



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΑ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Επεξεργασία και προστασία προσωπικών δεδομένων στο
πλαίσιο της λειτουργίας της Ελληνικής Αστυνομίας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Αλεξανδρή Βασιλικής

Επιβλέπων: Κρητικός Κυριάκος

Μέλη εξεταστικής επιτροπής: Μήτρου Αίλιαν
Κωνσταντίνου Ελισάβετ

Σάμος, Μάρτιος 2026

Πρόλογος και ευχαριστίες

Η ολοκλήρωση της παρούσας διπλωματικής εργασίας σηματοδοτεί το τέλος ενός ιδιαίτερα σημαντικού κύκλου σπουδών, ο οποίος συνέβαλε ουσιαστικά τόσο στην ακαδημαϊκή μου κατάρτιση όσο και στην προσωπική μου εξέλιξη.

Αρχικά, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Κρητικό Κυριάκο για την πολύτιμη καθοδήγησή του και τον χρόνο, που διέθεσε για την εκπόνηση της εργασίας μου.

Ιδιαίτερη ευγνωμοσύνη οφείλω στην οικογένειά μου, η οποία με στήριξε σε όλη τη διάρκεια των σπουδών μου. Η ενθάρρυνση, η υπομονή και η πίστη τους στις δυνατότητές μου, αποτέλεσαν το θεμέλιο, πάνω στο οποίο στηρίχτηκε η ολοκλήρωση αυτής της διαδρομής.

Τέλος, θα ήθελα να ευχαριστήσω τη φίλη μου Άννα Μαρία, η οποία στάθηκε δίπλα μου στις πιο απαιτητικές στιγμές αυτής της προσπάθειας.

© [2026]

της

ΑΛΕΞΑΝΔΡΗ ΒΑΣΙΛΙΚΗΣ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Περιεχόμενα

1. Εισαγωγή.....	1
1.1. Το διαχρονικό ζήτημα της προστασίας προσωπικών δεδομένων.....	1
1.2. Αντικείμενο της εργασίας	2
1.3. Δομή της εργασίας.....	3
2. Έννοια και κατηγορίες προσωπικών δεδομένων - Η σπουδαιότητα της προστασίας τους	5
2.1. Έννοια και κατηγορίες προσωπικών δεδομένων	5
2.2. Προστασία προσωπικών δεδομένων	8
3. Μεθοδολογία Επισκόπησης.....	10
3.1. Εισαγωγή.....	10
3.2. Βασικός στόχος και ερευνητικά ερωτήματα	10
3.3. Διαδικασία αναζήτησης βιβλιογραφίας.....	12
3.4. Κριτήρια φιλτραρίσματος βιβλιογραφίας.....	14
3.5. Αποτελέσματα φιλτραρίσματος βιβλιογραφίας	15
4. Νομικό πλαίσιο για την προστασία των δεδομένων	21
4.1. Ευρωπαϊκές Συμβάσεις και Συνθήκες.....	21
4.2. Κανονισμός 2016/679 - GDPR	22
4.2.1. Από την Οδηγία 95/46/EK στον GDPR	22
4.2.2. Αρχές επεξεργασίας προσωπικών δεδομένων	23
4.2.2.1. Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων	26
4.2.3. Δικαιώματα υποκειμένου δεδομένων	28
4.3. Οδηγία (ΕΕ) 2016/680	34
4.4. Άρθρο 9Α του Συντάγματος.....	36
4.5. Ν. 4624/2019	37
4.5.1. Πεδίο εφαρμογής.....	37
4.5.2. Αρχές επεξεργασίας προσωπικών δεδομένων	38
4.5.2.1. Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων	40
4.5.3. Δικαιώματα υποκειμένου δεδομένων	41
4.6. Νόμος 5002/2022	45
4.7. Συμπεράσματα	48
5. Αρχή & Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.....	49
5.1. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - Α.Π.Δ.Π.Χ.....	49

5.1.1.	Εισαγωγή	49
5.1.2.	Καθήκοντα της Α.Π.Δ.Π.Χ.	49
5.2.	Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	50
5.2.1.	Εισαγωγή	50
5.2.2.	Καθήκοντα Υπεύθυνου Προστασίας Δεδομένων.....	51
6.	Χρήση και επεξεργασία των προσωπικών δεδομένων από την Ελληνική Αστυνομία	52
6.1.	Ανάλυση DNA	52
6.1.1.	Άρθρο 201 Κ.Π.Δ.	54
6.1.2.	Ειδικό αρχείο DNA	57
6.1.3.	Συμπεράσματα.....	57
6.2.	Άρση του απορρήτου των επικοινωνιών	58
6.2.1.	Τα στοιχεία της επικοινωνίας.....	58
6.2.2.	Άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας.....	59
6.2.3.	Άρση του απορρήτου των επικοινωνιών για τη διακρίβωση εγκλημάτων.....	60
6.2.4.	Διαδικασία της άρσης του απορρήτου.....	62
6.2.5.	Διαχείριση του υλικού της άρσης.....	63
6.2.5.1.	Για λόγους εθνικής ασφάλειας	63
6.2.5.2.	Για διακρίβωση εγκλημάτων	64
6.2.6.	Συμπεράσματα.....	65
6.3.	Δημοσιοποίηση προσωπικών δεδομένων κατηγορουμένων και καταδικασθέντων	66
6.3.1.	Συμπεράσματα.....	69
6.4.	Έκδοση αστυνομικού δελτίου ταυτότητας	69
6.4.1.	Απαραίτητα δικαιολογητικά.....	70
6.4.2.	Επεξεργασία και διατήρηση προσωπικών δεδομένων	73
6.4.3.	Δικαιώματα των υποκειμένων.....	75
6.4.4.	Συμπεράσματα.....	76
6.5.	Έκδοση διαβατηρίων	76
6.5.1.	Απαραίτητα δικαιολογητικά.....	77
6.5.2.	Επεξεργασία και διατήρηση προσωπικών δεδομένων	78
6.5.2.1.	Δεδομένα ειδικών κατηγοριών	80
6.5.3.	Μέτρα Ασφαλείας	82
6.5.4.	Δικαιώματα των υποκειμένων.....	83
6.5.5.	Συμπεράσματα.....	84
6.6.	Επιτήρηση δημόσιων χώρων	85
6.6.1.	Προεδρικό Διάταγμα 75/2020	86

6.6.1.1.	Υπεύθυνος επεξεργασίας.....	86
6.6.1.2.	Συστήματα επιτήρησης και διαχείριση δεδομένων	87
6.6.1.3.	Δικαιώματα των υποκειμένων	90
6.6.1.4.	Μέτρα ασφαλείας των δεδομένων του συστήματος.....	91
6.6.1.5.	Απόφαση τοποθέτησης και λειτουργίας του συστήματος επιτήρησης....	92
6.6.2.	Μελέτη περίπτωσης - Διαβούλευση για σύστημα επιτήρησης	93
6.6.3.	Συμπεράσματα.....	95
6.7.	Διαγωνισμός πρόσληψης ιδιωτών στις Σχολές της Ελληνικής Αστυνομίας	96
6.7.1.	Συμπεράσματα.....	99
6.8.	Διασυννοριακή ανταλλαγή προσωπικών δεδομένων.....	99
6.8.1.	Εθνικά σημεία επαφής – Υπεύθυνοι επεξεργασίας δεδομένων.....	100
6.8.2.	Επεξεργασία των δεδομένων.....	101
6.8.2.1.	Προφίλ DNA	101
6.8.2.2.	Δακτυλικά αποτυπώματα.....	102
6.8.2.3.	Άδειες κυκλοφορίας οχημάτων	103
6.8.3.	Σκοπός της επεξεργασίας	104
6.8.4.	Ακρίβεια των δεδομένων.....	105
6.8.5.	Χρόνος διατήρησης των δεδομένων.....	105
6.8.6.	Τεχνικά και οργανωτικά μέτρα.....	106
6.8.7.	Δικαιώματα των υποκειμένων.....	107
6.8.8.	Συμπεράσματα.....	107
6.9.	Συμπεράσματα	108
7.	Προκλήσεις και μέτρα αντιμετώπισης	109
7.1.	Προκλήσεις.....	109
7.1.1.	GDPR ή Οδηγία 2016/680;	109
7.1.2.	Ανθρώπινο δυναμικό	110
7.1.3.	Τεχνολογικοί περιορισμοί	110
7.1.4.	Κυβερνοαπειλές - κυβερνοεπιθέσεις	111
7.1.5.	Περιβαλλοντικές απειλές.....	112
7.2.	Μέτρα αντιμετώπισης προκλήσεων.....	112
7.2.1.	Μεθοδολογία διαχείρισης επικινδυνότητας.....	112
7.2.2.	Εκπαίδευση – Ενημέρωση.....	114
7.2.3.	Έλεγχος πρόσβασης.....	114
7.2.4.	Καταγραφή ενεργειών	116
7.2.5.	Κυβερνασφάλεια	117

7.2.6.	Αντίγραφα ασφαλείας (backups).....	118
7.2.7.	Κρυπτογραφία	118
7.2.8.	Ψευδωνυμοποίηση & Αωνυμοποίηση	119
7.3.	Μελέτες περίπτωσης	121
7.3.1.	Παραβιάσεις κατά την έκδοση ταυτοτήτων	121
7.3.2.	Κυβερνοεπίθεση «EMOTET»	124
7.4.	Συμπεράσματα	127
8.	Συμπεράσματα	129
	Βιβλιογραφία	132

Λίστα Σχημάτων

Σχήμα 1: Κατανομή βιβλιογραφίας ανά είδος / Χαρακτηρισμός βιβλιογραφίας.....	16
Σχήμα 2: Κατανομή υποκατηγοριών λευκής βιβλιογραφίας.....	17
Σχήμα 3: Κατανομή βιβλιογραφίας ανά εκδότη.....	18
Σχήμα 4: Κατανομή βιβλιογραφίας ανά έτος δημοσίευσης	19

Λίστα Πινάκων

Πίνακας 1: Αιτιολόγηση επιλογής ψηφιακών βάσεων δεδομένων	12
Πίνακας 2: Δικαιώματα υποκειμένων Οδηγία 2016/680 - Ν. 4624/2019	45
Πίνακας 3: Προκλήσεις - Μέτρα αντιμετώπισης	120

Λίστα εικόνων

Εικόνα 1: Διαχωρισμός προσωπικών δεδομένων.....	8
Εικόνα 2: Εμπρόσθια και οπίσθια όψη δελτίου αστυνομικής ταυτότητας.....	70
Εικόνα 3: Αίτηση - Υπεύθυνη δήλωση	72
Εικόνα 4: Αίτηση έκδοσης - αντικατάστασης δελτίου ταυτότητας.....	73
Εικόνα 5: Σύμβολο βιομετρικών διαβατηρίων.....	82
Εικόνα 6: Εμπρόσθια όψη διαβατηρίου	82
Εικόνα 7: Έντυπο άσκησης δικαιωμάτων υποκειμένων δεδομένων	91

Ακρωνύμια

ABAC	Attribute-based Access Control (Έλεγχος Προσπέλασης Βασισμένος σε Χαρακτηριστικά)
GDPR	General Data Protection Regulation (Γενικός Κανονισμός Προστασίας Δεδομένων)
RBAC	Role-Based Access Control (Έλεγχος Προσπέλασης Βασισμένος σε Ρόλους)
Α.Δ.Α.Ε.	Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
Α.Δ.Τ.	Αστυνομικό δελτίο ταυτότητας
Α.Π.Δ.Π.Χ.	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Δ.Α.Ε.Ε.Β.	Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας
Δ.Δ.Α.Σ.	Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας
Δ.Δ.Ε.Α.	Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας
Δ.Ε.ΔΙ.Κ.	Διεύθυνση Επιχειρήσεων και Διαχείρισης Κρίσεων
Δ.Ε.Ε.	Διεύθυνση Εγκληματολογικών Ερευνών
Ε.Δ.Δ.Α.	Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων
Ε.Ε.	Ευρωπαϊκή Ένωση
ΕΛ.ΑΣ.	Ελληνική Αστυνομία
Ε.Ο.Χ.	Ευρωπαϊκός Οικονομικός Χώρος
Ε.Σ.Δ.Α.	Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου
Ε.Σ.Κ.Ε.ΔΙ.Κ.	Ενιαίο Συντονιστικό Κέντρο Επιχειρήσεων και Διαχείρισης Κρίσεων
Ε.Υ.Π	Εθνική Υπηρεσία Πληροφοριών
Κ.Π.Δ.	Κώδικας Ποινικής Δικονομίας
Ν.Δ.	Νομοθετικό Διάταγμα
Π.Κ.	Ποινικός Κώδικας
Σ.Λ.Ε.Ε.	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
Χ.Θ.Δ.Ε.Ε.	Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
Υ.Α.	Υπουργική Απόφαση
Υ.ΠΑΙ.Θ.Α.	Υπουργείο Παιδείας, Θρησκευμάτων και Αθλητισμού
Υ.Π.Δ.	Υπεύθυνος Προστασίας Δεδομένων

Περίληψη

Η προστασία των προσωπικών δεδομένων συνιστά θεμελιώδες δικαίωμα κάθε φυσικού προσώπου, που κατοχυρώνεται ρητά στο άρθρο 9^Α του Συντάγματος, το οποίο σε συνδυασμό με το ευρωπαϊκό και εθνικό νομικό πλαίσιο, διαμορφώνει ένα αυστηρό και συνάμα δεσμευτικό πεδίο δράσης για την Ελληνική Αστυνομία (ΕΛ.ΑΣ.), κατά την άσκηση των καθηκόντων της.

Σκοπός της παρούσας διπλωματικής εργασίας, η οποία αποτελεί μελέτη ανασκόπησης, είναι η διερεύνηση του βαθμού και του τρόπου, με τον οποίο η Ελληνική Αστυνομία, εφαρμόζει τις βασικές αρχές επεξεργασίας δεδομένων και διασφαλίζει τα δικαιώματα των υποκειμένων στο πλαίσιο της λειτουργίας της. Παράλληλα, επιδιώκεται η ανάδειξη των προκλήσεων, που ανακύπτουν κατά την επεξεργασία και επηρεάζουν την προστασία των δεδομένων και η καταγραφή των τρόπων αντιμετώπισής τους.

Προς εκπλήρωση των παραπάνω στόχων πραγματοποιείται μια προσεκτική και διερευνητική προσέγγιση του ζητήματος, σε νομικό – θεωρητικό και πρακτικό επίπεδο. Πιο συγκεκριμένα, αναλύεται το ισχύον νομικό πλαίσιο, το οποίο ρυθμίζει την προστασία των δεδομένων, με ιδιαίτερη έμφαση στις βασικές αρχές επεξεργασίας και τα δικαιώματα των υποκειμένων. Στη συνέχεια, εξετάζονται σε βάθος οκτώ περιπτώσεις επεξεργασίας προσωπικών δεδομένων από την Ελληνική Αστυνομία, οι οποίες αφορούν προληπτικές, κατασταλτικές και διοικητικές της δράσεις, αναδεικνύοντας την εφαρμογή των βασικών αρχών επεξεργασίας και τη διασφάλιση των δικαιωμάτων των υποκειμένων. Η εργασία ολοκληρώνεται με την χαρτογράφηση των προκλήσεων, τις οποίες καλείται να αντιμετωπίσει η ΕΛ.ΑΣ. κατά την επεξεργασία των δεδομένων, και την διατύπωση συγκεκριμένων προτάσεων, για την υπερνίκηση αυτών και τη διασφάλιση της προστασίας των δεδομένων σε όλες τις δυνατές περιπτώσεις δράσεων της ΕΛ.ΑΣ..

Λέξεις κλειδιά: προσωπικά δεδομένα, Ελληνική Αστυνομία, GDPR, Οδηγία 2016/680, Ν. 4624/2019, βασικές αρχές επεξεργασίας, Α.Π.Δ.Π.Χ., ασφάλεια, ιδιωτικότητα, ανασκόπηση, προκλήσεις, προτάσεις βελτίωσης

Abstract

The protection of personal data constitutes a fundamental human right, explicitly enshrined in Article 9A of the Constitution, that in conjunction with the European and national legal framework shapes a strict and binding framework of action for the Hellenic Police during the exercise of its duties.

The purpose of this Master's thesis, which constitutes a review study, is to investigate the extent and the manner in which the Hellenic Police applies the core data processing principles and ensures the rights of data subjects in the framework of its operation. Furthermore, it aims to highlight the challenges arising during data processing and affect data protection, as well as to record the methods for addressing them.

In order to achieve the aforementioned objectives a careful and exploratory approach to the issue is conducted at a legal – theoretical and practical level. In particular, the current legal framework regulating data protection is analyzed, with a particular emphasis on the core processing principles and the rights of data subjects. Subsequently, eight cases of personal data processing by the Hellenic Police are examined in depth, concerning its preventive, repressive and administrative actions, highlighting the application of core processing principles and the safeguard of data subjects' rights. The thesis concludes with the mapping of the challenges that the Hellenic Police faces during data processing and the formulation of specific proposals to overcome these challenges and ensure data protection during all of its possible activities.

Keywords: personal data, Hellenic Police, GDPR, Directive 2016/680, Law 4624/2019, core principles of processing, Hellenic Data Protection Authority, security, privacy, review, challenges, improvement proposals.

1. Εισαγωγή

1.1. Το διαχρονικό ζήτημα της προστασίας προσωπικών δεδομένων

Το θεμελιώδες δικαίωμα της προστασίας των προσωπικών δεδομένων αποτελεί ένα διαχρονικό ζήτημα, το οποίο έχει απασχολήσει ιδιαίτερα τόσο τον ευρωπαϊό όσο και τον εθνικό νομοθέτη. Η ραγδαία ανάπτυξη της τεχνολογίας σε συνδυασμό με την ευρεία χρήση του διαδικτύου και την ψηφιοποίηση ολοένα και περισσότερων υπηρεσιών, έχει οδηγήσει στην συλλογή και επεξεργασία πλήθους προσωπικών δεδομένων, ευαίσθητων και μη («Η Καθημερινή», 2018). Ήδη από το 1995 άρχισαν να θεσπίζονται νομικά κείμενα, σε ευρωπαϊκό και εθνικό επίπεδο, που είχαν ως απώτερο σκοπό την προστασία αυτών των δεδομένων.

Υπό αυτό το πρίσμα, σε ευρωπαϊκό επίπεδο εφαρμόστηκε αρχικά η Οδηγία 95/46/ΕΚ και η Απόφαση Πλαίσιο 2008/977/ΔΕΥ, ωστόσο η μεν πρώτη με το πέρασμα των ετών αποδείχθηκε ανεπαρκής (Ryz, L. & Grest, L. 2016), ενώ η δεύτερη περιοριζόταν μόνο στη διασυννοριακή ανταλλαγή προσωπικών δεδομένων (Άρθρο 1 της Απόφασης πλαισίου). Έτσι, το 2016 τέθηκε σε ισχύ ο Γενικός Κανονισμός Προστασίας Δεδομένων, γνωστός και ως GDPR, ο οποίος αντικατέστησε την Οδηγία 95/46/ΕΚ και αποσκοπεί στην προστασία των προσωπικών δεδομένων των φυσικών προσώπων των κρατών μελών, λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις (Ryz, L. & Grest, L. 2016). Εκτός όμως από αυτόν, εκείνη την περίοδο εκδόθηκε και η Οδηγία 2016/680, η οποία αντικατέστησε την Απόφαση Πλαίσιο 2008/977/ΔΕΥ και ρυθμίζει την επεξεργασία των προσωπικών δεδομένων από τις αρμόδιες αρχές κατά την πρόληψη, καταστολή και διερεύνηση αξιόποινων πράξεων, καλύπτοντας έτσι ένα κρίσιμο κανονιστικό κενό, το οποίο υπήρχε με την προϊσχύσασα νομοθεσία (Εγχειρίδιο, 2018: 38).

Όσον αφορά την ελληνική έννομη τάξη, προκειμένου η χώρα μας να προσαρμόσει την Οδηγία 95/46/ΕΚ στο εθνικό μας δίκαιο θέσπισε τον Ν. 2472/1997 (Χριστοδούλου, Κ., 2020:2), ο οποίος με τις αλλαγές, που επήλθαν στην ευρωπαϊκή νομοθεσία και την ραγδαία ανάπτυξη του ψηφιακού κόσμου, κατέστη ανεπαρκής. Σε αυτό το πλαίσιο ψηφίστηκε ο Ν. 4624/2019, ο οποίος κατήργησε τον Ν. 2472/1997, πλην ορισμένων διατάξεών του, έθεσε μέτρα εφαρμογής του GDPR (Παναγοπούλου, Φ., 2019), ενσωμάτωσε την Οδηγία 2016/680 στην ελληνική νομοθεσία (Κανέλλος, Λ., 2020: 221) και καθόρισε τα καθήκοντα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.), ως αρμόδιας εποπτικής αρχής για τον έλεγχο τήρησης των νόμων περί προστασίας δεδομένων. Ασφαλώς το νομικό πλαίσιο συμπληρώνεται και από έτερους Νόμους, Προεδρικά Διατάγματα και Υπουργικές Αποφάσεις, που αφορούν εξειδικευμένες περιπτώσεις επεξεργασίας προσωπικών δεδομένων.

1.2. Αντικείμενο της εργασίας

Τόσο οι δημόσιοι όσο και οι ιδιωτικοί φορείς και οργανισμοί συλλέγουν και επεξεργάζονται προσωπικά δεδομένα πολιτών για διάφορους λόγους. Ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση της Ελληνικής Αστυνομίας, η οποία ως κατεξοχήν αρμόδια αρχή για την εξασφάλιση της δημόσιας και κρατικής ασφάλειας, αλλά και τη διενέργεια προληπτικών δράσεων, ποινικών ερευνών και προανακριτικών ενεργειών, συλλέγει και επεξεργάζεται καθημερινά μεγάλο όγκο προσωπικών δεδομένων, συχνά μάλιστα αυξημένης ευαισθησίας, όπως τα γενετικά και βιομετρικά δεδομένα¹. Σε καθημερινή βάση κατά την άσκηση των καθηκόντων της έρχεται αντιμέτωπη με το ιδιαίτερα αυστηρό και απαιτητικό νομικό πλαίσιο προστασίας δεδομένων, όπου οποιαδήποτε παρέκκλιση από αυτό ενδέχεται να οδηγήσει σε παραβίαση των ανθρωπίνων δικαιωμάτων.

Αντικείμενο της παρούσας εργασίας αποτελεί η διερεύνηση του τρόπου με τον οποίο η Ελληνική Αστυνομία επεξεργάζεται και προστατεύει τα προσωπικά δεδομένα στο πλαίσιο της λειτουργίας της με βάση την ισχύουσα νομοθεσία, τις διαδικτυακές πηγές και τη σχετική βιβλιογραφία από το έτος 1995, με ιδιαίτερη έμφαση στην χρονική περίοδο 2016-2025. Συγκεκριμένα, παρουσιάζεται το ισχύον νομικό πλαίσιο και εξετάζεται η εφαρμογή των βασικών αρχών επεξεργασίας προσωπικών δεδομένων και η διασφάλιση των δικαιωμάτων των υποκειμένων, μέσα από την ανάλυση συγκεκριμένων λειτουργιών, οι οποίες αφορούν προληπτικές, κατασταλτικές και διοικητικές δράσεις της Ελληνικής Αστυνομίας. Επιπλέον, παρουσιάζονται οι προκλήσεις, που δύναται να αντιμετωπίσει η ΕΛ.ΑΣ. κατά την επεξεργασία των δεδομένων και μέτρα καταπολέμησης αυτών.

Εκ των προαναφερθέντων, γίνεται σαφές ότι ο αντίκτυπος της εργασίας είναι διττός: νομικός και επιχειρησιακός. Αφενός, η παρούσα εργασία προβαίνει στην αποσαφήνιση της έννοιας και των κατηγοριών των προσωπικών δεδομένων, ενώ παράλληλα συμβάλλει στη συγκέντρωση και οργάνωση των διατάξεων περί προσωπικών δεδομένων, που ρυθμίζουν τις λειτουργίες της ΕΛ.ΑΣ., οι οποίες εμφανίζονται διάσπαρτες σε πλήθος ευρωπαϊκών και εθνικών νομικών κειμένων. Αφετέρου, η αναλυτική παρουσίαση συγκεκριμένων λειτουργιών της ΕΛ.ΑΣ. κατά τις οποίες επεξεργάζεται προσωπικά δεδομένα γεφυρώνει τη νομική θεωρία με την επιχειρησιακή πραγματικότητα, ενώ η ανάδειξη των προκλήσεων και των μέτρων αντιμετώπισής τους αποδεικνύει την πολυπλοκότητα της επεξεργασίας και της προστασίας αυτών των δεδομένων. Συνεπώς, η παρούσα εργασία θα μπορούσε να αξιοποιηθεί από την ΕΛ.ΑΣ., προς υποβοήθηση του έργου της και ειδικά για την υιοθέτηση κατάλληλων μέτρων καταπολέμησης των υφιστάμενων προκλήσεων, αλλά και προς «απόδειξη» σωστής και νομότυπης επεξεργασίας των δεδομένων των πολιτών, κάτι που αναμφισβήτητα αυξάνει την εμπιστοσύνη των τελευταίων προς την ΕΛ.ΑΣ..

¹ <https://www.astynomia.gr/odigos-tou-politi/prostasia-dedomenon-prosopikou-charaktira/>

1.3. Δομή της εργασίας

Η παρούσα εργασία απαρτίζεται από τα εξής κεφάλαια:

- Κεφάλαιο 2: «Έννοια και κατηγορίες προσωπικών δεδομένων - Η σπουδαιότητα της προστασίας τους»
Αναλύεται η έννοια των προσωπικών δεδομένων, οι κατηγορίες στις οποίες διακρίνονται και η σημασία της προστασίας τους σε ένα σύγχρονο κράτος δικαίου.
- Κεφάλαιο 3: «Μεθοδολογία»
Παρουσιάζεται η μεθοδολογία ανασκόπησης, που ακολουθήθηκε κατά την συγγραφή της παρούσας εργασίας, αναφορικά με την συλλογή, επιλογή και ανάλυση της σχετικής βιβλιογραφίας.
- Κεφάλαιο 4: «Νομικό πλαίσιο για την προστασία των δεδομένων»
Παρουσιάζεται το νομικό πλαίσιο που διέπει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και συγκεκριμένα οι Ευρωπαϊκές Συμβάσεις και Συνθήκες, ο GDPR, η Οδηγία 2016/680, το άρθρο 9Α του Συντάγματος, ο Ν. 4624/2019 και ο Ν. 5002/2022. Ιδιαίτερη έμφαση δίνεται στις βασικές αρχές επεξεργασίας και στα δικαιώματα των υποκειμένων των δεδομένων.
- Κεφάλαιο 5: «Αρχή και Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα»
Αποτυπώνονται τα καθήκοντα και οι αρμοδιότητες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και του Γραφείου Δεδομένων Προσωπικού Χαρακτήρα της Ελληνικής Αστυνομίας, στο οποίο προϊστάται ο Υπεύθυνος Προστασίας Δεδομένων της ΕΛ.ΑΣ., ως μηχανισμών εποπτείας της ορθής εφαρμογής των νομικών κειμένων προστασίας δεδομένων.
- Κεφάλαιο 6: «Χρήση και επεξεργασία των προσωπικών δεδομένων από την Ελληνική Αστυνομία»
Αναλύονται ενδεικτικές, αλλά συνάμα αντιπροσωπευτικές, περιπτώσεις επεξεργασίας προσωπικών δεδομένων από την Ελληνική Αστυνομία και συγκεκριμένα, η ανάλυση DNA, η άρση του απορρήτου των επικοινωνιών, η δημοσιοποίηση προσωπικών δεδομένων κατηγορουμένων και καταδικασθέντων, η έκδοση ταυτοτήτων και διαβατηρίων, η επιτήρηση των δημόσιων χώρων, η συμμετοχή υποψηφίων ιδιωτών στο διαγωνισμό εισαγωγής στις Σχολές της ΕΛ.ΑΣ και η διασυνοριακή συνεργασία μεταξύ των αρμόδιων αρχών των κρατών μελών, στο πλαίσιο αντιμετώπισης της τρομοκρατίας και του διασυνοριακού, εν γένει, εγκλήματος. Μέσα από τις περιπτώσεις αυτές, που αφορούν προληπτικές, κατασταλτικές και διοικητικές ενέργειες της ΕΛ.ΑΣ, διερευνάται ο τρόπος επεξεργασίας δεδομένων και αποδεικνύεται η εφαρμογή των βασικών αρχών επεξεργασίας από την Ελληνική Αστυνομία.
- Κεφάλαιο 7: «Προκλήσεις και τρόποι αντιμετώπισης»
Η εργασία αναδεικνύει τις προκλήσεις, που αντιμετωπίζει η ΕΛ.ΑΣ κατά την προστασία δεδομένων προσωπικού χαρακτήρα, όπως το εφαρμοστικό δίλλημα μεταξύ του GDPR και της Οδηγίας 2016/680, ο ανθρώπινος παράγοντας, οι

τεχνολογικοί περιορισμοί, οι αυξανόμενες κυβερνοεπιθέσεις και κυβερνοαπειλές και οι περιβαλλοντικές απειλές. Επιπλέον, αναλύονται οι τρόποι αντιμετώπισης των ανωτέρω προκλήσεων με ιδιαίτερη έμφαση στην εφαρμογή κατάλληλης μεθοδολογίας διαχείρισης επικινδυνότητας, την εκπαίδευση και επιμόρφωση του προσωπικού, τη διενέργεια ελέγχων πρόσβασης στους φυσικούς και ψηφιακούς πόρους της ΕΛ.ΑΣ., την καταγραφή ενεργειών επεξεργασίας δεδομένων, την ενίσχυση της κυβερνοασφάλειας, τη διατήρηση αντιγράφων ασφαλείας και την κρυπτογράφηση, ψευδωνυμοποίηση και ανωνυμοποίηση των δεδομένων που διακινούνται και αποθηκεύονται στα πληροφοριακά συστήματα και αρχεία της Ελληνικής Αστυνομίας. Τέλος, παρατίθενται δύο μελέτες περίπτωσης, που αφορούν Αποφάσεις της Α.Π.Δ.Π.Χ., αναφορικά με παραβιάσεις, που εντοπίστηκαν κατά την έκδοση ταυτοτήτων και την κυβερνοεπίθεση «ΕΜΟΤΕΤ», αποδεικνύοντας τη βαρύτητα των προκλήσεων και την επιτακτικότητα των μέτρων αντιμετώπισής τους.

Κεφάλαιο 8: «Συμπεράσματα»

Στο τελευταίο κεφάλαιο, παρατίθενται τα συμπεράσματα της μελέτης, που πραγματοποιήθηκε και προτείνονται τρόποι επέκτασης αυτής.

2. Έννοια και κατηγορίες προσωπικών δεδομένων - Η σπουδαιότητα της προστασίας τους

Η ιλιγγιώδης ταχύτητα των τεχνολογικών εξελίξεων και η επέκταση του ψηφιακού κόσμου έχουν αναγάγει τα προσωπικά δεδομένα και την προστασία αυτών σε ζήτημα μείζονος σημασίας, το οποίο δεν αφορά μόνο το άτομο και την κοινωνία, αλλά απασχολεί ιδιαίτερα και τις Αρχές επιβολής του Νόμου και τις νομοθετικές Αρχές (Abdulhammad, A., Cherries, M. & Okunola, A., 2024). Πρωταγωνιστικό ρόλο στην προστασία των προσωπικών δεδομένων έχει ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) («Η Καθημερινή», 2018), ο οποίος διακρίνει τα προσωπικά δεδομένα σε απλά και ευαίσθητα² (Άρθρα 4, 6, 9 και 10 του GDPR). Η διάκριση αυτή είναι σημαντική για την ορθή εφαρμογή του Κανονισμού και γενικότερα των νομοθετικών διατάξεων σχετικά με την προστασία των προσωπικών δεδομένων και την επεξεργασία τους, ώστε να διασφαλίζονται τα θεμελιώδη δικαιώματα των φυσικών προσώπων (Lawspot, 2013).

2.1. Έννοια και κατηγορίες προσωπικών δεδομένων

Η έννοια των προσωπικών δεδομένων αποτυπώνεται ρητά στο άρθρο 4 του Κανονισμού (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, ο οποίος τέθηκε σε εφαρμογή τον Μάιο του 2018. Συγκεκριμένα, ως προσωπικά δεδομένα νοούνται τα στοιχεία που αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, το οποίο καλείται «υποκείμενο των δεδομένων». Συνεπώς, τα εν λόγω δεδομένα αφορούν ένα πρόσωπο, του οποίου η ταυτότητα είτε είναι ήδη γνωστή είτε μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, με αναφορά σε κάποιο αναγνωριστικό στοιχείο της ταυτότητάς του, όπως για παράδειγμα, το όνομα, ο αριθμός ταυτότητας ή σε κάποιον παράγοντα που χαρακτηρίζει τη φυσιολογική, σωματική, ψυχολογική, γενετική, πολιτιστική, οικονομική ή κοινωνική ταυτότητα του συγκεκριμένου προσώπου. Ο ορισμός των προσωπικών δεδομένων είναι ευρύς και περιλαμβάνει κάθε είδους πληροφορία, που αφορά ένα φυσικό πρόσωπο, δηλαδή έναν άνθρωπο (Ιγγλεζάκης, Λ., 2018: 40). Συνεπώς, προσωπικά δεδομένα αποτελούν, ενδεικτικά, ο αριθμός δελτίου ταυτότητας (Α.Δ.Τ.) και τα στοιχεία αυτής, ο αριθμός φορολογικού μητρώου (ΑΦΜ), ο αριθμός μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ), ο αριθμός τηλεφώνου, η IP διεύθυνση, η διεύθυνση ηλεκτρονικού ταχυδρομείου (email), η ηλικία, το φύλο, οι φωτογραφίες, ο αριθμός τραπεζικής κάρτας, η διεύθυνση κατοικίας, η πινακίδα κυκλοφορίας οχήματος, οι αναρτήσεις σε κοινωνικά δίκτυα, τα φορολογικά στοιχεία, το δακτυλικό αποτύπωμα, η υπογραφή, κ.α. (Κανέλλος, Λ., 2020: 16).

Στο άρθρο 9 του Κανονισμού αναλύονται οι ειδικές κατηγορίες προσωπικών δεδομένων, γνωστά και ως «ευαίσθητα δεδομένα» (Άρθρο 10 της Αιτιολογικής

² Η διάκριση των δεδομένων σε απλά και ευαίσθητα υπήρχε ήδη με την προϊσχύσασα Οδηγία 95/46/ΕΚ (άρθρο 8) και την υιοθέτησε ο GDPR.

Έκθεσης του GDPR). Αυτά τα δεδομένα λόγω της φύσης τους χρήζουν ιδιαίτερης μεταχείρισης, καθώς η επεξεργασία τους μπορεί να προκαλέσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων (Άρθρο 51 Αιτιολογικής Έκθεσης του GDPR), όπως για παράδειγμα διακρίσεις σε βάρος του υποκειμένου, προσβολή αξιοπρέπειας, παραβίαση ιδιωτικότητας, κ.λπ. (Quinn, P., 2022: 1585). Ως ευαίσθητα δεδομένα νοούνται εκείνα που αναφέρονται σε:

- **φυλετική ή εθνοτική καταγωγή**, όπως Ρομά, εθνοτικοί κατάλογοι λαθρομεταναστών, προσφύγων και αιτούντων διεθνούς προστασίας
- **θρησκευτικές ή φιλοσοφικές πεποιθήσεις**, όπως Χριστιανοί Μάρτυρες του Ιεχωβά Ελλάδος, Μουσουλμανική Ένωση, σωματεία υγιεινής διατροφής
- **πολιτικά φρονήματα**, όπως μέλη, υποστηρικτές και χρηματοδότες πολιτικών κομμάτων, υποψήφιοι, εθνικοί βουλευτές, ευρωβουλευτές, εκπρόσωποι φοιτητικών παρατάξεων
- **συμμετοχή σε συνδικαλιστική οργάνωση**, όπως μέλη εργατικών κέντρων, ομοσπονδιών, συνδικάτων, επαγγελματικών οργανώσεων (ΓΣΕΕ, ΟΑΜΕ) (Κανέλλος, Α., 2020: 29)
- **γενετικά δεδομένα**, ήτοι δεδομένα που το άτομο έχει κληρονομήσει ή αποκτήσει. Αυτά προκύπτουν ύστερα από ανάλυση βιολογικού δείγματος του εν λόγω ατόμου (ιδίως DNA ή RNA) και παρέχουν μοναδικές πληροφορίες αναφορικά με την φυσιολογία ή την υγεία του
- **βιομετρικά δεδομένα**, ήτοι εκείνα που προκύπτουν όταν τα βιολογικά, φυσικά ή συμπεριφορικά χαρακτηριστικά του ατόμου υποβάλλονται σε ειδική τεχνική επεξεργασία και επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του συγκεκριμένου ατόμου (Άρθρο 4 GDPR). Τα δεδομένα αυτά έχουν τις εξής ιδιότητες:
 - είναι καθολικά, δηλαδή υπάρχουν σε κάθε άνθρωπο,
 - είναι μοναδικά, που σημαίνει ότι είναι διαφορετικά σε κάθε άνθρωπο και
 - είναι μόνιμα, δηλαδή δεν μεταβάλλονται με την πάροδο του χρόνου (Broumas, Α., 2019).

Παραδείγματα βιομετρικών δεδομένων αποτελούν οι εικόνες προσώπου συγκεκριμένων τεχνικών προδιαγραφών και τα δακτυλοσκοπημένα δεδομένα.

- **δεδομένα υγείας**, τα οποία αφορούν την παρελθούσα, παρούσα ή μελλοντική κατάσταση της σωματικής ή ψυχικής υγείας του ατόμου, καθώς και την παροχή υπηρεσιών υγειονομικής φροντίδας, όπως για παράδειγμα ιατρικές και εργαστηριακές εξετάσεις, συνταγές, αρχεία ασθενών, τιμολόγια για νοσηλείες και υγειονομική περίθαλψη, ιατρικά πιστοποιητικά για χορήγηση άδειας από την εργασίας, κ.λπ.
- **σεξουαλική ζωή και γενετήσιο προσανατολισμό του ατόμου**, όπως δεδομένα αναφορικά με την σεξουαλική συμπεριφορά και έλξη προς άτομα διαφορετικού φύλου

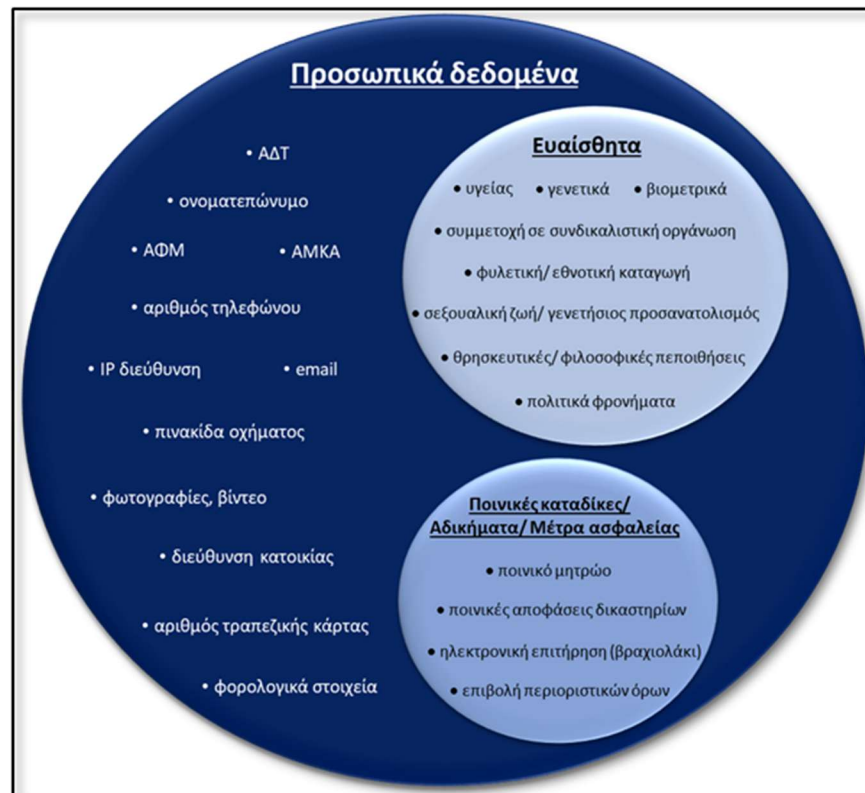
(ετεροφυλόφιλος/η), του ίδιου φύλου (ομοφυλόφιλος/η) ή και των δύο φύλων (αμφιφυλόφιλος) (Κανέλλος, Λ., 2020: 30).

Εκτός από τις προαναφερόμενες, άλλη μία ειδική κατηγορία προσωπικών δεδομένων, που αναφέρεται στο άρθρο 10 του Κανονισμού, είναι εκείνα που αφορούν **ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφαλείας**, όπως για παράδειγμα το ποινικό μητρώο, ποινικές αποφάσεις δικαστηρίων, επιβολή περιοριστικών όρων, δεδομένα ποινικής κατάστασης, ηλεκτρονική επιτήρηση υπόδικων, καταδίκων και κρατούμενων σε άδεια (Κανέλλος, Λ., 2020: 31). Αν και αυτά τα δεδομένα είναι ευαίσθητα, ο διαχωρισμός τους από εκείνα του άρθρου 9 έγκειται στο γεγονός ότι ο GDPR καθορίζει διαφορετικό πλαίσιο για την επεξεργασία τους.

Βάσει της ανάλυσης που προηγήθηκε, γίνεται κατανοητό ότι όσες πληροφορίες αφορούν ομάδες προσώπων, δεν συνιστούν προσωπικά δεδομένα, όπως για παράδειγμα αναφορά στη φοροδοτική ικανότητα των γιατρών (Ιγγλεζάκης, Ι., 2020:51).

Στην Εικόνα 1, που ακολουθεί, απεικονίζεται ο διαχωρισμός των απλών και ευαίσθητων δεδομένων³ εντός της γενικής κατηγορίας των προσωπικών δεδομένων. Λαμβάνοντας υπόψη ότι ο GDPR καθορίζει κλειστό αριθμό ειδικών κατηγοριών προσωπικών δεδομένων (δηλ. συγκεκριμένες κατηγορίες ευαίσθητων δεδομένων), όσα δεν ανήκουν σε αυτές τις συγκεκριμένες κατηγορίες θεωρούνται απλά (Χριστοδούλου, Κ., 2020: 32). Τα δεδομένα ειδικών κατηγοριών είναι προσωπικά, χωρίς να ισχύει το αντίστροφο, δηλαδή δεν είναι όλα τα προσωπικά δεδομένα, δεδομένα ειδικών κατηγοριών.

³ Συμπεριλαμβανομένων όσων αφορούν ποινικές καταδίκες, αδικήματα και μέτρα ασφαλείας.



Εικόνα 1: Διαχωρισμός προσωπικών δεδομένων

2.2. Προστασία προσωπικών δεδομένων

Με το πέρασμα των ετών, η ραγδαία ανάπτυξη της τεχνολογίας, η ευρεία χρήση του διαδικτύου και η ψηφιοποίηση των δημόσιων και ιδιωτικών υπηρεσιών, έχουν οδηγήσει τους πολίτες στην ανάγκη να παραχωρούν και να καταχωρούν τα προσωπικά τους δεδομένα στο διαδίκτυο όλο και περισσότερο, προκειμένου να εξυπηρετούν τα συμφέροντά τους («Η Καθημερινή», 2018). Ενδεικτικά παραδείγματα αποτελούν οι ηλεκτρονικές αγορές, η εργασία, οι υπηρεσίες υγείας και εκπαίδευσης, οι τραπεζικές συναλλαγές, τα μέσα κοινωνικής δικτύωσης, κ.λπ. Παρ' ότι η ψηφιοποίηση των υπηρεσιών έχει διευκολύνει σε πολύ μεγάλο βαθμό τις καθημερινές δραστηριότητες των ανθρώπων, η συλλογή και αποθήκευση των προσωπικών δεδομένων εγκυμονεί σοβαρούς κινδύνους, όπως η υποκλοπή των στοιχείων ταυτότητας, οι παραβιάσεις των δεδομένων, βλάβη της φήμης, απάτες, εκβιάσεις, η μη εξουσιοδοτημένη παρακολούθηση και επεξεργασία αυτών, κ.α., οι οποίοι μπορεί να οδηγήσουν σε παραβιάσεις της ιδιωτικής ζωής του ατόμου, με συνέπειες σε ψυχολογικό, οικονομικό και κοινωνικό επίπεδο (Crossa, C. & Holt, T., 2025: 17-18) (Ιγγλεζάκης, Ι., 2020: 71-72).

Η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα κάθε ατόμου, το οποίο κατοχυρώνεται στο άρθρο 8 παρ. 1 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και στο άρθρο 16 παρ. 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (Σ.Λ.Ε.Ε.), ενώ σε εθνικό επίπεδο προβλέπεται και κατοχυρώνεται στο άρθρο 9^Α του Συντάγματος (Άρθρο 1 της Αιτιολογικής

Έκθεσης του GDPR). Η έννοια του δικαιώματος είναι άρρηκτα συνδεδεμένη με την έννοια του προσώπου. Ως δικαίωμα νοείται η εξουσία που απονέμει το δίκαιο στο πρόσωπο προς πραγμάτωση εννόμου συμφέροντος, δηλαδή συμφέροντος που προστατεύεται από την έννομη τάξη. Για κάθε δικαίωμα ενός ατόμου αντιστοιχεί υποχρέωση του άλλου ή των άλλων ατόμων να το σέβονται και να μην το παραβιάζουν (Σπυρόπουλος, Φ., 2012: 1). Συνεπώς, η προστασία των προσωπικών δεδομένων και γενικότερα της ιδιωτικής ζωής του ατόμου αποτελεί κύριο μέλημα των κυβερνήσεων, φορέων και οργανισμών. Σε αυτό το πλαίσιο, θεσπίζονται και εφαρμόζονται κανονιστικές ρυθμίσεις, προκειμένου να διασφαλίζεται η προστασία των δικαιωμάτων των πολιτών, αλλά και η υπεύθυνη και νόμιμη διαχείριση των προσωπικών τους δεδομένων (Abdulhammad, A., Cherries, M. & Okunola, A., 2024). Με αυτό τον τρόπο, ενισχύεται η αίσθηση ασφάλειας των ατόμων ως προς την ιδιωτικότητά τους, αλλά και η εμπιστοσύνη τους ως προς τα ψηφιακά συστήματα και το πρόσωπο, τον φορέα, την Αρχή ή την υπηρεσία που έχει πρόσβαση στα δεδομένα τους και τα επεξεργάζεται (Σιασιάκος, Κ., Αναστασίου Σ. και Τούντας, Κ., 2016).

Σε αυτό το σημείο αξίζει να αναφερθεί ότι σύμφωνα με το άρθρο 1 του GDPR, ως επεξεργασία προσωπικών δεδομένων νοείται κάθε πράξη ή σύνολο πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε τέτοια δεδομένα ή σε σύνολα αυτών, όπως είναι η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή. Επεξεργασία με αυτοματοποιημένα μέσα είναι εκείνη που πραγματοποιείται με συστήματα που κάνουν αυτοματοποιημένη επεξεργασία δεδομένων και γίνεται κυρίως με ψηφιακά συστήματα, υπολογιστές και συστήματα βιντεοεπιτήρησης⁴ (Ιγγλεζάκης, Ι., 2018: 29). Με πιο απλά λόγια, η επεξεργασία αφορά τις πράξεις που λαμβάνουν χώρα σε όλο τον κύκλο ζωής των δεδομένων, από τη συλλογή μέχρι και την καταστροφή τους (Μήτρου, Α., 2017: 42).

Συνεπώς, ο διαχωρισμός των προσωπικών δεδομένων, όπως προβλέπεται από τον GDPR, είναι καθοριστικής σημασίας, καθώς επηρεάζει άμεσα τον τρόπο με τον οποίο αυτά μπορούν να τεθούν υπό επεξεργασία, όπως θα αναλυθεί στο Κεφάλαιο 4. Παρά τα οφέλη, που προσφέρει η ψηφιοποίηση των υπηρεσιών, η συνεχής έκθεση των προσωπικών δεδομένων των ατόμων σε κινδύνους, καθιστά αναγκαία την θέσπιση, αναθεώρηση και ειδικότερα την αυστηρή τήρηση σχετικών νομικών διατάξεων. Μόνο υπό αυτές τις προϋποθέσεις μπορεί να διασφαλιστεί η προστασία των προσωπικών δεδομένων και κατ' επέκταση της ιδιωτικότητας των φυσικών προσώπων.

⁴ Δεν θεωρείται επεξεργασία με αυτοματοποιημένα μέσα εκείνη που πραγματοποιείται με συμβατικούς μηχανισμούς ή μηχανές, όπως είναι για παράδειγμα οι μηχανές φαξ, οι τυπογραφικές μηχανές, η κλασική γραφομηχανή, κ.λπ.

3. Μεθοδολογία Επισκόπησης

3.1. Εισαγωγή

Στο παρόν κεφάλαιο παρουσιάζεται η μεθοδολογία που εφαρμόστηκε κατά την συγγραφή της εργασίας, η οποία αποτελεί βιβλιογραφική μελέτη ανασκόπησης, αναφορικά με την επεξεργασία και προστασία των προσωπικών δεδομένων στο πλαίσιο της λειτουργίας της Ελληνικής Αστυνομίας. Μία βιβλιογραφική μελέτη ανασκόπησης (Systematic Literature Review – SLR) αποσκοπεί στον εντοπισμό, συλλογή και ανάλυση των διαθέσιμων κειμένων (π.χ. άρθρα, διατριβές, βιβλία, κ.λπ.) και ενημερώνει τον αναγνώστη για τη σύγχρονη βιβλιογραφία αναφορικά με ένα συγκεκριμένο θέμα – αντικείμενο. Σκοπός είναι η συστηματική εξέταση της υφιστάμενης βιβλιογραφίας, η οποία αφορά ένα συγκεκριμένο θέμα σε συνάρτηση με ερευνητικά ερωτήματα προκειμένου να αναδειχθούν πεδία που χρήζουν περαιτέρω διερεύνησης ή να εντοπιστούν τυχόν κενά (Carrera-Rivera A., et al., 2022).

Υπό αυτό το πρίσμα, υιοθετήθηκαν ορισμένες βασικές οδηγίες, που προτείνονται από τη μεθοδολογία Systematic Literature Review των Kitchenham & Charters (2007), βάσει των οποίων προσδιορίστηκαν τα βήματα της μεθοδολογίας της παρούσας μελέτης ανασκόπησης. Έτσι, σε πρώτο βαθμό ορίζεται ο βασικός στόχος της εργασίας και τα ερευνητικά ερωτήματα, που τέθηκαν προς ανάπτυξη. Στην συνέχεια, παρουσιάζεται η διαδικασία αναζήτησης βιβλιογραφίας, που ακολουθήθηκε, και συγκεκριμένα οι λέξεις – κλειδιά που χρησιμοποιήθηκαν, τα κριτήρια ένταξης, αποκλεισμού και ποιότητας που εφαρμόστηκαν στην εντοπισμένη βιβλιογραφία, και τα αποτελέσματα από την εφαρμογή αυτών των κριτηρίων που οδήγησαν στην παραγωγή του τελικού συνόλου των κειμένων προς ανάλυση. Οι επόμενες ενότητες του τρέχοντος κεφαλαίου καλύπτουν το κάθε ένα βήμα ξεχωριστά, αναλύοντας παράλληλα τα αποτελέσματα από την εφαρμογή του.

3.2. Βασικός στόχος και ερευνητικά ερωτήματα

Η παρούσα μελέτη ανασκόπησης αποβλέπει στην ανάλυση του νομικού πλαισίου προστασίας δεδομένων, στη διερεύνηση του τρόπου, με τον οποίο η Ελληνική Αστυνομία επεξεργάζεται και προστατεύει, τόσο απλά όσο και ευαίσθητα, προσωπικά δεδομένα και στην ανάδειξη των προκλήσεων που δύναται να ανακύψουν και στα μέτρα αντιμετώπισής τους, στο πλαίσιο συγκεκριμένων λειτουργιών της.

Επομένως, τα ερευνητικά ερωτήματα, που απαντώνται στην μελέτη ανασκόπησης είναι τα ακόλουθα:

1) Ποιο είναι το ισχύον νομικό πλαίσιο προστασίας δεδομένων;

Αιτιολόγηση: Προκειμένου να τεθούν τα όρια νόμιμης δράσης της ΕΛ.ΑΣ. αναφορικά με την επεξεργασία προσωπικών δεδομένων είναι απαραίτητος ο σαφής προσδιορισμός του υφιστάμενου νομικού πλαισίου, σε ευρωπαϊκό και εθνικό επίπεδο.

Που απαντάται: Στο Κεφάλαιο 4

- 2) Ποιες είναι οι βασικές αρχές επεξεργασίας προσωπικών δεδομένων και τα δικαιώματα των υποκειμένων;

Αιτιολόγηση: Για την κατανόηση του τρόπου με τον οποίο η ΕΛ.ΑΣ. επεξεργάζεται και προστατεύει τα προσωπικά δεδομένα και την αξιολόγηση του κατά πόσο αυτός είναι συμβατός με το νομικό πλαίσιο προστασίας δεδομένων, πρέπει να οριστούν πρώτα οι βασικές αρχές επεξεργασίας και τα δικαιώματα των υποκειμένων.

Που απαντάται: Στο Κεφάλαιο 4

- 3) Ποια είναι τα καθήκοντα της Αρχής και του Γραφείου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;

Αιτιολόγηση: Η Αρχή και το Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνιστούν μηχανισμούς εποπτείας και ελέγχου, οι οποίοι διαδραματίζουν καθοριστικό ρόλο στη διασφάλιση της νόμιμης επεξεργασίας των προσωπικών δεδομένων. Συνεπώς, είναι απαραίτητη η παρουσίαση των αρμοδιοτήτων τους.

Που απαντάται: Στο Κεφάλαιο 5

- 4) Πώς επεξεργάζεται και προστατεύει η Ελληνική Αστυνομία τα προσωπικά δεδομένα, κατά την ανάλυση DNA, την άρση του απορρήτου των επικοινωνιών, τη δημοσιοποίηση στοιχείων κατηγορουμένων και καταδικασθέντων, την έκδοση ταυτοτήτων και διαβατηρίων, την επιτήρηση δημόσιων χώρων, τη συμμετοχή των υποψηφίων στις Σχολές της ΕΛ.ΑΣ. και τη διασυννοριακή συνεργασία;

Αιτιολόγηση: Αυτό το ερώτημα αποτελεί τον πυρήνα της παρούσας μελέτης, καθώς εξετάζει τον τρόπο με τον οποίο η ΕΛ.ΑΣ. επεξεργάζεται και προστατεύει τα προσωπικά δεδομένα, κατά τις ανωτέρω δράσεις της.

Που απαντάται: Στο Κεφάλαιο 6

- 5) Ποιες είναι οι προκλήσεις που προκύπτουν και ποια μέτρα αντιμετώπισης μπορούν να ληφθούν;

Αιτιολόγηση: Η εργασία θα ήταν ημιτελής, εάν δεν αναδεικνύονταν οι προκλήσεις και τα μέτρα αντιμετώπισης αυτών στο πλαίσιο επεξεργασίας και προστασίας των προσωπικών δεδομένων από την ΕΛ.ΑΣ..

Που απαντάται: Στο Κεφάλαιο 7

- 6) Τι προτείνεται για επέκταση της παρούσας μελέτης και για μελλοντική έρευνα;

Αιτιολόγηση: Με την παράθεση προτάσεων για επέκταση και για μελλοντική έρευνα, διασφαλίζεται ο διαχρονικός χαρακτήρας της μελέτης και αναδεικνύονται ερευνητικά κενά.

Που απαντάται: Στο Κεφάλαιο 8

Προς εκπλήρωση του ανωτέρω βασικού στόχου και απάντηση στα ερευνητικά ερωτήματα που τέθηκαν, πραγματοποιήθηκε στοχευμένη αναζήτηση βιβλιογραφίας με χρήση εξειδικευμένων λέξεων – κλειδιών, όπως αυτά αναφέρονται αναλυτικά στην ενότητα (Ενότητα 3.3), που ακολουθεί.

3.3. Διαδικασία αναζήτησης βιβλιογραφίας

Η αναζήτηση της βιβλιογραφίας που χρησιμοποιήθηκε για την συγγραφή της παρούσας εργασίας, έλαβε χώρα σε φυσικές βιβλιοθήκες, αλλά και στις ακόλουθες έγκριτες βάσεις δεδομένων, επίσημες ιστοσελίδες φορέων και εποπτικών Αρχών και ειδησεογραφικές πηγές:

Πίνακας 1: Αιτιολόγηση επιλογής ψηφιακών βάσεων δεδομένων

Βάση δεδομένων	Περιγραφή	Αιτιολόγηση επιλογής
Google Scholar	Μηχανή αναζήτησης με μεγάλο εύρος επιστημονικών πηγών ανεξαρτήτου κλάδου και εκδότη	Επιλέχθηκε για τον αρχικό εντοπισμό και συλλογή σχετικών κειμένων, λόγω του μεγάλου εύρους αποτελεσμάτων που παρέχει
ScienceDirect	Διεθνής μηχανή αναζήτησης για επιστημονικές έρευνες	Επιλέχθηκε για την αναζήτηση άρθρων σχετικών με την προστασία των προσωπικών δεδομένων σε ευρωπαϊκό επίπεδο
EUR-Lex	Επίσημη βάση της Ε.Ε. για την αναζήτηση Κανονισμών, Οδηγιών και Αποφάσεων των Ευρωπαϊκών Οργάνων	Επιλέχθηκε για κείμενα Οργάνων της Ε.Ε. καθώς είναι η επίσημη βάση του Ευρωπαϊκού Δικαίου
Kodiko.gr	Πηγή αναζήτησης της εθνικής νομοθεσίας, με τις τελευταίες τροποποιήσεις	Επιλέχθηκε για τον εντοπισμό των εθνικών νομικών κειμένων
Επίσημες ιστοσελίδες Φορέων και εποπτικών Αρχών	Ιστότοποι φορέων και εποπτικών Αρχών, μέσω των οποίων δημοσιεύονται Αποφάσεις, Εγκύκλιοι, κατευθυντήριες οδηγίες, ανακοινώσεις και λοιπές επίσημες πληροφορίες αναφορικά με την	Επιλέχθηκε για αξιοποίηση του επίσημου υλικού, που παρέχεται από αρμόδιους φορείς και εποπτικές Αρχές, συμπληρώνοντας περαιτέρω τις ακαδημαϊκές πηγές

	άσκηση των καθηκόντων της ΕΛ.ΑΣ.	
Ειδησεογραφικές πηγές	Αναγνωρισμένοι ειδησεογραφικοί ιστότοποι και νομικές ενημερωτικές πλατφόρμες με δημοσιογραφικά κείμενα και ενημερωτικά άρθρα	Χρησιμοποιήθηκαν επικουρικά στο πρωτογενές υλικό ως συμπληρωματικό, που αφορά την επικαιρότητα

Κατά την αναζήτηση, χρησιμοποιήθηκαν λέξεις – κλειδιά, οι οποίες αφορούν νομικά κείμενα προστασίας προσωπικών δεδομένων, δράσεις της Ελληνικής Αστυνομίας, κατά τις οποίες συλλέγει και επεξεργάζεται τέτοιου είδους δεδομένα, και υφιστάμενες προκλήσεις και τρόπους αντιμετώπισης αυτών. Βασικό κριτήριο της επιλογής των πηγών ήταν η κάλυψη του νομικού πλαισίου, αλλά και του αστυνομικού έργου, μέσα από την εξέταση αντιπροσωπευτικών περιπτώσεων.

Χρησιμοποιήθηκαν τόσο ελληνικές όσο και αγγλικές λέξεις – κλειδιά, οι οποίες μπορούν να διαχωριστούν στις εξής κατηγορίες:

Εννοιολογικοί όροι:

«προσωπικά δεδομένα», «personal data», «βασικές αρχές επεξεργασίας δεδομένων», «δικαιώματα των υποκειμένων»

Νομικό πλαίσιο:

«Γενικός Κανονισμός Προστασίας Δεδομένων», «GDPR», «Οδηγία 2016/680», «Law Enforcement Directive», «άρθρο 9^Α Συντάγματος», «Ν. 4624/2019», «Ν. 5002/2022», «Ν. 3471/2006», «Ν. 3917/2011», «Ν. 4620/2019», «Ν. 5187/2025», «ΠΔ 47/2005», «ΠΔ 75/2020», «ΠΔ 81/2021», «ΠΔ 25/2022», «Υ.Α. 3021/22/10-ο’/2025», «Υ.Α. 8200/0-297647/2018», «Απόφαση 2008/615/ΔΕΥ», «Απόφαση 2008/616/ΔΕΥ»

Πεδίο εφαρμογής - ΕΛ.ΑΣ.:

«ανάλυση DNA», «άρση του απορρήτου», «αστυνομική ταυτότητα», «Α.Δ.Τ.», «ελληνικά διαβατήρια», «δημοσιοποίηση στοιχείων», «επιτήρηση δημόσιων χώρων», «εισαγωγή στις Σχολές της ΕΛ.ΑΣ.», «διασυνοριακή συνεργασία»

Εποπτικοί μηχανισμοί και Σχετικές Αποφάσεις:

«Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», «Α.Π.Δ.Π.Χ.», «Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», «Απόφαση 43/2021», «Απόφαση 32/2024», «Γνωμοδότηση 4/2024»

Οι παραπάνω λέξεις – κλειδιά χρησιμοποιήθηκαν είτε μεμονωμένα είτε συνδυαστικά μεταξύ τους με τη χρήση των λογικών τελεστών «AND» και «OR», όπως υποδεικνύουν οι Kitchenham & Charters (2007).

Δεδομένου ότι στην παρούσα μελέτη εξετάζονται συγκεκριμένες περιπτώσεις, κατά τις οποίες η ΕΛ.ΑΣ. διαχειρίζεται προσωπικά δεδομένα, ευαίσθητα και μη, χρησιμοποιήθηκαν λέξεις – κλειδιά, που να καλύπτουν πληρέστερα το αντικείμενό της.

3.4. Κριτήρια φιλτραρίσματος βιβλιογραφίας

Κατά την επιλογή της βιβλιογραφίας σε μία μελέτη ανασκόπησης ορίζονται τρία είδη κριτηρίων αξιολόγησης αυτής που θα πρέπει να εφαρμοστούν:

- 1) Κριτήρια ένταξης
- 2) Κριτήρια αποκλεισμού
- 3) Κριτήρια ποιότητας

Τα κριτήρια ένταξης και αποκλεισμού βασίζονται στα μεταδεδομένα μίας δημοσίευσης και αφορούν, κυρίως, τη συνάφεια, το είδος, τη γλώσσα, το έτος της δημοσίευσης κ.λπ., ενώ τα κριτήρια ποιότητας βασίζονται στο περιεχόμενο της δημοσίευσης και αφορούν τον βαθμό κατανόησης και την επάρκεια του περιεχομένου της (Kitchenham, B., & Charters, S., 2007).

Τα κριτήρια ένταξης που εφαρμόστηκαν, αφορούν:

- Τη συνάφεια του κειμένου. Ένα κείμενο για να επιλεχτεί πρέπει να σχετίζεται άμεσα με το αντικείμενο της παρούσας εργασίας, δηλαδή να αφορά τα προσωπικά δεδομένα, το ισχύον νομικό πλαίσιο, την επεξεργασία των δεδομένων από την Ελληνική Αστυνομία και τη συμβολή των εποπτικών αρχών.
- Το είδος του κειμένου. Επιλέγονται μόνο νομικά κείμενα, επιστημονικά άρθρα, ακαδημαϊκά βιβλία, Αποφάσεις αρμόδιων Αρχών και Οργάνων, καθώς επίσης δημοσιεύσεις σε επίσημες ιστοσελίδες φορέων (π.χ. ΕΛ.ΑΣ., Υπουργείων, κ.λπ.) και σε επίσημους ενημερωτικούς και ειδησεογραφικούς ιστοτόπους, ως συμπληρωματικό υλικό της τρέχουσας επικαιρότητας.
- Η γλώσσα του κειμένου. Επιλέγονται κείμενα που είναι γραμμένα στην ελληνική και αγγλική γλώσσα. Η επιλογή αυτή αιτιολογείται από το γεγονός ότι το αντικείμενο της παρούσας μελέτης αφορά τόσο το εθνικό, όσο και ευρωπαϊκό νομικό πλαίσιο, αλλά και τις δράσεις της ΕΛ.ΑΣ..
- Το έτος του κειμένου. Για επιστημονικά άρθρα, βιβλία και ιστοσελίδες επιλέγεται το χρονικό διάστημα από το 2016 και μετά, ενώ για τα νομικά κείμενα επιλέγεται ως αρχή το έτος 1995, όταν θεσπίστηκε το Π.Δ. 4/1995, που ρυθμίζει την εισαγωγή στις Σχολές της ΕΛ.ΑΣ. με το σύστημα γενικών εξετάσεων.

Μετά τα κριτήρια ένταξης, εφαρμόζονται τα κριτήρια αποκλεισμού, προκειμένου να απορριφθούν πηγές, που παρ' ότι ικανοποιούν τα προαναφερόμενα κριτήρια

ένταξης, δεν είναι κατάλληλες ή απαραίτητες για την κάλυψη του θέματος της συγκεκριμένης εργασίας. Υπό αυτό το πρίσμα, τα κριτήρια αποκλεισμού, αφορούν:

- Τις παρωχημένες πληροφορίες του κειμένου. Απορρίπτονται κείμενα, που ενώ αναφέρονται στην επεξεργασία των δεδομένων από την Ελληνική Αστυνομία, δεν περιλαμβάνουν τις τελευταίες τροποποιήσεις της νομοθεσίας, με αποτέλεσμα να είναι μη αξιοποιήσιμα.
- Την προσβασιμότητα του κειμένου. Απορρίπτονται όσα κείμενα δεν είναι προσβάσιμα και είναι διαθέσιμη μόνο η εισαγωγή, περίληψη, τα συμπεράσματα ή μέρος αυτών.

Όσον αφορά τα κριτήρια ποιότητας, αυτά επικεντρώνονται:

- Στον βαθμό κατανόησης του περιεχόμενου. Εξετάζεται εάν ένα κείμενο παρουσιάζει σαφήνεια και συνοχή, ώστε να κατανοεί εύκολα ο εκάστοτε αναγνώστης το αντικείμενο που πραγματεύεται και τα συμπεράσματα που διατυπώνονται.
- Στην επάρκεια του περιεχομένου. Εξετάζεται εάν ένα κείμενο, παρέχει επαρκείς και χρήσιμες πληροφορίες για την συγκεκριμένη μελέτη.
- Στην επικάλυψη των κειμένων. Για την αποφυγή πλεονασμών, μεταξύ κειμένων με παρόμοιο περιεχόμενο, επιλέγονται εκείνα που καλύπτουν καλύτερα το θέμα της εργασίας.
- Στην συνάφεια του κειμένου. Για την ανάπτυξη του Κεφαλαίου 6 επιλέγονται κείμενα, που περιγράφουν πως εφαρμόζονται οι βασικές αρχές επεξεργασίας δεδομένων από την Ελληνική Αστυνομία και πως προστατεύονται τα προσωπικά δεδομένα στις συγκεκριμένες περιπτώσεις, που αποτυπώθηκαν στο 4ο ερευνητικό ερώτημα και όχι γενικά από δημόσιους και ιδιωτικούς φορείς και οργανισμούς, ή για άλλες δράσεις της ΕΛ.ΑΣ.

3.5. Αποτελέσματα φιλτραρίσματος βιβλιογραφίας

Βάσει των όσων έχουν προαναφερθεί, γίνεται σαφές ότι η αναζήτηση και επιλογή της βιβλιογραφίας, πραγματοποιήθηκε σε τρεις φάσεις. Στην πρώτη φάση, που αφορά την αναζήτηση με τη χρήση λέξεων – κλειδίων, εντοπίστηκαν 155 κείμενα με περιεχόμενο σχετικό με το θέμα της εργασίας. Στη δεύτερη φάση, εφαρμόστηκαν τα κριτήρια ένταξης και αποκλεισμού, που είχαν ως αποτέλεσμα τη διατήρηση 118 κειμένων. Στην τρίτη φάση, αφού εφαρμόστηκαν και τα κριτήρια ποιότητας και εξετάστηκε ενδελεχώς το περιεχόμενο κάθε κειμένου, επιλέχτηκαν τελικά 93 κείμενα.

Το υψηλό ποσοστό διατήρησης των πηγών (60%), οφείλεται στο γεγονός ότι κατά την αρχική αναζήτηση των κειμένων χρησιμοποιήθηκαν στοχευμένες λέξεις – κλειδιά και τέθηκαν εξειδικευμένα ερευνητικά ερωτήματα, που αφορούσαν την επεξεργασία προσωπικών δεδομένων και την προστασία τους από την ΕΛ.ΑΣ. στο πλαίσιο συγκεκριμένων λειτουργιών της, κάτι που οδήγησε στον εξ' αρχής περιορισμένο αριθμό πηγών.

Για την καλύτερη κατανόηση της (επιλεγμένης) βιβλιογραφίας, που χρησιμοποιήθηκε στην παρούσα διπλωματική εργασία, ακολουθούν τέσσερα σχήματα με ποσοτική απεικόνιση αυτής, στα οποία διαχωρίζεται ανά είδος, ανά εκδότη και ανά έτος δημοσίευσης.

