

**ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΓΕΝΙΚΟ ΤΜΗΜΑ ΔΙΚΑΙΟΥ**

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ:
ΔΙΚΑΙΟ ΚΑΙ ΕΥΡΩΠΑΪΚΗ ΕΝΟΠΟΙΗΣΗ
ΚΑΤΕΥΘΥΝΣΗ: ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΘΕΩΡΙΑ ΤΟΥ ΔΙΚΑΙΟΥ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπουσα Καθηγήτρια: Επίκουρη Καθηγήτρια κα. Όλγα Τσόλκα

με θέμα:

**Δίκτυα ανταλλαγής πληροφοριών στο
πλαίσιο της αστυνομικής συνεργασίας
σε ποινικές υποθέσεις στην Ε.Ε.
και προστασία προσωπικών δεδομένων.
Ειδικά ζητήματα εφαρμογής
της Απόφασης Prüm.**

Υποβληθείσα από τον
Κωνσταντίνο Μαργαρό
μεταπτυχιακό φοιτητή (Α.Μ.: 0911Μ009)

Αθήνα, Δεκέμβριος 2013

ΠΕΡΙΕΧΟΜΕΝΑ

	Σελ.
Abstract	5
<hr/>	
I. Εισαγωγή	6
<hr/>	
II. A. Ανταλλαγή πληροφοριών μεταξύ των αρχών επιβολής του νόμου στην Ε.Ε. - Επισκόπηση των βασικών υφιστάμενων διαύλων επικοινωνίας	7
1. Το σύστημα Πληροφοριών Σένγκεν (SIS) και η «αναβάθμισή» του σε SIS II	7
1.1. Βασικά χαρακτηριστικά του SIS	7
1.2. Δημιουργία του SIS II	8
2. Τα «εργαλεία» της Ευρωπόλ	10
3. Τα «εργαλεία» της Ιντερπόλ	11
4. Λοιποί δίαυλοι επικοινωνίας	13
<hr/>	
B. Η Απόφαση 2008/615/ΔΕΥ (Prüm)	14
<hr/>	
1. Προλεγόμενα	14
1.1. Η ανάδειξη της αρχής της διαθεσιμότητας	
1.2. Η Απόφαση – Πλαίσιο 2006/960/ΔΕΥ (Σουηδική Πρωτοβουλία)	16
2. Σκοπός και περιεχόμενο της Απόφασης 2008/615/ΔΕΥ	18
2.1. Γενικές παρατηρήσεις	
2.2. Ανταλλαγή δεδομένων DNA, δακτυλικών αποτυπωμάτων και οχημάτων	19
2.3. Ανταλλαγή δεδομένων στα πλαίσια σημαντικών γεγονότων	21
2.4. Μέτρα πρόληψης τρομοκρατικών πράξεων	23
2.5. Κοινές Επιχειρήσεις	23

III.	Προστασία προσωπικών δεδομένων στην Ε.Ε.	26
1.	Επί των πρωτοβουλιών σε ευρωπαϊκό περιφερειακό επίπεδο	26
2.	Τα κείμενα του Συμβουλίου της Ευρώπης επί της επιτασσύμενης προστασίας στον αστυνομικό τομέα	27
2.1	Κανονιστικό περιεχόμενο της Σύμβασης 108 του έτους 1981	27
2.2	Περιεχόμενο της Σύστασης R (87) 15 της Επιτροπής Υπουργών	29
3.	Κανονιστικό περιεχόμενο της Οδηγίας 95/46/ΕΚ	30
4.	Κανονιστικό περιεχόμενο της Απόφασης - Πλαίσιο 2008/977/ΔΕΥ	35
5.	Πρόταση Κανονισμού και Οδηγίας για την αναβάθμιση του καθεστώτος προστασίας προσωπικών δεδομένων στην Ε.Ε.	38
IV.	Προστασία προσωπικών δεδομένων στα δίκτυα ανταλλαγής πληροφοριών αστυνομικής συνεργασίας σε ευρωπαϊκό και εθνικό επίπεδο	42
1.	Προστασία προσωπικών δεδομένων στο Σύστημα Πληροφοριών Σένγκεν	42
2.	Προστασία προσωπικών δεδομένων στα εργαλεία της Ευρωπόλ	44
3.	Προστασία προσωπικών δεδομένων στα εργαλεία της Ιντερπόλ	49
4.	Προστασία προσωπικών δεδομένων στην Απόφαση Prüm	52
V.	Δικαστική και εξωδικαστική προστασία	56
1.	Θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων	56
1.1.	Το δικαίωμα ενημέρωσης	56
1.2.	Το δικαίωμα πρόσβασης	57
1.3.	Το δικαίωμα αντίρρησης	58
1.4.	Το δικαίωμα δικαστικής προσφυγής	60

