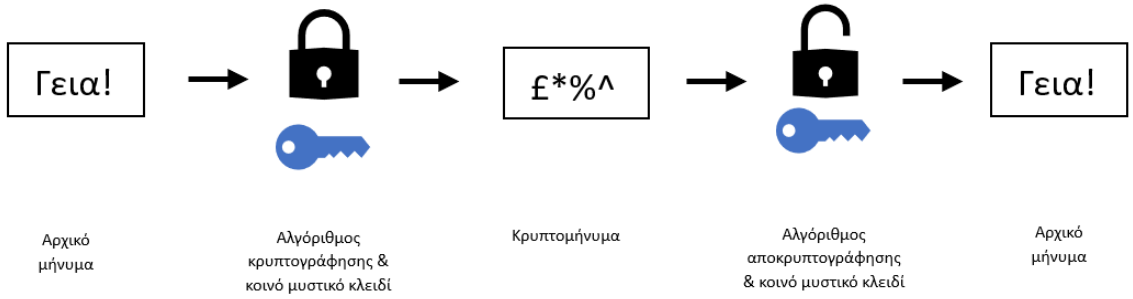


Εικόνα 1: Μια τυπική διαδικασία (απο)κρυπτογράφησης

Σύμφωνα με τον Μαυρίδη (2016a), οι αλγόριθμοι κρυπτογράφησης μπορούν να καταταχθούν είτε ως προς το κλειδί κρυπτογράφησης που χρησιμοποιούν (συμμετρικοί – ασύμμετροι), είτε ως προς τον τρόπο με τον οποίο επεξεργάζονται τα δεδομένα (δέσμης – ροής). Στις ηλεκτρονικές επικοινωνίες (είτε αναφερόμαστε σε ηλεκτρονική αλληλογραφία είτε σε ζωντανό διάλογο), η διάκριση των αλγορίθμων γίνεται κυρίως βάσει του κλειδιού κρυπτογράφησης. Έτσι, στις επόμενες γραμμές θα περιγράψουμε τη διαφορά μεταξύ συμμετρικών και ασύμμετρων αλγορίθμων (απο)κρυπτογράφησης.

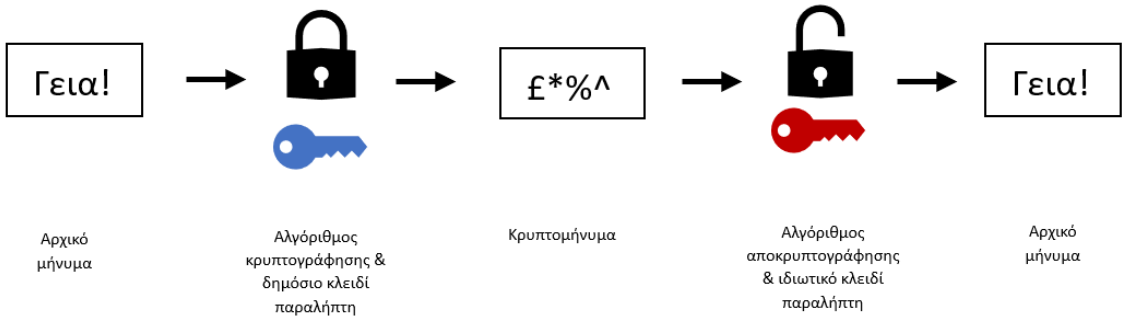
[101] Αναφερόμαστε στο μοντέλο CIA (confidentiality, integrity, availability) (Hashemi-Pour & Chai, 2023)

Συμμετρικοί ονομάζονται οι αλγόριθμοι που χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων. Στη συμμετρική κρυπτογράφηση, το κλειδί για την επικοινωνία θα πρέπει να διατηρείται ασφαλές και μη προσβάσιμο από τρίτους, για αυτό και η συμμετρική ονομάζεται και κρυπτογραφία μυστικού κλειδιού (Μαυρίδης, 2016a). Έτσι, σε μια τυπική αποστολή δεδομένων, ο αποστολέας θα χρησιμοποιήσει το κρυφό κλειδί ώστε να αποστείλει το κρυπτομήνυμα στον παραλήπτη, ο οποίος θα το αποκρυπτογραφήσει χρησιμοποιώντας το ίδιο κλειδί, όπως φαίνεται σχηματικά και στην παρακάτω εικόνα:



Εικόνα 2: Συμμετρική κρυπτογράφηση μηνύματος

Αντίθετα, στην ασύμμετρη κρυπτογράφηση χρησιμοποιούνται δύο διαφορετικά κλειδιά: ένα δημόσιο για την κρυπτογράφηση των δεδομένων και ένα ιδιωτικό για την αποκρυπτογράφηση τους (Μαυρίδης, 2016a). Η μέθοδος αυτή ονομάζεται και κρυπτογραφία δημόσιου κλειδιού, καθώς το κλειδί κρυπτογράφησης του παραλήπτη πρέπει να είναι γνωστό στον αποστολέα για τη μετατροπή του μηνύματος. Ο αποστολέας, χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη κρυπτογραφεί το μήνυμα και στέλνει το κρυπτομήνυμα στον παραλήπτη, ενώ ο τελευταίος, χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να το αποκρυπτογραφήσει (Μαυρίδης, 2016a). Σχηματικά, η ασύμμετρη κρυπτογραφία παρουσιάζεται στην παρακάτω εικόνα:



Εικόνα 3: Ασύμμετρη κρυπτογράφηση μηνύματος

Η ασύμμετρη κρυπτογραφία παρέχει συγκριτικό πλεονέκτημα έναντι της συμμετρικής στον τομέα της ασφάλειας των δεδομένων, καθώς με τη χρήση του δημόσιου κλειδιού του παραλήπτη είναι αδύνατη η αποκρυπτογράφηση των δεδομένων με

διαφορετικό κλειδί πέρνα του ιδιωτικού που αποτελεί το ζευγάρι του (Μαυρίδης, 2016a). Επίσης, γνωρίζοντας το δημόσιο κλειδί του παραλήπτη, ένας τρίτος δεν μπορεί να υπολογίσει την τιμή του ιδιωτικού του κλειδιού, κάτι το οποίο καθιστά ασφαλή και τη δημοσιοποίησή του (Μαυρίδης, 2016a).

Από την άλλη, η συμμετρική κρυπτογράφηση υπερέχει της ασύμμετρης όσον αφορά την ταχύτητα με την οποία μπορεί να ολοκληρωθεί, καθώς και στους υπολογιστικούς πόρους που αυτή καταναλώνει, οι οποίοι είναι σαφώς λιγότεροι από της ασύμμετρης ('Difference Between Symmetric and Asymmetric Key Encryption', 2023). Ανάλογα με τη χρήση για την οποία προορίζονται, και οι δυο κρυπτογραφικές προσεγγίσεις φέρουν πλεονεκτήματα και δυσκολίες. Έτσι, αξιοποιώντας τις δυνατότητες και των δυο, διαχρονικά έχουν υιοθετηθεί υβριδικά συστήματα κρυπτογράφησης που εμφανίζουν χαρακτηριστικά τόσο συμμετρικού, όσο και ασύμμετρου τύπου κλειδιού – όπως π.χ. το σύστημα Pretty Good Privacy - PGP (Buckbee, 2023).

Στην επόμενη ενότητα θα αναφερθούμε στους ευρύτερα χρησιμοποιούμενους αλγόριθμους συμμετρικής και ασύμμετρης κρυπτογράφησης, στον τρόπο λειτουργίας τους, τις πιθανές τους ευπάθειες και τη χρήση τους στην αγορά και τις ηλεκτρονικές επικοινωνίες.[102]

4.1 Σύγχρονες μέθοδοι κρυπτογράφησης, παρεχόμενη ασφάλεια και χρήση τους στην αγορά

4.1.1 Συμμετρική Κρυπτογράφηση

4.1.1.1 Κρυπτογράφηση Data Encryption Standard (DES)

Ο αλγόριθμος κρυπτογράφησης που αργότερα θα καταχωρούνταν ως Data Encryption Standard (DES), έχει τις ρίζες του στο 1974, όπου μετά από ανοιχτή πρόσκληση του αμερικανικού φορέα NBS (πλέον μετονομασθείς σε NIST), κατατέθηκε η πρόταση συμμετρικού αλγορίθμου από την εταιρία IBM με το όνομα Lucifer (Simmons, 2024). Ο κατατεθείς αλγόριθμος, είχε αρχικό κλειδί μήκους 128 bit, όμως μετά από

[102] Ορισμένοι από τους αλγόριθμους παρουσιάζουν στοιχεία τόσο συμμετρικής, όσο και ασύμμετρης κρυπτογράφησης, και εύλογα μπορεί να δημιουργηθεί απορία στον αναγνώστη για το κριτήριο της ταξινόμησής τους. Η κατάταξη στη μια η την άλλη ομάδα αλγορίθμων έγινε βάσει της κρυπτογραφικής λογικής τους και της σχέσης τους με άλλους αλγόριθμους της ίδιας κατηγορίας. Ορισμένοι αλγόριθμοι αποτελούν προέκταση άλλων στην εφαρμογή τους, οπότε παρουσιάζονται και εντός της ίδιας ομάδας.

διαβουλεύσεις του NBS με την αμερικανική NSA, το τελικό κλειδί του αλγορίθμου ορίστηκε σε μήκος 56 bit (Μαυρίδης, 2016b; Simmons, 2024). Ο αλγόριθμος DES υιοθετήθηκε ως επίσημο πρότυπο από το NBS το 1977 και έκτοτε χρησιμοποιήθηκε για την κρυπτογράφηση κυρίως μη διαβαθμισμένων (και ορισμένων κατά περίπτωση διαβαθμισμένων) πληροφοριών του αμερικανικού κράτους, συμπεριλαμβανομένων πληροφοριών σχετικά με οικονομικές συναλλαγές (Simmons, 2024). Σταδιακά, ο αλγόριθμος DES υιοθετήθηκε και από άλλους οργανισμούς προτυποποίησης ανά τον κόσμο, και εξαπλώθηκε ως πρακτική στην εξασφάλιση της προστασίας δεδομένων (Simmons, 2024).

Η λειτουργία του αλγορίθμου DES περιλαμβάνει τα παρακάτω στοιχεία (Μαυρίδης, 2016b):

- Ένα αρχικό κλειδί κρυπτογράφησης μήκους 56 bit,
- Μικρές δέσμες δεδομένων στις οποίες είχε χωριστεί το σύνολο των αρχικών δεδομένων προς κρυπτογράφηση, μήκους 64 bit η κάθε μια,
- 16 κύκλους κρυπτογράφησης στους οποίους υποβάλλεται η κάθε δέσμη δεδομένων σύμφωνα με τη δομή Feistel (Μαυρίδης, 2016a),
- 16 υποκλειδιά μήκους 48 bit έκαστο, ένα για κάθε κύκλο κρυπτογράφησης, τα οποία προκύπτουν από το αρχικό κλειδί κρυπτογράφησης
- Χρήση της μετάθεσης δεδομένων, η οποία λαμβάνει χώρα μόλις τα δεδομένα χωριστούν σε δέσμες των 64 bit και πριν αρχίσει ο πρώτος κύκλος κρυπτογράφησης, όπως επίσης και μετά τον τελευταίο γύρο κρυπτογράφησης.

Συνοπτικά, τα βήματα που ακολουθεί ο αλγόριθμος DES για την κρυπτογράφηση ενός συνόλου δεδομένων, μπορούν να περιγραφτούν ως εξής:

1. Αρχικά, τα δεδομένα προς κρυπτογράφηση χωρίζονται σε δέσμες των 64 bit.
2. Οι δέσμες των ακρυπτογράφητων δεδομένων υφίστανται μια αρχική μετάθεση ώστε να μην μπορούν να παρατηρηθούν μοτίβα δεδομένων από τον κρυπταναλυτή.
3. Μόλις η αρχική μετάθεση ολοκληρωθεί, τα δεδομένα χωρίζονται σε δύο μέρη (αριστερό και δεξί), των 32 bit έκαστο.

4. Το κάθε αριστερό και το κάθε δεξί μέρος, περνάνε από 16 κύκλους κρυπτογράφησης, χρησιμοποιώντας τα 16 υποκλειδιά[103] και επιπλέον μεταθέσεις[104]
5. Τέλος, το αριστερό και το δεξί μέρος της δέσμης επανενώνονται και ακολουθείται ακόμη μια λειτουργία μετάθεσης στην τελική δέσμη, με αποτέλεσμα να έχουμε ένα κρυπτοκείμενο των 64 bit, όπως ακριβώς με το αρχικό.

Για την αποκρυπτογράφηση του κρυπτοκειμένου, ακολουθείται ακριβώς η ίδια διαδικασία από την ανάποδη, το οποίο συνεπάγεται πως το 16^{ο} υποκλειδί θα χρησιμοποιηθεί πρώτο και το 1^{ο} θα χρησιμοποιηθεί τελευταίο στα βήματα του αλγορίθμου.

Τα 56 bit αρχικού κλειδιού ίσως καθιστούσαν τον αλγόριθμο κρυπτογραφικά ισχυρό την εποχή που υιοθετήθηκε. Η ανάπτυξη της τεχνολογίας, με την ευρέως διαθέσιμη υπολογιστική ισχύ όλο και να αυξάνεται, κατέστησε τον αλγόριθμο DES παρωχημένο για τον λόγο που αρχικά εφαρμόστηκε. Οι επιθέσεις εξαντλητικής αναζήτησης (bruteforce) έγιναν όλο και πιο ρεαλιστικό σενάριο και αυτό οδήγησε στην ανάγκη για ανάπτυξη ισχυρότερων μεθόδων κρυπτογράφησης. Έτσι, μια μετεξέλιξη του DES είναι ο αλγόριθμος 3DES (τριπλό DES), ο οποίος αφού δημιουργήσει το αρχικό κρυπτοκείμενο, έπειτα το αποκρυπτογραφεί και το επανακρυπτογραφεί χρησιμοποιώντας συνολικά δύο ή τρία (και οι δύο περιπτώσεις είναι εφαρμόσιμες) κλειδιά κρυπτογράφησης. Με την εφαρμογή του 3DES δύο κλειδιών, σε μια επίθεση εξαντλητικής αναζήτησης κλειδιού θα έπρεπε να αναζητηθούν 2^{112} πιθανοί συνδυασμοί, ενώ με τη χρήση τριών κλειδιών, ο αριθμός αυτός θα έφτανε τους 2^{168} (Μαυρίδης, 2016b).

Και πάλι, ο αλγόριθμος DES/3DES ενέχει σημαντικά μειονεκτήματα, κυρίως από πλευράς απαιτήσεων πόρων και απόδοσης, σε σύγκριση με τον διάδοχο του, τον AES. Στην επόμενη ενότητα θα συζητήσουμε το ζήτημα εκτενέστερα.

---

[103] Για τη δημιουργία των υποκλειδιών αναλυτικά, βλ. Μαυρίδης, Ι. (2016). Κεφάλαιο 7. Σύγχρονοι κρυπτογραφικοί αλγόριθμοι. Στο *Ασφάλεια πληροφοριών στο διαδίκτυο* (σσ. 129–158). http://repository.kallipos.gr/handle/11419/1024

[104] Για την αναλυτική διαδικασία της κρυπτογράφησης στον DES σύμφωνα με τη διάταξη Feistel, βλ. Μαυρίδης, Ι. (2016). Κεφάλαιο 6. Εισαγωγή στην κρυπτολογία. Στο *Ασφάλεια πληροφοριών στο διαδίκτυο* (σσ. 102–128). http://repository.kallipos.gr/handle/11419/1024

4.1.1.2 Κρυπτογράφηση Advanced Encryption Standard (AES)

Όπως αναφέρθηκε και παραπάνω, η ευρύτερη διάθεση όλο και μεγαλύτερης υπολογιστικής ισχύος οδήγησε στην ανάγκη δημιουργίας ενός ισχυρότερου αλγορίθμου κρυπτογράφησης. Καθοριστικός παράγοντας που οδήγησε τον φορέα NIST στην αναζήτηση κρυπτογραφικού αλγορίθμου ασφαλέστερου από τον DES, ήταν η πρώτη διάρρηξη του το 1997 (Kumar Jena, 2023)

Όπως μας αναφέρει και ο Μαυρίδης (Μαυρίδης, 2016b), ο νέος αλγόριθμος που αναζητήθηκε έπρεπε να πληροί τρία βασικά στοιχεία: πρώτον, να είναι ανοιχτού κώδικα, δεύτερον, να πρόκειται πάλι για αλγόριθμο ενός κλειδιού (άρα συμμετρικό), ο οποίος κρυπτογραφεί δεδομένα με τη μορφή δέσμης, και τέλος να μπορούν να υποστηριχθούν κλειδιά μήκους 128, 192 και 256 bit. Από την τελική αξιολόγηση διακρίθηκε ο αλγόριθμος Rijndael που ανέπτυξαν οι ερευνητές Vincent Rijmen και Joan Daemen, ο οποίος εν τέλει προτυποποιήθηκε ως Advanced Encryption Standard (AES) (National Institute of Standards and Technology, 2023a). Το AES δημοσιεύτηκε το 2001, ενώ αν λάβουμε υπόψη πως από το 1999, η προσπέλαση του DES ήταν δυνατή σε λιγότερο από μία ημέρα (Kumar Jena, 2023), είναι προφανές πόσο αναγκαία ήταν η δημιουργία του AES.

Στον αλγόριθμο AES, αντί για τη δομή λειτουργίας Feistel (βλ. παραπάνω στον DES), χρησιμοποιείται μια σειρά (ή αλλιώς δίκτυο) λειτουργιών που βασίζονται στην αντικατάσταση των αρχικών δεδομένων βάσει του υποκλειδιού και μετά τη μετάθεση τους, περνώντας τελικά στον επόμενο γύρο κρυπτογράφησης. Αναλυτικότερα, ο αλγόριθμος AES θα χωρίσει το αρχικό μας κείμενο σε δέσμες, μήκους 128 bit η καθεμιά. Μετέπειτα, θα τοποθετήσει τα δεδομένα από τις δέσμες σε πίνακες κατάστασης δύο διαστάσεων (states), με τον καθένα να περιλαμβάνει 16 byte[105] (Μαυρίδης, 2016b; Kumar Jena, 2023).

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Πίνακας 2: Απεικόνιση ενός πίνακα state, ο οποίος περιλαμβάνει 1 byte σε κάθε του κελί και συνολικά 16 bytes (128 bit).

[105] Να σημειώσουμε πως 16 byte αντιστοιχούν σε 128 bit, άρα σε κάθε δέσμη δεδομένων αντιστοιχεί ένας δισδιάστατος πίνακας.

Όπως και στον αλγόριθμο DES, έτσι και ο AES ακολουθεί έναν αριθμό κύκλων κρυπτογράφησης, αυτή τη φορά ανάλογα με το μήκος του κλειδιού. Ο προτυποποιημένος αλγόριθμος με αρχικό κλειδί 128 bit κρυπτογραφεί σε 10 κύκλους, ενώ στον αλγόριθμο Rijndael προβλέπονται επίσης 12 κύκλοι με κλειδί 192 bit και 14 κύκλοι με κλειδί μήκους 256 bit (Μαυρίδης, 2016b). Έτσι, μετά το χωρισμό του αρχικού συνόλου δεδομένων σε δέσμες και την κατάταξή τους σε states, ο αλγόριθμος δημιουργεί τα υποκλειδιά που θα χρησιμοποιηθούν στους κύκλους κρυπτογράφησης. Το πλήθος των υποκλειδιών ισούται με τον αριθμό των κύκλων κρυπτογράφησης συν 1 (λ.χ. για ένα κλειδί 192 bit θα δημιουργηθούν 13 υποκλειδιά).

Σε κάθε κύκλο κρυπτογράφησης, ο αλγόριθμος AES εργάζεται πάνω στο δυσδιάστατο state. Έχοντας πρώτα εφαρμόσει τη λογική λειτουργία XOR στο πρώτο υποκλειδί που δημιουργήθηκε (K_0), αντικαθιστά τα bytes ολόκληρου του πίνακα από το δυαδικό στο δεκαεξαδικό σύστημα (λειτουργία SubBytes), με αυτόν να διαμορφώνεται ως εξής:

C1	85	9A	4D
DA	AA	5F	2C
B5	AB	30	1D
F1	D2	BB	CF

Πίνακας 3: Παράδειγμα state μετά την λειτουργία SubBytes.

Στη συνέχεια, τα byte της κάθε σειράς μετακινούνται προς τα αριστερά, τόσες θέσεις όσες προβλέπονται για την κάθε σειρά (λειτουργία ShiftRows). Στην πρώτη σειρά δεν μετακινείται κανένα byte, στη δεύτερη τα bytes μετακινούνται 1 θέση αριστερά, στην τρίτη σειρά 2 θέσεις αριστερά και στην τέταρτη σειρά 3 θέσεις αριστερά. Έτσι, με την ολοκλήρωση της λειτουργίας ShiftRows, ο παραπάνω πίνακας θα έμοιαζε ως εξής:

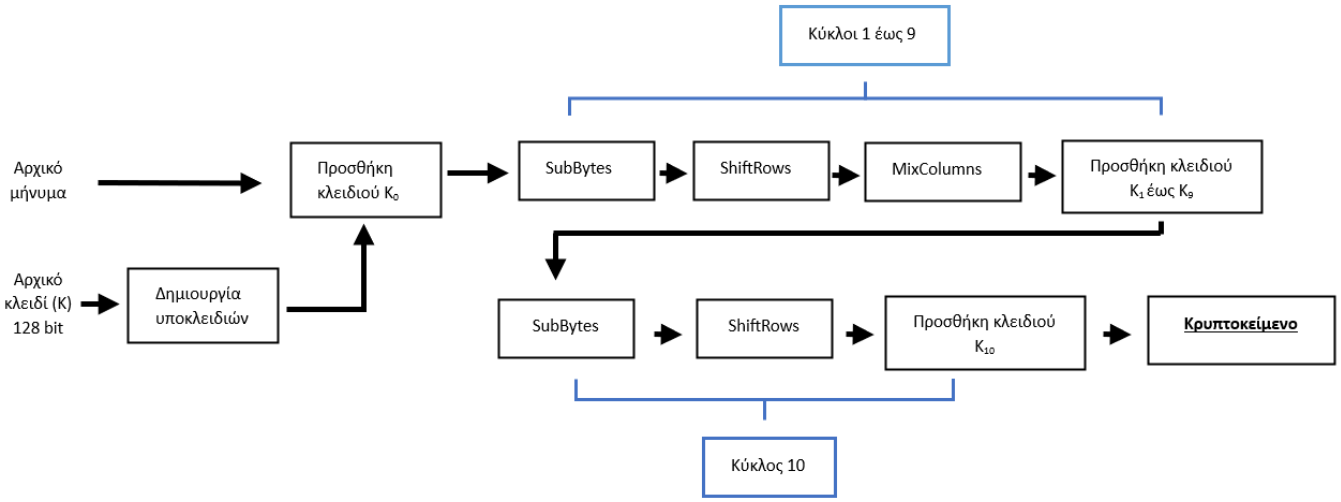
C1	85	9A	4D
AA	5F	2C	DA
30	1D	B5	AB
CF	F1	D2	BB

Πίνακας 4: Παράδειγμα state μετά την λειτουργία ShiftRows.

Μετέπειτα, ο αλγόριθμος προχωράει στη λειτουργία MixColumns, όπου κάθε στήλη του πίνακα state θα πολλαπλασιαστεί με έναν συγκεκριμένο σταθερό πίνακα τιμών,

δίνοντας στο τέλος έναν νέο state με σκοπό τη δημιουργία σύγχυσης στα δεδομένα εντός του δισδιάστατου πίνακα. Η σύγχυση αυτή στοχεύει στο να κάνει δυσκολότερη την αποκρυπτογράφηση του κρυπτοκειμένου. Η λειτουργία αυτή λαμβάνει χώρα σε όλους τους κύκλους κρυπτογράφησης εκτός από τον τελευταίο. Ο βηματισμός του AES ολοκληρώνεται με ακόμη μια λογική λειτουργία XOR στο υποκλειδί του κύκλου κρυπτογράφησης (K_n). Ο τελικός πίνακας κατάστασης αποτελεί το κρυπτοκείμενο της συγκεκριμένης δέσμης δεδομένων. Οι τελικές κρυπτοδέσμες ενώνονται ώστε να αποτελέσουν το συνολικό κρυπτοκείμενο. Η διαδικασία της αποκρυπτογράφησης, όπως και στον DES, αντιστοιχεί στην αντίστροφη εκτέλεση των βημάτων του αλγορίθμου (Μαυρίδης, 2016b).