Η κατανομή ανά είδος, παρουσιάζεται σε δύο επίπεδα. Το πρώτο αφορά τον χαρακτηρισμό της βιβλιογραφίας, βάσει του οποίου διαχωρίζεται σε λευκή (επιστημονικά άρθρα, ακαδημαϊκά βιβλία, Νόμοι, Αποφάσεις), γκρίζα (επίσημες ιστοσελίδες φορέων όπως ΕΛ.ΑΣ., Υπουργεία κλπ.) και κίτρινη (ειδησεογραφικοί ιστότοποι). Το δεύτερο επίπεδο περιλαμβάνει την κατανομή των υποκατηγοριών της λευκής βιβλιογραφίας.



Σχήμα 1: Κατανομή βιβλιογραφίας ανά είδος / Χαρακτηρισμός βιβλιογραφίας

Στο Σχήμα 1, παρουσιάζεται η κατανομή των 93 πηγών ανά είδος, βάσει του χαρακτηρισμού της βιβλιογραφίας. Η συνολική βιβλιογραφία διαχωρίστηκε σε τρεις μεγάλες κατηγορίες και συγκεκριμένα σε λευκή, γκρίζα και κίτρινη. Η λευκή περιλαμβάνει τα Επιστημονικά Άρθρα, τα Ακαδημαϊκά Βιβλία, τους Νόμους και τις Αποφάσεις, που χρησιμοποιήθηκαν κατά τη συγγραφή της εργασίας. Η πλειοψηφία των πηγών (69%) εντάσσεται στην λευκή κατηγορία, κάτι που επιβεβαιώνει την αξιοπιστία και βαρύτητα των χρησιμοποιούμενων πηγών. Η γκρίζα κατηγορία (16%) περιλαμβάνει τις επίσημες ιστοσελίδες φορέων, όπως η Ελληνική Αστυνομία, τα Υπουργεία, κ.λπ. και η κίτρινη κατηγορία (15%) περιλαμβάνει τις ειδησεογραφικές πηγές, όπως για παράδειγμα skai.gr, lawspot, «Η Καθημερινή», κ.λπ.. Τόσο η γκρίζα όσο και η κίτρινη βιβλιογραφία χρησιμοποιήθηκε επικουρικά στη λευκή, για αυτό και εμφανίζονται σε χαμηλότερα ποσοστά.



Σχήμα 2: Κατανομή υποκατηγοριών λευκής βιβλιογραφίας

Στο Σχήμα 2, παρουσιάζεται η κατανομή των 64 πηγών, που ανήκουν στην λευκή βιβλιογραφία, σε επιμέρους υποκατηγορίες. Πιο συγκεκριμένα, όπως προαναφέρθηκε, διαχωρίζονται σε Επιστημονικά Άρθρα, Ακαδημαϊκά Βιβλία, Νόμους και Αποφάσεις. Η πλειοψηφία της λευκής βιβλιογραφίας αφορά τους Νόμους (34%) κάτι που αντικατοπτρίζει τον κανονιστικό χαρακτήρα της εργασίας. Αξιοσημείωτη είναι και η συνεισφορά των Ακαδημαϊκών Βιβλίων (28%), τα οποία είναι εστιασμένα στην ελληνική πραγματικότητα και αφορούν κυρίως τις λειτουργίες της ΕΛ.ΑΣ., που περιγράφονται στο Κεφάλαιο 6, αλλά και τις ανακύπτουσες προκλήσεις κατά την επεξεργασία προσωπικών δεδομένων και τους τρόπους αντιμετώπισής τους. Οι Αποφάσεις (22%) και τα Επιστημονικά Άρθρα (16%) αποτελούν πηγές, που δεν θα μπορούσαν να λείπουν από μία τέτοιου είδους μελέτη, καθώς χρησιμοποιούνται για την πλήρη κάλυψη του θέματος της παρούσας εργασίας και αφορούν τόσο την εθνική όσο και ευρωπαϊκή πραγματικότητα. Η εμφάνιση αυτών σε μικρότερα ποσοστά αποδίδεται στο αντικείμενο της παρούσας εργασίας, καθώς περιορισμένες Αποφάσεις (π.χ. εποπτικών και δικαστικών Αρχών) συνδέουν άμεσα την προστασία των προσωπικών δεδομένων με την επεξεργασία τους από την Ελληνική Αστυνομία, ενώ τα Επιστημονικά Άρθρα επικεντρώνονται κυρίως στο ευρωπαϊκό επίπεδο.



Σχήμα 3: Κατανομή βιβλιογραφίας ανά εκδότη

Στο Σχήμα 3, παρουσιάζεται η κατανομή των 93 πηγών ανά εκδότη. Το σύνολο των πηγών κατανέμεται σε 6 κατηγορίες και συγκεκριμένα στις ακόλουθες:

1. «ΕΚΔΟΤΙΚΟΙ ΟΙΚΟΙ & ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ» : «ΔΙΑΔΟΣΗ ΓΝΩΣΗΣ»,
2. «ΕΥΡΩΠΑΪΚΑ ΘΕΣΜΙΚΑ & ΣΥΜΒΟΥΛΕΥΤΙΚΑ ΟΡΓΑΝΑ» : «ΥΠΕΡΕΘΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ»,
3. «ΕΘΝΙΚΑ ΝΟΜΟΘΕΤΙΚΑ & ΕΚΤΕΛΕΣΤΙΚΑ ΟΡΓΑΝΑ» : «ΠΑΡΑΓΩΓΗ ΝΟΜΩΝ & ΠΟΛΙΤΙΚΩΝ»
4. «ΕΠΟΠΤΙΚΕΣ ΑΡΧΕΣ» : «ΕΠΟΠΤΕΙΑ & ΛΟΓΟΔΟΣΙΑ»
5. «ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ» : «ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΕΠΙΒΟΛΗ»
6. «ΤΥΠΟΣ – ΜΜΕ» : «ΔΗΜΟΣΙΑ ΔΙΕΡΜΗΝΕΙΑ»

Η πλειοψηφία των πηγών προέρχεται – αθροιστικά - από τα Ευρωπαϊκά Θεσμικά και Συμβουλευτικά Όργανα (15%), καθώς και από τα Εθνικά Νομοθετικά & Εκτελεστικά Όργανα (27%) (σύνολο 42%), κάτι που είναι απόλυτα λογικό λαμβάνοντας υπόψη και την ανάλυση που προηγήθηκε στα Σχήμα 1 και Σχήμα 2. Πιο αναλυτικά, το 23,65% της συνολικής βιβλιογραφίας αφορά Νόμους, οι οποίοι εκδίδονται από τα Ευρωπαϊκά και Εθνικά Όργανα, που προαναφέρθηκαν. Επιπλέον, το 71,4% των Αποφάσεων (~10,75% επί του συνόλου) προέρχεται από Ευρωπαϊκά και Εθνικά Όργανα και το 46,6% της γκρίζας βιβλιογραφίας (~7,5% επί του συνόλου) αφορά αναρτήσεις στις επίσημες ιστοσελίδες φορέων. Οι πηγές αυτές αντικατοπτρίζουν την αναζήτηση σε νομικά και ερμηνευτικά κείμενα, που αφορούν το εξεταζόμενο θέμα.

Σε υψηλό ποσοστό εμφανίζονται και οι πηγές από Εκδοτικούς Οίκους και Βιβλιογραφικές Βάσεις Δεδομένων (30%), που περιλαμβάνουν τα Επιστημονικά

Άρθρα και τα Ακαδημαϊκά Βιβλία, που χρησιμοποιήθηκαν για την εκπόνηση της εργασίας.

Αρκετά αξιόλογο είναι και το ποσοστό της βιβλιογραφίας που προέρχεται από τον Τύπο και τα ΜΜΕ - ειδησεογραφικές πηγές (15%), η οποία χαρακτηρίζεται ως κίτρινη βιβλιογραφία, κάτι που υποδηλώνει ότι η επεξεργασία των δεδομένων από την Ελληνική Αστυνομία συνιστά ένα φλέγον ζήτημα με κοινωνικό αντίκτυπο.

Ασφαλώς, ένα μέρος των κειμένων, που χρησιμοποιήθηκαν κατά την συγγραφή της εργασίας, προέρχονται από την ίδια την Ελληνική Αστυνομία (5%), αλλά και από Εποπτικές Αρχές (8%), παρέχοντας πιο εξειδικευμένο υλικό, αφού τα κείμενα της ΕΛ.ΑΣ. έχουν πιο «επιχειρησιακό χαρακτήρα», ενώ αυτά των Εποπτικών Αρχών πιο «ελεγκτικό». Σε αυτές τις κατηγορίες εντάσσονται αναρτήσεις στην επίσημη ιστοσελίδα της ΕΛ.ΑΣ. και εποπτικών Αρχών, καθώς και Αποφάσεις και Γνωμοδοτήσεις, που έχει εκδώσει η Α.Π.Δ.Π.Χ. και η Α.Δ.Α.Ε..

Από την ανάλυση που πραγματοποιήθηκε γίνεται σαφές ότι οι πηγές, που χρησιμοποιήθηκαν, καλύπτουν όλες τις δυνατές περιπτώσεις που επιλέχθηκαν να εξεταστούν στην παρούσα εργασία, διασφαλίζοντας την ολιστική προσέγγιση του θέματος.



Σχήμα 4: Κατανομή βιβλιογραφίας ανά έτος δημοσίευσης

Στο Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε., παρουσιάζεται η κατανομή των 93 πηγών ανά έτος δημοσίευσης. Τα έτη αφορούν το χρονικό διάστημα από το 1995, που εκδόθηκε το Π.Δ. 4/1995 και αφορά την εισαγωγή στις Σχολές της ΕΛ.ΑΣ., μία διαδικασία που αναλύεται στην Ενότητα 6.7, μέχρι το έτος 2025. Δεδομένου ότι η παρούσα μελέτη εστιάζει στην επεξεργασία και προστασία των προσωπικών δεδομένων από την ΕΛ.ΑΣ., και λαμβάνοντας υπόψη ότι ο GDPR και η Οδηγία 2016/680 τέθηκαν σε ισχύ το έτος 2016, η αναζήτηση της βιβλιογραφίας αφορά κυρίως τα έτη από το 2016 και μετά. Όπως είναι αναμενόμενο, οι πηγές που χρησιμοποιήθηκαν στην μελέτη ανασκόπησης και αφορούν τα έτη πριν το 2016 και συγκεκριμένα το χρονικό διάστημα 1995-2014, είναι μόνο 17 (18,2%). Ωστόσο, δεν θα μπορούσε να αποκλειστεί από την παρούσα εργασία αυτό το εύρος ετών, καθόσον,

εκτός του ότι το 1995 θεσπίστηκε το προαναφερόμενο Προεδρικό Διάταγμα, συνέβησαν δύο σημαντικά γεγονότα και συγκεκριμένα εκδόθηκε ο Ν.2472/1997 και το 2001 κατοχυρώθηκε συνταγματικά η προστασία των προσωπικών δεδομένων, ως θεμελιώδες δικαίωμα. Από το 2016 και μετά, παρουσιάζεται ποικιλία στο πλήθος των κειμένων ανά έτος, καθώς κάποια έτη εκδόθηκαν περισσότερα κείμενα, ενώ άλλα λιγότερα. Εκείνα, όμως, που παρουσιάζουν ιδιαίτερο ενδιαφέρον είναι το έτος 2018, όταν δηλαδή τέθηκε σε εφαρμογή ο GDPR, το έτος 2019, όπου εφαρμόστηκε ο Ν. 4624/2019 που έθεσε μέτρα εφαρμογής του GDPR και ενσωμάτωσε την Οδηγία 2016/680 και το 2025, όπου εκδόθηκε ο Ν. 5187/2025 που αφορά τη λειτουργία της Ελληνικής Αστυνομίας, καθώς και άλλα κείμενα, που αφορούν τις δράσεις της. Το γεγονός, ότι το 81,8 % των πηγών, που χρησιμοποιήθηκαν, εκδόθηκαν από το 2016 και μετά, αποδεικνύει τον επίκαιρο χαρακτήρα της εργασίας. Αξιοσημείωτη είναι η αυξητική τάση, που σημειώνεται από το 2021 και έπειτα, η οποία οφείλεται στην ωρίμανση του βασικού εθνικού και ευρωπαϊκού νομικού πλαισίου και στη θέσπιση νέων Προεδρικών Διαταγμάτων, Υπουργικών Αποφάσεων και γενικά νομικών κειμένων, προσαρμοσμένων σε αυτό.

4. Νομικό πλαίσιο για την προστασία των δεδομένων

Στο παρόν κεφάλαιο παρουσιάζεται το ισχύον νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε ευρωπαϊκό και εθνικό επίπεδο. Αρχικά, γίνεται αναφορά στις ευρωπαϊκές συμβάσεις και συνθήκες, στις οποίες βασίζεται η ευρωπαϊκή νομοθεσία και συγκεκριμένα ο Γενικός Κανονισμός Προστασίας Δεδομένων - Κανονισμός 2016/679 (ΕΕ) και η Οδηγία (ΕΕ) 2016/680. Στη συνέχεια, αναλύεται το άρθρο 9^Α του Συντάγματος, με το οποίο κατοχυρώνεται το δικαίωμα στην προστασία των προσωπικών δεδομένων και ο Νόμος 4624/2019, με τον οποίο τίθενται μέτρα εφαρμογής του Κανονισμού 2016/679 (ΕΕ) και ενσωματώνεται η Οδηγία (ΕΕ) 2016/680 στην εθνική νομοθεσία για την προστασία των προσωπικών δεδομένων στην Ελλάδα.

4.1. Ευρωπαϊκές Συμβάσεις και Συνθήκες

Ήδη από το 1950 υιοθετήθηκε η Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, γνωστή ως Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (Ε.Σ.Δ.Α.), με απώτερο σκοπό, όπως προκύπτει και από τον τίτλο της, την προστασία των ανθρωπίνων δικαιωμάτων, μεταξύ των οποίων αυτό του σεβασμού της ιδιωτικής ζωής και της οικογενειακής ζωής (Άρθρο 8) και των θεμελιωδών ελευθεριών. Μάλιστα, με τη Σύμβαση αυτή συγκροτήθηκε το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (Ε.Δ.Δ.Α.), στο οποίο μπορεί να προσφύγει κάθε άτομο του οποίου τα δικαιώματα της Σύμβασης έχουν παραβιαστεί από κράτος που είναι μέλος σε αυτή (Κανέλλος, Λ., 2020: 112-113).

Το δικαίωμα προστασίας των προσωπικών δεδομένων κατοχυρώθηκε και με το άρθρο 16 της Συνθήκης Λειτουργίας της Ευρωπαϊκής Ένωσης⁵, η οποία αναθέτει αρμοδιότητα στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο να θεσπίζουν κανόνες για την προστασία των ατόμων έναντι της επεξεργασίας των προσωπικών τους δεδομένων από θεσμικά και λοιπά όργανα και τους οργανισμούς της Ευρωπαϊκής Ένωσης (Ε.Ε.), αλλά και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων, που εμπίπτουν στο πεδίο εφαρμογής του ενωσιακού δικαίου και σχετικά με την ελεύθερη κυκλοφορία αυτών των δεδομένων. Μάλιστα, με το άρθρο 16 της Σ.Λ.Ε.Ε. η προστασία των προσωπικών δεδομένων κατοχυρώνεται ως ξεχωριστό δικαίωμα από αυτό της ιδιωτικής ζωής, αναδεικνύοντας την σπουδαιότητά του (Ιγγλεζάκης, Ι., 2020: 26).

Ρυθμίσεις σχετικά με την προστασία των προσωπικών δεδομένων αποτυπώνονται και στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ε.Ε. (Χ.Θ.Δ.Ε.Ε.), ο οποίος από το 2009, που τέθηκε σε ισχύ η Συνθήκη της Λισαβόνας, αναγνωρίζεται νομικά ως πρωτογενής πηγή δικαίου και παράγει δεσμεύσεις για τους υπόχρεους. Με το άρθρο 8 του Χ.Θ.Δ.Ε.Ε. ορίζεται η πρότερη συγκατάθεση του υποκειμένου ως προαπαιτούμενο για τη νόμιμη επεξεργασία των προσωπικών του δεδομένων (Κανέλλος, Λ., 2020: 114). Η διατύπωση των παραγράφων 1 και 2 του άρθρου έχει ως εξής: «1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων

⁵ Η Συνθήκη Λειτουργίας της Ευρωπαϊκής Ένωσης τέθηκε σε ισχύ το 2009

προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.».

4.2. Κανονισμός 2016/679 - GDPR

4.2.1. Από την Οδηγία 95/46/EK στον GDPR

Η προστασία των προσωπικών δεδομένων, ήδη από το 1995, είχε προβληματίσει τον Ευρωπαϊκό νομοθέτη, ο οποίος εισήγαγε την Οδηγία 95/46/EK, που είχε ως βασικό στόχο την αποτροπή της κατάχρησης ή περιττής συλλογής προσωπικών δεδομένων πολιτών της Ευρωπαϊκής Ένωσης, διασφαλίζοντας την προστασία των προσωπικών δεδομένων και των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία αυτών των δεδομένων. Παρ' ότι ήταν πρωτοποριακή για την εποχή της, με το πέρασμα των ετών δέχτηκε κριτικές, αναφορικά με περιττές γραφειοκρατικές διαδικασίες που προέβλεπε, τη χρήση αόριστων και ασαφών ορισμών και κανόνων και τη διαφοροποιημένη, ασυνεπή και μη συνεκτική εφαρμογή των κοινοτικών κανόνων, η οποία οφείλονταν είτε στη μη ικανοποιητική ή πλημμελή ενσωμάτωση της Οδηγίας στο εθνικό δίκαιο των κρατών μελών είτε στις διαφορές στην ερμηνεία ή την εφαρμογή της (Μήτρου, Λ., 2017: 21-22). Επιπλέον, η αλματώδης εξάπλωση των διαδικτυακών υπηρεσιών και οι προκλήσεις της σύγχρονης ψηφιακής εποχής απέδειξαν ότι η Οδηγία δεν μπορεί να εφαρμοστεί αποτελεσματικά και έτσι κατέστη αναγκαία η δημιουργία ενός νομικού εργαλείου, που θα εγγυάται την προστασία των προσωπικών δεδομένων (Ryz, L. & Grest, L. 2016).

Σε αυτό το πλαίσιο, και ύστερα από τέσσερα χρόνια εντατικών διαβουλεύσεων (Κανέλλος, Λ., 2020: 1), το 2016 θεσπίστηκε ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) - Κανονισμός 2016/679 (ΕΕ), ο οποίος από το 2018 εφαρμόζεται υποχρεωτικά στον δημόσιο και ιδιωτικό τομέα και συνιστά Κανονισμό της ευρωπαϊκής νομοθεσίας για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο GDPR, αν και διατηρεί τις περισσότερες ρυθμίσεις που ενσωματώνονται στην Οδηγία 95/46/EK, αποτελεί τη σημαντικότερη αλλαγή των τελευταίων ετών, καθώς ανταποκρίνεται στις προκλήσεις που δημιούργησαν η εμφάνιση των μεγάλων δεδομένων (big data), η ολοένα και μεγαλύτερη χρήση των μέσων κοινωνικής δικτύωσης και γενικότερα ο ψηφιακός κόσμος (Ryz, L. & Grest, L. 2016). Επιπλέον, αντιμετωπίζει τις αδυναμίες και τα κενά που υπήρχαν στη νομοθεσία κατά το παρελθόν, επιβάλλοντας αυστηρούς κανόνες και υποχρεώσεις αναφορικά με την προστασία και επεξεργασία των προσωπικών δεδομένων από οργανισμούς και φορείς (Spalevic, Z. & Vicić, K., 2022: 56-57).

Βασική διαφοροποίηση του GDPR από την Οδηγία 95/46/EK αποτελεί το γεγονός ότι ως Κανονισμός εφαρμόζεται άμεσα και καθολικά σε όλα τα κράτη μέλη

και μάλιστα τόσο στους υπεύθυνους και εκτελούντες την επεξεργασία προσωπικών δεδομένων⁶ εντός της Ε.Ε., όσο και σε εκείνους εκτός Ε.Ε., εφόσον τα αγαθά και οι υπηρεσίες, που προσφέρουν αφορούν άτομα της Ευρωπαϊκής Ένωσης. Από το πεδίο εφαρμογής του GDPR εξαιρούνται δραστηριότητες, που αφορούν την εθνική ασφάλεια, την κοινή εξωτερική πολιτική και πολιτική ασφάλειας της Ένωσης, καθώς και εκείνες που εμπίπτουν στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας (Ιγγλεζάκης, Ι., 2018: 31-32). Από την άλλη, η Οδηγία, αν και αποτελεί ενωσιακή πράξη για τα κράτη μέλη, είναι δεσμευτική μόνο ως προς το επιδιωκόμενο αποτέλεσμα (Κανέλλος, Λ., 2020: 2), που σημαίνει ότι κάθε κράτος μέλος πρέπει να θεσπίσει τους δικούς του νόμους αρκεί να εκπληρώνεται ο τελικός σκοπός (Lawspot, 2017), πράγμα που οδηγεί σε ανομοιογενείς εφαρμογές (Ryz, L. & Grest, L. 2016).

4.2.2. Αρχές επεξεργασίας προσωπικών δεδομένων

Ο GDPR βασίζεται σε ένα σύνολο θεμελιωδών αρχών, που καθορίζουν τον τρόπο με τον οποίο οι δημόσιοι και ιδιωτικοί φορείς συλλέγουν και επεξεργάζονται τα προσωπικά δεδομένα. Αν και υιοθέτησε το βασικό σώμα των πέντε αρχών για την προστασία των προσωπικών δεδομένων που όριζε η Οδηγία 95/46/EK στο άρθρο 6, αναγνώρισε μία εξέχουσα θέση στην ασφάλεια των προσωπικών δεδομένων, εντάσσοντας την αρχή της ακεραιότητας και εμπιστευτικότητας (Μήτρου, Λ., 2021: 93), αλλά και στην αρχή της λογοδοσίας του υπεύθυνου επεξεργασίας. Δεδομένου ότι η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα κάθε φυσικού προσώπου, το οποίο κατοχυρώνεται συνταγματικά, όπως προαναφέρθηκε, θα πρέπει να συντρέχουν σωρευτικά και όχι διαζευκτικά (Ιγγλεζάκης, Ι., 2018: 63) οι ακόλουθες επτά βασικές αρχές επεξεργασίας προσωπικών δεδομένων, που ορίζονται στο άρθρο 5 του Κανονισμού:

1. Αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας

Κάθε επεξεργασία προσωπικών δεδομένων θα πρέπει να είναι σύννομη, θεμιτή και να γίνεται με διαφάνεια. Αυτό σημαίνει ότι θα πρέπει να είναι σύμφωνη με τη νομοθεσία, τους νόμους, τα προεδρικά διατάγματα, τις υπουργικές αποφάσεις και συνταγματικές αρχές (Ομάδα εργασίας του άρθρου 29, WP203, 2013: 20) και να

⁶ Σύμφωνα με το άρθρο 4 του GDPR, ως υπεύθυνος επεξεργασίας νοείται το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, που καθορίζει τους σκοπούς και τον τρόπο με τον οποίο πρόκειται να γίνει η επεξεργασία των προσωπικών δεδομένων του ατόμου. Ο σκοπός της επεξεργασίας αφορά, κυρίως, το ειδικό συμφέρον που υπηρετείται με την επεξεργασία, ενώ ο τρόπος επεξεργασίας αναφέρεται στις μορφές επεξεργασίας, π.χ. μέσω διαδικτύου και στα μέσα που χρησιμοποιούνται (π.χ. τεχνικό εξοπλισμό) (Ιγγλεζάκης, Ι., 2020: 65) Κατά το ίδιο άρθρο, ο εκτελών την επεξεργασία είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, το οποίο αν και αποτελεί χωριστή νομική οντότητα σε σχέση με τον υπεύθυνο επεξεργασίας, επεξεργάζεται τα προσωπικά δεδομένα για λογαριασμό του υπευθύνου της επεξεργασίας. Για παράδειγμα, τα πανεπιστημιακά και κρατικά εργαστήρια είναι εκτελούντες επεξεργασίας, μέσω αναλύσεων DNA υπόπτων τέλεσης εγκλημάτων, για λογαριασμό της Διεύθυνσης Εγκληματολογικών Ερευνών της Ελληνικής Αστυνομίας (Κανέλλος, Λ., 2020: 21-25). Εάν ο υπεύθυνος επεξεργασίας αναλάβει να εκτελέσει την επεξεργασία των προσωπικών δεδομένων με δικά του μέσα, τότε δεν υπάρχει εκτελών την επεξεργασία (Ιγγλεζάκης, Ι., 2020: 68).

ικανοποιείται τουλάχιστον μία από τις προϋποθέσεις, που προβλέπονται στο άρθρο 6 του Κανονισμού:

α. το υποκείμενο των δεδομένων έχει συναινέσει για την επεξεργασία των προσωπικών του δεδομένων. Όπως ορίζεται στο άρθρο 4 περ. 11 και στο άρθρο 7 του GDPR, η συγκατάθεση του ατόμου για επεξεργασία των προσωπικών του δεδομένων, θα πρέπει να είναι ρητή, δηλαδή να μην είναι σιωπηρή, τεκμαιρόμενη ή εικαζόμενη, συγκεκριμένη και όχι γενική για όλες τις επεξεργασίες, καθώς κάθε επεξεργασία θα πρέπει να προσδιορίζεται ειδικά, και ελεύθερη, δηλαδή να είναι συνειδητή ενέργεια του υποκειμένου, χωρίς εξαναγκασμό και πίεση ή αίσθηση ότι θα υποστεί αρνητικές συνέπειες εάν δεν συγκατατεθεί (Ιγγλεζάκης, Ι., 2020: 93). Η συγκατάθεση μπορεί να παρέχεται με γραπτή ή προφορική δήλωση, ή και με ηλεκτρονικά μέσα (Ιγγλεζάκης, Ι., 2020: 71). Με άλλα λόγια, το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει επακριβώς σε τι συναινεί.

Σε περίπτωση, όμως, που το υποκείμενο των προσωπικών δεδομένων είναι παιδί, η συγκατάθεση είναι σύννομη εάν το παιδί είναι τουλάχιστον 16 ετών, διαφορετικά αυτή θα πρέπει να παρέχεται από εκείνον που έχει την γονική μέριμνα του παιδιού (Άρθρο 8 του GDPR).

β. η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης, στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα, ύστερα από αίτησή του, σχετικά με την σύναψη της σύμβασης, όπως διαφημιστική ενημέρωση και πώληση προϊόντων ή παροχή υπηρεσιών

γ. η επεξεργασία είναι απαραίτητη για την συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας των δεδομένων, όπως πληρωμή φόρου εισοδήματος και αναγγελία πρόσληψης εργαζομένου στον ΟΑΕΔ

δ. η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή άλλου φυσικού προσώπου, όπως μεταφορά θύματος τροχαίου ατυχήματος σε νοσοκομείο, προστασία δημόσιας υγείας και εκπαίδευση τέκνων

ε. η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος, που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, όπως κοινωνική προστασία ευπαθών κοινωνικών ομάδων και έκδοση αστυνομικού δελτίου ταυτότητας

στ. η επεξεργασία είναι απαραίτητη για τα έννομα συμφέροντα του υπεύθυνου επεξεργασίας ή τρίτου, υπό την προϋπόθεση ότι αυτά δεν υπερκαλύπτονται από τα συμφέροντα, τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα. Η προϋπόθεση αυτή είναι ιδιαίτερα αυστηρή όταν το υποκείμενο των δεδομένων είναι παιδί.⁷

Επιπλέον, τα προσωπικά δεδομένα δεν θα πρέπει να συλλέγονται και να υποβάλλονται σε επεξεργασία με αθέμιτο τρόπο και μέσα και εν αγνοία του

⁷ Η περίπτωση αυτή δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

υποκειμένου. Επομένως, το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει ποιος επεξεργάζεται τα προσωπικά του δεδομένα, ποια δεδομένα έχουν τεθεί υπό επεξεργασία και για ποιο λόγο (Ιγγλεζάκης, Ι., 2020: 78-79).

2. Αρχή του περιορισμού του σκοπού

Η συλλογή των προσωπικών δεδομένων θα πρέπει να γίνεται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν θα πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία για σκοπούς που είναι ασύμβατοι με τους αρχικούς. Σε αυτό το σημείο αξίζει να σημειωθεί ότι τυχόν περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς, ωστόσο θα πρέπει να γίνεται με την προϋπόθεση ότι οι χρησιμοποιούμενες μέθοδοι αποκλείουν την ταυτοποίηση των υποκειμένων των δεδομένων και εξασφαλίζουν την προστασία των προσωπικών τους δεδομένων.

3. Αρχή της ελαχιστοποίησης των δεδομένων (Αρχή της αναλογικότητας)

Σε επεξεργασία υποβάλλονται μόνο τα προσωπικά δεδομένα, που είναι κατάλληλα και συναφή σε σχέση με τον σκοπό για τον οποίο επεξεργάζονται. Η εν λόγω αρχή έχει και ποιοτική και ποσοτική διάσταση. Άλλωστε, κατ' εφαρμογή της αρχής της αναλογικότητας, όπως αυτή ορίζεται στο άρθρο 5 παρ. 4 της Συνθήκης της Ευρωπαϊκής Ένωσης, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να γίνεται με το κατά περίπτωση καταλληλότερο, αναγκαϊότερο, προσφορότερο και λιγότερο επαχθές μέσο, που θα εξυπηρετεί αποτελεσματικότερα τους σκοπούς αυτής, με τη λιγότερη δυνατή προσβολή των εννόμων αγαθών και δικαιωμάτων των υποκειμένων των δεδομένων.

4. Αρχή της ακρίβειας

Τα προσωπικά δεδομένα, που τίθενται σε επεξεργασία θα πρέπει να είναι ακριβή και να επικαιροποιούνται, όταν αυτό είναι απαραίτητο. Σε περίπτωση που τα δεδομένα είναι ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας, ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει κατάλληλα μέτρα, ώστε να διορθώνονται ή να διαγράφονται άμεσα, χωρίς να απαιτείται η υποβολή σχετικού αιτήματος του υποκειμένου αυτών (Ιγγλεζάκης, Ι., 2020: 85).

5. Αρχή της περιόδου αποθήκευσης των δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να διατηρούνται υπό μορφή, που επιτρέπει την ταυτοποίηση του υποκειμένου αυτών και μόνο για το χρονικό διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας τους. Όπως ορίζεται στο άρθρο 39 της Αιτιολογικής Έκθεσης του GDPR, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή ή την περιοδική επανεξέταση των προσωπικών δεδομένων, ώστε να διασφαλίζεται ότι δεν διατηρούνται για περισσότερο χρόνο από όσο απαιτείται. Κατ' εξαίρεση τα δεδομένα μπορούν να αποθηκευτούν για μεγαλύτερα χρονικά διαστήματα, εφόσον υποβάλλονται σε επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής

έρευνας ή στατιστικούς σκοπούς, με την προϋπόθεση ότι εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του ατόμου.

6. Αρχή της ακεραιότητας και της εμπιστευτικότητας

Η επεξεργασία των προσωπικών δεδομένων θα πρέπει να γίνεται με τρόπο τέτοιο, ώστε να εξασφαλίζεται η ασφάλεια αυτών και συγκεκριμένα η προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά τους. Αυτό προϋποθέτει την εφαρμογή κατάλληλων τεχνικών ή οργανωτικών μέτρων από τον υπεύθυνο και εκτελούντα την επεξεργασία σε επίπεδο υποδομών, πληροφοριακών συστημάτων, εφαρμογών και προσωπικού (Κανέλλος, Λ., 2020: 149). Η εμπιστευτικότητα των δεδομένων είναι αδιαπραγμάτευτη και υπερέχει έναντι οποιασδήποτε σκοπιμότητας ή προσδοκώμενου οφέλους⁸.

7. Αρχή της λογοδοσίας

Η έννοια της λογοδοσίας, αν και σχετίζεται με την έννοια της ευθύνης, δεν ταυτίζεται με αυτή, καθώς αποτελούν αλληλοσυμπληρούμενες πτυχές της χρηστής διακυβέρνησης. Το βασικό περιεχόμενο αυτής της αρχής αφορά τόσο τον σχεδιασμό και την εφαρμογή μέτρων και πολιτικών, που διασφαλίζουν την συμμόρφωση με τον Κανονισμό στο σύνολό του, όσο και την υποχρέωση του υπεύθυνου επεξεργασίας των δεδομένων, να μπορεί να αποδείξει, ανά πάσα στιγμή, την συμμόρφωσή του με αυτόν (Μήτρου, Λ., 2017: 93-94). Με την αρχή αυτή μετατίθεται η ευθύνη εφαρμογής του Κανονισμού από την εποπτική αρχή στον υπεύθυνο επεξεργασίας, ο οποίος θα πρέπει να διαθέτει έγγραφα προς απόδειξη των μέτρων, που έχουν ληφθεί για την συμμόρφωση με τους κανόνες προστασίας προσωπικών δεδομένων, σε περίπτωση που το υποκείμενο αυτών ή οι εθνικές αρχές ελέγχου υποβάλουν σχετικό αίτημα (Ιγγλεζάκης, Ι., 2020: 87-88).

4.2.2.1. Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων

Σχετικά με τις ειδικές κατηγορίες προσωπικών δεδομένων που αναφέρθηκαν στην Ενότητα 2.1, λόγω του υψηλού βαθμού ευαισθησίας τους, υποβάλλονται σε πιο έντονη προστασία σε σχέση με τα υπόλοιπα δεδομένα, δηλαδή τα απλά (Χριστοδούλου, Κ., 2020: 34). Έτσι, η επεξεργασία τους επιτρέπεται μόνο σε συγκεκριμένες περιπτώσεις, οι οποίες αποτυπώνονται στο άρθρο 9 του Κανονισμού και είναι οι εξής:

- 1.** Το υποκείμενο των δεδομένων έχει συναινέσει ρητά για την επεξεργασία αυτών. Ωστόσο, ακόμα και εάν έχει δοθεί ρητή συγκατάθεση, εάν το ενωσιακό ή εθνικό δίκαιο προβλέπει ότι η απαγόρευση της επεξεργασίας τους δεν μπορεί να αρθεί από το υποκείμενο αυτών, τότε απαγορεύεται οποιαδήποτε επεξεργασία αυτών,
- 2.** Είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης

⁸ ΕΣΟΕΛ, 2021, «Μέθοδοι ανάλυσης δεδομένων στο πλαίσιο ελεγκτικών αποστολών», σελ. 84

και κοινωνικής προστασίας, εφόσον επιτρέπεται από το ενωσιακό ή εθνικό δίκαιο ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο,

3. Είναι απαραίτητη για την προστασία ζωτικών συμφερόντων του υποκειμένου ή τρίτου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συναινέσει,
4. Διενεργείται νόμιμα από έναν μη κερδοσκοπικό φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό σκοπό, με την προϋπόθεση ότι η επεξεργασία αφορά τα μέλη του ή πρόσωπα που έχουν συχνή επικοινωνία με αυτόν και τα δεδομένα δεν κοινοποιούνται σε τρίτους, χωρίς τη συγκατάθεση των υποκειμένων τους,
5. Τα δεδομένα έχουν δημοσιοποιηθεί προδήλως από το ίδιο το υποκείμενο,
6. Είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων,
7. Είναι απαραίτητη όταν υπάρχει ουσιαστικό δημόσιο συμφέρον σύμφωνα με το ενωσιακό ή εθνικό δίκαιο, το οποίο όμως είναι ανάλογο με τον επιδιωκόμενο στόχο και έχουν ληφθεί κατάλληλα μέτρα διασφάλισης των θεμελιωδών δικαιωμάτων και συμφερόντων του υποκειμένου των δεδομένων,
8. Είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών υπό την ευθύνη του επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου,
9. Είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, το οποίο προβλέπει κατάλληλα μέτρα προστασίας των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, και ειδικότερα του επαγγελματικού απορρήτου. Σε αυτή την περίπτωση συγκαταλέγονται η προστασία από σοβαρές διασυννοριακές απειλές κατά της υγείας, η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμακευτικών-ιατρικών προϊόντων,
10. Είναι απαραίτητη για σκοπούς αρχειοθέτησης, επιστημονικής ή ιατρικής έρευνας ή στατιστικών μελετών, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο και σε κάθε περίπτωση προστατεύονται τα δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων.

Ωστόσο, αν και ο GDPR προβλέπει τις βασικές αρχές, τις απαγορεύσεις και τις εξαιρέσεις σχετικά με την επεξεργασία των προσωπικών δεδομένων, τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν επιπλέον μέτρα σχετικά με την επεξεργασία γενετικών, βιομετρικών ή δεδομένων που αφορούν την υγεία (Άρθρο 9 του GDPR).

Όσον αφορά τα προσωπικά δεδομένα, που αφορούν **ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφαλείας**, η επεξεργασία τους υπόκεινται σε αυστηρούς ελέγχους και διενεργείται μόνο υπό τον έλεγχο δικαστικής αρχής ή μόνο

εάν η επεξεργασία επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, το οποίο προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (Άρθρο 10 του GDPR).

4.2.3. Δικαιώματα υποκειμένου δεδομένων

Ο GDPR έφερε σημαντικές αλλαγές και στα δικαιώματα του υποκειμένου των δεδομένων, καθώς όχι μόνο διατήρησε, αλλά και ενίσχυσε τα βασικά δικαιώματα, που είχαν κατοχυρωθεί με την Οδηγία 95/46/EK, προσθέτοντας παράλληλα το δικαίωμα στη φορητότητα και το δικαίωμα στη λήθη.

Πιο συγκεκριμένα, τα δικαιώματα που εξασφαλίζει ο GDPR στο υποκείμενο των δεδομένων είναι τα εξής:

1. Δικαίωμα διαφάνειας (άρθρο 12)

Με το άρθρο 12 του GDPR προβλέπεται η υποχρέωση του υπεύθυνου επεξεργασίας των δεδομένων να λαμβάνει τα κατάλληλα μέτρα, για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία, που αναφέρεται στις διατάξεις του δικαιώματος ενημέρωσης, αλλά και κάθε ανακοίνωση σχετικά με την ικανοποίηση των δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής των δεδομένων, περιορισμού της επεξεργασίας και εναντίωσης σε αυτή, αλλά και να ανακοινώνει σε αυτό τυχόν παραβίαση των προσωπικών του δεδομένων. Οι πληροφορίες αυτές θα πρέπει να παρέχονται σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, με απλή και σαφή διατύπωση, ειδικά όταν η πληροφορία απευθύνεται σε παιδιά. Σκοπός της εν λόγω διάταξης είναι η συναίνεση του υποκειμένου για επεξεργασία των προσωπικών του δεδομένων, να είναι αποτέλεσμα διαφανούς και πλήρους ενημέρωσης (Ιγγλεζάκης, Ι., 2020: 148).

2. Δικαίωμα ενημέρωσης (άρθρο 13 και 14)

Ανεξαρτήτως εάν τα προσωπικά δεδομένα έχουν συλλεχθεί από το υποκείμενο αυτών ή όχι, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να γνωρίσει στο υποκείμενο των δεδομένων:

- την ταυτότητα και τα στοιχεία επικοινωνίας αυτού και του εκπροσώπου του υπευθύνου επεξεργασίας, εάν υφίσταται,
- τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, κατά περίπτωση,
- τους σκοπούς επεξεργασίας και τη νομική βάση, στην οποία στηρίζεται η επεξεργασία,
- τους αποδέκτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων, εάν υπάρχουν,
- την τυχόν διαβίβαση των δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή διεθνή οργανισμό,

- και την ύπαρξη ή την απουσία απόφασης επάρκειας της Επιτροπής.⁹

Εκτός όμως από τα ανωτέρω, ο υπεύθυνος της επεξεργασίας, προκειμένου να εξασφαλίσει τη θεμιτή και διαφανή επεξεργασία των προσωπικών δεδομένων, παρέχει στο υποκείμενο επιπλέον πληροφορίες και συγκεκριμένα:

- το χρονικό διάστημα αποθήκευσης των δεδομένων, ή, όταν αυτό είναι αδύνατο να προσδιοριστεί, τα κριτήρια που το καθορίζουν,
- τη δυνατότητα υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση, διόρθωση ή διαγραφή των προσωπικών δεδομένων ή περιορισμό της επεξεργασίας αυτών ή εναντίωση στην επεξεργασία, καθώς και για φορητότητα των δεδομένων,
- όταν το υποκείμενο έχει συναινέσει για την επεξεργασία των δεδομένων του για συγκεκριμένο σκοπό, την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,
- το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,
- κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών και
- την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Σε περίπτωση που ο υπεύθυνος επεξεργασίας πρόκειται να επεξεργαστεί περαιτέρω τα προσωπικά δεδομένα, για σκοπό διαφορετικό από τον αρχικό, πριν από την εν λόγω περαιτέρω επεξεργασία, πρέπει να ενημερώσει το υποκείμενο των δεδομένων για τον σκοπό αυτόν και να παράσχει άλλες τυχόν αναγκαίες πληροφορίες, όπως αυτές αναφέρθηκαν στην προηγούμενη παράγραφο.

Εφόσον τα δεδομένα έχουν συλλεγεί από κάποιον τρίτο, το υποκείμενο αυτών θα πρέπει να ενημερωθεί για την πηγή από την οποία αυτά συλλέχθηκαν και πάντως να ενημερώνεται για όλα τα ανωτέρω εντός εύλογης προθεσμίας από τη συλλογή των δεδομένων του, η οποία δεν θα υπερβαίνει τον ένα μήνα.

⁹ Όταν πρόκειται για τις διαβιβάσεις που αναφέρονται στο άρθρο 46 ή 47 ή στο άρθρο 49 παράγραφος 1 δεύτερο εδάφιο, απαιτείται αναφορά στις ενδεδειγμένες ή κατάλληλες εγγυήσεις και τα μέσα για να αποκτηθεί αντίγραφο τους ή στο πού διατέθηκαν

Σε κάθε περίπτωση η ενημέρωση του υποκειμένου θα πρέπει να γίνεται σε απλή και κατανοητή γλώσσα και χωρίς αοριστίες και ακατάληπτους, στο ευρύ κοινό, νομικούς ή τεχνικούς όρους (Κανέλλος, Λ., 2020: 151).

3. Δικαίωμα πρόσβασης (άρθρο 15)

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται από τον υπεύθυνο της επεξεργασίας αναφορικά με το κατά πόσο τα προσωπικά του δεδομένα υπόκεινται ή όχι σε επεξεργασία και σε θετική περίπτωση, έχει το δικαίωμα πρόσβασης σε αυτά και σε πληροφορίες αναφορικά με:

- τους σκοπούς της επεξεργασίας,
- τις κατηγορίες των προσωπικών δεδομένων,
- τους αποδέκτες ή τις κατηγορίες αυτών, ιδίως όταν πρόκειται για αποδέκτες τρίτων χωρών ή διεθνείς οργανισμούς,
- το χρονικό διάστημα αποθήκευσης ή, όταν αυτό είναι αδύνατο να προσδιοριστεί, τα κριτήρια που το καθορίζουν,
- τη δυνατότητα να αιτηθεί στον υπεύθυνο επεξεργασίας τη διόρθωση ή διαγραφή των προσωπικών του δεδομένων ή τον περιορισμό της επεξεργασίας τους ή να ασκήσει το δικαίωμα αντίταξης στην εν λόγω επεξεργασία,
- το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,
- την προέλευση των δεδομένων, όταν αυτά συλλέγονται από τρίτο,
- την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων,
- και την τυχόν διαβίβαση σε τρίτη χώρα ή σε διεθνή οργανισμό.

Επιπλέον, το υποκείμενο των δεδομένων έχει δικαίωμα να αποκτήσει αντίγραφο των προσωπικών του δεδομένων, που υποβάλλονται σε επεξεργασία.

4. Δικαίωμα διόρθωσης (άρθρο 16)

Το άρθρο 16 του GDPR ορίζει ότι το υποκείμενο των δεδομένων έχει δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας να διορθώσει τα δεδομένα, που το αφορούν και είναι ανακριβή, χωρίς αδικαιολόγητη καθυστέρηση¹⁰. Επιπλέον, έχει το δικαίωμα να ζητήσει την συμπλήρωση ελλειπόντων δεδομένων προσωπικού χαρακτήρα¹¹. Η διόρθωση θα πρέπει να πραγματοποιηθεί το αργότερο εντός ενός μήνα από το αίτημα του υποκειμένου, ενώ το χρονικό διάστημα μπορεί να παραταθεί κατά δύο μήνες. Ο

¹⁰ Π.χ. εμφανίζεται ως έγγαμος, ενώ είναι διαζευγμένος

¹¹ Π.χ. τηλέφωνα και στοιχεία επικοινωνίας

υπεύθυνος επεξεργασίας είναι υποχρεωμένος να ενημερώνει άμεσα το υποκείμενο αναφορικά με τη διόρθωση των δεδομένων ή τους λόγους για τους οποίους δεν προτίθεται να συμμορφωθεί προς το αίτημά του (Ιγγλεζάκης, Ι., 2020: 156).

5. Δικαίωμα διαγραφής – «Δικαίωμα στη λήθη» (άρθρο 17)

Ο GDPR παρέχει στους πολίτες το δικαίωμα να ζητήσουν από τον υπεύθυνο επεξεργασίας την διαγραφή των προσωπικών τους δεδομένων, χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται, με τη σειρά του, να τα διαγράψει άμεσα. Έτσι, όταν το φυσικό πρόσωπο δεν θέλει να υποβληθούν σε περαιτέρω επεξεργασία τα δεδομένα του και δεν υπάρχει νόμιμος λόγος διατήρησής τους, αυτά πρέπει να διαγράφονται άμεσα. Το δικαίωμα αυτό ονομάζεται «δικαίωμα στη λήθη» και αποτυπώνεται στο άρθρο 17 του GDPR.

Ωστόσο, το εν λόγω δικαίωμα κάμπτεται όταν υπάρχει υπέρτερος νόμιμος λόγος διατήρησης των δεδομένων και συγκεκριμένα, όταν η επεξεργασία είναι απαραίτητη:

- για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση,
- για την τήρηση νομικής υποχρέωσης, που επιβάλλει την επεξεργασία βάσει του ενωσιακού ή εθνικού δικαίου του κράτους μέλους, στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας,
- για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας,
- για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1¹², εφόσον το δικαίωμα διαγραφής μπορεί να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη των σκοπών της εν λόγω επεξεργασίας
- και για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Η βασική καινοτομία, που εισάγει το δικαίωμα στη λήθη αφορά την προσπάθεια αντιμετώπισης του φαινομένου της ψηφιακής διάχυσης και αναπαραγωγής ενός περιεχομένου σε περισσότερους ιστότοπους. Αυτό σημαίνει ότι εάν το υποκείμενο υποβάλει αίτημα διαγραφής, ο υπεύθυνος επεξεργασίας, που δημοσιοποίησε τα προσωπικά δεδομένα οφείλει να ενημερώσει τους υπόλοιπους υπεύθυνους

¹² Σύμφωνα με το άρθρο 89 παρ. 1 του GDPR: «Η επεξεργασία για σκοπούς αρχειοθέτησης για το δημόσιο συμφέρον ή για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς υπόκειται σε κατάλληλες εγγυήσεις, σύμφωνα με τον παρόντα κανονισμό, ως προς τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, σύμφωνα με τον παρόντα κανονισμό. Οι εν λόγω εγγυήσεις διασφαλίζουν ότι έχουν θεσπιστεί τα τεχνικά και οργανωτικά μέτρα, ιδίως για να διασφαλίζουν την τήρηση της αρχής της ελαχιστοποίησης των δεδομένων. Τα εν λόγω μέτρα μπορούν να περιλαμβάνουν τη χρήση ψευδωνύμων, εφόσον οι εν λόγω σκοποί μπορούν να εκπληρωθούν κατ' αυτόν τον τρόπο. Εφόσον οι εν λόγω σκοποί μπορούν να εκπληρωθούν από περαιτέρω επεξεργασία η οποία δεν επιτρέπει ή δεν επιτρέπει πλέον την ταυτοποίηση των υποκειμένων των δεδομένων, οι εν λόγω σκοποί εκπληρώνονται κατ' αυτόν τον τρόπο.»

επεξεργασίας, που τα επεξεργάζονται, ώστε να διαγράψουν τυχόν συνδέσμους, αντίγραφα ή να διακόψουν οποιαδήποτε αναπαραγωγή αυτών (Μήτρου, Λ., 2017: 135).

6. Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18)

Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητήσει τον περιορισμό της επεξεργασίας αυτών από τον υπεύθυνο επεξεργασίας, όταν:

- αμφισβητεί την ακρίβεια αυτών,
- η επεξεργασία τους δεν προβλέπεται και αντί για διαγραφή των δεδομένων ζητάει τον περιορισμό στη χρήση τους,
- ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, και
- έχει αντιρρήσεις για την επεξεργασία τους και αναμένει την επαλήθευση του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερисχύουν έναντι των λόγων του.

Όταν το υποκείμενο ασκεί το εν λόγω δικαίωμα, τα δεδομένα του εκτός της αποθήκευσης, υπόκεινται σε επεξεργασία μόνο με τη συγκατάθεσή του ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή για λόγους σημαντικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους.

Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων που έχει εξασφαλίσει τον περιορισμό της επεξεργασίας, πριν την άρση αυτού.

7. Δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20)

Με τον GDPR το φυσικό πρόσωπο εκτός από το δικαίωμα πρόσβασης στα προσωπικά του δεδομένα, τα οποία έχει παράσχει στον υπεύθυνο επεξεργασίας σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, έχει δικαίωμα να διαβιβάζει ελεύθερα τα προσωπικά του δεδομένα από έναν υπεύθυνο επεξεργασίας σε έναν άλλο, χωρίς αντίρρηση του πρώτου, όταν η επεξεργασία βασίζεται σε συγκατάθεση¹³ ή σύμβαση¹⁴ και όταν διενεργείται με αυτοματοποιημένα μέσα¹⁵. Συνεπώς, θα πρέπει να συντρέχουν και οι δύο προϋποθέσεις για να μπορέσει το υποκείμενο των δεδομένων να ασκήσει το εν λόγω δικαίωμα. Το υποκείμενο των δεδομένων μπορεί να ζητήσει την απευθείας διαβίβαση των προσωπικών του δεδομένων από έναν υπεύθυνο επεξεργασίας σε έναν άλλο, όταν αυτό είναι τεχνικά εφικτό. Η εφαρμογή του συγκεκριμένου δικαιώματος περιορίζεται στα προσωπικά

¹³ Σύμφωνα με το άρθρο 6 παρ. 1 περ. α' ή το άρθρο 9 παρ. 2 περ. α' του GDPR

¹⁴ Σύμφωνα με το άρθρο 6 παρ. 1 περ. β' του GDPR

¹⁵ Π.χ. ένας συνδρομητής της εταιρείας Cosmote να ζητήσει τη μεταφορά των προσωπικών του δεδομένων στη Vodafone

δεδομένα που έχει παράσχει το ίδιο το υποκείμενο και όχι σε αυτά που παράγονται από τον εκάστοτε πάροχο για το υποκείμενο (Μήτρου, Λ., 2017: 137).

Ωστόσο, το δικαίωμα στη φορητότητα ασκείται με την επιφύλαξη του δικαιώματος στη λήθη, που προαναφέρθηκε, και δεν ισχύει για την επεξεργασία, που είναι απαραίτητη για την εκπλήρωση καθήκοντος, που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

8. Δικαίωμα εναντίωσης (άρθρο 21)

Το υποκείμενο των δεδομένων μπορεί να εναντιωθεί ανά πάσα στιγμή και για λόγους σχετικούς με την ιδιαίτερη κατάστασή του, στην επεξεργασία των προσωπικών του δεδομένων. Σε περίπτωση άσκησης του δικαιώματος εναντίωσης, ο υπεύθυνος επεξεργασίας παύει την επεξεργασία των δεδομένων, εκτός εάν καταδεικνύει επιτακτικούς και νόμιμους λόγους για την επεξεργασία, οι οποίοι υπερσχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή είναι αναγκαίοι για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. Όταν η επεξεργασία πραγματοποιείται για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικές μελέτες, το υποκείμενο διατηρεί το δικαίωμα εναντίωσης, εκτός εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος δημοσίου συμφέροντος.

9. Δικαίωμα μη υποβολής σε αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ (άρθρο 22)

Το άρθρο 22 του Κανονισμού ορίζει ότι το υποκείμενο των δεδομένων δικαιούται να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας των δεδομένων του, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζουν σημαντικά, όπως για παράδειγμα η αυτόματη απόρριψη λήψης τραπεζικού δανείου (Άρθρο 71 της Αιτιολογικής Έκθεσης του GDPR). Όπως προκύπτει από το άρθρο 4 του GDPR, η κατάρτιση προφίλ¹⁶ πρέπει να είναι μία αυτοματοποιημένη μορφή επεξεργασίας δεδομένων προσωπικού χαρακτήρα και να έχει ως στόχο την αξιολόγηση πτυχών ενός φυσικού προσώπου (Ομάδα εργασίας του άρθρου 29, WP251, 2018: 7).

Ωστόσο υπάρχουν ορισμένες περιπτώσεις, στις οποίες το εν λόγω δικαίωμα δεν υφίσταται και συγκεκριμένα όταν η αυτοματοποιημένη λήψη αποφάσεων:

- είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης, στην οποία συμμετέχει το υποκείμενο και ο υπεύθυνος επεξεργασίας,
- προβλέπεται από το ενωσιακό ή εθνικό δίκαιο του κράτους μέλους, στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και λαμβάνονται κατάλληλα μέτρα για

¹⁶ Η διαδικασία της κατάρτισης προφίλ περιλαμβάνει στατιστικές αναλύσεις για την πρόβλεψη σχετικά με φυσικά πρόσωπα και περιλαμβάνει κάποια μορφή αξιολόγησης ή κρίσης σχετικά με ένα πρόσωπο. Για παράδειγμα, η ταξινόμηση των ατόμων βάσει κοινών χαρακτηριστικών, όπως η ηλικία και το φύλο, για τη δημιουργία μίας συγκεντρωτικής γενικής εικόνας των πελατών μίας επιχείρησης. (Ιγγλεζάκης, Ι., 2020: 177-178)

την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, ή

- βασίζεται στη ρητή συγκατάθεση του υποκειμένου.

Στην πρώτη και στην τρίτη περίπτωση, ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει κατάλληλα μέτρα προστασίας των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, εξασφαλίζοντας κατ' ελάχιστο το δικαίωμα ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, το δικαίωμα έκφρασης άποψης και το δικαίωμα αμφισβήτησης της απόφασης.

10. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (άρθρο 77)

Ο GDPR, με την επιφύλαξη τυχόν έτερων διοικητικών ή δικαστικών προσφυγών, παρέχει στο υποκείμενο των δεδομένων το δικαίωμα να υποβάλει καταγγελία σε εποπτική αρχή, εάν θεωρεί ότι η επεξεργασία των δεδομένων του παραβιάζει τις διατάξεις του Κανονισμού. Σε περίπτωση υποβολής καταγγελίας, η εποπτική αρχή ενημερώνει τον καταγγέλλοντα για την έκβαση αυτής, καθώς και για τη δυνατότητα άσκησης δικαστικής προσφυγής.

Ωστόσο, ο υπεύθυνος ή ο εκτελών την επεξεργασία δύναται να περιορίσουν στα υποκείμενα των δεδομένων την άσκηση των δικαιωμάτων τους, που προβλέπονται στα άρθρα 12 έως 22, εφόσον κάτι τέτοιο προβλέπεται από το ενωσιακό ή εθνικό δίκαιο του κράτους μέλους, στο οποίο υπόκεινται οι πρώτοι, για λόγους εθνικής και δημόσιας ασφάλειας, εθνικής άμυνας, πρόληψης, διερεύνησης ή δίωξης εγκλημάτων, σημαντικών οικονομικών και κοινωνικών συμφερόντων, προστασίας της δικαιοσύνης και των δικαιωμάτων τρίτων ατόμων, ελέγχου παραβάσεων σε νομοθετικά κατοχυρωμένα επαγγέλματα, καθώς και για λόγους εκτέλεσης αστικών αξιώσεων (Άρθρο 23 του GDPR).

Εκ των προαναφερθέντων, γίνεται σαφές ότι ο GDPR δεν είναι απλώς ένα νομικό κείμενο, αλλά αποτελεί τον πυρήνα της προστασίας των προσωπικών δεδομένων σε ευρωπαϊκό επίπεδο, επιβάλλοντας υπευθυνότητα και διαφάνεια στους εμπλεκόμενους φορείς και οργανισμούς. Θέτει σαφείς κανόνες και προϋποθέσεις, που πρέπει να τηρούνται κατά την επεξεργασία των δεδομένων, διακρίνει τους ρόλους και τις υποχρεώσεις των φορέων και οργανισμών και κατοχυρώνει τα δικαιώματα των πολιτών, ενώ η παραβίαση των διατάξεών του επισύρει διοικητικές κυρώσεις, όπως αυτές ορίζονται στο άρθρο 83 του GDPR («Η Καθημερινή», 2018). Με την εφαρμογή του εν λόγω Κανονισμού, ενδυναμώνονται τα δικαιώματα των πολιτών της Ευρωπαϊκής Ένωσης, οι τελευταίοι αποκτούν ενεργό ρόλο και μεγαλύτερο έλεγχο στα προσωπικά τους δεδομένα και ενισχύεται το δικαίωμα προστασίας αυτών των δεδομένων (Spalevic, Z. & Vicić, K., 2022: 62).

4.3. Οδηγία (ΕΕ) 2016/680

Το 2016 εκτός από τον GDPR τέθηκε σε ισχύ και η Οδηγία (ΕΕ) 2016/680, με την οποία καταργήθηκε η Απόφαση πλαίσιο 977/2008/ΔΕΥ του Συμβουλίου. Η εν

λόγω Απόφαση, αν και διασφάλιζε υψηλό επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων, έναντι της επεξεργασίας των προσωπικών τους δεδομένων, στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις (Άρθρο 1 της Απόφασης πλαισίου), είχε περιορισμένο πεδίο εφαρμογής, καθώς οι διατάξεις της εφαρμόζονταν σε διασυννοριακές περιπτώσεις και όχι σε δραστηριότητες επεξεργασίας δεδομένων από την αστυνομία και τις αρμόδιες αρχές σε καθαρά εθνικό επίπεδο. Μάλιστα, δεν ήταν πάντα εύκολο για τις αρχές να διακρίνουν μεταξύ καθαρά εθνικής και διασυννοριακής επεξεργασίας ή να προβλέψουν αν ορισμένα προσωπικά δεδομένα θα αποτελούσαν σε μεταγενέστερο στάδιο αντικείμενο διασυννοριακής ανταλλαγής. Επιπλέον, η Απόφαση πλαίσιο δεν περιλάμβανε κάποιον μηχανισμό ή συμβουλευτικό όργανο, όπως η Ομάδα Εργασίας του άρθρου 29¹⁷, ώστε να εξασφαλίζεται κοινή ερμηνεία των διατάξεων της από τα κράτη μέλη και έτσι άφηνε μεγάλο περιθώριο διακριτικής ευχέρειας στους εθνικούς νόμους των κρατών μελών για την εφαρμογή τους (European Commission, 2012: 2).

Σε αυτό το πλαίσιο, θεσπίστηκε η Οδηγία 2016/680 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, μεταξύ αρμοδίων αρχών εντός της Ένωσης, προκειμένου να καλύψει τα κενά που είχαν δημιουργηθεί στη νομοθεσία με την Απόφαση πλαίσιο (Εγχειρίδιο, 2018: 38). Η εν λόγω Οδηγία, γνωστή και ως «Αστυνομική Οδηγία», επιτρέπει στις αρμόδιες αρχές να συλλέγουν και να ανταλλάσσουν πληροφορίες, που είναι απαραίτητες στο πλαίσιο ερευνών και διώξεων (Lawspot, 2018). Το πεδίο εφαρμογής της εκτείνεται σε εγχώριο επίπεδο, χωρίς να περιορίζεται στις ανταλλαγές δεδομένων μεταξύ των κρατών μελών, όπως συνέβαινε με την Απόφαση πλαίσιο 977/2008/ΔΕΥ του Συμβουλίου (Εγχειρίδιο, 2018: 39). Απώτερος σκοπός της Οδηγίας 2016/680 είναι να διασφαλίσει την προστασία των προσωπικών δεδομένων των ατόμων, που χρησιμοποιούνται από τις αρχές επιβολής του νόμου και συγκεκριμένα των θυμάτων, των μαρτύρων και των κατηγορουμένων/υπόπτων τέλεσης αξιόποινων πράξεων, διευκολύνοντας, παράλληλα, τη διασυννοριακή συνεργασία των αρχών στον αγώνα κατά του εγκλήματος και της τρομοκρατίας (Κανέλλος, Λ., 2020:126).

Ως αρμόδια αρχή ορίζεται στο άρθρο 3 της Οδηγίας κάθε δημόσια αρχή, στις αρμοδιότητες της οποίας, εμπίπτει η πρόληψη, η διερεύνηση, η ανίχνευση ή η δίωξη ποινικών αδικημάτων ή η εκτέλεση ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους, καθώς και κάθε άλλος δημόσιος ή ιδιωτικός, οργανισμός ή φορέας, στον οποίο το δίκαιο κράτους μέλους αναθέτει ρόλο δημόσιας αρχής και την εκτέλεση δημόσιων εξουσιών για τους ανωτέρω σκοπούς. Επομένως, αρμόδιες αρχές θεωρούνται, μεταξύ άλλων, οι

¹⁷ Η Ομάδα Εργασίας του άρθρου 29 συστάθηκε δυνάμει του άρθρου 29 της Οδηγίας 95/46/ΕΚ και αποτελούσε ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής. Με την έναρξη εφαρμογής του GDPR αντικαταστάθηκε από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ).

αστυνομικές, εισαγγελικές και δικαστικές αρχές (Κανέλλος, Λ., 2020: 123), οι οποίες συλλέγουν μεγάλο όγκο προσωπικών δεδομένων στο πλαίσιο άσκησης των καθηκόντων τους, όπως για παράδειγμα από τις δικογραφίες, στην προανάκριση, στην κύρια ανάκριση και γενικά κατά τον χειρισμό υποθέσεων (Κανέλλος, Λ., 2020:126).

Αν και η Οδηγία παρουσιάζει ομοιότητες με τον GDPR, υπάρχουν αρκετές διαφοροποιήσεις μεταξύ τους, οι οποίες είναι εύλογες, καθώς οι διατάξεις της είναι προσαρμοσμένες στις ειδικές ανάγκες των διωκτικών αρχών για την αποτελεσματική δίωξη των εγκλημάτων και την απονομή της ποινικής δικαιοσύνης (Κανέλλος, Λ., 2020: 278). Παρά τις διαφοροποιήσεις και τους περιορισμούς επιδιώκει να επιτύχει μία ισορροπία μεταξύ της προστασίας των προσωπικών δεδομένων και των συμφερόντων των αρμόδιων αρχών από την επεξεργασία αυτών, η οποία εξαρτάται από τα εθνικά νομοθετικά μέτρα των κρατών μελών (Maesa, C. 2016). Εφαρμόζεται συμπληρωματικά με τον GDPR, ωστόσο δεν βασίζεται στην συγκατάθεση των υποκειμένων, αλλά στην αναγκαιότητα για λόγους δημόσιας ασφάλειας και δικαιοσύνης, που σημαίνει ότι οι πολίτες δεν ασκούν πραγματικά έλεγχο στα προσωπικά τους δεδομένα (Leiser, M. & Custers, B., 2019: 375). Όταν τα κράτη μέλη αναθέτουν καθήκοντα στις αρμόδιες αρχές, για άλλους σκοπούς από αυτούς, που προβλέπονται στην Οδηγία αυτή, τότε η επεξεργασία των δεδομένων προσωπικού χαρακτήρα εμπίπτει στο πεδίο εφαρμογής του GDPR (Ιγγλεζάκης, Ι., 2020: 41).

Όπως προαναφέρθηκε για την Οδηγία 95/46/EK, έτσι και για την Οδηγία 2016/680 είναι απαραίτητη η ενσωμάτωσή της στο εθνικό δίκαιο του εκάστοτε κράτους μέλους. Στην περίπτωση της χώρας μας, η Οδηγία 2016/680 έχει ενσωματωθεί στον Ν. 4624/2019, και συγκεκριμένα στο κεφάλαιο IV στα άρθρα 43-82. Ανάλυση των σχετικών διατάξεων γίνεται στην Ενότητα 4.5 του τρέχοντος κεφαλαίου της παρούσας εργασίας.

4.4. Άρθρο 9Α του Συντάγματος

Ορισμένα δικαιώματα, λόγω της βαρύνουσας σημασίας τους για τα πρόσωπα, αλλά και την έννομη τάξη εν γένει, είναι αποτυπωμένα στο Σύνταγμα της Ελλάδας, αποκαλούνται συνταγματικά ή θεμελιώδη (Σπυρόπουλος, Φ., 2012: 5) και δεσμεύουν και τις τρεις εξουσίες – νομοθετική, εκτελεστική και δικαστική (Ράικος, Α., 2011: 39).

Όπως αναφέρθηκε και προηγουμένως, η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα κάθε ανθρώπου και κατοχυρώνεται από το άρθρο 9^Α του Συντάγματος, το οποίο προστέθηκε με την Αναθεώρηση του 2001. Συγκεκριμένα, σύμφωνα με το άρθρο αυτό: *«Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.»*

Η συνταγματική κατοχύρωση του εν λόγω δικαιώματος υποδηλώνει την αναγνώριση των κινδύνων, που προκαλεί η εξέλιξη της τεχνολογίας και αναδεικνύει την σπουδαιότητα της προστασίας των προσωπικών δεδομένων κάθε φυσικού προσώπου (Σπυρόπουλος, Φ., 2012: 12). Πρόκειται για ένα αμυντικό δικαίωμα, καθώς

εγγυάται στο άτομο μία σφαίρα ελεύθερης δράσης και ένα όριο, το οποίο δεν μπορεί να υπερβεί η κρατική εξουσία. Λειτουργεί, δηλαδή, ως ασπίδα του ατόμου προς την κρατική παρέμβαση (Ράικος, Α., 2011: 41).

4.5. N. 4624/2019

Στην ελληνική έννομη τάξη επί σειρά ετών και προς απόδειξη προσαρμογής της Ελλάδας στην Οδηγία 95/45/EK είχε τεθεί σε εφαρμογή ο Ν. 2472/1997 περί προστασίας προσωπικών δεδομένων (Χριστοδούλου, Κ., 2020:2). Ωστόσο, λόγω των ραγδαίων τεχνολογικών εξελίξεων και των αλλαγών, που επήλθαν στο ευρωπαϊκό νομοθετικό πλαίσιο αναφορικά με την προστασία των προσωπικών δεδομένων έναντι της επεξεργασίας τους, κρίθηκε απαραίτητη η θέσπιση ενός νέου Νόμου που θα ανταποκρίνεται αποτελεσματικότερα στα δεδομένα της εποχής. Η χώρα μας, ως κράτος μέλος της Ευρωπαϊκής Ένωσης, συμμορφώθηκε άμεσα με τις διατάξεις του GDPR και ψήφισε τον Ν. 4624/2019, καταργώντας τον προϋσχύσαντα Ν. 2472/1997, πλην ορισμένων διατάξεών του.

Πρόκειται για έναν Νόμο για την προστασία προσωπικών δεδομένων, ο οποίος εκφράζει τη βούληση του Έλληνα νομοθέτη στα πεδία εκείνα που ο GDPR παρέχει κάποιες «ρήτρες ευελιξίας», δηλαδή περιθώρια εθνικής ρύθμισης (Παναγοπούλου, Φ., 2019) και ενσωματώνει την Οδηγία 2016/680, καθορίζοντας τις ειδικές διατάξεις που εφαρμόζονται μεταξύ πολιτών και διωκτικών αρχών, όταν οι ενέργειες των τελευταίων εντάσσονται στο πλαίσιο διερεύνησης εγκλημάτων και επιβολής του νόμου (Κανέλλος, Α., 2020: 221). Παράλληλα αντικαθιστά το νομοθετικό πλαίσιο, που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, προκειμένου ο τρόπος δράσης της να είναι σύμφωνος με τον GDPR (Άρθρο 1 του Ν. 4624/2019).

4.5.1. Πεδίο εφαρμογής

Όπως ορίζει το άρθρο 2 του Νόμου, οι γενικές διατάξεις του εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, καθώς και στη μη αυτοματοποιημένη επεξεργασία αυτών, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης από δημόσιους ή ιδιωτικούς φορείς, με εξαίρεση την περίπτωση, που η επεξεργασία πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας. Η έννοια των δημόσιων φορέων αφορά μόνο ελληνικές δημόσιες αρχές και δημόσιους φορείς (Ιγγλεζάκης, Ι., 2020: 43).

Σύμφωνα με το άρθρο 3 του ίδιου Νόμου, οι διατάξεις του εφαρμόζονται στους δημόσιους φορείς, ενώ στους ιδιωτικούς υπό προϋποθέσεις και συγκεκριμένα εφόσον:

- ο υπεύθυνος ή εκτελών την επεξεργασία επεξεργάζεται προσωπικά δεδομένα εντός της Ελληνικής Επικράτειας,
- η επεξεργασία των προσωπικών δεδομένων γίνεται στο πλαίσιο των δραστηριοτήτων μίας εγκατάστασης του υπεύθυνου ή εκτελούντος την επεξεργασία εντός της Ελληνικής Επικράτειας, ή

- παρ' ότι ο υπεύθυνος ή εκτελών την επεξεργασία δεν διαθέτει εγκατάσταση σε κράτος μέλος της Ε.Ε. ή σε άλλο συμβαλλόμενο κράτος του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ.), εντάσσεται στο πεδίο εφαρμογής του GDPR.