2.	Κυρώσεις	60
2.1.	Διοικητικές κυρώσεις	60
2.2.	Ποινικές κυρώσεις	61
2.2.1.	Για πράξεις και παραλείψεις επί των οποίων η Αρχή δεν έχει ακόμη αποφανθεί	62
2.2.2.	Για μη συμμόρφωση σε αποφάσεις της Αρχής	62
2.3.	Αστικές κυρώσεις	63
3.	Ζητήματα πρακτικής αποτελεσματικότητας του νομοθετικού καθεστώτος των δικαιωμάτων κατά την επεξεργασία δεδομένων στα δίκτυα ανταλλαγής πληροφοριών στο πλαίσιο της αστυνομικής συνεργασίας	63
3.1.	Προλεγόμενα	63
3.2.	Εφαρμογή του δικαιώματος ενημέρωσης	64
3.3.	Εφαρμογή του δικαιώματος πρόσβασης	66
3.4.	Εφαρμογή του δικαιώματος αντίρρησης	67
<hr/>		
VI.	Επίλογος	68
<hr/>		
VII.	Βιβλιογραφία	70
<hr/>		

Abstract

As it is well-known, law enforcement authorities have been exchanging information on many issues, such as crime investigation, crime prevention and detection (e.g. gathering of evidence related to a specific crime), and public order and security safeguard. However, the exchange of information may imperil personal rights, mainly in connection with personal data protection, if we take into consideration the state-of-the-art technology that has maximized automated data processing.

This paper will include a review of the main communication channels used by law enforcement authorities both at a European Union and at an international level and of the Council Decision 2008/615/JHA (Prüm Decision) in which the principle of availability of information is applied. Moreover, the main points of legal texts governing personal data protection in respect of information exchange in the context of police cooperation in the European Union will be presented, while there will be a brief reference to the new legal instruments used for strengthening data protection regime.

The individual protection of personal data in relation to main police cooperation information exchange networks, as well as the judicial and out-of-court protection offered by the Greek legislation to the persons whose data are under processing in the context of information exchange, will also be dealt with in the framework of this paper.

Keywords:

Schengen Information System, Europol, Interpol, Prüm, information exchange networks, police cooperation, data protection, judicial protection, out-of-court protection.

I. Εισαγωγή

Στο παρόν πρώτο Κεφάλαιο (I) πραγματοποιείται μία σύντομη εισαγωγή στα θέματα που θα αναλυθούν στο πλαίσιο της παρούσας εργασίας.

Ως γνωστόν, οι αρχές επιβολής του νόμου ανταλλάσσουν πληροφορίες για διάφορους σκοπούς, ήτοι τη διερεύνηση εγκλημάτων, την πρόληψη του εγκλήματος, την ανίχνευσή του (π.χ. με επιχειρήσεις συλλογής στοιχείων σχετικά με το έγκλημα) και τη διασφάλιση της δημόσιας τάξης και ασφάλειας. Η ανταλλαγή πληροφοριών όμως ενέχει κινδύνους για τα ατομικά δικαιώματα, κυρίως όσον αφορά την προστασία των προσωπικών δεδομένων, ιδιαίτερα αν ληφθούν υπ' όψιν οι πρόσφατες τεχνολογικές εξελίξεις που έχουν μεγιστοποιήσει την αυτοματοποιημένη επεξεργασία δεδομένων.

Αντικείμενο του δεύτερου Κεφαλαίου (II) είναι η επισκόπηση των βασικών διαύλων επικοινωνίας των αρχών επιβολής του νόμου, τόσο στην Ε.Ε., όσο και σε διεθνές επίπεδο, αλλά και της Απόφασης 2008/615/ΔΕΥ, ευρέως αποκαλούμενη ως Απόφαση Prüm, στην οποία εφαρμόζεται η αρχή της διαθεσιμότητας των πληροφοριών.