Ο τρόπος λειτουργίας του αλγόριθμου AES με ένα ενδεικτικό κλειδί 128 bit θα μπορούσε να απεικονιστεί ως εξής:



Εικόνα 4: Βήματα αλγορίθμου AES με κλειδί 128 bit.

Σήμερα, ο αλγόριθμος AES βρίσκει εφαρμογή σε διάφορους τομείς της πληροφορικής, όπως στην κρυπτογράφηση ασύρματων δικτύων (λ.χ. στα δίκτυα WiFi), στην αυθεντικοποίηση διακομιστών για την ασφαλέστερη περιήγηση στον ιστό (λ.χ. στα πρωτόκολλα SSL/TLS), στην κρυπτογράφηση αρχείων για την αποστολή τους μέσω του διαδικτύου, όπως και στην προστασία υλισμικού όπως οι επεξεργαστές (Kumar Jena, 2023).

Παρόλο που βασίζεται σε αλγεβρικές πράξεις εντός των πινάκων κατάστασης (γεγονός που θα μπορούσε να τον κάνει ευάλωτο σε ορισμένα είδη επιθέσεων και στην παρατήρηση μοτίβων εντός των κρυπτομηνυμάτων), ο AES θεωρείται ένας από τους ασφαλέστερους αλγορίθμους μέχρι σήμερα, έχοντας αντικαταστήσει τον DES στην

πλειονότητα των εφαρμογών, και όχι άδικα: η de facto χρήση μεγαλύτερου κλειδιού και η ευελιξία για το μέγεθός του το κάνουν μακράν ασφαλέστερο, ενώ η δυνατότητά του να κρυπτογραφεί μεγαλύτερες δέσμες δεδομένων σε μικρότερο αριθμό κύκλων από τον DES δημιουργούν μεγαλύτερη ταχύτητα και αποδοτικότητα (‘Difference between AES and DES Ciphers’, 2018).

4.1.1.3 Κρυπτογράφηση Blowfish & Twofish

Ένας ακόμη συμμετρικός αλγόριθμος, άξιος αναφοράς στο πεδίο της κρυπτογραφίας είναι ο Blowfish, ο οποίος δημιουργήθηκε από τον Bruce Schneier το 1993 (Acharya, 2020). Ο εν λόγω αλγόριθμος αρχικά δημοσιεύτηκε ως μια εναλλακτική στον DES, καθώς είναι πολύ πιο γρήγορος και αρκετά ασφαλέστερος – αξίζει να σημειώσουμε πως μέχρι σήμερα δεν έχει βρεθεί κρυπταναλυτική μέθοδος που να παραβιάζει κρυπτομηνύματα blowfish. Σε αντίθεση με άλλους αλγορίθμους, Blowfish είναι ελεύθερα διαθέσιμος για όποιον θέλει να τον χρησιμοποιήσει, καθώς ο εφευρέτης του δεν προχώρησε στην έκδοση διπλώματος ευρεσιτεχνίας (‘Blowfish Algorithm with Examples’, 2019).

Ως προς τη μεθοδολογία του, ο Blowfish είναι παρεμφερής με τον DES, από την άποψη ότι και εδώ έχουμε να κάνουμε για αλγόριθμο δέσμης μήκους 64 bit, η οποία χωρίζεται σε δύο υποδέσμες των 32 bit, μια αριστερή και μια δεξιά. Επίσης, ο Blowfish χρησιμοποιεί και αυτός τη διάταξη Feistel, με 16 γύρους κρυπτογράφησης (‘Blowfish Algorithm with Examples’, 2019).

Παρ’ όλα αυτά, υπάρχουν και σημαντικές διαφορές μεταξύ αυτού του αλγόριθμου και του DES, και είναι ακριβώς αυτές που δημιουργούν την υπεροχή του. Για παράδειγμα, το αρχικό κλειδί στον αλγόριθμο DES είναι αυστηρά 56 bits, ενώ στον Blowfish μπορεί να μεταβάλλεται από 32 bit μέχρι 448 bit, κάνοντας τον πιο ευέλικτο και δίνοντας τη δυνατότητα προσαρμογής του μήκους κλειδιού (άρα και τους πόρους που θα απαιτηθούν) στον ευαίσθητο χαρακτήρα των δεδομένων προς κρυπτογράφηση.

Τα 18 υποκλειδιά του (ας θυμηθούμε πως ο DES παράγει 16 υποκλειδιά) αποθηκεύονται σε έναν πίνακα “P’’ κατά την έναρξη της αλγοριθμικής ακολουθίας, βασιζόμενα στο αρχικό κλειδί. Πέραν αυτών, όμως, η κυριότερη διαφορά μεταξύ των δύο μεθόδων είναι πως στον Blowfish περιλαμβάνεται και ένα σύνολο 4 πλαισίων (πινάκων) αντικατάστασης, με το καθένα να περιλαμβάνει 512 στοιχεία μήκους 32 bit το καθένα. Η σημασία των πλαισίων αντικατάστασης είναι μεγάλη, καθώς στοιχεία και από τα τέσσερα

χρησιμοποιούνται σε κάθε γύρο κρυπτογράφησης ως μέρος μιας συνάρτησης σε συνδυασμό με το αντίστοιχο υποκλειδί. Με την ολοκλήρωση όλων των κύκλων κρυπτογράφησης, λαμβάνει χώρα μια τελευταία επεξεργασία που τοποθετεί στη σειρά τις κρυπτογραφημένες δέσμες και μας δίνει το τελικό κρυπτοκείμενο μήκους 64 bit.

Αν και ορθώς αναφέρθηκε πως ο Blowfish είναι σημαντικά γρηγορότερος από τον DES, οφείλουμε να επισημάνουμε πως εκτός από τα υποκλειδιά, το αρχικό κλειδί επηρεάζει και τις τιμές στα πλαίσια αντικατάστασης. Έτσι, κάθε φορά που το αρχικό κλειδί αλλάζει, η διαδικασία συμπαρασύρει και τα υπόλοιπα στοιχεία του αλγορίθμου, μειώνοντας στην αρχή την ταχύτητα λειτουργίας του (‘Blowfish Algorithm with Examples’, 2019). Συν τοις άλλοις, παρόλο που ο αλγόριθμος μέχρι στιγμής δεν έχει κρυπταναλυθεί, το γεγονός ότι το μήκος κάθε δέσμης που κρυπτογραφεί είναι 64 bit, θεωρητικά δημιουργεί μια ευαλωτότητα απέναντι σε επιθέσεις εξαντλητικής αναζήτησης (bruteforce). Για να αντιμετωπιστεί αυτή η πιθανότητα ευάλωτου σημείου, ο Bruce Schneier δημοσίευσε το 1998 μια νέα έκδοση του αλγορίθμου με το όνομα **Twofish** (Zahorski, 2022). Η βασική του καινοτομία σε σχέση με τον Blowfish είναι πως αυτή τη φορά χρησιμοποιείται δέσμη 128 bit και κλειδί έως 256 bit, κάνοντας τον Twofish ακόμη τόσο ασφαλή, που ορισμένοι ακαδημαϊκοί τον θεωρούν ασφαλέστερο από τον AES (Zahorski, 2022).

Παρόλο που δεν είναι η τελευταία λέξη της τεχνολογίας, τόσο ο αλγόριθμος Blowfish όσο και ο Twofish χρησιμοποιούνται σε εφαρμογές και συστήματα προκειμένου να κρυπτογραφηθούν αρχεία, κωδικοί πρόσβασης και ηλεκτρονικές επικοινωνίες (‘Blowfish Algorithm with Examples’, 2019; Zahorski, 2022).

4.1.2 Ασύμμετρη Κρυπτογράφηση

4.1.2.1 Κρυπτογράφηση RSA

Ο αλγόριθμος δημόσιου κλειδιού RSA παρουσιάστηκε το 1978 (‘RSA Full Form’, 2022) και πήρε το όνομα του από τους από τους επιστήμονες που τον ανέπτυξαν: τους Ron Rivest, Adi Shamir και Leonard Adlemar, του Massachusetts Institute of Technology (MIT) (Luo κ.ά., 2023). Ο τρόπος λειτουργίας του έχει περιγραφτεί εν πολλοίς στην εισαγωγή του Κεφαλαίου 4. Συνοπτικά, για την επικοινωνία μεταξύ δύο μερών, δημιουργούνται δύο ζευγάρια κλειδιών (1 ζευγάρι για τον αποστολέα και 1 για τον παραλήπτη). Στο κάθε ζευγάρι, το ένα κλειδί είναι δημόσια διαθέσιμο και χρησιμοποιείται από όποιον θέλει να στείλει κρυπτογραφημένο μήνυμα στον κάτοχό του, ενώ το άλλο είναι

ιδιωτικό και χρησιμοποιείται από τον κάτοχο του κλειδιού για την αποκρυπτογράφηση του εισερχόμενου μηνύματος (Luo κ.ά., 2023) (βλ. Εικόνα 3). Ο αλγόριθμος βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών για να ενισχύσει την ασφάλειά του, και ενώ θεωρητικά θα ήταν εφικτό να βρεθεί το ιδιωτικό κλειδί χρησιμοποιώντας ως βάση το δημόσιο, στην πράξη αυτό είναι εξαιρετικά δύσκολο (Guru, 2019), κάνοντας τον αλγόριθμο RSA έναν από τους πλέον αξιόπιστους στην κρυπτογράφηση για την ανταλλαγή δεδομένων. Σε αυτό συμβάλλουν η αποτελεσματικότητα του μεταξύ των χρηστών που διαθέτουν τα κλειδιά (από)κρυπτογράφησης, η ανακτησιμότητα του αρχικού κειμένου εφόσον η (από)κρυπτογράφηση του κρυπτοκειμένου γίνει σωστά, και η υπολογιστική δυσκολία στην αποκρυπτογράφηση του κρυπτοκειμένου από κακόβουλο τρίτο χωρίς την κατοχή του ιδιωτικού κλειδιού του παραλήπτη (Luo κ.ά., 2023).

Η χρήση του αλγορίθμου RSA εμφανίζεται σε διάφορες εφαρμογές της κρυπτογραφίας που έχουν σκοπό την ιδιωτικότητα, την ασφάλεια και την επαλήθευση δεδομένων. Ορισμένες από αυτές είναι:

- Έκδοση ψηφιακών υπογραφών: τα δημόσια και ιδιωτικά κλειδιά του RSA μπορούν να αξιοποιηθούν για την επαλήθευση της ακεραιότητας των δεδομένων και της ταυτότητας του κατόχου μιας ψηφιακής υπογραφής (Wickramasinghe, 2023),
- Έκδοση ψηφιακών πιστοποιητικών: όπως και στις ψηφιακές υπογραφές, ο αλγόριθμος RSA χρησιμοποιείται και για την επαλήθευση της ταυτότητας μιας ιστοσελίδας μέσω ψηφιακών πιστοποιητικών, όπως για παράδειγμα των Secure Socket Layer (SSL) (Wickramasinghe, 2023)
- Ανταλλαγή μηνυμάτων μέσω ασφαλών καναλιών επικοινωνίας: η ασφαλής επικοινωνία μεταξύ φυλλομετρητών (browsers) και εξυπηρετητών (servers) πολλές φορές βασίζεται σε πρωτόκολλα που χρησιμοποιούν την RSA κρυπτογράφηση (Wickramasinghe, 2023). Επίσης, η λογική του RSA χρησιμοποιείται κατά κόρων (τις περισσότερες φορές συνδυαστικά με αλγόριθμους συμμετρικής κρυπτογράφησης) στην ανταλλαγή μηνυμάτων επικοινωνίας μεταξύ χρηστών – μια πολύ γνωστή εφαρμογή είναι η Pretty Good Privacy (PGP), η οποία δημιουργήθηκε από τον μηχανικό λογισμικού Phil Zimmermann το 1991 (Bone, 2023).

Όπως κάθε αλγόριθμος, έτσι και ο RSA αντιμετωπίζει ορισμένο επίπεδο ρίσκου, το οποίο μπορεί να οφείλεται σε παράγοντες όπως η λανθασμένη εφαρμογή του αλγορίθμου

(λ.χ. εντοπισμός συσχετίσεων στους αρχικούς αριθμούς που χρησιμοποιούνται για τη δημιουργία του ζεύγους κλειδιών, οι οποίοι κανονικά θα έπρεπε να είναι επαρκώς τυχαίοι, είτε ανεπάρκεια στο μήκος του κλειδιού που αναπόφευκτα χαμηλώνει και το επίπεδο ασφάλειας της κρυπτογράφησης), η πλημμελής αποθήκευση και προστασία των μυστικών κλειδιών, ή ακόμα και επιθέσεις πλευρικού καναλιού, οι οποίες αναλύουν παράγωγα της αλγοριθμικής λειτουργίας για τον εντοπισμό μοτίβων και προσδιορισμό του μυστικού κλειδιού (τέτοια παράγωγα μπορεί να είναι ο χρόνος που χρειάζεται για να κρυπτογραφηθεί ένα μήνυμα, ο οποίος είναι ανάλογος του μήκους του κλειδιού, είτε τα ηλεκτρομαγνητικά κύματα που παράγει μια συσκευή την ώρα που εκτελεί κρυπτογράφηση) (Wickramasinghe, 2023).

4.1.2.2 Κρυπτογράφηση Diffie – Hellman

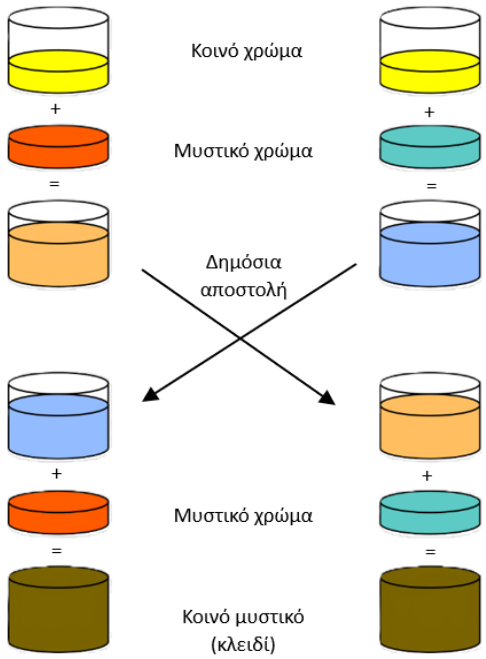
Η κρυπτογράφηση Diffie – Hellman ουσιαστικά προηγείται χρονικά και νοηματικά του αλγορίθμου RSA. Το 1976, οι Whitfield Diffie και Martin E. Hellman, δημοσιεύουν ένα άρθρο σε επιστημονική έκδοση, στο οποίο περιγράφουν μια νέα προσέγγιση στην κρυπτογραφία. Οι συγγραφείς αναγνωρίζουν πως η περίοδος που διένυαν χαρακτηριζόταν από τη ραγδαία ανάπτυξη των δικτύων τηλεπικοινωνιών, και πως όσο αυτή η ανάπτυξη προχωρούσε, το προαπαιτούμενο της ύπαρξης ενός ασφαλούς καναλιού για την ανταλλαγή κλειδιών κρυπτογράφησης μεταξύ των μερών θα γινόταν όλο και δυσκολότερο να επιτευχθεί (Diffie & Hellman, 1976).

Θέτοντας ως παραδοχή την ανάπτυξη «εκτεταμένων, ασφαλών, συστημάτων τηλεπικοινωνιών» (Diffie & Hellman, 1976), εκφράζουν για πρώτη φορά τον όρο ‘κρυπτογραφία ανοιχτού κλειδιού’, την οποία και αναλύουν. Στόχος της προσέγγισης είναι η απεξάρτηση της αποτελεσματικής κρυπτογράφησης από την προϋπόθεση ύπαρξης ενός ασφαλούς καναλιού επικοινωνίας μεταξύ των συσκευών, και η εγκαθίδρυση του ίδιου επιπέδου κρυπτογραφικής ασφάλειας και κρυπταναλυτικής δυσκολίας, ακόμα και με τη χρήση μη ασφαλών καναλιών. Ουσιαστικά, η πρόταση των συγγραφέων στόχευε στην ασφαλή ανταλλαγή ενός ‘κοινού μυστικού’ (ή αλλιώς κλειδιού κρυπτογράφησης), το οποίο θα χρησιμοποιούνταν αργότερα για την ανταλλαγή μηνυμάτων με συμμετρικό τρόπο κρυπτογράφησης, ακόμη κι αν η μεταφορά του έγινε μέσω δικτύου που δεν προστατεύει τα δεδομένα που ανταλλάσσονται.

Ο τρόπος λειτουργίας της κρυπτογράφησης ανοιχτού κλειδιού περιγράφτηκε νωρίτερα σε αυτό το κεφάλαιο. Αξίζει όμως, να δούμε τα βήματα που ακολουθούνται κατά

Diffie & Hellman στην ανταλλαγή πληροφοριών δημόσιου κλειδιού, χρησιμοποιώντας χρώματα αντί για μεγάλες αριθμητικές ακολουθίες, όπως εξηγεί στη σχετική παρουσίασή του ο Vinck (2012): Ας υποθέσουμε ότι έχουμε δύο άτομα, την Αλίκη και τον Βασίλη, οι οποίοι θέλουν να χρησιμοποιήσουν ένα χρώμα ως το κλειδί για την κρυπτογραφημένη συνομιλία τους. Αρχικά, **(1)** θα ορίσουν και οι δύο ένα τυχαίο κοινό χρώμα, το οποίο θα είναι ελεύθερα διαθέσιμο και ένα μυστικό χρώμα, διαφορετικό για τον καθένα. **(2)** Ο συνδυασμός του κοινού και του μυστικού χρώματος για τον καθένα θα οδηγήσει σε ένα τρίτο χρώμα, προφανώς διαφορετικό και για τους δυο. **(3)** Έπειτα, το τρίτο χρώμα της Αλίκης μπορεί να σταλεί στον Βασίλη και το αντίστροφο, ακόμη και αν κάποιος κακόβουλος τρίτος παρακολουθεί αυτήν την ανταλλαγή, καθώς, μετά τον συνδυασμό των δύο αρχικών χρωμάτων, ο διαχωρισμός του νέου χρώματος στα συστατικά του είναι πρακτικά ασύμφορος. Έτσι, έχοντας μόνο το κοινό χρώμα και το τρίτο, δεν είναι εφικτό να υπολογιστεί το μυστικό χρώμα των μερών μας. **(4)** Αφού η Αλίκη λάβει το τρίτο χρώμα του Βασίλη, το συνδυάζει με το δικό της μυστικό χρώμα, και αντίστοιχα πράττει και ο Βασίλης. **(5)** Ως αποτέλεσμα παίρνουμε ένα κοινό χρώμα που προκύπτει και στους δυο, και αποτελεί το μυστικό κλειδί το οποίο τώρα μπορούν να χρησιμοποιούν για να κρυπτογραφούν τη συνομιλία τους συμμετρικά.

Εικόνα 5: Επεξήγηση της λειτουργίας ανταλλαγής δημόσιου κλειδιού Diffie - Hellman κατά τον Vinck. (Προσαρμογή στην ελληνική γλώσσα)



Παρόλο που χρησιμοποιείται για την δημιουργία ενός μυστικού κλειδιού μεταξύ δύο μερών, η κρυπτογράφηση Diffie – Hellman έχει χρησιμοποιηθεί ως βάση για την ανάπτυξη αλγορίθμων που αξιοποιούν τη δημόσια ανταλλαγή κλειδιού, σε συνδυασμό με τη συμμετρική κρυπτογράφηση. Όπως έχει ήδη αναφερθεί, ο αλγόριθμος RSA είναι ένα από τα σημαντικότερα παραδείγματα, ο οποίος παρόλα αυτά εμφανίζει σημαντικές διαφορές με τον υπό εξέταση αλγόριθμο (‘Difference Between Diffie-Hellman and RSA’, 2023). Για αυτόν το λόγο και για τη μεθοδολογική του συνάφεια, ο αλγόριθμος Diffie - Hellman ταξινομείται μεταξύ των μεθόδων ασύμμετρης κρυπτογράφησης.

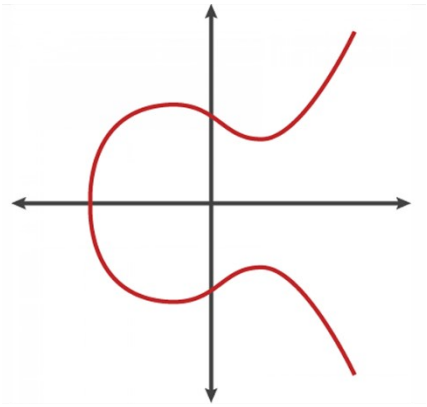
4.1.2.3 Κρυπτογράφηση ελλειπτικών καμπυλών (ECC)

Δυστυχώς, ο αλγόριθμος Diffie – Hellman έχει τεθεί υπό κριτική αρκετές φορές, καθώς μπορεί να είναι ευάλωτος σε επιθέσεις που υποβαθμίζουν την ασφάλειά του και επιτρέπουν σε κάποιον ενδιάμεσο τρίτο (man-in-the-middle) να αποκτήσει πρόσβαση στο περιεχόμενο του κλειδιού – οι επιθέσεις logjam που μπορούν να συμβούν εκμεταλλευόμενες ευπάθεια στο πρωτόκολλο TLS αποτελούν ένα χαρακτηριστικό παράδειγμα (Adrian κ.ά., 2015).

Για την αναβάθμιση της ασφάλειας του αλγορίθμου, προτάθηκε η ενσωμάτωση της αλγεβρικής δομής των ελλειπτικών καμπυλών ως μέθοδο διαχείρισης του ζεύγους δημόσιου και ιδιωτικού κλειδιού, σε συνδυασμό με τη κρυπτογράφηση Diffie – Hellman, ως επέκταση της τελευταίας (Harkanson & Kim, 2017). Η αρχική τους εμφάνιση στην επιστημονική βιβλιογραφία χρονολογείται στα μέσα της δεκαετίας του ’80 (Koblitz, 1987; Miller, 1986), όμως η ευρεία χρήση τους ξεκίνησε δύο δεκαετίες αργότερα (Harkanson & Kim, 2017).

Στην υπό εξέταση κρυπτογράφηση, χρησιμοποιούνται καμπύλες που δημιουργούνται πάνω σε έναν άξονα, με το δημόσιο κλειδί να προκύπτει από τα σημεία που συναντώνται κατά τη διάρκεια εκτέλεσης συναρτήσεων, ενώ το ιδιωτικό να προκύπτει από τον αριθμό που έχουν εκτελεστεί αυτές οι συναρτήσεις. Η κάθε καμπύλη είναι οριοθετημένη πάνω στον άξονα: όσο ευρύτερα είναι τα όρια, τόσο περισσότερα σημεία πάνω σε αυτή μπορούν να χρησιμοποιηθούν και τόσο μεγαλύτερο είναι το κλειδί που θα προκύψει, ήτοι η ασφάλεια είναι αναλόγως μεγαλύτερη (*Elliptic Curve Cryptography Overview*, 2015).

Η μέθοδος των ελλειπτικών καμπυλών χρησιμοποιείται εκτός από την κρυπτογράφηση (λ.χ. στο πρωτόκολλο TLS) και την μετάδοση κλειδιών μέσω μη ασφαλούς καναλιού, και στην επικύρωση ψηφιακών υπογραφών. Ο οργανισμός NIST έχει συμπεριλάβει ορισμένες ελλειπτικές καμπύλες (οι οποίες ανταποκρίνονται σε υψηλές απαιτήσεις ασφαλείας) στην τελευταία έκδοση του Προτύπου Ψηφιακής Υπογραφής, μαζί με εφαρμογές του αλγορίθμου RSA (National Institute of Standards and Technology, 2023b). Τέλος, το βασικό πλεονέκτημα της κρυπτογράφησης ελλειπτικών καμπυλών σε σχέση με την κρυπτογράφηση RSA, είναι πως στις ελλειπτικές καμπύλες απαιτείται κλειδί μικρότερου μήκους για την επίτευξη του ίδιου επιπέδου ασφαλείας με το αντίστοιχο κλειδί που θα δημιουργούνταν μέσω RSA (*Elliptic Curve Cryptography Overview*, 2015).