Συνεπώς, το εδαφικό πεδίο εφαρμογής του Ν. 4624/2019 ταυτίζεται με αυτό του GDPR (Ιγγλεζάκης, Ι., 2020: 43).

Ο Ν. 4624/2019 έχει θεσπίσει ορισμένα συμπληρωματικά μέτρα εφαρμογής του GDPR στο κεφάλαιο ΙΙΙ, ωστόσο ιδιαίτερο ενδιαφέρον παρουσιάζει το κεφάλαιο ΙV, με το οποίο, όπως προαναφέρθηκε, ενσωματώνεται η Οδηγία 2016/680 στην εθνική νομοθεσία και συγκεκριμένα στα άρθρα 43-82. Τα εν λόγω άρθρα ρυθμίζουν την επεξεργασία των προσωπικών δεδομένων στο πλαίσιο δράσεων της Ελληνικής Αστυνομίας και γενικότερα των αρμόδιων αρχών, για τους σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους, οι οποίες ενδέχεται να οδηγήσουν σε ποινικά αδικήματα, όπως για παράδειγμα οι διαδηλώσεις και τα αθλητικά γεγονότα (Τζέλλης, Δ. & Μυλώση, Μ., 2022: 35)¹⁸. Στο άρθρο 44 αποτυπώνεται ο ορισμός της αρμόδιας αρχής, όπως αυτή ορίστηκε στο άρθρο 3 της Οδηγίας 2016/680. Έτσι, ως αρμόδιες αρχές, ορίζονται οι αστυνομικές, εισαγγελικές και δικαστικές αρχές και συγκεκριμένα οι αστυνομικοί και οι προανακριτικοί υπάλληλοι, οι φυλακές, το Λιμενικό Σώμα, η Ελληνική Ακτοφυλακή, το Πυροσβεστικό Σώμα Ελλάδας, οι εισαγγελείς, οι ποινικοί δικαστές, συμπεριλαμβανομένων των ανακριτών και πταισματοδικών, καθώς και τα ποινικά δικαστήρια (Τζέλλης, Δ. & Μυλώση, Μ., 2022: 34-35), στο βαθμό που επεξεργάζονται προσωπικά δεδομένα για τους ανωτέρω σκοπούς. Επομένως, προκειμένου η επεξεργασία των προσωπικών δεδομένων να εμπίπτει στις διατάξεις των άρθρων 43-82 του Νόμου, δεν αρκεί να πραγματοποιείται μόνο από αρμόδιες αρχές, αλλά θα πρέπει να συντρέχει και κάποιος από τους προαναφερόμενους σκοπούς (Άρθρο 43 του Ν.4624/2019). Αξίζει να σημειωθεί ότι στις συγκεκριμένες διατάξεις ο υπεύθυνος επεξεργασίας μπορεί να είναι μόνο η αρμόδια αρχή, που καθορίζει τους σκοπούς και τους τρόπους επεξεργασίας των δεδομένων, σε αντίθεση με τον GDPR που μπορεί να είναι και φυσικό ή νομικό πρόσωπο (Άρθρο 44 του Ν.4624/2019).

4.5.2. Αρχές επεξεργασίας προσωπικών δεδομένων

Αρκετές από τις αρχές της Οδηγίας 2016/680, που αφορούν την επεξεργασία προσωπικών δεδομένων προσομοιάζουν με εκείνες του GDPR, ωστόσο λόγω της ιδιαιτερότητας του σκοπού και του πεδίου εφαρμογής της, ορισμένες αρχές του GDPR δεν περιλαμβάνονται σε αυτή (Maesa, C., 2016). Στο άρθρο 45 του Ν. 4624/2019 εισάγονται στην ελληνική νομοθεσία οι βασικές αρχές επεξεργασίας προσωπικών

¹⁸ Αξίζει να σημειωθεί ότι αστυνομικές έρευνες διοικητικής φύσεως, που πραγματοποιούνται για την αποτροπή μελλοντικού εγκλήματος, καθορίζονται από τις διατάξεις των άρθρων 74 παρ. 15, 93 παρ.1, 94, 96 και 99 του Π.Δ. 141/1991, ενώ (προ)ανακριτικές έρευνες ποινικοοικονομικής φύσεως, που αποβλέπουν στη διακρίβωση υφιστάμενου εγκλήματος, προβλέπονται από τα άρθρα 93 παρ.2 και 95 και από τις διατάξεις του Κώδικα Ποινικής Δικονομίας – Ν. 4620/2019 (Τζέλλης, Δ. & Μυλώση, Μ., 2022: 35).

δεδομένων της Οδηγίας 2016/680, οι οποίες πρέπει να τηρούνται σωρευτικά και στο σύνολό τους.

1. Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας

Η επεξεργασία των προσωπικών δεδομένων του υποκειμένου θα πρέπει να είναι σύννομη, δίκαιη και διαφανής (Άρθρο 45 του Ν. 4624/2019 και Άρθρο 26 της Αιτιολογικής Έκθεσης της Οδηγίας 2016/680). Οι λόγοι νομιμότητας της επεξεργασίας των δεδομένων, όπως αυτοί ορίζονται στο άρθρο 45^A του Ν. 4624/2019 (Άρθρο 8 της Οδηγίας), είναι πιο περιορισμένοι από αυτούς του GDPR, καθώς η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι σύννομη μόνο εάν και στο βαθμό, που είναι απαραίτητη στο πλαίσιο εκτέλεσης καθηκόντων της αρμόδιας αρχής για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους. (Ιγγλεζάκης, Ι., 2018: 35).

2. Αρχή του περιορισμού του σκοπού

Τα προσωπικά δεδομένα του υποκειμένου θα πρέπει να συλλέγονται μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς, ενώ η επεξεργασία τους για λόγους, που δεν συνάδουν με τους σκοπούς αυτούς απαγορεύεται ρητά.

Κατ' εξαίρεση, σύμφωνα με το άρθρο 47 του Ν. 4624/2019 (Άρθρα 4 και 9 παρ.1 της Οδηγίας), τα προσωπικά δεδομένα μπορούν να υποβληθούν σε επεξεργασία για σκοπό διαφορετικό από τον αρχικό, εάν ο υπεύθυνος επεξεργασίας είναι εξουσιοδοτημένος να τα επεξεργαστεί για νέο σκοπό και η επεξεργασία είναι απαραίτητη και ανάλογη προς τον νέο σκοπό.

3. Αρχή της ελαχιστοποίησης των δεδομένων (Αρχή της αναλογικότητας)

Τα δεδομένα, που υπόκεινται σε επεξεργασία θα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με τους σκοπούς αυτής.

4. Αρχή της ακρίβειας

Τα δεδομένα του υποκειμένου θα πρέπει να είναι ακριβή και να επικαιροποιούνται, όταν αυτό είναι απαραίτητο, ενώ επιπλέον, θα πρέπει να διασφαλίζεται η χωρίς καθυστέρηση διαγραφή ή διόρθωση ανακριβών δεδομένων, με γνώμονα πάντα τους σκοπούς της επεξεργασίας.

5. Αρχή της περιόδου αποθήκευσης των δεδομένων

Τα υπό επεξεργασία δεδομένα προσωπικού χαρακτήρα θα πρέπει να διατηρούνται σε μορφή, που επιτρέπει την ταυτοποίηση του υποκειμένου αυτών και μόνο για το χρονικό διάστημα, που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας.

6. Αρχή της ακεραιότητας και εμπιστευτικότητας

Η επεξεργασία των προσωπικών δεδομένων θα πρέπει να γίνεται με τρόπο, που θα εξασφαλίζει την ασφάλεια αυτών και θα αποτρέπει την μη εγκεκριμένη επεξεργασία

τους, απώλεια, καταστροφή ή φθορά, μέσω κατάλληλων τεχνικών ή οργανωτικών μέτρων.

7. Αρχή της λογοδοσίας

Ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να αποδεικνύει, ανά πάσα στιγμή, με πλήρη αιτιολόγηση την τήρηση των υποχρεώσεών του.

Αν και ο Έλληνας νομοθέτης στο άρθρο 49 του Ν. 4624/2019 κάνει αναφορά στη συγκατάθεση του υποκειμένου για την επεξεργασία των προσωπικών του δεδομένων, αυτή σύμφωνα με το γενικότερο πλαίσιο της Οδηγίας 2016/680 δεν αποτελεί νομική βάση για την επεξεργασία των προσωπικών δεδομένων. Και αυτό γιατί η εκτέλεση των καθηκόντων, που ανατίθεται από το νόμο στις αρμόδιες αρχές παρέχει σε αυτές τη δυνατότητα να απαιτούν ή να δίνουν εντολές στο άτομο να συμμορφωθεί προς σχετικά αιτήματα. Έτσι, το υποκείμενο των δεδομένων δεν έχει ουσιαστική και ελεύθερη επιλογή, με αποτέλεσμα οι ενέργειές του να μην μπορούν να θεωρηθούν ως ελεύθερη δήλωση βούλησης (Άρθρο 35 της Αιτιολογικής Έκθεσης της Οδηγίας 2016/680). Αυτό βέβαια είναι λογικό, αν αναλογιστεί κανείς ότι ένας ύποπτος τέλεσης αξιόποινης πράξης δεν θα συναινούσε στην επεξεργασία των προσωπικών του δεδομένων, προκειμένου να αποφύγει τυχόν σε βάρος του αποδεικτικά στοιχεία (Leiser, M. & Custers, B., 2019: 374).

4.5.2.1. Επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων

Στον Ν. 4624/2019 οι προϋποθέσεις επεξεργασίας των ειδικών κατηγοριών προσωπικών δεδομένων από αρμόδιες αρχές, όπως αυτές ορίστηκαν προηγουμένως, αναφέρονται στο άρθρο 46 (Άρθρο 10 της Οδηγίας). Πιο συγκεκριμένα, η επεξεργασία επιτρέπεται όταν είναι απολύτως αναγκαία για την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων, καθώς και την προστασία από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους και εφόσον:

- προβλέπεται ρητά από ενωσιακό ή εθνικό δίκαιο,
- επιβάλλεται για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
- η επεξεργασία αφορά δεδομένα που έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.

Συνεπώς, η επεξεργασία των ειδικών κατηγοριών προσωπικών δεδομένων δεν πραγματοποιείται ανεξέλεγκτα, αλλά υπό την προϋπόθεση της απόλυτης αναγκαιότητας για τους σκοπούς που ορίζονται στο άρθρο 43 του Ν. 4624/2019.

Ασφαλώς, θα πρέπει να λαμβάνονται αυξημένα μέτρα για τη διασφάλιση της προστασίας του υποκειμένου των δεδομένων. Συγκεκριμένα, πρέπει να διενεργείται αυστηρός έλεγχος για την ασφάλεια κατά την επεξεργασία τους και να περιορίζεται η πρόσβαση μόνο σε εξουσιοδοτημένα και κατάλληλα εκπαιδευμένα άτομα. Η ανάγκη διατήρησής τους πρέπει να εξετάζεται και να τεκμηριώνεται ανά τακτά διαστήματα,

ενώ επίσης πρέπει να τηρούνται χωριστά από τα υπόλοιπα – απλά δεδομένα. Επιπλέον, πρέπει να εφαρμόζονται τεχνικές κρυπτογράφησης των δεδομένων, αλλά και ψευδωνυμοποίησης, όπου αυτό είναι εφικτό. Τέλος, στις περιπτώσεις που τα δεδομένα ειδικών κατηγοριών θα πρέπει να διαβιβαστούν ή να τεθούν σε επεξεργασία για σκοπό διαφορετικό από τον αρχικό, πρέπει να διασφαλίζεται ο νόμιμος χαρακτήρας της επεξεργασίας και η προστασία των δικαιωμάτων του υποκειμένου (Άρθρο 46 του Ν. 4624/2019).

4.5.3. Δικαιώματα υποκειμένου δεδομένων

Ομοίως με τις αρχές, η Οδηγία 2016/680 αναγνωρίζει τα βασικά δικαιώματα του υποκειμένου που προβλέπει ο GDPR, ωστόσο λόγω του ειδικού χαρακτήρα των ποινικών ερευνών και των απαιτήσεων μυστικότητας, εισάγονται ορισμένοι περιορισμοί (Κανέλλος, 2020: 279, 292). Έτσι, τα άρθρα 13-17 της Οδηγίας, όπως ενσωματώνονται στα άρθρα 53-59 του Ν. 4624/2019, αποτυπώνουν τα δικαιώματα του υποκειμένου.

1. Γενικές πληροφορίες σχετικά με την επεξεργασία δεδομένων – Δικαίωμα διαφάνειας (άρθρο 53)

Ο υπεύθυνος επεξεργασίας οφείλει να παρέχει γενικές και εύκολα προσβάσιμες πληροφορίες στο κοινό, σε απλή και κατανοητή γλώσσα και μέσω του διαδικτυακού τόπου της εκάστοτε αρμόδιας αρχής, αναφορικά με:

- τους σκοπούς επεξεργασίας,
- τη δυνατότητα υποβολής αιτήματος στον ίδιο, για πρόσβαση, διόρθωση ή διαγραφή και περιορισμό της επεξεργασίας των προσωπικών δεδομένων,
- την ταυτότητα και τα στοιχεία επικοινωνίας αυτού και του υπεύθυνου προστασίας δεδομένων,
- το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και τα στοιχεία επικοινωνίας αυτής.

Θα πρέπει, ωστόσο, να ληφθεί υπόψη ότι προκειμένου να διασφαλιστεί η άσκηση των δικαιωμάτων του υποκειμένου, η γνωστοποίηση των στοιχείων ταυτότητας και επικοινωνίας του υπεύθυνου επεξεργασίας και του υπεύθυνου προστασίας δεδομένων, θέτει σε κίνδυνο την προστασία των προσωπικών τους δεδομένων, ειδικά όταν το υποκείμενο είναι ύποπτος ή κατηγορούμενος, καθώς ενδέχεται να τα χρησιμοποιήσει κακοπροαίρετα (Salami, E., 2017: 7).

2. Δικαίωμα ενημέρωσης (άρθρο 54)

Εκτός από τις πληροφορίες, που προαναφέρθηκαν, ο υπεύθυνος επεξεργασίας, σε συγκεκριμένες περιπτώσεις και ειδικά όταν η συλλογή των δεδομένων έλαβε χώρα υπό συνθήκες μυστικότητας, παρέχει στο υποκείμενο των δεδομένων συμπληρωματικές πληροφορίες προκειμένου να ενθαρρύνεται η άσκηση των δικαιωμάτων του. Οι πρόσθετες πληροφορίες αφορούν:

- τη νομική βάση, στην οποία στηρίζεται η επεξεργασία,
- το χρονικό διάστημα αποθήκευσης των δεδομένων ή, όταν αυτό είναι αδύνατο να προσδιοριστεί, τα κριτήρια που το καθορίζουν,
- τους αποδέκτες των δεδομένων (εάν υπάρχουν),
- συμπληρωματικές πληροφορίες, κυρίως όταν τα προσωπικά δεδομένα προσωπικού συλλέγονται εν αγνοία του υποκειμένου.

Ωστόσο, ο υπεύθυνος επεξεργασίας μπορεί να αναβάλει, περιορίσει ή παραλείψει την ενημέρωση του υποκειμένου, εάν κρίνει ότι αυτό είναι απαραίτητο για την εκτέλεση των καθηκόντων των αρμόδιων αρχών, την εθνική ή/και δημόσια ασφάλεια και την προστασία των έννομων συμφερόντων τρίτων.

Η συγκεκριμένη διάταξη είναι αρκετά ευρεία και επιτρέπει τη μη εφαρμογή του δικαιώματος ενημέρωσης. Ειδικά στις περιπτώσεις των υπόπτων ή κατηγορουμένων μπορεί να προβάλλεται το επιχείρημα ότι η παροχή τέτοιων πληροφοριών δύναται να εμποδίσει ή να βλάψει την έρευνα. Επομένως, το δικαίωμα της ενημέρωσης να μην υπάρχει κατ' αρχήν, όμως στην πράξη ενδέχεται να μην μπορεί να ασκηθεί σε αρκετές περιπτώσεις (Salami, E., 2017: 7).

3. Δικαίωμα πρόσβασης (άρθρο 55)

Το υποκείμενο των δεδομένων έχει δικαίωμα να ενημερώνεται, κατόπιν αιτήσεώς του, από τον υπεύθυνο επεξεργασίας αναφορικά με το κατά πόσο τα δεδομένα του υπόκεινται ή όχι σε επεξεργασία και σε θετική περίπτωση να αποκτά πρόσβαση σε αυτά και σε πληροφορίες που αφορούν:

- τα δεδομένα που υποβάλλονται σε επεξεργασία, την προέλευσή τους, καθώς και τις κατηγορίες τους,
- τους σκοπούς και τη νομική βάση της επεξεργασίας,
- τους αποδέκτες ή τις κατηγορίες αποδεκτών και κυρίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,
- το προβλεπόμενο χρονικό διάστημα αποθήκευσης ή, όταν αυτό είναι αδύνατο να προσδιοριστεί, τα κριτήρια που το καθορίζουν,
- τη δυνατότητα υποβολής αιτήματος στον υπεύθυνο επεξεργασίας, για διόρθωση ή διαγραφή και περιορισμό της επεξεργασίας των προσωπικών δεδομένων,
- το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή και τα στοιχεία επικοινωνίας αυτής.

Ωστόσο, η άσκηση του εν λόγω δικαιώματος υπόκειται σε ορισμένους περιορισμούς, καθώς δεν εφαρμόζεται σε δεδομένα που υποβάλλονται σε επεξεργασία επειδή δεν μπορούν να διαγραφούν και διατηρούνται για νομικούς λόγους ή σκοπούς ασφάλειας και ελέγχου των δεδομένων, εάν η παροχή πληροφοριών απαιτεί

δυσανάλογη προσπάθεια. Επιπλέον, στο υποκείμενο των δεδομένων δεν γνωστοποιείται η ταυτότητα των ατόμων από τα οποία αυτά συλλέχθηκαν, όταν κάτι τέτοιο μπορεί να θέσει σε κίνδυνο τη ζωή ή τη σωματική ακεραιότητα αυτών, καθώς και όταν πρόκειται για προστατευόμενους μάρτυρες ή πληροφοριοδότες (Κανέλλος, Λ., 2020: 293).

Επιπροσθέτως, ο υπεύθυνος επεξεργασίας δύναται να αρνηθεί ή να περιορίσει την παροχή πληροφοριών στο υποκείμενο των δεδομένων. Σε αυτή την περίπτωση, θα πρέπει να ενημερώσει το υποκείμενο άμεσα και εγγράφως για την απόφασή του γνωστοποιώντας τους σχετικούς λόγους, καθώς και για το δικαίωμά του να υποβάλει καταγγελία στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, αν θεωρεί ότι παραβιάζονται τα δικαιώματά του. Κατ' εξαίρεση, ο υπεύθυνος επεξεργασίας μπορεί να αρνηθεί την προαναφερόμενη γνωστοποίηση και αντίστοιχη αιτιολόγηση εάν η παροχή αυτών των πληροφοριών θέτει σε κίνδυνο την εκτέλεση των καθηκόντων των αρμόδιων αρχών, την εθνική ή/και δημόσια ασφάλεια και την προστασία των έννομων συμφερόντων τρίτων.

4. Δικαίωμα διόρθωσης ή διαγραφής και περιορισμού της επεξεργασίας (άρθρο 56)

Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν, χωρίς άσκοπη καθυστέρηση και να απαιτήσει την συμπλήρωση ελλειπών δεδομένων. Στο άρθρο 56 παρ. 1 διευκρινίζεται ότι στην περίπτωση δήλωσης ή απόφασης, για παράδειγμα σε κατάθεση μάρτυρα (Άρθρο 47 Αιτιολογικής Έκθεσης της Οδηγίας 2016/680) ή σε εκδοθείσα απόφαση, που αφορά το υποκείμενο των δεδομένων, εάν ανακύψει ζήτημα ανακρίβειας των στοιχείων του υποκειμένου, το περιεχόμενο αυτής παραμένει ανεπηρέαστο. Σε περίπτωση που το υποκείμενο των δεδομένων αμφισβητήσει την ακρίβεια των δεδομένων του, αλλά δεν μπορεί να εξακριβωθεί η ακρίβειά τους, ο υπεύθυνος επεξεργασίας μπορεί να περιορίσει την επεξεργασία τους αντί να τα διαγράψει. Σε αυτή την περίπτωση, θα πρέπει έπειτα να ενημερώσει το υποκείμενο πριν την άρση του περιορισμού.

Επιπλέον, το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας να διαγράψει τα δεδομένα του χωρίς καθυστέρηση, εάν με την επεξεργασία παραβιάζονται οι διατάξεις του Κεφαλαίου IV του Ν. 4624/2019, η γνώση των συγκεκριμένων δεδομένων δεν είναι πλέον απαραίτητη για την εκτέλεση των καθηκόντων των αρμόδιων αρχών, ή τα δεδομένα πρέπει να διαγραφούν επειδή ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος από το νόμο να προβεί σε αυτή την ενέργεια. Σημειώνεται πως, όπως προαναφέρθηκε, ο υπεύθυνος επεξεργασίας μπορεί να προβαίνει αυτοβούλως στη διαγραφή των δεδομένων του υποκειμένου, χωρίς κάποιο σχετικό αίτημα, εφόσον αυτό επιβάλλεται από τον νόμο.

Ωστόσο, ο υπεύθυνος επεξεργασίας αντί για διαγραφή δύναται να περιορίσει την επεξεργασία των δεδομένων και σε περίπτωση που:

- συντρέχει εύλογη υπόθεση ότι η διαγραφή των δεδομένων θα βλάψει τα έννομα συμφέροντα του υποκειμένου,
- τα δεδομένα πρέπει να διατηρηθούν, καθώς χρησιμεύουν ως αποδεικτικά μέσα για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους, και βασίζεται στο δίκαιο της Ένωσης ή των κρατών μελών,
- η διαγραφή είναι αδύνατη ή απαιτεί δυσανάλογη προσπάθεια λόγω του ειδικού τρόπου αποθήκευσης,

Τα προσωπικά δεδομένα, που υπόκεινται σε περιορισμένη επεξεργασία για έναν από τους παραπάνω λόγους, μπορούν να τεθούν σε επεξεργασία μόνο για τον σκοπό, που παρεμπόδισε την διαγραφή τους.

Για κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας τους, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να ενημερώνει το υποκείμενο των δεδομένων. Από την άλλη, σε περίπτωση που ο υπεύθυνος επεξεργασίας αρνηθεί να ικανοποιήσει το αίτημα του υποκειμένου για διόρθωση, διαγραφή ή περιορισμό θα πρέπει να το ενημερώσει εγγράφως και να παράσχει πληροφορίες για τους λόγους άρνησης, εκτός εάν συντρέχει κίνδυνος για την εκτέλεση των καθηκόντων των αρμόδιων αρχών, την εθνική ή/και δημόσια ασφάλεια και την προστασία των έννομων συμφερόντων τρίτων.

5. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή (άρθρο 58)

Δεδομένου ότι σε ένα κράτος δικαίου, ουδείς είναι υπεράνω του νόμου, οποιαδήποτε αντεγκληματική πολιτική θα πρέπει να έχει ως γνώμονα την προστασία των προσωπικών δεδομένων των ατόμων. Ως εκ τούτου, εάν κάποιο υποκείμενο θεωρεί ότι έχουν παραβιαστεί τα δικαιώματά του, έχει δικαίωμα να υποβάλει καταγγελία στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Κανέλλος, Λ., 2020: 126).

Σε περίπτωση που η καταγγελία υποβληθεί στην Α.Π.Δ.Π.Χ. και όχι στην αρμόδια εποπτική αρχή άλλου κράτους μέλους, διαβιβάζεται χωρίς καθυστέρηση σε αυτή και ενημερώνεται σχετικά το υποκείμενο.

Αξίζει να σημειωθεί ότι η επεξεργασία των προσωπικών δεδομένων, που πραγματοποιείται από δικαστικές και εισαγγελικές αρχές στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας, δεν εμπίπτει στην εποπτική αρμοδιότητα της Α.Π.Δ.Π.Χ. (Γριβοκωστόπουλος, Ι., 2021: 10).

6. Δικαιώματα υποκειμένου σε ποινικές έρευνες και διαδικασίες (άρθρο 59)

Τα δικαιώματα ενημέρωσης, πρόσβασης, διόρθωσης ή διαγραφής και περιορισμού της επεξεργασίας δεδομένων, που προαναφέρθηκαν, για σκοπούς πρόληψης, ανίχνευσης και δίωξης εγκλημάτων, καθώς και οι αντίστοιχες υποχρεώσεις των αρχών λαμβάνουν χώρα σύμφωνα με τους ισχύοντες εθνικούς ουσιαστικούς και δικονομικούς κανόνες και εγγυήσεις και συγκεκριμένα, σύμφωνα με όσα ορίζουν οι

διατάξεις του Κώδικα Ποινικής Δικονομίας (Κ.Π.Δ.), οι ειδικές δικονομικές διατάξεις και ο Κώδικας Οργανισμού Δικαστηρίων και Κατάστασης Δικαστικών Λειτουργιών (Κ.Ο.Δ.Κ.Δ.Λ.). Επομένως, για λοιπές επεξεργασίες δεδομένων από διωκτικές αρχές, όπως για παράδειγμα μισθοδοσία, προμήθειες εξοπλισμού, κ.λπ., ισχύει ο GDPR (Κανέλλος, Λ., 2020: 285).

Κατόπιν της ανάλυσης, που προηγήθηκε στις βασικές αρχές επεξεργασίας προσωπικών δεδομένων και στα δικαιώματα των υποκειμένων, αξίζει να σημειωθεί ότι η αρχή και το δικαίωμα της διαφάνειας, σε ορισμένες περιπτώσεις δύναται να μην εφαρμοστούν, λόγω του ειδικού χαρακτήρα των σκοπών επεξεργασίας δεδομένων, που καλύπτονται από το πεδίο εφαρμογής της Αστυνομικής Οδηγίας (Radtke, T., 2020: 246). Και αυτό γιατί, εάν η εκάστοτε αρμόδια αρχή έπρεπε να αποκαλύπτει κάθε επεξεργασία δεδομένων, που πραγματοποιεί, αυτό θα μπορούσε να αποτελέσει τροχοπέδη ή να θέσει σε κίνδυνο τις έρευνές της (Leiser, M. & Custers, B., 2019: 371).

Ακολουθεί συνοπτικός πίνακας των δικαιωμάτων του υποκειμένου που προβλέπει η Οδηγία 2016/680 και τα οποία έχουν ενσωματωθεί στην ελληνική νομοθεσία με τον Ν.4624/2019:

Πίνακας 2: Δικαιώματα υποκειμένων Οδηγία 2016/680 - Ν. 4624/2019

<u>Δικαιώματα υποκειμένων</u>	<u>Οδηγία 2016/680</u>	<u>Ν. 4624/2019</u>
Γενικές πληροφορίες σχετικά με την επεξεργασία δεδομένων	Άρθρο 12 και 13	Άρθρο 53
Δικαίωμα ενημέρωσης	Άρθρο 13	Άρθρο 54
Δικαίωμα πρόσβασης	Άρθρο 14 - 15	Άρθρο 55
Δικαίωμα διόρθωσης ή διαγραφής και περιορισμοί της επεξεργασίας	Άρθρο 16	Άρθρο 56
Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή	Άρθρο 52	Άρθρο 58
Δικαιώματα υποκειμένου σε ποινικές έρευνες και διαδικασίες	Άρθρο 18	Άρθρο 59

4.6. Νόμος 5002/2022

Άλλο ένα νομοθετικό κείμενο, που παρουσιάζει ιδιαίτερο ενδιαφέρον, είναι ο Ν. 5002/2022 για τη διαδικασία άρσης του απορρήτου των επικοινωνιών, την κυβερνοασφάλεια και την προστασία προσωπικών δεδομένων πολιτών. Η άρση του απορρήτου των επικοινωνιών αποτελεί μια ειδική ανακριτική πράξη, στην οποία δύναται να προβούν οι ανακριτικοί υπάλληλοι σε ορισμένες περιπτώσεις εγκλημάτων,

όπως αυτές ορίζονται στα άρθρα 254 παρ.1 και 255 παρ.1 του Ν. 4620/2019 – Κώδικας Ποινικής Δικονομίας (Κ.Π.Δ.), αλλά και σε έρευνες που προβλέπονται σε ειδικούς ποινικούς νόμους, όπως είναι ο Ν. 5002/2022 (Άρθρο 254 παρ. 6 του Κ.Π.Δ.).

Το απόρρητο των επιστολών, της ελεύθερης ανταπόκρισης και επικοινωνίας είναι απόλυτα απαραβίαστο, αποτελεί θεμελιώδες δικαίωμα κάθε ατόμου, το οποίο κατοχυρώνεται στο άρθρο 19 του Συντάγματος και προστατεύεται από την Ανεξάρτητη Αρχή Διασφάλισης του Απορρήτου του Επικοινωνιών (Α.Δ.Α.Ε.).¹⁹

Ως άρση απορρήτου των επικοινωνιών νοείται μία κατ' εξαίρεση επιτρεπόμενη διαδικασία βάσει της οποίας στοιχεία της επικοινωνίας, που είναι κατ' αρχήν απόρρητα, γνωστοποιούνται σε συγκεκριμένες Αρχές και για συγκεκριμένους λόγους.²⁰ Σύμφωνα με το άρθρο 3 του Π.Δ. 47/2005 η άρση του απορρήτου δεν αφορά την επικοινωνία, που γίνεται δια ζώσης, αλλά εκείνη, που διεξάγεται μέσω δικτύου επικοινωνίας ή παρόχου υπηρεσιών επικοινωνιών, που χρησιμοποιεί ο συνδρομητής/χρήστης σε βάρος του οποίου λαμβάνεται το μέτρο της άρσης. Στα στοιχεία της επικοινωνίας περιλαμβάνονται, μεταξύ άλλων, το περιεχόμενο της επικοινωνίας, ο τηλεφωνικός αριθμός εισερχόμενης και εξερχόμενης κλήσης, η ταυτότητα των εμπλεκόμενων μερών, η ώρα έναρξης και λήξης της επικοινωνίας, τα δεδομένα θέσης της τερματικής συσκευής – γεωγραφικό στίγμα, τα στοιχεία ταυτότητας της τερματικής συσκευής (IMEI, IM3I, TM3I), η διεύθυνση IP, κ.α. (Άρθρο 4 του Π.Δ. 47/2005). Δεδομένου ότι αυτά τα στοιχεία μπορούν να ταυτοποιήσουν άμεσα ή έμμεσα ένα φυσικό πρόσωπο, αποτελούν προσωπικά δεδομένα. Επομένως, όταν γίνεται άρση του απορρήτου, δίνεται πρόσβαση στα προσωπικά δεδομένα των εμπλεκόμενων μερών. Ωστόσο, σύμφωνα με το άρθρο 19 παρ. 3 του Συντάγματος, τα αποδεικτικά μέσα που θα προκύψουν από την άρση του απορρήτου, θα πρέπει να έχουν αποκτηθεί κατ' εφαρμογή των άρθρων 9 και 9Α του Συντάγματος, διαφορετικά απαγορεύεται να χρησιμοποιηθούν ενώπιον δικαστηρίου ή οποιασδήποτε άλλης αρχής (Παναγοπούλου, Φ., 2023: 52). Συνεπώς τα προστατευόμενα αγαθά των άρθρων 19 και 9^Α του Συντάγματος συνδέονται άρρηκτα μεταξύ τους (Παναγοπούλου, Φ., 2023: 51).

Αν και στο πρώτο εδάφιο του άρθρου 19 του Συντάγματος διακηρύσσεται το απόλυτο απαραβίαστο του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης και επικοινωνίας, στο δεύτερο εδάφιο προβλέπεται ότι το απόρρητο μπορεί κατ' εξαίρεση να αρθεί μόνο από δικαστική αρχή και μόνο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση συγκεκριμένων εγκλημάτων.

Με τον Ν. 2225/1994 καθορίστηκαν οι όροι και προϋποθέσεις για την άρση απορρήτου της επικοινωνίας (Lawspot, 2022), ενώ στην συνέχεια ψηφίστηκε ο Ν. 5002/2022, ο οποίος θωρακίζει και εκσυγχρονίζει τη διαδικασία άρσης του απορρήτου των επικοινωνιών.

Στο άρθρο 4 του Ν. 5002/2022 ορίζεται η διαδικασία, που πρέπει να ακολουθήσουν η Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.) και η Διεύθυνση

¹⁹ <https://adae.gov.gr/polites/ilektronikes-epikoinonies/syxnes-erotiseis#>

²⁰ <https://adae.gov.gr/polites/ilektronikes-epikoinonies/syxnes-erotiseis#>

Αντιμετώπισης Ειδικών Εγκλημάτων Βίας της Ελληνικής Αστυνομίας (Δ.Α.Ε.Ε.Β.) για να υποβάλλουν αίτημα για άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας σε εισαγγελικό λειτουργό, ενώ στο άρθρο 5 του ίδιου Νόμου, προβλέπεται η διαχείριση του υλικού, που αποκτήθηκε από την άρση του απορρήτου για τους ανωτέρω λόγους.

Εκτός από τα παραπάνω, ο Ν. 5002/2022 ορίζει στο άρθρο 6 τα αδικήματα, για τη διακρίβωση των οποίων είναι επιτρεπτή η άρση του απορρήτου των επικοινωνιών, καθώς και τη διαδικασία, που πρέπει να ακολουθήσει η αιτούσα αρχή για να υποβάλει το αίτημά της. Η απαρίθμηση των αδικημάτων βασίζεται στη φύση και ιδιαίτερη απαξία του αδικήματος, στην προσφορότητα του μέτρου της άρσης του απορρήτου ως μέσου εξιχνίασης των εγκλημάτων και στη βαρύτητα της επαπειλούμενης ποινής (Lawspot, 2022). Συγκεκριμένα, η άρση του απορρήτου επιτρέπεται για τη διακρίβωση κακουργημάτων:

- των άρθρων 134-152, 157-160Α, 183-191Α, 207-213, 308-315Α, 322-334, 363-353, 370-371, 235-237, 264, 265, 270, 272, 299, 374, 380, 385, 386 και 386Α του Ποινικού Κώδικα (Π.Κ. - Ν. 4619/2019)
- των άρθρων 15-20, 46, 47, 140 και 144 του Στρατιωτικού Ποινικού Κώδικα (Ν. 2287/1995)
- του Ν. 4557/2018, του άρθρου 157 παρ.1 περ.γ' Ν. 2960/2001, των άρθρων 28 και 31 του Ν. 4443/2016, του άρθρου 15 του Ν. 2168/1993, των άρθρων 20, 22 και 23 του Ν. 4139/2013, του άρθρου 11 του Ν. 3917/2011, του άρθρου 38 παρ.5 του Ν. 4624/2019, του άρθρου 28 του Ν. 1650/1986, του Ν. 4858/2021, του άρθρου 66 παρ.3 του Ν. 2121/1993, του άρθρου 132 παρ.4 του Ν. 2725/1999 και του άρθρου 30 του Ν. 4251/2014,

αλλά και πλημμελημάτων:

- των άρθρων 148, 187, 187Α, 187Β, 323Α, 324, 339, 342, 343, 346, 348, 348Α, 348Β, 348Γ, 351Α, 370ΣΤ, 386 και 386Α του Ποινικού Κώδικα
- των άρθρων 28 και 31 του Ν. 4443/2016 και του άρθρου 44 παρ. 1 εδ. γ' του Ν. 3959/2011.

Στο άρθρο 7 του Ν. 5002/2022, προβλέπεται η διαχείριση του υλικού, κατά την ποινική διαδικασία, που αποκτήθηκε από την άρση του απορρήτου των επικοινωνιών για τη διακρίβωση τέλεσης των ανωτέρω αδικημάτων.

Άλλη μία σημαντική διάταξη του Ν. 5002/2022 είναι αυτή του άρθρου 8, στο οποίο αποτυπώνεται η διαδικασία άρσης του απορρήτου, που ακολουθεί μετά την έκδοση του βουλεύματος ή της διάταξης περί άρσης.

Ο Ν. 5002/2022, εκτός από τις διατάξεις περί άρσης του απορρήτου των επικοινωνιών, εισήγαγε, τροποποίησε και αντικατέστησε διατάξεις του Ν. 4624/2019, με σκοπό την αποτελεσματικότερη προστασία των φυσικών προσώπων έναντι της

επεξεργασίας δεδομένων προσωπικού χαρακτήρα (Άρθρο 1 του Ν. 5002/2022).²¹ Μία εξαιρετικά σημαντική προσθήκη είναι αυτή του άρθρου 84^A στον Ν. 4624/2019 (Άρθρο 45 του Ν. 5002/2022), στο οποίο καθορίζονται οι όροι και προϋποθέσεις υπό τις οποίες η Ελληνική Αστυνομία, κατόπιν διάταξης Εισαγγελικής Αρχής, προβαίνει στη δημοσιοποίηση των στοιχείων της ταυτότητας, της εικόνας και της ποινικής δίωξης κατηγορουμένου ή καταδικασθέντος.

4.7. Συμπεράσματα

Συνοψίζοντας, ο GDPR και η Οδηγία 2016/680 αποτελούν αναμφίβολα emblematicά νομοθετικά επιτεύγματα σε επίπεδο Ευρωπαϊκής Ένωσης σχετικά με την προστασία των προσωπικών δεδομένων. Από τη μία ο GDPR εφαρμόζεται άμεσα σε όλα τα κράτη-μέλη της Ε.Ε., διαμορφώνοντας ενιαίο και δεσμευτικό πλαίσιο εφαρμογής του και από την άλλη η Οδηγία 2016/680 ρυθμίζει τον τρόπο επεξεργασίας των προσωπικών δεδομένων από τις αρμόδιες αρχές στο πλαίσιο πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων. Σε εθνικό επίπεδο, η ελληνική νομοθεσία έχει διαμορφώσει ένα ισχυρό πλαίσιο για την επεξεργασία και προστασία των προσωπικών δεδομένων των φυσικών προσώπων. Με το άρθρο 9^A του Συντάγματος κατοχυρώνεται ρητά η προστασία των προσωπικών δεδομένων ως θεμελιώδες δικαίωμα σε μία σύγχρονη, δημοκρατική, διαρκώς τεχνολογικά εξελισσόμενη κοινωνία. Παράλληλα, στο πλαίσιο συμμόρφωσης και προσαρμογής της χώρας μας στις ευρωπαϊκές απαιτήσεις θεσπίστηκε ο Ν. 4624/2019, με τον οποίο τίθενται μέτρα εφαρμογής του GDPR και ενσωματώνεται η Οδηγία 2016/680 στην ελληνική νομοθεσία, όπου η παραβίαση των διατάξεών του επισύρει ποινικές και διοικητικές κυρώσεις (Άρθρα 38, 39, 81 και 82 του Νόμου).

Αν και το βασικό νομικό πλαίσιο προστασίας δεδομένων, αποτελείται από τον GDPR, την Οδηγία 2016/680 και τον Ν. 4624/2019, καθοριστικής σημασίας είναι και ο Ν. 5002/2022, ο οποίος θωρακίζει και εκσυγχρονίζει την διαδικασία άρσης απορρήτου των επικοινωνιών και εισάγει τροποποιήσεις σε διατάξεις του Ν. 4624/2019 για την αποτελεσματικότερη προστασία των φυσικών προσώπων κατά την επεξεργασία των προσωπικών τους δεδομένων. Ωστόσο, εκτός από τα προαναφερόμενα νομικά κείμενα, η επεξεργασία και προστασία των προσωπικών δεδομένων στο πλαίσιο της λειτουργίας της Ελληνικής Αστυνομίας, ρυθμίζονται και από ένα ευρύτερο πλέγμα εθνικών διατάξεων, οι οποίες εξειδικεύουν και συμπληρώνουν το βασικό. Οι ειδικότερες διατάξεις αφορούν άλλους Νόμους, τον Κώδικα Ποινικής Δικονομίας (Κ.Π.Δ.) – Ν. 4620/2019, αλλά και Προεδρικά Διατάγματα ή Υπουργικές Αποφάσεις, τα οποία καθορίζουν τους όρους και τις προϋποθέσεις αναφορικά με την συλλογή και επεξεργασία προσωπικών δεδομένων, κατά τις προληπτικές, κατασταλτικές και διοικητικές δράσεις της Ελληνικής Αστυνομίας.

²¹ Στην ανάλυση του Ν. 4624/2019, που προηγήθηκε, έχουν ενσωματωθεί οι επικαιροποιημένες διατάξεις.

5. Αρχή & Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

5.1. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - Α.Π.Δ.Π.Χ.

5.1.1. Εισαγωγή

Κάθε κράτος μέλος είναι υποχρεωμένο να ορίζει μία ή περισσότερες ανεξάρτητες δημόσιες αρχές, που θα εποπτεύουν την εφαρμογή του GDPR, προκειμένου να προστατεύονται τα θεμελιώδη δικαιώματα και οι ελευθερίες των φυσικών προσώπων, κατά την επεξεργασία των προσωπικών τους δεδομένων (Άρθρο 51 του GDPR).

Στη χώρα μας, ως εποπτική αρχή ορίζεται η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.), η οποία συνιστά ανεξάρτητη δημόσια αρχή κατά το άρθρο 9Α του Συντάγματος και συστάθηκε με τον Ν. 2472/1997. Ζητήματα αναφορικά με τη λειτουργία και τις αρμοδιότητες της Α.Π.Δ.Π.Χ. ρυθμίζονται στα άρθρα 57-58 του GDPR και στο Κεφάλαιο II του Ν. 4624/2019 και συγκεκριμένα στα άρθρα 9-20.

Η Α.Π.Δ.Π.Χ. αποτελείται από έναν Πρόεδρο και έξι ακόμα μέλη, με αντίστοιχους αναπληρωτές. Η διάρκεια θητείας του καθενός είναι έξι έτη (Άρθρο 9 του Ν. 4624/2019). Αποστολή της είναι ο έλεγχος της εφαρμογής των νομικών κειμένων, που αφορούν την προστασία των προσωπικών δεδομένων, μεταξύ των οποίων του GDPR και του Ν. 4624/2019, καθώς και η άσκηση των αρμοδιοτήτων που της ανατίθενται (Άρθρα 51 και 55 του GDPR και 9 και 13 του Ν. 4624/2019).

5.1.2. Καθήκοντα της Α.Π.Δ.Π.Χ.

Η Α.Π.Δ.Π.Χ. έχει ευρύ φάσμα καθηκόντων και αρμοδιοτήτων, τα οποία καθορίζονται από το άρθρο 57 του GDPR και το άρθρο 13 του Ν. 4624/2019. Μεταξύ αυτών, η Α.Π.Δ.Π.Χ. ενημερώνει τους πολίτες αναφορικά με τα δικαιώματά τους και τους ευαισθητοποιεί σχετικά με τους κινδύνους, που εγκυμονεί η επεξεργασία των προσωπικών τους δεδομένων, δίνοντας ιδιαίτερη έμφαση στις περιπτώσεις, που η επεξεργασία αφορά δεδομένα παιδιών. Παράλληλα, λαμβάνει και χειρίζεται αιτήματα και καταγγελίες, που αφορούν τα δικαιώματα των φυσικών προσώπων και ζητήματα προστασίας των προσωπικών τους δεδομένων, ενημερώνοντας, σε κάθε περίπτωση, τον αιτούντα/ καταγγέλλοντα για την πορεία τους.

Επιπλέον, παρέχει συμβουλές στον υπεύθυνο και εκτελών την επεξεργασία των προσωπικών δεδομένων και διερευνά το κατά πόσο αυτοί εφαρμόζουν τις διατάξεις του GDPR, του Ν. 4624/2019 και εν γένει του νομικού πλαισίου για τα προσωπικά δεδομένα. Όταν διαπιστώνει παραβάσεις των νομοθετικών κειμένων περί προστασίας δεδομένων, δύναται να περιορίσει την επεξεργασία – προσωρινά ή οριστικά – καθώς και να προβεί σε επιπλήξεις ή να επιβάλλει σχετικά διοικητικά πρόστιμα (Άρθρο 58 του GDPR).

Συμβουλές παρέχει και στην κυβέρνηση, το εθνικό κοινοβούλιο και άλλους φορείς σχετικά με διοικητικά και νομοθετικά μέτρα, που αφορούν την προστασία των προσωπικών δεδομένων κατά την επεξεργασία τους, εκφράζοντας τη γνώμη της για κάθε διάταξη που πρόκειται να ενσωματωθεί σε νομοθετική ή κανονιστική πράξη.

Η Α.Π.Δ.Π.Χ. παρακολουθεί τις εξελίξεις των τεχνολογιών των πληροφοριών και επικοινωνιών και των εμπορικών πρακτικών, στο βαθμό που επηρεάζουν την προστασία των προσωπικών δεδομένων και εκδίδει κατευθυντήριες οδηγίες και συστάσεις που σχετίζονται με την επεξεργασία δεδομένων. Σε αυτό το πλαίσιο, καταρτίζει και εκδίδει κατάλογο με τις πράξεις για τις οποίες κρίνεται απαραίτητη η εκτίμηση αντικτύπου αναφορικά με την προστασία των δεδομένων κατά την επεξεργασία τους (Άρθρο 35 παρ. 4 του GDPR).

Εκτός των ανωτέρω, η Α.Π.Δ.Π.Χ. ενθαρρύνει την κατάρτιση κωδίκων δεοντολογίας και εφόσον διαπιστώσει ότι παρέχουν τις εγγυήσεις, που ορίζει ο GDPR τους εγκρίνει. Τέλος, κατά την εκτέλεση των αρμοδιοτήτων της συνεργάζεται με εποπτικές αρχές άλλων κρατών μελών για θέματα που αφορούν την επεξεργασία προσωπικών δεδομένων, ώστε να διασφαλίζεται ότι υφίσταται κοινό πλαίσιο εφαρμογής του GDPR από όλα τα κράτη μέλη (Άρθρο 57 του GDPR).

Γενικά, η Α.Π.Δ.Π.Χ. συμβάλλει στην επαύξηση της προστασίας των προσωπικών δεδομένων κατά την επεξεργασία τους, ενεργεί και λειτουργεί ως «συμπαραστάτης» σε όσους προσφεύγουν σε αυτή ενώ οι αποφάσεις της έχουν δεσμευτικό ή/και κυρωτικό χαρακτήρα (Μήτρου, Λ. 2002: 44).

Εκ των προαναφερθέντων, γίνεται σαφές ότι η Α.Π.Δ.Π.Χ. είναι αρμόδια να εποπτεύει και να ελέγχει την εφαρμογή και τήρηση των διατάξεων του GDPR και του Ν. 4624/2019 από την Ελληνική Αστυνομία στο μέτρο, που οι δράσεις της αφορούν επεξεργασία προσωπικών δεδομένων, αλλά και να παρέχει σχετικές συμβουλές και οδηγίες όταν αυτό κρίνεται απαραίτητο. Σε περίπτωση δε, που διαπιστώνει παρέκκλιση από τα οριζόμενα στον GDPR και τον Ν. 4624/2019 προβαίνει είτε σε περιορισμό της επεξεργασίας είτε σε επιπλήξεις ή επιβολή διοικητικών προστίμων (Άρθρο 15 του Ν. 4624/2019).

5.2. Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

5.2.1. Εισαγωγή

Με το άρθρο 12 του Ν. 5187/2025 συστάθηκε και λειτουργεί το Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο Αρχηγείο της Ελληνικής Αστυνομίας. Το εν λόγω γραφείο υπάγεται απευθείας στον Αρχηγό της ΕΛ.ΑΣ. και προΐσταται αυτού ο Υπεύθυνος Προστασίας Δεδομένων (Υ.Π.Δ.). Ο τελευταίος είναι αξιωματικός της Ελληνικής Αστυνομίας και ορίζεται με απόφαση του Αρχηγού.

Το Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα παρέχει στο έργο του Υ.Π.Δ. γραμματειακή και διοικητική υποστήριξη. Το συγκεκριμένο γραφείο είναι επανδρωμένο τόσο με πολιτικό όσο και με αστυνομικό προσωπικό, με την προϋπόθεση ότι οι αστυνομικοί, που το απαρτίζουν είναι ιεραρχικά κατώτεροι του Υ.Π.Δ.. Κατά την άσκηση των καθηκόντων του ο Υ.Π.Δ. δεν λαμβάνει εντολές και απευθύνεται απευθείας στον Αρχηγό της ΕΛ.ΑΣ.

5.2.2. Καθήκοντα Υπεύθυνου Προστασίας Δεδομένων

Βασική αποστολή του Υ.Π.Δ. είναι να διευκολύνει την συμμόρφωση των Υπηρεσιών της Ελληνικής Αστυνομίας με τον GDPR και τον Ν. 4624/2019 και να λειτουργεί ως σημείο επαφής μεταξύ των ενδιαφερομένων. Ο ρόλος του Υ.Π.Δ. είναι αποκλειστικά υποστηρικτικός και συμβουλευτικός και δεν φέρει ευθύνη σε περίπτωση που η εκάστοτε αστυνομική Υπηρεσία παραβιάσει τις διατάξεις του GDPR και του Ν. 4624/2019, κατά την εκτέλεση των καθηκόντων της.

Πιο συγκεκριμένα, λαμβάνοντας υπόψη τις διατάξεις του άρθρου 38 του GDPR και του άρθρου 8 του Ν. 4624/2019, ο Υ.Π.Δ. ενημερώνει και παρέχει συμβουλές στις αστυνομικές Υπηρεσίες και στους αρμόδιους υπαλλήλους αναφορικά με τις υποχρεώσεις τους που πηγάζουν από τον GDPR, τον Ν. 4624/2019 και γενικά τις διατάξεις περί προστασίας προσωπικών δεδομένων και εκδίδει σχετικές συστάσεις (Ομάδα εργασίας άρθρου 29, WP243, 2017: 23). Επιπλέον, παρέχει συμβουλευτική υποστήριξη, εφόσον του ζητηθεί, σχετικά με τη διενέργεια εκτίμησης αντικτύπου της εκάστοτε επεξεργασίας στα προσωπικά δεδομένα και παρακολουθεί την εν λόγω διαδικασία κατ' εφαρμογή του άρθρου 35 του GDPR.

Ο Υ.Π.Δ. παρακολουθεί, επίσης, την συμμόρφωση των υπεύθυνων επεξεργασίας με τον GDPR και άλλα κείμενα του ενωσιακού ή εθνικού δικαίου, που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα και την επεξεργασία αυτών, καθώς και με τις πολιτικές που ακολουθούν αναφορικά με την ανάθεση αρμοδιοτήτων, την ενημέρωση του προσωπικού, που συμμετέχει στην επεξεργασία και την ευαισθητοποίησή τους για το έργο, που επιτελούν. Εκτός των προαναφερόμενων, ο Υ.Π.Δ. λειτουργεί ως σημείο επαφής με τις εποπτικές αρχές και ιδίως με την Α.Π.Δ.Π.Χ. για θέματα, που αφορούν την επεξεργασία των δεδομένων, αλλά και για να πραγματοποιεί διαβουλεύσεις, όποτε κρίνεται απαραίτητο (Άρθρο 12 παρ. 3 του Ν. 5187/2025).

Εκ των προαναφερθέντων, γίνεται σαφές ότι σε περίπτωση που προκύψει παραβίαση της σχετικής νομοθεσίας προστασίας δεδομένων, ο Υ.Π.Δ. απευθύνεται στον Αρχηγό της ΕΛ.ΑΣ, προκειμένου να τον ενημερώσει σχετικά και γνωστοποιεί την παραβίαση στην Α.Π.Δ.Π.Χ. εκ μέρους του υπεύθυνου επεξεργασίας – δηλαδή της εκάστοτε αστυνομικής Υπηρεσίας, στην οποία σημειώθηκε η παραβίαση - καθώς λειτουργεί ως σημείο επαφής.

Σε κάθε περίπτωση, ο Υ.Π.Δ. πρέπει να λαμβάνει υπόψη τον κίνδυνο, που ενδέχεται να προκύψει κατά την επεξεργασία των δεδομένων, συνυπολογίζοντας τον σκοπό, τη φύση και το πεδίο εφαρμογής της (Άρθρο 12 παρ. 4 του Ν. 5187/2025).

Τέλος, τόσο ο Υ.Π.Δ. όσο και το προσωπικό, που απαρτίζει το Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Ελληνικής Αστυνομίας είναι υποχρεωμένοι να τηρούν το απόρρητο και την εμπιστευτικότητα, που επιβάλουν οι ενωσιακές και εθνικές διατάξεις προστασίας δεδομένων, κατά την άσκηση των καθηκόντων τους (Άρθρο 12 παρ. 5 του Ν. 5187/2025).

6. Χρήση και επεξεργασία των προσωπικών δεδομένων από την Ελληνική Αστυνομία

Η Ελληνική Αστυνομία, ως δημόσια υπηρεσία, αλλά και ως αρμόδια αρχή, όπως αυτή ορίζεται στο άρθρο 44 του Ν. 4624/2019, χειρίζεται καθημερινά προσωπικά δεδομένα φυσικών προσώπων προς εκπλήρωση της αποστολής της. Πιο συγκεκριμένα, ο χειρισμός αυτός εξυπηρετεί σκοπούς, που συνδέονται με την εξασφάλιση της δημόσιας τάξης και ασφάλειας, την ομαλή κοινωνική συμβίωση των πολιτών, την πρόληψη και καταστολή των εγκληματικών πράξεων, την προστασία του Κράτους και του δημοκρατικού πολιτεύματος καθώς και την αποτροπή παράτυπης εισόδου ή εξόδου αλλοδαπών από τη χώρα²². Στο πλαίσιο αυτό, η Ελληνική Αστυνομία οφείλει να τηρεί και να εφαρμόζει τις διατάξεις του GDPR και της Οδηγίας 2016/680, όπως αυτές έχουν ενσωματωθεί στο ελληνικό δίκαιο με τον Ν. 4624/2019, καθώς και κάθε άλλο νομικό κείμενο που διέπει την προστασία των προσωπικών δεδομένων, προκειμένου οι ενέργειές της να μην παραβιάζουν το συνταγματικά κατοχυρωμένο δικαίωμα της προστασίας προσωπικών δεδομένων.

Δεδομένου ότι το πεδίο δράσης της Ελληνικής Αστυνομίας είναι ιδιαίτερα ευρύ, η παρούσα εργασία περιορίζεται στην ανάλυση συγκεκριμένων περιπτώσεων, κατά τις οποίες η Ελληνική Αστυνομία επεξεργάζεται προσωπικά δεδομένα. Οι περιπτώσεις αυτές επιλέχθηκαν διότι αποτελούν ενδεικτικά, αλλά αντιπροσωπευτικά παραδείγματα επεξεργασίας προσωπικών δεδομένων από την Ελληνική Αστυνομία, τα οποία εκπληρώνουν διαφορετικούς σκοπούς. Περιλαμβάνουν τη συλλογή και διαχείριση τόσο απλών, όσο και ευαίσθητων προσωπικών δεδομένων και καλύπτουν προληπτικές, κατασταλτικές και εν γένει ανακριτικές, αλλά και διοικητικές δράσεις της ΕΛ.ΑΣ.. Ειδικότερα, παρουσιάζεται η ανάλυση DNA, η άρση του απορρήτου ως ειδική ανακριτική πράξη, η δημοσιοποίηση προσωπικών δεδομένων κατηγορουμένων/καταδικασθέντων, η διαχείριση των προσωπικών δεδομένων κατά την έκδοση ταυτοτήτων και διαβατηρίων, η χρήση συστημάτων επιτήρησης σε δημόσιους χώρους, η επεξεργασία των προσωπικών δεδομένων των υποψηφίων ιδιωτών που δηλώνουν συμμετοχή στις εξετάσεις κατάταξης στις Σχολές Αξιωματικών και Αστυφυλάκων, καθώς και η επεξεργασία των δεδομένων στο πλαίσιο διασυνοριακής συνεργασίας της Ελληνικής Αστυνομίας με αρμόδιες αρχές άλλων κρατών μελών. Έτσι, μέσα από την ανάλυση συγκεκριμένων λειτουργιών, διερευνάται ο τρόπος εφαρμογής των βασικών αρχών επεξεργασίας που ορίζουν τα νομικά κείμενα και γεφυρώνεται η νομική θεωρία με την επιχειρησιακή πραγματικότητα.

6.1. Ανάλυση DNA

Το γενετικό αποτύπωμα ή αλλιώς προφίλ DNA, περιλαμβάνει δεδομένα του μη κωδικοποιημένου τμήματος του γενετικού υλικού, τα οποία μπορούν να οδηγήσουν στην ταυτοποίηση του εκάστοτε προσώπου και παρέχουν πληροφορίες σχετικά με το φύλο, τη φυλετική ή εθνοτική προέλευση, τη συγγένεια κ.λπ. του συγκεκριμένου

²² <https://www.astynomia.gr/odigos-tou-politi/prostasia-dedomenon-prosopikou-charaktira/>

ατόμου (Ορφανός, Σ., 2022: 302). Συνεπώς, πρόκειται για προσωπικό δεδομένο, που εντάσσεται στην κατηγορία των ευαίσθητων.

Κάθε άτομο έχει μοναδικό γενετικό προφίλ – DNA, με εξαίρεση τους μονοζυγωτικούς διδύμους (Δημόπουλος, Χ., 2011: 528), το οποίο παραμένει αναλλοίωτο από την εμβρυϊκή ζωή μέχρι και μετά το θάνατο (Χατζηϊωάννου, Κ., 2023: 58). Τα δύο αυτά χαρακτηριστικά έχουν δώσει τη δυνατότητα στις διωκτικές αρχές να αναγνωρίζουν την ταυτότητα των δραστών και γενικότερα των φυσικών προσώπων και κατ' επέκταση να εξιχνιάζουν εγκλήματα μέσα από την ανάλυση DNA (Δημόπουλος, Χ., 2011: 528).

Όπως οι άνθρωποι αφήνουν δακτυλικά αποτυπώματα όταν ακουμπήσουν μία επιφάνεια, έτσι μπορούν να αφήσουν και βιολογικό τους υλικό, όπως για παράδειγμα τρίχες, κηλίδες αίματος, σπέρμα, σάλιο, κ.λπ., το οποίο περιέχει DNA (Ορφανός, Σ., 2021: 28). Σε περίπτωση εγκληματικής πράξης, το DNA που απομονώνεται από βιολογικό υλικό που βρέθηκε στη σκηνή του εγκλήματος συγκρίνεται με το DNA ενός υπόπτου και το αποτέλεσμα της αντιπαραβολής δίνει τη δυνατότητα στις διωκτικές αρχές να συμπεράνουν εάν τα δύο δείγματα DNA προέρχονται από το ίδιο άτομο ή όχι (Δημόπουλος, Χ., 2011: 528). Σε περίπτωση ταύτισης μπορεί να αποδειχθεί με βεβαιότητα ότι ο ύποπτος βρισκόταν στον τόπο του εγκλήματος, χωρίς όμως να σημαίνει απαραίτητα ότι είναι και ο δράστης (Ορφανός, Σ., 2021: 29). Ωστόσο, το DNA μπορεί να χρησιμοποιηθεί και για να αποκλείσει κάποια άτομα από το να είναι ύποπτοι ή ακόμα και για να αθώσει άτομα που έχουν καταδικαστεί, καθώς εάν δεν υπάρχει ταύτιση μεταξύ των δύο δειγμάτων, τότε το συγκεκριμένο πρόσωπο, που θεωρείται ως ύποπτο δεν μπορεί να είναι η πηγή του βιολογικού υλικού, που βρέθηκε επί σκηνής εγκλήματος (Ορφανός, Σ., 2021: 30, 32). Συνεπώς, η ανάλυση DNA διαδραματίζει καθοριστικό ρόλο στο πλαίσιο μίας ποινικής έρευνας για την εξακρίβωση των στοιχείων ταυτότητας του δράστη ενός εγκλήματος (Ορφανός, Σ., 2021: 35).

Κατά την ποινική διαδικασία, η ανάλυση DNA αποτελεί μορφή πραγματογνωμοσύνης, και συνιστά μία σύνθετη διαδικασία, καθώς αποτελείται από επιμέρους υπο-διαδικασίες και συγκεκριμένα τη συλλογή του βιολογικού υλικού και την μετέπειτα αποκωδικοποίηση των ενσωματωμένων σε αυτό δεδομένων μέσω ειδικής εργαστηριακής εξέτασης (Χατζηϊωάννου, Κ., 2023: 26). Η πραγματογνωμοσύνη εν γένει είναι ένα από τα σημαντικότερα αποδεικτικά μέσα, αποβλέπει στην ενίσχυση της κρίσης του δικαστή σε οποιοδήποτε ζήτημα αφορά την ποινική δίκη και απαιτεί ειδικές γνώσεις επιστήμης ή τέχνης, όπως για παράδειγμα η γραφολογική, η ψυχιατρική, η ιατροδικαστική πραγματογνωμοσύνη, η πραγματογνωμοσύνη επί των ψηφιακών πειστηρίων, κ.λπ.. Ιδιαίτερο χαρακτηριστικό της συνιστά το γεγονός ότι αν και αποτελεί ανακριτική πράξη, δεν διενεργείται από δικαστικούς λειτουργούς ή ανακριτικούς υπαλλήλους, αλλά από πρόσωπα ιδιώτες ή από δημόσιους υπαλλήλους, που δεν έχουν σχέση με την απονομή της δικαιοσύνης, οι

οποίοι αποκαλούνται ως όργανα αποδείξεως ή βοηθοί του δικαστή²³ (Χατζηϊωάννου, Κ., 2023: 19-23).

6.1.1. Άρθρο 201 Κ.Π.Δ.

Η πρώτη προσπάθεια ένταξης της ανάλυση DNA στο ελληνικό δίκαιο έλαβε χώρα το 2001 με τον Ν. 2928/2001, ενώ σήμερα αποτυπώνεται στο άρθρο 201 του Κ.Π.Δ.. Ωστόσο, όλα αυτά τα χρόνια μεσολάβησε πλήθος τροποποιήσεων μέχρι να πάρει την τελική μορφή που έχει σήμερα (Μπόκας, Ν., 2023).

Η ανάλυση DNA, ως ειδικότερη μορφή πραγματογνωμοσύνης, προβλέπεται από το άρθρο 201 του Κ.Π.Δ. προκειμένου να εξακριβωθεί η ταυτότητα του δράστη μίας αξιόποινης πράξης. Αρχικά, για να πραγματοποιηθεί η ανάλυση DNA θα πρέπει να πληρούνται σωρευτικά δύο βασικές προϋποθέσεις: πρώτον, θα πρέπει να υπάρχουν αποχρώσεις ενδείξεις ότι ένα άτομο έχει διαπράξει κακούργημα ή πλημμέλημα, για το οποίο προβλέπεται ποινή φυλάκισης τουλάχιστον ενός έτους (Άρθρο 201 παρ. 1 του Κ.Π.Δ.) και δεύτερον, θα πρέπει να βρεθεί στον τόπο του εγκλήματος ή στο σώμα του παθόντος βιολογικό υλικό, που να καθιστά πρόσφορη τη σύγκριση με το DNA του κατηγορουμένου (π.χ. τρίχες, αίμα, σπέρμα, δέρμα) (Χατζηϊωάννου, Κ., 2023: 30). Η λήψη του γενετικού υλικού από τον κατηγορούμενο πραγματοποιείται από τις αστυνομικές αρχές, σύμφωνα με τις οδηγίες της Υποδιεύθυνσης Βιολογικών και Βιοχημικών Εξετάσεων και Αναλύσεων (Άρθρο 55 του Ν. 5187/2025), κατόπιν σχετικής εντολής του αρμόδιου εισαγγελέα ή ανακριτή, σε οποιοδήποτε στάδιο της ποινικής διαδικασίας, δηλαδή είτε κατά τη διεξαγωγή της αυτεπάγγελτης προανάκρισης, είτε στο στάδιο της προκαταρκτικής εξέτασης ή κατά την κύρια ανάκριση, εφόσον αυτός κρίνει ότι μία τέτοια πράξη είναι απολύτως αναγκαία για την εξακρίβωση των στοιχείων ταυτότητας του δράστη (Ορφανός, Σ., 2022: 310). Σε κάθε στάδιο της διαδικασίας πρέπει να διασφαλίζεται απόλυτος σεβασμός στην αξιοπρέπεια του κατηγορουμένου, κατ' εφαρμογή της αρχής της αναλογικότητας. Αν το γενετικό υλικό πρέπει να ληφθεί από απόκρυφα μέρη του σώματος, η παρουσία εισαγγελικού λειτουργού καθίσταται υποχρεωτική (Άρθρο 201 παρ. 1 του Κ.Π.Δ.).

Η ανάλυση του DNA πρέπει να περιορίζεται αποκλειστικά στα στοιχεία, που είναι απολύτως απαραίτητα για την ταυτοποίηση του δράστη, δηλαδή δεν επιτρέπεται η εξέταση και καταγραφή άλλων δεδομένων, όπως πληροφορίες ιατρικές ή φυλετικής φύσης του προσώπου. Επιπλέον, για να είναι αξιοποιήσιμες οι πληροφορίες που θα προκύψουν, διενεργείται σε κρατικό ή πανεπιστημιακό εργαστήριο, επαρκώς εξοπλισμένο, που έχει συσταθεί νομίμως και με υψηλών προδιαγραφών προσωπικό (Δημόπουλος, Χ., 2018: 540), ώστε να εξασφαλίζεται ο αδιάβλητος χαρακτήρας της ανάλυσης και ο περιορισμός των σφαλμάτων (Χατζηϊωάννου, Κ., 2023: 56). Τέτοιο, για παράδειγμα, είναι το Εργαστήριο Ανάλυσης Βιολογικών Υλικών Ατόμων του Τμήματος Εθνικού Αρχείου Δεδομένων Γενετικών Τύπων της Διεύθυνσης Εγκληματολογικών Ερευνών (Δ.Ε.Ε.), το οποίο υπάγεται στην Ελληνική Αστυνομία

²³ Όπως για παράδειγμα γιατροί, ψυχίατροι, μηχανικοί, κ.λπ.

και πραγματοποιεί αναλύσεις DNA από βιολογικό υλικό ατόμων (Άρθρο 55 του Ν. 5187/2025).

Αξίζει να σημειωθεί ότι και ο κατηγορούμενος δικαιούται να ζητήσει την ανάλυση DNA προς υπεράσπισή του. Συνεπώς, σε μία τέτοια περίπτωση οι διωκτικές αρχές, οφείλουν να ικανοποιήσουν το αίτημά του, διαφορετικά προκύπτει απόλυτη ακυρότητα κατ' άρθρο 171 παρ. 1 περ. δ', 2του Κ.Π.Δ. (Δημόπουλος, Χ., 2018: 540). Συγκεκριμένα, απόλυτη ακυρότητα υπάρχει όταν δεν τηρούνται οι διατάξεις που καθορίζουν, μεταξύ άλλων, την υπεράσπιση του κατηγορουμένου και την άσκηση των δικαιωμάτων του, καθώς και όταν αυτός ζητήσει να ασκήσει δικαίωμα που προβλέπει ο νόμος και το δικαστήριο αρνηθεί ή δεν αποφανθεί επί του αιτήματός του.

Το βιολογικό υλικό από τα ίχνη, πειστήρια και αντικείμενα της υπό διερεύνησης υπόθεσης αναλύεται από το Εργαστήριο Ανάλυσης DNA Ιχνών Πειστηρίων του Τμήματος Ανάλυσης Βιολογικών Υλικών της Δ.Ε.Ε., ενώ το βιολογικό υλικό του κατηγορουμένου αναλύεται από το Εργαστήριο Ανάλυσης Βιολογικών Υλικών Ατόμων, που προαναφέρθηκε. Σε περίπτωση που η ανάλυση DNA αποβεί θετική, υπάρξει δηλαδή ταύτιση μεταξύ του δείγματος DNA του κατηγορουμένου και εκείνου που βρέθηκε στον τόπο του εγκλήματος ή στο σώμα του παθόντος, τότε το πόρισμα κοινοποιείται στον κατηγορούμενο και τα γενετικά αποτυπώματα του ατόμου τηρούνται στο ειδικό αρχείο DNA της Δ.Ε.Ε. του Αρχηγείου της Ελληνικής Αστυνομίας, για το οποίο θα γίνει λόγος στη συνέχεια. Τόσο ο κατηγορούμενος όσο και ο εισαγγελέας ή ανακριτής έχουν δικαίωμα να ζητήσουν την επανάληψη της ανάλυσης – και όχι τη λήψη νέου δείγματος DNA²⁴ (Ορφανός, Σ., 2023: 286). Τα γενετικά αποτυπώματα τηρούνται μέχρι να εκδοθεί αμετάκλητο απαλλακτικό βούλευμα ή αμετάκλητη αθωωτική απόφαση ή μέχρι να τεθεί η υπόθεση στο αρχείο. Αν, ωστόσο, προκύψει αντιστοιχία αυτών των γενετικών αποτυπωμάτων με άλλα μη ταυτοποιημένα αποτυπώματα που τηρούνται στο ίδιο αρχείο, τότε η διατήρησή τους συνεχίζεται έως την αμετάκλητη αθώωση του εν λόγω εμπλεκόμενου στις σχετικές υποθέσεις (Άρθρο 201 παρ. 2 του Κ.Π.Δ.). Τα δεδομένα αυτά τηρούνται για την αξιοποίησή τους στο πλαίσιο διερεύνησης είτε ανεξιχνίαστων είτε μελλοντικών εγκλημάτων (Ορφανός, Σ., 2023: 287), και σε κάθε περίπτωση καταστρέφονται με τον θάνατο του υποκειμένου (Άρθρο 201 παρ. 2 του Κ.Π.Δ.). Στο αντίθετο σενάριο, όπου το αποτέλεσμα της ανάλυσης αποβεί αρνητικό, το γενετικό αποτύπωμα καταστρέφεται αμέσως. Μόλις ολοκληρωθεί η ανάλυση, ανεξαρτήτως πορίσματος, το γενετικό υλικό, που ελήφθη από τον κατηγορούμενο, καταστρέφεται αμελλητί (Ορφανός, Σ., 2023: 287).