Στο τρίτο Κεφάλαιο (III) θα παρουσιαστούν τα βασικά σημεία των νομοθετημάτων που διέπουν την προστασία προσωπικών δεδομένων κατά την ανταλλαγή πληροφοριών στα πλαίσια της αστυνομικής συνεργασίας στην Ε.Ε., ενώ θα εκτεθούν συνοπτικά τα νέα νομικά εργαλεία με τα οποία επιχειρείται η ενδυνάμωση του καθεστώτος προστασίας.

Η επιμέρους προστασία προσωπικών δεδομένων στα κύρια δίκτυα ανταλλαγής πληροφοριών αστυνομικής συνεργασίας θα αποτελέσει αντικείμενο του τέταρτου Κεφαλαίου (IV), ενώ στο πέμπτο Κεφάλαιο (V) θα παρουσιαστεί η δικαστική και εξωδικαστική προστασία που προσφέρει η έννομη τάξη στον καθ' ού τα δεδομένα τυγχάνουν επεξεργασίας κατά την ανταλλαγή πληροφοριών.

II. Ανταλλαγή πληροφοριών μεταξύ των αρχών επιβολής του νόμου στην Ε.Ε. - Επισκόπηση των βασικών υφιστάμενων διαύλων επικοινωνίας

1. Το Σύστημα Πληροφοριών Σένγκεν (SIS) και η «αναβάθμισή» του σε SIS II

1.1. Βασικά χαρακτηριστικά του SIS

Το Σύστημα Πληροφοριών Σένγκεν (Schengen Information System - SIS) προέκυψε από τη βούληση ορισμένων Κρατών-μελών της Ε.Ε. να δημιουργήσουν έναν χώρο δίχως ελέγχους στα εσωτερικά σύνορα, διευκολύνοντας παράλληλα τη διέλευση των προσώπων διά μέσου των εξωτερικών τους συνόρων.¹ Με την εγκαθίδρυση του εν λόγω συστήματος, που βρίσκεται λειτουργία από το 1995, επιδιώχθηκε η διατήρηση της δημόσιας ασφάλειας, ή/και της εθνικής ασφάλειας, εντός του χώρου του Σένγκεν και η διευκόλυνση της κυκλοφορίας των προσώπων χάριν των πληροφοριών που διαβιβάζονται μέσω αυτού.

Το SIS αποτελεί ένα κεντρικό σύστημα πληροφοριών που περιλαμβάνει ένα εθνικό τμήμα σε κάθε συμμετέχον κράτος και μια υπηρεσία τεχνικής υποστήριξης στη Γαλλία. Τα Κράτη-μέλη μπορούν να εκδίδουν σήματα για πρόσωπα, των οποίων ζητείται η σύλληψη προκειμένου να εκδοθούν (ή πλέον για την εκτέλεση ευρωπαϊκού εντάλματος σύλληψης)· για υπηκόους τρίτων χωρών που χαρακτηρίζονται ανεπιθύμητοι· για εξαφανισθέντες· για μάρτυρες ή για πρόσωπα, των οποίων γίνεται δικαστική κλήτευση· για πρόσωπα και οχήματα, τα οποία είναι υπό εξαιρετική παρακολούθηση λόγω της απειλής που αποτελούν για τη δημόσια ή την εθνική ασφάλεια· για οχήματα, έγγραφα και όπλα που έχουν απολεσθεί ή κλαπεί· και για ύποπτα χαρτονομίσματα. Τα δεδομένα που καταχωρούνται στο SIS περιλαμβάνουν ονόματα και ψευδώνυμα, φυσικά χαρακτηριστικά, τόπο και ημερομηνία γέννησης, εθνικότητα και ένδειξη, αν το συγκεκριμένο πρόσωπο οπλοφορεί ή είναι βίαιο.

¹ Η εισαγωγή του συστήματος αυτού θεσπίστηκε στη Σύμβαση εφαρμογής της συμφωνίας του Σένγκεν της 14ης Ιουνίου 1985 μεταξύ των κυβερνήσεων των κρατών της Οικονομικής Ένωσης Μπενελούξ, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και της Γαλλικής Δημοκρατίας, σχετικά με τη σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα, ΕΕ L 239 της 22.9.2000, σ. 19.