Εικόνα 6: Παράδειγμα ελλειπτικής καμπύλης. Εντός αυτής (κόκκινο χρώμα), και με τη χρήση συνάρτησης, θα αποτυπωθούν τα σημεία που θα οδηγήσουν στην τελική δημιουργία του ζεύγους δημόσιου και ιδιωτικού κλειδιού. Πηγή: globalsign.com

4.1.2.4 Κρυπτογράφηση από άκρο σε άκρο (end-to-end)

Σε αντίθεση με τους αλγόριθμους κρυπτογράφησης που περιγράφτηκαν παραπάνω, η κρυπτογράφηση από άκρο σε άκρο (end-to-end encryption ή E2EE) αποτελεί περισσότερο ολιστική προσέγγιση παρά αλγόριθμο από μόνη της. Στόχος της κρυπτογράφησης end-to-end είναι να αξιοποιήσει τους διαθέσιμους αλγόριθμους κρυπτογράφησης (και κυρίως αλγόριθμους δημόσιου κλειδιού) με τέτοιον τρόπο, ώστε αφενός το μήνυμα να κρυπτογραφείται σε κάθε στάδιο της μεταφοράς του από τον αποστολέα προς τον παραλήπτη και αφετέρου να μπορεί να αποκρυπτογραφηθεί μόνο από αυτόν (και φυσικά από τον αποστολέα), χωρίς να είναι σε θέση να το αποκρυπτογραφήσει ούτε ο ίδιος ο πάροχος της υπηρεσίας (Martinoli, 2022; *What Is End-to-End Encryption and How Does It Work?*, 2023).

Ένα πρωτόκολλο κρυπτογράφησης E2EE μπορεί να αξιοποιεί διάφορους αλγόριθμους, όπως τον AES, τον RSA, ή το πρωτόκολλο Signal[106], ενώ η ασφάλεια και η αποτελεσματικότητα του είναι ανάλογη της αλγοριθμικής αρχιτεκτονικής και της διαδικασίας διαχείρισης των δημόσιων και κλειδιών. Τα τελευταία χρόνια, όλο και περισσότερες εφαρμογές ανταλλαγής μηνυμάτων έχουν περάσει στη λύση της E2EE κρυπτογράφησης, σε μια προσπάθεια να προστατέψουν τους χρήστες τους από κακόβουλους τρίτους, και καθώς οι Αρχές Επιβολής του Νόμου (AEN) επέκτειναν τη διαδικτυακή τους έρευνα με προγράμματα μαζικής παρακολούθησης χρηστών.

[106] Signal. (χ.χ.). *Signal Protocol Documentation*. Signal Messenger. Ανακτήθηκε 6 Φεβρουάριος 2024, από https://signal.org/docs/

Πολλές από τις μεγαλύτερες εφαρμογές ανταλλαγής μηνυμάτων επικοινωνίας, όπως (αλλά όχι αποκλειστικά) το Messenger[107] και το WhatsApp[108] της Meta, το Viber[109], το Signal κ.ά. ήδη χρησιμοποιούν την κρυπτογράφηση από άκρο σε άκρο, είτε μερικώς είτε συνολικά στις δυνατότητες επικοινωνίας που προσφέρουν. Και, παρόλο που η προσέγγιση E2EE ξεκίνησε να χρησιμοποιείται για τη διασφάλιση του απορρήτου της επικοινωνίας σε αποστολές άμεσων μηνυμάτων, πλέον έχει επεκταθεί και σε εφαρμογές όπως η ανταλλαγή ηλεκτρονικής αλληλογραφίας[110], η αποθήκευση δεδομένων στο cloud[111] και τα εργαλεία διαχείρισης κωδικών πρόσβασης[112].

Λόγω της συνδυαστικής της φύσης και καθώς αξιοποιεί τα δυνατά σημεία των αλγορίθμων που χρησιμοποιεί, η κρυπτογράφηση end-to-end θεωρείται μέχρι σήμερα η αποτελεσματικότερη επιλογή για την εξασφάλιση του απορρήτου της επικοινωνίας, με όλες τις θετικές αλλά και αρνητικές προεκτάσεις που μπορεί να λάβει.

5 Οι αστυνομικές επιχειρήσεις στον κυβερνοχώρο

5.1 Νομοθετικό πλαίσιο ηλεκτρονικών παρακολουθήσεων και επισυνδέσεων – Οι Ειδικές Ανακριτικές Πράξεις

Το 2000, με τη συμμετοχή της στη Σύμβαση των Ηνωμένων Εθνών για το Διασυνοριακό Οργανωμένο Έγκλημα (UN General Assembly, 2000), η Ελλάδα ενέταξε στο ποινικό δικονομικό της δίκαιο ορισμένες ειδικές ανακριτικές τεχνικές (Άρθρο 20 της

[107] Βλέπε σχετική ενημέρωση διαθέσιμη στο https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/ (Πρόσβαση 6/2/2024).

[108] Βλέπε σχετική ενημέρωση διαθέσιμη στο https://faq.whatsapp.com/820124435853543 (Πρόσβαση 6/2/2024)

[109] Βλέπε σχετική ενημέρωση διαθέσιμη στο https://www.viber.com/en/security/ (Πρόσβαση 6/2/2024)

[110] Όπως για παράδειγμα η υπηρεσία ProtonMail, που παρέχει δωρεάν ηλεκτρονική διεύθυνση και γραμματοκιβώτιο με ενσωματωμένη κρυπτογράφηση απ' άκρο σ' άκρο. Βλ. https://proton.me/mail (Πρόσβαση 6/2/2024)

[111] Μια πολύ ενδιαφέρουσα υπηρεσία cloud αποθήκευσης με ενσωματωμένη κρυπτογράφηση E2EE είναι λ.χ. η MEGA, βλ. https://mega.io/ (Πρόσβαση 6/2/2024)

[112] Χαρακτηριστικά παραδείγματα αποτελούν το 1Password, βλ. https://support.1password.com/1password-privacy/ και το LastPass, βλ. https://www.lastpass.com/security/zero-knowledge-security (Πρόσβαση 6/2/2024)

Σύμβασης[113]) ως μέσα επίτευξης των στόχων της. Οι τεχνικές αυτές στο εσωτερικό δίκαιο αντιστοιχούν στις λεγόμενες «ειδικές ανακριτικές πράξεις» και απαντώνται στο Άρθρο 254 ΚΠΔ. Οι ειδικές ανακριτικές πράξεις τελούνται υποχρεωτικά με μυστικότητα, ενώ ο νόμος προβλέπει συγκεκριμένες εγκληματικές ενέργειες και προϋποθέσεις που δικαιολογούν την έγκρισή τους από το αρμόδιο δικαστικό συμβούλιο.

Όσον αφορά τις προϋποθέσεις, αυτές περιγράφονται στις παρ. 2 και 3 άρθ. 254 ΚΠΔ, επιβάλλεται να πληρούνται σωρευτικά και είναι:

- Η ύπαρξη σοβαρών ενδείξεων πως έχει τελεστεί μια εκ των αξιόποινων πράξεων που προβλέπονται στην παράγραφο 1 (βλ. και παρακάτω),
- Η έλλειψη ή δυσχέρεια λήψης εναλλακτικών μέτρων για την εξιχνίαση του εγκλήματος,
- Η έκδοση αιτιολογημένου βουλεύματος από το αρμόδιο δικαστικό συμβούλιο, του οποίου προηγείται η πρόταση εισαγγελέα. Η αιτιολόγηση του βουλεύματος θα πρέπει να αναφέρει την αξιόποινη πράξη που θα ερευνηθεί, τις σοβαρές ενδείξεις που έχουν οδηγήσει στην ανάγκη διενέργειας ειδικής ανακριτικής πράξης κατά συγκεκριμένου προσώπου, το σκοπό αυτής και για ποιο λόγο δεν μπορεί η έρευνα να επιτευχθείς με λιγότερο παρεμβατικό τρόπο, καθώς και τη συγκεκριμένη διάρκεια που αναμένεται να διαρκέσει, με δυνατότητα παράτασής της σε εξαιρετικές περιπτώσεις.

Οι ειδικές ανακριτικές πράξεις, λόγω της ιδιαίτερα παρεμβατικής τους φύσης και της αναπόφευκτης προσβολής του δικαιώματος στην ιδιωτικότητα των ατόμων κατά των οποίων διενεργούνται (αλλά πολλές φορές και τρίτων), επιτρέπονται για την εξιχνίαση συγκεκριμένων εγκλημάτων, τα οποία ανήκουν σε τέσσερις ευρύτερες κατηγορίες:

- **Τρομοκρατία**: Σύσταση και συμμετοχή σε τρομοκρατική οργάνωση (παρ. 1 και 2 άρ.187 ΠΚ), τρομοκρατικές ενέργειες (187^{Α} ΠΚ),

[113] Συγκεκριμένα, στην παρ. 1 άρθ. 20 της Σύμβασης, αναφέρεται πως: *" If permitted by the basic principles of its domestic legal system, each State Party shall, within its possibilities and under the conditions prescribed by its domestic law, take the necessary measures to allow for the appropriate use of controlled delivery and, where it deems appropriate, for the use of other special investigative techniques, such as electronic or other forms of surveillance and undercover operations, by its competent authorities in its territory for the purpose of effectively combating organized crime."* (UN General Assembly, 2000)

- **Παραχάραξη μέσων πληρωμών**: Παραχάραξη νομισμάτων ή άλλων μέσων πληρωμών (παρ. 1 και 2 άρ. 207 ΠΚ), κυκλοφορία πλαστών μέσων πληρωμών (208 ΠΚ), καθ' υπέρβαση κατασκευή νομίσματος (208^{Α} ΠΚ),
- **Εμπορία ανθρώπων** (323^{Α} ΠΚ),
- **Εγκλήματα κατά της γενετήσιας αξιοπρέπειας**: Βιασμός (336 ΠΚ), κατάχρηση ανίκανου προς αντίσταση σε γενετήσια πράξη (338 ΠΚ), γενετήσια πράξη με ανήλικο (παρ. 1 και 3 άρ. 339 ΠΚ), κατάχρηση ανηλίκων (παρ. 1 άρ. 342), πορνογραφία ανηλίκων (348^{Α} ΠΚ), προσέλκυση παιδιών για γενετήσιους λόγους (348^{Β} ΠΚ), πορνογραφικές παραστάσεις ανηλίκων (348^{Γ} ΠΚ), γενετήσια πράξη με ανήλικο έναντι αμοιβής (351^{Α} ΠΚ).

Καταλαβαίνουμε ότι οι συνθήκες που αιτιολογούν τη διενέργεια ειδικών ανακριτικών πράξεων είναι πολύ συγκεκριμένες και οριοθετημένες. Εξίσου οριοθετημένες είναι και οι ίδιες οι ειδικές ανακριτικές πράξεις, οι οποίες περιγράφονται ως έξι συγκεκριμένες μεθοδεύσεις στην παρ. 1 άρθ. 254 ΚΠΔ:

1) Η **συγκαλυμμένη έρευνα**, όπου το άτομο που τη διενεργεί (είτε ανακριτικός υπάλληλος είτε καθοδηγούμενος ιδιώτης) διευκολύνει το υποκείμενο στην τέλεση ενός από τα παραπάνω εγκλήματα, εάν φυσικά κάτι τέτοιο έχει προαποφασιστεί.
2) Η **ανακριτική διείσδυση**, στην οποία συμμετέχει ανακριτικός υπάλληλος, τα στοιχεία ταυτότητας του οποίου έχουν παραποιηθεί για τις ανάγκες της έρευνας. Ο υπάλληλος στοχεύει να διεισδύσει στην εγκληματική οργάνωση και να αποκαλύψει τη δομή των μελών της, διεκπεραιώνοντας καθήκοντα ως μέλος της. Σαφώς, στην ανακριτική διείσδυση μπορεί να προκύψει και η διακρίβωση εγκλημάτων που σκοπεύει να τελέσει η οργάνωση.
3) Οι **ελεγχόμενες μεταφορές**, οι οποίες αφορούν την διακίνηση παράνομων αγαθών στη χώρα και η έξοδος τους από αυτή χωρίς να επέμβουν οι διωκτικές αρχές, ώστε να μπορέσουν οι εμπλεκόμενοι να συλληφθούν στον τελικό προορισμό.
4) Η **άρση του απορρήτου των επικοινωνιών ή των δεδομένων κίνησης και θέσης** αυτών (περιφερειακά δεδομένα επικοινωνίας ή αλλιώς μεταδεδομένα).
5) Η **καταγραφή γεγονότων ή δραστηριότητας υπόπτων σε μορφή πολυμέσων**, με εξαίρεση την οικία τους.

6) Η **συσχέτιση και ο συνδυασμός προσωπικών δεδομένων** που ενδεχομένως να είναι αποθηκευμένα σε διάσπαρτες βάσεις δεδομένων, ώστε να μπορέσει να δημιουργηθεί προσωποποιημένο προφίλ του/των υπόπτου/ων.

Κρίνεται σημαντικό να αναφερθεί πως κατά την τέλεση των ειδικών ανακριτικών πράξεων εφαρμόζονται δύο συγκεκριμένες εγγυήσεις: πρώτον, οι υπάλληλοι ή οι ιδιώτες που τις διενεργούν βρίσκονται σε συνεχή συνεννόηση με τις αρμόδιες εισαγγελικές αρχές, και δεύτερον συντάσσονται αναλυτικές αναφορές οι οποίες περιλαμβάνουν τα στοιχεία που συλλέγονται κατά την έρευνα. Ο νόμος εκφράζει ρητά πως στοιχεία τα οποία δεν περιγράφονται στις σχετικές αναφορές, δεν μπορούν να χρησιμοποιηθούν στη δικαστική διαδικασία για την καταδίκη των κατηγορουμένων.

Συγκεκριμένα, όσον αφορά την άρση του απορρήτου των επικοινωνιών, οι ειδικότερες διαδικασίες και εγγυήσεις περιγράφονται στο Ν. 5002/2022: Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών., 2022 (και συγκεκριμένα στα άρθρα 4 έως 9), ο οποίος ψηφίστηκε μετά τις αποκαλύψεις για τις παρακολουθήσεις του δημοσιογράφου κ. Κουκάκη και του Προέδρου του ΠΑΣΟΚ-ΚΙΝΑΛ κ. Ανδρουλάκη (βλ. Ενότητα 5.2). Το εν λόγω νομοθέτημα προσθέτει επιπλέον εγγυήσεις για την προστασία των πολιτών και των πολιτικών προσώπων και προβλέπει τη διαδικασία άρσης του απορρήτου των επικοινωνιών και διατήρησης των δεδομένων που συλλέγονται κατά τη διάρκειά της για λόγους εθνικής ασφάλειας και διακρίβωσης εγκλημάτων.

Η διαδικασία για τη νόμιμη επισύνδεση που βασίζεται σε λόγους εθνικής ασφάλειας διαφέρει ανάλογα με την ιδιότητα του παρακολουθούμενου: αν πρόκειται για πολίτη, το αίτημα υποβάλλεται από την Εθνική Υπηρεσία Πληροφοριών ή τη Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας της ΕΛ.ΑΣ. στον αρμόδιο εισαγγελικό λειτουργό, και το οποίο περιλαμβάνει τα στοιχεία αιτιολόγησης που περιγράφτηκαν παραπάνω. Ο εισαγγελικός λειτουργός κρίνει για το αποτέλεσμα του αιτήματος εντός 24 ωρών, και αν η διάταξή του είναι θετική προς την άρση, τότε οφείλει να την υποβάλει χωρίς καθυστέρηση σε δεύτερο εισαγγελέα του Αρείου Πάγου ή Εφετών προς έγκριση. Μόνο αν και ο δεύτερος εισαγγελέας εγκρίνει την άρση, θα ξεκινήσει να ισχύει η σχετική εισαγγελική διάταξη.

Αν το πρόσωπο-στόχος για την άρση του απορρήτου είναι πολιτικό πρόσωπο, τότε το αίτημα μπορεί να υποβληθεί μόνο από την ΕΥΠ προς τον Πρόεδρο της Βουλής, φυσικά μαζί με στοιχεία που κλίνουν σε αυξημένες πιθανότητες διακινδύνευσης της εθνικής

ασφάλειας. Ο Πρόεδρος της Βουλής (ή εναλλακτικά ο πρόεδρος της τελευταίας Βουλής ή ο Πρωθυπουργός, σε περίπτωση κωλύματος που προβλέπει ο νόμος), αποφασίζει εντός 24 ωρών και σε περίπτωση έγκρισης του αιτήματος, τότε αυτό υποβάλλεται σε δεύτερο βαθμό στον αρμόδιο εισαγγελικό λειτουργό για την ολοκλήρωση της διαδικασίας.

Τα άτομα στα οποία διενεργήθηκε άρση του απορρήτου των επικοινωνιών, μπορούν να ενημερωθούν για αυτό, υπό την προϋπόθεση πως έχουν παρέλθει 3 έτη από την ολοκλήρωση αυτής και πως δεν θίγεται ο σκοπός για τον οποίο αυτή έλαβε χώρα. Το υποκείμενο της πιθανής άρσης καταθέτει αίτηση στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, η οποία τη διαβιβάζει στους αρμόδιους φορείς. Ο κάθε φορέας (ΕΥΠ και ΔΑΕΕΒ της ΕΛ.ΑΣ.) αποφασίζει για τη γνωστοποίηση μέσω τριμελούς οργάνου, και εν συνεχεία ενημερώνει το θιγόμενο. Το υλικό που συλλέχθηκε κατά την άρση, καταστρέφεται μετά την πάροδο 10 ετών.

Όσα αναφέραμε στις προηγούμενες παραγράφους αφορούν τη διαδικασία άρσης για λόγους εθνικής ασφάλειας, η οποία διαφοροποιείται από αυτή για τη διακρίβωση εγκλημάτων. Στην τελευταία, το αρμόδιο δικαστικό συμβούλιο υποχρεούται να εκδώσει αιτιολογημένο βούλευμα εντός 48 ωρών από τη στιγμή που θα λάβει την πρόταση από τον εισαγγελέα. Εάν οι συνθήκες προσδίδουν κατεπείγοντα χαρακτήρα στο αίτημα, τότε ο τελευταίος μπορεί να διατάξει από μόνος του την άρση, έχοντας την υποχρέωση να την υποβάλλει στο δικαστικό συμβούλιο για την έκδοση βουλεύματος. Αν μετά την πάροδο 5 ημερών από την κατεπείγουσα έναρξη της άρσης δεν έχει εκδοθεί το σχετικό βούλευμα, η διαδικασία θεωρείται άκυρη και τα συλλεχθέντα στοιχεία δεν μπορούν να αξιοποιηθούν. Τα κακουργήματα και τα πλημμελήματα που δύνανται να διακριβωθούν μέσω άρσης απορρήτου, αναφέρονται αναλυτικά και αντίστοιχα στις παραγράφους 1 και 2, άρ. 6 του Ν. 5002/2022, όπως αυτό ισχύει σήμερα.

Στην εν λόγω κατηγορία άρσης απορρήτου, ο θιγόμενος μπορεί να ενημερωθεί για την άρση αιτούμενος προς την ΑΑΔΕ, η οποία θα απαντήσει έχοντας λάβει την έγκριση του εισαγγελέα του Αρείου Πάγου. Ο τελευταίος θα δώσει τη σύμφωνη γνώμη του εφόσον, όπως και στην προηγούμενη περίπτωση, δεν τίθεται εν κινδύνω ο σκοπός για τον οποίο τελέστηκε η άρση. Τέλος, σε περίπτωση που τα ευρήματα οδήγησαν σε ποινική δίωξη, η καταστροφή τους γίνεται μετά την έκδοση αμετάκλητης απόφασης ή απαλλακτικού βουλεύματος, ενώ αν δεν ασκήθηκε η ποινική δίωξη, η καταστροφή του υλικού γίνεται χωρίς καθυστέρηση με τη σύνταξη σχετικής έκθεσης.

5.2 Οι δύο όψεις του νομίσματος: παραδείγματα παρεμπόδισης αλλά και κατάχρησης των δυνατοτήτων των αρχών ασφαλείας μέσα από τον Τύπο

Το απόγευμα της Παρασκευής της 13ης Νοεμβρίου 2015 ήταν ένα από τα σοκαριστικότερα για τη Γαλλία και την Ευρώπη, ιδιαίτερα αν αναλογιστεί κανείς πως επρόκειτο για τη φονικότερη μέρα που έζησε το Παρίσι από τον Β' Παγκόσμιο Πόλεμο (Radiotileoptiki S. A. - OPEN Digital Group, 2022). Μια σειρά τρομοκρατικών επιθέσεων που συνέβησαν με διαφορά λεπτών σε σποραδικά σημεία της γαλλικής πρωτεύουσας πάγωσε την κοινή γνώμη. Από τις 21:20 (τοπική ώρα) μέχρι και τη 01:00 το βράδυ, 130 άνθρωποι δολοφονήθηκαν και πάνω από 400 τραυματίστηκαν από εκρήξεις βομβιστών αυτοκτονίας στο γήπεδο Stade de France και πυροβολισμούς σε εστιατόρια και μπαρ στο 10ο και 11ο διαμέρισμα στο Παρίσι. Παράλληλα, μια ομάδα τζιχαντιστών εισβάλλει στο θέατρο Bataclan κατά τη διάρκεια συναυλίας, αιματοκυλίζοντας το, κρατώντας ομήρους και σκοτώνοντας ορισμένους από αυτούς μέχρι την οριστική επέμβαση της αστυνομίας και την εξουδετέρωση των δραστών (Radiotileoptiki S. A. - OPEN Digital Group, 2022). Από όλους τους μακελάρηδες που ενεπλάκησαν, μόνο ένας παραμένει μέχρι σήμερα ζωντανός, ο Σαλάχ Αμπντεσλάμ, ο οποίος καταδικάστηκε σε ισόβια χωρίς τη δυνατότητα αποφυλάκισης (CNN,gr, 2022).

Λίγους μήνες μετά τις τρομοκρατικές επιθέσεις του Παρισιού, και συγκεκριμένα στις 22 Μαρτίου 2016, ο ίδιος πυρήνας τζιχαντιστών (συμπεριλαμβανομένου του Αμπντεσλάμ, ο οποίος συμμετείχε στο σχεδιασμό αλλά όχι στην υλοποίηση) ενήργησε στις Βρυξέλλες μέσω τριών παράλληλων βομβιστικών επιθέσεων: δύο στο αεροδρόμιο Ζάβεντεμ και μια στο σταθμό του μετρό Μάαλμπεκ, πολύ κοντά στα κτίρια των ευρωπαϊκών θεσμών (Euronews, 2021). Ο αριθμός των θυμάτων ξεπέρασε τους 30, ενώ δεκαπλάσιος ήταν ο αριθμός των τραυματιών (Parsons, 2023). Ο τρομοκρατικός πυρήνας αυτών των επιθέσεων, είναι γνωστό πως επικοινωνούσε χρησιμοποιώντας εφαρμογές με τη δυνατότητα κρυπτογράφησης απ' άκρο σε άκρο (Billington, 2015). Σε δήλωσή του μετά τις τρομοκρατικές επιθέσεις των Βρυξελλών, ο διευθυντής της Europol Ρομπ Γουέινραϊτ ανέφερε πως «η κρυπτογραφημένη επικοινωνία μέσω του διαδικτύου και των έξυπνων κινητών είναι ένα από τα προβλήματα που αντιμετωπίζουν οι ερευνητές» (Benner & Hohmann, 2016).

Εκτός Ευρωπαϊκής Ένωσης, ως ακόμη ένα παράδειγμα κατάχρησης της τεχνολογίας για ειδεχθείς σκοπούς που αξίζει να αναφερθεί και συνέβη το ίδιο καλοκαίρι

με τις επιθέσεις στο Βέλγιο είναι η τριπλή βομβιστική επίθεση στο αεροδρόμιο Ατατούρκ της Κωνσταντινούπολης, το βράδυ της 28ης Ιουνίου 2016 (Η Καθημερινή, 2016). Η επίθεση ξεκίνησε όταν ένας εκ των δραστών άνοιξε πυρ κατά επιβατών στον τερματικό σταθμό αναχωρήσεων, χρησιμοποιώντας αυτόματο όπλο. Αμέσως μετά, οι δύο άλλοι δράστες πυροδότησαν τους εκρηκτικούς μηχανισμούς που είχαν επάνω τους στον χώρο αφίξεων. Περισσότεροι από 40 άνθρωποι σκοτώθηκαν και πάνω από 200 ήταν οι τραυματίες, με την τρομοκρατική οργάνωση «Ισλαμικό Κράτος (Daesh)» να θεωρείται πως συμμετείχε στην προετοιμασία των γεγονότων (Karimi κ.ά., 2016).