²⁴ Αν το υποκείμενο των δεδομένων ασκήσει αυτό το δικαίωμα, τότε οφείλει να διορίσει τεχνικό σύμβουλο με δικές του δαπάνες. Ο τεχνικός σύμβουλος μπορεί να παρευρίσκεται κατά τη διεξαγωγή των εργασιών των πραγματογνωμόνων, να αποκτά πρόσβαση στα ίδια έγγραφα και πληροφορίες με αυτούς και να λάβει αντίγραφο της έκθεσης της πραγματογνωμοσύνης. Επιπλέον, μπορεί να ζητήσει να εξετάσει αυτός το πρόσωπο ή το πράγμα που αποτέλεσε αντικείμενο της πραγματογνωμοσύνης, κατόπιν σχετικής του αίτησης και έγκρισης αυτής από το αρμόδιο όργανο (Άρθρο 207 του Κ.Π.Δ.).

Όσον αφορά την καταστροφή του γενετικού αποτυπώματος, το υποκείμενο αυτού ενημερώνεται με οποιοδήποτε μέσο – γραπτώς, ηλεκτρονικά, προφορικά ή τηλεφωνικά - προκειμένου να παραστεί στη διαδικασία καταστροφής με συνήγορο²⁵ και τεχνικό σύμβουλο. Επιφορτισμένος με την υποχρέωση της ενημέρωσης είναι αρμόδιος υπάλληλος της Δ.Ε.Ε., ο οποίος οφείλει να ενημερώσει το ενδιαφερόμενο πρόσωπο τουλάχιστον πέντε μέρες πριν την προγραμματισμένη καταστροφή, συντάσσοντας για αυτή σχετική βεβαίωση (Άρθρο 201 παρ. 3 του Κ.Π.Δ.). Η συγκεκριμένη διάταξη είναι ιδιαίτερα σημαντική διότι θωρακίζει την καταστροφή των γενετικών δεδομένων με σημαντικές δικαστικές εγγυήσεις, ενώ παράλληλα προσφέρει διαφάνεια στην όλη διαδικασία (Ορφανός, Σ., 2022: 287).

Κρίσιμο ζήτημα αποτελεί η περίπτωση κατά την οποία ο κατηγορούμενος δεν συναινεί στη λήψη γενετικού δείγματος και κατ' επέκταση στην ανάλυση DNA. Δεδομένου ότι στο άρθρο 201 παρ. 1 του Κ.Π.Δ. αναφέρεται ρητά ότι είναι υποχρεωτική η λήψη του γενετικού υλικού, αυτό συνεπάγεται και τη δια βίας εκτέλεση της εντολής του αρμόδιου εισαγγελέα ή ανακριτή, καθώς χωρίς αυτή ματαιώνεται το υποχρεωτικό της λήψης, όπως ρητά ορίζει ο νόμος (Δημόπουλος, Χ., 2018: 552). Η δια βίας λήψη γενετικού υλικού προσβάλλει την ανθρώπινη αξιοπρέπεια, επειδή το ανθρώπινο σώμα μετατρέπεται σε αντικείμενο, καθώς ο κατηγορούμενος δεν καλείται να συμπράξει νοητικά στη διαδικασία, δεδομένου ότι το DNA δεν είναι αποτέλεσμα της πνευματικής του υπόστασης. Ωστόσο, οι πράξεις δικονομικού καταναγκασμού, παρ' ότι προσβάλλουν έννομα ατομικά αγαθά, δεν συνιστούν άδικες πράξεις όταν επιχειρούνται σύμφωνα με διατάξεις που προβλέπει ο νόμος, τις οποίες επιτρέπει ή ανέχεται το Σύνταγμα (Δημόπουλος, Χ., 2018: 553) και πάντως στο μέτρο που είναι αναγκαίες και ανάλογες με την διερεύνηση της εκάστοτε υπόθεσης. Εξάλλου η ποινική δίκη εκ της φύσης της έχει καταναγκαστικό χαρακτήρα, συνεπώς οι ανακριτικές πράξεις πρέπει να διενεργούνται ανεξαρτήτως της θέλησης του ατόμου (Γνωμοδότηση 15/2011 του Αρείου Πάγου). Η λήψη γενετικού υλικού δια εξαναγκασμού επιτρέπεται μόνο όταν συντρέχουν σωρευτικά οι εξής προϋποθέσεις:

- η σοβαρότητα του αδικήματος είναι τέτοια που δικαιολογεί την επιβολή του εξαναγκασμού,
- δεν υπάρχει άλλος, λιγότερο επαχθής τρόπος απόκτησης πληροφοριών,
- δεν τίθεται σε κίνδυνο η υγεία του ατόμου,
- υπάρχουν σοβαρές ενδείξεις ενοχής του ατόμου,
- το άτομο δεν πρέπει να υπόκειται σε προσβλητική, ταπεινωτική και εξευτελιστική μεταχείριση από τις αστυνομικές αρχές,
- πρέπει να διασφαλίζονται δικαστικές εγγυήσεις, ώστε η διαδικασία να γίνεται νόμιμα και με σεβασμό στα ανθρώπινα δικαιώματα (Μπόκας, Ν., 2023).

²⁵ Σύμφωνα με το άρθρο 200 του Κ.Π.Δ., αν ο κατηγορούμενος δεν έχει συνήγορο, τότε διορίζεται συνήγορος αυτεπαγγέλτως

Σε κάθε περίπτωση όμως θα πρέπει να λαμβάνονται υπόψη τα ανθρώπινα δικαιώματα και οι ατομικές ελευθερίες, οι οποίες δεν είναι, ούτε μπορεί να είναι απεριόριστες, καθώς σύμφωνα με το Συμβούλιο της Επικρατείας (ΣτΕ) υπόκεινται σε περιορισμούς. Οι περιορισμοί πρέπει να δικαιολογούνται από λόγους δημόσιου συμφέροντος, να βρίσκονται σε λογική συνάφεια με τον σκοπό, που θέλουν να εξυπηρετήσουν και να είναι κατάλληλοι, αποτελεσματικοί και αναγκαίοι για τον σκοπό που τέθηκαν (Μπόκας, Ν., 2023).

6.1.2. Ειδικό αρχείο DNA

Στο πλαίσιο εξιχνίασης εγκλημάτων και αναβάθμισης της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος, η Ευρωπαϊκή Ένωση με την Απόφαση 2008/615/ΔΕΥ (γνωστή ως Απόφαση Prüm) υποχρέωσε τα κράτη μέλη να δημιουργήσουν τράπεζες - αρχεία γενετικών αποτυπωμάτων με στόχο την διασυνοριακή ανταλλαγή των στοιχείων τους (Μήτρου, Α., 2014: 105), όπως αυτή περιγράφεται στην Ενότητα 6.8.

Στην Ελλάδα το ειδικό αρχείο δεδομένων γενετικών τύπων – ειδικό αρχείο DNA τηρείται στη Δ.Ε.Ε. και συγκεκριμένα στο Τμήμα Εθνικού Αρχείου Δεδομένων Γενετικών Τύπων, το οποίο υπάγεται στην Υποδιεύθυνση Βιολογικών και Βιοχημικών Εξετάσεων και Αναλύσεων. Το εν λόγω Τμήμα είναι υπεύθυνο για την οργάνωση και λειτουργία του Ειδικού Αρχείου Γενετικών Τύπων, στο οποίο καταχωρίζονται γενετικά προφίλ ατόμων, για τις ανάγκες της ποινικής έρευνας και τον εντοπισμό αγνώστων δραστών μέσω αταυτοποίητων γενετικών αποτυπωμάτων (Άρθρο 55 παρ. 5 του Ν. 5187/2025).

Αρμόδιος για την εποπτεία του αρχείου είναι αντεισαγγελέας ή εισαγγελέας εφετών, ο οποίος ορίζεται από το Ανώτατο Δικαστικό Συμβούλιο και αναλαμβάνει καθήκοντα που δεν μπορούν να ξεπερνούν τα δύο έτη (Άρθρο 201 παρ. 2 του Κ.Π.Δ.).

6.1.3. Συμπεράσματα

Συνοψίζοντας, η ανάλυση DNA διενεργείται μόνο κατόπιν σχετικής παραγγελίας από εισαγγελέα ή ανακριτή, όταν υπάρχουν σοβαρές ενδείξεις ότι ένα φυσικό πρόσωπο έχει διαπράξει συγκεκριμένα εγκλήματα, με απώτερο σκοπό την ταυτοποίηση του δράστη. Επιπλέον, περιορίζεται στα απολύτως αναγκαία για την ταυτοποίηση του δράστη δεδομένα οπότε δεν περιλαμβάνει πρόσθετες πληροφορίες. Η ανάλυση DNA διενεργείται σε κρατικά και πανεπιστημιακά εργαστήρια και το αποτέλεσμα αυτής κοινοποιείται στο υποκείμενο. Σε περίπτωση που το πόρισμα είναι θετικό, τόσο ο εισαγγελέας ή ανακριτής όσο και ο κατηγορούμενος έχουν δικαίωμα να ζητήσουν την επανάληψη της ανάλυσης. Το γενετικό υλικό καταστρέφεται αμέσως μετά την ανάλυση, ενώ τα γενετικά αποτυπώματα, εάν το αποτέλεσμα της ανάλυσης αποβεί θετικό, τηρούνται στο ειδικό αρχείο DNA της Δ.Ε.Ε., για συγκεκριμένο χρόνο, όπως ορίζει το άρθρο 201 παρ. 2 του Κ.Π.Δ., με σκοπό την εξιχνίαση ανεξιχνίαστων ή μελλοντικών εγκλημάτων, διαφορετικά καταστρέφονται αμέσως. Η εποπτεία του ειδικού αρχείου DNA έχει ανατεθεί σε αντεισαγγελέα ή εισαγγελέα εφετών, ο οποίος ορίζεται με απόφαση του Ανώτατου Δικαστικού Συμβουλίου, συνεπώς οι αρμόδιοι

υπάλληλοι της Δ.Ε.Ε. που διαχειρίζονται το ειδικό αρχείο DNA οφείλουν να ενημερώνουν ανά πάσα στιγμή τον εποπτεύοντα για οποιαδήποτε ενέργεια λαμβάνει χώρα σχετικά με αυτό το αρχείο.

Επομένως, οι ενέργειες που λαμβάνουν χώρα κατά την ανάλυση DNA συμβαδίζουν με την αρχή της νομιμότητας, του σκοπού, της ελαχιστοποίησης, του περιορισμένου χρόνου αποθήκευσης των δεδομένων, της ακρίβειας, της ακεραιότητας και εμπιστευτικότητας και της λογοδοσίας, που προβλέπει η Οδηγία 2016/680. Ωστόσο, στον Κ.Π.Δ. δεν προβλέπεται υποχρεωτική η εξαναγκαστική λήψη DNA, υπό συγκεκριμένους όρους, όπως το να λαμβάνει χώρα μόνο όταν η ταυτοποίηση του δράστη καθίσταται αδύνατη με οποιονδήποτε άλλο ηπιότερο τρόπο ή μέσο, για παράδειγμα με τη λήψη δακτυλικών αποτυπωμάτων, λήψη μαρτυρικών καταθέσεων για περιγραφή και τυχόν αναγνώριση του δράστη, ανάλυση βιντεοληπτικού υλικού από κάμερες ασφαλείας, κ.λπ.. Η παράλειψη αυτή έχει ως αποτέλεσμα να λαμβάνεται εξαναγκαστικά γενετικό υλικό, ακόμα και δια της βίας, κατά παράβαση της αρχής της αναλογικότητας. Σε κάθε περίπτωση θα πρέπει να σταθμίζονται τα δικονομικά δικαιώματα του κατηγορουμένου και ο εξαναγκασμός να επιχειρείται ως το επαχθέστερο μέτρο.

6.2. Άρση του απορρήτου των επικοινωνιών

Όπως προαναφέρθηκε στην Ενότητα 4.6 της παρούσας εργασίας, η άρση του απορρήτου των επικοινωνιών αποτελεί μία ειδική ανακριτική πράξη, που προβλέπεται από τα άρθρα 254 και 255 του Κ.Π.Δ. και συνιστά παρέμβαση στα προσωπικά δεδομένα των ατόμων. Για το λόγο αυτό ενεργοποιείται σε συγκεκριμένες περιπτώσεις αξιόποινων πράξεων. Προς αποφυγή παραβίασης των θεμελιωδών δικαιωμάτων των ατόμων σε βάρος των οποίων πραγματοποιείται η εν λόγω πράξη, αλλά και τυχόν ακυρότητας της διαδικασίας, πρέπει να τηρούνται αυστηρά οι διατάξεις του Ν. 5002/2022.

6.2.1. Τα στοιχεία της επικοινωνίας

Κατά το πέραςμα των ετών έχουν υπάρξει διάφορες αντικρουόμενες απόψεις ως προς τα στοιχεία της επικοινωνίας που προστατεύει το άρθρο 19 του Συντάγματος. Συγκεκριμένα, τόσο το άρθρο 19 του Συντάγματος όσο και ο Ν. 2225/1994, που ίσχυε για την άρση του απορρήτου των επικοινωνιών πριν την θέσπιση του Ν. 5002/2022, δεν όριζαν ρητά αν τα στοιχεία της επικοινωνίας περιορίζονται στο περιεχόμενο της επικοινωνίας αυτό καθ' αυτό ή αν περιλαμβάνουν και τα εξωτερικά στοιχεία αυτής, δηλαδή τα στοιχεία ταυτότητας των επικοινωνούντων, τον τόπο, τον χρόνο, τη διάρκεια της επικοινωνίας, κ.λπ., οπότε επικρατούσε η (σωστή εν τέλει) άποψη ότι υπό την προστασία του απορρήτου περιλαμβάνονται και τα εξωτερικά στοιχεία. Η Α.Δ.Α.Ε. με την υπ' αριθ. 1/2005 γνωμοδότησή της έκρινε ότι όλα τα εξωτερικά στοιχεία της επικοινωνίας προστατεύονται, όπως το περιεχόμενο αυτής και συνεπώς για να χορηγηθούν στις αρμόδιες αρχές πρέπει να τηρείται η προβλεπόμενη εκ του Νόμου διαδικασία άρσης του απορρήτου (Γνωμοδότηση 1/2005 της Α.Δ.Α.Ε.). Αυτό προκύπτει μάλιστα και από το άρθρο 4 του Π.Δ. 47/2005, το οποίο περιγράφει

αναλυτικά όλα τα στοιχεία της επικοινωνίας, περιλαμβανομένων των εξωτερικών στοιχείων, που δύναται να αναφέρονται σε μία διάταξη άρσης του απορρήτου.

Επί του θέματος έχει εκφράσει την άποψή του ο Άρειος Πάγος με σχετικές αποφάσεις και γνωμοδοτήσεις. Ενδεικτικά, στην υπ' αριθ. 2/2017 γνωμοδότηση του Αρείου Πάγου υποστηρίζεται ότι από το απόρρητο δεν προστατεύεται μόνο το περιεχόμενο της επικοινωνίας αλλά και τα εξωτερικά στοιχεία αυτής. Από την άλλη με την υπ' αριθ. 78/2021 Απόφασή του θεωρεί ότι το άρθρο 19 του Συντάγματος περιορίζεται μόνο στο περιεχόμενο της επικοινωνίας, αφήνοντας έξω από την προστατευτική του σφαίρα τα εξωτερικά στοιχεία αυτής και πως η αποκάλυψη των τελευταίων, στο πλαίσιο διακρίβωσης εγκλημάτων, δεν αποτελεί απαγορευμένο αποδεικτικό μέσο.

Με τον Ν. 5002/2022 αποσαφηνίστηκε αυτή η σύγχυση, καθώς τόσο στο άρθρο 4 παρ. 4 περ. δ', όσο και στο άρθρο 6 παρ. 4 περ. ζ', αναφέρεται ρητά ότι αντικείμενο της επικοινωνίας αποτελούν και τα εξωτερικά στοιχεία αυτής και συνεπώς παρέχεται σε αυτά η ίδια προστασία, που παρέχεται για το περιεχόμενο της επικοινωνίας. Ο Ν. 5002/2022 αποτυπώνει επακριβώς και αναλυτικά τη διαδικασία, που πρέπει να τηρούν οι αρμόδιες αρχές στο πλαίσιο άρσης του απορρήτου των επικοινωνιών, η οποία, μάλιστα, διαφοροποιείται όταν πραγματοποιείται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση συγκεκριμένων εγκλημάτων (Άρθρα 4-8 του Ν. 5002/2022).

6.2.2. Άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας

Η άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας, ήτοι για λόγους, που σχετίζονται με την εθνική άμυνα, την κυβερνοασφάλεια, την ενεργειακή ασφάλεια και την εξωτερική πολιτική (Άρθρο 3 του Ν. 5002/2022), προβλέπεται ρητά από το άρθρο 6 του Ν. 5002/2022. Σύμφωνα με αυτό, η Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.) και η Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας της Ελληνικής Αστυνομίας (Δ.Α.Ε.Ε.Β.), μπορούν να υποβάλλουν αίτημα άρσης απορρήτου των επικοινωνιών για τους παραπάνω λόγους, είτε όταν το κρίνουν απαραίτητο είτε όταν ενημερωθούν σχετικά από κάποια δημόσια αρχή (Άρθρο 4 παρ. 1 του Ν. 5002/2022). Το αίτημα υποβάλλεται σε εισαγγελικό λειτουργό και περιλαμβάνει: (α) τους λόγους για τους οποίους υφίσταται κίνδυνος για την εθνική ασφάλεια και αναγκαιότητα για άρση του απορρήτου, (β) τα μέσα επικοινωνίας που αφορά η άρση, (γ) το ακριβές αντικείμενο της άρσης, δηλαδή το περιεχόμενο της επικοινωνίας ή/ και τα εξωτερικά στοιχεία αυτής, (δ) την εδαφική έκταση εφαρμογής και (ε) την χρονική διάρκεια της άρσης, η οποία σε κάθε περίπτωση πρέπει να είναι απολύτως αναγκαία (Άρθρο 4 παρ. 2 του Ν. 5002/2022).

Ο εισαγγελικός λειτουργός αποφασίζει εντός 24 ωρών για την άρση ή όχι του απορρήτου, συντάσσοντας σχετική διάταξη. Σε περίπτωση έγκρισης του αιτήματος για άρση του απορρήτου η διάταξη πρέπει να περιλαμβάνει τα στοιχεία που αναφέρονται στο αίτημα, καθώς και την ημερομηνία έκδοσης της εγκριτικής διάταξης, ενώ σε περίπτωση απόρριψης του σχετικού αιτήματος, η διάταξη πρέπει να περιέχει μόνο την

Υπηρεσία, που αιτήθηκε την άρση και την ημερομηνία έκδοσης της απορριπτικής διάταξης. Επιπλέον, σύμφωνα με το άρθρο 139 του Κ.Π.Δ. η διάταξη θα πρέπει να αιτιολογείται ειδικά και εμπεριστατωμένα, ανεξαρτήτως εάν με αυτή εγκρίνεται ή απορρίπτεται το αίτημα της άρσης. Η εγκριτική διάταξη του εισαγγελικού λειτουργού, συνοδευόμενη από το αίτημα και τα σχετικά έγγραφα που τέθηκαν υπόψη για την αξιολόγηση αυτού, υποβάλλονται σε δεύτερο εισαγγελικό λειτουργό – αντεισαγγελέα του Αρείου Πάγου ή εισαγγελέα Εφετών – ο οποίος, αντίστοιχα, εντός 24 ωρών αποφασίζει για την έγκριση ή απόρριψη του αιτήματος περί άρσης και εν συνεχεία αποστέλλει όλα τα σχετικά έγγραφα στην αιτούσα Υπηρεσία, χωρίς να διατηρεί αντίγραφα αυτών. Ως έναρξη ισχύος ορίζεται η ημερομηνία έγκρισης από τον δεύτερο εισαγγελικό λειτουργό (Άρθρο 4 παρ. 2, 4 και 5 του Ν. 5002/2022).

Η εγκριτική ή απορριπτική διάταξη τηρείται σε ηλεκτρονικό αρχείο της Υπηρεσίας που χειρίζεται την υπόθεση, δηλαδή της Ε.Υ.Π. ή της Δ.Α.Ε.Ε.Β., από τον αρμόδιο εισαγγελικό λειτουργό. Τα φυσικά αρχεία των διατάξεων ψηφιοποιούνται, κατόπιν απόφασης του Διοικητή της Ε.Υ.Π. ή του Διευθυντή της Δ.Α.Ε.Ε.Β., προκειμένου να ενσωματωθούν στο ηλεκτρονικό αρχείο, που προαναφέρθηκε, και μόλις παρέλθει ένα έτος από την ψηφιοποίησή τους, καταστρέφονται. Για την καταστροφή των φυσικών αρχείων συντάσσεται σχετική έκθεση (Άρθρο 4 παρ. 6 του Ν. 5002/2022).

Το άτομο, που είχε τεθεί υπό παρακολούθηση μπορεί να ενημερωθεί για το μέτρο της άρσης του απορρήτου, αφού παρέλθουν τρία έτη από τη λήξη της σχετικής διάταξης περί άρσης του απορρήτου, υπό την προϋπόθεση ότι η ενημέρωση δεν θέτει σε κίνδυνο τον σκοπό, για τον οποίο διατάχθηκε η άρση. Για να γίνει όμως αυτό, πρέπει να έχει υποβληθεί πρώτα σχετικό αίτημα στην Α.Δ.Α.Ε., η οποία στην συνέχεια το προωθεί στην Ε.Υ.Π. και στην Δ.Α.Ε.Ε.Β.. Επί του αιτήματος αποφαινεται τριμελές όργανο, αποτελούμενο από δύο εισαγγελικούς λειτουργούς και τον Πρόεδρο της Α.Δ.Α.Ε. εντός εξήντα ημερών. Σε περίπτωση που γίνει δεκτό, το θιγόμενο πρόσωπο ενημερώνεται για την επιβολή της άρσης και τη διάρκεια αυτής. Πριν παρέλθει ένα έτος από την υποβολή ενός αιτήματος, το υποκείμενο δεν μπορεί να υποβάλει νέο (Άρθρο 4 παρ. 7 του Ν. 5002/2022).

6.2.3. Άρση του απορρήτου των επικοινωνιών για τη διακρίβωση εγκλημάτων

Οι Υπηρεσίες της Ελληνικής Αστυνομίας, κεντρικές και μη, δύναται να αιτηθούν την άρση απορρήτου των επικοινωνιών προκειμένου να εξιχνιάσουν την τέλεση συγκεκριμένων κακουργημάτων και πλημμελημάτων, όπως αυτά ρητά ορίζονται στο άρθρο 6 παρ. 1 και 2 του Ν. 5002/2022 και προαναφέρθηκαν στην Ενότητα 4.6 της παρούσας εργασίας.

Μετά από πρόταση του εισαγγελέα, το αρμόδιο δικαστικό συμβούλιο αποφαινεται επί της άρσης εντός 48 ωρών, εκδίδοντας σχετικό αιτιολογημένο βούλευμα. Κατ' εξαίρεση σε περιπτώσεις, που θεωρούνται ιδιαίτερα επείγουσες, ο εισαγγελέας ή ο ανακριτής μπορούν να διατάζουν απευθείας την άρση του απορρήτου,

οι οποίοι υποχρεούνται, εντός τριών ημερών, να παραπέμψουν την υπόθεση στο αρμόδιο δικαστικό συμβούλιο, το οποίο με τη σειρά του ελέγχει αν πράγματι συντρέχουν λόγοι του κατεπείγοντος. Αν το δικαστικό συμβούλιο κρίνει ότι δεν συντρέχει εξαιρετικά επείγουσα περίπτωση, η διάταξη που εξέδωσε ο εισαγγελέας ή ο ανακριτής παύει να ισχύει αυτοδικαίως. Επιπλέον, εάν εντός πέντε ημερών δεν εκδοθεί βούλευμα για την άρση του απορρήτου, τα ευρήματα που θα προκύψουν από αυτήν είναι μη αξιοποιήσιμα (Άρθρο 6 παρ. 3 του Ν. 5002/2022).

Η διάταξη ή το βούλευμα που εκδίδεται για την άρση του απορρήτου περιλαμβάνει συγκεκριμένα και σαφή στοιχεία. Ειδικότερα, αναφέρονται:

- η αστυνομική υπηρεσία, ο εισαγγελέας ή ο ανακριτής που αιτείται την άρση,
- το αδίκημα που διερευνάται,
- οι σοβαρές ενδείξεις ότι το άτομο, σε βάρος του οποίου ζητείται η άρση, εμπλέκεται στην υπόθεση,
- οι λόγοι επιβολής της άρσης και ότι η περαιτέρω διερεύνηση της υπόθεσης καθίσταται εξαιρετικά δυσχερής έως απίθανη, με οποιοδήποτε άλλο, λιγότερο επαχθές μέτρο,
- ο απώτερος σκοπός αυτής,
- τα μέσα επικοινωνίας, στα οποία θα εφαρμοστεί το συγκεκριμένο μέτρο,
- το αντικείμενο της άρσης και συγκεκριμένα το περιεχόμενο της επικοινωνίας ή/ και τα εξωτερικά στοιχεία αυτής,
- η εδαφική έκταση και η χρονική διάρκεια εφαρμογής, η οποία πρέπει να περιορίζεται στο απολύτως απαραίτητο χρονικό διάστημα,
- η ημερομηνία έκδοσης της διάταξης περί άρσης,
- τα στοιχεία του φυσικού προσώπου σε βάρος του οποίου διατάσσεται η άρση του απορρήτου.

Σε περίπτωση που το σχετικό αίτημα για την άρση του απορρήτου απορριφθεί, τότε βούλευμα ή η διάταξη που εκδίδονται περιλαμβάνουν την αστυνομική Υπηρεσία, τον εισαγγελέα ή τον ανακριτή, που αιτήθηκε την άρση και την ημερομηνία της απορριπτικής διάταξης (Άρθρο 6 παρ. 4 και 5 του Ν. 5002/2022). Είτε πρόκειται για βούλευμα είτε για διάταξη, θα πρέπει να περιλαμβάνεται και σχετική αιτιολόγηση της απόρριψης (Άρθρο 139, 254 του Κ.Π.Δ. και άρθρου 6 παρ. 3 του Ν. 5002/2022).

Εκτός από το άμεσα εμπλεκόμενο στην υπόθεση άτομο, για το οποίο υπάρχουν σοβαρές ενδείξεις ενοχής, η άρση του απορρήτου δύναται να επιβληθεί και κατά τρίτου προσώπου, αμέτοχου στο έγκλημα, προκειμένου να εξακριβωθούν τα πλήρη στοιχεία ταυτότητας του κατηγορουμένου ή ο τόπος κατοικίας του, υπό την προϋπόθεση ότι η ταυτοποίηση και ο εντοπισμός του κατηγορουμένου είναι αδύνατη με οποιονδήποτε άλλο τρόπο (Άρθρο 6 παρ. 6 του Ν. 5002/2022). Σε αυτή την περίπτωση, κάθε πληροφορία, που προκύπτει και αφορά το τρίτο πρόσωπο καταστρέφεται αμελλητί

μόλις επιτευχθεί ο σκοπός της έρευνας. Ωστόσο, εάν από το συλλεχθέν υλικό διαπιστωθεί ότι το τρίτο πρόσωπο έχει τελέσει κακούργημα που σχετίζεται με αδικήματα κατά της ζωής, της σωματικής ακεραιότητας, της προσωπικής ή γενετήσιας ελευθερίας, του πολιτεύματος ή της ακεραιότητας της χώρας, τότε διατηρείται και μπορεί να χρησιμοποιηθεί ως αποδεικτικό μέσο σε δίκη για το συγκεκριμένο αδίκημα (Άρθρο 254 του Κ.Π.Δ.).

Όταν παρέλθει η ημερομηνία ισχύος της διάταξης περί άρσης, ο θιγόμενος έχει δικαίωμα να ενημερωθεί από την Α.Δ.Α.Ε. για την επιβολή του μέτρου της άρσης, αφού πρώτα υποβάλει σχετικό αίτημα. Η Α.Δ.Α.Ε. και εφόσον συμφωνεί ο Εισαγγελέας του Αρείου Πάγου, οφείλει εντός προθεσμίας εξήντα ημερών, να απαντήσει στο αίτημα του ενδιαφερόμενου, υπό την προϋπόθεση ότι με την ενημέρωση δεν συντρέχει κίνδυνος για τον σκοπό για τον οποίο εφαρμόστηκε το συγκεκριμένο μέτρο (Άρθρο 6 παρ. 8 του Ν. 5002/2022).

6.2.4. Διαδικασία της άρσης του απορρήτου

Ένα πολύ ουσιαστικό και καθοριστικής σημασίας άρθρο του Ν. 5002/2022 είναι το άρθρο 8, στο οποίο περιγράφεται η διαδικασία της άρσης του απορρήτου και πιο συγκεκριμένα πως γίνεται, ποιος ενημερώνεται, πώς και πού τηρούνται τα στοιχεία, το χρονικό διάστημα που διαρκεί η άρση, ποιος έχει πρόσβαση στα δεδομένα της άρσης, καθώς και τι ποινές επιβάλλονται σε περίπτωση παραβίασης της προβλεπόμενης από το Νόμο διαδικασίας.

Αφού εκδοθεί το βούλευμα ή η διάταξη, βάσει του οποίου πρόκειται να πραγματοποιηθεί η άρση του απορρήτου των επικοινωνιών, απόσπασμα αυτού αποστέλλεται άμεσα και κρυπτογραφημένα στον επικεφαλής του νομικού προσώπου, στο οποίο ανήκει το επίμαχο μέσο επικοινωνίας, ή σε περίπτωση δημόσιας υπηρεσίας ενημερώνεται επιπλέον ο Υπουργός, στον οποίο αυτή υπάγεται. Ολόκληρο το βούλευμα ή η διάταξη, αποστέλλεται μόνο στην Α.Δ.Α.Ε., κρυπτογραφημένο και σε μορφή, που δεν μπορεί να τροποποιηθεί. Η Α.Δ.Α.Ε. με τη σειρά της το αποθηκεύει σε ειδική βάση δεδομένων, στην οποία έχουν πρόσβαση αποκλειστικά και μόνο ο Πρόεδρος αυτής, καθώς και δύο μέλη της Ολομέλειάς της. Η εξαγωγή δεδομένων από τη βάση συνιστά ποινικά κολάσιμη πράξη, συνεπώς όποιος παραβιάσει αυτή την απαγόρευση, φέρει ποινική ευθύνη (Άρθρο 8 παρ. 1 και 2 του Ν. 5002/2022).

Αξίζει να σημειωθεί, ότι η Ε.Υ.Π. και η Δ.Α.Ε.Ε.Β. διαθέτουν ηλεκτρονικές πλατφόρμες, μέσω των οποίων πραγματοποιείται η αποστολή του κρυπτογραφημένου εγγράφου, που προαναφέρθηκε (Άρθρο 8 παρ. 3 του Ν. 5002/2022). Οι τεχνικές και διαδικαστικές λεπτομέρειες, που αφορούν τη λειτουργία της ηλεκτρονικής πλατφόρμας και την διαδικασία για την παράδοση των διατάξεων, καθορίζονται για την μεν Ε.Υ.Π. με κοινή απόφαση του Διοικητή της και του Υπουργού Δικαιοσύνης, ενώ για τη Δ.Α.Ε.Ε.Β. με κοινή απόφαση των Υπουργών Προστασίας του Πολίτη και Δικαιοσύνης, οι οποίες αποφάσεις δεν δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως (Άρθρο 47 παρ. 1 και 2 του Ν. 5002/2022).

Η άρση του απορρήτου μπορεί να διαρκέσει μέχρι δύο μήνες, ενώ υπάρχει η δυνατότητα χορήγησης παρατάσεων έως δύο μήνες κάθε φορά, με την προϋπόθεση ότι εξακολουθούν να συντρέχουν οι λόγοι της άρσης. Γενικά όμως, η συνολική διάρκεια δεν μπορεί να ξεπεράσει τους δέκα μήνες. Κατ' εξαίρεση και μόνο για λόγους εθνικής ασφάλειας η άρση του απορρήτου μπορεί να υπερβεί τους δέκα μήνες, εφόσον υπάρχουν συγκεκριμένα στοιχεία, που υποδηλώνουν την ύπαρξη σοβαρού και άμεσου κινδύνου για την εθνική ασφάλεια, τα οποία όμως θα πρέπει να επιβεβαιώνονται κάθε φορά που χορηγείται σχετική παράταση. Όταν λήξει η διάρκεια της άρσης ή παρέλθει το ανώτατο επιτρεπόμενο χρονικό όριο, αυτή παύει αυτόματα. Ωστόσο, εάν ο σκοπός της άρσης επιτευχθεί νωρίτερα από το προβλεπόμενο χρονικό διάστημα, τότε διακόπτεται με νέα διάταξη του οργάνου που την επέβαλε (Άρθρο 8 παρ. 4 του Ν. 5002/2022).

Όταν ολοκληρωθεί η διαδικασία της άρσης συντάσσεται σχετική έκθεση από την υπηρεσία που την πραγματοποίησε, στην οποία αναφέρονται οι ενέργειες που έγιναν, ο τόπος, ο χρόνος και ο τρόπος αυτών και το ονοματεπώνυμο των ατόμων, που συμμετείχαν σε αυτή. Στην συνέχεια, αντίγραφα της έκθεσης αποστέλλονται εσωκλειστα σε φάκελο στην αρχή που αιτήθηκε την άρση, στην αρχή που την διέταξε και στην Α.Δ.Α.Ε. (Άρθρο 8 παρ. 5 του Ν. 5002/2022).

Ζητήματα σχετικά με τις ενέργειες, που πραγματοποιούνται στα συστήματα των παρόχων ηλεκτρονικών επικοινωνιών αναφορικά με την διασύνδεση των στοιχείων ταυτοποίησης των συνδρομητών με τα δεδομένα επικοινωνίας τους, καθορίζονται με κοινή πράξη της Α.Π.Δ.Π.Χ. και της Α.Δ.Α.Ε. (Άρθρο 13 του Ν. 3471/2006).

Το νομικό πρόσωπο, στο οποίο ανήκει το μέσο επικοινωνίας, είναι υποχρεωμένο να παρέχει στην αρχή που αιτήθηκε την άρση κάθε πληροφορία και συνδρομή σχετική με τη διάταξη, διαφορετικά τιμωρείται με ποινή φυλάκισης τουλάχιστον 6 μηνών. Σε περίπτωση που υπάλληλος του συγκεκριμένου νομικού προσώπου γνωστοποιήσει σε τρίτους τη διενέργεια της άρσης ή περιεχόμενο αυτής κατά παράβαση της υποχρέωσής του για εχεμύθεια, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο ετών (Άρθρο 8 παρ. 8 του Ν. 5002/2022).

6.2.5. Διαχείριση του υλικού της άρσης

Ο Ν. 5002/2022 προβλέπει διαφορετικό τρόπο διαχείρισης του υλικού, που προκύπτει από την άρση του απορρήτου ανάλογα με το αν αυτή πραγματοποιείται για λόγους εθνικής ασφάλειας ή για λόγους εξιχνίασης αδικημάτων.

6.2.5.1. Για λόγους εθνικής ασφάλειας

Κατόπιν πρότασης της αρμόδιας Υπηρεσίας και έγκρισης του τριμελούς οργάνου, που αποτελείται από δύο εισαγγελικούς λειτουργούς και τον Πρόεδρο της Α.Δ.Α.Ε. (Άρθρο 4 παρ. 7 του Ν. 5002/2022), οι φάκελοι με το σχετικό υλικό τεκμηρίωσης για άρση για λόγους εθνικής ασφάλειας, δύναται να καταστραφούν, υπό την προϋπόθεση ότι έχουν παρέλθει δέκα έτη από την παύση ισχύος της διάταξης βάσει της οποίας έγινε η άρση (Άρθρο 5 παρ.1 του Ν. 5002/2022).

Σε περίπτωση που ο εισαγγελικός λειτουργός κρίνει ότι το υλικό που προέκυψε από το σύστημα επισυνδέσεων²⁶ μπορεί να χρησιμοποιηθεί ως αποδεικτικό μέσο για την άσκηση ποινικής δίωξης, τότε αυτό αντιγράφεται σε υλικό φορέα (π.χ. USB) και διαβιβάζεται με νέα διάταξη στην αρμόδια εισαγγελική υπηρεσία. Με τη διάταξη αυτή ορίζεται, επιπλέον, ότι θα αποσταλεί μόνο το μέρος του υλικού, που έχει αποδεικτική αξία στη διακρίβωση εγκλημάτων, ενώ εκείνο που δεν έχει σχέση με τον λόγο επιβολής της άρσης, καταστρέφεται αμελλητί ενώπιον της αρχής που εξέδωσε τη διάταξη περί άρσης (Άρθρο 5 παρ. 2 και 5 του Ν. 5002/2022).

Αφού παρέλθουν έξι μήνες από την παύση ισχύος της εγκριτικής διάταξης για άρση του απορρήτου, το υλικό που αποτυπώθηκε στο σύστημα επισυνδέσεων, διαγράφεται από αυτό, εκτός εάν η αρμόδια υπηρεσία κρίνει απαραίτητη τη διατήρησή του για συσχέτιση με άλλη, υπό εξέλιξη, έρευνα, ή λόγω χρήσης του ως αποδεικτικό μέσο για την άσκηση ποινικής δίωξης. Κατ' εξαίρεση, το υλικό αυτό μπορεί να διαγραφεί από το σύστημα σε διάστημα μικρότερο των έξι μηνών, κατόπιν γραπτής πρότασης της Ε.Υ.Π. ή της Δ.Α.Ε.Ε.Β.. Όλο το υλικό που έχει εξαχθεί από το σύστημα επισυνδέσεων και έχει αποτυπωθεί σε έγχαρτη μορφή ή υλικό φορέα καταστρέφεται εντός έξι μηνών από την πάροδο ισχύος της διάταξης περί άρσης του απορρήτου, με εξαίρεση τις περιπτώσεις που κρίνεται απαραίτητη η διατήρησή του. Το υλικό που δεν αφορά την υπό διερεύνηση υπόθεση καταστρέφεται απευθείας ενώπιον της αρχής που διέταξε την άρση του απορρήτου. Πάντως, σε κάθε περίπτωση, για την καταστροφή ή διαγραφή του υλικού, είναι απαραίτητη η σύνταξη σχετικής έκθεσης από τον υπάλληλο που τη διενεργεί (Άρθρο 5 παρ. 3-6 του Ν. 5002/2022).

6.2.5.2. Για διακρίβωση εγκλημάτων

Οι πληροφορίες και τα στοιχεία, που προκύπτουν κατά την άρση του απορρήτου στο πλαίσιο διακρίβωσης αδικημάτων, ενσωματώνονται στη δικογραφία, μόνο εάν η αρμόδια αρχή, που διέταξε το μέτρο κρίνει ότι μπορούν να αξιοποιηθούν ως αποδεικτικό υλικό είτε υπέρ είτε κατά του κατηγορουμένου. Ο αρμόδιος εισαγγελέας ή ανακριτής αποφασίζει ποιο τμήμα του συλλεχθέντος υλικού θα ενταχθεί στη δικογραφία, περιορίζοντάς το αποκλειστικά σε εκείνο που συμβάλλει ουσιαστικά στην υπόθεση (Άρθρο 7 παρ.1 του Ν. 5002/2022).

Κάθε πληροφορία, που προκύπτει από την άρση, αξιοποιείται στη δίκη της υπόθεσης για την οποία εκδόθηκε η σχετική διάταξη, υπό την προϋπόθεση ότι πρόκειται για αδίκημα για το οποίο προβλέπεται η ειδική ανακριτική πράξη της άρσης. Κατ' εξαίρεση, κατόπιν απόφασης του δικαστικού συμβουλίου, το υλικό αυτό δύναται να χρησιμοποιηθεί και σε άλλη ποινική διαδικασία για την εξιχνίαση των αδικημάτων, που προβλέπει ο Ν. 5002/2022. Επιπλέον, όταν οι υπό διερεύνηση υποθέσεις αφορούν αξιόποινες πράξεις ατόμων με προνομιακές πληροφορίες και χειραγώγηση της αγοράς ή τον ελεύθερο ανταγωνισμό, το υλικό που έχει συλλεχθεί από την άρση κατά την

²⁶ Σύμφωνα με το άρθρο 2 του Π.Δ. 47/2025, ως επισύνδεση νοείται η σύνδεση τρίτου προσώπου σε δίκτυο επικοινωνιών, ώστε να παρακολουθεί την επικοινωνία που πραγματοποιείται και να λαμβάνει άμεσα τόσο το περιεχόμενο, όσο και στοιχεία αυτής. Επομένως, σύστημα επισυνδέσεων είναι το τεχνικό μέσο που επιτρέπει την προαναφερόμενη διαδικασία.

ποινική διερεύνηση αυτών, μπορεί να χρησιμοποιηθεί με απόφαση του διοικητικού συμβουλίου, κατόπιν αιτήματος της Επιτροπής Κεφαλαιαγοράς και της Επιτροπής Ανταγωνισμού, αντίστοιχα, και ύστερα από πρόταση του αρμόδιου εισαγγελέα, κατά τη διοικητική διαδικασία και για την επιβολή διοικητικών προστίμων (Άρθρο 7 παρ. 2 και 3 του Ν. 5002/2022).

Σε κάθε περίπτωση, εάν εκδοθεί αμετάκλητη απόφαση, αμετάκλητο απαλλακτικό βούλευμα ή εφόσον στο πλαίσιο προκαταρκτικής εξέτασης δεν προκύψει λόγος για άσκηση ποινικής δίωξης, όλα τα στοιχεία και το υλικό, που συλλέχθηκαν από την άρση του απορρήτου καταστρέφονται, χωρίς καθυστέρηση, ενώπιον της αρχής που τη διέταξε και συντάσσεται σχετική έκθεση (Άρθρο 7 παρ. 4 του Ν. 5002/2022).

Αν και γενικά απαγορεύεται η αξιοποίηση των αποδεικτικών μέσων, που έχουν συλλεχθεί στο πλαίσιο της άρσης, κατά παράβαση των διατάξεων του άρθρου 9Α του Συντάγματος, όταν αυτά αποτελούν το μοναδικό αποδεικτικό στοιχείο για την αθώωση του κατηγορουμένου, κάμπτεται ο απόλυτος χαρακτήρας της απαγόρευσης (Παναγοπούλου, Φ., 2023: 54).

Σε κάθε περίπτωση, το υλικό που συλλέγεται από την άρση είτε για λόγους εθνικής ασφάλειας είτε για τη διακρίβωση αξιόποινων πράξεων δεν μπορεί να χρησιμοποιηθεί σε άλλη υπόθεση, για σκοπό διαφορετικό από εκείνον για τον οποίο συλλέχθηκε, καθώς κάτι τέτοιο επισύρει ακυρότητα, πλην των περιπτώσεων που αναφέρθηκαν προηγουμένως.

6.2.6. Συμπεράσματα

Παρ' ότι το απόρρητο των επικοινωνιών αποτελεί ξεχωριστό θεμελιώδες δικαίωμα από αυτό της προστασίας των προσωπικών δεδομένων, υφίσταται στενή λειτουργική σύνδεση μεταξύ τους, καθώς σύμφωνα με το άρθρο 19 παρ. 3 του Συντάγματος, η αξιοποίηση του υλικού, που προκύπτει από την άρση του απορρήτου προϋποθέτει την τήρηση των κανόνων και εγγυήσεων, που διέπουν την προστασία των προσωπικών δεδομένων. Από το ισχύον νομικό πλαίσιο και τις προβλεπόμενες διαδικασίες προκύπτει ότι η άρση του απορρήτου βρίσκεται σε αντιστοιχία με τις βασικές αρχές επεξεργασίας της Οδηγίας 2016/680.

Η Ελληνική Αστυνομία προβαίνει σε άρση του απορρήτου μόνο κατόπιν σχετικής εισαγγελικής διάταξης ή βουλεύματος και μόνο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση εγκλημάτων. Στο αίτημα, που υποβάλλει η ΕΛ.ΑΣ στην αρμόδια εισαγγελική αρχή προσδιορίζει με σαφήνεια το απολύτως αναγκαίο χρονικό διάστημα για το οποίο πρέπει να γίνει άρση, τα μέσα επικοινωνίας, στα οποία πρόκειται να γίνει η άρση και γενικά τα στοιχεία, που είναι απαραίτητα και σχετίζονται με την υπό διερεύνηση υπόθεση. Αφού εκδοθεί η εισαγγελική διάταξη ή το βούλευμα, συλλέγονται και αποθηκεύονται μόνο εκείνα τα στοιχεία, που είναι απαραίτητα και έχουν αποδεικτική αξία για την υπόθεση για την οποία ζητήθηκε, ενώ τα υπόλοιπα καταστρέφονται σύμφωνα με την προβλεπόμενη από το νόμο διαδικασία. Μόνο σε ειδικές περιπτώσεις κατ' εξαίρεση, το συλλεχθέν υλικό μπορεί να χρησιμοποιηθεί και για άλλους σκοπούς ή υποθέσεις (π.χ. κατόπιν απόφασης του δικαστικού συμβουλίου

για την εξιχνίαση των αδικημάτων που προβλέπει ο Ν. 5002/2022). Επιπλέον, τα δεδομένα, που προκύπτουν από την άρση διατηρούνται για συγκεκριμένο χρονικό διάστημα, που ορίζεται ρητά στον Ν. 5002/2022.

Η διαδικασία αυτή διασφαλίζει τη νομιμότητα, την αναλογικότητα, τον περιορισμό του σκοπού, την ακρίβεια, την ασφάλεια των δεδομένων και τον περιορισμό του χρόνου αποθήκευσης των δεδομένων, ενώ η πρόσβαση στο υλικό περιορίζεται σε συγκεκριμένα πρόσωπα. Δεδομένου ότι οποιαδήποτε ενέργεια καταγράφεται και τηρείται φάκελος τεκμηρίωσης, η τήρηση των προβλεπόμενων εγγυήσεων μπορεί να αποδειχθεί ανά πάσα στιγμή, πράγμα που ενισχύει την αξιοπιστία και την συνταγματική νομιμότητα της άρσης. Τέλος, το άτομο σε βάρος, του οποίου επιβάλλεται το μέτρο της άρσης του απορρήτου, δύναται να ενημερωθεί για αυτό, σύμφωνα με τη διαδικασία, που ορίζει ο Ν. 5002/2022.

Επομένως, οι ενέργειες της Ελληνικής Αστυνομίας κατά την επεξεργασία των δεδομένων, στο πλαίσιο της άρσης του απορρήτου, συμβαδίζουν με τις βασικές αρχές επεξεργασίας, που προβλέπει η ενσωματωμένη στον Ν. 4624/2019, Οδηγία 2016/680, καθώς το αυστηρό νομικό πλαίσιο της άρσης είναι απόλυτα συμβατό με αυτές. Έτσι, δεν παραβιάζονται τα θεμελιώδη δικαιώματα των εμπλεκόμενων προσώπων, μεταξύ των οποίων είναι κι αυτό της προστασίας των προσωπικών δεδομένων.

6.3. Δημοσιοποίηση προσωπικών δεδομένων κατηγορουμένων και καταδικασθέντων

Πριν τη θέσπιση του Ν. 4624/2019, το νομικό κείμενο, που ρύθμιζε την προστασία των προσωπικών δεδομένων σε εθνικό επίπεδο ήταν ο Ν. 2472/1997. Όταν τέθηκε σε ισχύ ο Ν. 4624/2019 και συγκεκριμένα με το άρθρο 84 αυτού, καταργήθηκε μεγάλο μέρος του Ν. 2472/1997, πλην ορισμένων διατάξεων, μεταξύ των οποίων εκείνη της δημοσιοποίησης των προσωπικών δεδομένων των ατόμων, στα οποία έχει ασκηθεί ποινική δίωξη ή έχουν καταδικαστεί για συγκεκριμένα αδικήματα. Η συγκεκριμένη διαδικασία αποτυπωνόταν στο άρθρο 2 παρ. β του Ν. 2472/1997 και εφαρμοζόταν συνδυαστικά με το άρθρο 3 παρ. 2 εδ. β' του ίδιου Νόμου. Η διατήρηση αποσπασματικών ρυθμίσεων προκάλεσε σύγχυση ερμηνείας και οδήγησε στην έκδοση εισαγγελικών αποφάσεων περί δημοσιοποίησης προσωπικών δεδομένων κατηγορουμένων ή καταδικασθέντων, στις οποίες, λόγω νομοτεχνικής ασάφειας, μαζί με τη διάταξη του Ν. 2472/1997 που ήταν σε ισχύ, γινόταν εσφαλμένα αναφορά και σε άλλες καταργημένες διατάξεις του Ν. 2472/1997 αντί για τις ισχύουσες ρυθμίσεις του Ν. 4624/2019, ο οποίος έχει ενσωματώσει την Οδηγία 2016/680 και καθιερώνει ένα νέο ειδικό πλαίσιο επεξεργασίας προσωπικών δεδομένων στο πλαίσιο της ποινικής δικαιοσύνης. Λόγω των ανωτέρω και δεδομένου ότι σύμφωνα με τη νομολογία του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου και του Δικαστηρίου της Ευρωπαϊκής Ένωσης οι εθνικές διατάξεις πρέπει να είναι σαφείς και ακριβείς, ειδικά όταν αφορούν περιορισμό των θεμελιωδών δικαιωμάτων των ατόμων, κρίθηκε αναγκαία η θέσπιση μίας νέας διάταξης, η οποία θα ρυθμίζει επακριβώς τη διαδικασία δημοσιοποίησης προσωπικών δεδομένων κατηγορουμένων και καταδικασθέντων (Άρθρο 45 της Αιτιολογικής Έκθεσης του Ν. 5002/2022).

Σε αυτό το πλαίσιο με τον Ν. 5002/2022 τέθηκε σε ισχύ η νέα διάταξη περί δημοσιοποίησης των προσωπικών δεδομένων και φωτογραφιών κατηγορουμένων και καταδικασθέντων, η οποία αποτυπώνεται στο άρθρο 45 του Ν. 5002/2022 και προστέθηκε στον Ν. 4624/2019 με το άρθρο 84Α. Σύμφωνα με αυτή η Ελληνική Αστυνομία, κατόπιν διάταξης του Εισαγγελέα Πρωτοδικών ή Εφετών, δημοσιοποιεί για διάστημα έως έξι μηνών τα στοιχεία ταυτότητας, τη φωτογραφία, καθώς και την ποινική δίωξη κατηγορουμένου ή καταδικασθέντος, που έχει διαπράξει συγκεκριμένα αδικήματα. Ειδικότερα, η πράξη της δημοσιοποίησης λαμβάνει χώρα σε περιπτώσεις κακουργημάτων, πλημμελημάτων των άρθρων 363-353 του Π.Κ. που αφορούν εγκλήματα κατά της γενετήσιας ελευθερίας και εγκλήματα οικονομικής εκμετάλλευσης ζωής, καθώς και πλημμελημάτων για τα οποία προβλέπεται ποινή φυλάκισης τουλάχιστον δύο ετών (Άρθρο 84Α του Ν. 4624/2019). Συνεπώς, οι εισαγγελικές αρχές διαδραματίζουν ρόλο υπεύθυνου επεξεργασίας των δεδομένων, η Ελληνική Αστυνομία εκτελούντος την επεξεργασία, ενώ ο κατηγορούμενος ή καταδικασθείς είναι το υποκείμενο των δεδομένων (Άρθρο 45 της Αιτιολογικής Έκθεσης του Ν. 5002/2022).

Απώτερος σκοπός της δημοσιοποίησης αυτών των στοιχείων είναι η διερεύνηση, εξιχνίαση ή ποινική δίωξη των αξιόποινων πράξεων, που έχει διαπράξει το συγκεκριμένο πρόσωπο και η διευκόλυνση της εκτέλεσης εντάλματος σύλληψης ή καταδικαστικής απόφασης, που έχει εκδοθεί σε βάρος φυσικού προσώπου για τα αδικήματα αυτά (Άρθρο 84Α του Ν. 4624/2019). Πιο συγκεκριμένα, η δημοσιοποίηση των στοιχείων κατηγορουμένου ή καταδικασθέντος, μπορεί να συμβάλλει στην αναγνώριση αυτού από άλλα θύματα της ίδιας υπόθεσης, που πιθανόν να κινητοποιηθούν και να καταθέσουν για αυτή, ή να αναγνωρισθεί ο κατηγορούμενος ή καταδικασθείς από θύματα άλλων προγενέστερων ανεξιχνίαστων υποθέσεων. Επιπλέον, σε περίπτωση που έχει εκδοθεί ένταλμα σύλληψης σε βάρος του ατόμου, του οποίου δημοσιοποιούνται τα στοιχεία, η δημοσιοποίηση συμβάλλει στον εντοπισμό και τη σύλληψή του, για την εκτέλεση του εντάλματος. Τέλος, η δημοσιοποίηση, αποβλέπει στην αποτροπή ενδεχόμενης απειλής της δημόσιας ασφάλειας, αλλά και στην προστασία του κοινωνικού συνόλου από τα συγκεκριμένα ή παρεμφερή εγκλήματα²⁷.

Προκειμένου η αρμόδια εισαγγελική αρχή να εκδώσει διάταξη για δημοσιοποίηση στοιχείων, η αρμόδια αρχή, όπως αυτή ορίζεται στο άρθρο 44 του Ν. 4624/2019, υποβάλει σχετικό αίτημα. Έτσι, στο πλαίσιο προανάκρισης υποβάλει το αίτημα η Ελληνική Αστυνομία και πιο συγκεκριμένα η Υπηρεσία, που επιλαμβάνεται της υπόθεσης, ενώ όταν διενεργείται κύρια ανάκριση, το αίτημα υποβάλλεται από τον ανακριτή. Η εκδοθείσα εισαγγελική διάταξη περιλαμβάνει τα στοιχεία ταυτότητας του υποκειμένου, τη φωτογραφία του, την ποινική δίωξη που του ασκήθηκε ή την καταδίκη, αλλά και πραγματικά περιστατικά της υπόθεσης, που κρίνονται αναγκαία,

²⁷ <https://www.astynomia.gr/dimosiopoisi-me-eisangelikes-diataxeis-fotografion-stoicheion-taftotitas-kai-arithmon-epikoinonias-me-tis-astynomikes-arches-gia-sovares-ypotheseis-gia-tis-opoies-ziteitai-i-voitheia-ton-politon/>

τον στόχο, σκοπό, τρόπο και τα μέσα της δημοσιοποίησης, καθώς και το χρονικό διάστημα, που αυτά θα παραμείνουν δημοσιοποιημένα και θα αναπαράγονται (Άρθρο 84Α του Ν. 4624/2019).

Κατά τη δημοσιοποίηση των προσωπικών δεδομένων κατηγορουμένων, πέραν των γενικών προϋποθέσεων, πρέπει να λαμβάνεται επιπλέον υπόψη το τεκμήριο της αθωότητας, που κατοχυρώνεται στο άρθρο 6 παρ.2 της Ε.Σ.Δ.Α., αλλά και στο άρθρο 71 του Κ.Π.Δ., σύμφωνα με το οποίο οι κατηγορούμενοι θεωρούνται αθώοι μέχρι να αποδειχθεί νομίμως η ενοχή τους. Συνεπώς, θα πρέπει να αναφέρεται ρητά ότι το φυσικό πρόσωπο φέρει την ιδιότητα του κατηγορουμένου, για να μην του αποδίδεται αυθαίρετα η επιβαρυντική ιδιότητα του καταδικασθέντος.

Όπως προαναφέρθηκε η δημοσιοποίηση δεν μπορεί να υπερβαίνει τους έξι μήνες. Συνεπώς, μόλις παρέλθει το χρονικό διάστημα, που έχει οριστεί για τη δημοσιοποίηση, παύει αυτόματα η ισχύς της εισαγγελικής διάταξης. Σε περίπτωση δε, που ο σκοπός αυτής επιτευχθεί σε χρονικό διάστημα μικρότερο από το ορισθέν, τότε η αρμόδια εισαγγελική αρχή ανακαλεί την εκδοθείσα διάταξη με νέα, την οποία η Ελληνική Αστυνομία εκτελεί αμέσως (Άρθρο 84Α του Ν. 5002/2022).

Από τη στιγμή, που η εισαγγελική διάταξη ανακοινωθεί στον κατηγορούμενο ή καταδικασθέντα, αυτός έχει δικαίωμα εντός δύο ημερών να ασκήσει προσφυγή ενώπιον του Προϊσταμένου της Εισαγγελίας Πρωτοδικών, ή, αν η υπόθεση εκκρεμεί στο Εφετείο, ενώπιον του Προϊσταμένου της Εισαγγελίας Εφετών. Σε κάθε περίπτωση, ο αρμόδιος Προϊστάμενος οφείλει να αποφανθεί επί της προσφυγής εντός δύο ημερών. Ωστόσο, μέχρι να εκδοθεί η απόφασή του δεν επιτρέπεται ούτε να εκτελεστεί η αρχική διάταξη ούτε να δημοσιοποιηθούν τα προσωπικά δεδομένα του φυσικού προσώπου. Η μόνη περίπτωση που δεν ισχύει αυτό και η εισαγγελική διάταξη εκτελείται αμέσως είναι τα κακουργήματα της εγκληματικής οργάνωσης (άρθρο 187 Π.Κ.), των τρομοκρατικών πράξεων και τρομοκρατικής οργάνωσης (άρθρο 187Α Π.Κ.), της αξιόποινης υποστήριξης²⁸ (άρθρο 187Β Π.Κ.), τα εγκλήματα κατά της γενετήσιας ελευθερίας και οικονομικής εκμετάλλευσης της γενετήσιας ζωής (άρθρα 336-353 Π.Κ.), καθώς και οι κακουργηματικές πράξεις βίας, στις οποίες ο αρμόδιος εισαγγελέας κρίνει ότι ο δράστης είναι ιδιαίτερα επικίνδυνος για τη δημόσια τάξη και ασφάλεια και διαφεύγει τη σύλληψη. Σε αυτή την περίπτωση, η διάταξη, εάν έχει εκδοθεί από τον Εισαγγελέα Πρωτοδικών πρέπει να επικυρωθεί εντός 24 ωρών από τον Εισαγγελέα Εφετών, διαφορετικά, μόλις παρέλθει το εν λόγω χρονικό διάστημα, παύει η ισχύς της αυτοδικαίως (Άρθρο 84Α του Ν. 5002/2022).

Η Ελληνική Αστυνομία δημοσιοποιεί τα προσωπικά δεδομένα των κατηγορουμένων και καταδικασθέντων στην επίσημη ιστοσελίδα της (www.astynomia.gr), στην οποία έχει ελεύθερη πρόσβαση οποιοδήποτε άτομο. Όπως εύκολα μπορεί να παρατηρήσει κανείς, σε κάθε δημοσίευση εκτός από τα προσωπικά στοιχεία και τις φωτογραφίες του εμπλεκόμενου προσώπου, αναφέρεται η ημερομηνία

²⁸ Ως αξιόποινη υποστήριξη νοείται η παροχή πληροφοριών ή μέσων, που διευκολύνουν την δράση εγκληματικών ή τρομοκρατικών οργανώσεων κατά τη διάπραξη κακουργημάτων (Άρθρο 187Β της Αιτιολογικής Έκθεσης του Π.Κ.)

αυτής, η εισαγγελική αρχή που εξέδωσε την απόφαση, οι αξιόποινες πράξεις για τις οποίες ασκήθηκε ποινική δίωξη ή καταδικάστηκε το συγκεκριμένο πρόσωπο, ο σκοπός της δημοσιοποίησης, η ημερομηνία μέχρι την οποία θα παραμείνουν δημοσιοποιημένα τα στοιχεία του, αλλά και η Υπηρεσία και το τηλέφωνο επικοινωνίας αυτής, που επιλήφθηκε της υπόθεσης. Τυχόν διατήρηση ή/και αναπαραγωγή των ως άνω δημοσιευμένων πληροφοριών απαγορεύεται από οποιονδήποτε μετά το πέρας του ορισθέντος χρονικού διαστήματος δημοσιοποίησης.

6.3.1. Συμπεράσματα

Η Ελληνική Αστυνομία, ως εκτελών την επεξεργασία, δεν δημοσιοποιεί ανεξέλεγκτα και αυτοβούλως τα προσωπικά στοιχεία, τις φωτογραφίες και την ποινική δίωξη ή καταδίκη φυσικών προσώπων, παρά μόνο κατόπιν σχετικής εισαγγελικής διάταξης και για συγκεκριμένο χρονικό διάστημα, κατ' εφαρμογή των αρχών της νομιμότητας και της περιόδου αποθήκευσης.

Προς διασφάλιση των αρχών της ελαχιστοποίησης των δεδομένων και του σκοπού, δημοσιοποιούνται μόνο τα απολύτως απαραίτητα δεδομένα που ορίζει ο νόμος και η δημοσιοποίηση λαμβάνει χώρα μόνο όταν αυτό κρίνεται απαραίτητο για τους σκοπούς και υπό τις προϋποθέσεις, που αναφέρθηκαν στο παρόν κεφάλαιο.

Τα προσωπικά δεδομένα, που δημοσιοποιούνται είναι ακριβή και επικαιροποιημένα για την ορθή ενημέρωση του κοινού και αναφέρεται ρητά εάν το πρόσωπο που αφορούν είναι κατηγορούμενος ή καταδικασθείς, καθώς και τα αδικήματα που έχει διαπράξει, ενώ σε περίπτωση σφάλματος ή αλλαγής αυτών διορθώνονται άμεσα. Επιπλέον, στο πλαίσιο της αρχής της ακεραιότητας και εμπιστευτικότητας η δημοσιοποίηση λαμβάνει χώρα μέσω της επίσημης ιστοσελίδας της Ελληνικής Αστυνομίας και απαγορεύεται οποιαδήποτε μη εξουσιοδοτημένη επεξεργασία σε αυτή.

Τέλος, δεδομένου, ότι στη δημοσιοποίηση αναφέρεται ρητά η ημερομηνία αυτής, η εισαγγελική αρχή που την διέταξε, το χρονικό διάστημα που έχει οριστεί για τη δημοσιοποίηση και ο σκοπός αυτής, μπορεί να αποδειχθεί, ανά πάσα στιγμή ότι οι αναρτήσεις στην ιστοσελίδα της ΕΛ.ΑΣ., που αφορούν τη δημοσιοποίηση στοιχείων κατηγορουμένων ή καταδικασθέντων είναι σύμφωνες με τις βασικές αρχές επεξεργασίας δεδομένων που προβλέπει ο GDPR και ο Ν. 4624/2019.

6.4. Έκδοση αστυνομικού δελτίου ταυτότητας

Κάθε Έλληνας πολίτης που κατοικεί μόνιμα ή προσωρινά στην Ελλάδα και έχει συμπληρώσει το 12^ο έτος της ηλικίας του είναι υποχρεωμένος να εκδώσει αστυνομικό δελτίο ταυτότητας (Α.Δ.Τ.) (Άρθρο 1 του Ν.Δ. 127/1969). Το Α.Δ.Τ. αποτελεί επίσημο έγγραφο, με το οποίο πιστοποιείται η ταυτότητα ενός ατόμου. Το έργο της έκδοσης Α.Δ.Τ. έχουν αναλάβει αστυνομικές Υπηρεσίες και συγκεκριμένα τα Τμήματα ή Υποδιευθύνσεις Δίωξης και Εξιχνίασης Εγκλημάτων, ενώ σε περιοχές που δεν υφίσταται τέτοια Υπηρεσία, η ταυτότητα εκδίδεται από το Αστυνομικό Τμήμα της περιοχής (Άρθρο 1 της Υ.Α. 8200/0-297647/2018).

αυτή, για να την ανακτήσει ο αστυνομικός υπάλληλος (Άρθρο 6 της Υ.Α. 8200/0-297647/2018).

Επιπλέον, ο ενδιαφερόμενος συμπληρώνοντας στην αίτηση – υπεύθυνη δήλωση, που παρατίθεται στη συνέχεια και υπόδειγμα της οποίας είναι αναρτημένο στο ΦΕΚ 2687/Β/30-5-2025, τα προσωπικά του στοιχεία και συγκεκριμένα το ονοματεπώνυμο του ίδιου, του πατέρα του και της μητέρας του, την ημερομηνία και τον τόπο γέννησής του, τον αριθμό του Α.Δ.Τ. που ήδη κατέχει (αν δεν εκδίδει Α.Δ.Τ. για πρώτη φορά), το τηλέφωνό του, τη διεύθυνση κατοικίας του και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του, δηλώνει αφενός την ορθότητα των προσωπικών του στοιχείων, αφετέρου την επιθυμία και συναίνεσή του η αστυνομική Υπηρεσία να αναζητήσει αυτεπαγγέλτως τα στοιχεία, που απαιτούνται για το (νέο) Α.Δ.Τ. στο Πληροφοριακό Σύστημα «Μητρώο Πολιτών». Ωστόσο, σε περίπτωση αδυναμίας σύνδεσης στο εν λόγω σύστημα, η αστυνομική Υπηρεσία αναζητά αυτεπαγγέλτως τα απαραίτητα στοιχεία από πιστοποιητικό του Δήμου όπου είναι εγγεγραμμένο το άτομο (Άρθρο 6 της Υ.Α. 8200/0-297647/2018).

 ΑΙΤΗΣΗ - ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ (άρθρο 8 Ν. 1599/1986 και άρθρο 3 παρ. 3 Ν.2690/1999)							
Η ακρίβεια των στοιχείων που υποβάλλονται με αυτή τη δήλωση μπορεί να ελεγχθεί με βάση το αρχείο άλλων υπηρεσιών (άρθρο 8 παρ.4 Ν. 1599/1986) Περιγραφή Αιτήματος: Αυτεπάγγελτη αναζήτηση των στοιχείων δημοτολογίου από το Πληροφοριακό Σύστημα «Μητρώο Πολιτών» ή το Δημοτολόγιο του οικείου Δήμου και αυτεπάγγελτη αναζήτηση του Προσωπικού Αριθμού από το Μητρώο Προσωπικού Αριθμού, κατ' εφαρμογή των Ν.4727/2020, Ν.2690/1999 και Ν.3242/2004, για την έκδοση Δελτίου Ταυτότητας.							
Προς:				ΗΜΕΡΟΜΗΝΙΑ			
ΣΤΟΙΧΕΙΑ ΑΙΤΟΥΝΤΟΣ							
Ο-Η Όνομα:				Επώνυμο:			
Όνομα Πατέρα:				Επώνυμο Πατέρα:			
Όνομα Μητέρας:				Επώνυμο Μητέρας:			
Ημερομηνία γέννησης:				Τόπος Γέννησης:			
Αριθ. Δελτ. Ταυτότητας:				Τηλέφωνο Επικοινωνίας:			
Τόπος Κατοικίας:		Οδός:		Αριθ:		ΤΚ:	
Δ/ση Ηλεκτρ. Ταχυδρομείου (E-mail):							
Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις, που προβλέπονται από τις διατάξεις της παρ.6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι τα ανωτέρω στοιχεία και οι απαντήσεις επί των κάτωθι ερωτημάτων είναι ακριβή και επιθυμώ την αυτεπάγγελτη αναζήτηση των δημοτολογικών μου στοιχείων από το Πληροφοριακό Σύστημα «Μητρώο Πολιτών» ή το Δημοτολόγιο του οικείου Δήμου και του Προσωπικού Αριθμού μου από το Μητρώο Προσωπικού Αριθμού, κατ' εφαρμογή των Ν.4727/2020, Ν.2690/1999 και Ν.3242/2004, για την έκδοση Δελτίου Ταυτότητας.							
Έλεγχος Ταυτοπροσωπίας							
A/A	Ερώτηση	Απάντηση					
1							
2							
3							
Ο/Η Δηλ							

Εικόνα 3: Αίτηση - Υπεύθυνη δήλωση

Εκτός από τα παραπάνω, η αστυνομική Υπηρεσία συμπληρώνει την αίτηση έκδοσης – αντικατάστασης Α.Δ.Τ., η οποία παρέχεται στο ΦΕΚ 2687/Β/30-5-2025, βάσει των στοιχείων του ατόμου, που έχουν προκύψει από το Πληροφοριακό Σύστημα «Μητρώο Πολιτών» ή το πιστοποιητικό του Δήμου και στην συνέχεια ο ενδιαφερόμενος, αφού ελέγξει την ορθότητα αυτών, την υπογράφει (Άρθρο 6 της Υ.Α. 8200/0-297647/2018). Στην αίτηση έκδοσης – αντικατάστασης Α.Δ.Τ. αναγράφονται με ελληνικούς και λατινικούς χαρακτήρες το ονοματεπώνυμο του ενδιαφερόμενου και των γονέων του, η ημερομηνία, ο τόπος και η χώρα γέννησής του, ο δήμος εγγραφής, ο αριθμός δημοτολογίου, το φύλο, η διεύθυνση κατοικίας του, η ιθαγένειά του, το ύψος, το τηλέφωνο και ο προσωπικός του αριθμός.