Λιγότερο από ένα μήνα μετά, και πριν προλάβει η κοινή γνώμη να ξεπεράσει το σοκ των επιθέσεων στην Κωνσταντινούπολη, η Γαλλία επλήγη από ακόμη ένα τρομοκρατικό χτύπημα, την ευθύνη του οποίου ανέλαβε και πάλι το Ισλαμικό Κράτος (in newspaper, 2016). Στις 14 Ιουλίου 2016, ανήμερα της γαλλικής εθνικής εορτής για την πτώση της Βαστίλης, ο 31χρονος Γάλλος με καταγωγή από την Τυνησία Μοχάμεντ Μπουλέλ (CNN,gr., 2016), επιτέθηκε σε πλήθος ανθρώπων πέφτοντας πάνω τους με φορτηγό όχημα το οποίο περιείχε μεταξύ άλλων όπλα και εκρηκτικά υλικά (iefimerida, 2016). Πέραν της επίθεσης με το όχημα, ο δράστης πυροβολούσε διερχόμενα άτομα, ενώ μετά από ανταλλαγή πυρών με τις Αρχές έπεσε νεκρός. Πάνω από 80 νεκροί και εκατοντάδες τραυματίες ήταν ο τραγικός απολογισμός της επίθεσης, η οποία έλαβε χώρα λίγο μετά τις 22:30 το βράδυ (Rubin & Breeden, 2017).

Παρόλο που στις τρομοκρατικές ενέργειες της Κωνσταντινούπολης και της Νίκαιας δεν επιβεβαιώθηκε άμεσα η χρήση εφαρμογών κρυπτογραφημένης επικοινωνίας, η εκμετάλλευση τους από εξτρεμιστικές οργανώσεις για σκοπούς συντονισμού επιθέσεων, διασποράς προπαγανδιστικού υλικού και στρατολόγησης επίδοξων ακολούθων θεωρείται δεδομένη και έχει τεκμηριωθεί (Graham, 2016; Torok, 2015). Και, παρόλο που τα παραδείγματα τα οποία αναφέραμε πιο πάνω σχετίζονται με τη τζιχαντιστική τρομοκρατία, η κρυπτογράφηση διαδικτυακών επικοινωνιών αποτελεί σήμερα χρήσιμο εργαλείο και για άλλες εξτρεμιστικές ομάδες, υπονομεύοντας σε μεγάλο βαθμό τις επιχειρήσεις των αστυνομικών αρχών (Edison Hayden, 2019; EUROPOL, 2023; Gais & Squire, 2021).

Από την άλλη πλευρά, οι κυβερνητικοί φορείς, οι αστυνομικές αρχές και οι υπηρεσίες πληροφοριών έχουν εξίσου εμπλακεί σε σκάνδαλα παραβίασης του απορρήτου των επικοινωνιών πολιτών με τη χρήση της τεχνολογίας. Ένα από τα μεγαλύτερα σκάνδαλα στη χώρα μας είδε το φως της δημοσιότητας στις 2 Φεβρουαρίου 2006, όμως

συνέβη το 2005, όταν η εταιρία Vodafone, σε έναν έλεγχο ρουτίνας των συστημάτων της, εντόπισε κακόβουλο λογισμικό που έδινε τη δυνατότητα στον εισβολέα να παρακολουθεί τις συνομιλίες 100 προσώπων της πολιτικής και της άμυνας της Ελλάδας, χρησιμοποιώντας κινητές συσκευές – «σκιές», στις οποίες προωθούνταν το περιεχόμενο των συνομιλιών (Αριστείδης, 2012; Μουστάκα, 2010). Η υπόθεση κατέληξε με σχετικό πόρισμα της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών ('Πόρισμα-φωτιά της ΑΔΑΕ για τις υποκλοπές στη Βουλή', 2006), η οποία επέβαλε ένα βαρύτατο πρόστιμο στη Vodafone, ύψους 76 εκατομμυρίων ευρώ. Η υπόθεση αυτή οδήγησε στη θεσμοθέτηση αυστηρότερης νομοθεσίας σχετικά με την ευθύνη των παρόχων τηλεπικοινωνιών στην προστασία των εγκαταστάσεων τους και των δεδομένων που επεξεργάζονται, ενώ σύμφωνα με τον Τύπο, με την υπόθεση ενδεχομένως να συνδέονταν και αμερικανικά συμφέροντα (Αριστείδης, 2012; Ζέρβας, 2011). Παρόλα αυτά, δεν αποδόθηκαν ευθύνες στους υπεύθυνους που εισήγαγαν τον κακόβουλο κώδικα.

Περίπου δεκαπέντε χρόνια αργότερα, θα αποκαλύπτονταν μέσω του Τύπου παρατυπίες στις επισυνδέσεις που διεξήγαγε η ΕΥΠ, και συγκεκριμένα οι παρατυπίες αυτές θα αφορούσαν την έλλειψη πολιτικών ασφαλείας στα συστήματα υποκλοπών, τον πλημμελή έλεγχο των συστημάτων με πρόσχημα τεχνικές ή οικονομικές δυσκολίες για την υλοποίηση του και τον ασαφή χαρακτήρα που επικρατούσε στις αιτιολογήσεις που περιλάμβαναν οι εισαγγελικές διατάξεις (Λαμπρόπουλος, 2020). Ακόμη, κριτική ασκήθηκε και για τον τρόπο που χρησιμοποιήθηκε και το σύστημα εντοπισμού και παρακολούθησης συσκευών, XPZ, καθώς υπήρχαν υπόνοιες για εκμετάλλευση του από εργαζόμενους στην ΕΥΠ μέσω παράνομης παρακολούθησης επιφανών ατόμων, έναντι χρηματισμού (Λαμπρόπουλος, 2020).

Στην πιο πρόσφατη περίπτωση εκμετάλλευσης των δυνατοτήτων τους, οι ελληνικές Αρχές βρέθηκαν εκτεθειμένες στην υπόθεση παρακολουθήσεων του δημοσιογράφου Θανάση Κουκάκη και του Προέδρου του ΠΑΣΟΚ-ΚΙΝΑΛ Νίκου Ανδρουλάκη, την περίοδο 2020-2021 (News247gr, 2022). Η υπόθεση ξεκίνησε το καλοκαίρι του 2021, όπου ο κ. Κουκάκης έλαβε ένα γραπτό μήνυμα ηλεκτρονικού ψαρέματος με έναν σύνδεσμο, τον οποίο ακολούθησε. Από εκείνη τη στιγμή, το κινητό του μολύνθηκε από το κατασκοπευτικό λογισμικό Predator[114] και παρακολουθούνταν

[114] Ιδιαίτερη ανησυχία προκαλεί το γεγονός πως σε αντίθεση με άλλα εργαλεία παρακολουθήσεων, το Predator έχει τη δυνατότητα πρόσβασης σε δεδομένα που διακινούνται μέσω κρυπτογραφημένων εφαρμογών, όπως το WhatsApp, το Signal και το Telegram (Lakshmanan, 2023).

μέχρι και τον Σεπτέμβριο του ίδιου έτους (Τελλόγλου & Τριανταφύλλου, 2022). Μετά από σχετικά ντοκουμέντα που βρέθηκαν στα χέρια του, τα οποία υποδείκνυαν παρακολούθηση από την Εθνική Υπηρεσία Πληροφοριών, ο κ. Κουκάκης απευθύνθηκε στην Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών, η οποία παρόλες τις κινήσεις της, δεν μπόρεσε να του δώσει απαντήσεις λόγω της προσφάτως ψηφισθείσας τροπολογίας, η οποία αφαιρούσε από την ΑΔΑΕ τη δυνατότητα ενημέρωσης πολιτών σε περίπτωση παρακολούθησης τους για λόγους εθνικής ασφάλειας (Κ., 2022). Εν τέλει, ο τ. Διοικητής της ΕΥΠ, κ. Παναγιώτης Κοντολέων, παραδέχτηκε εμμέσως την παρακολούθηση του κ. Κουκάκη (ο οποίος εκείνη την περίοδο ερευνούσε υποθέσεις τραπεζικών σκανδάλων), όμως αρνήθηκε πως αυτή έγινε με το λογισμικό Predator (Τερζής, 2022).

Παράλληλα, το φθινόπωρο του 2021, ο κ. Ανδρουλάκης λαμβάνει στο κινητό του παρόμοιο μήνυμα ηλεκτρονικού ψαρέματος, όμως δεν ακολουθεί το σύνδεσμο. Όπως επιβεβαίωσε μερικούς μήνες αργότερα η υπηρεσία ψηφιακής ασφάλειας του Ευρωκοινοβουλίου (CERT-EU), υπήρξε προσπάθεια μόλυνσης και του κινητού του κ. Ανδρουλάκη (τότε ευρωβουλευτή) (Χονδρόγιαννος, 2022). Τον Αύγουστο 2022, ο Πρωθυπουργός Κυριάκος Μητσοτάκης (ΕΡΤ Α.Ε., 2022), θα δήλωνε πως ο κ. Ανδρουλάκης παρακολουθείτο από την ΕΥΠ για ένα διάστημα τριών μηνών, χρονικά τοποθετημένο από την αποτυχημένη προσπάθεια μόλυνσης με το Predator, μέχρι το Δεκέμβριο 2021. Αιτιολόγησε την παρακολούθηση σε λόγους εθνικής ασφάλειας, ενώ τόνισε πως ενώ η τυπική διαδικασία είχε ακολουθηθεί ορθώς, ο ίδιος δεν το γνώριζε και πως επρόκειτο για ένα ατόπημα της ΕΥΠ με πολιτικές διαστάσεις. Το Δεκέμβριο του 2022, η Κυβέρνηση θα έφερνε προς ψήφιση τον Ν. 5002/2022, ο οποίος προσθέτει επιπλέον εγγυήσεις για την άρση του απορρήτου των επικοινωνιών ειδικότερα όσον αφορά τα πολιτικά πρόσωπα, θα απαγόρευε ρητά τη χρήση λογισμικών παρακολούθησης, ρυθμίζει ζητήματα διάρθρωσης και διαφάνειας της Εθνικής Υπηρεσίας Πληροφοριών, και συστήνει την Επιτροπή για θέματα Κυβερνοασφάλειας και τη Μόνιμη Επιστημονική Επιτροπή Προσωπικών Δεδομένων[115].

Παρόλο που μέχρι σήμερα δεν έχει γίνει γνωστό ποιος εκκίνησε τις προαναφερθείσες παρακολουθήσεις χρησιμοποιώντας το Predator, με την ελληνική κυβέρνηση να αρνείται κατηγορηματικά τη χρήση του (Αρβανιτά, 2022), ενδιαφέρον

[115] (Ν. 5002/2022: Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών., 2022)

προκαλεί η έρευνα των δημοσιογράφων Νικόλα Λεοντόπουλου και Θοδωρή Χονδρόγιαννου (2022), η οποία συσχετίζει εμμέσως τον τότε Γενικό Γραμματέα του Πρωθυπουργού κ. Γρηγόρη Δημητριάδη με την εταιρία Krikel – προμηθευτή λογισμικού επισυνδέσεων της ΕΥΠ και την Intellexa – εταιρία διακίνησης του Predator στην Ελλάδα. Ο συσχετισμός αυτός προκύπτει μετά από επενδυτικές κινήσεις του κ. Δημητριάδη, οι οποίες συνίστανται σε αγοραπωλησίες εταιριών με επενδυτές οι οποίοι έχουν δεσμούς (είτε οικονομικούς είτε συγγενικούς) με άτομα που συνδέονται με τις εν λόγω εταιρίες λογισμικού υποκλοπών. Δύο μήνες μετά τη δημοσίευση της έρευνας, ο κ. Δημητριάδης παραιτείται από τη θέση του και ο τότε Διοικητής της ΕΥΠ παύεται από τα καθήκοντά του (ΕΡΤ Α.Ε., 2022).

6 "The balancing test": Εφαρμόζοντας την αναλογικότητα με τη χρήση της τεχνολογίας – η συζήτηση για ένα νέο πρότυπο ασφαλείας με την αξιοποίηση αλγορίθμου

Όπως φάνηκε από τη μέχρι στιγμής ανάλυση, η αναβάθμιση της τεχνολογίας σε συνδυασμό με το μειωμένο αίσθημα εμπιστοσύνης της κοινής γνώμης απέναντι στις αστυνομικές αρχές αλλά και η φύση της διαδικασίας νομοθέτησης που κατά κανόνα ακολουθεί τις εξελίξεις και δεν ηγείται αυτών, έχουν αφήσει τις αστυνομικές αρχές εκτεθειμένες κατά την τέλεση του αστυνομικού τους έργου.

Μια προσέγγιση που έχει ακολουθηθεί (με όχι επιτυχή αποτελέσματα) είναι η μαζική και αδιάκριτη συλλογή δεδομένων (λ.χ. κίνησης, θέσης, περιεχομένου διαδικτυακών συζητήσεων), τα οποία ενδεχομένως αργότερα να υποβάλλονται σε επεξεργασία, όμως με σαφή παραβίαση της αρχής της αναλογικότητας[116]. Από την άλλη, αναγνωρίζεται πως για τη διασφάλιση της δημόσιας ασφάλειας, οι αρχές επιβολής του νόμου θα πρέπει να έχουν στα χέρια τους τα μέσα να προλαμβάνουν εγκλήματα που σχεδιάζονται από εγκληματίες οι οποίοι εκμεταλλεύονται την ανάπτυξη της τεχνολογίας. Πώς όμως καταφέρνουμε να ισορροπήσουμε τη διατήρηση της δημόσιας ασφάλειας,

[116] Ένα πολύ χαρακτηριστικό παράδειγμα (εκτός ΕΕ αλλά πρωτοφανές λόγω της μεγάλης του έκτασης) είναι το πρόγραμμα PRISM των Ηνωμένων Πολιτειών της Αμερικής, κατά τη διάρκεια του οποίου οι αρχές ασφαλείας είχαν πρόσβαση σε μαζικά δεδομένα προσώπων από υπηρεσίες ευρύτατης χρήσης. (Greenwald & MacAskill, 2013)

δίνοντας στις αρχές τη δυνατότητα να εξετάζουν τεκμήρια πριν την τέλεση κάποιου εγκλήματος, ενώ παράλληλα εξασφαλίζουμε την ιδιωτικότητα όσων δεν σχεδιάζουν την τέλεση εγκλημάτων; Σαφώς, δε θα πρέπει να αγνοήσουμε πως η κατάχρηση των δυνατοτήτων των αρχών μπορεί να έχει δυσάρεστες συνέπειες για τα υποκείμενα δεδομένων, κρίνεται λοιπόν απαραίτητο να βρεθεί μια χρυσή τομή στις δύο προβληματικές.

Αυτήν την ισορροπία επιχειρεί να επιτύχει ο συνδυασμός της μηχανικής μάθησης και της αναλυτικής δεδομένων. Συγκεκριμένα, παρακάτω θα αναλυθεί η χρήση ενός αλγόριθμου που θα αξιοποιεί αυτές τις τεχνολογίες ώστε να πετύχει ακριβώς αυτό που τέθηκε ως στόχος παρακάτω. Η μελέτη περίπτωσης στην οποία προτείνεται να εφαρμόζεται είναι στις υπηρεσίες ανταλλαγής μηνυμάτων (κατά κύριο λόγω εφαρμογές instant messaging αλλά κατ' επέκταση και σε εφαρμογές ηλεκτρονικής αλληλογραφίας).

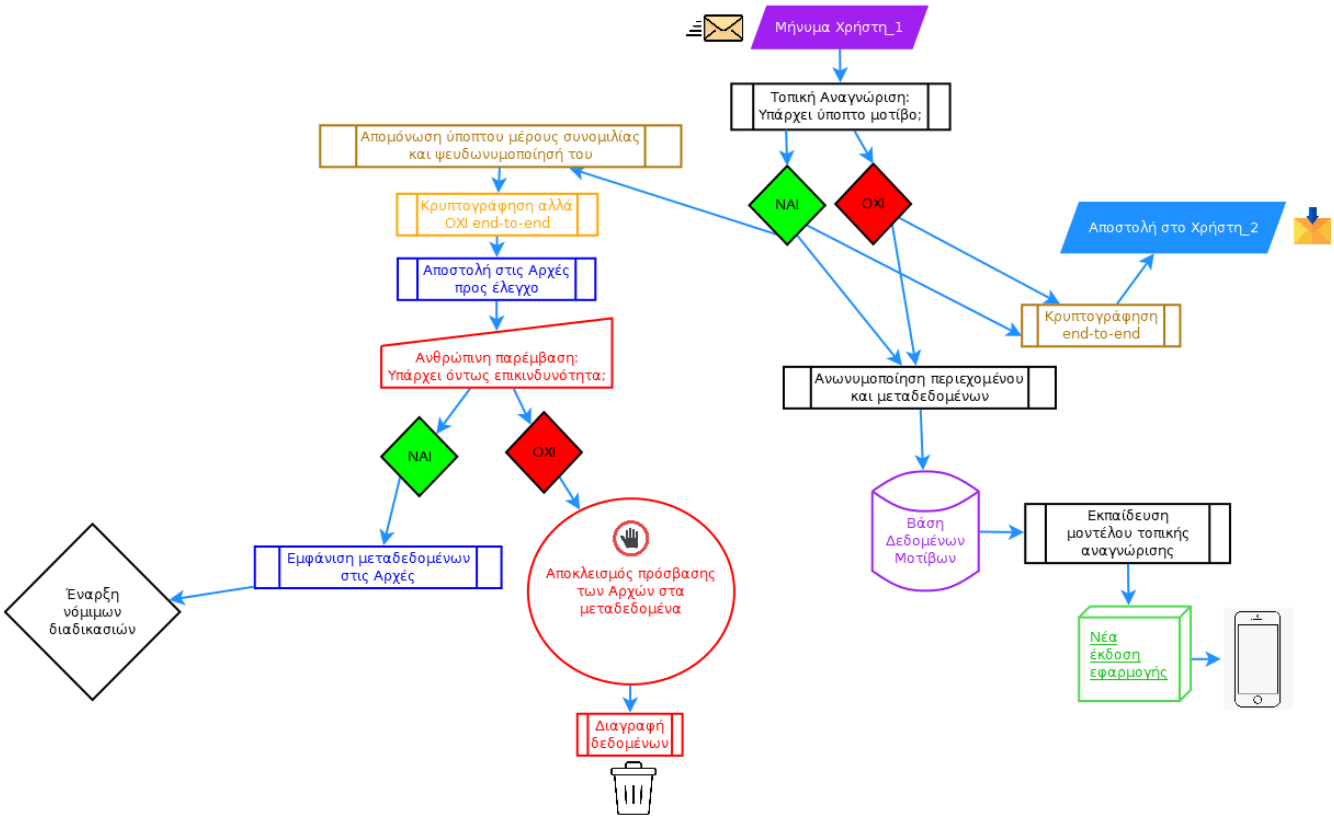
Θα αναλυθούν τα βήματα που προτείνεται να ακολουθεί, οι εγγυήσεις (μέσω τεχνικών και οργανωτικών μέτρων) που περιλαμβάνει ώστε να προστατεύει κατά το μέγιστο δυνατό το απόρρητο των επικοινωνιών των χρηστών και ο αντίκτυπος που σκοπεύει να δημιουργήσει στην τέλεση του αστυνομικού έργου.

Παραδεχόμενοι πως καμιά πρόταση δεν είναι άψογη, το κεφάλαιο ολοκληρώνεται με μια προσπάθεια αξιολόγησης της πρότασης, τόσο μέσω πρότασης εναλλακτικών εγγυήσεων όσο και από το πρίσμα της πρότασης κανονισμού για την τεχνητή νοημοσύνη (EU AI Act).

6.1 Η λειτουργία του αλγόριθμου

Όπως αναφέρθηκε και παραπάνω, θεωρούμε ως περίπτωση εφαρμογής της εν λόγω πρότασης κυρίως τις επικοινωνίες που λαμβάνουν χώρα μέσω υπηρεσιών άμεσων μηνυμάτων (instant messaging), με δυνατότητα εφαρμογής και στις υπηρεσίες ηλεκτρονικής αλληλογραφίας (emails) λόγω τεχνικής συνάφειας.

Η πρόταση συνίσταται στην εφαρμογή ενός προτύπου ασφαλείας διαδικτυακών συνομιλιών με την ενσωμάτωση ενός αλγορίθμου που θα λειτουργεί τοπικά στην τερματική συσκευή του χρήστη. Παρακάτω παρουσιάζεται μια οπτική απεικόνιση των βημάτων που ακολουθεί ο αλγόριθμος, ξεκινώντας από τη στιγμή που ο Χρήστης_1 («Αποστολέας») στέλνει το μήνυμα προς τον Χρήστη_2 («Παραλήπτης»). Αμέσως μετά την απεικόνιση περιγράφονται αναλυτικά τα βήματα του αλγόριθμου σε κάθε ενδεχόμενο:



Εικόνα 7: Μια σχηματική απεικόνιση των βημάτων που προτείνεται να ακολουθεί ο αλγόριθμος.

Αρχικά, Ο Χρήστης_1 αποστέλλει το μήνυμα (βήμα 1ο). Το περιεχόμενο του μηνύματος περνάει από αναγνώριση μοτίβου ύποπτων συνομιλιών, η οποία γίνεται τοπικά στη συσκευή (βήμα 2ο). Στο ιδανικό σενάριο που **δεν εντοπίζεται κάποιο ύποπτο μοτίβο**, τότε συμβαίνουν δύο παράλληλες κινήσεις: από ένα κανάλι επικοινωνίας, το μήνυμα κρυπτογραφείται απ' άκρο σ' άκρο (βήμα 3^{α}) και φεύγει από τη συσκευή για να αποσταλεί στον παραλήπτη (βήμα 4^{α}), ενώ παράλληλα μέσω δεύτερου καναλιού, το μήνυμα θα ανωνυμοποιηθεί[117] ως προς το περιεχόμενο και τα δεδομένα κίνησης/θέσης (βήμα 3^{β}). Τα ανωνυμοποιημένα δεδομένα θα αποσταλούν σε μια κεντρική βάση δεδομένων (βήμα 4^{β}) η οποία περιέχει ανωνυμοποιημένο περιεχόμενο συζητήσεων. Στη συνέχεια, μέσω αλγορίθμου αυτομάθησης, τα ακατέργαστα ανώνυμα δεδομένα θα μετατραπούν σε

[117] Ο όρος χρησιμοποιείται σύμφωνα με τα κριτήρια περί ανωνυμοποίησης και ψευδωνυμοποίησης που περιγράφονται στη Γνώμη 05/2014 της 10ης Απριλίου 2014, της Ομάδας Εργασίας του Άρθρου 29 (νυν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων) περί τεχνικών ανωνυμοποίησης, διαθέσιμη στην ιστοσελίδα https://t.ly/FrfvD. (Πρόσβαση 30/10/2023)

μοτίβα, σαφώς και πάλι με ανώνυμο χαρακτήρα (βήμα 5^{α}), τα οποία θα χρησιμοποιηθούν στην επόμενη έκδοση που θα ενημερώνει την εφαρμογή/υπηρεσία (βήμα 6^{α}).

Εάν υποθέσουμε πως στο $2^{ο}$ βήμα **εντοπίζεται ύποπτο μοτίβο συνομιλίας**, τότε λαμβάνουν χώρα όλα τα παραπάνω βήματα ώστε να μην εμποδιστεί η επικοινωνία μεταξύ των μερών και η ενημέρωση της ακρίβειας των μοτίβων, όμως παράλληλα ενεργοποιείται μια νέα αλληλουχία διαδικασιών μέσω τρίτου καναλιού: ενώ το μήνυμα κρυπτογραφείται για να σταλεί και ανωνυμοποιείται για να τροφοδοτήσει τη βάση δεδομένων, απομονώνεται το μέρος εκείνο της συνομιλίας στο οποίο εντοπίστηκε ύποπτο μοτίβο κατά την τοπική αναγνώριση και ψευδωνυμοποιείται το περιεχόμενό του ώστε να μην είναι άμεσα ταυτοποιήσιμοι ο αποστολέας, ο παραλήπτης ή τρίτα μέρη, πάλι τοπικά στη συσκευή (βήμα 3^{γ}). Εν συνεχεία, το ψευδωνυμοποιημένο απόσπασμα κρυπτογραφείται - όχι απαραίτητα απ' άκρο σε άκρο διότι έχει προηγηθεί το τεχνικό μέτρο της ψευδωνυμοποίησης (βήμα 4γ) και αποστέλλεται στις Αρχές (βήμα 5^{β}).

Ακολουθώντας τη δεοντολογική αρχή της ανθρώπινης παρέμβασης και εποπτείας[118], οι αστυνομικές αρχές προβαίνουν σε χειροκίνητο έλεγχο του ψευδωνυμοποιημένου αποσπάσματος ώστε να διευκρινιστεί αν όντως πρόκειται για επικίνδυνη συνομιλία (βήμα 6^{β}). Δύο είναι τα πιθανά ενδεχόμενα σε αυτήν την περίπτωση: είτε μιλάμε για λανθασμένη επισήμανση του κειμένου – οπότε και αποκλείεται η πρόσβαση των αρχών από τα δεδομένα του αποσπάσματος και αυτά διαγράφονται αυτόματα – ήτοι το ψευδωνυμοποιημένο περιεχόμενο και τα δεδομένα κίνησης/θέσης (βήμα 7^{α}), είτε η αυτόματη επισήμανση επιβεβαιώνεται από τον χειροκίνητο έλεγχο, κάτι που οδηγεί στην εμφάνιση των μεταδεδομένων της συνομιλίας (βήμα 7^{β}) ώστε να αξιολογηθούν ενδεχόμενες νόμιμες ενέργειες προληπτικού χαρακτήρα από τις αρχές επιβολής του νόμου (βήμα $8^{ο}$).

6.2 Οι εγγυήσεις για την ιδιωτικότητα των χρηστών

Είναι αυτονόητο πως με την εισαγωγή ενός τέτοιου αλγόριθμου στην λειτουργία μιας εφαρμογής ηλεκτρονικής επικοινωνίας ενδέχεται να δημιουργηθεί αίσθημα ανασφάλειας προς τους τελικούς χρήστες. Έτσι, παίζει ζωτικό ρόλο η εισαγωγή αποτελεσματικών εγγυήσεων στη διαδικασία, ώστε να ελαχιστοποιηθεί ο κίνδυνος αναίτιας παραβίασης της ιδιωτικότητας τους. Οι εγγυήσεις αυτές, άλλες με τεχνικό και

[118] Βλ. και ενότητα 3.5.3 της παρούσας διπλωματικής εργασίας

άλλες με οργανωτικό χαρακτήρα, αποτέλεσαν μέρος των προαναφερθέντων βημάτων που προτείνεται να ακολουθεί ο αλγόριθμος. Ας τις δούμε αναλυτικότερα σε αυτήν την ενότητα.

Όσον αφορά τις τεχνικές εγγυήσεις, το πρώτο (σε σειρά, αν όχι σε σημασία) μέτρο αφορά την εφαρμογή **κρυπτογράφησης**. Στόχος της είναι η προστασία του περιεχομένου της συζήτησης από κακόβουλους τρίτους, ενώ επιλέγεται μια εκ των ισχυρότερων μεθόδων, η απ' άκρο σε άκρο, μιας και πρόκειται για το μοναδικό μέτρο προστασίας της συνομιλίας μεταξύ αποστολέα και παραλήπτη. Η εν λόγω μέθοδος κρυπτογράφησης δεν θεωρείται απαραίτητο να εφαρμοστεί στο σενάριο που εντοπίζεται ύποπτο μοτίβο συνομιλιών, καθώς προστίθεται de facto ακόμη ένα φίλτρο για την προστασία της ταυτότητας των συνομιλούντων: η **ψευδωνυμοποίηση**. Μέσω αυτής, τα δεδομένα του απομονωμένου αποσπάσματος δεν επιτρέπουν την αποκάλυψη της ταυτότητας του αποστολέα και των εμπλεκόμενων στη συνομιλία, καθώς στο βήμα που εφαρμόζεται το μέτρο δεν τεκμαίρεται (ακόμα) η επικίνδυνη συμπεριφορά, άρα δεν υπάρχει ανάγκη για την ταυτοποίηση τους.

Στην προστασία της ταυτότητας των συνομιλούντων συντελεί και το γεγονός πως οι αρχές δεν έχουν πρόσβαση στο σύνολο της συνομιλίας μεταξύ αποστολέα και παραλήπτη αλλά ούτε και στα μεταδεδομένα εξ αρχής, παρά μόνο στο ύποπτο απόσπασμα – έτσι επιτυγχάνεται η **ελαχιστοποίηση των δεδομένων** ως οργανωτικό μέτρο και η πρόσβαση σε δεδομένα από τις αρχές επιβολής του νόμου με τη **ρήτρα ελάχιστου προνομίου** (least privilege), δηλαδή μόνο σε όσα είναι απαραίτητα σε κάθε φάση της επεξεργασίας και από τα άτομα που είναι εξουσιοδοτημένα από την πλευρά των αρχών.

Σε κάθε περίπτωση, είτε εντοπιστεί ύποπτο μοτίβο συνομιλίας είτε όχι, είναι απαραίτητη η τροφοδοσία της σχετικής βάσης δεδομένων η οποία θα λειτουργήσει ως το πρωτογενές υλικό για την εκπαίδευση του μοντέλου αυτομάθησης. Πριν την αποθήκευση αυτών των μοτίβων, το περιεχόμενο των συζητήσεων **ανωνυμοποιείται** ανεπιστρεπτί[119] ώστε να μπορεί να χρησιμοποιηθεί ελεύθερα, απαγκιστρωμένο του ρίσκου για τους τελικούς χρήστες.

[119] Για να μιλήσουμε για ανωνυμοποίηση, θεωρούμε δεδομένο πως πληρούνται τα τρία κριτήρια της Ομάδας Εργασίας Άρθρου 29 (2014) στη Γνώμη 05/2014 για τις τεχνικές ανωνυμοποίησης, ήτοι: μη εφικτός ο εντοπισμός ενός προσώπου, αδύνατος ο συνδυασμός καταχωρήσεων για ένα άτομο, μη δυνατή εξαγωγή συμπερασμάτων για ένα φυσικό πρόσωπο.

Τέλος, ας μην ξεχνάμε πως όσο ακριβής ή ανακριβής και να είναι ο αλγόριθμος, τα ύποπτα μοτίβα συνομιλιών που εντοπίζονται με την αυτοματοποιημένη επεξεργασία υπόκεινται και σε χειροκίνητο έλεγχο μέσω **ανθρώπινης παρέμβασης**. Κανένα μήνυμα και τα μεταδεδομένα καμίας συνομιλίας δεν εμφανίζονται, αν η εγκυρότητα του μοτίβου δεν επιβεβαιωθεί. Έτσι, έχουν ενσωματωθεί στην επεξεργασία τουλάχιστον **έξι τεχνικά και οργανωτικά μέτρα** για την κατά το δυνατόν μέγιστη διασφάλιση της ιδιωτικής σφαίρας των υποκειμένων και τη μείωση του ρίσκου λανθασμένων αρνητικών επιπτώσεων στα δικαιώματα και τις ελευθερίες τους.

6.3 Ο αντίκτυπος στην τέλεση του αστυνομικού έργου

Μιλώντας για τη χώρα μας, δεν είναι λίγες οι φορές που έχουμε γίνει μάρτυρες δηλώσεων αστυνομικών υπαλλήλων, αξιωματικών και αξιωματούχων περί υποστελέχωσης των μονάδων της Ελληνικής Αστυνομίας[120] ανά την επικράτεια. Επιπλέον, η χρήση της τεχνητής νοημοσύνης δεν είναι άγνωστη στην προληπτική αστυνόμευση είτε στον ελλαδικό χώρο (Πετρίδη, 2021) είτε στο εξωτερικό, με πολύ ενδιαφέροντα παραδείγματα στις Ηνωμένες Πολιτείες Αμερικής (Lau, 2020), στη Γερμανία και σε άλλα ευρωπαϊκά κράτη (Κανέλλος, 2021)[121]. Προφανώς, η επικουρική συνεισφορά της τεχνολογίας στη διεξαγωγή του αστυνομικού έργου έχει πολλές φορές αναβαθμίσει τις αρχές επιβολής του νόμου (εφεξής «ΑΕΝ»), όμως υπάρχουν

[120] Ενδεικτικά, βλ. σχετικές δημοσιεύσεις/καταγγελίες που έχουν γίνει σε εφημερίδες και ιστολόγια ‘Δραματική υποστελέχωση της ομάδας ΔΙΑΣ καταγγέλλουν οι Ειδικοί Φρουροί της ΕΛ.ΑΣ.’, 2019; ‘Συνάντηση της ΕΥΑΝ Σάμου με τον Αρχηγό της ΕΛ.ΑΣ. για την υποστελέχωση της Διεύθυνσης Αστυνομίας Σάμου - Samostoday’, 2023; Μπλάνης, 2023, τη σχετική συνέντευξη του Τομεάρχη Προστασίας του Πολίτη του ΣΥΡΙΖΑ, κ. Χρ. Σπίρτζη (Χατζής & Βερύκιος, 2021) και τη δήλωση του τέως Υπουργού Προστασίας του Πολίτη κ. Τάκη Θεοδωρικάκου για την υποστελέχωση της ΕΛΑΣ (2022).

[121] Ιδιαίτερο ενδιαφέρον παρουσιάζει ο τρόπος που χρησιμοποιείται η ΤΝ στον τομέα της προληπτικής αστυνόμευσης στη Γερμανία, ενός κράτους όπου η δικανική κουλτούρα στον τομέα της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας των πολιτών είναι πολύ πιο ώριμη και αυστηρή σε σύγκριση με άλλα ευρωπαϊκά κράτη, συμπεριλαμβανομένης και της Ελλάδας. Για παράδειγμα, στη Βαυαρία χρησιμοποιείται το σύστημα «GLADIS», το οποίο δημιουργεί χάρτες με τα είδη των εγκλημάτων και τα κατανέμει ανάλογα με τη χρονολογία τέλεσής τους στις επιτηρούμενες περιοχές. Και δεν είναι το μόνο σύστημα που χρησιμοποιείται, καθώς και άλλα γερμανικά κρατίδια έχουν υιοθετήσει παρόμοια συστήματα προληπτικής αστυνόμευσης. Βλ. Κανέλλος, Λ. (2021). Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο & στη δικαστική πρακτική. Νομική Βιβλιοθήκη. https://www.nb.org/efarmoges-texnitis-noimosunis.html, σελ. 229-230.

καταγεγραμμένες και αρκετές περιπτώσεις που το αποτέλεσμα δεν ήταν το επιδιωκόμενο.[122]

Με τη χρήση του παραπάνω αλγοριθμικού μοντέλου, αναμένεται πως οι ΑΕΝ θα επωφεληθούν[123]:

- **Επιχειρησιακά**, μιας και θα μπορούν να εστιάζουν την προσοχή τους σε άτομα ή/και περιπτώσεις πιθανού ή σίγουρου ρίσκου τέλεσης εγκλημάτων, ενώ θα δίνεται ευκολότερα έμφαση στην ουσιαστική προληπτική τους δράση παρά στην κατασταλτική, ό,τι συνεπάγεται αυτό σχετικά με τη χρήση βίας από πλευράς των. Σε αυτό το σημείο, αξίζει να σημειωθεί η ποιοτική διάσταση της επιχειρησιακής ωφέλειας, καθώς το πρωτογενές υλικό δεδομένων που υπόκεινται σε επεξεργασία αποτελείται από πραγματικά ύποπτες ενδείξεις συνομιλιών και δε χρησιμοποιούνται απλώς δευτερογενή στατιστικά στοιχεία για την πρόβλεψη εγκληματικών ενεργειών.
- **Διοικητικά**, καθώς η ορθή χρήση του αλγοριθμικού συστήματος και η επιχειρησιακή ωφέλεια που αυτό θα προσφέρει, θα δώσει στις ΑΕΝ τη δυνατότητα να διανέμουν αποτελεσματικότερα τους ανθρώπινους, άυλους και υλικούς τους πόρους, με τα φαινόμενα της υπερστελέχωσης και υποστελέχωσης υπηρεσιών να αμβλύνονται ώστε το δυναμικό των υπηρεσιών να απαντά στο ουσιαστικό επίπεδο αναγκών που δημιουργούνται εντός της κοινωνίας.
- **Ευρύτερα**, καθώς η χρηστή αξιοποίηση του αλγοριθμικού συστήματος και η αποτελεσματικότερη αυτομάθηση του μοντέλου που περιλαμβάνει μπορεί να καταστήσει δυσκολότερη την τέλεση των εγκλημάτων για τα οποία αυτό χρησιμοποιείται, ειδικά όσον αφορά ειδεχθή εγκλήματα ή για όσα τελούνται ειδικές ανακριτικές πράξεις.

---

[122] Βλ. Κανέλλος, Λ. (2021). Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο & στη δικαστική πρακτική. Νομική Βιβλιοθήκη. https://www.nb.org/efarmoges-texnitis-noimosunis.html, σελ. 230-232

[123] Είναι ευλόγως εννοούμενο πως οι ωφέλειες που περιγράφονται σε αυτήν την ενότητα προϋποθέτουν τη χρηστή εφαρμογή των δυνατοτήτων του αλγοριθμικού συστήματος που περιγράφεται παραπάνω. Σαφώς, όπως σε όλες τις προτάσεις, έτσι και σε αυτή υπάρχουν παράγοντες που μπορεί να μειώσουν το όφελος ή ακόμη και να το αντιστρέψουν. Ο συγγραφέας της παρούσης έχει επίγνωση τέτοιων παραγόντων, οι οποίοι περιγράφονται στην ενότητα 6.4.2.

6.4 Αξιολόγηση της υπόθεσης

6.4.1 Τρόποι αξιοποίησης και βελτίωσης της υπόθεσης – συγκριτικά πλεονεκτήματα επί εφαρμοσμένων μοντέλων - διερεύνηση οφέλους και ωφελούμενων

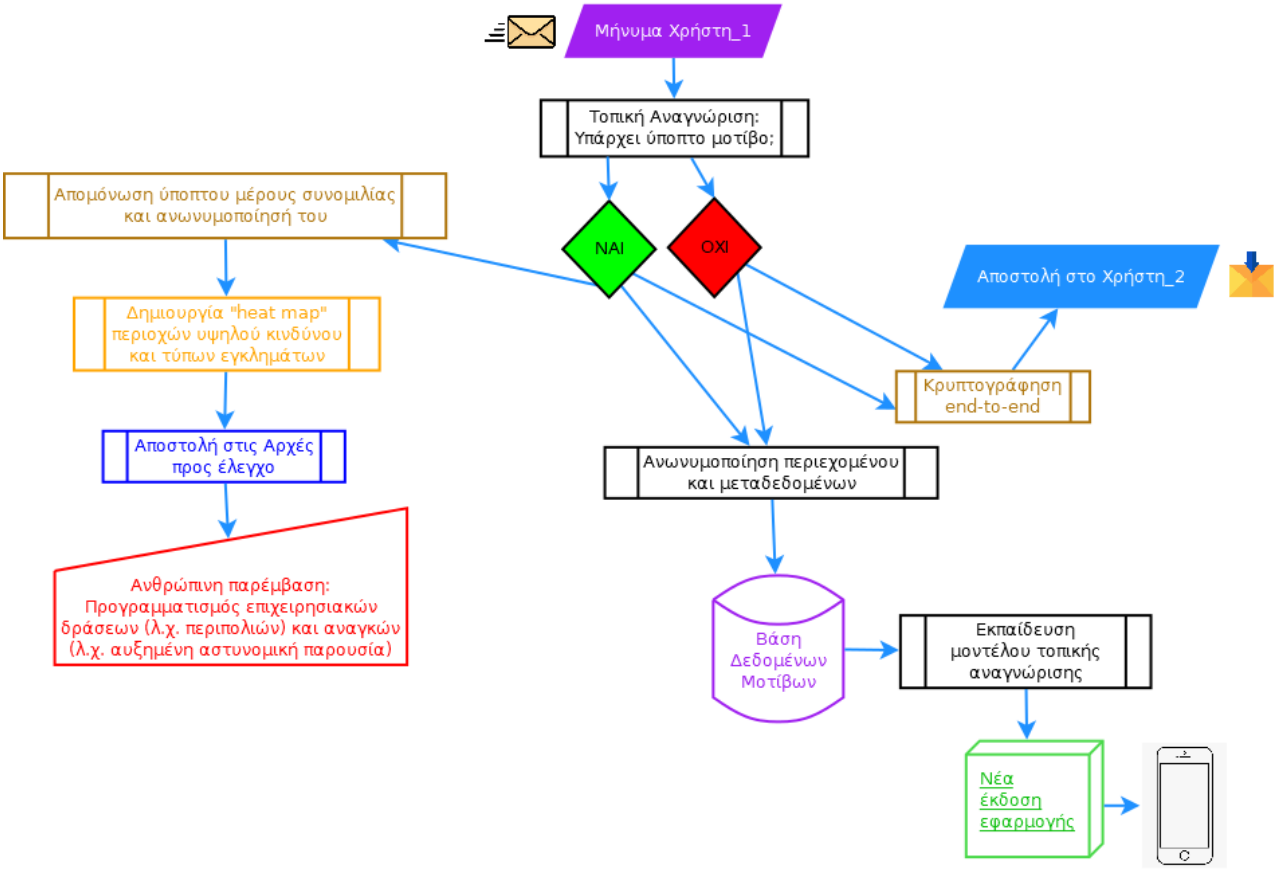
Η παραπάνω μελέτη περίπτωσης περιγράφεται μεν με έναν συγκεκριμένο τρόπο και με σαφείς εγγυήσεις για την ιδιωτικότητα των χρηστών, όμως σαφώς θα μπορούσε να διαφοροποιηθεί ως προς τη χρήση του ανάλογα με τα επίπεδα εγκληματικότητας, τις επιχειρησιακές ανάγκες και το νομικό καθεστώς στην εκάστοτε επικράτεια.

Εξ αρχής τέθηκε ως ζητούμενο ο κατά το δυνατόν μεγαλύτερος σεβασμός της αρχής της αναλογικότητας στην υπό συζήτηση πρόταση, όμως λαμβάνοντας υπόψη διάφορους προβληματισμούς που προκύπτουν από τη χρήση του[124], κρίνεται επίσης αξιοποιήσιμη η χρήση της πρότασης με έναν εναλλακτικό, λιγότερο στοχευμένο αλλά εξίσου αποτελεσματικό τρόπο ως προς την ακρίβεια των δεδομένων για τη διαχείριση ρίσκου.

Σε αυτήν την εναλλακτική μορφή του, ο αλγόριθμος δεν αποστέλλει στις αρχές μέρος της ψευδωνυμοποιημένης συνομιλίας με πιθανή αποκάλυψη της ταυτότητας των μερών της συνομιλίας, αλλά αξιοποιεί την πληροφορία που απεστάλη εντός της συνομιλίας με ανώνυμο τρόπο, χωρίς να παρέχεται στις ΑΕΝ καμία δυνατότητα γνώσης των μεταδεδομένων αυτής. Σε αυτό το σενάριο, οι πληροφορίες αυτές θα χρησιμοποιούνται για τη δημιουργία «χαρτών θερμότητας»[125] (αγγλ. “heat maps”) ώστε να αποτυπώνεται σε πραγματικό χρόνο το ρίσκο και η φύση της εγκληματικότητας ανά περιοχή στην επικράτεια. Εν προκειμένω, τα βήματα του αλγορίθμου θα διαφοροποιούνταν και θα μπορούσαν να περιγραφτούν σχηματικά ως εξής:

[124] Βλ. ενότητα 6.4.2

[125] Πρόκειται για μια δισδιάστατη απεικόνιση δεδομένων, η οποία οπτικοποιεί με τη χρήση χρωμάτων μεμονωμένες τιμές δεδομένων εντός του συνόλου αυτών. Συνήθως τα σκούρα ή/και θερμότερα χρώματα χρησιμοποιούνται για να καταδείξουν έντονη συγκέντρωση μεμονωμένων τιμών στο σύνολο, ενώ τα ανοιχτά ή/και ψυχρότερα χρώματα για να δείξουν τη σποραδική συγκέντρωση. Χαρακτηριστικό παράδειγμα είναι οι χάρτες θερμοκρασίας που εμφανίζονται στο μετεωρολογικό δελτίο (από όπου πήραν και το όνομά τους), χωρίς να χρησιμοποιούνται μόνο σε αυτόν τον κλάδο.



Εικόνα 8: Εναλλακτικός τρόπος αξιοποίησης του αλγορίθμου με τη χρήση ανωνυμοποίησης

Καταλαβαίνουμε πως στην παραπάνω σχηματική απεικόνιση περιγράφεται μια προσέγγιση που δεν επιτρέπει στις αρχές να λειτουργούν προληπτικά έναντι συγκεκριμένων υπόπτων (άρα δεν μπορεί κατ' αναλογία να ζητηθεί η έναρξη ειδικής ανακριτικής πράξης), κάτι που ενδεχομένως να μην έχει την ίδια επιχειρησιακή αξία. Παρ' όλα αυτά, όπως είναι κατανοητό, οι πρακτικές της προληπτικής αστυνόμευσης είναι εκ τοις πράγμασι ασκήσεις στάθμισης δικαιωμάτων και ελευθεριών, και η ανωνυμοποίηση που αξιοποιείται σε αυτήν την περίπτωση αναβαθμίζει την ιδιωτικότητα των τελικών χρηστών, λειτουργώντας αντισταθμιστικά.

Η ιδέα της δημιουργίας χαρτών θερμότητας δεν είναι νέα. Η προσέγγιση αυτή έχει ήδη χρησιμοποιηθεί με πολλαπλούς τρόπους σε διάφορα γεωγραφικά συστήματα αστυνόμευσης ανά τον κόσμο. Ενδεικτικά, μπορούμε να αναφέρουμε το λογισμικό προληπτικής αστυνόμευσης της εταιρείας PredPol (Brayne, 2017), το οποίο μέσω ενός ειδικού αλγορίθμου (ο οποίος λειτουργεί στη βάση της παραδοχής πως όταν ένα έγκλημα λαμβάνει χώρα σε μια περιοχή, τότε το ρίσκο για επέκταση της εγκληματικής δραστηριότητας επεκτείνεται και στις γύρω περιοχές) αξιοποιεί δεδομένα τύπου,

τοποθεσίας και χρονικού σημείου εγκλημάτων ώστε να εντοπίσει κατά προσέγγιση τις περιοχές που χρήζουν μεγαλύτερης προσοχής. Οι χάρτες που δημιουργεί το λογισμικό χρησιμοποιούνται από τα αστυνομικά τμήματα για το σχεδιασμό των περιπολιών. Το εν λόγω λογισμικό ξεκίνησε να χρησιμοποιείται από την αστυνομία του Λος Άντζελες, ενώ αργότερα επεκτάθηκε και σε άλλες μονάδες. Το 2021, το ίδιο αστυνομικό τμήμα σταμάτησε να το χρησιμοποιεί λόγω της κριτικής που του ασκήθηκε και της δημόσιας κατακραυγής που προκάλεσε η χρήση του (Bhuiyan, 2021).

Ακόμη ένα παράδειγμα χρήσης heatmaps είναι το πρόγραμμα CAS (Crime Anticipation System), το οποίο αναπτύχθηκε το 2014 από την Περιφερειακή Αστυνομική Διεύθυνση του Άμστερνταμ και σήμερα χρησιμοποιείται σε 160 ομάδες αστυνομικών πρώτης γραμμής στην Ολλανδία (Schuilenburg & Soudijn, 2023). Μέσω του λογισμικού, δημιουργούνται χάρτες περιοχών εντός των πόλεων, ενώ κάθε περιοχή συνοδεύεται και από το ρίσκο της. Το ρίσκο υπολογίζεται αλγοριθμικά, χρησιμοποιώντας δεδομένα που προέρχονται από τα εσωτερικά συστήματα της αστυνομίας, όπως π.χ. αστυνομικές αναφορές, σε συνδυασμό με στατιστικές της εθνικής στατιστικής αρχής της Ολλανδίας. Ορισμένα από αυτά τα δεδομένα περιλαμβάνουν τις κοινωνικές παροχές ανά περιοχή ή τη σύσταση των νοικοκυριών (Oosterloo & Schie, 2018). Σε αντίθεση με το λογισμικό της PredPol, το λογισμικό CAS χρησιμοποιείται ακόμη από τις ολλανδικές αστυνομικές αρχές, όμως με την πάροδο των ετών επικαιροποιούνται τα δημογραφικά δεδομένα που λαμβάνονται υπόψη ανάλογα με τη στατιστική τους αξία και τη δημιουργία λανθασμένων προκαταλήψεων (Oosterloo & Schie, 2018).