Αίτηση έκδοσης - αντικατάστασης δελτίου			
ΦΩΤΟΓΡΑΦΙΑ	ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ ΓΕΝ. Δ/ΝΣΗ ΑΣΦΑΛΕΙΑΣ & ΑΣΤΥΝΟΜΕΥΣΗΣ / ΔΙΕΥΘΥΝΣΗ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΚΡΑΤΟΥΣ ΑΙΤΗΣΗ ΕΚΔΟΣΗΣ ΔΕΛΤΙΟΥ ΤΑΥΤΟΤΗΤΑΣ – ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ (Συμπληρώνεται από την Αρχή Έκδοσης)		
	ΑΡΙΘΜΟΣ ΑΙΤΗΣΗΣ (Συμπληρώνεται Αυτόματα με την ολοκλήρωση)	ΑΡΧΗ ΕΚΔΟΣΗΣ: (Συμπληρώνεται Αυτόματα) ΗΜΕΡΟΜΗΝΙΑ: (Συμπληρώνεται Αυτόματα) ΑΡΙΘΜΟΣ ΠΑΡΑΒΟΛΟΥ ΕΚΔΟΣΗΣ: (Συμπληρώνεται Αυτόματα)	
ΕΠΩΝΥΜΟ			
SURNAME			
ΟΝΟΜΑ			
NAME			
ΟΝΟΜΑ ΠΑΤΕΡΑ			
FATHER'S NAME			
ΕΠΩΝΥΜΟ ΠΑΤΕΡΑ			
ΟΝΟΜΑ ΜΗΤΕΡΑΣ			
MOTHER'S NAME			
ΕΠΩΝΥΜΟ ΜΗΤΕΡΑΣ			
ΤΟΠΟΣ ΓΕΝΝΗΣΗΣ	ΧΩΡΑ ΓΕΝΝΗΣΗΣ (ΛΙΣΤΑ ΙΣΑΟ)		
PLACE OF BIRTH			
ΗΜ. ΓΕΝΝΗΣΗΣ	ΦΥΛΟ / SEX	ΟΜ. ΑΙΜΑΤΟΣ	
ΔΗΜΟΣ ΕΓΓΡΑΦΗΣ		ΥΨΟΣ	
ΑΡ. ΔΗΜΟΤΟΛΟΓΙΟΥ	ΙΘΑΓΕΝΕΙΑ	ΕΛΛΗΝΙΚΗ / GRC (προεκτυπωμένο)	
ΔΙΕΥΘ. ΚΑΤΟΙΚΙΑΣ		T.K.	
ΠΟΛΗ ΚΑΤΟΙΚΙΑΣ		ΤΗΛΕΦΩΝΟ	
e-MAIL		ΠΡΟΣΩΠΙΚΟΣ ΑΡ.	
Με ατομική ευθύνη και γνωρίζοντας τις κυρώσεις που προβλέπονται από τις διατάξεις της παραγράφου 6 του άρθρου 22 του Ν. 1599/1986 παρακαλώ να μου χορηγήσετε δελτίο ταυτότητας λόγω: (ΑΡΧΙΚΗΣ ΕΚΔΟΣΗΣ, ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ ΠΑΛΑΙΟΥ ΤΥΠΟΥ, ΑΠΡΑΞΙΑΣ, ΚΛΟΠΗΣ, ΦΘΟΡΑΣ, ΜΕΤΑΒΟΛΗΣ ΣΤΟΙΧΕΙΩΝ, ΛΗΨΗΣ ΙΣΧΥΟΣ, ΑΝΑΓΡΑΦΗΣ ΠΡΟΣΩΠΙΚΟΥ ΑΡΙΘΜΟΥ), του υπ' αριθ. δελτίου ταυτότητας.			
ΥΠΟΓΡΑΦΗ ΑΙΤΟΥΝΤΟΣ			
	(ΧΕΙΡΟΓΡΑΦΗ)	(ΑΠΟ SIGNATURE PAD)	
ΕΠΩΝΥΜΟ ΜΑΡΤΥΡΑ			
ΟΝΟΜΑ ΜΑΡΤΥΡΑ			
ΑΡΙΘΜΟΣ ΕΓΓΡΑΦΟΥ	ΕΙΔΟΣ ΕΓΓΡΑΦΟΥ		
ΒΕΒΑΙΩΝΩ ΤΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΑΝΩΤΕΡΩ ΕΝΔΙΑΦΕΡΟΜΕΝΟΥ ΚΑΙ ΕΙΚΟΝΙΖΟΜΕΝΟΥ			
ΥΠΟΓΡΑΦΗ ΜΑΡΤΥΡΑ			
ΛΗΨΗ ΔΑΚΤΥΛΙΚΩΝ ΑΠΟΤΥΠΩΜΑΤΩΝ			
ΔΕΞΙΟΣ ΔΕΙΚΤΗΣ	ΑΡΙΣΤΕΡΟΣ ΔΕΙΚΤΗΣ		
(Συμπληρώνεται Αυτόματα το δάκτυλο και το ποσοστό %)	(Συμπληρώνεται Αυτόματα το δάκτυλο και το ποσοστό %)		
ΠΡΟΣΩΡΙΝΗ ΑΔΥΝΑΜΙΑ	ΜΟΝΙΜΗ ΑΔΥΝΑΜΙΑ		
(Συμπληρώνεται Αυτόματα βάσει επιλογής στην εφαρμογή Βιομετρικών)	(Συμπληρώνεται Αυτόματα βάσει επιλογής στην εφαρμογή Βιομετρικών)		
ΕΛΕΓΧΕΤΑΙ ΚΑΙ ΒΕΒΑΙΩΝΕΤΑΙ Η ΑΚΡΙΒΕΙΑ ΤΩΝ ΣΤΟΙΧΕΙΩΝ ΤΗΣ ΑΙΤΗΣΗΣ			
Ο ΠΑΡΑΛΑΒΟΝ	(ΟΝΟΜΑΤΕΠΩΝΥΜΟ/ΒΑΘΜΟΣ)		(ΥΠΟΓΡΑΦΗ)
Ο ΔΙΟΙΚΗΤΗΣ	(ΟΝΟΜΑΤΕΠΩΝΥΜΟ/ΒΑΘΜΟΣ)		(ΥΠΟΓΡΑΦΗ)

Εικόνα 4: Αίτηση έκδοσης - αντικατάστασης δελτίου ταυτότητας

Εάν το άτομο, που πρόκειται να εκδώσει Α.Δ.Τ. επιθυμεί να αναγράφεται σε αυτό η ομάδα και το RHESUS του αίματός του, οφείλει να προσκομίσει έγγραφο από νοσηλευτικό ίδρυμα ή υγειονομικό εργαστήριο ή ακόμα και κάρτα αιμοδότη, όπου να αναγράφονται αυτά τα στοιχεία. Σε περίπτωση δε, που φέρει δερματοστιξία στο πρόσωπο, δηλαδή τατουάζ, απαιτείται ιατρικό έγγραφο από το οποίο να προκύπτει η μονιμότητα αυτής (Άρθρο 6 της Υ.Α. 8200/0-297647/2018).

6.4.2. Επεξεργασία και διατήρηση προσωπικών δεδομένων

Για την έκδοση Α.Δ.Τ. λαμβάνονται δύο δακτυλικά αποτυπώματα από τον ενδιαφερόμενο, ένα από κάθε δείκτη, τα οποία μαζί με τον προσωπικό αριθμό, τη φωτογραφία και τα στοιχεία της μηχανικώς αναγνώσιμης ζώνης, αποθηκεύονται στο ηλεκτρονικό μέσο αποθήκευσης, που είναι ενσωματωμένο στο Α.Δ.Τ. (Άρθρο 3 παρ. 4 της Υ.Α. 8200/0-297647/2018). Η φωτογραφία και τα δακτυλικά αποτυπώματα αποτελούν ευαίσθητα προσωπικά δεδομένα και συλλέγονται προκειμένου να ενσωματωθούν στον μικροεπεξεργαστή (τσιπ) του Α.Δ.Τ., ώστε να διασφαλίζεται η

γνησιότητα, ακεραιότητα και εμπιστευτικότητα των δεδομένων, αλλά και η γνησιότητα του Α.Δ.Τ..

Η λήψη των δακτυλικών αποτυπωμάτων πραγματοποιείται από τον εξουσιοδοτημένο για την έκδοση του Α.Δ.Τ. αστυνομικό υπάλληλο με ειδικό, ηλεκτρονικό εξοπλισμό, που χρησιμοποιείται αποκλειστικά για αυτό τον σκοπό. Αν ωστόσο υπάρχει μόνιμη ή προσωρινή βλάβη στον δείκτη, λαμβάνεται αποτύπωμα από τον αντίχειρα, μέσο ή παράμεσο κατά σειρά, ενώ αν πρόκειται για μονόχειρα λαμβάνεται αποτύπωμα και από δεύτερο δάκτυλο του ίδιου χεριού με την ίδια σειρά, που προαναφέρθηκε. Οποιαδήποτε αδυναμία λήψης δακτυλικού αποτυπώματος θα πρέπει να αποδεικνύεται με ιατρικό έγγραφο, πλην των περιπτώσεων εμφανούς ακρωτηριασμού (Άρθρο 3 της Υ.Α. 8200/0-297647/2018). Μάλιστα, στην περίπτωση αδυναμίας λήψης δακτυλικού αποτυπώματος η διάρκεια ισχύος του δελτίου ταυτότητας περιορίζεται στους 12 μήνες, σε αντίθεση με τα 10 χρόνια που ισχύει κανονικά³¹. Με την πάροδο 90 ημερών από την έκδοση του Α.Δ.Τ., τα δακτυλικά αποτυπώματα διαγράφονται με αυτοματοποιημένο τρόπο (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Η αστυνομική Υπηρεσία αφού συγκεντρώσει την αίτηση και όλα τα απαραίτητα δικαιολογητικά για την έκδοση του ΑΔΤ, τα οποία περιλαμβάνουν απλά και ευαίσθητα προσωπικά δεδομένα, ελέγχει την ορθότητα και γνησιότητα αυτών και στη συνέχεια τα αποστέλλει σε ψηφιακή μορφή στη Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας (Δ.Δ.Ε.Α.), η οποία είναι αρμόδια για την εκτύπωσή του (Άρθρο 2 της Υ.Α. 8200/0-297647/2018). Σύμφωνα με το άρθρο 12 της Υ.Α. 8200/0-297647/2018, η διαδικασία αποστολής των δικαιολογητικών στην Δ.Δ.Ε.Α. και επιμέρους σχετικές λεπτομέρειες καθορίζονται με Απόφαση του Αρχηγού της ΕΛ.ΑΣ., που δεν δημοσιεύεται στο ευρύ κοινό. Αφού ολοκληρωθεί η εκτύπωση του Α.Δ.Τ., η Δ.Δ.Ε.Α. το αποστέλλει στην αστυνομική Υπηρεσία που υποβλήθηκε η αίτηση και τα δικαιολογητικά, προκειμένου να το χορηγήσει στον δικαιούχο της.

Κατ' εφαρμογή του άρθρου 3 του Ν.Δ. 127/1969 η εκδούσα αστυνομική Υπηρεσία τηρεί ειδικό αρχείο Α.Δ.Τ., στο οποίο αποθηκεύονται όλα τα δικαιολογητικά και τα στοιχεία για την έκδοση του εκάστοτε Α.Δ.Τ.. Τα δικαιολογητικά τηρούνται στο αρχείο της συγκεκριμένης Υπηρεσίας μέχρι να παρέλθει η ημερομηνία ισχύος του Α.Δ.Τ. ή την αντικατάσταση αυτού (Άρθρο 10 της Υ.Α. 8200/0-297647/2018). Επιπλέον, η Διεύθυνση Προστασίας του Κράτους του Αρχηγείου της Ελληνικής Αστυνομίας και συγκεκριμένα το Τμήμα Ταυτοτήτων και Αρχείων, σύμφωνα με το άρθρο 10 της Υ.Α. 8200/0-297647/2018, τηρεί ηλεκτρονικό αρχείο Α.Δ.Τ., στο οποίο αποθηκεύονται τα δικαιολογητικά και τα στοιχεία που περιέχει κάθε Α.Δ.Τ., που εκδίδεται από αστυνομικές Υπηρεσίες (Άρθρο 22 του Ν. 5187/2025). Τα δεδομένα, που αποθηκεύονται στην ηλεκτρονική εφαρμογή «Ταυτότητες Ελλήνων Πολιτών» του

³¹ <https://www.astynomia.gr/odigos-tou-politi/dikaiologitika/ekdosi-deltiou-taftotitas/>

«Police on Line»³², δεν διαγράφονται, προκειμένου να είναι εύκολα προσβάσιμα από οποιαδήποτε Υπηρεσία της Ελληνικής Αστυνομίας, ώστε να ελέγχει τη νομιμότητα εγγράφων, να εξακριβώνει τα στοιχεία των ατόμων όταν χρειάζεται, να διερευνά αξιόποινες πράξεις κ.λπ. (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Όταν εκδίδεται νέο Α.Δ.Τ. προς αντικατάσταση του παλαιού ο φυσικός φάκελος του παλαιού με τα σχετικά δικαιολογητικά έκδοσης καταστρέφεται από την αστυνομική Υπηρεσία, που το είχε εκδώσει, ενώ το παλαιό Α.Δ.Τ. χρησιμοποιείται ως δικαιολογητικό στο φάκελο του νέου Α.Δ.Τ., εκτός αν συντρέχει περίπτωση κλοπής ή απώλειας (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Η διαδικασία που τηρείται για την καταστροφή των Α.Δ.Τ. και των δικαιολογητικών, που έχουν υποβληθεί στην εκδούσα αρχή, καθορίζεται με την Απόφαση του Αρχηγού της Ελληνικής Αστυνομίας, που προαναφέρθηκε (Άρθρο 12 της Υ.Α. 8200/0-297647/2018).

Αξίζει να σημειωθεί ότι η Ελληνική Αστυνομία παρέχει σε δημόσιους φορείς τη δυνατότητα πρόσβασης σε διαδικτυακές υπηρεσίες προκειμένου να ελέγχουν τη γνησιότητα και εγκυρότητα των Α.Δ.Τ. Ελλήνων πολιτών, καθώς και την ορθότητα των στοιχείων των κατόχων τους, στο πλαίσιο εκτέλεσης των καθηκόντων τους, όταν αυτό απαιτείται. Για παράδειγμα, αυτό μπορεί να συμβεί στο πλαίσιο εξυπηρέτησης πολιτών, προκειμένου να πραγματοποιηθεί η ταυτοποίησή τους. Η πρόσβαση παρέχεται μέσω του Κέντρου Διαλειτουργικότητας του Υπουργείου Ψηφιακής Διακυβέρνησης.

6.4.3. Δικαιώματα των υποκειμένων

Κάθε φυσικό πρόσωπο, που αιτείται την έκδοση Α.Δ.Τ. δικαιούται να ζητήσει από την αρμόδια αστυνομική Υπηρεσία να αποκτήσει πρόσβαση στα δεδομένα του που έχουν συλλεχθεί, αλλά και διόρθωση αυτών σε περίπτωση που διαπιστωθεί πως είναι εσφαλμένα ή ελλιπή. Επιπλέον, δύναται να ασκήσει τα δικαιώματα της διαγραφής και περιορισμού της επεξεργασίας, σύμφωνα με τις προϋποθέσεις και περιορισμούς που προβλέπονται στα άρθρα 17 και 21 του GDPR, σε συνδυασμό με τις διατάξεις του Κεφαλαίου ΙΙΙ του Ν. 4624/2019.

Για να αποκτήσει πρόσβαση στα προσωπικά του δεδομένα, το φυσικό πρόσωπο θα πρέπει να υποβάλλει σχετική έγγραφη αίτηση στην αστυνομική Υπηρεσία, που κατέθεσε την αίτηση και τα δικαιολογητικά έκδοσης Α.Δ.Τ., κατ' εφαρμογή του άρθρου 5 του Κώδικα Διοικητικής Διαδικασίας (Κ.Δ.Δ.), η οποία εντός 20 ημερών είτε χορηγεί στον ενδιαφερόμενο τα αιτούμενα στοιχεία είτε, σε περίπτωση απόρριψης του αιτήματος, παραθέτει τους σχετικούς λόγους (Άρθρο 5 του Κ.Δ.Δ.).

Σε περίπτωση που ο αιτών κρίνει ότι παραβιάζονται τα προσωπικά του δεδομένα κατά τη διαδικασία έκδοσης Α.Δ.Τ., μπορεί να υποβάλλει καταγγελία στην

³² Το «Police on Line» είναι εσωτερικό δίκτυο της Ελληνικής Αστυνομίας μέσω του οποίου καταχωρούνται και αναζητούνται δεδομένα φυσικών προσώπων, οχημάτων και υποθέσεων και πραγματοποιείται διακίνηση αλληλογραφίας μεταξύ των αστυνομικών Υπηρεσιών της χώρας.

Α.Π.Δ.Π.Χ., στα στοιχεία επικοινωνίας, που παρέχονται στην ιστοσελίδα της Ελληνικής Αστυνομίας.

6.4.4. Συμπεράσματα

Η Ελληνική Αστυνομία είναι αρμόδια για την έκδοση Α.Δ.Τ. Ελλήνων πολιτών βάσει νομικής υποχρέωσης και ενημερώνει λεπτομερώς τους ενδιαφερόμενους, τόσο για τη διαδικασία όσο και για τα δικαιολογητικά, που απαιτούνται για την έκδοση αυτού, κατ' εφαρμογή των αρχών της νομιμότητας, αντικειμενικότητας και διαφάνειας.

Για την έκδοση Α.Δ.Τ., η εκδούσα αστυνομική Υπηρεσία συλλέγει και επεξεργάζεται τα απολύτως απαραίτητα προσωπικά δεδομένα, χωρίς να ζητάει από τον ενδιαφερόμενο τη χορήγηση δεδομένων, που δεν σχετίζονται και δεν είναι αναγκαία για την ταυτοποίησή του και γενικά την έκδοση Α.Δ.Τ.. Συγκεκριμένα, συλλέγει τόσο απλά προσωπικά δεδομένα, όπως το ονοματεπώνυμο του ενδιαφερόμενου και των γονέων του, η ημερομηνία και ο τόπος γέννησης, η ιθαγένεια, η διεύθυνση κατοικίας, ο προσωπικός αριθμός και το φύλο, όσο και ευαίσθητα, όπως η φωτογραφία συγκεκριμένων προδιαγραφών, τα δακτυλικά αποτυπώματα και η ιατρική βεβαίωση όταν συντρέχει σχετικός λόγος, κατ' εφαρμογή της αρχής ελαχιστοποίησης δεδομένων.

Βάσει της αρχής του σκοπού και του χρόνου αποθήκευσης των δεδομένων, τα δεδομένα συλλέγονται από την ΕΛ.ΑΣ με αποκλειστικό σκοπό την έκδοση Α.Δ.Τ. και παραμένουν αποθηκευμένα για συγκεκριμένο χρονικό διάστημα, μετά το πέρας του οποίου καταστρέφονται. Επιπλέον, σε περίπτωση όπου διαπιστωθούν από τον αιτούντα ελλιπή ή εσφαλμένα δεδομένα κατά τη διαδικασία έκδοσης του Α.Δ.Τ., το τελευταίο ακυρώνεται και η διαδικασία εκκινά εκ νέου, προκειμένου τα δεδομένα να είναι ακριβή.

Προς διασφάλιση της ακεραιότητας και εμπιστευτικότητας των δεδομένων, η αίτηση και τα δικαιολογητικά υποβάλλονται αυτοπροσώπως από τον ενδιαφερόμενο, παραλαμβάνονται από εξουσιοδοτημένο, για την έκδοση του Α.Δ.Τ., αστυνομικό υπάλληλο και στην συνέχεια υποβάλλονται αμέσως στη Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας προκειμένου να εκδοθεί το Α.Δ.Τ..

Με την τήρηση της αίτησης και των δικαιολογητικών σε αρχείο, μπορεί να αποδειχθεί, ανά πάσα στιγμή, η εφαρμογή των βασικών αρχών επεξεργασίας δεδομένων, κατά την έκδοση ενός Α.Δ.Τ., από την ΕΛ.ΑΣ..

6.5. Έκδοση διαβατηρίων

Η Ελληνική Αστυνομία καθίσταται υπεύθυνος επεξεργασίας και για τα προσωπικά δεδομένα, που απαιτούνται για την έκδοση ελληνικών διαβατηρίων. Αρχικά ως διαβατήριο ορίζεται το έγγραφο, με το οποίο ο κάτοχος αυτού μπορεί να εισέρχεται και να εξέρχεται της χώρας, δηλαδή της Ελλάδος. Το ελληνικό διαβατήριο είναι ατομικό, χορηγείται μόνο σε Έλληνες πολίτες και έχει χρονική ισχύ 10 έτη³³ (Άρθρα 1 και 2 του Π.Δ. 25/2022). Η διαδικασία και τα απαραίτητα έγγραφα που

³³ Αν ο κάτοχος είναι ανήλικος κάτω των 14 ετών, το διαβατήριο έχει ισχύ 3 έτη

απαιτούνται για την έκδοση διαβατηρίου, καθώς και το περιεχόμενο αυτών ορίζονται στο Προεδρικό Διάταγμα 25/2022 και στην Υπουργική Απόφαση 3021/22/10-ο'-2025.

6.5.1. Απαραίτητα δικαιολογητικά

Προκειμένου να εκδοθεί ελληνικό διαβατήριο, κατ' εφαρμογή των διατάξεων του άρθρου 1 της Υ.Α. 3021/22/10-ο'-2025, ο ενδιαφερόμενος υποβάλλει αυτοπροσώπως στο αρμόδιο Γραφείο Διαβατηρίων³⁴ του τόπου κατοικίας του τα δικαιολογητικά, που απαιτούνται για την έκδοση και συγκεκριμένα:

- αίτηση-υπεύθυνη δήλωση, η οποία συμπληρώνεται ηλεκτρονικά από τον αρμόδιο αστυνομικό, και στην οποία δηλώνει ο ενδιαφερόμενος τα πλήρη στοιχεία ταυτότητας και επικοινωνίας, τη διεύθυνση κατοικίας του, το ύψος και το χρώμα ματιών του, εάν είχε στην κατοχή του διαβατήριο, το οποίο χάθηκε, κλάπηκε ή χρήζει αντικατάστασης, εάν έχει καταδικασθεί τελεσίδικα, για τα αδικήματα α) της πλαστογραφίας, πλαστογραφίας πιστοποιητικών, υφαρπαγής ψευδούς βεβαίωσης, υπεξαγωγής εγγράφων ή ψευδούς δήλωσης κατά παράβαση των άρθρων 216, 217, 220, 222 και 224 του Π.Κ. και του άρθρου 22 παρ. 6 του ν. 1599/1986, τα οποία σχετίζονται με την έκδοση, χρήση, απώλεια ή κλοπή διαβατηρίου ή Α.Δ.Τ. ή β) της αρπαγής, εμπορίας ανθρώπων, αρπαγής ανηλίκων και διακίνηση λαθρομεταναστών κατά παράβαση των άρθρων 322, 323Α, 324 του Π.Κ. ή γ) του άρθρου 29 παρ. 5-7 του Ν. 4251/2014 αναφορικά με τη διευκόλυνση εισόδου πολίτη τρίτης χώρας στην Ελλάδα ή εξόδου του από αυτή, χωρίς να προηγηθεί ο προβλεπόμενος από το Νόμο έλεγχος, τη διευκόλυνση παράνομης παραμονής πολίτη τρίτης χώρας ή παρεμπόδισης του έργου των αστυνομικών αρχών για τον εντοπισμό, την σύλληψη και την απέλαση αυτού και την κατοχή, χρήση ή παράνομη παρακράτηση γνήσιου διαβατηρίου ή άλλου ταξιδιωτικού εγγράφου, που ανήκει σε τρίτο πρόσωπο, καθώς και των αδικημάτων του άρθρου 30 παρ.1 και 2 του ίδιου Νόμου, που αφορούν πλοιάρχους, κυβερνήτες και οδηγούς κάθε μεταφορικού μέσου, οι οποίοι μεταφέρουν ή κρύβουν πολίτες τρίτων χωρών, χωρίς δικαίωμα εισόδου στην Ελλάδα, παραβιάζονται την υποχρέωση ελέγχου των εγγράφων τους. Επιπλέον δηλώνει αν εκτίει ποινή στερητική της ελευθερίας ή είναι προσωρινά κρατούμενος, αν είναι ανυπότακτος ή λιποτάκτης, καθώς και εάν του έχει επιβληθεί το μέτρο απαγόρευσης εξόδου από τη χώρα, καθώς και αν υπάρχει σε βάρος του τελεσίδικη καταδικαστική απόφαση, η οποία δεν έχει εκτελεστεί, ή ένταλμα σύλληψης, ενώ παράλληλα δηλώνει ότι έχει ενημερωθεί για την επεξεργασία των δεδομένων του και τα δικαιώματά του,

³⁴ Όπως αυτά ορίζονται στο άρθρο 3 του Π.Δ. 126/2005 αναφορικά με την ίδρυση Διεύθυνσης Διαβατηρίων. Στην επίσημη ιστοσελίδα της Διεύθυνσης Διαβατηρίων και Εγγράφων Ασφαλείας της Ελληνικής Αστυνομίας, υπάρχουν αναλυτικές πληροφορίες για όλα τα Γραφεία Διαβατηρίων που λειτουργούν στην Ελλάδα και τις περιοχές που εξυπηρετεί το καθένα, καθώς και για τα Γραφεία Διαβατηρίων του εξωτερικού.

- πρόσφατη έγχρωμη ψηφιακή φωτογραφία του με συγκεκριμένες προδιαγραφές, την οποία υποβάλλει ο ενδιαφερόμενος μέσω της εφαρμογής myPhoto στην διαδικτυακή πύλη gov.gr, ενώ σε περίπτωση απόκλισης από τις προκαθορισμένες τεχνικές προδιαγραφές, συνυποβάλλεται ιατρικό έγγραφο με την πάθηση του ατόμου,
- επίδειξη ενεργού Α.Δ.Τ. του ενδιαφερόμενου είτε σε φυσική είτε σε ψηφιακή μορφή μέσω της εφαρμογής gov.gr wallet,
- παράβολα πληρωμής των τελών έκδοσης διαβατηρίου και εξόδων αποστολής των δικαιολογητικών προς και από την Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας,
- ιατρικά έγγραφα, όταν το διαβατήριο εκδίδεται κατ' εξαίρεση για νοσηλεία του ενδιαφερόμενου/αιτούντος στο εξωτερικό.

Αν ο αιτών έχει καταδικασθεί τελεσίδικα για κάποιο από τα προαναφερόμενα αδικήματα, αν εκτίει ποινή στερητική της ελευθερίας ή είναι προσωρινά κρατούμενος, αν είναι ανυπότακτος ή λιποτάκτης, καθώς και εάν του έχει επιβληθεί το μέτρο απαγόρευσης εξόδου από τη χώρα, δεν του χορηγείται ελληνικό διαβατήριο, πλην των εξαιρέσεων που προβλέπουν οι παράγραφοι 3 και 4 του άρθρου 1 του Π.Δ. 25/2022 με χρονική ισχύς που ορίζεται στο άρθρο 2 του ίδιου Π.Δ..

6.5.2. Επεξεργασία και διατήρηση προσωπικών δεδομένων

Η αστυνομική Υπηρεσία που παραλαμβάνει τα ανωτέρω δικαιολογητικά, προβαίνει σε λήψη και κρυπτογράφηση δύο δακτυλικών αποτυπωμάτων του αιτούντος και συγκεκριμένα των δεικτών και των δύο χεριών του, πλην των περιπτώσεων, που πρόκειται για ανήλικο άτομο που δεν έχει συμπληρώσει το 12^ο έτος της ηλικίας του. Αν η λήψη δακτυλικού αποτυπώματος δείκτη καθίσταται αδύνατη, λαμβάνεται αποτύπωμα από τα επόμενα δάκτυλα κατά σειρά, όπως ισχύει και στην περίπτωση έκδοσης Α.Δ.Τ.. Επιπλέον, σε περίπτωση μονόχειρα, λαμβάνεται αποτύπωμα και από δεύτερο δάκτυλο του υπάρχοντος χεριού, με τη σειρά που έχει προαναφερθεί. Προς απόδειξη της προσωρινής ή μόνιμης αδυναμίας λήψης δακτυλικών αποτυπωμάτων ο αιτών πρέπει να προσκομίσει στην αστυνομική Υπηρεσία ιατρικό έγγραφο από το οποίο να προκύπτει αυτή (Άρθρο 1 παρ. 8 της Υ.Α. 3021/22/10-ο'/2025). Σε περίπτωση που συντρέχει τέτοιου είδους αδυναμία, το διαβατήριο που εκδίδεται έχει χρονική ισχύ 8 μηνών (Άρθρο 2 παρ.2 του Π.Δ. 25/2022).

Αφού η παραλαβούσα Υπηρεσία ελέγξει την εγκυρότητα και ορθότητα των υποβληθέντων δικαιολογητικών, τα διαβιβάζει ηλεκτρονικά στη Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας του Αρχηγείου της Ελληνικής Αστυνομίας μέσω κατάλληλου δικτύου, εφαρμόζοντας τεχνικά και οργανωτικά μέτρα, ώστε να διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των προσωπικών δεδομένων, που υπόκεινται σε επεξεργασία. Σε περίπτωση, όμως, που καθίσταται αδύνατη η ηλεκτρονική αποστολή των εγγράφων, αυτά αποστέλλονται ταχυδρομικώς (Άρθρο 2 παρ. 3 της Υ.Α. 3021/22/10-ο'/2025).

Η Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας του Αρχηγείου της Ελληνικής Αστυνομίας συλλέγει και επεξεργάζεται τα στοιχεία των πολιτών, που επιθυμούν να εκδώσουν ελληνικό διαβατήριο βασιζόμενη στη νομική βάση επεξεργασίας του άρθρου 6 παρ.1 και συγκεκριμένα των περιπτώσεων γ' και ε' του GDPR. Πρακτικά αυτό σημαίνει ότι η επεξεργασία συνιστά νόμιμη υποχρέωσή της, αλλά και πράξη που εκτελείται στο πλαίσιο άσκησης δημόσιας εξουσίας και εξυπηρέτησης δημόσιου συμφέροντος, με σκοπό την έκδοση ελληνικού διαβατηρίου³⁵.

Η εν λόγω Διεύθυνση όταν παραλάβει την αίτηση και τα δικαιολογητικά, προς εκπλήρωση των σκοπών και αρμοδιοτήτων της, όπως αυτές ορίζονται στο άρθρο 26 του Ν. 5187/2025 και του άρθρου 11 του Ν. 3480/2006, τα ψηφιοποιεί – όταν έχουν αποσταλεί σε φυσική μορφή - και τα αποθηκεύει σε βάση δεδομένων, προκειμένου να τα επεξεργαστεί, ελέγχει τη γνησιότητα και πληρότητά τους και εφόσον διαπιστώσει ότι συντρέχουν οι νόμιμες προϋποθέσεις, εκδίδει το διαβατήριο εντός πέντε εργάσιμων ημερών από την ημέρα, που θα παραλάβει την αίτηση. Στην συνέχεια, αποστέλλει ταχυδρομικώς το διαβατήριο στην αστυνομική Υπηρεσία, όπου κατατέθηκε η αίτηση έκδοσης, προκειμένου να παραληφθεί από τον κάτοχό του. Μαζί με το διαβατήριο επιστρέφει στην εν λόγω Υπηρεσία τα δικαιολογητικά, εάν υποβλήθηκαν σε έντυπη μορφή, τα οποία τηρούνται στο αρχείο σε φυσική μορφή και καταστρέφονται με την πάροδο δέκα ετών από την ημερομηνία υποβολής τους. Κατ' εξαίρεση, η κρυπτογραφημένη σελίδα, που περιέχει τα δακτυλικά αποτυπώματα του αιτούντος καταστρέφεται αμέσως μετά την επεξεργασία τους από την Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας, συνεπώς δεν επιστρέφεται στην αρμόδια αστυνομική Υπηρεσία. Επιπλέον, δεν τηρούνται στο αρχείο οι αποτυπώσεις των ψηφιακών φωτογραφιών (Άρθρο 3 παρ.1 και 3 και Άρθρο 7 παρ.1 της Υ.Α. 3021/22/10-ο'/2025). Εκτός των προαναφερθέντων, η Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας:

- τηρεί ηλεκτρονικό αρχείο με τα εκδοθέντα ελληνικά διαβατήρια και τα δικαιολογητικά, βάσει των οποίων αυτά εκδόθηκαν, όπου τα τελευταία διαγράφονται με το πέρας 15ετίας από την υποβολή τους (Άρθρο 7 της Υ.Α. 3021/22/10-ο'/2025), και λαμβάνει αντίγραφα ασφαλείας,
- λαμβάνει τεχνικά και οργανωτικά μέτρα για την προστασία των συλλεχθέντων προσωπικών δεδομένων από ενδεχόμενη διαρροή, απώλεια, καταστροφή ή οποιαδήποτε αθέμιτη επεξεργασία,
- καταχωρεί σε εθνικές (εγχώρια αστυνομική βάση) και διεθνείς βάσεις δεδομένων (Σύστημα πληροφοριών Schengen - SIS II) τα διαβατήρια που έχουν κλαπεί, ακυρωθεί και απολεσθεί,
- καταγράφει και εκδίδει στατιστικά στοιχεία σχετικά με τα εκδοθέντα διαβατήρια,

³⁵ <https://www.passport.gov.gr/npc/data.html>

- πιστοποιεί την αυθεντικότητα των δεδομένων που περιλαμβάνονται ηλεκτρονικά στα ελληνικά διαβατήρια και των συστημάτων ελέγχου της γνησιότητας αυτών.

Κάθε ελληνικό διαβατήριο, που εκδίδεται περιέχει τη φωτογραφία, το ονοματεπώνυμο, την ημερομηνία, τον τόπο και τη χώρα γέννησης, την ιθαγένεια, το φύλο και το ύψος του κατόχου του. Επιπλέον, αναγράφεται ο αριθμός διαβατηρίου, η εκδούσα αρχή και η ημερομηνία έκδοσης και λήξης. Στο διαβατήριο περιλαμβάνεται επίσης η υπογραφή του κατόχου, όταν αυτός είναι άνω των 12 ετών, και μικροεπεξεργαστής (τσιπ), ο οποίος περιέχει τη φωτογραφία του κατόχου, τα στοιχεία που είναι αποτυπωμένα στη μηχανικώς αναγνώσιμη ζώνη του διαβατηρίου και τα δακτυλικά αποτυπώματα του κατόχου. Στις περιπτώσεις που ο κάτοχος είναι κάτω των 12 ετών ή υφίσταται μόνιμη ή προσωρινή αδυναμία λήψης δακτυλικών αποτυπωμάτων, ο μικροεπεξεργαστής (τσιπ) περιέχει τα ανωτέρω στοιχεία πλην των δακτυλικών αποτυπωμάτων (Άρθρο 5 της Υ.Α. 3021/22/10-ο'/2025).

6.5.2.1. Δεδομένα ειδικών κατηγοριών

Από την ανάλυση που προηγήθηκε, γίνεται σαφές ότι τα Γραφεία Διαβατηρίων και η Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας συλλέγουν και επεξεργάζονται τόσο απλά όσο και ευαίσθητα προσωπικά δεδομένα. Πιο συγκεκριμένα, τα απλά δεδομένα αφορούν τα στοιχεία Α.Δ.Τ. και στοιχεία του δημοτολογίου του αιτούντος, τα στοιχεία επικοινωνίας του, όπως το τηλέφωνο, το email και η διεύθυνση κατοικίας, αλλά και υπεύθυνες δηλώσεις, εξουσιοδοτήσεις και έγγραφα δημόσιων υπηρεσιών και αρχών.

Όσον αφορά τα προσωπικά δεδομένα ειδικών κατηγοριών, αυτά περιλαμβάνουν τη φωτογραφία ειδικών προδιαγραφών του αιτούντος, δύο δακτυλικά του αποτυπώματα και σε συντρέχουσα περίπτωση, ιατρικά έγγραφα και πληροφορίες ή έγγραφα αναφορικά με ποινικές καταδίκες ή εντάλματα σύλληψης σε βάρος του, για τα αδικήματα που προαναφέρθηκαν, καθώς και εκείνα που αφορούν την απαγόρευση εξόδου του από την Ελλάδα, την έκτιση ποινής φυλάκισης ή προσωρινής του κράτησης και την κήρυξη του ως ανυπότακτου ή λιποτάκτη.

Τα ψηφιακά δικαιολογητικά, που περιλαμβάνουν τέτοια δεδομένα, αποθηκεύονται σε κρυπτογραφημένη μορφή στην κεντρική βάση δεδομένων της Διεύθυνσης Διαβατηρίων και Εγγράφων Ασφαλείας μέχρι να διαγραφούν, ενώ οι ψηφιακές αποτυπώσεις των δακτυλικών αποτυπωμάτων, που συλλέγονται προκειμένου να ενσωματωθούν στον μικροεπεξεργαστή του διαβατηρίου, αποθηκεύονται σε κρυπτογραφημένη μορφή στη Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας μέχρι την λήξη ισχύος του διαβατηρίου ή την ακύρωσή του και στη συνέχεια διαγράφονται εντός 30 ημερών (Άρθρο 7 παρ. 2 και 3 της Υ.Α. 3021/22/10-ο'/2025).

Σε αυτό το σημείο αξίζει να σημειωθεί, ότι τόσο τα ψηφιακά δικαιολογητικά όσο και τα βιομετρικά δεδομένα διαγράφονται αυτοματοποιημένα, με ασφαλή τρόπο, που δεν επιτρέπει την περαιτέρω αθέμιτη επεξεργασία τους ή ανάκτησή τους, ενώ κάθε

τέτοια ενέργεια διαγραφής καταγράφεται στο ηλεκτρονικό αρχείο της Διεύθυνσης (Άρθρο 7 της Υ.Α. 3021/22/10-ο'/2025).

Η φωτογραφία και τα δακτυλικά αποτυπώματα συλλέγονται με σκοπό να:

- ενσωματωθούν στον μικροεπεξεργαστή (τσιπ) του εκδοθέντος ελληνικού διαβατηρίου, ώστε να εξασφαλίζεται η ακεραιότητα, εμπιστευτικότητα και αυθεντικότητα των δεδομένων, κατ' εφαρμογή του άρθρου 1 του Κανονισμού (ΕΚ) 2252/2004,
- διατηρηθούν σε ηλεκτρονικό αρχείο εκδοθέντων διαβατηρίων, ώστε να επιβεβαιώνεται η εγκυρότητα και γνησιότητα των διαβατηρίων,
- επαληθεύεται η αυθεντικότητα και γνησιότητα των δεδομένων, που αποθηκεύονται στον μικροεπεξεργαστή του διαβατηρίου, ιδιαίτερα όταν αυτό χρησιμοποιείται για την τέλεση σοβαρών αξιόποινων πράξεων, όπως για παράδειγμα το οργανωμένο έγκλημα, η τρομοκρατία και η παράνομη εμπορία ατόμων.

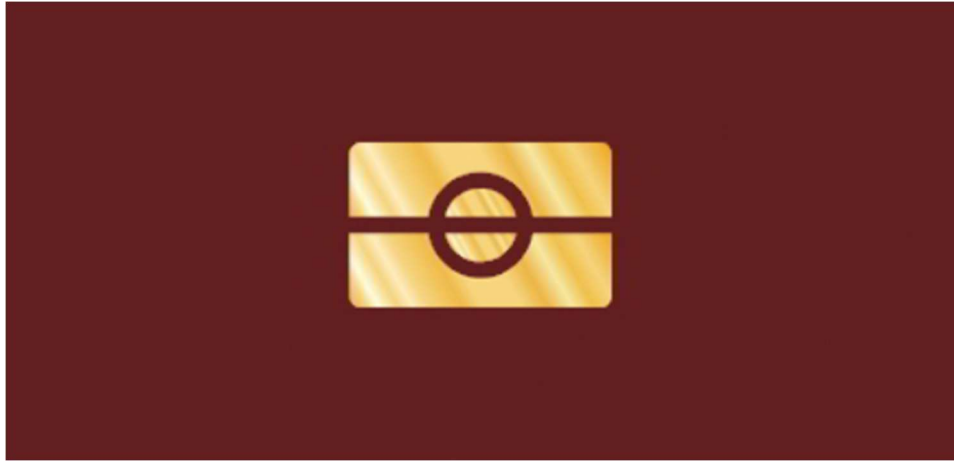
Άλλωστε, σύμφωνα με τον ICAO³⁶, το πρόσωπο αποτελεί το βασικό βιομετρικό στοιχείο, που συμβάλει στην ταυτοποίηση ενός ατόμου, ενώ τα δακτυλικά αποτυπώματα λειτουργούν συμπληρωματικά³⁷.

Αναφορικά με τα ιατρικά έγγραφα, αυτά συλλέγονται με σκοπό να διαπιστωθεί τυχόν μόνιμη ή προσωρινή αδυναμία λήψης δακτυλικών αποτυπωμάτων ή να αποδειχθεί ιατρική ανάγκη για νοσηλεία του αιτούντος στο εξωτερικό και κατ' επέκταση κατ' εξαίρεση έκδοση διαβατηρίου, ενώ οποιαδήποτε πληροφορία ή έγγραφο σχετικά με ποινικές καταδίκες ή εντάλματα σύλληψης σε βάρος του, για τα αδικήματα που έχουν προαναφερθεί, καθώς και εκείνο που αφορά την απαγόρευση εξόδου του από την Ελλάδα, την έκτιση ποινής φυλάκισης ή προσωρινής του κράτησης και την κήρυξή του ως ανυπότακτου ή λιποτάκτη συλλέγεται, προκειμένου να διαπιστωθεί αν συντρέχουν νόμιμοι λόγοι να του χορηγηθεί διαβατήριο.

Τα σύγχρονα βιομετρικά διαβατήρια φέρουν στο κάτω μέρος της εμπρόσθιας όψης τους (δείτε Εικόνα 5 και Εικόνα 6) το εξής σύμβολο:

³⁶ Ο ICAO (International Civil Aviation Organization - Διεθνής Οργανισμός Πολιτικής Αεροπορίας) είναι οργανισμός που ρυθμίζει ζητήματα αναφορικά με τις διεθνείς αερομεταφορές (https://eclass.pegasusaviation.gr/modules/document/file.php/UAS153/%CE%91%CE%95%CE%A1%CE%9F%CE%A0%CE%9F%CE%A1%CE%99%CE%9A%CE%9F%CE%99%20%CE%9F%CE%A1%CE%93%CE%91%CE%9D%CE%99%CE%A3%CE%9C%CE%9F%CE%99%E2%80%93%CE%A5%CE%A0%CE%97%CE%A1%CE%95%CE%A3%CE%99%CE%95%CE%A3_W.pdf)

³⁷ <https://www.passport.gov.gr/e-passport/biometrics.html>



Εικόνα 5: Σύμβολο βιομετρικών διαβατηρίων



Εικόνα 6: Εμπρόσθια όψη διαβατηρίου

Όπως και στην περίπτωση των ταυτοτήτων, έτσι και στα διαβατήρια η Ελληνική Αστυνομία παρέχει σε δημόσιους φορείς τη δυνατότητα πρόσβασης σε διαδικτυακές υπηρεσίες προκειμένου να ελέγχουν τη γνησιότητα και εγκυρότητα των ελληνικών διαβατηρίων, καθώς και την ορθότητα των στοιχείων των κατόχων τους, στο πλαίσιο εκτέλεσης των καθηκόντων τους, μέσω του Κέντρου Διαλειτουργικότητας του Υπουργείου Ψηφιακής Διακυβέρνησης.

6.5.3. Μέτρα Ασφαλείας

Η Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας, προκειμένου να εξασφαλίζει την ακεραιότητα και εμπιστευτικότητα των δεδομένων και εγγράφων, που

συλλέγει και διαχειρίζεται, λαμβάνει αυξημένα μέτρα ασφαλείας. Συγκεκριμένα, φρουρείται επί 24ωρης βάσης και επιτηρείται με κάμερες ασφαλείας, ενώ η είσοδος σε αυτή γίνεται με τη χρήση έξυπνης κάρτας και δακτυλικού αποτυπώματος³⁸.

Επιπλέον, λαμβάνει τεχνικά και οργανωτικά μέτρα ασφαλείας, τα οποία επικεντρώνονται:

- στην εφαρμογή ισχυρών μηχανισμών κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων ειδικών κατηγοριών,
- στη χρήση διαπιστευτηρίων για τον διαβαθμισμένο έλεγχο φυσικής και ηλεκτρονικής πρόσβασης στο χώρο, όπου βρίσκονται τα δεδομένα,
- στη χρήση συστήματος εξουσιοδότησης χρηστών με σαφώς προσδιορισμένους ρόλους και δικαιώματα, ώστε κάθε χρήστης να έχει πρόσβαση στα απολύτως αναγκαία, για την εκτέλεση των καθηκόντων του, δεδομένα,
- στον αυστηρά περιορισμένο αριθμό των υπαλλήλων, που έχει πρόσβαση στα δεδομένα ειδικών κατηγοριών,
- στην αυτοματοποιημένη ηλεκτρονική καταγραφή των ενεργειών των χρηστών επί των δεδομένων,
- στην κατάλληλη εκπαίδευση των χρηστών των συστημάτων, ανάλογα με τα καθήκοντα και τις αρμοδιότητες, που τους έχουν ανατεθεί,
- στη λήψη μέτρων για την εξασφάλιση της εμπιστευτικότητας, ακεραιότητας, αuthεντικότητας και διαθεσιμότητας των δεδομένων,
- στη λήψη μέτρων για την προστασία των δεδομένων από ενδεχόμενη αθέμιτη απώλεια, αλλοίωση, καταστροφή, μη εξουσιοδοτημένη πρόσβαση και οποιαδήποτε άλλη παράνομη επεξεργασία τους.

Ασφαλώς, όλα αυτά τα μέτρα ελέγχονται και αναθεωρούνται σε τακτική βάση, ώστε να ανταποκρίνονται στις σύγχρονες τεχνολογικές απαιτήσεις.

Αξίζει να σημειωθεί ότι όταν τα δικαιολογητικά και εκδοθέντα διαβατήρια διαβιβάζονται ταχυδρομικώς, η διαβίβαση πραγματοποιείται μέσω εταιρειών παροχής ταχυδρομικών υπηρεσιών, συμβαλλόμενες με το Υπουργείο Προστασίας του Πολίτη, οι οποίες οφείλουν να λαμβάνουν όλα τα απαραίτητα μέτρα για τη διασφάλιση της ακεραιότητας, εμπιστευτικότητας, διαθεσιμότητας και γενικά της προστασίας των διαβιβαζόμενων δεδομένων (Άρθρο 8 της Υ.Α. 3021/22/10-ο’/2025).

6.5.4. Δικαιώματα των υποκειμένων

Ο αιτών δύναται να αποκτήσει πρόσβαση στα δεδομένα του που συλλέγονται για την έκδοση διαβατηρίου, καθώς και να ζητήσει τη διόρθωσή τους σε περίπτωση που τα στοιχεία είναι εσφαλμένα ή ελλιπή. Επιπλέον, έχει τη δυνατότητα να ασκήσει τα

³⁸ <https://www.passport.gov.gr/npc/est.html>

δικαιώματα της διαγραφής, περιορισμού της επεξεργασίας και εναντίωσης, που προβλέπονται στον GDPR και συγκεκριμένα στα άρθρα 17, 18 και 21, αντίστοιχα, σε συνδυασμό με τα άρθρα 34 και 35 του Ν. 4624/2019, αλλά και να υποβάλλει καταγγελία στην Α.Π.Δ.Π.Χ..

Το υποκείμενο των δεδομένων για να αποκτήσει πρόσβαση στα προσωπικά του δεδομένα θα πρέπει να υποβάλλει σχετική έγγραφη αίτηση, στην αστυνομική Υπηρεσία που κατέθεσε την αίτηση και τα δικαιολογητικά έκδοσης διαβατηρίου, κατ' εφαρμογή του άρθρου 5 του Κ.Δ.Δ.. Η παραλαβούσα Υπηρεσία, εντός 20 ημερών είτε χορηγεί στον ενδιαφερόμενο τα αιτούμενα στοιχεία είτε, σε περίπτωση απόρριψης του αιτήματος, παραθέτει τους σχετικούς λόγους (Άρθρο 5 του Κ.Δ.Δ.). Ωστόσο, και για να ασκήσει τα υπόλοιπα δικαιώματά του, που αναφέρθηκαν στην προηγούμενη παράγραφο, ο ενδιαφερόμενος θα πρέπει να υποβάλει σχετικό αίτημα στο Γραφείο Διαβατηρίων, που κατέθεσε την αίτησή του. Ειδικά για το δικαίωμα διόρθωσης, σε περίπτωση που τα δεδομένα είναι εσφαλμένα ή ελλιπή, εκδίδεται νέο διαβατήριο.³⁹

Πληροφορίες αναφορικά με την έκδοση διαβατηρίων, την επεξεργασία των προσωπικών δεδομένων στο πλαίσιο αυτής, τα Γραφεία Διαβατηρίων ανά Νομό στην ελληνική επικράτεια, αλλά και στο εξωτερικό, καθώς και τα στοιχεία επικοινωνίας της Α.Π.Δ.Π.Χ. είναι αναρτημένες στην ιστοσελίδα www.passport.gov.gr.

6.5.5. Συμπεράσματα

Η Ελληνική Αστυνομία συλλέγει και επεξεργάζεται τόσο απλά όσο και ευαίσθητα προσωπικά δεδομένα κατά την έκδοση διαβατηρίων βάσει νομικής υποχρέωσης, αλλά και στο πλαίσιο άσκησης δημόσιας εξουσίας, όπως ρητά προβλέπει ο GDPR στο άρθρο 6. Οι πολίτες ενημερώνονται για την επεξεργασία των δεδομένων τους μέσω της αίτησης, που υποβάλλουν για την έκδοση διαβατηρίου, αλλά και μέσω της επίσημης ιστοσελίδας της Διεύθυνσης Διαβατηρίων και Εγγράφων Ασφαλείας, στην οποία υπάρχουν αναλυτικές πληροφορίες αναφορικά με την έκδοση ελληνικού διαβατηρίου, τα δεδομένα που συλλέγονται και τίθενται σε επεξεργασία στο πλαίσιο αυτού, τα δικαιώματά τους και τη δυνατότητα υποβολής καταγγελίας στην Α.Π.Δ.Π.Χ.. Μάλιστα, σε κάθε σημείο υποδοχής υποβολής αιτημάτων έκδοσης ελληνικών διαβατηρίων βρίσκεται αναρτημένο σε εμφανές σημείο ενημερωτικό σημείωμα με τις ανωτέρω πληροφορίες (Άρθρο 6 παρ. 8 της Υ.Α. 3021/22/10-ο'/2025).

Τα δεδομένα συλλέγονται από την Ελληνική Αστυνομία αποκλειστικά για τον έλεγχο τήρησης των απαιτούμενων προϋποθέσεων, την ταυτοποίηση του αιτούντος και την εξασφάλιση ότι τα ελληνικά διαβατήρια εκδίδονται με τρόπο νόμιμο, ασφαλή και αξιόπιστο. Επομένως, δεν επιτρέπεται η χρήση των δεδομένων για διαφορετικό σκοπό.

Επιπλέον, η ΕΛ.ΑΣ. συλλέγει τα απολύτως απαραίτητα δεδομένα από τον αιτούντα, χωρίς να ζητάει δεδομένα, που δεν έχουν σχέση με την ταυτοποίηση αυτού και γενικότερα την έκδοση του διαβατηρίου. Προκειμένου να εκδώσει το ελληνικό διαβατήριο ελέγχει την ακρίβεια των δεδομένων και σε περίπτωση που διαπιστωθούν

³⁹ <https://www.passport.gov.gr/npc/data.html>

από τον αιτούντα ελλιπή ή εσφαλμένα δεδομένα, τότε ακυρώνεται το εκδοθέν διαβατήριο και εκδίδεται νέο με τα σωστά στοιχεία, κατόπιν αίτησης του ενδιαφερόμενου στο κατά τόπο αρμόδιο Γραφείο Διαβατηρίων.

Η αίτηση, τα δικαιολογητικά και τα προσωπικά δεδομένα του αιτούντα τηρούνται στην αστυνομική Υπηρεσία που υποβλήθηκαν, αλλά και στην Διεύθυνση Διαβατηρίων και Εγγράφων Ασφαλείας για συγκεκριμένο χρονικό διάστημα, μετά το πέρας του οποίου καταστρέφονται αυτόματα.

Τέλος, η Ελληνική Αστυνομία λαμβάνει μέτρα ασφαλείας ώστε να εξασφαλίζει την ακεραιότητα και εμπιστευτικότητα των δεδομένων και εγγράφων της, ενώ τηρώντας ηλεκτρονικό αρχείο με τις αιτήσεις και τα δικαιολογητικά των εγγράφων, αλλά και αντίγραφα ασφαλείας είναι σε θέση ανά πάσα στιγμή να τεκμηριώσει τη νόμιμη έκδοση ελληνικού διαβατηρίου.

6.6. Επιτήρηση δημόσιων χώρων

Η εγκατάσταση και χρήση συστημάτων επιτήρησης, που καταγράφουν ήχο ή εικόνα σε δημόσιους χώρους, για την συλλογή και επεξεργασία προσωπικών δεδομένων, επιτρέπεται μόνο σε συγκεκριμένες περιπτώσεις. Ειδικότερα, όπως ορίζει το άρθρο 14 του Ν. 3917/2011, τα εν λόγω συστήματα μπορούν να χρησιμοποιηθούν για την προστασία της εθνικής άμυνας και του πολιτεύματος, την αποτροπή πράξεων προδοσίας σε βάρος της χώρας, την πρόληψη και καταστολή αξιόποινων πράξεων που απειλούν τη δημόσια τάξη, αλλά και σοβαρών εγκλημάτων, όπως εγκλήματα βίας, εμπορία ναρκωτικών, εγκλήματα που θέτουν σε κίνδυνο τις συγκοινωνίες, καθώς και εγκλήματα κατά της ιδιοκτησίας, όταν υπάρχουν επαρκή στοιχεία και ενδείξεις ότι διαπράχθηκαν ή επίκειται να διαπραχθούν τέτοια εγκλήματα, αλλά και για τη ρύθμιση και διαχείριση της κυκλοφορίας στο οδικό δίκτυο. Σε κάθε περίπτωση, πάντως, τα συστήματα αυτά μπορούν να χρησιμοποιηθούν μόνο από κρατικές αρχές κατ' εφαρμογή της αρχής της αναλογικότητας (άρθρο 14 του Ν. 3917/2011).

Ως δημόσιος χώρος νοείται κάθε χώρος, που προορίζεται για κοινή χρήση σύμφωνα με τη νομοθεσία και τα σχέδια πόλεων, οι ανοιχτοί χώροι, στους οποίους παρέχεται ελεύθερη πρόσβαση σε απροσδιόριστο πλήθος ατόμων, προκειμένου να χρησιμοποιηθούν από κοινού και με νόμιμο τρόπο, αλλά και οι σταθμοί επιβίβασης και αποβίβασης ατόμων στα μέσα μαζικής μεταφοράς (Άρθρο 14 του Ν. 3917/2011).

Λαμβάνοντας υπόψη τις διατάξεις του GDPR, του Ν. 4624/2019, του άρθρου 14 του Ν. 3917/2011, αλλά και του Ν. 4703/2020 περί δημόσιων υπαίθριων συναθροίσεων και κατόπιν της υπ' αριθ. 3/2020 γνωμοδότησης της Α.Π.Δ.Π.Χ. και λοιπών γνωμοδοτήσεων, εισηγήσεων και αποφάσεων, εκδόθηκε το Π.Δ. 75/2020⁴⁰, το οποίο ρυθμίζει και εξειδικεύει τους κανόνες, που ισχύουν για την εγκατάσταση και χρήση συστημάτων επιτήρησης σε δημόσιους χώρους, στο μέτρο που πραγματοποιείται συλλογή και επεξεργασία προσωπικών δεδομένων για την επίτευξη των σκοπών που

⁴⁰ <https://www.kodiko.gr/nomothesia/document/638933>

αναφέρθηκαν προηγουμένως, διασφαλίζοντας παράλληλα τα δικαιώματα των ατόμων που θίγονται κατά τη λειτουργία αυτών των συστημάτων (Άρθρο 1 του Π.Δ. 75/2020).

6.6.1. Προεδρικό Διάταγμα 75/2020

Οι ρυθμίσεις του Π.Δ. 75/2020 ισχύουν για κάθε είδους σύστημα επιτήρησης, που τοποθετείται σε δημόσιο χώρο, ανεξαρτήτως από τα τεχνικά του χαρακτηριστικά, δηλαδή αν λειτουργεί με αναλογική ή ψηφιακή τεχνολογία, εάν χρησιμοποιεί σταθερές, κινητές ή περιστρεφόμενες κάμερες, τοποθετημένες σε σταθερά σημεία ή σε οχήματα ξηράς, θάλασσας ή αέρος, επανδρωμένα ή μη, ή αν μεταφέρονται από άτομα. Επιπλέον, καλύπτει και τις ηλεκτρονικές συσκευές ή συστήματα που μπορούν να καταγράψουν εικόνα, είτε συνεχώς είτε κατά διαστήματα. Για παράδειγμα, τέτοια συστήματα είναι τα κλειστά κυκλώματα τηλεόρασης, μαζί με τυχόν επιπλέον εξοπλισμό που απαιτείται για τη μετάδοση, αποθήκευση και επεξεργασία εικόνας και ήχου (Άρθρο 2 του Π.Δ. 75/2020).

Επιπλέον, το Π.Δ. 75/2020 στο άρθρο 3 εξειδικεύει τους σκοπούς για την εκπλήρωση των οποίων επιτρέπεται η εγκατάσταση και λειτουργία αυτών των συστημάτων. Πιο συγκεκριμένα, επιτρέπεται για την πρόληψη και καταστολή των εγκλημάτων των άρθρων 183-191Α, 264-315Α, 322-353 και 372-405 του Π.Κ., καθώς και των κακουργημάτων του Ν. 4139/2013 περί εξαρτησιογόνων ουσιών, προκειμένου να αποδειχθεί η τέλεση αυτών και να ταυτοποιηθεί ο δράστης, αλλά και για τη διαχείριση της κυκλοφορίας, και πιο συγκεκριμένα τη διαχείριση έκτακτων συμβάντων στο οδικό δίκτυο, τη ρύθμιση και τον έλεγχο της κυκλοφορίας των οχημάτων, αλλά και την πρόληψη και διαχείριση τροχαίων ατυχημάτων και δυστυχημάτων.

6.6.1.1. Υπεύθυνος επεξεργασίας

Δεδομένου ότι αρμόδιες αρχές για την πρόληψη, καταστολή, διερεύνηση, εξιχνίαση και δίωξη αξιόποινων πράξεων, αλλά και την εκτέλεση ποινικών κυρώσεων είναι η Ελληνική Αστυνομία, το Λιμενικό Σώμα, η Ελληνική Ακτοφυλακή και το Πυροσβεστικό Σώμα, ως υπεύθυνοι επεξεργασίας των προσωπικών δεδομένων, που συλλέγονται από τα συστήματα επιτήρησης, καθίστανται οι ανωτέρω Υπηρεσίες. Όσον αφορά τη διαχείριση της κυκλοφορίας στο οδικό δίκτυο και των τροχαίων ατυχημάτων – δυστυχημάτων υπεύθυνος επεξεργασίας είναι αποκλειστικά η Ελληνική Αστυνομία (Άρθρο 4 του Π.Δ. 75/2020).

Σύμφωνα με την υπ' αριθ. 1691/20/2501985 από 13/11/2020 Απόφαση του Αρχηγού της Ελληνικής Αστυνομίας⁴¹ η Διεύθυνση Επιχειρήσεων και Διαχείρισης Κρίσεων (Δ.Ε.ΔΙ.Κ.) (πρώην Ενιαίο Συντονιστικό Κέντρο Επιχειρήσεων και Διαχείρισης Κρίσεων (Ε.Σ.Κ.Ε.ΔΙ.Κ.)) ορίστηκε αρμόδια αναφορικά με τον σχεδιασμό, την οργάνωση και την υλοποίηση των ενεργειών, που πηγάζουν από τον ορισμό της Ελληνικής Αστυνομίας, ως υπεύθυνου επεξεργασίας προσωπικών δεδομένων, κατά το άρθρο 4 του Π.Δ. 75/2020. Πιο συγκεκριμένα, η Δ.Ε.ΔΙ.Κ. είναι επιφορτισμένη με όλες τις ενέργειες, που απαιτούνται ώστε να διασφαλίζεται η τήρηση

⁴¹ <https://diavgeia.gov.gr/doc/6%CE%9A%CE%A7646%CE%9C%CE%A4%CE%9B%CE%92-5%CE%A3%CE%A9?inline=true>

των διατάξεων, που αφορούν την εγκατάσταση και χρήση συστημάτων επιτήρησης σε δημόσιους χώρους, προκειμένου η επεξεργασία των προσωπικών δεδομένων, που συλλέγονται από αυτά να είναι σύμφωνη με τους σκοπούς που προβλέπει ο Ν. 3917/2011 και το Π.Δ. 75/2020, διασφαλίζοντας ταυτόχρονα τα δικαιώματα των ατόμων, που θίγονται από τη χρήση των συστημάτων επιτήρησης.

6.6.1.2. Συστήματα επιτήρησης και διαχείριση δεδομένων

Τα συστήματα επιτήρησης δεν μπορούν να εγκαθίστανται και να χρησιμοποιούνται ανεξέλεγκτα σε οποιονδήποτε δημόσιο χώρο, παρά μόνο στο μέτρο που είναι απαραίτητα για την εκπλήρωση των σκοπών που προαναφέρθηκαν, εφόσον αυτοί δεν μπορούν να επιτευχθούν με ηπιότερα μέσα και υπό την προϋπόθεση ότι υπάρχουν σοβαρές και πραγματικές ενδείξεις, όπως για παράδειγμα στατιστικά στοιχεία, μελέτες, μαρτυρίες, πληροφορίες κ.λπ., ότι στον συγκεκριμένο χώρο διαπράττονται ή πρόκειται να διαπραχθούν αξιόποινες πράξεις. Σε κάθε περίπτωση, πάντως, τα συστήματα επιτηρούν συγκεκριμένο χώρο και δεν καταγράφουν χώρους που δεν είναι δημόσιοι ή συνιστούν εσωτερικό κατοικιών (Άρθρο 5 παρ. 1 και 2 του Π.Δ. 75/2020). Επιπλέον, θα πρέπει να είναι συγχρονισμένη η ώρα και η ημερομηνία με την πραγματική, προκειμένου τα δεδομένα, που καταγράφονται, συλλέγονται και επεξεργάζονται να είναι ακριβή και αξιοποιήσιμα.

Ειδικά ως προς τα φορητά συστήματα επιτήρησης, αυτά επιτρέπονται μόνο σε περιπτώσεις που συντρέχει άμεσος κίνδυνος τέλεσης ορισμένων εκ των αξιόποινων πράξεων που αναφέρονται στο άρθρο 3 του Π.Δ. 75/2020, κατόπιν σχετικής απόφασης της Ελληνικής Αστυνομίας, στην οποία περιγράφονται αναλυτικά τα πραγματικά στοιχεία και οι λόγοι που καθιστούν αναγκαία και απαραίτητη τη λειτουργία τους (Άρθρο 5 παρ. 3 του Π.Δ. 75/2020).

Με τα συστήματα επιτήρησης η Ελληνική Αστυνομία, όπως και κάθε υπεύθυνος επεξεργασίας, λαμβάνει και καταγράφει δεδομένα εικόνας και ήχου από δημόσιους χώρους, τα οποία πολλές φορές μπορεί να οδηγήσουν στην ταυτοποίηση φυσικών προσώπων, συνεπώς συνιστούν προσωπικά δεδομένα.

Η εστίαση των καμερών κατά την επιτήρηση ενός δημόσιου χώρου επιτρέπεται μόνο για να διαπιστωθεί η διάπραξη ενός εγκλήματος, που εμπίπτει στον κατάλογο του άρθρου 3 του Π.Δ. 75/2020, κατόπιν αιτιολογημένης απόφασης της Ελληνικής Αστυνομίας και έγκρισης αυτής από εισαγγελέα πρωτοδικών. Σε κατεπείγουσες περιπτώσεις δύναται να πραγματοποιηθεί η εστίαση κατόπιν απόφασης της Ελληνικής Αστυνομίας και στη συνέχεια να ενημερωθεί άμεσα ο αρμόδιος εισαγγελέας, ο οποίος μπορεί να διατάξει τη διακοπή της διαδικασίας.

Τα δεδομένα, που συλλέγονται και τίθενται σε επεξεργασία κατά τη ρύθμιση της κυκλοφορίας, περιορίζονται μόνο στην αναγνώριση των πινακίδων κυκλοφορίας των οχημάτων και στην κατηγορία αυτών, δηλαδή αν πρόκειται για επιβατικά, φορτηγά, κ.λπ. (Άρθρο 7 παρ. 1 του Π.Δ. 75/2020).

Αν από τα δεδομένα ήχου, που έχουν συλλεχθεί από τα συστήματα κατά την επιτήρηση δημόσιων χώρων, είναι δυνατή η ταυτοποίηση προσώπων, τότε

απαγορεύεται η καταγραφή και επεξεργασία τους, εκτός εάν υπάρχει ειδική, πλήρως αιτιολογημένη απόφαση της Ελληνικής Αστυνομίας, η οποία έχει εγκριθεί από τον αρμόδιο εισαγγελέα. Η εξαίρεση αυτή εφαρμόζεται αποκλειστικά και μόνο για τον εντοπισμό και την αναγνώριση ατόμων, που εμπλέκονται σε εγκλήματα των άρθρων 183-191Α, 264-315Α, 322-353 και 372-405 του Π.Κ., καθώς και των κακουργημάτων του Ν. 4139/2013 περί εξαρτησιογόνων ουσιών, τα οποία περιλαμβάνονται στο άρθρο 6 παρ. 1 του Ν. 5002/2022 αναφορικά με την άρση απορρήτου για την διακρίβωση αξιόποινων πράξεων, υπό την προϋπόθεση ότι η περαιτέρω διερεύνηση της υπόθεσης καθίσταται αδύνατη ή εξαιρετικά δυσχερής με οποιονδήποτε άλλο τρόπο, λόγω του είδους και της έκτασης της παραβατικής συμπεριφοράς. Στην απόφαση της Ελληνικής Αστυνομίας αναφέρεται ρητά η αξιόποινη πράξη που διερευνάται, τα στοιχεία που συνδέουν τα ερευνώμενα άτομα με την τέλεση της αξιόποινης πράξης, ο σκοπός της επεξεργασίας των δεδομένων, η αδυναμία ή δυσχέρεια διαλεύκανσης της υπόθεσης με οποιοδήποτε άλλο τρόπο και μέσο και το απολύτως απαραίτητο χρονικό διάστημα επεξεργασίας των δεδομένων (Άρθρο 7 του Π.Δ. 75/2020).

Τα δεδομένα, που συλλέγονται από τα συστήματα επιτήρησης διατηρούνται το πολύ για 15 μέρες, μετά το πέρας των οποίων διαγράφονται αυτόματα και με τρόπο, που δεν είναι δυνατή η ανάκτησή τους. Κατ' εξαίρεση μπορούν να διατηρηθούν για μεγαλύτερο διάστημα εάν συντρέχει λόγος διερεύνησης των εγκλημάτων, που αναφέρονται στο άρθρο 3 του Π.Δ. 75/2020 και τα οποία έχουν προαναφερθεί. Σε αυτή την περίπτωση τα δεδομένα διατηρούνται μέχρι να εκδοθεί αμετάκλητη δικαστική απόφαση ή να παύσει οριστικά η δίωξη ή να παραγραφεί το διερευνώμενο αδίκημα. Όταν πληρείται μία από αυτές τις προϋποθέσεις, οι αρμόδιες δικαστικές αρχές ενημερώνουν την Ελληνική Αστυνομία, ώστε να προχωρήσει στη διαγραφή των σχετικών δεδομένων (Άρθρο 8 παρ. 1 του Π.Δ. 75/2020).

Τα δεδομένα δύναται να διατηρηθούν και όταν υφίστανται τεκμηριωμένες υπόνοιες ότι το υποκείμενο των δεδομένων προετοιμάζει και σχεδιάζει τη μελλοντική διάπραξη αδικημάτων του άρθρου 3 του Π.Δ. 75/2020. Οι υπόνοιες βασίζονται σε μαρτυρίες, σχετικές πληροφορίες αναφορικά με τις κινήσεις και επαφές του συγκεκριμένου προσώπου, αλλά και στο είδος, τη βαρύτητα και το πλήθος των εγκλημάτων για τα οποία έχει καταδικασθεί ή κατηγορηθεί κατά το παρελθόν. Για να διατηρηθούν αυτά τα δεδομένα, η Ελληνική Αστυνομία εκδίδει πλήρως αιτιολογημένη απόφαση, η οποία επαναξιολογείται κάθε δύο χρόνια (Άρθρο 8 παρ. 2 του Π.Δ. 75/2020).

Άλλη μία εξαίρεση, που επιτρέπει τη διατήρηση των δεδομένων που συλλέγονται από τα συστήματα επιτήρησης είναι η χρήση τους αποκλειστικά για εκπαιδευτικούς σκοπούς, όπως για παράδειγμα η εκπαίδευση των χειριστών του συστήματος. Σε αυτή την περίπτωση, εντός 15 ημερών από τη συλλογή των δεδομένων επιλέγονται εκείνα, που θεωρούνται απαραίτητα και χρήσιμα για τον συγκεκριμένο σκοπό και στην συνέχεια εντός δύο μηνών ανωνυμοποιούνται, προκειμένου να καθίσταται αδύνατη η ταυτοποίηση οποιουδήποτε ατόμου. Κάθε πρόσωπο, που χρησιμοποιεί αυτά τα

δεδομένα για εκπαιδευτικούς λόγους – εκπαιδευτής, εκπαιδευόμενος ή τρίτος – υπογράφει δήλωση εχεμύθειας (Άρθρο 8 παρ. 3 του Π.Δ. 75/2020).