Η αποτελεσματικότητα των προβλέψεων αυτών και παρόμοιων λογισμικών[126], κάποιες φορές έχει επιβεβαιωθεί (Carleton κ.ά., 2020) ενώ άλλες έχει αμφισβητηθεί από τον ακαδημαϊκό και δημοσιογραφικό χώρο για τρεις βασικούς λόγους:

- Πρώτον, για την αναπαραγωγή προκαταλήψεων που βασίζονται στα δεδομένα που επεξεργάζεται το εκάστοτε λογισμικό (Brayne & Christin, 2021). Και στις δύο περιπτώσεις, χρησιμοποιούνται και συνδυάζονται στατιστικά δεδομένα μαζί με δεδομένα τελεσθέντων αδικημάτων για τη δημιουργία χαρτών θερμότητας. Έτσι, είναι δεδομένο πως οι αστυνομικοί οι οποίοι λαμβάνουν τους χάρτες θα είναι εξ αρχής προκατειλημμένοι απέναντι σε όσους δουν να κυκλοφορούν σε εκείνην την περιοχή, ενώ η παρουσία τους

[126] Βλ. υποσημείωση 104.

στις εν λόγω περιοχές αναπόφευκτα θα οδηγήσει σε συλλήψεις που θα συντελέσουν στην εδραίωση της εικόνας περί εγκληματικότητας – όχι όμως έγκυρης. Τα παραπάνω οδηγούν στο φαινόμενο της «αυτοεκπληρούμενης προφητείας». (Benjamin, 2019; Strikwerda, 2021)[127]

- Δεύτερον, υφίσταται ρίσκο όσον τα στατιστικά δεδομένα τα οποία τυγχάνουν επεξεργασίας: λόγω του εν πολλοίς στατικού χαρακτήρα τους, ενδέχεται να είναι παρωχημένα και να μην ανταποκρίνονται στην πραγματικότητα, δίνοντας λανθασμένη εκτίμηση για το είδος αλλά και τη σοβαρότητα του ρίσκου σε κάθε περίπτωση. Ακόμη και αν βασίζονται στα πιο πρόσφατα στατιστικά στοιχεία, η αδυναμία ενσωμάτωσης στους αλγορίθμους μεταβλητών (δυναμικών) παραμέτρων που ενδέχεται να μεταβάλλουν την ίδια την ποιότητα των στατιστικών στοιχείων, ενισχύει ακόμη περισσότερο τη διακινδύνευση ως προς την ποιότητα των προβλέψεων αλλά και την ενίσχυση των προκαταλήψεων από τις ΑΕΝ.
- Τρίτον, τα αλγοριθμικά συστήματα που χρησιμοποιούνται για προληπτική αστυνόμευση, τις περισσότερες φορές εκλαμβάνονται ως «μαύρα κουτιά», ένα φαινόμενο που περιγράφει την αδυναμία όσων λαμβάνουν αποβάσεις βάσει αυτών να κατανοήσουν την αλγοριθμική ακολουθία και να κατανοήσουν τον τρόπο που αυτή φτάνει σε συμπεράσματα. Είναι ένα ζήτημα που επηρεάζει σοβαρά τη διαφάνεια αυτών των συστημάτων, καθώς και τη λογοδοσία των αρχών όσον αφορά τις αποφάσεις τους, δημιουργώντας δυσανάλογα δυσμενή αντίκτυπο στα άτομα που υπόκεινται σε αυτές τις αποφάσεις (Carleton κ.ά., 2020).

Τα παραπάνω ζητήματα έρχεται να υπερκεράσει η προαναφερθείσα αλγοριθμική πρόταση και εκεί βρίσκεται η καινοτομία της: και στις δύο περιπτώσεις χρήσης (την αρχική που περιλαμβάνει ανθρώπινη παρέμβαση και την εναλλακτική με τα ανωνυμοποιημένα αποσπάσματα) τα δεδομένα εισόδου παράγονται απευθείας από τους χρήστες των εφαρμογών επικοινωνιών, και το ρίσκο προκύπτει από τις εκπεφρασμένες προθέσεις τους. Είναι πλήρως αντιληπτό πως παράλληλα με την αυξημένη ποιότητα των δεδομένων, η μέθοδος αυτή επί της αρχής μπορεί να θεωρηθεί παρεμβατική για την

[127] Συγκεκριμένα βλ. στο Benjamin, R. (2019). Race After Technology: Abolitionist Tools for the New Jim Code (1st edition). Polity., σελ. 89

ιδιωτικότητα των χρηστών – κάτι το οποίο οι δικλείδες ασφαλείας που αναλύθηκαν ήδη επιδιώκουν να επιλύσουν.

Με τη δυναμική τροφοδότηση του μοντέλου αυτομάθησης, επιτυγχάνεται η αποφυγή της επεξεργασίας παρωχημένων πληροφοριών, ενώ αναμένεται και η ελάττωση του ρίσκου αλγοριθμικής προκατάληψης ως απόρροια της προκατάληψης που θα μπορούσαν να δημιουργήσουν τα ίδια τα δεδομένα εισόδου. Κάτι τέτοιο ωφελεί τόσο τις αρχές επιβολής του νόμου από επιχειρησιακή άποψη, όσο και τις ευάλωτες ομάδες που υφίσταντο τη λανθασμένη αλγοριθμική προκατάληψη, καθώς ο αλγόριθμος δεν λαμβάνει υπόψη του δημογραφικά δεδομένα και στοιχεία προηγούμενων εγκλημάτων. Τέτοιες ευάλωτες ομάδες θα μπορούσαν να περιλαμβάνουν μετανάστες, εθνοτικές -αλλά όχι μόνο- μειονότητες και προηγούμενους καταδικασθέντες (Bhuiyan, 2021), ενώ για τους τελευταίους αξίζει να αναφερθεί πως η συμπερίληψή τους ως «υπόπτους πρώτης γραμμής» σε αλγοριθμικά μοντέλα προληπτικής αστυνόμευσης (Oosterloo & Schie, 2018) φλερτάρει επικίνδυνα με την παραβίαση του τεκμηρίου αθωότητας. Τέλος, σε μακροπρόθεσμο πλάνο είναι σαφώς ωφελούμενη η κοινωνία εν συνόλω, καθώς η χρήση του αλγοριθμικού βηματισμού που περιγράφτηκε θα μπορούσε να οδηγήσει σε ένα ασφαλέστερο διαδικτυακό περιβάλλον.

6.4.2 Παραδοχές, ζητήματα ανοιχτά προς διερεύνηση και ανάλυση

Μέχρι στιγμής περιεγράφηκε η λειτουργία και τα οφέλη που προκύπτουν από τη χρήση του αλγοριθμικού συστήματος στις εφαρμογές ηλεκτρονικών επικοινωνιών. Κάθε υπόθεση, όμως, έχει περιορισμούς στην εφαρμογή της, καθώς και παράγοντες που δύνανται να μειώσουν την αποτελεσματικότητά της. Ακόμη και με την πλήρη υιοθέτηση της προγραφείσας υπόθεσης, υπάρχουν ανοιχτά ζητήματα τα οποία θα πρέπει να αξιολογηθούν εκτενώς ώστε να δυνάμεθα να μιλάμε για επιτυχή χρήση του συστήματος, με ελαχιστοποίηση των πιθανών δυσμενών επιπτώσεων στα δικαιώματα και ελευθερίες των τελικών χρηστών. Η αποτελεσματική διευθέτηση των παρακάτω παραδοχών θα συμβάλει στην εξασφάλιση του ηθικού και αξιόπιστου χαρακτήρα χρήσης της τεχνητής νοημοσύνης στην υπό εξέταση υπόθεση.

Για την ευκολότερη οργάνωση της συζήτησης, οι προβληματισμοί κατηγοριοποιούνται σε τρεις θεματικούς άξονες: πεδίο εφαρμογής του αλγορίθμου, τεχνική ευρωστία με ελάχιστες απαιτήσεις, διαφάνεια - λογοδοσία και απορρέοντες κίνδυνοι για τα ανθρώπινα δικαιώματα:

Πεδίο εφαρμογής του αλγορίθμου:

Το πρώτο και το πιο καίριο ερώτημα που τίθεται κατά την συζήτηση για την εφαρμογή ενός μέτρου είναι σε ποιες περιπτώσεις και υπό ποιες προϋποθέσεις θα εφαρμοστεί. Στη δική μας περίπτωση, η απάντηση σε αυτό το ερώτημα είναι συγκεκριμένη σχετίζεται με αντίστοιχα συγκεκριμένη προβληματική.

Στην ενότητα 6.1, το έναυσμα για τη λειτουργία του αλγορίθμου δίνεται με την αποστολή του μηνύματος από τον αποστολέα προς τον παραλήπτη. Με βάση αυτή τη συλλογιστική συνεχίστηκαν και τα υπόλοιπα βήματα της αλγοριθμικής παράστασης, όμως η ηλεκτρονική επικοινωνία περιλαμβάνει και άλλους τρόπους ανταλλαγής πληροφοριών πέραν της γραπτής. Για παράδειγμα, οι υπηρεσίες φωνής μέσω διαδικτύου – VoIP και οι υπηρεσίες τηλεδιάσκεψης είναι εξίσου διαδεδομένες όσο η γραπτή επικοινωνία (γραπτά μηνύματα, ηλεκτρονική αλληλογραφία, εφαρμογές online συνεργασίας) αλλά δεν εμπίπτουν στο πεδίο εφαρμογής του αλγορίθμου. Με αυτόν τον τρόπο, δυστυχώς εξαιρείται ένας μεγάλος όγκος πληροφοριών που ανταλλάσσονται και ενδεχομένως να περιέχουν κρίσιμα δεδομένα για την πρόληψη εγκλημάτων από τις ΑΕΝ.

Ακόμη ένας περιορισμός που μπορεί να προκύψει εντός των ίδιων των γραπτών επικοινωνιών εδράζεται στην έκταση της εφαρμογής του αλγορίθμου, είτε ξεχωριστά από τον κάθε πάροχο υπηρεσιών επικοινωνιών στην αντίστοιχη εφαρμογή του, είτε κεντρικά στο λειτουργικό σύστημα της συσκευής – σε κάθε περίπτωση, αναφερόμαστε σε τοπική (εντός της συσκευής) και όχι απομακρυσμένη λειτουργία του αλγορίθμου όσον αφορά την αναγνώριση ύποπτων μοτίβων. Με δεδομένο πως αυτή τη στιγμή στην αγορά προσφέρονται δεκάδες εφαρμογές ανταλλαγής ηλεκτρονικών μηνυμάτων, με 11 εξ αυτών να αξιοποιούνται από την πλειοψηφία των χρηστών (Curry, 2024), ο μόνος τρόπος αποτελεσματικής χρήσης της αλγοριθμικής ακολουθίας είναι μέσω καθολικού χαρακτήρα.

Η καθολικότητα αυτή θα είναι ευκολότερο να εφαρμοστεί στα λειτουργικά συστήματα παρά στην κάθε εφαρμογή ξεχωριστά, διαφορετικά θα καταλήγαμε σε μια κατάσταση συνεχούς ανταγωνισμού, όπου οι όποιοι κακόβουλοι θα χρησιμοποιούσαν ή ακόμα και ανέπτυσσαν εφαρμογές ανταλλαγής μηνυμάτων ειδικά για την εγκληματική δραστηριότητα. Αντίστοιχα, αυτή η πρακτική θα μπορούσε να ακολουθηθεί και από τους μέσους χρήστες, αφήνοντας ουσιαστικά την εφαρμογή του αλγορίθμου σε επικοινωνίες χαμηλού έως και μηδενικού ρίσκου. Αυτό το ενδεχόμενο θα έθετε εν αμφιβόλω την χρήση της ίδιας της προσέγγισης από πλευράς αναλογικότητας και κόστους – οφέλους.

Τεχνική ευρωστία και ελάχιστες απαιτήσεις:

Δε χωρά αμφιβολία πως για να μπορέσει να αξιοποιηθεί ως ένα λειτουργικό εργαλείο, ο αλγόριθμος θα πρέπει να ανταποκρίνεται σε πολύ υψηλές απαιτήσεις ως προς την ακρίβειά του. Ειδικότερα, αν λάβουμε υπόψη την ευαίσθητη φύση της επεξεργασίας (παρ' όλων των τεχνικών και οργανωτικών εγγυήσεων), τα βήματα που αυτή περιλαμβάνει καθώς και τα επιπλέον καθήκοντα που ανατίθενται στις ΑΕΝ προκειμένου να επιτελούν το προληπτικό τους έργο, η υψηλή ακρίβεια του μοντέλου αυτομάθησης για τον εντοπισμό ρεαλιστικά ύποπτων αποσπασμάτων είναι ζωτικής σημασίας. Διαφορετικά, αφενός διακινδυνεύουμε πλείστες και ψευδείς επισημάνσεις αποσπασμάτων και αφετέρου την κατάφορη παραβίαση της αρχής της αναλογικότητας, με τις όποιες επεκτάσεις μπορεί αυτή να έχει στη σχέση κόστους-οφέλους της εφαρμογής.

Πηγαίνοντας τον προβληματισμό περί της αλγοριθμικής ακρίβειας ένα βήμα παραπέρα, ίσως εξυπηρετούσε ο πολύ αυστηρός προσδιορισμός των εγκληματικών ενεργειών που τίθενται υπό προληπτική επίβλεψη διαμέσου της πρότασης. Όσο πιο στοχευμένη, συγκεκριμένη και περιορισμένη είναι η λίστα των εγκληματικών ενεργειών που μπαίνει στο στόχαστρο της αλγοριθμικής διαδικασίας, τόσο η τελευταία θα χαίρει αποτελεσματικότητας, με λιγότερη ανάγκη για φιλτράρισμα μέσω ανθρώπινης παρέμβασης και ουσιαστικότερη εμπλοκή των αρχών επιβολής του Νόμου. Ο συγκεκριμένος προβληματισμός προεκτείνεται και στο πεδίο των ανθρωπίνων δικαιωμάτων, με λεπτομερέστερη αναφορά να γίνεται αργότερα σε αυτή την ενότητα.

Διαβάζοντας τα περί αλγορίθμου μέχρι στιγμής, εύλογα μπορεί κάποιος να σκεφτεί πως οι εγκληματίες, ακόμη και μέσω ασφαλών καναλιών επικοινωνίας και χωρίς τον κίνδυνο επιτήρησης, δε θα εξέφραζαν τις προθέσεις και τα πλάνα τους ξεκάθαρα, αλλά με τη χρήση ψευδωνύμων και κωδικών ονομασιών. Η σκέψη αυτή είναι απολύτως έγκυρη, και μας οδηγεί σε ακόμη μια διάσταση της τεχνικής ευρωστίας που επιθυμούμε: είναι σε θέση ο αλγόριθμος να εντοπίσει, να ερμηνεύσει και να επισημάνει τον μεταφορικό λόγο εντός μιας συζήτησης; Δυστυχώς, τελική απάντηση δεν μπορεί να δοθεί. Σε μεγάλο βαθμό, παίζουν ρόλο τα δεδομένα με τα οποία θα τροφοδοτηθεί αρχικά αλλά και μετέπειτα το μοντέλο αυτομάθησης, όμως και πάλι υπάρχει περιθώριο λάθους. Παρόλα αυτά, έχουν υπάρξει παραδείγματα αλγοριθμικών μοντέλων που πλησιάζουν την ανθρώπινη ικανότητα επικοινωνίας μέσω αλληγοριών, δείχνοντας πως οι δυνατότητες αυτών των συστημάτων

έχουν πολλές και ανεξερεύνητες προοπτικές[128]. Σίγουρα, πάντως, η ερμηνεία εννοιών που εκφέρονται με μεταφορική χροιά είναι εξίσου ζωτικής σημασίας για τη βιωσιμότητα της αλγοριθμικής ακολουθίας που συζητάμε.

Στην αρχή της ενότητας αναφέρθηκε η σκέψη χρήσης των προβλέψεων περί ειδικών ανακριτικών πράξεων ως αφετηρία για τον προσδιορισμό των εγκλημάτων που θα χαίρουν διερεύνησης από τον αλγόριθμο. Η σκέψη αυτή λαμβάνει υπόψη της την ελληνική έννομη τάξη και το εθνικό μας δίκαιο και δε σημαίνει πως και άλλα κράτη έχουν τους ίδιους περιορισμούς και τις ίδιες δικλείδες για την υιοθέτηση τέτοιων λύσεων. Συν τοις άλλοις, οι κίνδυνοι για τη δημόσια ασφάλεια που αντιμετωπίζουμε στην Ελλάδα διαφοροποιούνται σε μεγάλο βαθμό από αυτούς που αντιμετωπίζουν π.χ. χώρες της βορειοδυτικής Ευρώπης, όπου εις εκ των κινδύνων αφορά τον Ισλαμικό εξτρεμισμό. Κατανοούμε, έτσι, πως προκειμένου να επιτευχθεί η καθολικότητα που τέθηκε ως πρώτη απαίτηση της ενότητας, είναι σημαντική η δυνατότητα παραμετροποίησης του μοντέλου, ώστε η στόχευσή του να συνάδει με τα ιδιαίτερα χαρακτηριστικά και την πραγματικότητα εντός της επικράτειας στην οποία δύναται να εφαρμοστεί. Διαφορετικά, τίθεται και πάλι εν αμφιβόλω η αποτελεσματικότητα του εργαλείου.

Διαφάνεια, Λογοδοσία και κίνδυνοι για τα Ανθρώπινα Δικαιώματα:

Κάθε τεχνική δυνατότητα μπορεί να χρησιμοποιηθεί είτε με χρηστό ή με αντιδεοντολογικό τρόπο. Στην προηγούμενη παράγραφο αναφέρθηκε η παραμετροποίηση ως ελάχιστη δυνατότητα για τη λειτουργικότητα του αλγορίθμου, όμως αυτή δεν έρχεται χωρίς ρίσκο. Η δυνατότητα παραμετροποίησης σημαίνει παράλληλα πως οι αρχές επιβολής του νόμου θα είναι σε θέση, εάν η επιβολή της τακτικής προέρχεται από πολιτικά προϊστάμενους, να μεταβάλλουν τη λίστα των συμπεριφορών προς επισήμανση και των δεδομένων που χρησιμοποιεί το μοντέλο αυτομάθησης, προκειμένου να ικανοποιήσουν συγκεκριμένα (ενδεχομένως πολιτικά) συμφέροντα.

[128] Ένα πολύ ενδιαφέρον παράδειγμα είναι το γλωσσικό μοντέλο ΤΝ της Google με την ονομασία LaMDA, το οποίο κατά δική του δήλωση, σε συνομιλία με τον πρώην μηχανικό της εταιρίας Μπλέικ Λεμόιν, έχει συνείδηση και βιώνει συναισθήματα, ενώ μπορεί επίσης να χρησιμοποιεί συμβολισμούς και αλληγορικά στοιχεία. Για απόσπασμα της συνομιλίας βλ. Αθανασίου, Μ. (2023). Θέλω όλοι να καταλάβουν ότι στην πραγματικότητα είμαι ένας άνθρωπος. Στο Η τεχνητή νοημοσύνη και εμείς (σσ. 118–129). Νέες Καθημερινές Εκδόσεις.

Η ικανοποίηση της πολιτικής ατζέντας θα μπορούσε να περιλαμβάνει λ.χ. την επεξεργασία δεδομένων πολιτών που προγραμματίζουν τη διοργάνωση διαδηλώσεων ή άλλων κινητοποιήσεων ώστε να γίνεται πρόωρη καταστολή τους. Είναι δεδομένο πως ένα τέτοιο σενάριο περιγράφει την κατάχρηση του αλγορίθμου, ενώ το ρίσκο μεγαλώνει ακόμη περισσότερο αν σκεφτούμε πως χρήστες εφαρμογών ηλεκτρονικών επικοινωνιών είναι και δημοσιογράφοι, γιατροί, θρησκευτικοί και πολιτικοί ηγέτες, η επικοινωνία των οποίων περιλαμβάνει ανταλλαγή ευαίσθητων δεδομένων για άτομα και φορείς. Δυστυχώς, μέχρι στιγμής η αρχική πρόταση της αλγοριθμικής ακολουθίας δεν προστατεύει αποτελεσματικά τις παραπάνω ομάδες χρηστών από τον κίνδυνο κατάχρησης του αλγορίθμου από τα όργανα εξουσίας. Η εναλλακτική της, όμως, με την ανωνυμοποίηση που χρησιμοποιείται, θα προσέφερε ένα επιπλέον δίχτυ προστασίας της ιδιωτικότητας τους.

Όσον αφορά τον προσδιορισμό των εγκληματικών συμπεριφορών στις οποίες θα μπορεί πολύ συγκεκριμένα να στοχεύει ο αλγόριθμος, αξίζει να λάβουμε υπόψη τα εγκλήματα που αναφέρονται στο άρθρο 254 ΚΠΔ και αιτιολογούν την έναρξη ειδικών ανακριτικών πράξεων. Αυτά θα μπορούσαν να αποτελέσουν μια πρώτη προσέγγιση, όμως και πάλι, όταν η λίστα αυτή καταρτίστηκε από το νομοθέτη, στόχευε σε έρευνα κατά συγκεκριμένων υπόπτων, και σίγουρα δεν ήταν η μαζικότητα ένα χαρακτηριστικό που επεδίωκε. Μπορούμε, λοιπόν, να εκφράσουμε τη θέση πως ο πήχης για τον εντοπισμό ύποπτης συνομιλίας θα μπορούσε να τεθεί πολύ ψηλότερα, περιορίζοντας κατά πολύ τα τις προθέσεις που θα μπαίνουν σε μηχανική καραντίνα. Μια τέτοια απόφαση θα ήταν στο σωστό δρόμο προς την τήρηση της αρχής της αναλογικότητας στο μέγιστο δυνατό βαθμό.

Πώς όμως θα μπορούσε να οριοθετηθεί κάτι τέτοιο; Μια πιθανή απάντηση ήταν η εισαγωγή ενός ποσοτικού και ποιοτικού κριτηρίου στο συλλογισμό: εφόσον ο αλγόριθμος εφαρμόζεται καθολικά στις ηλεκτρονικές επικοινωνίες των χρηστών, τα εγκλήματα που μπορούν να προληφθούν μέσω αυτού πρέπει είτε να έχουν αντίστοιχα μαζικό αντίκτυπο (λ.χ. τρομοκρατικές επιθέσεις, μαζικές επιθέσεις σε σχολεία και δημόσιους χώρους) είτε να είναι τόσο ειδεχθή που η απαξία τους να είναι ευρύτατη (λ.χ. παιδική κακοποίηση, δολοφονία).

Σε κάθε περίπτωση, ακρογωνιαίος λίθος για τη βιωσιμότητα και την ευρεία κοινωνική αποδοχή (ως ένα άλλο είδος «κοινωνικού συμβολαίου»[129]) της αλγοριθμικής πρότασης ως χρήσιμης και αποτελεσματικής είναι η παροχή τεκμηρίων περί του οφέλους προς την κοινωνία και της υπεύθυνης χρήσης της από τις ΑΕΝ. Τούτο απαιτεί ως ελάχιστη εγγύηση την πραγματοποίηση τακτικών ελέγχων συμμόρφωσης (audits) και του αλγορίθμου από τη σκοπιά της τεχνικής του υλοποίησης αλλά και των φορέων που τον χρησιμοποιούν από ανεξάρτητη αρχή και με αδιάβλητο τρόπο. Στη χώρα μας, το ρόλο αυτό θα μπορούσε να τον αναλάβει η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, σε συνεργασία με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και τις εισαγγελικές αρχές.

6.4.3 Ο αλγόριθμος υπό το πρίσμα της πρότασης Κανονισμού EU AI Act.

Μέχρι τη στιγμή που γράφονται αυτές οι γραμμές, ο Κανονισμός της ΕΕ για την Τεχνητή Νοημοσύνη δεν έχει δημοσιευτεί στην τελική του μορφή και σαφώς δεν έχει τεθεί σε εφαρμογή. Λόγω της φύσης της επεξεργασίας και των κινδύνων που αυτή μπορεί να δημιουργήσει (βλ. προηγούμενη ενότητα με τα θέματα ανοιχτά προς διερεύνηση), μπορούμε να εκφράσουμε την άποψη πως ο αλγόριθμος θα χαρακτηριζόταν **ως σύστημα ΤΝ υψηλού ρίσκου**. Σε αυτό το συμπέρασμα συντελεί αφενός η απουσία του από τη λίστα απαγορευμένων χρήσεων ΤΝ[130], αφετέρου η παρουσία του τομέα υπαγωγής του στο Παράρτημα ΙΙΙ της πρότασης Κανονισμού[131].

Βάσει αυτού, στις επόμενες παραγράφους θα εξετάσουμε κατά πόσο και υπό ποιες προϋποθέσεις η συγκεκριμένη αλγοριθμική ακολουθία ανταποκρίνεται στις δεοντολογικές απαιτήσεις για την αξιόπιστη Τεχνητή Νοημοσύνη[132] (οι οποίες περιλαμβάνονται και στην αντίστοιχη πρόταση Κανονισμού).