Η Ελληνική Αστυνομία μπορεί να χρησιμοποιεί συστήματα επιτήρησης κατά τη διάρκεια δημόσιων υπαίθριων συναθροίσεων για τους σκοπούς του άρθρου 3 του Π.Δ. 75/2020, κατόπιν πλήρως αιτιολογημένης απόφασής της, αναφορικά με τους λόγους που κρίνεται απαραίτητη η επιτήρηση, το χρόνο ενεργοποίησης των συστημάτων και το χρονικό διάστημα λειτουργίας τους, η οποία εγκρίνεται από αρμόδιο εισαγγελέα πρωτοδικών και εφόσον έχουν ενημερωθεί σχετικά με τη λειτουργία των συστημάτων ο υπεύθυνος και οι μετέχοντες στη συνάθροιση. Συνεπώς, η αιτιολογημένη απόφαση της ΕΛ.ΑΣ., η έγκριση αυτής από αρμόδιο εισαγγελέα και η ενημέρωση του υπεύθυνου και των μετεχόντων στη συνάθροιση αποτελούν βασικές προϋποθέσεις, που πρέπει να συντρέχουν σωρευτικά και όχι διαζευκτικά.

Κατά την επιτήρηση δημόσιας υπαίθριας συνάθροισης είναι δυνατή η λήψη πλήρους εικόνας προκειμένου να διαπιστωθεί το πλήθος των παρευρισκόμενων ατόμων, αλλά και η διαδρομή αυτής, αποκλειστικά για τους σκοπούς, που προβλέπει το Προεδρικό Διάταγμα 75/2020, εφόσον κρίνεται απαραίτητη για την ομαλή διεξαγωγή της συγκέντρωσης και δεν γίνεται εστίαση σε συγκεκριμένα πρόσωπα. Αν η συνάθροιση ολοκληρωθεί ομαλά, τα στοιχεία που έχουν συλλεχθεί από τα συστήματα επιτήρησης καταστρέφονται αυτόματα με μέριμνα της Ελληνικής Αστυνομίας, μέσα σε 48 ώρες από τη στιγμή, που έληξε η συνάθροιση. Διαφορετικά, αν λάβει χώρα κάποιο περιστατικό, που εμπίπτει στους σκοπούς της επιτήρησης, διατηρούνται για μεγαλύτερο χρονικό διάστημα, όπως ορίστηκε προηγουμένως (Άρθρο 6 του Π.Δ. 75/2020). Σε δημόσιες συναθροίσεις, που δεν λαμβάνουν χώρα επεισόδια⁴², ενδέχεται να διαπραχθούν τα αδικήματα της απείθειας, της βίας κατά υπαλλήλων και δικαστικών προσώπων, της στάσης και της παραβίασης των μέτρων για την πρόληψη ασθενειών (Άρθρα 169, 167, 170 και 285 του Π.Κ.). Αν, όμως, ξεσπάσουν επεισόδια, τότε αυτά συνήθως αφορούν τα αδικήματα της σωματικής βλάβης σε οποιαδήποτε μορφή της – απλή, επικίνδυνη - βαριά, της φθοράς ξένης ιδιοκτησίας, της έκρηξης, της κατασκευής και κατοχής εκρηκτικών υλών, παραβιάσεις των διατάξεων του Ν. 2168/1993 «Περί όπλων» και της απόπειρας ανθρωποκτονίας (Άρθρα 308, 309, 310, 378, 270, 272 του Π.Κ.) (Εθνικό Σχέδιο, 2021: 20).

Όσον αφορά τη διάθεση των δεδομένων, που συλλέγονται από τα συστήματα επιτήρησης, αυτά μπορούν να χορηγηθούν σε δικαστικές, εισαγγελικές ή διοικητικές αρχές, ανάλογα με τον σκοπό για τον οποίο συλλέχθηκαν ή/και στο θύμα ή στον φερόμενο ως δράστη μίας υπόθεσης, εφόσον το συγκεκριμένο πρόσωπο έχει υποβάλλει σχετικό αίτημα και έχει αποδείξει ότι τα δεδομένα αυτά είναι αναγκαία προκειμένου να θεμελιώσει ή να ασκήσει νομικές αξιώσεις. Σε κάθε περίπτωση, ανεξαιρέτως, η Ελληνική Αστυνομία πρέπει να εξασφαλίζει ότι τα δεδομένα, που διαβιβάζονται δεν

⁴² Τα επεισόδια συνιστούν διατάραξη της κοινής ειρήνης κατ' άρθρο 189 του Π.Κ. και συνεπώς προϋποθέτουν συμμετοχή ατόμων σε συγκεντρωμένο πλήθος, που με ενωμένες δυνάμεις διαπράττουν βιαιοπραγίες κατά προσώπων ή πραγμάτων. Συνεπώς, αδικήματα που διαπράττονται από μεμονωμένα άτομα και δεν απαιτούν τη δράση ατόμων με ενωμένες δυνάμεις, δεν θεωρούνται επεισόδια.

έχουν αλλοιωθεί, είναι τα απολύτως απαραίτητα και αναγκαία και διαβιβάζονται με ασφαλή τρόπο, χωρίς να διακυβεύεται η ακεραιότητά τους ή να ελλοχεύει κίνδυνος υποκλοπής (Άρθρο 9 του Π.Δ. 75/2020).

6.6.1.3. Δικαιώματα των υποκειμένων

Σχετικά με τα δικαιώματα των υποκειμένων, των οποίων τα δεδομένα τίθενται σε επεξεργασία, εκτός από τις διατάξεις που προβλέπονται από τον GDPR και τον Ν. 4624/2019, στο άρθρο 10 του Π.Δ. 75/2020 αποτυπώνεται η υποχρέωση της Ελληνικής Αστυνομίας να ενημερώνει το κοινό, που εισέρχεται σε χώρο που επιτηρείται, για την ύπαρξη συστημάτων επιτήρησης. Η ενημέρωση δύναται να πραγματοποιηθεί με κάθε πρόσφορο μέσο, ήτοι τηλεβόες, προφορική ενημέρωση των υποκειμένων, εμφανείς πινακίδες, ανάρτηση στην επίσημη ιστοσελίδα της Ελληνικής Αστυνομίας και στους επίσημους λογαριασμούς αυτής στα μέσα κοινωνικής δικτύωσης, ενώ περιλαμβάνει τον σκοπό, τον υπεύθυνο επεξεργασίας και κάθε χρήσιμη πληροφορία σχετικά με την επιτήρηση (Άρθρο 10 του Π.Δ. 75/2020).

Επιπλέον, το υποκείμενο των δεδομένων έχει δικαίωμα να υποβάλλει αίτημα και να ζητήσει πληροφορίες για τα δεδομένα, που έχουν καταγραφεί και το αφορούν, για τους αποδέκτες αυτών, αλλά και να ζητήσει αντίγραφο του σχετικού υλικού. Προς διευκόλυνση της αναζήτησης κρίνεται απαραίτητο ο αιτών να προσδιορίσει τον τόπο και τον χρόνο, που ενδεχομένως έλαβε χώρα η καταγραφή των προσωπικών του δεδομένων. Η Ελληνική Αστυνομία οφείλει να του απαντήσει εντός 30 ημερών, ενημερώνοντάς τον εάν υφίστανται τέτοιο υλικό, και σε θετική περίπτωση, εάν στα δεδομένα, που πρόκειται να χορηγηθούν στον αιτούντα περιλαμβάνονται εικόνες ή ηχητικά αποσπάσματα που αφορούν τρίτα πρόσωπα, προβαίνει σε κάλυψη ή αφαίρεση αυτών, αντίστοιχα (Άρθρο 10 του Π.Δ. 75/2020).

Όπως εύκολα μπορεί να διαπιστώσει κανείς, σε κάθε ανακοίνωση της Ελληνικής Αστυνομίας στην επίσημη σελίδα της στον ιστότοπο <https://www.astynomia.gr/systimata-epitirisis-2-0/> αναφορικά με την εγκατάσταση και λειτουργία συστημάτων επιτήρησης, εκτός από την συγκεκριμένη κατά περίπτωση απόφαση της Διεύθυνσης Επιχειρήσεων και Διαχείρισης Κρίσεων και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας που είναι το Αρχηγείο της Ελληνικής Αστυνομίας, παρέχεται υπόδειγμα εντύπου αίτησης των φυσικών προσώπων που επιθυμούν να ασκήσουν τα δικαιώματα της πρόσβασης, διόρθωσης, διαγραφής ή/ και περιορισμού της επεξεργασίας, αναφορικά με τα προσωπικά τους δεδομένα.

ΕΝΤΥΠΟ ΑΣΚΗΣΗΣ ΔΙΚΑΙΩΜΑΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ							
[Χρήση αποκλειστικά για την ικανοποίηση αιτημάτων των υποκειμένων δεδομένων. Συμπληρώστε με κεφαλαίους χαρακτήρες. Τα πεδία με (*) είναι υποχρεωτικά.]							
1. Στοιχεία υποκειμένου των δεδομένων							
Διεύθυνση *	Επώνυμο*: Όνομα*: Οδός: Αριθμός: Τ.Κ.: Πόλη: Χώρα: ΑΔΤ* ή Διαβατηρίου*: Email: Τηλέφωνο/α επικοινωνίας**:						
2. Στοιχεία εκπροσώπου του υποκειμένου των δεδομένων³ (Σε περίπτωση εκπροσώπησης του υποκειμένου των δεδομένων, συμπληρώνεται υποχρεωτικά ο παρακάτω πίνακας.)							
Διεύθυνση *	Επώνυμο*: Όνομα*: Οδός: Αριθμός: Τ.Κ.: Πόλη: Χώρα: ΑΔΤ* ή Διαβατηρίου*: Email: Τηλέφωνο/α επικοινωνίας**:						
1. Συμπληρώνεται υποχρεωτικά είτε η ταχυδρομική είτε η ηλεκτρονική δ/ση του αιτούντα (e-mail). 2. Το τηλέφωνο επικοινωνίας συμπληρώνεται για επικοινωνία με τον αιτούντα σε περίπτωση που κριθεί απαραίτητο. 3. Συμπληρώνεται μόνον όπου εφαρμόζεται, π.χ. όταν το υποκείμενο των δεδομένων είναι ανήλικο τέκνο σύμφωνα με τις διατάξεις του Αστικού Κώδικα ή όταν η εκπροσώπηση ενώπιον της αρμόδιας Αρχής έχει ανατεθεί σε πληρεξούσιο δικηγόρο ή άλλο τρίτο πρόσωπο. Υποβάλλεται απαραίτητως συνημμένα και η ηλεκτρονική εξουσιοδότηση ή εξουσιοδότηση με βεβαίωση του γνησίου της υπογραφής του εξουσιοδοτούμενου. 4. Η συμπλήρωση των στοιχείων ηλεκτρονικής διεύθυνσης ταχυδρομείου καθώς και τα τηλέφωνα επικοινωνίας είναι <u>υποχρεωτικά</u> γιατί για τον εντοπισμό των προσωπικών δεδομένων του αιτούντα σε βιολογικό υλικό θα απαιτηθούν περαιτέρω στοιχεία για την ταυτοποίησή του. 5. Το έντυπο μπορεί να υποβληθεί μέσω μηνύματος ηλεκτρονικού ταχυδρομείου στην ηλεκτρονική διεύθυνση kerik@astynomia.gr ή μέσω συμβατικής αλληλογραφίας στην διεύθυνση: ΚΕΠΙΚ, Π. Κανελλοπούλου 4 τ.κ.10177, Αθήνα							
3. Δικαίωμα στο οποίο αφορά το αίτημα* (επιλέξτε το δικαίωμα το οποίο επιθυμείτε να ασκήσετε)							
☐ Δικαίωμα πρόσβασης ☐ Δικαίωμα διόρθωσης ☐ Δικαίωμα διαγραφής ☐ Δικαίωμα περιορισμού επεξεργασίας							
4. Περιγραφή αιτήματος* (Παρακαλείσθε όπως καταγράψετε αναλυτικά το αίτημά σας στο παρακάτω πεδίο)							
5. Σχετικά έγγραφα/στοιχεία (Απαραίτηστε τα συνημμένα έγγραφα)							
<table border="1"><tr><td>1.</td><td>Ηλεκτρονική υπεύθυνη δήλωση (e-δίστι)⁵ ή, ελλείψει αυτής, αντίγραφο επικυρωμένης από Κ.Ε.Π. ή Α.Τ. υπεύθυνης δήλωσης του άρθρου 8 του Ν. 1599/1986 με βεβαίωση του γνησίου υπογραφής*, με την οποία θα δηλώνεται η ακρίβεια των επί της αίτησης στοιχείων του υποκειμένου.*</td></tr><tr><td>2.</td><td>Αντίγραφο κατεχόμενου Α.Δ.Τ. ή διαβατηρίου.*</td></tr><tr><td>3.</td><td>Πρόσφατη φωτογραφία υψηλής ανάλυσης του αιτούντα (υποκείμενο της επεξεργασίας)</td></tr></table>		1.	Ηλεκτρονική υπεύθυνη δήλωση (e-δίστι) ⁵ ή, ελλείψει αυτής, αντίγραφο επικυρωμένης από Κ.Ε.Π. ή Α.Τ. υπεύθυνης δήλωσης του άρθρου 8 του Ν. 1599/1986 με βεβαίωση του γνησίου υπογραφής*, με την οποία θα δηλώνεται η ακρίβεια των επί της αίτησης στοιχείων του υποκειμένου.*	2.	Αντίγραφο κατεχόμενου Α.Δ.Τ. ή διαβατηρίου.*	3.	Πρόσφατη φωτογραφία υψηλής ανάλυσης του αιτούντα (υποκείμενο της επεξεργασίας)
1.	Ηλεκτρονική υπεύθυνη δήλωση (e-δίστι) ⁵ ή, ελλείψει αυτής, αντίγραφο επικυρωμένης από Κ.Ε.Π. ή Α.Τ. υπεύθυνης δήλωσης του άρθρου 8 του Ν. 1599/1986 με βεβαίωση του γνησίου υπογραφής*, με την οποία θα δηλώνεται η ακρίβεια των επί της αίτησης στοιχείων του υποκειμένου.*						
2.	Αντίγραφο κατεχόμενου Α.Δ.Τ. ή διαβατηρίου.*						
3.	Πρόσφατη φωτογραφία υψηλής ανάλυσης του αιτούντα (υποκείμενο της επεξεργασίας)						
6. Υπογραφή αιτούντος*							
Ημερομηνία	Υπογραφή						
6. Σε περίπτωση υποβολής αίτησης από υποκείμενο που διαμένει ή εργάζεται στην ελληνική επικράτεια, απαιτείται η υποβολή συνημμένης ηλεκτρονικής υπεύθυνης δήλωσης (e-δίστι) προκειμένου να διενεργηθεί με μεγαλύτερη αξιοπιστία η ταυτοποίησή του. Σε κάθε περίπτωση, η αρμόδια Αρχή διατηρεί το δικαίωμα να επιβεβαιώνει την αλήθεια και την ακρίβεια των στοιχείων του αιτούντα και να εφαρμόζει οποτεδήποτε διαδικασίες επαλήθευσης - ταυτοποίησης με σκοπό την επιβεβαίωση της ταυτότητάς του.							

Εικόνα 7: Έντυπο άσκησης δικαιωμάτων υποκειμένων δεδομένων

Κατ' εφαρμογή των διατάξεων του άρθρου 10 παρ. 4 και 5 του Π.Δ. 75/2020, η ΕΛ.ΑΣ. δύναται να αρνηθεί να ικανοποιήσει το αίτημα του υποκειμένου για τους λόγους που προβλέπει ο GDPR στο άρθρο 23 και ο Ν. 4624/2019 στα άρθρα 32, 54, 55 και 56. Σε αυτή την περίπτωση, αλλά και σε εκείνη, που ο αιτών δεν λάβει σχετική απάντηση εντός του προβλεπόμενου χρόνου, έχει τη δυνατότητα να προσφύγει στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, εκτός εάν χαίρουν εφαρμογής οι διατάξεις των άρθρων 10 παρ. 5 και 59 του Ν. 4624/2019.

6.6.1.4. Μέτρα ασφαλείας των δεδομένων του συστήματος

Η Ελληνική Αστυνομία, ως υπεύθυνος επεξεργασίας, οφείλει να λαμβάνει κατάλληλα μέτρα κατά τον σχεδιασμό, εγκατάσταση και λειτουργία ενός συστήματος επιτήρησης, προκειμένου να περιορίζονται στο μέγιστο δυνατό οι κίνδυνοι για τα προσωπικά δεδομένα. Κατά την επιλογή των μέτρων λαμβάνονται υπόψη η διαθέσιμη τεχνολογία, το κόστος εγκατάστασης και χρήσης του εκάστοτε συστήματος, ο σκοπός και ο τρόπος λειτουργίας του, καθώς και οι ενδεχόμενοι κίνδυνοι σε βάρος των πολιτών (Άρθρο 11 του Π.Δ. 75/2020).

Για την ασφάλεια των δεδομένων, που συλλέγονται από το σύστημα επιτήρησης, η ΕΛ.ΑΣ. θέτει σε λειτουργία ένα σύστημα διαχείρισης της ασφάλειας αυτών, ώστε τα δεδομένα να προστατεύονται από τυχόν καταστροφή, απώλεια, μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ή παράνομη χρήση, διασφαλίζοντας παράλληλα την

αποκατάστασή τους σε συντρέχουσα περίπτωση. Σε αυτό το πλαίσιο συντάσσει πολιτική ασφαλείας, η οποία αναθεωρείται ανά τακτά διαστήματα και όποτε αυτό κρίνεται απαραίτητο και εξειδικεύει τα μέτρα ασφαλείας που πρέπει να εφαρμόζονται, ελέγχοντας και αξιολογώντας συστηματικά την τήρησή τους (Άρθρο 11 του Π.Δ. 75/2020).

Σύμφωνα με την παράγραφο 3 του άρθρου 11 του Π.Δ. 75/2020 τα μέτρα ασφαλείας που οφείλει να λαμβάνει η Ελληνική Αστυνομία περιλαμβάνουν κατ' ελάχιστο:

- τη διάκριση των ρόλων και δικαιωμάτων των χρηστών του συστήματος διαχείρισης ασφάλειας των δεδομένων αναφορικά με την προβολή, εξαγωγή και διαγραφή δεδομένων, την εξουσιοδότηση για εξαγωγή δεδομένων, την ανάθεση ρόλων σε άλλους χρήστες, την τεχνική υποστήριξη και τον έλεγχο των ενεργειών που πραγματοποιούνται,
- την εκπαίδευση των χρηστών ανάλογα με τις αρμοδιότητές τους,
- την πρόσβαση στα δεδομένα και στους χώρους των εγκαταστάσεων μόνο από εξουσιοδοτημένα και κατάλληλα εκπαιδευμένα άτομα,
- την πρόσβαση στο λογισμικό του συστήματος επιτήρησης, μόνο με χρήση του ονόματος χρήστη και του αντίστοιχου κωδικού, που χρησιμοποιούνται αποκλειστικά από μοναδικό χρήστη,
- την καταγραφή των ενεργειών που γίνονται επί των δεδομένων του συστήματος, η οποία, σε κάθε περίπτωση, περιλαμβάνει τα στοιχεία του χρήστη, τον χρόνο και τον σκοπό της πρόσβασης στα δεδομένα, καθώς και το είδος της πρόσβασης ή διαβίβασης των δεδομένων,
- την πρόσβαση στο σύστημα μόνο από συγκεκριμένα τερματικά, με ασφαλές δίκτυο και μεθόδους κρυπτογράφησης βάσει των διεθνών προτύπων,
- τη λήψη επιπρόσθετων μέτρων, κατόπιν εκτίμησης του αντικτύπου κινδύνου στα προσωπικά δεδομένα για τις περιπτώσεις που χρησιμοποιούνται φορητά συστήματα επιτήρησης.

6.6.1.5. Απόφαση τοποθέτησης και λειτουργίας του συστήματος επιτήρησης

Τόσο για την εγκατάσταση όσο και τη λειτουργία ενός συστήματος επιτήρησης, όπως έχει προαναφερθεί, απαιτείται πλήρως αιτιολογημένη απόφαση της Ελληνικής Αστυνομίας.

Σύμφωνα με το άρθρο 12 παρ. 1 του Π.Δ. 75/2020, προκειμένου να εγκατασταθεί ένα σύστημα επιτήρησης απαιτείται προηγούμενη απόφαση της Ελληνικής Αστυνομίας, η οποία πρέπει να περιέχει συγκεκριμένες πληροφορίες. Ειδικότερα, στην απόφαση αναφέρεται το σημείο, που πρόκειται να τοποθετηθεί το σύστημα, τα τεχνικά του χαρακτηριστικά και οι λόγοι που καθιστούν νόμιμη και απαραίτητη την επιτήρηση του συγκεκριμένου χώρου. Η απόφαση έχει ισχύ για το πολύ μέχρι τρία έτη και πρέπει να επαναξιολογείται σε τακτική βάση.

Για να τεθεί σε λειτουργία ένα σύστημα επιτήρησης απαιτείται νέα απόφαση της Ελληνικής Αστυνομίας, στην οποία περιγράφονται, όπως έχει ήδη αναφερθεί στην παρούσα εργασία, η ημερομηνία ενεργοποίησης και το χρονικό διάστημα λειτουργίας του, η εμβέλειά του και ο λόγος που κρίνεται απαραίτητη η λειτουργία του. Εάν συντρέχουν σχετικοί λόγοι, το χρονικό διάστημα λειτουργίας του συστήματος δύναται να παραταθεί με νέα πλήρως αιτιολογημένη απόφαση της Ελληνικής Αστυνομίας (Άρθρο 12 παρ. 2 του Π.Δ. 75/2020).

Προτού εγκατασταθεί και τεθεί σε λειτουργία ένα σύστημα επιτήρησης, η ΕΛ.ΑΣ. εκτιμά και αξιολογεί τον αντίκτυπο της επιτήρησης στα προσωπικά δεδομένα και την ιδιωτικότητα των φυσικών προσώπων. Ακόμα και εάν εγκατασταθεί νέο λογισμικό ή προστεθεί εξοπλισμός στον ήδη υπάρχοντα, ειδικά εάν διαφοροποιούνται τα τεχνικά χαρακτηριστικά και οι δυνατότητες επεξεργασίας των προσωπικών δεδομένων, η Ελληνική Αστυνομία προβαίνει σε εκ νέου εκτίμηση του αντικτύπου των επιπτώσεων της επεξεργασίας. Όπως έχει ήδη προαναφερθεί, η απόφαση περί λειτουργίας των συστημάτων επιτήρησης κοινοποιούνται στο κοινό με κάθε πρόσφορο μέσο, ήτοι πινακίδες, ανακοινώσεις στην επίσημη ιστοσελίδα της Ελληνικής Αστυνομίας, τηλεβόες, κ.λπ. (Άρθρο 12 παρ. 1 και 2 του Π.Δ. 75/2020).

Δεδομένου ότι η δράση της Ελληνικής Αστυνομίας δεν είναι ανεξέλεγκτη και αυθαίρετη, τόσο η απόφαση εγκατάστασης όσο και λειτουργίας των συστημάτων υποβάλλονται στον αρμόδιο εισαγγελέα πρωτοδικών, ώστε να εξετάσει τα διαλαμβανόμενα σε αυτές και σε συντρέχουσα περίπτωση, να ζητήσει τυχόν επιπρόσθετες πληροφορίες, προκειμένου να ελέγξει αν τηρούνται τα προβλεπόμενα από το νόμο (Άρθρο 12 παρ. 3 του Π.Δ. 75/2020).

6.6.2. Μελέτη περίπτωσης - Διαβούλευση για σύστημα επιτήρησης

Σύμφωνα με την υπ' αριθ. 4/2024 Γνωμοδότηση της Α.Π.Δ.Π.Χ.⁴³, το έτος 2024 η Ελληνική Αστυνομία συνέταξε και υπέβαλε για διαβούλευση σε αυτή, κατ' εφαρμογή του άρθρου 67 του Ν. 4624/2019, Μελέτη Εκτίμησης Αντικτύπου αναφορικά με την προμήθεια συστήματος επιτήρησης με σταθερές και περιστρεφόμενες κάμερες, οι οποίες καταγράφουν και ήχο, για τις ανάγκες της Γενικής Αστυνομικής Διεύθυνσης Αττικής, με σκοπό την αντιμετώπιση της εγκληματικότητας και τη διαχείριση της κυκλοφορίας στο οδικό δίκτυο. Επειδή το εν λόγω σύστημα εξυπηρετεί σκοπούς, που υπάγονται τόσο στον GDPR, όπως η διαχείριση κυκλοφορίας, όσο και στην Οδηγία 2016/680, όπως ενσωματώθηκε στο ελληνικό δίκαιο με τον Ν. 4624/2019, η διαβούλευση με την Α.Π.Δ.Π.Χ. ζητήθηκε διότι η συλλογή και επεξεργασία των δεδομένων με το εν λόγω σύστημα ενδέχεται να εγκυμονούν υψηλό κίνδυνο για αυτά. Η Α.Π.Δ.Π.Χ. αφού εξέτασε το αίτημα της Ελληνικής Αστυνομίας βάσει αυτών των διατάξεων, διαπίστωσε ότι επί του συνόλου ικανοποιεί τις απαιτούμενες προϋποθέσεις που προβλέπει το άρθρο 65 παρ. 3 του Ν. 4624/2019.

⁴³ https://www.dpa.gr/sites/default/files/2024-12/%CE%93%CE%9D%CE%A9%CE%9C%CE%9F%CE%94%CE%9F%CE%A4%CE%97%CE%A3%CE%97%204_2024%20anonym.pdf

Πιο συγκεκριμένα, διαπίστωσε ότι η εκτίμηση αντικτύπου της ΕΛ.ΑΣ. περιείχε τον σκοπό και τις λειτουργίες του συστήματος, την εκτίμηση της αναγκαιότητας και αναλογικότητας της επεξεργασίας σχετικά με τους σκοπούς χρήσης του συστήματος, την εκτίμηση των κινδύνων, που ενδέχεται να προκύψουν κατά την συλλογή και επεξεργασία των προσωπικών δεδομένων και μέτρα για την αντιμετώπισή τους, καθώς και γνωμοδότηση του Υπεύθυνου Προστασίας Δεδομένων (Υ.Π.Δ.) της Ελληνικής Αστυνομίας, για τον οποίο έγινε λόγος στην Ενότητα 5.2.2 της παρούσας εργασίας.

Η Α.Π.Δ.Π.Χ. επεσήμανε ότι η μελέτη εκτίμησης αντικτύπου δεν αφορά τη χρήση μεθόδων αυτοματοποιημένης επεξεργασίας με συστήματα τεχνητής νοημοσύνης ή αυτόματης αναγνώρισης πινακίδων, τα οποία, έτσι και αλλιώς, δεν προβλέπονται από το ισχύον νομικό πλαίσιο λειτουργίας της Ελληνικής Αστυνομίας.

Επιπλέον, διατύπωσε ορισμένες συμβουλές προς την Ελληνική Αστυνομία, αναφορικά με την ενίσχυση της διαφάνειας, την ενίσχυση του ρόλου του Υ.Π.Δ., τον καθορισμό ελάχιστων τεχνικών προδιαγραφών των συστημάτων και τη χρήση του υλικού για εκπαιδευτικούς σκοπούς.

Πιο συγκεκριμένα, η Α.Π.Δ.Π.Χ. σύστησε στην Ελληνική Αστυνομία, προκειμένου να ενισχύσει τη διαφάνεια των ενεργειών της, να παράσχει πληροφορίες στα υποκείμενα των δεδομένων για το εύρος περιοχών που θα καλύπτει μία κάμερα, αξιοποιώντας τις σύγχρονες τεχνολογίες, όπως για παράδειγμα οι διαδικτυακοί χάρτες και δημοσιεύοντας το πλήρες περιεχόμενο της απόφασης λειτουργίας αυτής και όχι περίληψη ή επιλεκτικά στοιχεία της απόφασης. Λαμβάνοντας υπόψη τον όγκο και την πολυπλοκότητα των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων, που χειρίζεται η ΕΛ.ΑΣ., η Α.Π.Δ.Π.Χ. έκρινε ότι ένας μόνο Υ.Π.Δ. δεν αρκεί για να ανταπεξέλθει στις απαιτήσεις όλων των περιπτώσεων που του ανατίθενται, συμπεριλαμβανομένης της υπό διαβούλευσης περίπτωσης και πως είναι απαραίτητη η υποστήριξή του, τόσο με κατάλληλους πόρους όσο και με επιπρόσθετο προσωπικό. Για το λόγο αυτό, αξίζει να σημειωθεί ότι στο πλαίσιο αναδιοργάνωσης της ΕΛ.ΑΣ., όπως αναφέρθηκε στην Ενότητα 5.2, στην Ελληνική Αστυνομία λειτουργεί από το 2025 Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, το οποίο παρέχει υποστήριξη στον Υ.Π.Δ..

Όσον αφορά τις τεχνικές προδιαγραφές των συσκευών, η Α.Π.Δ.Π.Χ. σύστησε να προσδιοριστούν συγκεκριμένες ελάχιστες προδιαγραφές, όπως για παράδειγμα η ασφαλής μετάδοση, δυνατότητες θόλωσης, απόκρυψης περιοχών και επαναφορά εστίασης, κλπ., που θα διασφαλίζουν την προστασία των δεδομένων ήδη από τον σχεδιασμό και θα επικαιροποιούνται σε τακτική βάση.

Τέλος, η Α.Π.Δ.Π.Χ. διαπίστωσε ότι στην Μελέτη Εκτίμησης Αντικτύπου της Ελληνικής Αστυνομίας υπήρχαν ασάφειες ως προς τη χρήση του συλλεχθέντος υλικού για εκπαιδευτικούς σκοπούς κατόπιν ανωνυμοποίησής του, επισημαίνοντας ότι θα πρέπει να υπάρχει πλήρης ανωνυμοποίηση των δεδομένων και διασφάλιση ότι θα είναι αδύνατη η μεταγενέστερη ταυτοποίηση φυσικών προσώπων.

6.6.3. Συμπεράσματα

Η Ελληνική Αστυνομία χρησιμοποιεί συστήματα επιτήρησης δημόσιων χώρων, για συγκεκριμένους σκοπούς, που αφορούν την πρόληψη και καταστολή των αξιόποινων πράξεων που αποτυπώνονται στον κατάλογο του άρθρου 3 του Π.Δ. 75/2020, αλλά και τη ρύθμιση κυκλοφορίας του οδικού δικτύου, κατόπιν απόφασής της, η οποία υποβάλλεται άμεσα σε αρμόδιο εισαγγελέα προς ενημέρωση και έλεγχο της νομιμότητας και στη συνέχεια εφόσον εγκριθεί, κοινοποιείται στο κοινό με κάθε πρόσφορο μέσο προκειμένου να λαμβάνει γνώση, κατ' εφαρμογή της αρχής της νομιμότητας, αντικειμενικότητας και διαφάνειας και της αρχής του σκοπού. Έτσι, απαγορεύεται η καταγραφή και χρήση των δεδομένων για οποιονδήποτε άλλο σκοπό, όπως για παράδειγμα την απλή παρακολούθηση των πολιτών.

Τα δεδομένα, που καταγράφονται είναι τα απολύτως απαραίτητα για τον εκάστοτε συγκεκριμένο σκοπό, δεν πρέπει να αλλοιώνονται και διατηρούνται για συγκεκριμένο χρονικό διάστημα, μετά το πέρας του οποίου διαγράφονται αυτόματα. Επιπλέον, τα συστήματα επιτήρησης είναι συγχρονισμένα με την πραγματική ώρα και ημερομηνία και καταγράφουν συγκεκριμένους, ειδικά ορισμένους δημόσιους χώρους και όχι χώρους που δεν είναι δημόσιοι ή συνιστούν εσωτερικό κατοικιών. Έτσι, λοιπόν, διασφαλίζονται οι αρχές της ελαχιστοποίησης των δεδομένων, της περιόδου αποθήκευσης και της ακρίβειας αυτών.

Δεδομένου ότι η Ελληνική Αστυνομία λαμβάνει οργανωτικά και τεχνικά μέτρα για την προστασία των δεδομένων, ελέγχει την πρόσβαση σε αυτά και τηρεί αρχείο με τις ενέργειες, που πραγματοποιούνται κατά τη λειτουργία των συστημάτων επιτήρησης και την επεξεργασία των δεδομένων, προστατεύει το συλλεχθέν υλικό από τυχόν μη εξουσιοδοτημένη πρόσβαση, εξασφαλίζοντας την ακεραιότητα και εμπιστευτικότητα των δεδομένων. Με τα αρχεία που τηρεί η Ελληνική Αστυνομία και τις αποφάσεις που εκδίδει, μπορεί να αποδείξει, όποτε της ζητηθεί, τόσο σε εισαγγελικές αρχές, όσο και στην Α.Π.Δ.Π.Χ. ότι εφαρμόζει τις νομικά κατοχυρωμένες βασικές αρχές επεξεργασίας των δεδομένων.

Μάλιστα, όπως αποδεικνύεται με την υπ' αριθ. 4/2024 Γνωμοδότηση της Α.Π.Δ.Π.Χ., η Ελληνική Αστυνομία στο πλαίσιο προμήθειας συστήματος επιτήρησης και πριν αυτό εγκατασταθεί και τεθεί σε λειτουργία, διατύπωσε μελέτη εκτίμησης αντικτύπου, το οποίο υπέβαλε στην Α.Π.Δ.Π.Χ. για διαβούλευση, ώστε να λάβει την επίσημη γνώμη της σχετικά με την συμμόρφωση του συστήματος και της χρήσης αυτού με το νομικό πλαίσιο περί προστασίας προσωπικών δεδομένων, όπως ορίζει το άρθρο 67 του Ν. 4624/2019.

Συνεπώς, η Ελληνική Αστυνομία κατά την επιτήρηση των δημόσιων χώρων με συστήματα καταγραφής δεδομένων, μεριμνά για την προστασία των προσωπικών δεδομένων και εφαρμόζει τις βασικές αρχές επεξεργασίας, που προβλέπει ο GDPR και ο Ν. 4624/2019.

6.7. Διαγωνισμός πρόσληψης ιδιωτών στις Σχολές της Ελληνικής Αστυνομίας

Κάθε χρόνο πλήθος νέων ατόμων υποβάλλει αιτήσεις για την κατάταξή τους στις Σχολές Αξιωματικών και Αστυφυλάκων της Ελληνικής Αστυνομίας. Σύμφωνα με το άρθρο 4 του Π.Δ. 4/1995⁴⁴, όπως τροποποιήθηκε και ισχύει σήμερα, κάθε υποψήφιος οφείλει να υποβάλλει αυτοπροσώπως στην κατά τόπο αρμόδια αστυνομική Υπηρεσία συμπληρωμένη ενυπόγραφη αίτηση συμμετοχής και τα απαιτούμενα δικαιολογητικά, αλλά και να συμμετέχει στις προκαταρκτικές εξετάσεις, οι οποίες αποτελούνται από τις υγειονομικές και ψυχομετρικές εξετάσεις καθώς και τις αθλητικές δοκιμασίες. Η παραλαβή των αιτήσεων και των δικαιολογητικών πραγματοποιείται από τον Διοικητή της Υπηρεσίας ή άλλον Αξιωματικό, που ορίζεται αρμόδιος για αυτή (Άρθρο 4 του Π.Δ. 4/1995).

Όπως προκύπτει από την επίσημη ιστοσελίδα της Ελληνικής Αστυνομίας⁴⁵, καθώς και από προκηρύξεις αυτής αναφορικά με τον εν θέματι διαγωνισμό, στην υποβληθείσα αίτηση το φυσικό πρόσωπο παραχωρεί προσωπικά του δεδομένα, τα οποία διαχειρίζεται το Αρχηγείο της Ελληνικής Αστυνομίας, ως υπεύθυνος επεξεργασίας. Κατά την υποβολή της αίτησης, ο υποψήφιος ενημερώνεται από την Ελληνική Αστυνομία ότι τα δεδομένα του πρόκειται να τεθούν σε επεξεργασία, υπογράφοντας σχετικό έντυπο ενημέρωσης.

Πιο συγκεκριμένα, τα δεδομένα αφορούν τα στοιχεία ταυτότητας του υποψηφίου, τον κωδικό υποψηφίου, που του χορηγείται από το Υπουργείο Παιδείας, Θρησκευμάτων και Αθλητισμού (Υ.ΠΑΙ.Θ.Α.), τον ΑΜΚΑ του και ιατρικά του στοιχεία που προκύπτουν από τις εργαστηριακές και κλινικές εξετάσεις που υποβάλλεται προκειμένου να συμπληρωθεί το απαιτούμενο Δελτίο Υγειονομικής Εξέτασης, καθώς και εκείνα που προκύπτουν από την εξέτασή του από την Υγειονομική Επιτροπή Κατάταξης. Επιπλέον, η Ελληνική Αστυνομία συλλέγει και επεξεργάζεται δεδομένα, που αφορούν τις επιδόσεις του στις αθλητικές δοκιμασίες, την καταλληλότητά του ή μη κατά τις ψυχιατρικές εξετάσεις και εφόσον έχει επιτύχει στις προκαταρκτικές εξετάσεις, τον βαθμό του στις πανελλαδικές εξετάσεις της Δευτεροβάθμιας Εκπαίδευσης και τυχόν άλλα στοιχεία – κριτήρια που καθορίζουν την εισαγωγή του στις Σχολές της Αστυνομίας (όπως για παράδειγμα εάν ανήκει σε πολύτεκνη οικογένεια, εάν είναι τέκνο αστυνομικού που απεβίωσε εν ώρα καθήκοντος, κ.λπ.).

Υποβάλλοντας την εν λόγω αίτηση ο υποψήφιος εξουσιοδοτεί την Ελληνική Αστυνομία να αναζητήσει τα προαναφερόμενα στοιχεία από το Υ.ΠΑΙ.Θ.Α., την ταυτόχρονη συμμετοχή του ή μη στις Σχολές των Ενόπλων Δυνάμεων, του Πυροσβεστικού ή του Λιμενικού Σώματος, το ποινικό του μητρώο και την ύπαρξη τυχόν ποινικής εκκρεμότητας, την ενδεχόμενη θέση του σε δικαστική συμπαράσταση, την εγγραφή του σε έτερη σχολή Τριτοβάθμιας Εκπαίδευσης ή Δημόσια ΣΑΕΚ, την τυχόν χρήση ναρκωτικών ουσιών, καθώς και κάθε άλλη πληροφορία, που αφορά για παράδειγμα την οικογενειακή του κατάσταση, εάν ο υποψήφιος έχει δηλώσει ότι ανήκει σε κάποια ειδική κατηγορία.

⁴⁴ <https://www.kodiko.gr/nomothesia/document/413643>

⁴⁵ <https://www.astynomia.gr/elliniki-astynomia/anthropino-dynamiko/proslipseis-prosopikou/enimerosi-dilosi-sygkatathesis-gia-tin-epexergasia-prosopikon-dedomenon/>

Η αστυνομική Υπηρεσία, στην οποία υποβάλλεται η αίτηση, αφού συλλέξει όλα τα απαραίτητα δικαιολογητικά για τη συμμετοχή του υποψηφίου στον διαγωνισμό και την κατάταξή του στο Σώμα, ελέγχει την ακρίβεια, εγκυρότητα και πληρότητα αυτών. Στην συνέχεια, υποβάλει την αίτηση και τα δικαιολογητικά στην οικεία Διεύθυνση Αστυνομίας, η οποία με τη σειρά της ελέγχει τη γνησιότητα των δικαιολογητικών και καταχωρεί τις αιτήσεις σε ειδικό πληροφοριακό σύστημα της ΕΛ.ΑΣ..

Σε περίπτωση που ο υποψήφιος συμμετέχει στις προκαταρκτικές εξετάσεις των Σχολών των Ενόπλων Δυνάμεων, του Πυροσβεστικού ή Λιμενικού Σώματος και επιτύχει σε αυτές, αλλά έχει δηλώσει παράλληλα την επιθυμία του για κατάταξη στις Σχολές της Αστυνομίας, η Ελληνική Αστυνομία δύναται να εξετάσει τη γνησιότητα της βεβαίωσης ικανότητας, που θα προσκομίσει ο υποψήφιος μέσω του Γενικού Επιτελείου Εθνικής Άμυνας (Γ.Ε.ΕΘ.Α.), του Πυροσβεστικού ή Λιμενικού Σώματος, κατά περίπτωση. Αντίστοιχα, αν ο υποψήφιος επιτύχει στις προκαταρκτικές εξετάσεις της Ελληνικής Αστυνομίας, αλλά έχει δηλώσει επιθυμία συμμετοχής και στις Σχολές Ενόπλων Δυνάμεων, Πυροσβεστικού ή Λιμενικού Σώματος, η Ελληνική Αστυνομία επιβεβαιώνει μέσω εγγράφου της προς τις αρμόδιες Υπηρεσίες των ανωτέρω Σχολών, την ικανότητα του υποψηφίου.

Απώτερος σκοπός της συλλογής και διαχείρισης όλων των προαναφερόμενων δεδομένων είναι ο έλεγχος της εγκυρότητας και νομιμότητας της αίτησης συμμετοχής του υποψηφίου, η υπαγωγή του ή όχι σε ειδική κατηγορία υποψηφίων, η συμμετοχή του στις προκαταρκτικές εξετάσεις, η υποβολή των στοιχείων των επιτυχόντων στις προκαταρκτικές εξετάσεις υποψηφίων στο Υ.ΠΑΙ.Θ.Α., ώστε το τελευταίο να εκδώσει τα αποτελέσματα εισαγωγής σε Σχολές της Τριτοβάθμιας Εκπαίδευσης, η εν συνεχεία κατάταξη στο Σώμα της Ελληνικής Αστυνομίας των υποψηφίων που πληρούν τις απαραίτητες προϋποθέσεις και η εξασφάλιση της διαφάνειας και της νομιμότητας καθ' όλη τη διάρκεια της διαδικασίας πρόσληψης προσωπικού.

Αποδέκτες των δεδομένων του εκάστοτε υποψηφίου είναι η Ελληνική Αστυνομία, καθώς τα στοιχεία των επιτυχόντων αποτελούν μέρος του ατομικού τους φακέλου, που τηρεί η ΕΛ.ΑΣ, ενώ εκείνων που δεν θα προσληφθούν τηρούνται για 35 χρόνια, όπως ορίζει το άρθρο 3 του Π.Δ. 245/1997, πλην των αποτελεσμάτων των υγειονομικών εξετάσεων, που καταστρέφονται με την πάροδο ενός έτους ή σε περίπτωση δικαστικής διένεξης όταν εκδοθεί αμετάκλητη απόφαση. Επιπλέον, όπως ήδη προαναφέρθηκε, αποδέκτης είναι και το Υ.ΠΑΙ.Θ.Α., προκειμένου να ταυτοποιήσει ότι ο υποψήφιος που έχει κριθεί κατάλληλος για τις Σχολές της Ελληνικής Αστυνομίας ταυτίζεται με το άτομο που έχει δηλώσει στο μηχανογραφικό του δελτίο προτίμηση για την εισαγωγή του σε αυτές τις Σχολές, ώστε να εκδοθούν ορθά και αξιόπιστα αποτελέσματα εισαγωγής στην Τριτοβάθμια Εκπαίδευση. Δεδομένου ότι ο υποψήφιος, που έχει δηλώσει επιθυμία για εισαγωγή στις Σχολές της Αστυνομίας μπορεί να συμμετέχει στις προκαταρκτικές εξετάσεις των Σχολών των Ενόπλων Δυνάμεων, του Πυροσβεστικού ή Λιμενικού Σώματος, ή το αντίστροφο, αποδέκτες των δεδομένων του είναι το Γ.Ε.ΕΘ.Α, το Πυροσβεστικό ή Λιμενικό Σώμα, αναλόγως σε ποιας σχολής τις προκαταρκτικές εξετάσεις θα συμμετέχει και για ποιες σχολές έχει δηλώσει επιθυμία. Προκειμένου να διασφαλίζεται η διαφάνεια και νομιμότητα της διαδικασίας πρόσληψης προσωπικού, αλλά και να εξασφαλίζεται το δικαίωμα προσβολής των Αποφάσεων ή πινάκων ικανών και προσληφθέντων,

αποδέκτες είναι και οι υπόλοιποι συνυποψήφιοι, υπό τους περιορισμούς, που προβλέπουν οι διατάξεις του GDPR και του Ν. 4624/2019. Για παράδειγμα, μπορούν να δουν εάν ένας υποψήφιος κρίθηκε ικανός στις υγειονομικές εξετάσεις, αλλά δεν μπορούν να έχουν πρόσβαση στα ιατρικά του έγγραφα. Τέλος, αποδέκτες είναι και δημόσιοι φορείς ή και δικαστικοί λειτουργοί. Σε κάθε περίπτωση, πρόσβαση στα δεδομένα έχουν μόνο εξουσιοδοτημένα πρόσωπα από κάθε υπηρεσία, φορέα ή οργανισμό.

Ο υποψήφιος των Σχολών της Ελληνικής Αστυνομίας δικαιούται να γνωρίζει ποια δεδομένα του πρόκειται να τεθούν σε επεξεργασία και έχει τη δυνατότητα να ασκήσει τα δικαιώματα της αντίρρησης και εναντίωσης στην επεξεργασία, αποκλειστικά και μόνο για να διορθώσει ή συμπληρώσει τυχόν εσφαλμένα ή ελλιπή στοιχεία, ώστε να είναι ακριβή και επικαιροποιημένα. Αν, όμως, φέρει αντίρρηση με την όλη διαδικασία της επεξεργασίας των δεδομένων του, στο πλαίσιο δήλωσης συμμετοχής του στον διαγωνισμό, η αίτησή του απορρίπτεται απευθείας και δεν λαμβάνεται υπόψη. Αξίζει να σημειωθεί ότι εάν ο υποψήφιος δεν παράσχει ενυπόγραφα την συγκατάθεσή του στην επεξεργασία των δεδομένων του, η αίτηση συμμετοχής του στον διαγωνισμό είναι άκυρη.

Σε περίπτωση που ο υποψήφιος ζητήσει τη διαγραφή δεδομένων του, η εκάστοτε αστυνομική υπηρεσία δύναται να αρνηθεί να ικανοποιήσει το αίτημά του, εάν τα συγκεκριμένα δεδομένα πρέπει να διατηρηθούν προκειμένου να ασκήσει νόμιμες αξιώσεις της ή να εκτελέσει τα καθήκοντά της, όπως αυτά ορίζονται από την κείμενη νομοθεσία. Για παράδειγμα, ένας υποψήφιος μπορεί να ζητήσει να διαγραφούν τα αποτελέσματα των υγειονομικών ή ψυχομετρικών του εξετάσεων. Η Ελληνική Αστυνομία, όμως, δεν μπορεί να προβεί σε αυτή την ενέργεια, καθώς αφενός πρέπει να τα διατηρήσει για συγκεκριμένο χρονικό διάστημα, αφετέρου μπορεί να χρειαστούν σε περίπτωση ένστασης, προσφυγής ή δικαστικής διένεξης αναφορικά με την καταλληλότητα του υποψηφίου.

Η υποβολή αιτήσεως και δήλωση συγκατάθεσης του υποψηφίου γίνεται με την αυτοπρόσωπη παρουσία αυτού στην αρμόδια αστυνομική Υπηρεσία του τόπου κατοικίας του. Από το έτος 2026 οι ενδιαφερόμενοι θα υποβάλλουν ηλεκτρονικά τις αιτήσεις τους μέσω της Ενιαίας Ψηφιακής Πύλης της Δημόσιας Διοίκησης (ΕΨΠ – gov.gr). Για να μπορέσουν να καταθέσουν την αίτησή τους, θα πρέπει να διαθέτουν Α.Φ.Μ., κωδικούς taxisnet, να έχουν επιβεβαιώσει τα στοιχεία επικοινωνίας τους στο Εθνικό Μητρώο Επικοινωνίας και να έχουν λάβει από το Υ.ΠΑΙ.Θ.Α. κωδικό υποψηφίου για τις πανελλαδικές εξετάσεις.

Η νέα αυτή ψηφιακή διαδικασία είναι το αποτέλεσμα μακράς και αποτελεσματικής συνεργασίας του Υπουργείου Ψηφιακής Διακυβέρνησης και των Διευθύνσεων Ένστολου Προσωπικού και Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Αρχηγείου της Ελληνικής Αστυνομίας. Η εφαρμογή της αποδεικνύει την δέσμευση της Ελληνικής Αστυνομίας να αξιοποιεί τις σύγχρονες τεχνολογίες Πληροφορικής και Επικοινωνιών, με σκοπό τη μείωση της

γραφειοκρατίας, την επιτάχυνση και απλοποίηση της υφιστάμενης διαδικασίας και τη μείωση του χρόνου διεκπεραίωσης αυτής⁴⁶.

6.7.1. Συμπεράσματα

Η ΕΛ.ΑΣ. στο πλαίσιο πρόσληψης ιδιωτών στις Σχολές Αξιωματικών και Αστυφυλάκων της Ελληνικής Αστυνομίας συλλέγει και επεξεργάζεται τα απολύτως απαραίτητα προσωπικά δεδομένα, ευαίσθητα και μη, καθώς και εκείνα που αφορούν ποινικές καταδίκες και γενικότερα ποινικές εκκρεμότητες του υποψηφίου, κατ' εφαρμογή της αρχής της ελαχιστοποίησης των δεδομένων.

Δεδομένου ότι είναι αρμόδια για τις αιτήσεις των υποψηφίων και τους ενημερώνει για την όλη διαδικασία και τα δεδομένα που απαιτούνται, τόσο μέσω της επίσημης ιστοσελίδας της και της προκήρυξης που εκδίδει, όσο και κατά την υποβολή της αίτησης, με ειδικό έντυπο που υπογράφει ο ενδιαφερόμενος, γίνεται σαφές ότι οι ενέργειες της Ελληνικής Αστυνομίας είναι σύμφωνες με την αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας.

Τα δεδομένα, που συλλέγει και διαχειρίζεται, χρησιμοποιούνται αποκλειστικά για την συμμετοχή του υποψηφίου στις εξετάσεις των σχολών της Ελληνικής Αστυνομίας και διατηρούνται για συγκεκριμένο χρονικό διάστημα, κατ' εφαρμογή των αρχών του σκοπού και της περιόδου αποθήκευσης.

Ο υποψήφιος υποβάλει αυτοπροσώπως στην κατά τόπο αρμόδια αστυνομική Υπηρεσία την αίτηση και τα δικαιολογητικά, τα οποία παραλαμβάνει αρμόδιος Αξιωματικός. Προκειμένου να είναι έγκυρη η αίτηση του υποψηφίου, τα δεδομένα που συλλέγονται πρέπει να είναι ακριβή και επικαιροποιημένα. Για το λόγο αυτό, ελέγχεται η ακρίβεια και εγκυρότητα από τον παραλαμβάνοντα αστυνομικό και στην συνέχεια υποβάλλονται στην αρμόδια Διεύθυνση Αστυνομίας, η οποία με τη σειρά της ελέγχει την γνησιότητα αυτών, εξασφαλίζοντας την ακεραιότητα και εμπιστευτικότητα των δεδομένων.

Επομένως, λαμβάνοντας υπόψη όλα όσα παρατέθηκαν αναφορικά με την συλλογή και επεξεργασία προσωπικών δεδομένων των υποψηφίων, γίνεται σαφές ότι τηρείται και η αρχή της λογοδοσίας και η διαδικασία στο σύνολό της είναι σύμφωνη με τις βασικές αρχές επεξεργασίας, διασφαλίζοντας την προστασία των δεδομένων.

6.8. Διασυνοριακή ανταλλαγή προσωπικών δεδομένων

Η συλλογή και επεξεργασία προσωπικών δεδομένων, που διεξάγει η Ελληνική Αστυνομία, δεν περιορίζονται μόνο σε εθνικό επίπεδο, αλλά επεκτείνονται και σε διασυνοριακό. Το ισχύον ενωσιακό δίκαιο που ρυθμίζει την αυτοματοποιημένη αναζήτηση και ανταλλαγή δεδομένων για την αστυνομική συνεργασία των κρατών μελών σε ποινικές υποθέσεις, διέπεται, αφενός μεν από τις Αποφάσεις 2008/615/ΔΕΥ⁴⁷ και 2008/616/ΔΕΥ⁴⁸ (πλαίσιο Prüm), αφετέρου δε από τον Κανονισμό 2024/982 (ΕΕ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (πλαίσιο Prüm II). Πιο συγκεκριμένα, η Απόφαση 2008/615/ΔΕΥ θεσπίζει το νομικό πλαίσιο της

⁴⁶ <https://www.astynomia.gr/file/2025/10/24102025anakoinosipaneladikes.pdf>

⁴⁷ <https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32008D0615>

⁴⁸ <https://eur-lex.europa.eu/eli/dec/2008/616/oj/?locale=el>

διασυνοριακής συνεργασίας των κρατών μελών σχετικά με την ανταλλαγή πληροφοριών που αφορούν προφίλ DNA, δακτυλικά αποτυπώματα και στοιχεία κυκλοφορίας οχημάτων, μεταξύ των αρμόδιων αρχών της Ε.Ε., στο πλαίσιο πρόληψης και διερεύνησης αξιόποινων πράξεων (Άρθρο 1 της Απόφασης 2008/615/ΔΕΥ) και η Απόφαση 2008/616/ΔΕΥ⁴⁹ καθορίζει τις τεχνικές και διοικητικές διατάξεις εφαρμογής της πρώτης. Από την άλλη μεριά, ο Κανονισμός 2024/982 έρχεται να τροποποιήσει – συμπληρώσει τις προαναφερόμενες Αποφάσεις προκειμένου να ενισχύσει έτσι περισσότερο τη διασυνοριακή συνεργασία, με απόλυτο σεβασμό στα θεμελιώδη δικαιώματα των φυσικών προσώπων και δη αυτών στην ιδιωτική ζωή και στην προστασία των προσωπικών δεδομένων (Άρθρο 2 του Κανονισμού 2024/982).

Ωστόσο, κατά ρητή επιταγή του άρθρου 25 παρ. 2 της Απόφασης 2008/615/ΔΕΥ, δεδομένου ότι οι προαναφερόμενες πληροφορίες αποτελούν προσωπικά δεδομένα και μάλιστα τόσο απλά, όπως τα στοιχεία κυκλοφορίας οχημάτων, όσο και ευαίσθητα, όπως τα προφίλ DNA και τα δακτυλικά αποτυπώματα, προκειμένου να καταστεί δυνατή η διασυνοριακή ανταλλαγή τους, τα κράτη μέλη οφείλουν να ενσωματώσουν στο εθνικό τους δίκαιο το Κεφάλαιο 6 της Απόφασης (2008/615/ΔΕΥ), το οποίο ρυθμίζει την προστασία των δεδομένων. Σε εθνικό επίπεδο, το Κεφάλαιο 6 της Απόφασης, ενσωματώθηκε στο Π.Δ. 81/2021⁵⁰.

6.8.1. Εθνικά σημεία επαφής – Υπεύθυνοι επεξεργασίας δεδομένων

Η ανταλλαγή δεδομένων σε διασυνοριακό επίπεδο πραγματοποιείται μέσω των εθνικών σημείων επαφής των κρατών μελών. Στη χώρα μας, τα εθνικά σημεία επαφής ορίζονται στο άρθρο 4 του Π.Δ. 81/2021 και είναι τα ακόλουθα:

- η Δ.Ε.Ε., για την αυτοματοποιημένη αναζήτηση και σύγκριση προφίλ DNA και την αυτοματοποιημένη αναζήτηση δεδομένων που αφορούν δακτυλικά αποτυπώματα,
- η Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας (Δ.Δ.Α.Σ.) του Αρχηγείου της Ελληνικής Αστυνομίας⁵¹, για την παροχή δεδομένων προσωπικού ή μη χαρακτήρα για σημαντικά γεγονότα με διασυνοριακή διάσταση και την παροχή πληροφοριών για την πρόληψη τρομοκρατικών πράξεων,
- η Υπηρεσία Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων⁵² του Υπουργείου Υποδομών και Μεταφορών, για ανακτήσεις των άλλων κρατών μελών της Ε.Ε. από το Εθνικό Μητρώο αδειών κυκλοφορίας μηχανοκίνητων οχημάτων.

⁴⁹ <https://eur-lex.europa.eu/eli/dec/2008/616/oj/?locale=el>

⁵⁰ <https://www.kodiko.gr/nomothesia/document/755180/p.d.-81-2021>

⁵¹ Η Δ.Δ.Α.Σ. είναι αρμόδια για τη διεθνή αστυνομική συνεργασία και ανταλλαγή πληροφοριών με έτερες Υπηρεσίες και Οργανισμούς σε διεθνές και ευρωπαϊκό επίπεδο, διασφαλίζοντας την ασφάλεια των ανταλλασσόμενων δεδομένων και τη νομιμότητα των διαδικασιών (Άρθρο 24 του Ν. 5187/2025).

⁵² Η Υπηρεσία Υποστήριξης Πληροφορικής και Ηλεκτρονικών Συστημάτων ασχολείται με την ανάπτυξη, διαχείριση, ασφάλεια και τεχνική υποστήριξη των πληροφοριακών συστημάτων και δικτύων του Υπουργείου Υποδομών και Μεταφορών, διασφαλίζοντας τη συνεχή και ασφαλή και λειτουργία τους σύμφωνα με τα εθνικά και ευρωπαϊκά πρότυπα (https://www.ggde.gr/index.php?option=com_k2&view=item&id=4925:ypiresia-ypostiriks-pli-roforikis-kai-ilektronikon-systimaton&Itemid=348).

Σε εθνικό επίπεδο, τα προσωπικά δεδομένα που ανταλλάσσονται στο πλαίσιο διασυνοριακής συνεργασίας μεταξύ των κρατών μελών, υποβάλλονται σε επεξεργασία μόνο από τις δημόσιες αρχές και φορείς, που είναι αρμόδιες ή συμμετέχουν με οποιονδήποτε τρόπο στην διασυνοριακή ανταλλαγή δεδομένων, όπως αυτή ρυθμίζεται από το Π.Δ. 81/2021. Έτσι, ως υπεύθυνοι επεξεργασίας νοούνται κατά κύριο λόγο η ΕΛ.ΑΣ., οι δικαστικές και εισαγγελικές αρχές και το Υπουργείο Υποδομών και Μεταφορών (Άρθρο 5 του Π.Δ. 81/2021). Εκτός από αυτούς, δύναται να προβούν σε επεξεργασία των δεδομένων και άλλες αρμόδιες αρχές και φορείς, όπως η Α.Π.Δ.Π.Χ., η Ανεξάρτητη Αρχή Δημοσίων Εσόδων, το Λιμενικό Σώμα, η Λιμενική Ακτοφυλακή και τα τελωνεία, στο πλαίσιο των αρμοδιοτήτων τους (Άρθρο 7 του Π.Δ. 81/2021).

6.8.2. Επεξεργασία των δεδομένων

Η Ελληνική Αστυνομία και οι αρμόδιες αρχές των άλλων κρατών μελών της Ε.Ε. ανταλλάσσουν μεταξύ τους προσωπικά δεδομένα, σύμφωνα με τα οριζόμενα στα προαναφερόμενα νομικά κείμενα.

6.8.2.1. Προφίλ DNA

Στο πλαίσιο διερεύνησης αξιόποινων πράξεων, τα κράτη μέλη επιτρέπουν στα εθνικά σημεία επαφής των έτερων κρατών μελών και στην Europol να αποκτούν πρόσβαση στα δεδομένα αναφοράς DNA των εθνικών τους αρχείων DNA και να προβαίνουν σε αυτοματοποιημένες αναζητήσεις μέσω σύγκρισης των προφίλ DNA που είναι αποθηκευμένα στις δικές τους βάσεις δεδομένων DNA με εκείνα που είναι αποθηκευμένα στις βάσεις δεδομένων DNA των άλλων κρατών μελών και της Europol. Τα δεδομένα αναφοράς αφορούν το προφίλ DNA⁵³ και τον αριθμό αναφοράς, συνεπώς δεν περιέχουν περαιτέρω δεδομένα που να καθιστούν εφικτή την άμεση αναγνώριση του υποκειμένου. Επιπλέον, τυχόν αταυτοποίητα προφίλ DNA πρέπει να φέρουν σχετική σήμανση (Άρθρο 5 και 6 του Κανονισμού 2024/982).

Η αυτοματοποιημένη αναζήτηση πραγματοποιείται κατόπιν υποβολής αιτήματος, μέσω του εθνικού σημείου επαφής του αιτούντος κράτους μέλους, που περιλαμβάνει τον κωδικό αυτού, την ημερομηνία, την ώρα και τον αύξοντα αριθμό του αιτήματος, τα δεδομένα αναφοράς DNA, καθώς και εάν πρόκειται για ταυτοποιημένο ή αταυτοποίητο προφίλ DNA (Άρθρο 9 του Κανονισμού 2024/982).

Αφού πραγματοποιηθεί η αυτοματοποιημένη αναζήτηση και σύγκριση, το αιτούν κράτος μέλος λαμβάνει αυτοματοποιημένη απάντηση - έκθεση αντιστοιχίας, η οποία περιλαμβάνει το αποτέλεσμα της αναζήτησης, δηλαδή εάν διαπιστώθηκαν αντιστοιχίες ή όχι μεταξύ των συγκρινόμενων προφίλ DNA, την ημερομηνία, την ώρα και τον αύξοντα αριθμό του αιτήματος, αλλά και της απάντησης - έκθεσης αντιστοιχίας, τους αριθμούς αναφοράς προφίλ DNA καθώς και τους κωδικούς του αιτούντος και του αιτούμενου κράτους μέλους, εάν πρόκειται για ταυτοποιημένα ή αταυτοποίητα προφίλ DNA, καθώς και αυτά (προφίλ DNA), για τα οποία προκύπτει αντιστοιχία (Άρθρο 9 του Κανονισμού 2024/982). Επιπλέον, για την εξασφάλιση της εμπιστευτικότητας και της ακεραιότητας των διαβιβαζόμενων δεδομένων, τα κράτη μέλη και η Europol,

⁵³ Το προφίλ DNA συνιστά έναν κωδικό που αποτελείται από αριθμούς και γράμματα (Άρθρο 4 του Κανονισμού 2024/982)

λαμβάνουν κατάλληλα μέτρα, μεταξύ των οποίων περιλαμβάνονται κρυπτογραφικές τεχνικές (Άρθρο 8 του Κανονισμού 2024/982).

Είναι δέον να σημειωθεί ότι η Eurpol, η αποστολή και τα καθήκοντα της οποίας διέπονται από τις διατάξεις του Κανονισμού (ΕΕ) 2016/794, αποτελεί υποστηρικτικό οργανισμό, που λειτουργεί ως κόμβος συντονισμού, συνεργασίας και πληροφόρησης μεταξύ των αρμόδιων αρχών των κρατών μελών της Ε.Ε. για την πρόληψη και καταπολέμηση σοβαρών εγκλημάτων (Άρθρο 3 του Κανονισμού 2016/794). Στο πλαίσιο αυτό, τα κράτη μέλη έχουν μόνο έμμεση πρόσβαση στη βάση δεδομένων της Eurpol, βάσει συστήματος αντιστοιχίας ή αναντιστοιχίας, ενώ η οποιαδήποτε περαιτέρω πληροφορία, σε περίπτωση αντιστοιχίας, καθορίζεται σύμφωνα με απόφαση του παρόχου των πληροφοριών και κατόπιν διμερών συμφωνιών μεταξύ των εμπλεκόμενων κρατών μελών και της Eurpol (Άρθρο 6 του Κανονισμού 2024/982 και Άρθρο 20 του Κανονισμού 2016/794).

Αν κατά τη διαδικασία που περιγράφηκε παραπάνω προκύψει αντιστοιχία μεταξύ των συγκρινόμενων προφίλ DNA, τα εθνικά σημεία επαφής αιτούντος και αιτούμενου κράτους μέλους, μπορούν να επιβεβαιώσουν την αντιστοιχία μεταξύ των συγκρινόμενων προφίλ DNA και να διασφαλίσουν τη διενέργεια μη αυτοματοποιημένης επανεξέτασης από έναν τουλάχιστον εξειδικευμένο υπάλληλο του προσωπικού τους, ο οποίος θα επιβεβαιώσει αυτή την αντιστοιχία (Άρθρο 6 του Κανονισμού 2024/982).

Η επεξεργασία δεδομένων κατά την αυτοματοποιημένη αναζήτηση ή σύγκριση προφίλ DNA στο πλαίσιο της διασυνοριακής συνεργασίας της ΕΛ.ΑΣ. και των αρμόδιων αρχών άλλων κρατών μελών επιτρέπεται μόνο για ορισμένους σκοπούς και συγκεκριμένα: (α) για να διαπιστωθεί εάν ταυτίζονται τα συγκρινόμενα δεδομένα, (β) για να προετοιμαστεί και να υποβληθεί αίτημα αστυνομικής ή δικαστικής συνδρομής, σε περίπτωση που υπάρχει αντιστοιχία μεταξύ των συγκρινόμενων δεδομένων και (γ) για να πραγματοποιηθεί καταγραφή αρχείων (Άρθρο 6 παρ. 2 του Π.Δ. 81/2021 και Άρθρο 50 του Κανονισμού 2024/982). Σε εθνικό επίπεδο, η αυτοματοποιημένη αναζήτηση και σύγκριση πραγματοποιείται μέσω της Δ.Ε.Ε., ενώ η παροχή περαιτέρω δεδομένων πραγματοποιείται μέσω της Δ.Δ.Α.Σ., υπό τον σεβασμό και τις προϋποθέσεις που προβλέπονται στο άρθρο 47 του Κανονισμού 2024/982.

6.8.2.2. Δακτυλικά αποτυπώματα

Τα κράτη μέλη επιτρέπουν στα εθνικά σημεία επαφής των άλλων κρατών μελών και στην Eurpol να αποκτούν πρόσβαση και στα δακτυλοσκοπικά δεδομένα αναφοράς που διατηρούνται στις εθνικές τους βάσεις δεδομένων, που έχουν δημιουργηθεί στο πλαίσιο πρόληψης, διερεύνησης και εξιχνίασης ποινικών αδικημάτων και να πραγματοποιούν αυτοματοποιημένες αναζητήσεις συγκρίνοντας τα δακτυλοσκοπικά δεδομένα αναφοράς (Άρθρα 10 και 11 του Κανονισμού 2024/982).

Τα δακτυλοσκοπικά δεδομένα αναφοράς περιλαμβάνουν τα δακτυλοσκοπικά δεδομένα και τον αριθμό αναφοράς τους και δεν περιέχουν στοιχεία, με τα οποία μπορεί να ταυτοποιηθεί το υποκείμενο των δεδομένων. Τα δακτυλοσκοπικά δεδομένα περιέχουν εικόνες λανθανόντων και μη δακτυλικών αποτυπωμάτων, εικόνες λανθανόντων και μη αποτυπωμάτων παλάμης, πίνακες με κωδικοποιημένες πληροφορίες αυτών και δεν περιέχουν στοιχεία, από τα οποία μπορεί να ταυτοποιηθεί

το υποκείμενο των δεδομένων. Όσα δακτυλοσκοπικά δεδομένα είναι αταυτοποίητα πρέπει να φέρουν σχετική σήμανση (Άρθρο 4 και 10 του Κανονισμού 2024/982).

Η αυτοματοποιημένη αναζήτηση πραγματοποιείται μέσω του εθνικού σημείου επαφής του αιτούντος κράτους μέλους κατόπιν υποβολής σχετικού αιτήματος, στο οποίο αναφέρονται ο κωδικός του αιτούντος κράτους μέλους, η ημερομηνία, η ώρα και ο αριθμός του αιτήματος, καθώς και τα δακτυλοσκοπικά δεδομένα αναφοράς, που πρόκειται να υποβληθούν σε σύγκριση (Άρθρο 15 παρ. 1 του Κανονισμού 2024/982).

Μόλις ολοκληρωθεί η αυτοματοποιημένη σύγκριση, το αιτούν κράτος μέλος λαμβάνει σχετική απάντηση, στην οποία αναφέρονται το αποτέλεσμα αυτής, δηλαδή εάν υπήρξε αντιστοιχία ή όχι μεταξύ των συγκρινόμενων δακτυλοσκοπικών δεδομένων, η ημερομηνία, η ώρα και ο αριθμός του αιτήματος και της απάντησης, οι αριθμοί αναφοράς των δακτυλοσκοπικών δεδομένων αλλά και οι κωδικοί του αιτούντος και του αιτούμενου κράτους μέλους, καθώς και τα δακτυλοσκοπικά δεδομένα, για τα οποία προέκυψε η αντιστοιχία (Άρθρο 15 παρ. 1 του Κανονισμού 2024/982). Για την εξασφάλιση της εμπιστευτικότητας και της ακεραιότητας των διαβιβαζόμενων δεδομένων, τα κράτη μέλη και η Europol, λαμβάνουν κατάλληλα μέτρα, μεταξύ των οποίων περιλαμβάνονται κρυπτογραφικές τεχνικές (Άρθρο 13 παρ. 1 και 2 του Κανονισμού 2024/982).

Ομοίως, εάν προκύψει αντιστοιχία μεταξύ των συγκρινόμενων δακτυλοσκοπικών δεδομένων, το αιτούν κράτος μέλος έχει τη δυνατότητα να την επιβεβαιώσει, ενημερώνοντας παράλληλα το αιτούμενο κράτος μέλος, ώστε να διασφαλίσει τη διενέργεια μη αυτοματοποιημένης επανεξέτασης από έναν τουλάχιστον εξειδικευμένο υπάλληλο του προσωπικού του τελευταίου, ο οποίος θα επιβεβαιώσει αυτή την αντιστοιχία (Άρθρο 11 παρ.2 του Κανονισμού 2024/982).