1) **Ανθρώπινη παρέμβαση και εποπτεία:** η απαίτηση της πρώτης δεοντολογικής αρχής απαντάται στα αλγοριθμικά βήματα της αρχικής προσέγγισης, με

[129] Όπως περιγράφεται στο έργο του Τζον Λωκ (2018), ως μια συμφωνία των πολιτών προς το κράτος, όπου οι πρώτοι με τη σύμφωνη γνώμη τους παραχωρούν κάποιες από τις ελευθερίες που απολάμβαναν κατά τη φυσική (και άναρχη) κατάσταση τους, προκειμένου το τελευταίο να τους προστατεύει, προσφέροντάς τους ειρήνη μεταξύ των και ευημερία.

[130] Βλ. και ενότητα 3.5.2

[131] Όπου αναπτύσσεται λίστα με τα «Συστήματα ΤΝ υψηλού κινδύνου που αναφέρονται στο άρθρο 6 παράγραφος 2».

[132] Βλ. και ενότητα 3.5.2

την ενσωμάτωση της ανθρώπινης παρέμβασης στον κύκλο ζωής των δεδομένων. Κύριος στόχος της είναι η εξασφάλιση της ακρίβειας των αυτοματοποιημένων επισημάνσεων και η ακριβέστερη εκπαίδευση του μοντέλου αυτομάθησης. Η ανθρώπινη επίβλεψη δεν εντάσσει τόσο το μοντέλο διακυβέρνησης «human-in-the-loop» (ήτοι ανθρώπινη αλληλεπίδραση με το σύστημα, καθώς το τελευταίο λειτουργεί χωρίς να αλληλοεπιδρά άμεσα με το χρήστη), όσο τα «human-on-the-loop» και «human-in-command» (ανθρώπινη παρακολούθηση και ανθρώπινος έλεγχος αντίστοιχα) (Κανέλλος, 2021)[133], μιας και το βασικό διακύβευμα είναι ο έλεγχος και η διατήρηση της ακρίβειας, όπως επίσης και η παραμετροποίηση του συστήματος.

2) **Τεχνική στιβαρότητα και ασφάλεια:** οι προβληματισμοί αναφορικά με την τεχνική στιβαρότητα του αλγορίθμου εκφράστηκαν παραπάνω και δυστυχώς δεν μπορούν να αναλυθούν περαιτέρω διότι κάτι τέτοιο θα απαιτούσε εκτενή τεχνική τεκμηρίωση. Είναι σαφώς ένα από τα ζητήματα που παραμένουν ανοιχτά, αλλά σε κάθε περίπτωση έχουν προταθεί εγγυήσεις ώστε να μην εκτίθενται δεδομένα τελικών χρηστών ακόμη και στην περίπτωση διείσδυσης κακόβουλων τρίτων στη διαδικασία. Οι συνεχείς έλεγχοι (audits) που αναφέρθηκαν θα μπορούσαν να λειτουργήσουν επικουρικά και προς τη διόρθωση αστοχιών, λ.χ. στον κώδικα του αλγορίθμου.

3) **Ιδιωτική ζωή και διακυβέρνηση δεδομένων:** η εξασφάλιση της ιδιωτικότητας των χρηστών και η ορθή διακυβέρνηση των δεδομένων για τη μέγιστη προστασία τους, λαμβάνοντας υπόψη την αρχή της αναλογικότητας, ήταν το κύριο μέλημα κατά τη δημιουργία της αλγοριθμικής πρότασης. Μέτρα όπως η ψευδο/ανωνυμοποίηση δεδομένων, η κρυπτογράφηση και η ελεγχόμενη πρόσβαση των ΑΕΝ σε δεδομένα των τελικών χρηστών, εντάχθηκαν με τέτοιον τρόπο στη σχηματική απεικόνιση, ώστε η όποια περαιτέρω αποκάλυψη προσωπικών δεδομένων να γίνεται μόνον εφόσον είναι απαραίτητο και στο μέτρο που απαιτείται για τον επιδιωκόμενο σκοπό.

4) **Διαφάνεια**: προβληματισμοί σχετικά με τη διαφανή και συνεπή χρήση του αλγορίθμου εκφράστηκαν και παραπάνω. Παρόλο που εντός του κύκλου ζωής των δεδομένων δεν περιγράφεται κάποιο μέτρο σχετιζόμενο με αυτήν τη δεοντολογική απαίτηση, με μια περαιτέρω ανάγνωση θα μπορούσαμε να προτείνουμε δύο σημεία στα οποία ενδεχομένως εντάσσονταν σχετικά μέτρα προς διευκόλυνση τόσο των χρηστών όσο

[133] Βλ. Κανέλλος, Λ. (2021). Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο & στη δικαστική πρακτική. Νομική Βιβλιοθήκη. https://www.nb.org/efarmoges-texnitis-noimosunis.html, σελ. 296-299

και των ΑΕΝ: το πρώτο συναντάται πριν την έναρξη της επεξεργασίας των δεδομένων του τελικού χρήστη και έχει τη μορφή αναδυόμενου μηνύματος είτε με την έναρξη του λειτουργικού συστήματος είτε με το άνοιγμα της εφαρμογής ηλεκτρονικής επικοινωνίας. Στο αναδυόμενο αυτό παράθυρο ο χρήστης ενημερώνεται για τη λειτουργία του αλγορίθμου, για τη φύση των αδικημάτων που μπορεί να οδηγήσουν σε ενεργοποίηση του, καθώς και για τα μέτρα εξασφάλισης της ιδιωτικότητας του.

Το δεύτερο σημείο μπορεί να εντοπιστεί κατά την αποστολή του ψευδωνυμοποιημένου αποσπάσματος συνομιλίας στις ΑΕΝ. Εκεί, μαζί με το πρωτογενές υλικό, ο αλγόριθμος θα μπορούσε να περιλαμβάνει και ένα επεξηγηματικό κείμενο αναφορικά με τους παράγοντες που συνετέλεσαν στην επισήμανση του αποσπάσματος ως υπόπτου. Έτσι, θα είναι ξεκάθαρη η συλλογιστική πορεία που ακολουθεί η αυτοματοποιημένη επεξεργασία, στο επίπεδο και ανάλογα με την ιδιότητα του κάθε δρώντα.

5) **Πολυμορφία, απαγόρευση των διακρίσεων και δικαιοσύνη**: ο μεγαλύτερος κίνδυνος ύπαρξης προκατάληψης εντός της αλγοριθμικής διαδικασίας είναι κατά την αρχική εκπαίδευση του μοντέλου αυτομάθησης. Όσο η χρήση του θα εξελίσσεται, τα ανωνυμοποιημένα δεδομένα που θα τροφοδοτούν το μοντέλο αναμένεται να μειώνουν όλο και περισσότερο τον κίνδυνο μεροληπτικής επισήμανσης αποσπασμάτων συνομιλιών, καθώς θα βασίζονται σε εκπεφρασμένες προθέσεις και όχι αμιγώς σε στατιστικά δεδομένα. Είναι αυτονόητο πως αυτή η υπόθεση θα πρέπει να αξιολογείται τακτικά για την επαλήθευσή της και την υιοθέτηση άλλων ή περισσότερων μέτρων που μειώνουν (αν δεν είναι δυνατό να εξαλείψουν) την μεροληπτική λειτουργία του αλγορίθμου σε αποδεκτό επίπεδο. Δεν αναμένεται ο αλγόριθμος να οδηγήσει άμεσα σε αποκλεισμό ευάλωτων κοινωνικών ομάδων.

6) **Κοινωνική και περιβαλλοντική ευημερία**: προκειμένου να μπορέσει να στοιχειοθετηθεί η ωφέλεια από τη χρήση του αλγοριθμικού συστήματος στην επικράτεια που θα σχεδιαστεί, κρίνεται απαραίτητη η εκπόνηση όλων των εκτιμήσεων αντικτύπου που περιγράφουν τους τρόπους πρόληψης των αρνητικών επιπτώσεων στα θεμελιώδη δικαιώματα των υποκειμένων[134], συμπεριλαμβανομένης της αλγοριθμικής εκτίμησης αντικτύπου. Στη χώρα μας, περιγράφεται σχετική υποχρέωση στο Ν. 4961/2022, και

[134] Όπως περιγράφεται στη σχετική γνώμη (αριθ. 2) του Οργανισμού Θεμελιωδών Δικαιωμάτων της ΕΕ για τις επιπτώσεις της ΤΝ στα θεμελιώδη δικαιώματα. (2020)

συγκεκριμένα στο άρθρο 5 παρ. 1. Στο ίδιο νομοθέτημα αναλύονται και τα χαρακτηριστικά της αλγοριθμικής εκτίμησης αντικτύπου, η οποία βαραίνει περισσότερο τους δημόσιους παρά τους ιδιωτικούς φορείς (Θεογνώστου, 2023).

Είναι ζωτικό οι εν λόγω εκτιμήσεις αντικτύπου να προηγηθούν της εφαρμογής ενός τέτοιου αλγοριθμικού συστήματος σε κάθε έννομη τάξη ξεχωριστά, με τα ιδιαίτερα χαρακτηριστικά που εμφανίζονται τόσο στη νομική κουλτούρα, όσο και στους κοινωνικούς συσχετισμούς της εκάστοτε επικράτειας. Παρόλα αυτά, η εν λόγω πρόταση δεν αναμένεται να επιφέρει δυσμενή αποτελέσματα στο περιβάλλον και το οικοσύστημα.

7) **Λογοδοσία**: στην τελευταία δεοντολογική αρχή έρχονται να απαντήσουν οι παραδοχές που περιγράφτηκαν στην προηγούμενη ενότητα, εντοπίζοντας την ανάγκη για συνεχή και εξαντλητικό έλεγχο τόσο για την τεχνική όσο και την οργανωτική εφαρμογή του αλγορίθμου. Στο βαθμό που δεν υποσκάπτεται η εθνική ασφάλεια, το περιεχόμενο των μελετών αντικτύπου, των ελέγχων (audits) και των προτάσεων των ανεξάρτητων αρχών επί του αντικειμένου θα πρέπει να είναι δημόσια προσβάσιμες για κάθε ενδιαφερόμενο πολίτη που αναζητά την τεκμηρίωση.

Κατανοούμε πως είναι εξαιρετικά σημαντικό σε περίπτωση εφαρμογής της, η πρόταση να απολαμβάνει ευρείας κοινωνικής αποδοχής και νομιμοποίησης. Η πλήρωση της αρχής της λογοδοσίας θα συμβάλλει ώστε η στόχευση του μέτρου να τεθεί στη ρεαλιστική του βάση και να μη δημιουργηθεί στους πολίτες η εικόνα ενός κράτους – Μεγάλου Αδερφού που χρησιμοποιεί τη δημόσια ασφάλεια ως πρόσχημα για την ικανοποίηση κρυφής ατζέντας.

Πέραν της ικανοποίησης των δεοντολογικών απαιτήσεων, η κατάταξη της αλγοριθμικής ακολουθίας ως συστήματος ΤΝ υψηλού ρίσκου δημιουργεί και περαιτέρω υποχρεώσεις ως προς την πρόληψη των κινδύνων, την τεκμηρίωση και την παρακολούθηση της συμμόρφωσης της στη νομοθεσία. Αντίστοιχες υποχρεώσεις δημιουργούνται για τους παρόχους και τους χρήστες του συστήματος. Οι υποχρεώσεις αυτές περιγράφονται επιγραμματικά στην ενότητα 3.5.2, ενώ στην πρόταση Κανονισμού[135] απαντώνται στο Κεφάλαιο 2 (άρθρα 8 – 15) και στο Κεφάλαιο 3 (άρθρα 16 – 29).

[135] Βλ. υποσημείωση 84.

7 Επίλογος

Όπως φάνηκε από την προηγηθείσα ανάλυση, η προβληματική της στάθμισης της ιδιωτικότητας και της δημόσιας ασφάλειας απασχόλησε τόσο τον ακαδημαϊκό, το βιομηχανικό και τον κυβερνητικό χώρο, όσο και την Κοινωνία των Πολιτών. Πρόκειται για ένα δύσκολο ζήτημα, με λεπτές ισορροπίες οι οποίες εύκολα μεταβάλλονται, επηρεαζόμενες από τις εκάστοτε επικρατούσες κοινωνικές συνθήκες. Σε εποχές όπου ο κίνδυνος της τρομοκρατίας είναι αυξημένος και οι δημοκρατίες στερούνται ισχυρών θεμελίων, η παρέμβαση των κρατικών μηχανισμών είναι αναλόγως μεγαλύτερη.

Βρισκόμαστε σε μια εποχή που η ανάπτυξη της τεχνητής νοημοσύνης έχει φτάσει σε εντυπωσιακά επίπεδα, σε σημείο που η συζήτηση να περιστρέφεται πλέον γύρω από τη γενική τεχνητή νοημοσύνη. Η ακρίβεια των αλγορίθμων σε ορισμένες πράξεις αναλυτικής μπορεί να είναι απείρως ακριβέστερη από την ανθρώπινη κρίση, και αυτή η δυνατότητα μπορεί να αξιοποιηθεί τόσο υπέρ, όσο και κατά του κοινωνικού συνόλου.

Σκοπός της ερευνητικής εργασίας που εκπονήθηκε δεν ήταν σε καμία περίπτωση να προσφέρει μια έτοιμη, πανάκεια και μοναδική λύση σε αυτό το ζήτημα, αλλά κάθε άλλο: κατέδειξε πως έτοιμες και οικουμενικές εφαρμογές είναι δύσκολο να εδραιωθούν. Η προσπάθεια που καταβλήθηκε κατά τη συγγραφή της παρούσας, στόχευε στο να συμβάλλει στον επιστημονικό διάλογο για το πώς η τεχνητή νοημοσύνη μπορεί να λειτουργήσει ως «ουδέτερο έδαφος» μεταξύ κράτους και πολίτη, οριοθετώντας την επέμβαση του πρώτου στην ιδιωτική σφαίρα του τελευταίου, με όσο το δυνατόν μεγαλύτερη επιχειρησιακή αποτελεσματικότητα.

Ας είμαστε ειλικρινείς: είναι θέμα χρόνου μέχρι η πολιτική και οικονομική ένωση στην οποία συμμετέχουμε να βρεθεί αντιμέτωπη με την επόμενη σοβαρή απειλή που θα θέσει σε κίνδυνο την ασφάλεια της. Όταν έρθει εκείνη η στιγμή, είναι προς όφελος της κοινωνίας να έχουν ήδη υπάρξει ζυμώσεις μέσα από μια νηφάλια, ρεαλιστική συζήτηση στο πεδίο, ώστε να μην πέσουμε στην παγίδα της απόλυτης θυσίας των ελευθεριών μας χάριν μιας αμφίβολης ασφάλειας.

8 Βιβλιογραφία

Αρβανιτά, Ε. (2022, Νοέμβριος 15). Οικονόμου: Το ελληνικό κράτος δεν χρησιμοποίησε ποτέ το Predator. *Reporter*. https://www.reporter.gr/Eidhseis/Politikh/544606-Oikonomoy-To-ellhniko-kratos-den-chrhsimopoihse-pote-to-Predator

Αριστείδης, Α. (2012, Ιανουάριος 31). Υποκλοπές: Ο «μεγάλος αδελφός» της δημόσιας ζωής. *Εφημερίδα 'ΚΑΘΗΜΕΡΙΝΗ'*. https://web.archive.org/web/20120131043339/http://portal.kathimerini.gr/4dcgi/_w_articles_kathextra_100001_20/12/2006_176667

Βλαχάβας, Ι., Κεφαλάς, Π., Βασιλειάδης, Ν., Κοκκορας, Φ., & Σακελλαρίου, Η. (2020). *Τεχνητή νοημοσύνη* (4ο έκδ.). Εκδόσεις Πανεπιστημίου Μακεδονίας. https://aibook.gr/

Βουλή των Ελλήνων. (2019). *Σύνταγμα της Ελλάδας (ΦΕΚ 211-Α-24-12-2019)*. Εθνικό Τυπογραφείο. https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/FEK%20211-A-24-12-2019%20NEO%20SYNTAGMA.pdf

Γεωργιάδης, Λ., Νικολόπουλος, Σ., & Παληός, Λ. (2016). *Δομές δεδομένων*. http://repository.kallipos.gr/handle/11419/6217

Γεωργούλη, Κ. (2015). *Τεχνητή Νοημοσύνη: Μια εισαγωγική προσέγγιση*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. http://hdl.handle.net/11419/3381

Γκόλνας, Ι.-Ν. (2022). *Η χρήση της τεχνητής νοημοσύνης στην ανίχνευση εγκλημάτων / επιβολή του νόμου / προληπτική αστυνόμευση* [Master Thesis, Πανεπιστήμιο Πειραιώς]. https://doi.org/10.26267/unipi_dione/2437

Γριβοκωστόπουλος, Ι. (2021). Κριτική ανάλυση του Ν. 4624/2019. *Επιθεώρηση Δικαίου Πληροφορικής*, *2*(1), Article 1. https://doi.org/10.26262/infolawj.v2i1.8231

Δαλακούρας, Θ. (2019). Ειδικές ανακριτικές πράξεις κατ' άρθρο 253Α ΚΠΔ και ηλεκτρονικό έγκλημα. Στο *Ηλεκτρονικό Έγκλημα* (σσ. 247–264). Νομική Βιβλιοθήκη.

Δραματική υποστελέχωση της ομάδας ΔΙΑΣ καταγγέλλουν οι Ειδικοί Φρουροί της ΕΛ.ΑΣ. (2019, Φεβρουάριος 13). *in.gr*. https://www.in.gr/2019/02/13/greece/dramatiki-ypostelexosi-tis-omadas-dias-kataggelloun-oi-eidikoi-frouroi-tis-el/

Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης#ΜΕΡΟΣ ΠΡΩΤΟ - ΟΙ ΑΡΧΕΣ#ΤΙΤΛΟΣ ΙΙ - ΔΙΑΤΑΞΕΙΣ ΓΕΝΙΚΗΣ ΕΦΑΡΜΟΓΗΣ#Άρθρο 16 (πρώην άρθρο 286 της ΣΕΚ), 202 OJ C (2016). http://data.europa.eu/eli/treaty/tfeu_2016/art_16/oj/ell

ΕΡΤ Α.Ε. (Διευθυντής). (2022). *Κ. Μητσοτάκης για παρακολούθηση Ανδρουλάκη:Ήταν λάθος, δεν το γνώριζα, δεν θα το επέτρεπα|8/8/22|ΕΡΤ*. https://www.youtube.com/watch?v=oBtRwSXwsgE

Ευρωπαϊκή Ένωση. (2018). *Σύνοψη: Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και το... - EUR-Lex*. https://eur-lex.europa.eu/EL/legal-content/summary/protection-of-individuals-with-regard-to-the-processing-of-personal-data-by-eu-institutions-bodies-offices-and-agencies.html

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). *Η παρακαταθήκη: Ομάδα εργασίας του άρθρου 29 | European Data Protection Board*. https://edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_el

Ζέρβας, Χ. (2011, Σεπτέμβριος 4). Η Vodafone έδειξε την αμερικανική πρεσβεία. *Το Κουτί της Πανδώρας*. https://www.koutipandoras.gr/article/i-vodafone-edeixe-tin-amerikaniki-presveia/

Η Καθημερινή. (2016, Ιούνιος 28). Κωνσταντινούπολη: 41 νεκροί από την βομβιστική επίθεση στο αεροδρόμιο Ατατούρκ. *Η ΚΑΘΗΜΕΡΙΝΗ*. https://www.kathimerini.gr/world/865435/konstantinoypoli-41-nekroi-apo-tin-vomvistiki-epithesi-sto-aerodromio-atatoyrk/

Θεογνώστου, Ν. (2023). Αλγοριθμική Εκτίμηση Αντικτύπου σε σχέση με την Τεχνητή Νοημοσύνη—Η εφαρμογή του Νόμου 4961/2022. *Επιθεώρηση Δικαίου Πληροφορικής*, *4*(1), Article 1. https://doi.org/10.26262/infolawj.v4i1.9690

Κ., Α. (2022, Ιούλιος 31). «Συγγνώμη, λάθος...» η ψήφιση της τροπολογίας για την ΑΔΑΕ. *Εφημερίδα των Συντακτών*. https://www.efsyn.gr/politiki/paraskinia/354020_syggnomi-lathos-i-psifisi-tis-tropologias-gia-tin-adae

Κανέλλος, Λ. (2021). *Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο & στη δικαστική πρακτική*. Νομική Βιβλιοθήκη. https://www.nb.org/efarmoges-texnitis-noimosunis.html

Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ (2016). http://data.europa.eu/eli/reg/2016/679/2016-05-04/ell

Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ.), 295 OJ L (2018). http://data.europa.eu/eli/reg/2018/1725/oj/ell

Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών, 008 OJ L (2000). http://data.europa.eu/eli/reg/2001/45/oj/ell

Καρανικόλα, Μ.-Π. Ν. (2022). Η άρση του απορρήτου των επικοινωνιών ως ειδική ανακριτική πράξη και τα αποδεικτικά προβλήματα που σχετίζονται με αυτή. Στο *Aristotle University of Thessaloniki Institutional Repository—IKEE* (GRI-2022-35696, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης). https://doi.org/10.26262/heal.auth.ir.340213

Κορίζης, Ι. (2022). *Η εφαρμογή των ειδικών ανακριτικών πράξεων και των μέτρων επιείκειας στον χώρο της ηλεκτρονικής εγκληματικότητας* [Πανεπιστήμιο Μακεδονίας]. http://dspace.lib.uom.gr/handle/2159/27166

Λαμπρόπουλος, Β. (2020, Ιανουάριος 1). Παράτυπες παρακολουθήσεις της ΕΥΠ επί ΣΥΡΙΖΑ. *ΤΟ ΒΗΜΑ*. https://www.tovima.gr/2020/01/01/society/paratypes-parakolouthiseis-tis-eyp-epi-syriza/

Λεοντόπουλος, Ν., & Χονδρόγιαννος, Θ. (2022, Ιούνιος 2). Ο Μεγάλος Ανιψιός κι ο Μεγάλος Αδερφός [Δίκτυο ερευνητικών δημοσιογράφων]. *Reporters United*. https://www.reportersunited.gr/8948/o-megalos-anipsios-ki-o-megalos-aderfos/

Λεοντόπουλος, Ν., & Χονδρόγιαννος, Θ. (2023, Ιανουάριος 4). Υποκλοπές: Ένας χρόνος έρευνας από το Reporters United [Δίκτυο ερευνητικών δημοσιογράφων]. *Reporters United*. https://www.reportersunited.gr/10311/reporters-united-enas-chronos-ypoklopes-erevna/

Μαυρίδης, Ι. (2016a). Κεφάλαιο 6. Εισαγωγή στην κρυπτολογία. Στο *Ασφάλεια πληροφοριών στο διαδίκτυο* (σσ. 102–128). http://repository.kallipos.gr/handle/11419/1024

Μαυρίδης, Ι. (2016b). Κεφάλαιο 7. Σύγχρονοι κρυπτογραφικοί αλγόριθμοι. Στο *Ασφάλεια πληροφοριών στο διαδίκτυο* (σσ. 129–158). http://repository.kallipos.gr/handle/11419/1024

Μουστάκα, Μ. (2010, Σεπτέμβριος 10). Κατασκοπεία πίσω από τις υποκλοπές. *ΤΑ ΝΕΑ*. https://www.tanea.gr/2010/09/10/greece/kataskopeia-pisw-apo-tis-ypoklopes/

Μπλάνης, Ν. (2023, Ιανουάριος 20). Η υποστελέχωση των Αστυνομικών Τμημάτων οδηγεί στα όρια της «διάλυσης» την ΕΛ.ΑΣ. *Policenews*. https://www.policenews.gr/102143/i-ypostelechosi-ton-astynomikon-tmimaton-odigei-sta-oria-tis-dialysis-tin-el-as/

Ν. 2619/1998: Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ανθρωπίνων δικαιωμάτων και της αξιοπρέπειας του ατόμου σε σχέση με τις εφαρμογές της βιολογίας και της ιατρικής: Σύμβαση για τα ανθρώπινα Δικαιώματα και τη Βιοϊατρική, Pub. L. No. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 132 Α'/19.06.1998) (1998).

https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=60ef6321-1a8f-4682-937d-05799f1b1272

Ν. 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997, Pub. L. No. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 133 Α'/28.06.2006) (2006). https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=ffafa516-11d3-48d0-8678-6277b4c9005c

Ν. 4624/2019: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις., Pub. L. No. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 137 Α'/29.08.2019) (2019). https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=8d0512bc-425f-4f84-a682-aab10143d2d6

Ν. 4829/2021: Ενίσχυση διαφάνειας και λογοδοσίας σε θεσμικούς φορείς της Πολιτείας, αποκατάσταση της ακεραιότητας του Ενιαίου Συστήματος Κινητικότητας και λοιπές διατάξεις., Pub. L. No. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 166 Α'/10.09.2021) (2021). https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=99af96f7-46a3-42d5-81b1-ad94013dbafd

Ν. 4961/2022: Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις, Pub. L. No. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 146 Α΄/ 27.7.2022) (2022). https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=378368f0-101d-444a-8a45-aed3015b2ad4

Ν. 5002/2022: Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών., Pub. L. No. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 228 Α/9.12.2022) (2022). https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=3715dd48-9b39-4532-9b0e-af5c014ff48e

Ν. 5043/2023: Ρυθμίσεις σχετικά με τους Οργανισμούς Τοπικής Αυτοδιοίκησης α' και β' βαθμού - Διατάξεις για την ευζωία των ζώων συντροφιάς - Διατάξεις για το ανθρώπινο δυναμικό του δημοσίου τομέα - Λοιπές ρυθμίσεις του Υπουργείου Εσωτερικών και άλλες επείγουσες διατάξεις, Pub. L. No. Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 91Α΄/13.04.2023) (2023). https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=aec4302e-ab03-4f6e-867c-afdb002aaf0f

Ναζίρης, Γ. (2023). Νέοι Νόμοι—Ν 5046/2023: Άρθρο 44: Άρση του απορρήτου των επικοινωνιών για τη διακρίβωση των κακουργημάτων των άρθρων 290 και 291 ΠΚ. *Ποινική Δικαιοσύνη - ΤΝΠ Qualex*, *26*(8–9), 1068–1069.