Και σε αυτή την περίπτωση η επεξεργασία δεδομένων επιτρέπεται μόνο (α) για να διαπιστωθεί εάν ταυτίζονται τα συγκρινόμενα δεδομένα, (β) για να προετοιμαστεί και να υποβληθεί αίτημα αστυνομικής ή δικαστικής συνδρομής, σε περίπτωση που υπάρχει αντιστοιχία μεταξύ των συγκρινόμενων δεδομένων και (γ) για να πραγματοποιηθεί καταγραφή βάσει του άρθρου 9 του Π.Δ. 81/2021 (Άρθρο 6 παρ. 2 του Π.Δ. 81/2021). Σε εθνικό επίπεδο, η αυτοματοποιημένη αναζήτηση και σύγκριση πραγματοποιείται μέσω της Δ.Ε.Ε., ενώ για την παροχή περαιτέρω δεδομένων υποβάλλεται αίτημα αστυνομικής συνδρομής μέσω Δ.Δ.Α.Σ. ή αίτημα δικαστικής συνδρομής, υπό τον σεβασμό και τις προϋποθέσεις που προβλέπονται στο άρθρο 47 του Κανονισμού 2024/982.

6.8.2.3. Άδειες κυκλοφορίας οχημάτων

Τα κράτη μέλη παρέχουν στα αρμόδια εθνικά σημεία επαφής των άλλων κρατών μελών τη δυνατότητα να πραγματοποιούν αυτοματοποιημένες αναζητήσεις και να αποκτούν πρόσβαση σε εθνικά τους δεδομένα, που αφορούν οχήματα και τους ιδιοκτήτες – κατόχους αυτών. Στην τελευταία περίπτωση κατά την αναζήτηση χρησιμοποιούνται το ονοματεπώνυμο και η ημερομηνία γέννησης του ιδιοκτήτη, ενώ εάν είναι νομικό πρόσωπο η επωνυμία αυτού (Άρθρο 16 του Κανονισμού 2024/982).

Οι αυτοματοποιημένες αναζητήσεις, πραγματοποιούνται μέσω της εφαρμογής «Ευρωπαϊκό σύστημα πληροφοριών για οχήματα και άδειες οδήγησης» - Eucaris

(Άρθρο 17 του Κανονισμού 2024/982) και διεξάγονται με την καταχώρηση: είτε (α) του πλήρους αριθμού του επίμαχου οχήματος, είτε (β) της άδειας κυκλοφορίας αυτού ή (γ) εφόσον προβλέπεται από το εθνικό δίκαιο του αιτούμενου κράτους μέλους, των στοιχείων σχετικά με τον ιδιοκτήτη – κάτοχο του οχήματος (Άρθρο 16 του Κανονισμού 2024/982). Προς διασφάλιση της προστασίας των ανταλλασσόμενων δεδομένων μέσω της εφαρμογής «Eucaris» χρησιμοποιούνται κρυπτογραφικές μέθοδοι (Άρθρο 17 του Κανονισμού 2024/982).

Οι προαναφερόμενες αναζητήσεις διενεργούνται σύμφωνα με το εθνικό δίκαιο του αιτούντος κράτους μέλους (Άρθρο 16 του Κανονισμού 2024/982). Στην περίπτωση της χώρας μας, η διαδικασία αυτή ρυθμίζεται από το Π.Δ. 81/2021, σύμφωνα με το οποίο κατά τη διασυνοριακή συνεργασία της ΕΛ.ΑΣ. με αρμόδιες αρχές άλλων κρατών μελών, τα παρεχόμενα δεδομένα μπορούν να χρησιμοποιηθούν μόνο για την αυτόματη απάντηση στα αιτήματα αναζήτησης που υποβάλλονται και για να καταγραφεί ότι έγινε αναζήτηση σχετικά με αυτά, ώστε να ελέγχεται ο νόμιμος χαρακτήρας της. Έτσι, η αρμόδια εθνική αρχή, π.χ. η ΕΛ.ΑΣ., δεν μπορεί να χρησιμοποιήσει τα δεδομένα της απάντησης για υπόθεση διαφορετική από εκείνη για την οποία πραγματοποιήθηκε η αναζήτηση (Άρθρο 6 παρ. 4 του Π.Δ. 81/2021).

Τόσο τα κράτη μέλη, όσο και η Europol, τηρούν αρχεία καταγραφής (log files) για τις αναζητήσεις που πραγματοποιούνται σχετικά με δεδομένα αδειών κυκλοφορίας οχημάτων. Τα κράτη μέλη καταγράφουν τόσο τις αναζητήσεις που πραγματοποιούν οι δικές τους αρμόδιες αρχές, όσο και τις αναζητήσεις που αιτούνται τα έτερα κράτη μέλη, ενώ η Europol καταγράφει τις αναζητήσεις που πραγματοποιεί το εξουσιοδοτημένο προσωπικό της. Τα αρχεία καταγραφής περιλαμβάνουν το ποιος έκανε την αναζήτηση (κράτος μέλος ή Europol), την ημερομηνία και ώρα του αιτήματος και της απάντησης, καθώς και τις εθνικές βάσεις δεδομένων στις οποίες υποβλήθηκε αίτημα αναζήτησης και εκείνες που έδωσαν θετικές απαντήσεις (Άρθρο 18 του Κανονισμού 2024/982). Αντίστοιχη υποχρέωση τήρησης αρχείων από τα κράτη μέλη και τη Europol ισχύει και στην περίπτωση των αυτοματοποιημένων αναζητήσεων προφίλ DNA και δακτυλοσκοπικών δεδομένων (Άρθρο 40 του Κανονισμού 2024/982).

Τα αρχεία καταγραφής χρησιμοποιούνται για το παραδεκτό της αναζήτησης και τον έλεγχο της προστασίας των προσωπικών δεδομένων, αλλά και για στατιστικούς σκοπούς. Επιπλέον, λαμβάνονται κατάλληλα μέτρα ώστε αυτά να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ενώ διαγράφονται με το πέρασ 3 ετών από τη δημιουργία τους, εκτός εάν απαιτούνται για εν εξελίξει διαδικασίες ελέγχου (π.χ. από εποπτικές Αρχές προκειμένου να αποδειχθεί η νομιμότητα και το παραδεκτό της επεξεργασίας των δεδομένων). Στην τελευταία περίπτωση, διαγράφονται όταν δεν είναι πλέον απαραίτητα για αυτές τις διαδικασίες. Στα αρχεία καταγραφής έχουν πρόσβαση οι υπεύθυνοι επεξεργασίας των δεδομένων για σκοπούς αυτοελέγχου, αλλά και για την παρακολούθηση της νομιμότητας της επεξεργασίας των δεδομένων (Άρθρα 18 και 40 του Κανονισμού 2024/982).

6.8.3. Σκοπός της επεξεργασίας

Τα προσωπικά δεδομένα που παρέχονται σε κράτη μέλη ή την Europol, μπορούν να υποβληθούν σε επεξεργασία μόνο για τους σκοπούς για τους οποίους παρασχέθηκαν από το αιτούμενο κράτος μέλος στο πλαίσιο διασυνοριακής συνεργασίας για θέματα,

που αφορούν την δικαστική και αστυνομική συνεργασία σε ποινικές υποθέσεις, ενώ επεξεργασία για διαφορετικούς σκοπούς επιτρέπεται μόνο κατόπιν άδειας του αιτούμενου κράτους μέλους και εφόσον αυτό προβλέπεται από το εθνικό του δίκαιο (Άρθρο 2 και 50 του Κανονισμού 2024/982). Σε περίπτωση, που η Ελλάδα είναι το αιτούμενο κράτος μέλος, τότε η άδεια παρέχεται από την αρμόδια αρχή, που καθίσταται υπεύθυνος επεξεργασίας, διαμέσου του εθνικού σημείου επαφής, υπό την προϋπόθεση ότι η επεξεργασία των δεδομένων προβλέπεται από τον Ν. 4624/2019 (Άρθρο 6 παρ. 1 του Π.Δ. 81/2021).

6.8.4. Ακρίβεια των δεδομένων

Οι υπεύθυνοι επεξεργασίας των δεδομένων, όπως αυτοί ορίστηκαν στην Ενότητα 6.8.1, μεριμνούν για την ακρίβεια και επικαιροποίηση των δεδομένων, που παρέχουν σε άλλα κράτη μέλη. Υπό αυτό το πρίσμα, όταν διαπιστωθεί αυτοδικαίως ή από αναφορά του υποκειμένου των δεδομένων ή κατόπιν δικαστικής απόφασης, ότι τα δεδομένα που παρασχέθηκαν είναι εσφαλμένα ή μη επικαιροποιημένα ή ότι δεν έπρεπε να έχουν αποσταλεί, τότε ενημερώνεται το αιτούν κράτος μέλος μέσω του εθνικού σημείου επαφής. Στην περίπτωση, που το αιτούν κράτος μέλος είναι η χώρα μας, η αρμόδια αρχή που χειρίζεται τον φάκελο των δεδομένων, υποχρεούται να διαγράψει ή να διορθώσει τα δεδομένα και να ενημερώσει παράλληλα τις δημόσιες αρχές και φορείς, του άρθρου 7 του Π.Δ. 81/2021, προκειμένου να προβούν στις δικές τους ενέργειες διόρθωσης ή διαγραφής, αντίστοιχα (Άρθρο 8 παρ. 1 του Π.Δ. 81/2021).

Σε περίπτωση που το υποκείμενο των δεδομένων αμφισβητεί την ακρίβεια των δεδομένων, που το αφορούν, χωρίς όμως να μπορεί να αποδειχθεί με βεβαιότητα η ακρίβεια ή ανακρίβεια αυτών, τα δεδομένα δεν διαγράφονται ούτε διορθώνονται, αλλά, επισημαίνονται, κατόπιν αίτησής του, με σχετική επισήμανση, η οποία δύναται να αφαιρεθεί μόνο εάν προκύψουν νεότερα στοιχεία, που μπορούν να θεμελιώσουν την ακρίβεια αυτών και πάντως κατόπιν άδειας του υποκειμένου ή απόφασης του αρμόδιου δικαστηρίου, της Α.Π.Δ.Π.Χ. ή του Ευρωπαϊού Επόπτη Προστασίας Δεδομένων⁵⁴ (Άρθρο 8 παρ. 2 του Π.Δ. 81/2021 και Άρθρο 51 του Κανονισμού 2024/982).

6.8.5. Χρόνος διατήρησης των δεδομένων

Τα δεδομένα, που παρέχονται στο αιτούν κράτος μέλος ή στην Europol διαγράφονται αμέσως μετά τις αυτόματες απαντήσεις σε αναζητήσεις, εκτός εάν συντρέχει λόγος διατήρησής τους για περαιτέρω επεξεργασία (Άρθρο 6 παρ. 3, 4 του Π.Δ. 81/2021 και άρθρο 50 του Κανονισμού 2024/982).

Τα προσωπικά δεδομένα, που έχουν ανταλλαχθεί νομίμως στο πλαίσιο της διασυνοριακής συνεργασίας της Ελληνικής Αστυνομίας με τις αρμόδιες αρχές άλλων κρατών μελών ή την Europol, διαγράφονται όταν δεν χρειάζονται πλέον για τον σκοπό, για τον οποίο παρασχέθηκαν, καθώς και όταν παρέλθει το μέγιστο χρονικό διάστημα διατήρησης, που προβλέπεται από το εθνικό δίκαιο, υπό την προϋπόθεση ότι η αιτούμενη αρχή ενημερώσει την αιτούσα για αυτό το διάστημα, αλλά και από τον

⁵⁴ Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων ελέγχει και διασφαλίζει ότι τα όργανα και οι οργανισμοί της Ε.Ε. επεξεργάζονται τα προσωπικά δεδομένα νόμιμα και με ασφάλεια. Πέραν των ελέγχων, εκδίδει συστάσεις και εκθέσεις, συνεργάζεται με εποπτικές αρχές και παρακολουθεί την εφαρμογή κάθε ενωσιακής πράξης που αφορά την προστασία των δικαιωμάτων των φυσικών προσώπων, κατά την επεξεργασία των προσωπικών τους δεδομένων (Άρθρο 52 του Κανονισμού 2018/1725).

Κανονισμό (ΕΕ) 2016/794. Επιπλέον, διαγράφονται και εκείνα που δεν έπρεπε να έχουν παραχθεί ή ληφθεί (Άρθρο 8 παρ. 3,4 του Π.Δ. 81/2021 και άρθρο 51 του Κανονισμού 2024/982). Σε κάθε περίπτωση, ωστόσο, η διαγραφή των δεδομένων απαιτεί σχετική τεκμηρίωση, η οποία δύναται να χρησιμοποιηθεί αποκλειστικά στο πλαίσιο ελέγχου προστασίας των δεδομένων και διαγράφεται από τον υπεύθυνο επεξεργασίας με την πάροδο έξι μηνών από την ενημέρωση του υποκειμένου των δεδομένων, εκτός εάν βρίσκεται έλεγχος σε εξέλιξη, οπότε διατηρείται μέχρι την ολοκλήρωσή του (Άρθρο 8 παρ. 5 του Π.Δ. 81/2021).

Κατ' εξαίρεση, τα προσωπικά δεδομένα δεν διαγράφονται όταν η διαγραφή τους θα μπορούσε να θέσει σε κίνδυνο τα συμφέροντα του υποκειμένου, για παράδειγμα όταν αποτελούν αποδεικτικό στοιχείο υπέρ του, καθώς και όταν είναι απαραίτητα για δικαστική χρήση. Σε αυτές τις περιπτώσεις, τα δεδομένα «κλειδώνονται» και τα έγγραφα, που τα περιέχουν, είτε σε έντυπη είτε σε ψηφιακή μορφή, επισημαίνονται με σχετική ένδειξη. Αυτό πρακτικά σημαίνει ότι τα κλειδωμένα δεδομένα, που αφορούν προφίλ DNA, δακτυλικά αποτυπώματα και άδειες κυκλοφορίας οχημάτων στο πλαίσιο διασυνοριακής συνεργασίας της Ελληνικής Αστυνομίας και των αρμόδιων αρχών των άλλων κρατών μελών ή της Ευροpol, μπορούν να χρησιμοποιηθούν αποκλειστικά και μόνο για τον σκοπό, που παρεμπόδιζε τη διαγραφή τους (Άρθρο 8 παρ. 6 του Π.Δ. 81/2021 και άρθρο 51 του Κανονισμού 2024/982).

6.8.6. Τεχνικά και οργανωτικά μέτρα

Η Ελληνική Αστυνομία, όπως και όλοι οι φορείς, που παρέχουν και λαμβάνουν προσωπικά δεδομένα στο πλαίσιο διασυνοριακής συνεργασίας κατά το Π.Δ. 81/2021 και τον Κανονισμό 2024/982, εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλίζεται η προστασία των δεδομένων από τυχαία απώλεια, αλλοίωση, καταστροφή και μη εξουσιοδοτημένη πρόσβαση και επεξεργασία. Πιο συγκεκριμένα:

- για το παραδεκτό των αναζητήσεων και της παροχής δεδομένων τηρούνται αρχεία καταγραφής κάθε αυτοματοποιημένης και μη αναζήτησης, αλλά και παροχής και λήψης δεδομένων και εφαρμόζονται κατάλληλα μέτρα για την προστασία αυτών των αρχείων από μη εξουσιοδοτημένη ή αντικανονική χρήση (Άρθρα 9 παρ.2-4 του Π.Δ. 81/2021),
- χρησιμοποιούνται τεχνικές κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων, τόσο κατά τη μεταφορά όσο και κατά την αποθήκευσή τους,
- οι αυτοματοποιημένες αναζητήσεις και συγκρίσεις των δεδομένων πραγματοποιούνται μόνο από εξουσιοδοτημένα άτομα των εθνικών σημείων επαφής.

Επιπλέον, κατά τη σύγκριση προφίλ DNA με αυτά που τηρούνται στο εθνικό αρχείο, καθώς και κατά την ταυτοποίηση δακτυλικών αποτυπωμάτων από το αυτόματο σύστημα αναγνώρισης δακτυλικών και παλαμικών αποτυπωμάτων⁵⁵, σε κάθε

⁵⁵ Το αυτόματο σύστημα αναγνώρισης δακτυλικών και παλαμικών αποτυπωμάτων (Α.Σ.Α.Δ.Π.Α.) βρίσκεται στη Δ.Ε.Ε. και συγκρίνει τα αποτυπώματα (δακτυλικά και παλαμικά), που συλλέγονται από την Ελληνική Αστυνομία από τόπους εγκλημάτων με αυτά που είναι ήδη καταχωρημένα από άτομα που έχουν σημειωθεί κατά το παρελθόν (https://www.astynomia.gr/file/2015/05/292_paroyysiadi_dee.pdf).

εξουσιοδοτημένο χρήστη του αρχείου ή συστήματος αποδίδεται μοναδικός αναγνωριστικός αριθμός, τον οποίο χρησιμοποιεί ο χρήστης σε κάθε ανάκτηση ή διαβίβαση δεδομένων (Άρθρο 10 του Π.Δ. 81/2021).

6.8.7. Δικαιώματα των υποκειμένων

Σε περίπτωση παραβίασης των προσωπικών δεδομένων, που ανταλλάσσονται κατά τη διασυνοριακή συνεργασία, η Ελληνική Αστυνομία, ως υπεύθυνος επεξεργασίας, ενημερώνει την Α.Π.Δ.Π.Χ., όπως ορίζει το άρθρο 63 του Ν. 4624/2019, ενημερώνοντας παράλληλα και το υποκείμενο αυτών των δεδομένων (Άρθρο 12 του Π.Δ. 81/2021).

Επιπλέον, η Ελληνική Αστυνομία παρέχει στο υποκείμενο των δεδομένων πληροφορίες αναφορικά με την επεξεργασία των δεδομένων του, τον σκοπό αυτής, το δικαίωμα πρόσβασης, διόρθωσης ή διαγραφής των δεδομένων, καθώς και το δικαίωμα υποβολής καταγγελίας στην Α.Π.Δ.Π.Χ. (Άρθρο 13 και 14 του Π.Δ. 81/2021).

6.8.8. Συμπεράσματα

Από την ανάλυση, που πραγματοποιήθηκε στο παρόν κεφάλαιο γίνεται σαφές ότι η Ελληνική Αστυνομία στο πλαίσιο διασυνοριακής συνεργασίας με αρμόδιες αρχές άλλων κρατών μελών ή της Europol, ανταλλάσσει προσωπικά δεδομένα, τόσο απλά όσο και ευαίσθητα, με σκοπό την πρόληψη και διερεύνηση αξιόποινων πράξεων και κυρίως την αντιμετώπιση της τρομοκρατίας και του διασυνοριακού εγκλήματος, βάσει της αρχής της νομιμότητας. Τα παρεχόμενα δεδομένα δεν μπορούν να χρησιμοποιηθούν για σκοπό διαφορετικό από αυτόν για τον οποίο ζητήθηκαν, παρά μόνο κατόπιν σχετικής άδειας του κράτους μέλους, που διαχειρίζεται το αρχείο των δεδομένων και εφόσον αυτό προβλέπεται από το εθνικό δίκαιο.

Επιπλέον, κατά την διασυνοριακή ανταλλαγή δεδομένων, η ΕΛ.ΑΣ. διαβιβάζει μόνο τα απολύτως απαραίτητα δεδομένα, που περιγράφηκαν προηγουμένως ανά περίπτωση, διασφαλίζοντας τον ακριβή και επικαιροποιημένο χαρακτήρα τους, προβαίνοντας σε διόρθωση αυτών όταν προκύψει αποδεδειγμένο σφάλμα.

Προς διασφάλιση της αρχής της περιόδου αποθήκευσης, κατά την αυτοματοποιημένη αναζήτηση και σύγκριση, τα παρεχόμενα δεδομένα διαγράφονται αμέσως μετά την απάντηση στο λαμβάνον κράτος μέλος, ενώ σε περίπτωση περαιτέρω συνεργασίας με τις αρχές των άλλων κρατών μελών, διατηρούνται μόνο για τον σκοπό, που παρασχέθηκαν και για το χρονικό διάστημα, που προβλέπει το εθνικό δίκαιο του παρέχοντος κράτους μέλους.

Με την εφαρμογή τεχνικών και οργανωτικών μέτρων, η ΕΛ.ΑΣ. αποτρέπει την μη εξουσιοδοτημένη πρόσβαση, αλλοίωση, καταστροφή ή διαρροή των δεδομένων, διασφαλίζοντας την ακεραιότητα και εμπιστευτικότητα των δεδομένων.

Τέλος, η καταγραφή κάθε ενέργειας στο πλαίσιο διασυνοριακής συνεργασίας, παρέχει στην Ελληνική Αστυνομία τη δυνατότητα να τεκμηριώνει και να αποδεικνύει το παραδεκτό των αναζητήσεων και της παροχής δεδομένων.

6.9. Συμπεράσματα

Οι αστυνομικές Υπηρεσίες κατά την άσκηση των καθηκόντων τους συλλέγουν και επεξεργάζονται τόσο απλά όσο και ευαίσθητα προσωπικά δεδομένα. Η Ελληνική Αστυνομία διαθέτει μεγάλο εύρος δραστηριοτήτων, εκ των οποίων κάποιες υπόκεινται στον GDPR, ενώ κάποιες άλλες αφορούν την πρόληψη, διερεύνηση και ποινική δίωξη αξιόποινων πράξεων, οπότε υπάγονται στην Οδηγία 2016/680, όπως ενσωματώθηκε στο κεφάλαιο IV του Ν. 4624/2019.

Στο παρόν κεφάλαιο παρουσιάστηκε και αναλύθηκε η επεξεργασία και προστασία των προσωπικών δεδομένων, στο πλαίσιο συγκεκριμένων λειτουργιών της ΕΛ.ΑΣ., που αφορούν την ανάλυση DNA, την άρση του απορρήτου των επικοινωνιών, τη δημοσιοποίηση προσωπικών δεδομένων κατηγορουμένων και καταδικασθέντων, την έκδοση ταυτοτήτων και διαβατηρίων, την επιτήρηση δημόσιων χώρων, τον διαγωνισμό πρόσληψης ιδιωτών στις Σχολές της Ελληνικής Αστυνομίας και τη διασυνοριακή συνεργασία της ΕΛ.ΑΣ με αρμόδιες αρχές άλλων κρατών μελών.

Από τις προαναφερόμενες περιπτώσεις, η ανάλυση DNA, η άρση του απορρήτου των επικοινωνιών, η δημοσιοποίηση προσωπικών δεδομένων κατηγορουμένων και καταδικασθέντων, καθώς και η διασυνοριακή συνεργασία, υπάγονται αμιγώς στο κεφάλαιο IV του Ν. 4624/2019, καθώς αφορούν περιπτώσεις συλλογής και επεξεργασίας δεδομένων από αρμόδια αρχή για την πρόληψη, διερεύνηση και ποινική δίωξη αδικημάτων. Δεδομένου ότι η συλλογή και επεξεργασία δεδομένων για την έκδοση ταυτοτήτων και διαβατηρίων διενεργούνται από την Ελληνική Αστυνομία στο πλαίσιο άσκησης δημόσιας εξουσίας και όχι για την πρόληψη και διερεύνηση ποινικών αδικημάτων, υπάγονται στον GDPR και σε διατάξεις του Ν. 4624/2019, που αφορούν μέτρα εφαρμογής αυτού. Η συλλογή και διαχείριση προσωπικών δεδομένων κατά την επιτήρηση δημόσιων χώρων μπορεί να υπάγεται είτε στον GDPR είτε στο κεφάλαιο IV του Ν. 4624/2019, ανάλογα με τον απώτερο σκοπό της. Ειδικότερα, οι περιπτώσεις που αφορούν την πρόληψη, καταστολή και διερεύνηση ποινικών αδικημάτων ρυθμίζονται από το κεφάλαιο IV του Ν. 4624/2019, ενώ η διαχείριση της κυκλοφορίας στο οδικό δίκτυο ρυθμίζεται από τον GDPR και τις σχετικές διατάξεις του Ν. 4624/2019. Τέλος, η διαχείριση των προσωπικών δεδομένων των υποψηφίων των Σχολών της Ελληνικής Αστυνομίας υπάγεται στον GDPR και σε σχετικές διατάξεις του Ν. 4624/2019.

Συνεπώς, κατόπιν της ανάλυσης που προηγήθηκε για κάθε επιμέρους λειτουργία της ΕΛ.ΑΣ., καταλήγουμε στο συμπέρασμα ότι η Ελληνική Αστυνομία, κατά την συλλογή και επεξεργασία προσωπικών δεδομένων μεριμνά για την προστασία αυτών εφαρμόζοντας τις βασικές αρχές επεξεργασίας, που προβλέπουν τα νομικά κείμενα και οι οποίες αναλύθηκαν στις Ενότητες 4.2.2 και 4.5.2 (όσον αφορά τον GDPR και τον Ν. 4624/2019, αντίστοιχα).

7. Προκλήσεις και μέτρα αντιμετώπισης

Η διαδικασία της επεξεργασίας των προσωπικών δεδομένων και η διασφάλιση της προστασίας αυτών στο πλαίσιο της λειτουργίας της ΕΛ.ΑΣ. δεν είναι εύκολη υπόθεση, αλλά αποτελεί μία σύνθετη διαδικασία, καθώς απαιτεί αποτελεσματική και σύννομη άσκηση των αρμοδιοτήτων και καθηκόντων της με παράλληλη διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων.

Αν και από την ανάλυση, που πραγματοποιήθηκε στα προηγούμενα κεφάλαια γίνεται αντιληπτό ότι η Ελληνική Αστυνομία εφαρμόζει τις διατάξεις που ορίζει ο GDPR και ο Ν. 4624/2019 και μεριμνά για την προστασία των προσωπικών δεδομένων, υπάρχουν ορισμένες προκλήσεις, που δύναται να ανακύψουν κατά την επεξεργασία τους, οι οποίες επικεντρώνονται στο δίλημμα επιλογής του κατάλληλου νομικού κειμένου, στο ανθρώπινο δυναμικό, στους τεχνολογικούς περιορισμούς, στις κυβερνοεπιθέσεις & κυβερνοαπειλές, καθώς και στις περιβαλλοντικές απειλές.

7.1. Προκλήσεις

7.1.1. GDPR ή Οδηγία 2016/680;

Μία σημαντική πρόκληση που αντιμετωπίζουν οι αρμόδιες αρχές και συνεπώς και η Ελληνική Αστυνομία, κατά την επεξεργασία προσωπικών δεδομένων, είναι η επιλογή του κατάλληλου νομικού κειμένου.

Όπως έχει ήδη αναφερθεί, η Οδηγία 2016/680, που έχει ενσωματωθεί στον Ν. 4624/2019, εφαρμόζεται στις περιπτώσεις, που η Ελληνική Αστυνομία και εν γένει οι αρμόδιες αρχές επεξεργάζονται δεδομένα με σκοπό την πρόληψη, καταστολή, ανίχνευση και ποινική δίωξη αξιόποινων πράξεων. Στις υπόλοιπες περιπτώσεις, εφαρμόζεται ο GDPR (Ιγγλεζάκης, Ι., 2020: 41).

Κατά την εκτέλεση των καθηκόντων της, που εμπίπτουν στην άσκηση δημόσιας εξουσίας, όπως είναι για παράδειγμα η έκδοση διαβατηρίων, παρ' όλο που η λειτουργία αυτή υπάγεται στον GDPR, γίνεται χρήση και αποκτάται πρόσβαση σε δεδομένα, που αφορούν το ποινικό μητρώο του ενδιαφερόμενου, τα οποία έχουν συλλεχθεί κατ' εφαρμογή της Οδηγίας 2016/680. Εάν κατά τον έλεγχο των ποινικών δεδομένων, προκύψει για παράδειγμα ότι εκκρεμεί σε βάρος του ενδιαφερόμενου κάποια καταδικαστική υπόθεση, ή ότι διώκεται στα όρια του αυτοφώρου, τότε ενεργοποιείται η Οδηγία 2016/680. Συνεπώς, σε αυτές τις περιπτώσεις δημιουργείται σύγχυση σχετικά με το ποιο νομικό κείμενο θα εφαρμοστεί τελικά. Αν η ΕΛ.ΑΣ. εφαρμόσει μόνο τον GDPR υπάρχει κίνδυνος να αποκαλύψει στον ενδιαφερόμενο «απόρρητες» πληροφορίες, που εμπίπτουν στην Οδηγία 2016/680. Αν εφαρμόσει μόνο την Οδηγία 2016/680 ενδέχεται να περιορίσει αδικαιολόγητα τα δικαιώματα του πολίτη, όπως αυτό της πρόσβασης στα δεδομένα.

Επομένως, χρειάζονται ιδιαίτερο χειρισμό τέτοιες περιπτώσεις. Λογικό επακόλουθο της επιλογής του GDPR ή της Οδηγίας 2016/680 είναι η επίδραση στην άσκηση των δικαιωμάτων των υποκειμένων, καθώς η Οδηγία είναι πιο αυστηρή και προβλέπει περιορισμούς σε αυτά και ιδίως στο δικαίωμα πρόσβασης, ενημέρωσης και

διαγραφής, για λόγους δημόσιας ασφάλειας και στο πλαίσιο πρόληψης και καταστολής του εγκλήματος. Η διαφοροποίηση αυτή προκαλεί σύγχυση στα υποκείμενα των δεδομένων, όταν τα δεδομένα τους τίθενται υπό επεξεργασία από τις αστυνομικές αρχές (Aidinlis et al., 2024: 19).

Μάλιστα, λαμβάνοντας υπόψη ότι οι δράσεις της Ελληνικής Αστυνομίας κατά την διερεύνηση και ποινική δίωξη των αξιόποινων πράξεων πραγματοποιούνται υπό μυστικότητα και επομένως περιορισμένη διαφάνεια, η άσκηση των δικαιωμάτων των υποκειμένων είναι εξίσου περιορισμένη (Κανέλλος, 2020: 279, 292), ενισχύοντας κατ' επέκταση την ανησυχία των τελευταίων για την προστασία των δεδομένων και της ιδιωτικότητάς τους, σε περίπτωση εσφαλμένης επιλογής νομικού κειμένου.

Συνεπώς, δεν είναι πάντα εύκολη η διάκριση και επιλογή ανάμεσα στον GDPR και την Οδηγία 2016/680, με αποτέλεσμα να δημιουργείται νομική αβεβαιότητα και αυξημένος κίνδυνος για την προστασία των δεδομένων.

7.1.2. Ανθρώπινο δυναμικό

Σε έναν οργανισμό το ανθρώπινο δυναμικό διαδραματίζει καθοριστικό ρόλο στην ασφάλεια των συστημάτων και των πληροφοριών, καθώς όταν διαθέτει κατάλληλες δεξιότητες και γνώσεις μπορεί να συμβάλει σημαντικά στην προστασία αυτών. Από την άλλη όμως, η αδιαφορία, η αμάθεια ή/και η ημιμάθεια, αλλά και οι δόλιες κακόβουλες ενέργειες του προσωπικού, μπορούν να επιφέρουν επιζήμιες επιπτώσεις στα πληροφοριακά συστήματα και τα δεδομένα που διαχειρίζεται ο οργανισμός (Κοκολάκης, Σ., 2021: 57).

Αυτό, ασφαλώς, ισχύει και στην περίπτωση της Ελληνικής Αστυνομίας. Η ορθή εφαρμογή των βασικών αρχών επεξεργασίας δεδομένων και ο σεβασμός στα δικαιώματα των υποκειμένων, δεν εξαρτάται αποκλειστικά από το νομικό πλαίσιο ή τα πληροφοριακά συστήματα, που χρησιμοποιούνται αλλά σε μεγάλο βαθμό και από την συμπεριφορά, κατάρτιση και ευαισθητοποίηση του αστυνομικού προσωπικού. Το ανθρώπινο δυναμικό συνιστά έναν κρίσιμο παράγοντα κατά την επεξεργασία προσωπικών δεδομένων από την ΕΛ.ΑΣ., καθώς τυχόν ελλειπείς γνώσεις και εσφαλμένες ερμηνείες των διατάξεων, δύνανται να οδηγήσουν σε παραβιάσεις της προστασίας αυτών των δεδομένων.

7.1.3. Τεχνολογικοί περιορισμοί

Προκειμένου η ΕΛ.ΑΣ. να διασφαλίζει την προστασία των δεδομένων κατά την επεξεργασία τους, θα πρέπει να ακολουθεί τις τεχνολογικές αλλαγές, που αφορούν τα συστήματά της, με τα οποία συλλέγει, αποθηκεύει και διαχειρίζεται προσωπικά δεδομένα. Αυτό πρακτικά σημαίνει ότι τα απαρχαιωμένα ή παλαιού τύπου συστήματα δύναται να περιορίζουν την εφαρμογή ισχυρών μεθόδων κρυπτογράφησης, τους ελέγχους πρόσβασης και γενικά τους μηχανισμούς παρακολούθησης των συστημάτων. Φυσικά, ακόμα και σε ένα σύγχρονο σύστημα η μη τακτική επικαιροποίηση του λογισμικού προστασίας περιορίζει σημαντικά την ασφάλεια του συστήματος. Οι περιορισμοί αυτοί δημιουργούν με τη σειρά τους τρωτά σημεία στα συστήματα της

ΕΛ.ΑΣ., με αποτέλεσμα να αυξάνονται οι πιθανότητες κυβερνοεπίθεσης (Μωραΐτης, Μ., Partner, Valida, Α., 2024)⁵⁶.

Ασφαλώς, οποιαδήποτε αλλαγή στον υλικοτεχνικό εξοπλισμό της Ελληνικής Αστυνομίας, θα πρέπει να εξετάζεται πρώτα ως προς τις πιθανές επιπτώσεις, που ενδέχεται να επιφέρει στην ασφάλεια των πληροφοριακών συστημάτων αλλά και των πληροφοριών (Κοκολάκης, Σ., 2021: 60), καθώς μία τέτοια αλλαγή μπορεί να προκαλέσει αλλοίωση, καταστροφή ή και μη εξουσιοδοτημένη πρόσβαση σε αρχείο δεδομένων προσωπικού χαρακτήρα.

7.1.4. Κυβερνοαπειλές - κυβερνοεπιθέσεις

Άλλη μία πρόκληση, εξίσου σημαντική, που καλείται να λάβει υπόψη της η Ελληνική Αστυνομία κατά την επεξεργασία προσωπικών δεδομένων, προκειμένου να διασφαλίσει την προστασία αυτών στο πλαίσιο άσκησης των καθηκόντων της είναι μια ενδεχόμενη κυβερνοαπειλή ή κυβερνοεπίθεση, που μπορεί να εμφανιστεί στα πληροφοριακά της συστήματα.

Σύμφωνα με το άρθρο 2 του Κανονισμού (ΕΕ) 2019/881 «Πράξη για την Κυβερνοασφάλεια» ως κυβερνοαπειλή νοείται ένα πιθανό συμβάν ή μία ενέργεια που μπορεί να προκαλέσει ζημία ή να επηρεάσει γενικά αρνητικά, με οποιονδήποτε τρόπο, τη λειτουργία των συστημάτων και δικτύων πληροφοριών, τους χρήστες αυτών, καθώς και κάθε άλλο τρίτο πρόσωπο. Επομένως, λόγος για κυβερνοεπίθεση γίνεται όταν αυτό το συμβάν λάβει, τελικά, χώρα.

Η ταχύτητα εξελισσόμενη ψηφιοποίηση των υπηρεσιών στον σύγχρονο ψηφιακό κόσμο δημιουργεί ένα ιδιαίτερα ελκυστικό πεδίο για τους κακόβουλους χρήστες⁵⁷. Οι διαδικτυακοί κίνδυνοι εμφανίζουν ποικιλομορφία (Πρώτο Θέμα, 2024)⁵⁸ και οι κυβερνοεπιθέσεις γίνονται ολοένα και πιο σύνθετες και δυσδιάκριτες, καθώς οι κακόβουλοι χρήστες εκμεταλλεύονται την ελλιπή ενημέρωση των χρηστών και την απουσία της συνεχούς επίβλεψης των συστημάτων και δικτύων⁵⁹.

Οι πιο επιβλαβείς και επικίνδυνες κυβερνοεπιθέσεις θεωρούνται πως είναι οι ransomware, οι DDOS και οι Zero-Day επιθέσεις, καθώς και το phishing (skai.gr, 2025)⁶⁰, ενώ μία από τις πιο συνηθισμένες επιπτώσεις είναι η υποκλοπή / διαρροή δεδομένων, άρα και προσωπικών ή ευαίσθητων.

Επομένως, μία κυβερνοεπίθεση δεν επηρεάζει μόνο τη λειτουργία του εκάστοτε συστήματος, αλλά έχει άμεση επίδραση και στα φυσικά πρόσωπα, είτε αυτά αφορούν τους χρήστες των συστημάτων ή/και τρίτα πρόσωπα.

⁵⁶ <https://netweek.gr/katanoisi-ton-prokliseon-tis-sostis-efarmogis-tou-gdpr/>

⁵⁷ <https://cyber.gov.gr/kyvernoepitheseis/kyvernoepitheseis-kyvernoasfaleia/>

⁵⁸ <https://www.protothema.gr/greece/article/1552671/kuvernoasfaleia-ena-stoihima-pou-kamia-etairia-den-ehei-perithorio-na-hasei/>

⁵⁹ <https://cyber.gov.gr/kyvernoepitheseis/kyvernoepitheseis-kyvernoasfaleia/>

⁶⁰ <https://www.skai.gr/news/technology/kyvernoepitheseis-poes-einai-oi-pio-epikindynes-gia-krati-organismous-kai-epixeiriseis>

7.1.5. Περιβαλλοντικές απειλές

Οι υποδομές και τα συστήματα της ΕΛ.ΑΣ., αντιμετωπίζουν και περιβαλλοντικές απειλές, οι οποίες μπορεί να οφείλονται σε φυσικές (π.χ. πυρκαγιές, σεισμούς, πλημμύρες κ.λπ.) ή σε ανθρωπογενείς καταστροφές (π.χ. βανδαλισμούς, εκρήξεις, τρομοκρατικές ενέργειες, εξεγέρσεις κ.λπ.) (Κοκολάκης, Σ., 2021: 59).

Έτσι, για παράδειγμα, ένα φυσικό φαινόμενο, όπως μία πλημμύρα, δύναται να προκαλέσει την εισροή μεγάλης ποσότητας υδάτων στο χώρο εγκατάστασης των servers, με αποτέλεσμα την πρόκληση σοβαρής υλικής βλάβης στον εξοπλισμό. Επακόλουθο αυτής ενδέχεται να είναι η ανεπανόρθωτη αλλοίωση ή διαγραφή των αρχείων, που χειρίζεται ψηφιακά η εκάστοτε αστυνομική Υπηρεσία. Λαμβάνοντας υπόψη ότι στα αρχεία βρίσκονται αποθηκευμένα, μεταξύ άλλων, προσωπικά δεδομένα πολιτών, ένα τέτοιο συμβάν δύναται να έχει ως αποτέλεσμα την πρόωρη καταστροφή των δεδομένων.

Επιπλέον, ανθρωπογενείς καταστροφές, όπως εκρηκτικές επιθέσεις ή πράξεις βανδαλισμού σε αστυνομικές Υπηρεσίες, δύναται να προκαλέσουν σοβαρές υλικές ζημιές στις υποδομές και τον τεχνικό εξοπλισμό τους. Τέτοιου είδους περιστατικά μπορούν να οδηγήσουν όχι μόνο σε διακοπή της λειτουργίας των συστημάτων, αλλά και σε ολική ή μερική καταστροφή των ψηφιακών και έντυπων προσωπικών δεδομένων, που τηρούνται σε αυτές.

7.2. Μέτρα αντιμετώπισης προκλήσεων

Η Ελληνική Αστυνομία, όπως και κάθε δημόσιος και ιδιωτικός φορέας ή οργανισμός, κατά την επεξεργασία προσωπικών δεδομένων οφείλει να εφαρμόζει της βασικές αρχές, που προβλέπουν τα νομικά κείμενα και να μεριμνά για την προστασία των δεδομένων, ώστε να αποφεύγονται περιπτώσεις παραβίασης των νομικών διατάξεων, οι οποίες επιφέρουν κυρώσεις. Προκειμένου να το επιτύχει, πρέπει να λαμβάνει κατάλληλα μέτρα, που αφορούν τόσο τα συστήματα και τις υποδομές της όσο και το ανθρώπινο δυναμικό, τα οποία θα έχουν ως απώτερο σκοπό την ελαχιστοποίηση του κινδύνου παραβίασης των προσωπικών δεδομένων και την προστασία τους. Τα εν λόγω μέτρα αφορούν κατά κύριο λόγο την εφαρμογή κατάλληλης μεθοδολογίας διαχείρισης επικινδυνότητας, την εκπαίδευση και ενημέρωση του προσωπικού, τη διενέργεια ελέγχων πρόσβασης σε ψηφιακούς και φυσικούς πόρους, την καταγραφή των ενεργειών στα συστήματα και φυσικά αρχεία της ΕΛ.ΑΣ., την εφαρμογή ενός συνόλου ενεργειών ασφάλειας στον κυβερνοχώρο, την τήρηση αντιγράφων ασφαλείας και την κρυπτογραφία, ψευδωνυμοποίηση και ανωνυμοποίηση των δεδομένων.

7.2.1. Μεθοδολογία διαχείρισης επικινδυνότητας

Στο πλαίσιο μίας ολιστικής διαχείρισης των κινδύνων που αφορούν τα προστατευόμενα αγαθά, όπως είναι οι υποδομές, τα συστήματα, ο δικτυακός εξοπλισμός, τα μέσα αποθήκευσης και μεταφοράς και ασφαλώς τα ίδια τα δεδομένα, η ΕΛ.ΑΣ. οφείλει να εφαρμόζει συνεχώς μία κατάλληλα σχεδιασμένη μεθοδολογία διαχείρισης επικινδυνότητας, η οποία θα διασφαλίζει την συστηματική αποτίμηση και αντιμετώπιση των σχετικών κινδύνων. Αρχικά, ως επικινδυνότητα ορίζεται το γινόμενο

της πιθανότητας να πραγματοποιηθεί ένα επεισόδιο ασφάλειας επί το κόστος που αυτό θα επιφέρει, δηλαδή την επακόλουθη συνέπεια στην ΕΛ.ΑΣ.. Ένα επεισόδιο μπορεί για παράδειγμα να συνιστά φυσικές απειλές (φωτιά, πλημμύρα, κ.λπ.), κακόβουλες ενέργειες (hacking, virus, βανδαλισμοί κ.λπ.), ανθρώπινα λάθη (διαγραφή βάσης δεδομένων), αστοχίες εξοπλισμού (βλάβες), κ.λπ.

Απαραίτητη προϋπόθεση για την αποτελεσματική εφαρμογή μίας μεθοδολογίας διαχείρισης επικινδυνότητας αποτελεί ο πρότερος καθορισμός των κριτηρίων αποδοχής των κινδύνων, δηλαδή το επίπεδο που είναι διατεθειμένη η ΕΛ.ΑΣ. να αποδεχτεί, ώστε στην συνέχεια να εκτιμηθούν και να αντιμετωπιστούν (προληπτικά ή αντιδραστικά) τυχόν επεισόδια ασφάλειας.

Το πρώτο στάδιο διαχείρισης της επικινδυνότητας, που αφορά την εκτίμηση αυτής, αποτελείται από τρία επιμέρους στάδια, τον εντοπισμό, την ανάλυση και την αξιολόγηση της επικινδυνότητας. Υπό αυτό το πρίσμα, η ΕΛ.ΑΣ. θα πρέπει να εντοπίζει και να αναλύει τους παράγοντες, που συνιστούν απειλή για τα πληροφοριακά συστήματα της ΕΛ.ΑΣ. και τα προσωπικά δεδομένα, που διαχειρίζεται και να υπολογίζει το επίπεδο του κινδύνου⁶¹. Ακολούθως, θα πρέπει να το συγκρίνει με τα προκαθορισμένα όρια αποδοχής, ώστε να προσδιορίζει τους κινδύνους, που τα υπερβαίνουν και να τους ιεραρχεί, για να αποφασίσει, στην συνέχεια, ποιοι κίνδυνοι πρέπει να αντιμετωπιστούν κατά προτεραιότητα (Κοκολάκης, Σ., 2021: 66). Επομένως, με την εκτίμηση της επικινδυνότητας αποτυπώνονται οι κίνδυνοι και οι πιθανότητες εμφάνισής τους.

Το δεύτερο στάδιο διαχείρισης αφορά την αντιμετώπιση της επικινδυνότητας, όπου η ΕΛ.ΑΣ. θα πρέπει να προβαίνει σε κάθε ενέργεια, που αποβλέπει στη μείωση του επιπέδου της επικινδυνότητας και στη διατήρησή του εντός των προκαθορισμένων αποδεκτών ορίων, όπως για παράδειγμα στην επιλογή και εφαρμογή κατάλληλων μέτρων προστασίας και στη διαμόρφωση πολιτικών ασφάλειας πληροφοριών (Κοκολάκης, Σ., 2021: 66).

Μάλιστα, η ΕΛ.ΑΣ. θα πρέπει να καταρτίζει ένα Σχέδιο Επιχειρησιακής Συνέχειας, το οποίο να περιλαμβάνει όλες τις απαραίτητες ενέργειες και διαδικασίες που θα πρέπει να ακολουθεί το αστυνομικό προσωπικό για την αποτελεσματική διαχείριση περιστατικών και διαταράξεων της λειτουργίας τους, με σκοπό την εύρυθμη επιχειρησιακή της λειτουργία (Κοκολάκης, Σ. 2021: 63).

Τα δύο στάδια διαχείρισης, που προαναφέρθηκαν, ακολουθεί ένα τρίτο που αφορά την παρακολούθηση και επιθεώρηση των κινδύνων, επιπέδων επικινδυνότητας και αντίστοιχων ενεργειών μείωσής τους αλλά και των διαδικασιών, εργαλείων και κανόνων διοίκησης της υφιστάμενης μεθοδολογίας, ώστε να διασφαλίζεται ότι είναι επικαιροποιημένοι, αντιμετωπίζουν αποτελεσματικά την τρέχουσα επικινδυνότητα και συμβαδίζουν με τους στόχους της ΕΛ.ΑΣ.. Τα στάδια αυτά εκτελούνται με κυκλικό τρόπο σε συνεχή βάση.

⁶¹ Η εκτίμηση του κινδύνου, συνήθως, γίνεται σε ποσοτικούς όρους.

7.2.2. Εκπαίδευση – Ενημέρωση

Άλλο ένα εξαιρετικά σημαντικό μέτρο αντιμετώπισης των προκλήσεων είναι η εκπαίδευση του προσωπικού. Η Ελληνική Αστυνομία θα πρέπει να διασφαλίζει ότι οι αστυνομικοί υπάλληλοι είναι επαρκώς ενημερωμένοι για τα νομικά κείμενα προστασίας δεδομένων και την ορθή εφαρμογή τους καθώς και για τις καλές πρακτικές ασφάλειας, που πρέπει να ακολουθούν. Αυτό μπορεί να το εξασφαλίσει με τακτικές ενημερώσεις και επιμορφωτικά σεμινάρια, ιδίως όταν επέρχονται αλλαγές ή τροποποιήσεις στα νομικά κείμενα, αλλά και με την ανάρτηση οδηγιών, σε σημείο που να έχουν όλοι πρόσβαση, αναφορικά με τις βασικές αρχές επεξεργασίας δεδομένων, τα δικαιώματα των υποκειμένων, τόσο όταν εφαρμόζεται ο GDPR, όσο και όταν εφαρμόζεται η Οδηγία 2016/680, την ορθή χρήση του υπηρεσιακού email και των εφαρμογών που χρησιμοποιεί, την ασφαλή αποθήκευση αρχείων, τη χρήση ισχυρών κωδικών πρόσβασης, την αξιολόγηση και αναφορά περιστατικών ασφαλείας, κ.λπ..

Ωστόσο, δεδομένου ότι πολλές απειλές στα πληροφοριακά συστήματα οφείλονται σε αδυναμία, αμέλεια ή/και κακόβουλες ενέργειες των χρηστών, η ΕΛ.ΑΣ. θα πρέπει να μεριμνά για προγράμματα εκπαίδευσης και ευαισθητοποίησης του αστυνομικού προσωπικού, σχετικά με την ασφάλεια των πληροφοριακών συστημάτων, τις επιθέσεις που ενδέχεται να προκύψουν και τον χειρισμό τους (Κοκολάκης, Σ., 2021: 57). Με αυτό τον τρόπο, διαμορφώνεται μία κουλτούρα ασφάλειας, προκειμένου οι ενέργειες των υπαλλήλων να είναι σύμφωνες με τις βασικές αρχές και τους στόχους ασφαλείας που έχουν τεθεί (Καρύδα, Μ., 2021: 111).

Μάλιστα, μέσω της εκπαίδευσης και της σωστής ενημέρωσης του αστυνομικού προσωπικού θα πρέπει να γίνεται σαφές πότε εφαρμόζεται ο GDPR και πότε η Οδηγία 2016/680.

7.2.3. Έλεγχος πρόσβασης

Εκτός από την ενημέρωση και εκπαίδευση των αστυνομικών υπαλλήλων, θα πρέπει να εφαρμόζονται έλεγχοι σχετικά με την αιτούμενη πρόσβαση τόσο στους φυσικούς όσο και ψηφιακούς πόρους της ΕΛ.ΑΣ.. Αυτό πρακτικά σημαίνει ότι θα πρέπει να ελέγχεται κάθε πρόσβαση στις εγκαταστάσεις, στα πληροφοριακά συστήματα της ΕΛ.ΑΣ, όσο στα προσωπικά δεδομένα που η ΕΛ.ΑΣ. διαχειρίζεται. Ο έλεγχος πρόσβασης αφορά τις διαδικασίες που ακολουθούνται και τα μέτρα, που λαμβάνονται ώστε να προστατεύονται, οι εγκαταστάσεις, τα συστήματα και τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση (Κοκολάκης, Σ., 2021: 58).

Όσον αφορά τον έλεγχο πρόσβασης στους ψηφιακούς πόρους, κάθε αστυνομικός, ανάλογα με τη θέση και τα καθήκοντα, που του έχουν ανατεθεί σε μία αστυνομική Υπηρεσία, θα πρέπει να έχει συγκεκριμένα δικαιώματα πρόσβασης στα συστήματα αυτής και να γνωρίζει επακριβώς ποιες είναι οι υποχρεώσεις του, όσον αφορά τους κωδικούς πρόσβασης, το υπηρεσιακό email, τη χρήση του διαδικτύου κ.λπ. (Κοκολάκης, Σ., 2021: 58-59).

Λαμβάνοντας υπόψη ότι ο έλεγχος πρόσβασης αποτελεί βασικό πυλώνα της ασφάλειας των πληροφοριακών συστημάτων, ο οποίος καθορίζεται από σαφώς

ορισμένες πολιτικές ασφαλείας και κανόνες πρόσβασης, οι τελευταίες πρέπει να ευθυγραμμίζονται με τις απαιτήσεις της ΕΛ.ΑΣ. και να εφαρμόζονται μέσω κατάλληλων μηχανισμών αυθεντικοποίησης και εξουσιοδότησης. Πιο συγκεκριμένα, για την ενίσχυση της ασφάλειας των συστημάτων και των δεδομένων, ακόμα και σε περιπτώσεις τεχνολογικών περιορισμών, σε επίπεδο αυθεντικοποίησης του εκάστοτε χρήστη είναι απαραίτητη η χρήση πολυπαραγοντικού ελέγχου (Multi-Factor Authentication -MFA), δηλαδή ο συνδυασμός τεχνικών αυθεντικοποίησης (Μάγκος, Ε. & Χρυσικόπουλος, Β., 2021: 284). Αυτό μπορεί να επιτευχθεί για παράδειγμα με τη χρήση ατομικής κάρτας πρόσβασης, με τη χρήση OTP⁶² μέσω του υπηρεσιακού email, κ.λπ..

Όσον αφορά τις τεχνικές εξουσιοδότησης, ανάλογα με τα χαρακτηριστικά του χρήστη (π.χ. ταυτότητα, ρόλος, βαθμίδα, κ.λπ.), που εξετάζεται στο πλαίσιο λήψης απόφασης για πρόσβαση σε ένα πληροφοριακό σύστημα, υπάρχουν διάφορα μοντέλα ελέγχου προσπέλασης, που έχουν διαμορφωθεί και εφαρμοστεί με το πέρασμα των ετών. Μία από τις πιο διαδεδομένες μέχρι σήμερα προσεγγίσεις για την ανάπτυξη συστημάτων ελέγχου προσπέλασης που θα μπορούσε να εφαρμόζεται είναι ο Έλεγχος Προσπέλασης Βασισμένος σε Ρόλους (Role-Based Access Control – RBAC), ο οποίος στηρίζεται στην αξιοποίηση ρόλων, ιεραρχιών ρόλων και περιορισμών διαχωρισμού καθηκόντων. Συνεπώς, τα δικαιώματα πρόσβασης σε αυτή την περίπτωση δεν παρέχονται σε άτομα-αστυνομικούς, αλλά σε ρόλους που έχουν συγκεκριμένα άτομα-αστυνομικοί (π.χ. Γραμματέας, Διοικητής, κ.λπ.) (Μαυρίδης, Ι., Σαλονικιάς, Σ. & Khair, M., 2021:309, 314). Έτσι, κάθε αστυνομικός έχει δικαίωμα πρόσβαση σε τμήματα του συστήματος και πληροφορίες, ανάλογα με το ρόλο που του έχει αποδοθεί από το ίδιο το σύστημα (Αστερίου, Β., et al., 2021:343).

Από την άλλη μεριά, η εφαρμογή των διατάξεων για την προστασία των προσωπικών δεδομένων, αλλά και η πρόληψη για την αποφυγή διαρροής δεδομένων, έχει καταστήσει αναγκαία την εφαρμογή αυστηρών διαδικασιών συνεχούς ελέγχου των προσβάσεων στα δεδομένα που υφίστανται στα πληροφοριακά συστήματα της ΕΛ.ΑΣ.. Σε αυτό το πλαίσιο η ΕΛ.ΑΣ. θα πρέπει να εφαρμόζει Έλεγχο Προσπέλασης Βασισμένο σε Χαρακτηριστικά (Attribute-based Access Control – ABAC), σύμφωνα με τον οποίο οι περιορισμοί πρόσβασης δεν βασίζονται μόνο στον εκάστοτε ρόλο του αστυνομικού, αλλά και σε άλλους παράγοντες – συνθήκες περιβάλλοντος, όπως είναι το είδος της πληροφορίας, η τοποθεσία από την οποία απαιτείται η πρόσβαση στην πληροφορία, η ώρα πρόσβασης, η συχνότητα, κ.λπ. (Μαυρίδης, Ι., Σαλονικιάς, Σ. και Khair, M., 2021: 317).

Επειδή το μοντέλο ABAC είναι πιο δύσκολο και σύνθετο στην εφαρμογή του, θα πρέπει να εφαρμόζεται με ιδιαίτερη προσοχή και να συνοδεύεται από κατάλληλες πολιτικές/κανόνες πρόσβασης και την απαραίτητη τεχνολογία, ειδικότερα όσον αφορά την ακριβή (precise) διαίσθηση του περιβάλλοντος. Από την άλλη μεριά, το ABAC υπάγει (subsumes) το RBAC οπότε δεν χρειάζεται η ταυτόχρονη εφαρμογή των δύο

⁶² One Time Password – προσωρινός αριθμητικός κωδικός, που ισχύει για λίγα λεπτά και για συγκεκριμένη χρήση

αυτών μοντέλων. Όμως, λόγω της προαναφερόμενης δυσκολίας εφαρμογής του ABAC, προκρίνεται η εφαρμογή του εκάστοτε μοντέλου από τα δύο ανά περίπτωση (δηλαδή ανά είδος συστήματος). Με την ταυτόχρονη εφαρμογή των δύο αυτών μοντέλων επιτυγχάνεται υψηλότερο επίπεδο ασφαλείας στα πληροφοριακά συστήματα της ΕΛ.ΑΣ. ανάλογα με το είδος τους και τις ανάγκες ασφαλείας, και συνεπώς και στα προσωπικά δεδομένα που διαχειρίζονται από τα συστήματα αυτά.

Αναφορικά με τον έλεγχο πρόσβασης στις εγκαταστάσεις της ΕΛ.ΑΣ. – ή αλλιώς τη φυσική ασφάλεια – θα πρέπει αρχικά να διαχωρίζονται οι χώροι των αστυνομικών Υπηρεσιών σε δημόσιους και ελεγχόμενους. Στην περίπτωση των τελευταίων, θα πρέπει να έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα, κάτι που μπορεί να εξασφαλιστεί για παράδειγμα με τη χρήση κάρτας εισόδου/εξόδου. Επιπλέον, επειδή πλήθος πολιτών επισκέπτεται τις Υπηρεσίες της ΕΛ.ΑΣ., θα πρέπει να λαμβάνονται μέτρα στο πλαίσιο εξυπηρέτησής τους προς αποφυγή ενεργειών, που μπορεί να επιφέρουν επιζήμια αποτελέσματα στην προστασία των δεδομένων (π.χ. υποκλοπή, αλλοίωση, καταστροφή, κ.λπ) και στη λειτουργία των πληροφοριακών της συστημάτων. Αυτό μπορεί να επιτευχθεί με την καταγραφή εισόδου/εξόδου των πολιτών, τη συνοδεία τους στους χώρους της εκάστοτε Υπηρεσίας και τη σωστή ενημέρωσή τους, τόσο από το ίδιο το αστυνομικό προσωπικό όσο και με την τοποθέτηση, σε εμφανή σημεία, σχετικών σημάνσεων στους χώρους περιορισμένης πρόσβασης (Κοκολάκης, Σ., 2021:59). Γενικά, ο έλεγχος πρόσβασης, είτε σε ψηφιακούς είτε σε φυσικούς πόρους, συνιστά μία σύνθετη διαδικασία ασφάλειας των πληροφοριών, καθώς εξαρτάται από την συμπεριφορά των ατόμων, αλλά και το λογισμικό που ελέγχει την πρόσβαση στα συστήματα και την αλληλεπίδρασή τους (Κοκολάκης, Σ., 2021: 59).

7.2.4. Καταγραφή ενεργειών

Άλλο ένα ισχυρό μέτρο, που συμβάλει στην αντιμετώπιση των προκλήσεων που αναφέρθηκαν στην Ενότητα 7.1 είναι η καταγραφή των ενεργειών, που λαμβάνουν χώρα τόσο στα συστήματα της ΕΛ.ΑΣ., όσο και στα φυσικά της αρχεία. Αυτό σημαίνει ότι θα πρέπει να καταγράφεται οποιαδήποτε ενέργεια πραγματοποιείται σε ένα σύστημα, ώστε να εντοπίζονται τυχόν απειλές, όπως για παράδειγμα προσπάθεια κυβερνοεπίθεσης και να εξασφαλίζεται η λογοδοσία των χρηστών του (Κοκολάκης, Σ., 2021: 61). Με την καταγραφή των ενεργειών ανιχνεύονται και ενδεχόμενες προσπάθειες πρόσβασης από μη εξουσιοδοτημένους χρήστες, όπως για παράδειγμα όταν γίνονται συνεχόμενες αποτυχημένες προσπάθειες πρόσβασης. Τα αρχεία καταγραφής θα πρέπει να αναλύονται και να αξιολογούνται, με τη χρήση κατάλληλων συστημάτων ανάλυσης πληροφορίας, σε τακτική βάση από τη Διεύθυνση Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης της Ελληνικής Αστυνομίας, για την ανίχνευση ύποπτων δραστηριοτήτων, που απειλούν τόσο τα συστήματα όσο και τα δεδομένα. Μάλιστα, η ανάλυση δύναται να οδηγήσει στην ανακάλυψη τυχόν κενών ασφαλείας, που μπορεί να οφείλονται για παράδειγμα σε ανεπαρκείς πολιτικές ασφαλείας ή κανόνες πρόσβασης, δίνοντας έτσι τη δυνατότητα να καλυφθούν μετέπειτα αυτά τα κενά. Φυσικά, θα πρέπει να καταγράφεται και κάθε

ενέργεια, που πραγματοποιείται στα φυσικά αρχεία της εκάστοτε Υπηρεσίας, στα οποία περιέχονται προσωπικά δεδομένα πολιτών. Ενδεικτικά, αυτό θα μπορούσε να πραγματοποιηθεί με την τήρηση βιβλίου εισόδου – εξόδου εγγράφων, όπου θα καταγράφεται η ημερομηνία εισόδου – εξόδου αυτών, τα στοιχεία του αστυνομικού, που χρεώνεται ή αποκτά πρόσβαση στο εκάστοτε έγγραφο και υπογραφή αυτού, κ.λπ..

7.2.5. Κυβερνασφάλεια

Η ασφάλεια των πληροφοριακών συστημάτων και των δικτύων γίνεται ολοένα και πιο σημαντική, πράγμα που αντανακλάται και από τις σημαντικές εξελίξεις που έχουν σημειωθεί από το έτος 2010 και έπειτα αναφορικά με τις νομοθετικές ρυθμίσεις και κανονιστικές παρεμβάσεις σχετικά με τον κυβερνοχώρο σε επίπεδο Ευρωπαϊκής Ένωσης. Η Οδηγία 2016/1148⁶³, η οδηγία NIS και NIS 2⁶⁴ και ο Κανονισμός 2019/881⁶⁵ αποτελούν μόνο ορισμένα παραδείγματα (Μήτρου, Λ., 2021: 74-75). Η υιοθέτηση και εφαρμογή ενός συνόλου μηχανισμών ασφαλείας στον κυβερνοχώρο, το οποίο αφενός επαρκεί για τη μείωση των κινδύνων σε αποδεκτό επίπεδο και αφετέρου δεν επιβαρύνει την αποδοτικότητα του συστήματος, ούτε προκαλεί αγανάκτηση στους χρήστες του, καθίσταται αναγκαία και απαραίτητη τόσο για την καταπολέμηση των διαρκώς εξελισσόμενων απειλών, όσο και για την βελτίωση και εξασφάλιση της μέγιστης δυνατής προστασίας των χρηστών των πληροφοριακών και επικοινωνιακών συστημάτων, αλλά και των δεδομένων που συλλέγονται και ανταλλάσσονται μέσω αυτών.

Σε αυτό το πλαίσιο, το Τμήμα Ασφάλειας Πληροφοριών και Προστασίας Δεδομένων της Διεύθυνσης Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης της Ελληνικής Αστυνομίας συντάσσει και επικαιροποιεί την Πολιτική Ασφάλειας Πληροφοριών και Πληροφοριακών Συστημάτων⁶⁶, σύμφωνα με τις τεχνολογικές εξελίξεις, τις υφιστάμενες ανάγκες της Ελληνικής Αστυνομίας, τη διαχείριση της επικινδυνότητας και τα αποτελέσματά της. Επιπλέον, οφείλει να ενημερώνει και να καθοδηγεί τους αστυνομικούς υπαλλήλους αναφορικά με την ορθή χρήση των συστημάτων και τη λήψη μέτρων ασφαλείας, ενώ παράλληλα ελέγχει τη συμμόρφωσή τους με την προαναφερόμενη πολιτική ασφαλείας (Άρθρο 37 του Ν. 5187/2025). Ασφαλώς, για να είναι αποτελεσματική και εφαρμόσιμη μία πολιτική ασφαλείας θα πρέπει να είναι εύκολα κατανοητή, πλήρης και να μην εξαρτάται αποκλειστικά από την υφιστάμενη τεχνολογία, ώστε να μην χρειάζεται συχνή αναθεώρηση (Κοκολάκης, Σ., 2021: 55). Επιπλέον, η Πολιτική Ασφάλειας

⁶³ Η Οδηγία 2016/1148 ρυθμίζει την ασφάλεια συστημάτων δικτύων και πληροφοριών στην Ε.Ε.

⁶⁴ Η Οδηγία NIS 2, που αναθεώρησε την Οδηγία NIS, θεσπίστηκε το 2022 και ρυθμίζει την προστασία κρίσιμων δικτύων και συστημάτων πληροφορικής από κυβερνοαπειλές (<https://cyber.gov.gr/odigia-nis2/>).

⁶⁵ Ο Κανονισμός 2019/881 αφορά τον Οργανισμό της Ε.Ε. για την Κυβερνοασφάλεια (ENISA) και την πιστοποίηση της κυβερνοασφάλειας στον τομέα των τεχνολογιών πληροφορικής και επικοινωνιών

⁶⁶ Ως πολιτική ασφαλείας πληροφοριών και πληροφοριακών συστημάτων νοείται το σύνολο των αρχών και κανόνων, που καθοδηγούν τις ληφθείσες αποφάσεις και την συμπεριφορά των χρηστών των πληροφοριακών συστημάτων και γενικά όσων εμπλέκονται στη λειτουργία αυτών (Κοκολάκης, Σ., 2021: 54)

Πληροφοριών και Πληροφοριακών Συστημάτων θα πρέπει να επικαιροποιείται κάθε φορά, που αυτό κρίνεται σκόπιμο.

Δεδομένου ότι οι χρήστες των πληροφοριακών συστημάτων συνιστούν κρίσιμο παράγοντα για την πρόληψη και αντιμετώπιση απειλών, με την συστηματική εκπαίδευση και ευαισθητοποίηση του αστυνομικού προσωπικού, ενισχύεται η ικανότητά τους να αναγνωρίζουν έγκαιρα τυχόν απειλές και κινδύνους, να εφαρμόζουν ορθές πρακτικές ασφάλειας και γενικά να συμβάλλουν στην προστασία των πληροφοριακών υποδομών και κατ' επέκταση των προσωπικών δεδομένων.

7.2.6. Αντίγραφα ασφαλείας (backups)

Η θωράκιση της ΕΛ.ΑΣ. έναντι του κινδύνου υποκλοπής, απώλειας ή καταστροφής των προσωπικών δεδομένων, που τηρεί στα αρχεία της, προϋποθέτει την τήρηση αντιγράφων ασφαλείας (backups). Με τα αντίγραφα ασφαλείας διασφαλίζεται η ανάκτηση των δεδομένων μετά από ένα κρίσιμο συμβάν, όπως για παράδειγμα μετά από κυβερνοεπίθεση και φυσική ή ανθρωπογενή καταστροφή, παρέχοντας παράλληλα στην ΕΛ.ΑΣ. τη δυνατότητα να συνεχίζει τη λειτουργία της, παρά τις προκληθείσες διαταράξεις (Κοκολάκης, Σ., 2021: 63).

Σύμφωνα με τον ENISA, τα αντίγραφα ασφαλείας θα πρέπει να δημιουργούνται και να διατηρούνται με ασφαλή τρόπο, βάσει μίας δομημένης στρατηγικής που καθορίζει τη συχνότητα δημιουργίας τους και τα μέσα με τα οποία αυτή πραγματοποιείται. Για την αποτελεσματικότερη προστασία των δεδομένων συνήθως απαιτείται η χρήση δύο διαφορετικών τύπων μέσων αποθήκευσης. Επιπλέον, η δημιουργία τους θα πρέπει να είναι αυτοματοποιημένη και να υποστηρίζεται η ανάκτηση προηγούμενων εκδόσεων αντιγράφων. Παράλληλα, η προστασία των αντιγράφων ασφαλείας απαιτεί την εφαρμογή ισχυρής κρυπτογράφησης και κατάλληλων μηχανισμών ελέγχου πρόσβασης, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και να κατοχυρώνεται η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των δεδομένων. Ωστόσο, προκειμένου να διασφαλίζεται η λειτουργικότητα και αξιοπιστία των αντιγράφων ασφαλείας, θα πρέπει να διενεργούνται τακτικοί έλεγχοι και δοκιμές ανάκτησης των δεδομένων (ENISA, 2025).

7.2.7. Κρυπτογραφία

Επειδή στα προσωπικά δεδομένα κάθε ατόμου μπορούν να έχουν πρόσβαση συγκεκριμένα πρόσωπα, για συγκεκριμένο σκοπό και για καθορισμένο χρονικό διάστημα, προκειμένου να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα αυτών είναι απαραίτητη η χρήση ισχυρών κρυπτογραφικών τεχνικών από την Ελληνική Αστυνομία. Ως κρυπτογραφία ορίζεται η διαδικασία κατά την οποία, με τη χρήση αλγορίθμων και κρυπτογραφικών κλειδιών, τα δεδομένα μετατρέπονται από αναγνώσιμη σε μη κατανοητή μορφή οπότε μπορεί να αποκτήσει πρόσβαση στο περιεχόμενό τους μόνο ο κάτοχος του αντίστοιχου κλειδιού αποκρυπτογράφησης (Ιγγλεζάκης, Ι, 2018: 148). Κρυπτογραφικές μέθοδοι θα πρέπει να χρησιμοποιούνται και κατά τη μεταφορά των δεδομένων σε έτερες αστυνομικές υπηρεσίες ή σε τρίτους, ανεξαρτήτως του μέσου μεταφοράς, όπως για παράδειγμα μέσω email, USB, CD, κ.λπ. (Κοκολάκης, Σ., 2021: 59, 61). Εξάλλου, όπως ορίζεται και στο άρθρο 32 του GDPR,

για την ασφαλή επεξεργασία των προσωπικών δεδομένων πρέπει να εφαρμόζεται, μεταξύ άλλων, η τεχνική της κρυπτογράφησης αυτών.

Υπάρχουν δύο είδη κρυπτογραφίας, η συμμετρική και η ασύμμετρη. Στην πρώτη περίπτωση, όλες οι οντότητες που συμμετέχουν στην επικοινωνία – διαβίβαση δεδομένων έχουν το ίδιο μυστικό κλειδί και μόνο αυτές μπορούν να ανακτήσουν τα δεδομένα από την κρυπτογραφημένη τους μορφή. Στη δεύτερη περίπτωση τα δεδομένα προστατεύονται με δημόσιο κλειδί και μόνο ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού μπορεί να ανακτήσει τα κρυπτογραφημένα δεδομένα (Κολοκοτρώνης, Ν., Λιμνιώτης, Κ. & Ριζομυλιώτης, Π., 2021: 235-236). Στην ασύμμετρη κρυπτογραφία εντάσσεται και η ψηφιακή υπογραφή (Κολοκοτρώνης, Ν., Λιμνιώτης, Κ. & Ριζομυλιώτης, Π., 2021: 260), με την οποία οι αστυνομικοί υπάλληλοι υπογράφουν έγγραφα, που έχουν συντάξει και αποστέλλουν σε εσωτερικές και εξωτερικές υπηρεσίες. Η επιλογή της εκάστοτε μεθόδου εξαρτάται από τα δεδομένα, που πρέπει να προστατευτούν κάθε φορά και τις ενέργειες, που πρόκειται να γίνουν επ' αυτών. Σε κάθε περίπτωση, η αποτελεσματικότητα της κρυπτογραφίας εξαρτάται από τα εργαλεία και τους αλγόριθμους (κρυπτογράφησης) που χρησιμοποιούνται (Κοκολάκης, Σ., 2021: 59), αλλά και από τον τρόπο που διαμορφώνονται οι αλγόριθμοι αυτοί, τα χαρακτηριστικά των κλειδιών που χρησιμοποιούνται και τον τρόπο διαχείρισης των κλειδιών.

7.2.8. Ψευδωνυμοποίηση & Ανωνυμοποίηση

Οι κίνδυνοι και οι προκλήσεις, που ανακύπτουν κατά την επεξεργασία των προσωπικών δεδομένων μπορούν να περιοριστούν και με δύο ακόμα τεχνικές, την ψευδωνυμοποίηση και ανωνυμοποίηση των δεδομένων (Ιγγλεζάκης, Ι., 2018: 147-149).

Ως ψευδωνυμοποίηση ορίζεται η επεξεργασία κατά την οποία τα προσωπικά δεδομένα αντικαθίστανται από κάποιο «ψευδώνυμο», ώστε να μην είναι δυνατή η άμεση ταυτοποίηση του υποκειμένου χωρίς τη χρήση περαιτέρω πληροφοριών, υπό την προϋπόθεση ότι οι τελευταίες διατηρούνται χωριστά και προστατεύονται με κατάλληλα μέτρα. Με αυτό τον τρόπο αποτρέπεται η απόδοσή τους στο συγκεκριμένο υποκείμενο, ενώ παράλληλα διατηρείται η δυνατότητα επανασύνδεσης με αυτό, όταν απαιτείται (Άρθρο 4 του GDPR). Εφόσον, λοιπόν, με την μέθοδο της ψευδωνυμοποίησης τα δεδομένα χάνουν τη σύνδεση με το υποκείμενο, δεν αποτελούν προσωπικά δεδομένα. Εάν, όμως αποδοθούν και πάλι στο φυσικό πρόσωπο, τότε συνιστούν ξανά προσωπικά δεδομένα, κάτι που μπορεί να συμβεί για παράδειγμα με την ύπαρξη πίνακα αντιστοίχισης του «ψευδώνυμου» στο υποκείμενο των δεδομένων (Ιγγλεζάκης, Ι., 2018: 148). Η μέθοδος της ψευδωνυμοποίησης ενδείκνυται κατά τη δοκιμή λογισμικών και εφαρμογών στα πληροφοριακά συστήματα της ΕΛ.ΑΣ..

Η τεχνική της ανωνυμοποίησης διαφέρει από την ψευδωνυμοποίηση και αφορά την διαδικασία κατά την οποία από ένα σύνολο δεδομένων τα στοιχεία ταυτοποίησης διαγράφονται οριστικά, ώστε να μην είναι δυνατή η συσχέτισή τους με το υποκείμενο των δεδομένων. Σε αντίθεση με την ψευδωνυμοποίηση, η ανωνυμοποίηση αποτελεί μία μη αναστρέψιμη διαδικασία μέσω της οποίας η σύνδεση των δεδομένων με το φυσικό πρόσωπο διακόπτεται οριστικά, παρέχοντας σημαντικές εγγυήσεις στην

προστασίας της ιδιωτικής ζωής των ατόμων. Δεδομένου ότι η ανωνυμοποίηση επιφέρει την οριστική και μη αναστρέψιμη αποσύνδεση των πληροφοριών από το υποκείμενο των δεδομένων – υπό την προϋπόθεση ότι χρησιμοποιούνται κατάλληλοι αλγόριθμοι και τεχνικές, προς αποφυγή επανασύνδεσης μέσω εξωτερικών πηγών - τα στοιχεία που προκύπτουν δεν συνιστούν πλέον προσωπικά δεδομένα (Ιγγλεζάκης, Ι., 2018: 148-149). Ενδεικτικά, η μέθοδος αυτή είναι ιδιαίτερα χρήσιμη στο πλαίσιο εκπαίδευσης του αστυνομικού προσωπικού με τη χρήση πραγματικών υποθέσεων, αλλά και για την έκδοση μηνιαίων ή/και ετησίων αναφορών για ερευνητικούς και στατιστικούς σκοπούς.

Συνοψίζοντας τα όσα παρατέθηκαν στις Ενότητες 7.1 και 7.2 προκύπτει ο ακόλουθος πίνακας:

Πίνακας 3: Προκλήσεις - Μέτρα αντιμετώπισης

<u>Προκλήσεις</u>	<u>Μέτρα αντιμετώπισης</u>
GDPR ή Οδηγία 2016/680;	Εκπαίδευση – Ενημέρωση
Ανθρώπινο δυναμικό	Εκπαίδευση – Ενημέρωση Έλεγχος πρόσβασης Καταγραφή ενεργειών Αντίγραφα ασφαλείας
Τεχνολογικοί Περιορισμοί	Έλεγχος Πρόσβασης Καταγραφή ενεργειών Κυβερνοασφάλεια Αντίγραφα ασφαλείας Κρυπτογραφία
Κυβερνοαπειλή – Κυβερνοεπίθεση	Έλεγχος Πρόσβασης Καταγραφή ενεργειών Κυβερνοασφάλεια Αντίγραφα ασφαλείας Κρυπτογραφία Ψευδωνυμοποίηση - Ανωνυμοποίηση
Περιβαλλοντικές απειλές	Αντίγραφα ασφαλείας

Ασφαλώς, μία κατάλληλη μεθοδολογία διαχείρισης επικινδυνότητας, θα πρέπει να εφαρμόζεται για την αντιμετώπιση οποιασδήποτε πρόκλησης.

7.3. Μελέτες περίπτωσης

Υστερα από την ανάλυση των προκλήσεων και των προτάσεων αντιμετώπισης αυτών, ιδιαίτερο ενδιαφέρον παρουσιάζουν δύο μελέτες περίπτωσης, στις οποίες διαπιστώθηκε παραβίαση των βασικών αρχών επεξεργασίας δεδομένων στο πλαίσιο λειτουργίας της ΕΛ.ΑΣ. και επιβλήθηκαν σχετικές κυρώσεις από την Α.Π.Δ.Π.Χ..

7.3.1. Παραβιάσεις κατά την έκδοση ταυτοτήτων

Με αφορμή καταγγελία, που υπέβαλε πολίτης ενώπιον της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σε βάρος του Υπουργείου Προστασίας του Πολίτη, λόγω του ότι στις 25/08/2023 ζήτησε να ενημερωθεί από το Υπουργείο αναφορικά με την έκδοση των νέων ταυτοτήτων και την νομιμότητα της επεξεργασίας των δεδομένων που συλλέγονται και παρ' ότι στις 19/09/2023 απέστειλε σχετική υπενθύμιση, δεν έλαβε τελικά απάντηση επί του αιτήματός του, η Α.Π.Δ.Π.Χ. εξέτασε αυτεπαγγέλτως την ως άνω υπόθεση. Συγκεκριμένα, κάλεσε το Υπουργείο Προστασίας του Πολίτη, στο οποίο υπάγεται η Ελληνική Αστυνομία, σε συνεδρίαση στις 05/12/2023 προς ακρόαση, στην οποία παρευρέθηκαν ο Τμηματάρχης του Τμήματος Ταυτοτήτων και Αρχείων, ο Προϊστάμενος του Γραφείου Ταυτοτήτων / Τμήμα Ταυτοτήτων και Αρχείων και ο Υπεύθυνος Προστασίας Δεδομένων της Ελληνικής Αστυνομίας. Άπαντες εξέφρασαν προφορικά τις απόψεις τους και εν συνεχεία δόθηκε προθεσμία στους ανωτέρω προκειμένου να υποβάλλουν σχετικά έγγραφα υπομνήματα προς υποστήριξη των ισχυρισμών τους (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Με την παρέλευση της χορηγηθείσας προθεσμίας, η Α.Π.Δ.Π.Χ. αφού μελέτησε τα έγγραφα υπομνήματα διαπίστωσε ότι η Ελληνική Αστυνομία δεν είχε συμμορφωθεί πλήρως με τον GDPR στο πλαίσιο έκδοσης δελτίου ταυτότητας των πολιτών (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.). Πιο συγκεκριμένα, εντόπισε καθυστέρηση και ελλείψεις στην προβλεπόμενη εκ του Νόμου εκτίμηση αντικτύπου αναφορικά με την προστασία των δεδομένων, κατά παράβαση του άρθρου 35 του GDPR, αλλά και πλημμέλειες στην ενημέρωση των πολιτών σχετικά με την επεξεργασία των δεδομένων τους κατά την έκδοση δελτίου ταυτότητας, κατά παράβαση των άρθρων 13 και 14 του GDPR (sakkoulasonline, 2024)⁶⁷.

Ειδικότερα, η Α.Π.Δ.Π.Χ. διαπίστωσε ότι η Ελληνική Αστυνομία δεν είχε πραγματοποιήσει εγκαίρως εκτίμηση αντικτύπου της επεξεργασίας στα δεδομένα των υποκειμένων πριν την έναρξη έκδοσης δελτίων ταυτότητας, ως όφειλε, σύμφωνα με το άρθρο 35 παρ. 1 του GDPR, αλλά αφού είχε ξεκινήσει η διαδικασία έκδοσης και αυτό κατόπιν επικοινωνίας με την Α.Π.Δ.Π.Χ. (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Επιπλέον, η Ελληνική Αστυνομία, αν και υποστήριξε ότι είχε εκδώσει και δημοσιεύσει σχετική ενημέρωση στην επίσημη ιστοσελίδα της, την οποία έχει αποστείλει και στις αστυνομικές Υπηρεσίες, ώστε να αναρτηθεί σε εμφανές σημείο για την ενημέρωση των πολιτών, η Α.Π.Δ.Π.Χ., κατόπιν έρευνας, διαπίστωσε ότι η ενημέρωση δεν είχε αναρτηθεί στην ιστοσελίδα της μέχρι τα τέλη Φεβρουαρίου του

⁶⁷ <https://www.sakkoulas-online.gr/news/apdpch-32-2024-prostimo-tis-apdpch-sto-ypourgeio-prostasias-tou-politi-os-ypavthyno-epexergasias-anaforika-me-tin-ekdosi-neou-typou-tavtotitas>

έτους 2024, ενώ η διαδικασία έκδοσης δελτίων ταυτότητας είχε ξεκινήσει ήδη από τον Σεπτέμβριο του έτους 2023. Μάλιστα, η Αρχή παρατήρησε ότι στην αναρτηθείσα ενημέρωση η ΕΛ.ΑΣ. αναφερόταν σε εσφαλμένες διατάξεις και υπήρχαν νομικές ασάφειες. Συγκεκριμένα, για την επεξεργασία των βιομετρικών δεδομένων γινόταν λόγος για «πρόδηλη ενεργή συγκατάθεση» του υποκειμένου, η οποία αποτελεί εσφαλμένη νομική βάση για την συγκεκριμένη επεξεργασία, δεδομένου ότι η έκδοση δελτίου ταυτότητας πραγματοποιείται κατά την άσκηση δημόσιας εξουσίας κατ' εφαρμογή του άρθρου 6 παρ. 1 του GDPR. Προκειμένου η συγκατάθεση να αποτελεί έγκυρη νομική βάση πρέπει να παρέχεται ελεύθερα, όπως ορίζει το άρθρο 4 του GDPR. Συνεπώς, δεν μπορεί να γίνεται λόγος για ελεύθερη συγκατάθεση όταν το υποκείμενο δεν έχει ελεύθερη επιλογή ως προς την επεξεργασία των δεδομένων του. Επιπλέον, η Α.Π.Δ.Π.Χ. διαπίστωσε ότι στην ενημέρωση της Ελληνικής Αστυνομίας γινόταν αναφορά στο άρθρο 46 του Ν. 4624/2019 για την επεξεργασία των δεδομένων ειδικών κατηγοριών. Ωστόσο, το συγκεκριμένο άρθρο αφορά την επεξεργασία των δεδομένων από κάθε δημόσια αρχή, όπως η Ελληνική Αστυνομία, στο πλαίσιο πρόληψης, ανίχνευσης, διερεύνησης ή ποινικής δίωξης εγκλημάτων, όπως ορίζει το άρθρο 43 του Ν. 4624/2019. Επομένως, στην προκειμένη περίπτωση δεν μπορεί να εφαρμοστεί το συγκεκριμένο άρθρο, αλλά το άρθρο 9 του GDPR (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Τέλος, στο ενσωματωμένο ηλεκτρονικό μέσο αποθήκευσης στο δελτίο ταυτότητας, εκτός από τη φωτογραφία και τα δύο δακτυλικά αποτυπώματα του κατόχου καταχωρίζονταν και επιπλέον στοιχεία και συγκεκριμένα το επώνυμο των γονέων του, ο Δήμος εγγραφής, ο αριθμός δημοτολογίου και ο τόπος έκδοσης της ταυτότητας. Τα δεδομένα αυτά, ωστόσο, δεν περιλαμβάνονται μεταξύ των υποχρεωτικών που προβλέπει το άρθρο 3 παρ. 5 του Κανονισμού (ΕΕ) 2019/1157 και η Ελληνική Αστυνομία στα υπομνήματά της δεν τεκμηρίωσε επαρκώς τους σκοπούς της επεξεργασίας τους και την ανάγκη συμπερίληψής τους στο δελτίο ταυτότητας (Γκατζούφας, Α., 2024: 671).

Συνοψίζοντας, η Α.Π.Δ.Π.Χ. διαπίστωσε ότι η Ελληνική Αστυνομία παραβίασε το άρθρο 35 παρ.1 του GDPR, αναφορικά με την διενέργεια εκτίμησης αντικτύπου, τα άρθρα 13 και 14 του GDPR αναφορικά με την ενημέρωση των υποκειμένων για την επεξεργασία των δεδομένων τους και το άρθρο 24 του GDPR, καθώς δεν τήρησε την αρχή της ελαχιστοποίησης των δεδομένων, αφού δεν αιτιολόγησε επαρκώς την ανάγκη καταχώρησης ορισμένων στοιχείων στο ηλεκτρονικό μέσο αποθήκευσης, που είναι ενσωματωμένο στα δελτία ταυτότητας (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Η Α.Π.Δ.Π.Χ. κατ' εφαρμογή των διατάξεων του άρθρου 83 παρ.2 περ.θ' του GDPR και του άρθρου 39 παρ. 1 του Ν.4624/2019 και αφού έλαβε υπόψη ότι:

- οι προαναφερόμενες παραβάσεις αφορούν την υποχρέωση του υπεύθυνου επεξεργασίας να λογοδοτεί για τις ενέργειες, στις οποίες προβαίνει κατά την επεξεργασία προσωπικών δεδομένων, αλλά και τα δικαιώματα των υποκειμένων που κατοχυρώνει ο GDPR,

- η επεξεργασία των δεδομένων εντάσσεται στις βασικές δραστηριότητες της Ελληνικής Αστυνομίας και ειδικότερα στην έκδοση δελτίου ταυτότητας,
- επηρεάζεται μεγάλος αριθμός φυσικών προσώπων και συγκεκριμένα οι Έλληνες πολίτες, που έχουν υποχρέωση να εκδώσουν δελτίο ταυτότητας,
- ο επιδιωκόμενος σκοπός της επεξεργασίας είναι θεμιτός και δεν προκύπτουν άμεσες και σοβαρές επιπτώσεις στα υποκείμενα των δεδομένων από αυτή,
- η Ελληνική Αστυνομία πραγματοποίησε εκτίμηση αντικτύπου της επεξεργασίας και ενημέρωση των πολιτών, κατόπιν παρέμβασης της Α.Π.Δ.Π.Χ., ωστόσο με σημαντικές παραλείψεις και καθυστερήσεις,

επέβαλε στο Υπουργείο Προστασίας του Πολίτη πρόστιμο ύψους 50.000 ευρώ για την παράβαση των άρθρων 13 και 14 του GDPR σχετικά με την ενημέρωση των πολιτών και πρόστιμο ύψους 100.000 ευρώ για την παράβαση του άρθρου 35 παρ.1 του GDPR αναφορικά με την εκτίμηση αντικτύπου (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Τέλος, η Α.Π.Δ.Π.Χ. διέταξε το Υπουργείο Προστασίας του Πολίτη κατ' εφαρμογή του άρθρου 58 παρ. 2 του GDPR, όπως επικαιροποιήσει την εκτίμηση αντικτύπου, που πραγματοποίησε και αιτιολογήσει την καταχώρηση στο ενσωματωμένο ηλεκτρονικό μέσο αποθήκευσης επιπρόσθετων στοιχείων από αυτά που προβλέπει ο Κανονισμός (ΕΕ) 2019/1157. Επιπλέον, έδωσε εντολή στο Υπουργείο να προβεί σε όλες τις απαραίτητες ενέργειες, που αφορούν την επεξεργασία των δεδομένων κατά την έκδοση των δελτίων ταυτότητας, ενημερώνοντάς την σχετικά (Απόφαση 32/2024 της Α.Π.Δ.Π.Χ.).

Βάσει των όσων αναφέρονται στην υπ' αριθ. 32/2024 Απόφαση της Α.Π.Δ.Π.Χ., τα «λάθη», που έγιναν και οδήγησαν στην επιβολή προστίμου στο Υπουργείο Προστασίας του Πολίτη, ενδεχομένως να οφείλονται στο γεγονός, ότι εκείνη την χρονική περίοδο βρισκόντουσαν σε εξέλιξη πολυάριθμες υπηρεσιακές ενέργειες με σκοπό την έγκαιρη έναρξη της διαδικασίας έκδοσης των νέων τύπου δελτίων ταυτότητας, στο πλαίσιο εκπλήρωσης των ευρωπαϊκών και διεθνών υποχρεώσεων της χώρας. Έτσι, η επιτακτική ανάγκη άμεσης ενεργοποίησης της διαδικασίας έκδοσης ταυτοτήτων, σε συνδυασμό με το ότι το νέο νομικό πλαίσιο περί έκδοσης νέου τύπου Α.Δ.Τ. πιθανόν δεν είχε αφομοιωθεί πλήρως, σε επίπεδο εφαρμογής, οδήγησε στα «σφάλματα», που αναλύθηκαν παραπάνω.

Προκειμένου να αποφευχθούν ανάλογες πλημμέλειες στο μέλλον, κρίνεται απαραίτητη η έγκαιρη εκπαίδευση και ενημέρωση του αστυνομικού προσωπικού επί των νέων – αναθεωρημένων υπηρεσιακών διαδικασιών και των κανονιστικών διατάξεων, που τις προβλέπουν. Στο πλαίσιο της εκπαίδευσης αυτής, θα πρέπει να περιλαμβάνονται σαφείς ερμηνευτικές οδηγίες, που θα εκμηδενίζουν ενδεχόμενες ασάφειες, κατά την εφαρμογή των νομικών κειμένων στην πράξη. Επιπλέον, είναι αναγκαία η πρόβλεψη ενός εύλογου μεταβατικού σταδίου, το οποίο θα παρέχει στα στελέχη της ΕΛ.ΑΣ. επαρκή χρόνο για την αφομοίωση των νέων δεδομένων, διασφαλίζοντας έτσι την ορθή και εμπρόθεσμη εκτέλεση των απαιτούμενων ενεργειών.

7.3.2. Κυβερνοεπίθεση «EMOTET»

Το έτος 2020 ένας πολίτης απέστειλε στην Ελληνική Αστυνομία μήνυμα μέσω ηλεκτρονικού ταχυδρομείου, το οποίο περιείχε, μεταξύ άλλων, προσωπικά του δεδομένα. Συγκεκριμένα, εκτός από τη διεύθυνση ηλεκτρονικού του ταχυδρομείου, συμπεριλαμβάνονταν το ονοματεπώνυμό του και ο κωδικός του για την υπηρεσία Passenger Locator Form⁶⁸.

Κατόπιν τούτου και ενώ δεν είχε λάβει κάποια απάντηση από την Ελληνική Αστυνομία, έλαβε τέσσερα μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία εμφανίζονταν ψευδώς ότι προέρχονται από την ΕΛ.ΑΣ. Τα εν λόγω μηνύματα είτε περιείχαν κακόβουλο λογισμικό είτε συνδέσμους, που οδηγούσαν σε κακόβουλο λογισμικό. Σύμφωνα με τον καταγγέλλοντα, οι διευθύνσεις IP από τις οποίες φέρεται να απεστάλησαν τα επίμαχα μηνύματα αντιστοιχούσαν σε χώρες εκτός Ελλάδας. Μάλιστα, από το περιεχόμενο των μηνυμάτων συνάγεται το συμπέρασμα ότι το αρχικό μήνυμα, που είχε αποστείλει ο πολίτης στην Ελληνική Αστυνομία είχε διαρρεύσει σε άγνωστα τρίτα πρόσωπα.

Αφού επικοινωνήσει τηλεφωνικά ο καταγγέλλων με την Ελληνική Αστυνομία, ενημερώθηκε για την ύπαρξη προβλήματος ασφάλειας στο ηλεκτρονικό της ταχυδρομείο. Στην συνέχεια, η Ελληνική Αστυνομία ενημέρωσε και εγγράφως τον καταγγέλλοντα, διαβιβάζοντας την απάντησή της στην Α.Π.Δ.Π.Χ., ότι τις ημερομηνίες που έλαβε τα επίμαχα μηνύματα μέσω ηλεκτρονικού ταχυδρομείου βρισκόταν εν εξελίξει κυβερνοεπίθεση σε παγκόσμιο επίπεδο ονόματι «EMOTET» και ότι αυτά απεστάλησαν από λογαριασμούς, που δεν έχουν καμία σχέση με την Ελληνική Αστυνομία.

Σύμφωνα με την από 27/01/2021 ανακοίνωση της Europol, η κυβερνοεπίθεση «EMOTET» αφορά κακόβουλο λογισμικό, το οποίο διαδίδεται μέσω μηνυμάτων ηλεκτρονικής αλληλογραφίας. Πιο συγκεκριμένα, τα μηνύματα περιείχαν επισυναπτόμενα αρχεία σε μορφή Word με ψευδές – παραπλανητικό περιεχόμενο, όπως υποτιθέμενα αποδεικτικά πληρωμής ή ενημερώσεις για τον COVID-19. Όταν ο παραλήπτης του μηνύματος «άνοιγε» το αρχείο, του ζητούταν να ενεργοποιήσει ορισμένες μακροεντολές, επιτρέποντας με αυτό τον τρόπο την εγκατάσταση του κακόβουλου λογισμικού στο σύστημά του.

Η Α.Π.Δ.Π.Χ. ζήτησε από την Ελληνική Αστυνομία να περιγράψει επακριβώς τις ενέργειες, στις οποίες προέβη για να κατοχυρώσει την ασφάλεια των συστημάτων της. Όπως γνωστοποίησε η Ελληνική Αστυνομία στην Α.Π.Δ.Π.Χ., στελέχη της Διεύθυνσης Πληροφορικής σε συνεργασία με εξωτερικούς υπαλλήλους τεχνικής υποστήριξης των συστημάτων της ΕΛ.ΑΣ. διερεύνουν την πιθανότητα παράνομης διείσδυσης ή μόλυνσης των εξυπηρετητών της, με αρνητικό αποτέλεσμα.

⁶⁸ Πρόκειται για μία ηλεκτρονική φόρμα, στην οποία οι ταξιδιώτες συμπλήρωναν υποχρεωτικά τα στοιχεία επικοινωνίας και διαμονής τους πριν την άφιξή τους σε μία χώρα. Από το 2022 έχει καταργηθεί η υποχρέωση συμπλήρωσης αυτής της φόρμας.

Επιπλέον, με σκοπό τον περιορισμό της διάδοσης του κακόβουλου λογισμικού «EMOTET», έλαβε ένα σύνολο οργανωτικών και τεχνικών μέτρων. Συγκεκριμένα, ενισχύθηκαν οι μηχανισμοί ελέγχου ηλεκτρονικής αλληλογραφίας, με την εφαρμογή ισχυρότερων φίλτρων για περιπτώσεις κακόβουλου ή ανεπιθύμητου περιεχομένου, αποκλείστηκαν κάποιοι αποστολείς, προστέθηκαν φίλτρα με συγκεκριμένες λέξεις – κλειδιά και εγκαταστάθηκαν οι πιο πρόσφατες ενημερώσεις λογισμικού. Οι μηχανισμοί ελέγχου ηλεκτρονικής αλληλογραφίας ενισχύθηκαν και στους εξυπηρετητές του ηλεκτρονικού ταχυδρομείου της ΕΛ.ΑΣ., εφαρμόζοντας ισχυρότερα φίλτρα για κακόβουλο ή ανεπιθύμητο περιεχόμενο, παρ' ότι παράγουν αρκετά ψευδώς θετικά αποτελέσματα.

Στο πλαίσιο ενίσχυσης των σταθμών εργασίας (όπως για παράδειγμα οι επιτραπέζιοι υπολογιστές) πραγματοποιήθηκε πλήρης επαναφορά των συστημάτων (format) σε τέσσερις περιπτώσεις που εντοπίστηκαν μολύνσεις, οι οποίες συνέβαλαν στην επιτυχή εκδήλωση της κυβερνοεπίθεσης, έγιναν αναβαθμίσεις του MS Outlook, όπου ήταν αναγκαίο και ελέγχθηκε συνολικά η κατάσταση του αντιβιοτικού λογισμικού. Επιπροσθέτως, εξετάστηκε το σύνολο των σταθμών εργασίας για τον εντοπισμό μηνυμάτων με ύποπτο περιεχόμενο, επανακαθορίστηκαν οι κωδικοί πρόσβασης των χρηστών και προωθήθηκε η χρήση webmail αντί του MS Outlook.

Προκειμένου η Ελληνική Αστυνομία να ενημερώσει το προσωπικό της για την κυβερνοεπίθεση και τους τρόπους αντιμετώπισης αυτής, συνέταξε έγγραφο, το οποίο διαβιβάστηκε στις Υπηρεσίες της. Επιπλέον, ενημέρωσε σχετικά το εθνικό CERT⁶⁹, τη Διεύθυνση Δίωξης Κυβερνοεγκλήματος (πρώην Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος), την Α.Π.Δ.Π.Χ. και έτερους οργανισμούς.

Η συγκεκριμένη περίπτωση αφορά περιστατικό παραβίασης προσωπικών δεδομένων, όπως αυτό ορίζεται στο άρθρο 4 του GDPR. Όπως διαπίστωσε η Α.Π.Δ.Π.Χ., η Ελληνική Αστυνομία δεν την ενημέρωσε άμεσα, ως όφειλε βάσει του άρθρου 33 του GDPR, παρ' ότι υπήρχαν ουσιαστικοί και υψηλοί κίνδυνοι για τα υποκείμενα των δεδομένων. Η Α.Π.Δ.Π.Χ. ενημερώθηκε για πρώτη φορά για το συμβάν από την ΕΛ.ΑΣ. μέσω της διαβίβασης της απάντησης της τελευταίας προς τον καταγγέλλοντα, η οποία ήταν ελλιπής, καθώς δεν περιείχε πλήρεις πληροφορίες. Συγκεκριμένα, η απάντηση περιοριζόταν στο ότι τα επίμαχα μηνύματα δεν προέρχονταν από την Ελληνική Αστυνομία, χωρίς να αποσαφηνίζεται ότι έλαβε χώρα περιστατικό ασφαλείας που την αφορούσε και το οποίο είχε ως επακόλουθο την παραβίαση των προσωπικών του δεδομένων. Επιπλέον, δεν ενημέρωσε τα θιγόμενα πρόσωπα, σύμφωνα με το άρθρο 34 του GDPR, ούτε εξέδωσε δημόσια ανακοίνωση για το περιστατικό.

⁶⁹ Το Εθνικό CERT (Computer Emergency Response Team) είναι η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων της Ελλάδας, η οποία είναι αρμόδια για την υποστήριξη φορέων της Κεντρικής Κυβέρνησης σχετικά με την πρόληψη, προειδοποίηση και αντιμετώπιση κυβερνοεπιθέσεων, ενώ παράλληλα συντονίζει την ανταλλαγή πληροφοριών για τέτοια περιστατικά (<https://www.nis.gr/downloads/national-cert/RFC2350-GR.pdf>).

Εκτός των ανωτέρω, παρ' ότι η Ελληνική Αστυνομία φέρεται να προέβη σε ενέργειες για τη διαχείριση και διερεύνηση του περιστατικού, η Α.Π.Δ.Π.Χ. διαπίστωσε ότι δεν εξετάστηκε σε βάθος το συμβάν. Ειδικότερα, από τα έγγραφα της Ελληνικής Αστυνομίας προς την Α.Π.Δ.Π.Χ. δεν προκύπτει ότι διερευνήθηκε το πλήθος των θιγόμενων προσώπων, ούτε το είδος των δεδομένων που παραβιάστηκαν, με αποτέλεσμα να μην πραγματοποιείται η απαιτούμενη αξιολόγηση συνεπειών που προβλέπουν τα άρθρα 33 και 34 του GDPR. Επιπλέον, δεν διευκρινίζεται εάν τα ληφθέντα μέτρα υιοθετήθηκαν κατόπιν ειδικής και τεκμηριωμένης αξιολόγησης των κινδύνων, που συνδέονται με την συγκεκριμένη περίπτωση, καθώς δεν παρατέθηκε αναλυτική αιτιολόγηση ως προς την πληρότητα και καταλληλότητά τους.

Τέλος, όπως προέκυψε από τα συλλεχθέντα στοιχεία και πληροφορίες ορισμένα συστήματα και λογισμικά προστασίας της Ελληνικής Αστυνομίας δεν είχαν επικαιροποιηθεί, γεγονός που υποδηλώνει ανεπαρκή διαδικασία τακτικού ελέγχου και επικαιροποίησης των μέτρων ασφαλείας, ανεξαρτήτως εάν αυτή η παράλειψη συνέβαλε άμεσα ή έμμεσα στο περιστατικό.

Η Α.Π.Δ.Π.Χ. λαμβάνοντας, λοιπόν, υπόψη όλα τα ανωτέρω, παρατήρησε ότι η Ελληνική Αστυνομία παραβίασε τα άρθρα 32, 33 και 34 του GDPR σχετικά με την ασφάλεια της επεξεργασίας και τη γνωστοποίηση περιστατικών παραβίασης, καθώς και το άρθρο 15 του GDPR, όσον αφορά την πλημμελή ανταπόκριση στο δικαίωμα πρόσβασης στα δεδομένα. Σε συνδυασμό με την φύση και έκταση της κυβερνοεπίθεσης «EMOTET» και τις ενέργειες, στις οποίες προέβη η Ελληνική Αστυνομία για την αντιμετώπιση του περιστατικού και την αποτροπή παρόμοιων μελλοντικών συμβάντων, η Α.Π.Δ.Π.Χ. κατ' εφαρμογή του άρθρου 58 παρ. 2 περ. β' του GDPR, απηύθυνε στην Ελληνική Αστυνομία επίπληξη (Απόφαση 43/2021 της Α.Π.Δ.Π.Χ.).

Η ανάλυση του συγκεκριμένου περιστατικού αναδεικνύει την κυβερνοεπίθεση ως μία εξαιρετικά κρίσιμη πρόκληση που καλείται να αντιμετωπίσει η ΕΛ.ΑΣ. κατά την επεξεργασία προσωπικών δεδομένων, στο πλαίσιο της λειτουργίας της. Ο εντοπισμός τεσσάρων μολύνσεων σε σταθμούς εργασίας της ΕΛ.ΑΣ., οι οποίες δημιούργησαν πρόσφορο έδαφος στην επιτυχή εξέλιξη της επίθεσης, υποδηλώνει την μη έγκαιρη αναγνώριση των απειλών από το αστυνομικό προσωπικό. Παράλληλα, η διαπίστωση ύπαρξης μη επικαιροποιημένων συστημάτων και λογισμικών προστασίας αναδεικνύει σημαντικούς τεχνολογικούς περιορισμούς, οι οποίοι συνιστούν συστημική ευπάθεια, ανεξαρτήτως του βαθμού επίδρασής τους στο συμβάν.

Η αποτροπή παρόμοιων περιστατικών στο μέλλον προϋποθέτει μία ολιστική προσέγγιση, η οποία θα εστιάζει στην εκπαίδευση και ενημέρωση του αστυνομικού προσωπικού, ώστε να αναγνωρίζει άμεσα απειλές και επιθέσεις (π.χ. ύποπτα συνημμένα αρχεία) και να ακολουθεί τα πρωτόκολλα γνωστοποίησης παραβιάσεων. Επιπλέον, η θωράκιση της ΕΛ.ΑΣ. απαιτεί την υιοθέτηση προηγμένων εργαλείων κυβερνοασφάλειας, αποτελούμενα από ισχυρά αντιβιοτικά λογισμικά και επικαιροποιημένα λειτουργικά συστήματα, ικανών να αποκρούσουν εξελεγμένες απειλές, τα οποία θα ελέγχονται σε τακτική βάση. Καθοριστικής σημασίας είναι και η εφαρμογή κατάλληλων κρυπτογραφικών τεχνικών, τόσο κατά τη διαβίβαση όσο και

την αποθήκευση προσωπικών δεδομένων, ώστε να εξασφαλίζεται ότι ακόμα και σε περίπτωση διαρροής τους, δεν θα είναι αξιοποιήσιμα από τους κακόβουλους δράστες. Σε κάθε περίπτωση, πάντως, για την ανθεκτικότητα και προστασία των αγαθών της ΕΛ.ΑΣ. είναι απαραίτητη η εφαρμογή κατάλληλης μεθοδολογίας διαχείρισης επικινδυνότητας, με την οποία θα εντοπίζονται, αξιολογούνται και ιεραρχούνται οι απειλές περιοδικά, ώστε να προσαρμόζονται, στην συνέχεια, οι αμυντικές της στρατηγικές στις διαρκώς μεταβαλλόμενες κυβερνοαπειλές. Στο πλαίσιο των στρατηγικών αυτών, είναι απαραίτητη και η εφαρμογή μίας πολύ-επίπεδης αρχιτεκτονικής ασφαλείας που να ενσωματώνει στο κατάλληλο σημείο τον κάθε μηχανισμό και μέτρο ασφαλείας που περιλαμβάνεται στο Σχέδιο Επιχειρησιακής Συνέχειας έτσι ώστε όχι μόνο να μειώνονται οι απειλές/κίνδυνοι αλλά και να ελαχιστοποιείται ο αντίκτυπός τους εφόσον αυτές/αυτοί πραγματοποιηθούν.

7.4. Συμπεράσματα

Από την ανάλυση του τρέχοντος κεφαλαίου, προκύπτει ότι η επεξεργασία και προστασία των προσωπικών δεδομένων, στο πλαίσιο λειτουργίας της Ελληνικής Αστυνομίας δεν αποτελεί μια εύκολη διαδικασία, καθώς μπορούν να ανακύψουν διάφορες προκλήσεις. Το δίλημμα μεταξύ GDPR ή Οδηγίας 2016/680, το ανθρώπινο δυναμικό, οι τεχνολογικοί περιορισμοί, οι κυβερνοαπειλές & κυβερνοεπιθέσεις, καθώς και οι περιβαλλοντικές απειλές, καθιστούν τη διαδικασία της επεξεργασίας ιδιαίτερα σύνθετη και τα προσωπικά δεδομένα (διαρκώς) εκτεθειμένα σε κινδύνους.

Οι κυβερνοεπιθέσεις και οι σύγχρονες τεχνολογικές εξελίξεις αναδεικνύουν τον αναγκαίο χαρακτήρα της ενίσχυσης της κυβερνοασφάλειας και της προστασίας των πληροφοριακών συστημάτων της Ελληνικής Αστυνομίας. Παράλληλα, ο ανθρώπινος παράγοντας αποτελεί κρίσιμο ζήτημα, καθώς η μη ορθή εφαρμογή των διατάξεων των νομικών κειμένων, η κακόβουλη διάθεση ή η ανεπαρκής εκπαίδευση, μπορεί να οδηγήσει σε παραβιάσεις των προσωπικών δεδομένων, ακόμα και αν υπάρχουν τα κατάλληλα τεχνικά μέτρα προστασίας αυτών. Επιπλέον, οι περιβαλλοντικές απειλές, που μπορεί να οφείλονται σε φυσικές ή ανθρωπογενείς καταστροφές, δύναται να επιφέρουν επιβλαβείς επιπτώσεις στις υποδομές, στα συστήματα και κατ' επέκταση στα προσωπικά δεδομένα, που χειρίζονται οι αστυνομικές Υπηρεσίες.

Οι τρόποι αντιμετώπισης που προτάθηκαν, όπως η εφαρμογή κατάλληλης μεθοδολογίας διαχείρισης επικινδυνότητας, η συνεχής εκπαίδευση και ενημέρωση του προσωπικού, η διενέργεια ελέγχων πρόσβασης στους φυσικούς και ψηφιακούς πόρους της ΕΛ.ΑΣ., η συστηματική καταγραφή των ενεργειών που λαμβάνουν χώρα, η ενίσχυση της κυβερνοασφάλειας, η διατήρηση αντιγράφων ασφαλείας, η κρυπτογραφία, ψευδωνυμοποίηση και ανωνυμοποίηση των δεδομένων αποτελούν τους βασικούς πυλώνες για τη διασφάλιση της προστασίας των προσωπικών δεδομένων κατά την επεξεργασία τους από την ΕΛ.ΑΣ..

Μάλιστα, οι μελέτες περίπτωσης, που εξετάστηκαν και αφορούν Αποφάσεις της Α.Π.Δ.Π.Χ σχετικά με διαπιστωθείσες παραβάσεις από την ΕΛ.ΑΣ. κατά την έκδοση δελτίων ταυτότητας και την κυβερνοεπίθεση «EMOTET», απέδειξαν ότι οι

προαναφερόμενες προκλήσεις δύναται να επηρεάσουν ουσιωδώς την προστασία των προσωπικών δεδομένων, αναδεικνύοντας παράλληλα τη σπουδαιότητα των μέτρων αντιμετώπισής τους.

8. Συμπεράσματα

Η προστασία των προσωπικών δεδομένων δεν αποτελεί μόνο νομική υποχρέωση, που απορρέει από τον GDPR, τον Ν. 4624/2019 που έχει ενσωματώσει την Οδηγία 2016/680, τον Ν. 5002/2022 και εν γένει τα νομικά κείμενα, αλλά μία ουσιώδη εγγύηση του κράτους δικαίου και θεμελιώδες δικαίωμα κάθε φυσικού προσώπου, που κατοχυρώνεται συνταγματικά στο άρθρο 9^Α του Συντάγματος της Ελλάδος.

Η ανάλυση που πραγματοποιήθηκε κατέδειξε ότι το υφιστάμενο νομικό πλαίσιο προστασίας δεδομένων διαμορφώνει ένα αρκετά απαιτητικό και αυστηρό σύνολο κανόνων σχετικά με την επεξεργασία των δεδομένων από την ΕΛ.ΑΣ. Η επεξεργασία, που αφορά την πρόληψη, καταστολή και διερεύνηση αξιόποινων πράξεων από αρμόδιες αρχές επιβολής του νόμου, ρυθμίζεται από την Οδηγία 2016/680, όπως ενσωματώθηκε στο εθνικό μας δίκαιο, η οποία καθορίζει ειδικές εγγυήσεις και περιορισμούς, διαφοροποιημένους από αυτούς του GDPR, ο οποίος εφαρμόζεται σε όλες τις υπόλοιπες περιπτώσεις.

Κατά την επεξεργασία προσωπικών δεδομένων από την Ελληνική Αστυνομία καθοριστικός είναι ο ρόλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ως εποπτικού μηχανισμού της ορθής εφαρμογής της ισχύουσας νομοθεσίας, καθώς και του Υπεύθυνου Προστασίας Δεδομένων της ΕΛ.ΑΣ, ο οποίος λειτουργεί, μεταξύ άλλων, ως σύνδεσμος μεταξύ των αστυνομικών Υπηρεσιών και της Α.Π.Δ.Π.Χ..

Η ανάλυση DNA, η άρση του απορρήτου των επικοινωνιών, η δημοσιοποίηση στοιχείων κατηγορουμένων και καταδικασθέντων, η έκδοση ταυτοτήτων και διαβατηρίων, η επιτήρηση δημόσιων χώρων, η συμμετοχή υποψηφίων ιδιωτών στο διαγωνισμό εισαγωγής στις Σχολές της Ελληνικής Αστυνομίας και η διασυννοριακή συνεργασία μεταξύ των αρμόδιων αρχών των κρατών μελών, αποτελούν μόνο ορισμένες, αλλά ουσιαστικές περιπτώσεις, οι οποίες καταδεικνύουν την έκταση και την ευαισθησία των δεδομένων, που συλλέγει και επεξεργάζεται η Ελληνική Αστυνομία σε καθημερινή βάση, στο πλαίσιο της λειτουργίας της. Η επεξεργασία αυτή αφορά τόσο απλά όσο και ευαίσθητα δεδομένα και εγκυμονεί αυξημένους κινδύνους για τα δικαιώματα των υποκειμένων, καθιστώντας επιβεβλημένη την αυστηρή τήρηση των βασικών αρχών επεξεργασίας δεδομένων, που ορίζουν τα νομικά κείμενα. Αν και η τήρηση των διατάξεων του ευρωπαϊκού και εθνικού δικαίου δεν αποτελεί ένα στατικό αποτέλεσμα, αλλά μία διαρκή διαδικασία, από την εξέταση των επιμέρους περιπτώσεων επεξεργασίας δεδομένων, προκύπτει ότι η ΕΛ.ΑΣ. κατά την άσκηση των καθηκόντων της μεριμνά για την προστασία των προσωπικών δεδομένων.

Οι προκλήσεις, που εντοπίστηκαν και αναλύθηκαν, και συγκεκριμένα το δίλημμα επιλογής του GDPR ή της Οδηγίας 2016/680, το ανθρώπινο δυναμικό, οι τεχνολογικοί περιορισμοί, οι κυβερνοεπιθέσεις & κυβερνοαπειλές στα πληροφοριακά συστήματα, και οι περιβαλλοντικές απειλές, που αποδίδονται σε φυσικές και ανθρωπογενείς καταστροφές, επιβεβαιώνουν ότι τα προσωπικά δεδομένα είναι διαρκώς εκτεθειμένα σε κινδύνους και η επεξεργασία τους συνιστά μία σύνθετη διαδικασία. Ο κρίσιμος

χαρακτήρας των προκλήσεων αποτυπώνεται και στις δύο μελέτες περίπτωσης, που παρουσιάστηκαν αναφορικά με τις παραβιάσεις, που σημειώθηκαν στο πλαίσιο έκδοσης ταυτοτήτων και τη διαρροή προσωπικών δεδομένων ένεκα της κυβερνοεπίθεσης «EMOTET». Υπό αυτό το πρίσμα, η προστασία των δεδομένων, απαιτεί την εφαρμογή μίας κατάλληλης μεθοδολογίας διαχείρισης της επικινδυνότητας, συστηματική εκπαίδευση του προσωπικού, κατάλληλους ελέγχους πρόσβασης στους ψηφιακούς και φυσικούς πόρους της ΕΛ.ΑΣ., πλήρη καταγραφή, τεκμηρίωση και ανάλυση των ενεργειών επεξεργασίας, διαρκή μέριμνα για την κυβερνοασφάλεια των συστημάτων της, ασφαλή και συχνή διατήρηση αντιγράφων ασφαλείας, καθώς και κρυπτογράφηση, ψευδωνυμοποίηση και ανωνυμοποίηση των δεδομένων. Ασφαλώς, πολλά από τα προαναφερόμενα μέτρα θα πρέπει να εφαρμόζονται υπό το πρίσμα μίας πολύ-επίπεδης αρχιτεκτονικής ασφάλειας.

Συμπερασματικά, αν και το νομικό οπλοστάσιο υφίσταται, η διαρκής ευαισθητοποίηση και επαγγελματική κατάρτιση του αστυνομικού προσωπικού σχετικά με την επεξεργασία των δεδομένων και την σπουδαιότητα της προστασίας τους είναι απαραίτητες, προκειμένου να εξασφαλίζεται διαρκώς ισορροπία μεταξύ άσκησης δημόσιας εξουσίας και σεβασμού των θεμελιωδών δικαιωμάτων των ατόμων.

Με την παρούσα εργασία τέθηκαν οι βάσεις για την κατανόηση του νομικού πλαισίου προστασίας δεδομένων, την εφαρμογή του από την Ελληνική Αστυνομία κατά την επεξεργασία προσωπικών δεδομένων σε συγκεκριμένες λειτουργίες της και την ανάδειξη των προκλήσεων, που ανακύπτουν. Η εκπόνηση αυτής αποτέλεσε μία ουσιαστική εμβάθυνση στην πρακτική διάσταση της προστασίας των προσωπικών δεδομένων, αναδεικνύοντας ότι η επεξεργασία και προστασία των προσωπικών δεδομένων δεν συνιστά απλώς μία νομική υποχρέωση, αλλά μία διαρκή και σύνθετη διαδικασία, που απαιτεί γνώσεις και υπευθυνότητα.

Ωστόσο, η παρούσα μελέτη θα μπορούσε να επεκταθεί από μελλοντικούς ερευνητές με τους εξής τρόπους:

- Να διερευνηθούν οι προκλήσεις από τη χρήση των καμερών ΑΙ, που έχουν τοποθετηθεί από τον Δεκέμβριο του 2025 για την καταγραφή τροχονομικών παραβάσεων και η επίδραση τους στην προστασία των προσωπικών δεδομένων.
- Να διαμοιραστούν και συμπληρωθούν ερωτηματολόγια σε αστυνομικούς, που εμπλέκονται άμεσα στις διαδικασίες επεξεργασίας δεδομένων που εξετάστηκαν, αναφορικά με το επίπεδο κατάρτισής τους και την εφαρμογή του νομικού πλαισίου προστασίας δεδομένων κατά την άσκηση των καθηκόντων τους.
- Να πραγματοποιηθεί συνέντευξη με τον Υπεύθυνο Προστασίας Δεδομένων της ΕΛ.ΑΣ., προκειμένου να καταγραφούν οι πρακτικές δυσκολίες εφαρμογής του νομικού πλαισίου.

- Να πραγματοποιηθεί έρευνα για το πώς εφαρμόζουν οι αστυνομικές αρχές άλλων χωρών της Ε.Ε. τις βασικές αρχές επεξεργασίας δεδομένων κατά την άσκηση των καθηκόντων τους.
- Να πραγματοποιηθεί μελέτη και σε άλλες δραστηριότητες, που επιτελεί η ΕΛ.ΑΣ. και σχετίζονται με την συλλογή και επεξεργασία των προσωπικών δεδομένων των πολιτών και να αναλυθεί ο τρόπος επεξεργασίας τους.

Βιβλιογραφία

- Abdulhammad, A., Cherries, M. & Okunola, A., (2024), «*The Role of Data Protection Regulations in Ensuring Data Privacy*», διαθέσιμο στην ιστοσελίδα https://www.researchgate.net/publication/387470741_The_Role_of_Data_Protection_Regulations_in_Ensuring_Data_Privacy
- Aidinlis, S., Barnard-Wills, D., Cochrane, L., Garstka, K., Gurzawska, A. & Hughes, J., (2024), «*Between GDPR and Law Enforcement Directive in Security Research: The Use of Personal Data by Law Enforcement Authorities*», διαθέσιμο στην ιστοσελίδα <https://ejlt.org/index.php/ejlt/article/view/957/1094>
- Crossa, C. & Holt, T., (2025), «*Beyond fraud and identity theft: assessing the impact of databreaches on individual victims*», Journal Of Crime And Justice, Routledge, διαθέσιμο στην ιστοσελίδα <https://www.tandfonline.com/doi/epdf/10.1080/0735648X.2025.2535007?needAccess=true>
- ENISA, (2025), «*TECHNICAL IMPLEMENTATION GUIDANCE*», διαθέσιμο στην ιστοσελίδα: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf
- European Commission, (2012), «*Proposal for a directive of the european parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*», διαθέσιμο στην ιστοσελίδα <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010>
- Leiser, M. & Custers, B., (2019), «*The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*», European Data Protection Law Review. Vol. 5, nr. 3, σσ. 367-378, διαθέσιμο στην ιστοσελίδα https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4014545
- Maesa, C., (2016), «*Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)*», διαθέσιμο στην ιστοσελίδα <https://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/>

- Quinn, P., (2022), «*The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework – CORRIGENDUM*», σσ. 1583–1612, German Law Journal, διαθέσιμο στην ιστοσελίδα https://www.researchgate.net/publication/358444864_The_Difficulty_of_Defining_Sensitive_Data-The_Concept_of_Sensitive_Data_in_the_EU_Data_Protection_Framework_-_CORRIGENDUM
- Ryz, L. & Grest, L. (2016), «*A new era in data protection*», διαθέσιμο στην ιστοσελίδα <https://www.sciencedirect.com/science/article/abs/pii/S1361372316300288>
- Radtke, T., (2020), «*The Concept Of Joint Control Under The Data Protection Law Enforcement Directive 2016/680 In Contrast To The GDPR*», σσ. 242-251, διαθέσιμο στην ιστοσελίδα <https://www.jipitec.eu/jipitec/article/view/285/279>,
- Salami, E., (2017), «*The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the Existing Privacy Regime*», διαθέσιμο στην ιστοσελίδα https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2912449
- Spalevic, Z. & Vićentijević, K., (2022), «*GDPR and challenges of personal data protection*», διαθέσιμο στην ιστοσελίδα https://www.researchgate.net/publication/360434912_GDPR_and_challenges_of_personal_data_protection
- Απόφαση 43/2021 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Απόφαση 32/2024 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Απόφαση 2008/615/ΔΕΥ του Συμβουλίου σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος
- Απόφαση 2008/616/ΔΕΥ του Συμβουλίου για την εφαρμογή της απόφασης 2008/615/ΔΕΥ σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος
- Αστερίου, Β., Κουρής, Κ., Πετρίδου, Σ., Νικοπολιτίδης, Π. και Παπαδημητρίου, Γ., (2021), «*Ασφάλεια στα Λειτουργικά Συστήματα και στην Εικονικοποίηση*», σε Κάτσικας, Σ., Γκριτζάλης, Σ. και Λαμπρινουδάκης, Κ. (επιμ.) Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο (σσ. 333-360), Αθήνα: Νέων Τεχνολογιών

- Broumas, A., (2019), «*Το Νομικό Πλαίσιο της Επεξεργασίας Βιομετρικών Δεδομένων*», διαθέσιμο στην ιστοσελίδα <https://lawandtech.eu/2019/09/09/biometric-data/>
- Γκατζούφας, Α., (2024), «*Α.Π.Δ.Π.Χ. 32/2024 επιβολή προστίμου 150.000 ευρώ στο Υπουργείο Προστασίας του πολίτη για ζητήματα προστασίας προσωπικών δεδομένων που αφορούν την έκδοση των νέου τύπου δελτίων ταυτότητας*», διαθέσιμο στην ιστοσελίδα <https://www.epoliteia.gr/wp-content/uploads/2024/12/%CE%A3%CE%A7%CE%9F%CE%9B%CE%99%CE%91-3.12.pdf>
- Γνωμοδότηση 4/2024 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Γνωμοδότηση 1/2005 της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών
- Γνωμοδότηση 15/2011 του Αρείου Πάγου
- Γνωμοδότηση 2/2017 του Αρείου Πάγου
- Γνωμοδότηση 78/2021 του Αρείου Πάγου
- Γριβοκωστόπουλος, Ι., (2021), «*Κριτική ανάλυση του Ν. 4624/2019*», διαθέσιμο στην ιστοσελίδα: <https://ejournals.lib.auth.gr/infolawj/article/view/8231/7989>
- Δημόπουλος, Χ., (2011), «*Ανακριτική*», 2^η Έκδοση, Αθήνα, Νομική Βιβλιοθήκη
- «*Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*», (2018), διαθέσιμο στην ιστοσελίδα: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
- «*Εθνικό Σχέδιο Διαχείρισης των Δημοσίων Υπαίθριων Συναθροίσεων*», (2021), διαθέσιμο στην ιστοσελίδα https://www.minocp.gov.gr/file/2021/01/27012021-ethniko_sxedio2.pdf
- EPTNEWS, (2023), «*Νέες ταυτότητες: 23 ερωτήσεις και απαντήσεις – Τα χαρακτηριστικά τους και τα fake news*», διαθέσιμο στην ιστοσελίδα <https://www.ertnews.gr/eidiseis/ellada/nees-taytotites-23-erotiseis-kai-apantiseis-ta-xaraktiristika-tous-kai-ta-fake-news/>
- ΕΣΟΕΛ, (2021), «*Μέθοδοι ανάλυσης δεδομένων στο πλαίσιο ελεγκτικών αποστολών*», Έκδοση 1.0

- Η Καθημερινή, (2018), «*GDPR: Οι αλλαγές στην προστασία προσωπικών δεδομένων στο διαδίκτυο*», διαθέσιμο στην ιστοσελίδα <https://www.kathimerini.com.cy/gr/politiki/gdpr-o-xartis-allagwn-stin-prostasia-prosopikwn-dedomenon-sto-diadiktyo>
- Η Καθημερινή, (2018), «*Η ευρωπαϊκή ισχύς και ο κανονισμός GDPR*», διαθέσιμο στην ιστοσελίδα <https://www.kathimerini.gr/opinion/964984/i-eyropaiki-ischys-kai-o-kanonismos-gdpr/>
- Η Καθημερινή, (2018), «*Προστασία προσωπικών δεδομένων: ο νέος κανονισμός που μας αφορά όλους*», διαθέσιμο στην ιστοσελίδα <https://www.kathimerini.gr/society/957098/prostasia-prosopikon-dedomenon-o-neos-kanonismos-poy-mas-afora-oloys-vinteo/>
- Ιγγλεζάκης, Ι., (2018), «*Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων (Κανονισμός 2016/679) – Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων*», 2^η έκδοση, Interactive Learning
- Ιγγλεζάκης, Ι., (2020), «*Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων Κανονισμός 2016/679 και ο Εφαρμοστικός Νόμος (Ν.4624/2019)*», 3^η έκδοση, Interactive Learning
- Κανέλλος, Ι., Λ., (2020), «*The GDPR handbook για DPOs, Επιχειρήσεις & Οργανισμούς*», Αθήνα: Νομική Βιβλιοθήκη
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου – «*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)*»
- Κανονισμός (ΕΕ) 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου – «*Για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Europol) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ*»
- Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου – «*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*»

- Κανονισμός (ΕΕ) 2024/982 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου - «Σχετικά με την αυτοματοποιημένη αναζήτηση και ανταλλαγή δεδομένων για την αστυνομική συνεργασία, και για την τροποποίηση των αποφάσεων 2008/615/ΔΕΥ και 2008/616/ΔΕΥ του Συμβουλίου και των κανονισμών (ΕΕ) 2018/1726, (ΕΕ) 2019/817 και (ΕΕ) 2019/818 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (κανονισμός Prüm II)»
- Καρύδα, Μ., (2021), «Ασφάλεια Πληροφοριακών Συστημάτων και Ανθρώπινος Παράγοντας» σε Κάτσικας, Σ., Γκριτζάλης, Σ. και Λαμπρινουδάκης, Κ. (επιμ.) Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο (σσ. 103-125), Αθήνα: Νέων Τεχνολογιών
- Κοκολάκης, Σ., (2021), «Διακυβέρνηση και Διοίκηση Ασφάλειας Πληροφοριών» σε Κάτσικας, Σ., Γκριτζάλης, Σ. και Λαμπρινουδάκης, Κ. (επιμ.) Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο (σσ. 47-72), Αθήνα: Νέων Τεχνολογιών
- Lawspot, (2013), «Προσωπικά δεδομένα», διαθέσιμο στην ιστοσελίδα <https://www.lawspot.gr/voithitika-keimena/prosopika-dedomena/>
- Lawspot, (2017), «Κανονισμοί, Οδηγίες και άλλες νομοθετικές πράξεις της Ευρωπαϊκής Ένωσης», διαθέσιμο στην ιστοσελίδα <https://www.lawspot.gr/voithitika-keimena/kanonismoi-odigies-kai-alles-nomothetikes-praxeis-tis/>
- Lawspot, (2017), «Προσωπικά δεδομένα και διασυνοριακή συνεργασία σε θέματα αστυνομικής και δικαστικής συνεργασίας (Σχέδιο Νόμου)», διαθέσιμο στην ιστοσελίδα <https://www.lawspot.gr/nomika-nea/prosopika-dedomena-kai-diasynoriaki-synergasia-se-themata-astynomikis-kai-dikastikis/>
- Lawspot, (2018), «Νέοι κανόνες για την προστασία των δεδομένων στον τομέα της αστυνομίας και της ποινικής δικαιοσύνης», διαθέσιμο στην ιστοσελίδα <https://www.lawspot.gr/nomika-nea/neoi-kanones-gia-tin-prostasia-ton-dedomenon-ston-tomea-tis-astynomias-kai-tis-poinikis/>
- Lawspot, (2022), «Άρση απορρήτου, κυβερνοασφάλεια και προσωπικά δεδομένα: Σε διαβούλευση το νομοσχέδιο του Υπ. Δικαιοσύνης και Επικρατείας», διαθέσιμο στην ιστοσελίδα <https://www.lawspot.gr/nomika-nea/arsis-aporrityoy-kyvernoasfaleia-kai-prosopika-dedomena-se-diavouleysi-nomoshedio-toy-yp/>
- Lawspot, (2022), «Άρση του απορρήτου για τη διακρίβωση εγκλημάτων: Για ποια εγκλήματα επιτρέπεται η άρση σύμφωνα με το νέο Νόμο 5002/2022», διαθέσιμο

στην ιστοσελίδα <https://www.lawspot.gr/nomika-nea/arsi-toy-aporritoy-gia-ti-diakrivosi-egklimatou-gia-poia-egklimata-epitrepetai-i-arsi/>

- Μάγκος, Ε. & Χρυσικόπουλος, Β., (2021), «*Αυθεντικοποίηση Οντότητας*», σε Κάτσικας, Σ., Γκριτζάλης, Σ. και Λαμπρινουδάκης, Κ. (επιμ.) Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο (σσ. 279-301), Αθήνα: Νέων Τεχνολογιών
- Μαυρίδης, Ι., Σαλονικιάς, Σ. & Khair, M., (2021), «*Έλεγχος προσπέλασης και εξουσιοδότησης*», σε Κάτσικας, Σ., Γκριτζάλης, Σ. και Λαμπρινουδάκης, Κ. (επιμ.) Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο (σσ. 303-332), Αθήνα: Νέων Τεχνολογιών
- Μήτρου, Λ., (2002), «*Η προστασία των προσωπικών δεδομένων στο πεδίο των εργασιακών σχέσεων. Η συμβολή της Αρχής*», σε Δόνος, Π., Μήτρου, Λ., Μίτλεττον, Φ & Παπακωνσταντίνου, Ευ., «*Η αρχή προστασίας προσωπικών δεδομένων & η επαύξηση της προστασίας των δικαιωμάτων*» (σσ. 21-45), Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα
- Μήτρου, Λ., (2014), «*Τράπεζες Γενετικών Δεδομένων και εξιχνίαση του εγκλήματος*», σε Καϊάφα-Γκμπάντι, Μ., Κουνουγέρη-Μανωλεδάκη, Ε. & Συμεωνίδου-Καστανίδου, Ε., «*Ανάλυση DNA & δικαστηριακή πράξη*» (σσ. 87-114), Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα
- Μήτρου, Λ., (2017), «*Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων. Νέο δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα*», Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα
- Μήτρου, Λ., (2021), «*Το κανονιστικό πλαίσιο της (Κυβερνο)Ασφάλειας*» σε Κάτσικας, Σ., Γκριτζάλης, Σ. και Λαμπρινουδάκης, Κ. (επιμ.) Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο (σσ. 73-101), Αθήνα: Νέων Τεχνολογιών
- Μπόκας, Ν., (2023), «*Λήψη και Ανάλυση DNA στην ποινική δίκη με το νέο Κ.Π.Δ.*», διαθέσιμο στην ιστοσελίδα https://www.crimetimes.gr/lipsi-kai-analysi-dna-stin-poiniki-diki-me/#_ftn38
- Μωραΐτης, Μ., Partner, Valida, Α., (2024), «*Κατανόηση των προκλήσεων της σωστής εφαρμογής του GDPR*», διαθέσιμο στην ιστοσελίδα <https://netweek.gr/katanoisi-ton-prokliseon-tis-sostis-efarmogis-tou-gdpr/>
- Νόμος 3471/2006 – «*Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997*»

- Νόμος 3917/2011 – «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»
- Νόμος 4620/2019 – «Κώδικας Ποινικής Δικονομίας»
- Νόμος 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»
- Νόμος 5002/2022 – «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών»
- Νόμος 5187/2025 – «Αναδιοργάνωση της δομής της Ελληνικής Αστυνομίας και αναβάθμιση της εκπαίδευσης του ένστολου προσωπικού της Εκσυγχρονισμός του θεσμού της ηλεκτρονικής επιτήρησης υπόδικων, κατάδικων και κρατούμενων σε άδεια Ρύθμιση θεμάτων κρατούμενων σε σωφρονιστικά καταστήματα και άλλες διατάξεις»
- Οδηγία 2016/680 «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»
- Ομάδα εργασίας άρθρου 29, WP243, (2017), «Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων», διαθέσιμο στην ιστοσελίδα https://www.dpa.gr/sites/default/files/2019-12/wp243rev01_el.pdf
- Ομάδα εργασίας του άρθρου 29, WP250, (2018), «Κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679», διαθέσιμο στην ιστοσελίδα https://www.dpa.gr/sites/default/files/2020-05/wp250rev01_el.pdf
- Ομάδα εργασίας του άρθρου 29, WP251, (2018), «Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679»
- Ομάδα εργασίας του άρθρου 29, WP203, (2013), «Opinion 03/2013 on purpose limitation», διαθέσιμο στην ιστοσελίδα

<https://www.incliva.es/wp-content/uploads/2021/02/Opinion-03.2013-on-purpose-limitation-del-Grupo-de-Trabajo-del-Articulo-....pdf>

- Ορφανός, Σ., (2022), «*Η ανάλυση DNA στο ελληνικό και ευρωπαϊκό δικονομικό δίκαιο*», Αθήνα, Νομική Βιβλιοθήκη
- Παναγοπούλου, Φ., (2019), «*Νόμος 4624/2019 και Εφαρμογή GDPR: Πολλά υποσχόμενος, αλλά παράλληλα καθυστερημένος*», διαθέσιμο στην ιστοσελίδα <https://www.syntagmawatch.gr/trending-issues/nomos-4624-2019-kai-efarmogi-gdpr-polla-yposchomenos-alla-parallila-kathysterimenos/>
- Παναγοπούλου, Φ., (2023), «*Σύνταγμα κατ'ερμηνεία – Άρθρο 19*», διαθέσιμο στην ιστοσελίδα <https://www.syntagmawatch.gr/my-constitution/arthro-19/>
- Προεδρικό Διάταγμα 4/1995 – «*Εισαγωγή στις Σχολές Αξιωματικών και Αστυφυλάκων με το σύστημα των γενικών εξετάσεων*»
- Προεδρικό Διάταγμα 245/1997 – «*Εκκαθάριση αρχείων των υπηρεσιών της Ελληνικής Αστυνομίας*»
- Προεδρικό Διάταγμα 47/2005 – «*Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφαλισή του*»
- Προεδρικό Διάταγμα 75/2020 – «*Χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους*»
- Προεδρικό Διάταγμα 81/2021 – «*Μεταφορά στην ελληνική νομοθεσία του κεφαλαίου 6 της απόφασης 2008/615/ΔΕΥ του Συμβουλίου της 23ης Ιουνίου 2008 σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος*»
- Προεδρικό Διάταγμα 25/2022 – «*Προϋποθέσεις χορήγησης διαβατηρίων, χρονική ισχύς, αντικατάσταση, απώλεια και ακύρωση αυτών*»
- Πρώτο Θέμα, (2024), «*Κυβερνοασφάλεια: Ένα στοίχημα που καμία εταιρεία δεν έχει περιθώριο να χάσει*», διαθέσιμο στην ιστοσελίδα <https://www.protothema.gr/greece/article/1552671/kuvernoasfaleia-ena-stoihima-pou-kamia-etairia-den-ehi-perithorio-na-hasei/>
- Ράικος, Α., (2011), «*Γενική Πολιτειολογία & Συνταγματικό Δίκαιο. Θεμελιώδη Δικαιώματα*», 4^η έκδοση, Αθήνα: Νομική Βιβλιοθήκη
- Σιασιάκος, Κ., Αναστασίου Σ. και Τούντας, Κ., (2016), «*Εκτίμηση των Επιπτώσεων σχετικά με την Προστασία Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης*», διαθέσιμο στην ιστοσελίδα

https://www.researchgate.net/publication/317109414_Ektimese_ton_Epiptoseon_sche_tika_me_ten_Prostasia_Dedomenon_se_erga_Elektronikes_Diakuberneses

- ΣΚΑΪ, (2025), «Οι πιο επικίνδυνες κυβερνοεπιθέσεις - Πώς μπορούν να τις αντιμετωπίσουν κράτη, οργανισμοί και επιχειρήσεις», διαθέσιμο στην ιστοσελίδα <https://www.skai.gr/news/technology/kyvernoepitheseis-poies-einai-oi-pio-epikindynes-gia-krati-organismous-kai-epixeiriseis>
- Σπυρόπουλος, Κ., Φ., (2012), «Εισαγωγή στο Συνταγματικό Δίκαιο II. Θεμελιώδη δικαιώματα.», Αθήνα: ΘΕΜΙΣ-Νικ.Α.Σάκκουλας & ΣΙΑ Ο.Ε.
- Σύνταγμα της Ελλάδας
- Τζέλλης, Δ. & Μυλώση, Μ., (2022), «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Αθήνα: Νομική Βιβλιοθήκη
- Υπουργείο Ψηφιακής Διακυβέρνησης, (2025), «Προσωπικός Αριθμός», διαθέσιμο στην ιστοσελίδα https://www.minocp.gov.gr/file/2025/06/02062025proswpikos_arithmos.pdf
- Υπουργική Απόφαση 3021/22/10-ο΄/2025– «Ρυθμίσεις για την έκδοση διαβατηρίων Ελλήνων πολιτών. Δικαιολογητικά και διαδικασία έκδοσης, τύπος και περιεχόμενο ενδείξεων διαβατηρίου, τήρηση αρχείου και ζητήματα προσωπικών δεδομένων»
- Υπουργική Απόφαση 8200/0-297647/2018/2018 - «Έκδοση νέου τύπου Δελτίου Ταυτότητας Ελλήνων πολιτών»
- Χατζηϊωάννου, Κ., (2023), «Η στάθμιση και αξιολόγηση της πραγματογνωμοσύνης DNA από τον ποινικό δικαστή», Θεσσαλονίκη
- <https://www.astynomia.gr/odigos-tou-politi/dikaiologitika/ekdosi-deltiou-taftotitas/>
- <https://www.astynomia.gr/odigos-tou-politi/dikaiologitika/ekdosi-deltiou-taftotitas/enimerosi-gia-tin-epexergasia-dedomenon-prosopikou-charaktira-apo-ti-diefthynsi-kratikis-asfaleias-archigeiou-ellinikis-astynomias/>
- https://www.minocp.gov.gr/file/2025/06/02062025proswpikos_arithmos.pdf
- <https://www.astynomia.gr/file/2025/10/24102025anakoinosipanelladikes.pdf>
- <https://www.astynomia.gr/elliniki-astynomia/anthropino-dynamiko/proslipseis-prosopikou/enimerosi-dilosi-sygkatathesis-gia-tin-epexergasia-prosopikon-dedomenon/>

- <https://www.passport.gov.gr/npc/est.html>
- <https://diavgeia.gov.gr/doc/6%CE%9A%CE%A7646%CE%9C%CE%A4%CE%9B%CE%92-5%CE%A3%CE%A9?inline=true>
- <https://cyber.gov.gr/kyvernoepitheseis/kyvernoepitheseis-kyvernoasfaleia/>
- <https://cyber.gov.gr/odigia-nis2/>
- <https://www.sakkoulas-online.gr/news/apdpch-32-2024-prostimo-tis-apdpch-sto-ypourgeio-prostasias-tou-politi-os-ypenvthyno-epexergasias-anaforika-me-tin-ekdosi-neou-typou-tavtotitas>
- https://www.ggde.gr/index.php?option=com_k2&view=item&id=4925:ypiresia-ypostirixsis-pliroforikis-kai-ilektronikon-systimaton&Itemid=348
- <https://adae.gov.gr/polites/ilektronikes-epikoinonies/syxnes-erotiseis#>
- https://www.astynomia.gr/file/2015/05/292_paroyiasi_dee.pdf
- <https://www.nis.gr/downloads/national-cert/RFC2350-GR.pdf>