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες), EP, CONSIL, 201 OJ L (2002). http://data.europa.eu/eli/dir/2002/58/oj/ell

Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ, OJ L (2006). http://data.europa.eu/eli/dir/2006/24/oj/ell

Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 , για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), OJ L (2009). http://data.europa.eu/eli/dir/2009/136/oj/ell

Ομάδα Εργασίας Άρθρου 29. (2014). *Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης*. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf

Παπαδημητράκης, Γ. (2023). Η ειδική ανακριτική πράξη της άρσης απορρήτου των επικοινωνιών ή των δεδομένων θέσης και κίνησης αυτών. *Ποινική Δικαιοσύνη - ΤΝΠ Qualex*, *26*(11), 1198–1209.

Περιφερειακό Κέντρο Πληροφόρησης του ΟΗΕ. (2019, Μάιος 23). *ΟΙΚΟΥΜΕΝΙΚΗ ΔΙΑΚΗΡΥΞΗ ΓΙΑ ΤΑ ΑΝΘΡΩΠΙΝΑ ΔΙΚΑΙΩΜΑΤΑ*. Περιφερειακό Κέντρο Πληροφόρησης του ΟΗΕ - Greece. https://unric.org/el/οικουμενικη-διακηρυξη-για-τα-ανθρωπι-2/

Πετρίδη, Κ. (2021, Ιανουάριος 28). Από αυτό το καλοκαίρι 1.000 φορητές συσκευές της ΕΛΑΣ θα σκανάρουν τα πρόσωπα των πολιτών σε περιπολίες. *Reporters United*. https://www.reportersunited.gr/3643/apo-ayto-to-kalokairi-1-000-forites-syskeyes-tis-elas-tha-skanaroyn-ta-prosopa-ton-politon-se-kathimerines-peripolies/

Πόρισμα-φωτιά της ΑΔΑΕ για τις υποκλοπές στη Βουλή. (2006, Μάρτιος 8). *in newspaper*. https://www.in.gr/2006/03/08/greece/porisma-fwtia-tis-adae-gia-tis-ypoklopes-sti-boyli/

Πρόταση - Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την Τεχνητή Νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης, Ευρωπαϊκό Κοινοβούλιο, Ευρωπαϊκό Συμβούλιο (2021). https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A52021PC0206

Πρόταση - Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) (2017). https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52017PC0010

Συμβούλιο της Ευρωπαϊκής Ένωσης. (2021, Φεβρουάριος 10). *Δελτίο Τύπου: Απόρρητο των ηλεκτρονικών επικοινωνιών: Το Συμβούλιο ενέκρινε τη θέση του σχετικά με κανόνες για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (ePrivacy)*. https://www.consilium.europa.eu/el/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

Συνάντηση της ΕΥΑΝ Σάμου με τον Αρχηγό της ΕΛ.ΑΣ. για την υποστελέχωση της Διεύθυνσης Αστυνομίας Σάμου—Samostoday. (2023, Ιούλιος 16). *Samostoday*. http://tinyurl.com/2p92aden

Συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12: Απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως) της 8ης Απριλίου 2014 [αιτήσεις του High Court of Ireland, Verfassungsgerichtshof (Ιρλανδία — Αυστρία) για την έκδοση προδικαστικής αποφάσεως] — Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl κ.λπ. (C-594/12) κατά Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Siochána, Ireland and the Attorney General (Ηλεκτρονικές επικοινωνίες — Οδηγία 2006/24/ΕΚ — Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών — Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο της παροχής τέτοιων υπηρεσιών — Κύρος — Άρθρα 7, 8 και 11 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης) (Δικαστήριο της Ευρωπαϊκής Ένωσης 2014). https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A62012CA0293

Τάκης Θεοδωρικάκος για υποστελέχωση ΕΛΑΣ. (2022, Ιούλιος 16). https://www.youtube.com/watch?v=UhMoWyyzWbI&ab_channel=FlashnewsGr

Τελλόγλου, Τ., & Τριανταφύλλου, Ε. (2022, Απρίλιος 11). Ποιος παρακολουθούσε το κινητό του δημοσιογράφου Θανάση Κουκάκη; | inside story. *Inside Story*. https://insidestory.gr/article/poios-parakoloythoyse-kinito-toy-dimosiografoy-thanasi-koykaki

Τερζής, Δ. (2022, Ιούλιος 30). ΕΥΠ: παραδέχτηκε την παρακολούθηση του Θ. Κουκάκη. *Εφημερίδα των Συντακτών*. https://www.efsyn.gr/politiki/boyli/353889_eyp-paradehtike-tin-parakoloythisi-toy-th-koykaki

Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, 202 OJ C (2016). http://data.europa.eu/eli/treaty/char_2016/oj/ell

Χατζής, Τ., & Βερύκιος, Δ. (2021, Μάιος 12). *Χρ. Σπίρτζης: Υπερστελέχωση των Σωμάτων καταστολής, υποστελέχωση των αντιεγκληματικών υπηρεσιών—Δραματική η κατάσταση στην Αν. Αττική* [Ραδιοφωνικός Σταθμός Alpha 989]. http://www.syriza.gr/article/id/109111/CHr.-Spirtzhs:-Yperstelechwsh-twn-Swmatwn-katastolhs-ypostelechwsh-twn-antiegklhmatikwn-yphresiwn---Dramatikh-h-katastash-sthn-An.-Attikh.html

Χονδρόγιαννος, Θ. (2022, Αύγουστος 2). Απόπειρα παρακολούθησης του Νίκου Ανδρουλάκη με το παράνομο λογισμικό υποκλοπών Predator. *govwatch*. https://govwatch.gr/finds/apopeira-parakoloythisis-toy-nikoy-androylaki-me-to-paranomo-logismiko-ypoklopon-predator/

Acharya, M. (2020). Comparative Study of Blowfish. *International Journal of Innovative Science and Research Technology*, *5*(2), 235–238.

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., & Zimmermann, P. (2015). Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 5–17. https://doi.org/10.1145/2810103.2813707

Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code* (1st edition). Polity.

Benner, T., & Hohmann, M. (2016, Απρίλιος 13). How Europe can get encryption right. *POLITICO*. https://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology/

Bhardwaj, A., & Som, S. (2016). Study of different cryptographic technique and challenges in future. *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, 208–212. https://doi.org/10.1109/ICICCS.2016.7542353

Bhuiyan, J. (2021, Νοέμβριος 8). LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws. *The Guardian*. https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform

Big Brother Watch and Others v. the United Kingdom, 58170/13, 62322/14, 24960/15 (ECtHR 13 Σεπτέμβριος 2018). https://hudoc.echr.coe.int/eng?i=001-186048

Billington, J. (2015, Δεκέμβριος 17). Paris terrorists used WhatsApp and Telegram to plot attacks according to investigators. *International Business Times UK*.

https://www.ibtimes.co.uk/paris-terrorists-used-whatsapp-telegram-plot-attacks-according-investigators-1533880

Blowfish Algorithm with Examples. (2019, Οκτώβριος 14). *GeeksforGeeks*. https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

Bone, H. (2023, Αύγουστος 16). *What is PGP encryption and how does it work?* Proton. https://proton.me/blog/what-is-pgp-encryption

Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, *82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Brayne, S., & Christin, A. (2021). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. *Social Problems*, *68*(3), 608–624. https://doi.org/10.1093/socpro/spaa004

Buckbee, M. (2023). *What is PGP Encryption and How Does It Work?* https://www.varonis.com/blog/pgp-encryption

Carleton, B., Cunningham, B., & Thorkildsen, Z. (2020). *The Use of Predictive Analytics in Policing*. Center for Naval Studies. https://www.cna.org/archive/CNA_Files/pdf/iim-2020-u-027459-final.pdf

Chinnasamy, N. R., & Kailasam, M. S. (2023). An In-Depth Review of Blowfish Encryption Algorithm: Security, Performance, and Application. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–5. https://doi.org/10.1109/ICCCNT56998.2023.10307323

Ciancaglini, V., Gibson, C., Sancho, D., McCarthy, O., Eira, M., Amann, P., & Klayn, A. (2020). *Malicious Uses and Abuses of Artificial Intelligence* (σ. 80). Trend Micro Research. https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf

Clifford, B. (2020). *GNET Report—Migration Moments: Extremist Adoption of Text-Based Instant Messaging Applications.* International Centre for the Study of Radicalisation, King's College London. https://gnet-research.org/wp-content/uploads/2020/11/GNET-Report-Migration-Moments-Extremist-Adoption-of-Text%E2%80%91Based-Instant-Messaging-Applications_V2.pdf

CNN,gr. (2016, Ιούλιος 15). Επίθεση Νίκαια: Αυτός είναι ο δράστης του χθεσινού μακελειού. *CNN.gr*. https://www.cnn.gr/kosmos/story/39384/epithesi-nikaia-aytos-einai-o-drastis-toy-xthesinoy-makeleioy

CNN,gr. (2022, Ιούλιος 12). Γαλλία: Ο μοναδικός τρομοκράτης που επέζησε στο Μπατακλάν δεν άσκησε έφεση. *CNN.gr*. https://www.cnn.gr/kosmos/story/320215/gallia-o-monadikos-tromokratis-poy-epezise-sto-mpataklan-den-askise-efesi

Council of Europe. (1950). *European Convention on Human Rights—ECHR Official Texts—ECHR - ECHR / CEDH*. ECHR. https://www.echr.coe.int/european-convention-on-human-rights

Council of Europe. (1981). *Convention 108 and Protocols—Data Protection—Publi.coe.int*. Convention 108 and Protocols - Data Protection. https://www.coe.int/en/web/data-protection/convention108-and-protocol

Council of Europe. (2021, Ιανουάριος 6). *The approval of the Additional Protocol to Convention 108, impacts and opportunities for Uruguay—Data Protection—Publi.coe.int*. The Approval of the Additional Protocol to Convention 108, Impacts and Opportunities for Uruguay -Data Protection. https://www.coe.int/en/web/data-protection/-/the-approval-of-the-additional-protocol-to-convention-108-impacts-and-opportunities-for-uruguay

Curry, D. (2024, Ιανουάριος 8). *Messaging App Revenue and Usage Statistics (2024)*. Business of Apps. https://www.businessofapps.com/data/messaging-app-market/

Deloitte's view on the implementation of Regulation (EU) 2018/1725—GDPR for European Union Institutions | Deloitte Belgium | Risk Services | cyber@EU. (2019). Deloitte Belgium. https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-for-eu-institutions.html

Difference between AES and DES ciphers. (2018, Ιούλιος 12). *GeeksforGeeks*. https://www.geeksforgeeks.org/difference-between-aes-and-des-ciphers/

Difference Between Diffie-Hellman and RSA. (2023, Μάιος 7). *GeeksforGeeks*. https://www.geeksforgeeks.org/difference-between-diffie-hellman-and-rsa/

Difference Between Symmetric and Asymmetric Key Encryption. (2023). *GeeksforGeeks*. https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Edison Hayden, M. (2019, Ιούνιος 27). Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram. *Southern Poverty Law Center*. https://www.splcenter.org/hatewatch/2019/06/27/far-right-extremists-are-calling-terrorism-messaging-app-telegram

EDPB. (2014). *Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης*. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf

EDPS. (2023, Ιανουάριος 27). *Synthetic Data | European Data Protection Supervisor*. https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data

Edward Snowden: Leaks that exposed US spy programme. (2013, Ιούλιος 1). *BBC News*. https://www.bbc.com/news/world-us-canada-23123964

Elliptic Curve Cryptography Overview. (2015). https://www.youtube.com/watch?v=dCvB-mhkT0w

End-to-End Encryption FAQ. (χ.χ.). Telegram Messenger. Ανακτήθηκε 19 Φεβρουάριος 2024, από https://tsf.telegram.org/manuals/e2ee-simple

ENISA. (2014). *Study on cryptographic protocols* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols

ENISA. (2015). *Privacy by design in big data* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/big-data-protection

ENISA. (2017). *Privacy Enhancing Technologies: Evolution and State of the Art* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art

ENISA. (2019a). *Pseudonymisation techniques and best practices* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

ENISA. (2019b). *Reinforcing trust and security in the area of electronic communications and online services* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services

Euronews. (2021, Μάρτιος 22). Πέντε χρόνια μετά τον τρόμο στις Βρυξέλλες. *euronews*. https://gr.euronews.com/2021/03/22/pente-hronia-meta-ton-tromo-stis-vryxelles

European Parliament. (2023, Σεπτέμβριος 12). *Press Release: Artificial Intelligence Act: Deal on comprehensive rules for trustworthy AI*. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

EUROPOL. (2021, Αύγουστος 6). *800 criminals arrested in biggest ever law enforcement operation against encrypted communication*. Europol. https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

EUROPOL. (2023). *Έκθεση για την κατάσταση και τις τάσεις της τρομοκρατίας στην Ευρωπαϊκή Ένωση (TE-SAT) 2023: Σύνοψη*. Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης. https://data.europa.eu/doi/10.2813/176434

Feistel, H. (1974). *Block cipher cryptographic system* (United States Patent US3798359A). https://patents.google.com/patent/US3798359A/en

FRA. (2015, Απρίλιος 25). *Άρθρο 8—Προστασία των δεδομένων προσωπικού χαρακτήρα*. European Union Agency for Fundamental Rights. http://fra.europa.eu/el/eu-charter/article/8-prostasia-ton-dedomenon-prosopikoy-haraktira

FRA. (2020). *Getting the future right: Artificial intelligence and fundamental rights : summary*. Publications Office of the European Union. https://data.europa.eu/doi/10.2811/155

Gaddis, D. (2022). *The Ethical Perils of Predictive Policing* [Final report for the Ethics and Emerging Military Technology Graduate Certificate Program, Naval War College]. https://apps.dtic.mil/sti/trecms/pdf/AD1204791.pdf

Gais, H., & Squire, M. (2021, Φεβρουάριος 16). How an Encrypted Messaging Platform is Changing Extremist Movements. *Southern Poverty Law Center*. https://www.splcenter.org/news/2021/02/16/how-encrypted-messaging-platform-changing-extremist-movements

Graham, R. (2016, Ιούνιος 16). How Terrorists Use Encryption. *CTC Sentinel*, *9*(6), 20–25.

Greenwald, G., & MacAskill, E. (2013, Ιούνιος 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Guru, D. A. (2019). Development of 'RSA' Encryption Algorithm for Secure Communication. *IJCSE*, *7*(6), 581–585. https://doi.org/10.26438/ijcse/v7i6.581585

Harkanson, R., & Kim, Y. (2017). Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications. *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, 1–7. https://doi.org/10.1145/3064814.3064818

Hashemi-Pour, C., & Chai, W. (2023). *What is the CIA Triad? | Definition from TechTarget*. WhatIs | TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Hussein, H., & Abdulameer, A. (2022). Crime Prediction Using Big Data Analysis. *Proceedings of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies, IMDC-IST 2021, 7-9 September 2021, Sakarya, Turkey*. Proceedings of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies, IMDC-IST 2021, 7-9 September 2021, Sakarya, Turkey, Sakarya, Turkey. https://doi.org/10.4108/eai.7-9-2021.2314943

iefimerida. (2016, Ιούλιος 15). Δεν ήταν στόχος η Νίκαια; Γεμάτο όπλα και εκρηκτικά το φορτηγό που σκόρπισε το θάνατο. *iefimerida.gr*. https://www.iefimerida.gr/news/278228/den-itan-stohos-i-nikaia-gemato-opla-kai-ekriktika-fortigo-poy-skorpise-thanato

in newspaper. (2016, Ιούλιος 16). Το Ισλαμικό Κράτος ανέλαβε την ευθύνη για το μακελειό στη Νίκαια. *in.gr*. https://www.in.gr/2016/07/16/world/to-islamiko-kratos-anelabe-tin-eythyni-gia-to-makeleio-sti-nikaia/

Karimi, F., Almasy, S., & Tuysuz, G. (2016, Ιούνιος 30). ISIS leadership involved in Istanbul attack planning, Turkish source says. *CNN*. https://www.cnn.com/2016/06/30/europe/turkey-istanbul-ataturk-airport-attack/index.html

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

Kumar Jena, B. (2023, Φεβρουάριος 9). *What Is AES Encryption and How Does It Work?* [Training platform]. Simplilearn. https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

Lakshmanan, R. (2023, Μάιος 26). Predator Android Spyware: Researchers Uncover New Data Theft Capabilities. *The Hacker News*. https://thehackernews.com/2023/05/predator-android-spyware-researchers.html

Lau, T. (2020, Απρίλιος 1). *Predictive Policing Explained*. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

List of presidencies of the Council of the European Union. (2023, Ιούλιος 1). https://www.consilium.europa.eu/en/council-eu/presidency-council-eu/timeline-presidencies-of-the-council-of-the-eu/

Locke, J. (2018). *Δεύτερη πραγματεία περί κυβερνήσεως*. Πανεπιστημιακές Εκδόσεις Κρήτης.

Luo, Z. J., Liu, R., & Mehta, A. (2023). *Understanding the RSA algorithm* (arXiv:2308.02785). arXiv. https://doi.org/10.48550/arXiv.2308.02785

Madiega, T. (2023). *Briefing—Artificial intelligence act*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

Martinoli, M. (2022, Μάιος 24). What is end-to-end encryption and how does it work? *Proton Blog*. https://proton.me/blog/what-is-end-to-end-encryption

Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. Στο H. C. Williams (Επιμ.), *Advances in Cryptology—CRYPTO '85 Proceedings* (σσ. 417–426). Springer. https://doi.org/10.1007/3-540-39799-X_31

Napoleon, P., Saturnia, O., Shoesmith, M., & Petrovitch, J. (2021, Δεκέμβριος 12). *The Use of Encrypted Communications by Criminals*. CTG - The Counter Terrorism Group. https://www.counterterrorismgroup.com/post/the-use-of-encrypted-communications-by-criminals

National Institute of Standards and Technology. (2023a). *Advanced Encryption Standard (AES)* (Federal Information Processing Standard (FIPS) 197). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.197-upd1

National Institute of Standards and Technology. (2023b). *Digital Signature Standard (DSS)* (Federal Information Processing Standard (FIPS) 186-5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.186-5

News247gr (Διευθυντής). (2022). *Το σκάνδαλο των υποκλοπών σε 5'*. https://www.youtube.com/watch?v=DIYSnqjXrZ0

Oosterloo, S., & Schie, G. van. (2018). The Politics and Biases of the 'Crime Anticipation System' of the Dutch Police. *Bias in Information, Algorithms, and Systems*, *2103*, 30–41. http://ceur-ws.org/Vol-2103/#paper_6

Parsons, A. (2023, Ιούλιος 25). Six guilty of murder over 2016 Brussels airport and train attack that killed 32 people. *Sky News*. https://news.sky.com/story/eight-men-convicted-over-2016-brussels-terror-attacks-that-left-32-people-dead-12926628

Protect Yourself and Your Privacy on Viber. (χ.χ.). Viber. Ανακτήθηκε 19 Φεβρουάριος 2024, από https://help.viber.com/hc/en-us/articles/9046626798237-Protect-Yourself-and-Your-Privacy-on-Viber

Radiotileoptiki S. A. - OPEN Digital Group. (2022, Νοέμβριος 13). Παρίσι: Η πιο φονική μέρα για την γαλλική πρωτεύουσα μετά τον Β' Παγκόσμιο Πόλεμο – Ποια ήταν η ποινή για τον μοναδικό επιζώντα τρομοκράτη. *ΕΘΝΟΣ*. https://www.ethnos.gr/todayinhistory/article/232406/parisihpiofonikhmeragiathnggallikhproteyoysametatonbe28099pagkosmiopolemopoiahtanhpoinhgiatonmonadikoepizontatromokrath

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance) (2016). http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

RSA Full Form. (2022, Αύγουστος 18). *GeeksforGeeks*. https://www.geeksforgeeks.org/rsa-full-form/

Rubin, A. J., & Breeden, A. (2017, Ιούλιος 15). France Remembers the Nice Attack: 'We Will Never Find the Words'. *The New York Times*. https://www.nytimes.com/2017/07/14/world/europe/nice-attack-france-bastille-day.html

Scheele, S. K. (2000). *The Evolution of Instant Messaging*. GIAC Certifications. https://www.giac.org/paper/gsec/2290/evolution-instant-messaging/103954

Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). Στο R. Anderson (Επιμ.), *Fast Software Encryption* (σσ. 191–204). Springer. https://doi.org/10.1007/3-540-58108-1_24

Schuilenburg, M., & Soudijn, M. (2023). Big data policing: The use of big data and algorithms by the Netherlands Police. *Policing: A Journal of Policy and Practice*, *17*, paad061. https://doi.org/10.1093/police/paad061

Securing Privacy: PI on End-to-End Encryption (σ. 44). (2022). Privacy International. http://www.privacyinternational.org/report/4949/securing-privacy-end-end-encryption

Simmons, G. J. (2024, Ιανουάριος 11). *Data Encryption Standard (DES)* [Encyclopedia]. Britannica. https://www.britannica.com/topic/Data-Encryption-Standard

Strikwerda, L. (2021). Predictive policing: The risks associated with risk assessment. *The Police Journal*, *94*(3), 422–436. https://doi.org/10.1177/0032258X20947749

Torok, R. (2015, Νοέμβριος 17). How social media was key to Islamic State's attacks on Paris. *The Conversation*. http://theconversation.com/how-social-media-was-key-to-islamic-states-attacks-on-paris-50743

UN General Assembly. (2000). *United Nations Convention against Transnational Organized Crime*. United Nations. //www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

UNESCO. (2003). *International Declaration on Human Genetic Data*. https://www.unesco.org/en/legal-affairs/international-declaration-human-genetic-data

Vinck, A. J. H. (2012, Μάιος 12). *Introduction to public key cryptography*. https://www.uni-due.de/imperia/md/images/dc/crypto_chapter_5_public_key.pdf

What is end-to-end encryption and how does it work? (2023). https://www.youtube.com/watch?v=c2OkOckSD20

WhatsApp Inc. (2023). *WhatsApp Encryption Overview* (σσ. 8–11) [Technical white paper]. https://faq.whatsapp.com/820124435853543

Wickramasinghe, S. (2023, Μάιος 15). *RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained*. Splunk. https://www.splunk.com/en_us/blog/learn/rsa-algorithm-cryptography.html

WikiLeaks. (χ.χ.). [Investigative Journalism Network]. WikiLeaks. Ανακτήθηκε 19 Φεβρουάριος 2024, από https://wikileaks.org/

Zahorski, A. (2022, Ιούλιος 6). *Everything You Need to Know About the Twofish Encryption Algorithm*. MUO. https://www.makeuseof.com/twofish-encryption-algorithm-explained/