Στα δεδομένα αυτά έχουν πρόσβαση η Αστυνομία, οι αρχές συνοριακού ελέγχου, οι τελωνειακές και δικαστικές αρχές, στο πλαίσιο ποινικών διαδικασιών, εντός των αντίστοιχων νόμιμων εξουσιών τους. Οι υπηρεσίες μετανάστευσης και οι προξενικές αρχές έχουν πρόσβαση στα δεδομένα που αφορούν υπηκόους τρίτων χωρών και που περιλαμβάνονται σε καταστάσεις προσώπων, τα οποία χαρακτηρίζονται ως ανεπιθύμητα, καθώς και στα καταχωρισθέντα απολεσθέντα ή κλαπέντα έγγραφα. Η Ευρωπόλ μπορεί να έχει πρόσβαση σε ορισμένες κατηγορίες δεδομένων του SIS, ιδίως σε καταχωρήσεις για εκζητούμενα πρόσωπα, των οποίων έχει ζητηθεί η σύλληψη, καθώς και για πρόσωπα που βρίσκονται υπό εξαιρετική παρακολούθηση, λόγω απειλής για τη δημόσια ή την εθνική ασφάλεια. Η Eurojust δύναται να έχει πρόσβαση σε καταχωρήσεις μόνον για εκζητούμενα πρόσωπα, των οποίων ζητείται η σύλληψη και για μάρτυρες ή πρόσωπα, των οποίων έχει γίνει δικαστική κλήτευση.

Το SIS έχει πλέον πλήρη εφαρμογή στα 22 Κράτη-μέλη, καθώς και στην Ελβετία, τη Νορβηγία, το Λιχτενστάιν και την Ισλανδία. Το Ηνωμένο Βασίλειο και η Ιρλανδία μετέχουν σε πτυχές της αστυνομικής συνεργασίας της σύμβασης του Σένγκεν και στο SIS, με εξαίρεση τις καταχωρήσεις για υπηκόους τρίτων χωρών, τα ονόματα των οποίων βρίσκονται σε κατάσταση προσώπων που χαρακτηρίζονται ως ανεπιθύμητα. Η Κύπρος, η Βουλγαρία και η Ρουμανία έχουν υπογράψει τη σύμβαση του Σένγκεν, αλλά δεν την έχουν ακόμη θέσει σε εφαρμογή.

Από τις αναζητήσεις στο SIS προκύπτει «θετική απάντηση» («hit»), όταν τα αναζητούμενα στοιχεία αντιστοιχούν στη συγκεκριμένη καταχώριση. Εφόσον λάβουν θετική απάντηση, οι αρμόδιες αρχές δύνανται, μέσω του δικτύου των γραφείων SIRENE, να ζητήσουν συμπληρωματικές πληροφορίες σχετικά με τα υποκείμενα της καταχώρισης².

1.2. Δημιουργία του SIS II

Με την ένταξη νέων κρατών μελών στον χώρο του Σένγκεν, αυξήθηκε αντίστοιχα και το μέγεθος της βάσης δεδομένων SIS: από τον Ιανουάριο του

² SIRENE (Supplementary Information Request at National Entry - αίτηση συμπληρωματικών πληροφοριών για εθνικές καταχωρίσεις).

2008 ως τον Ιανουάριο του 2010 αυξήθηκε από 22,9 σε 31,6 εκατομμύρια ο συνολικός αριθμός των καταχωρήσεων στο SIS.³ Για να ανταποκριθούν στην αναμενόμενη αυτή αύξηση του όγκου των δεδομένων και στις νέες ανάγκες των χρηστών, τα Κράτη-μέλη αποφάσισαν το 2001 να δημιουργήσουν ένα σύστημα πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) και ανέθεσαν το έργο αυτό στην Επιτροπή.⁴ Σκοπός του SIS II είναι να εξασφαλίζει υψηλό επίπεδο ασφάλειας στον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης, με αναβάθμιση των λειτουργιών του συστήματος πρώτης γενιάς και να διευκολύνει την κυκλοφορία των προσώπων χάρη στη διαβίβαση πληροφοριών μέσω αυτού.

Εκτός από τις αρχικές κατηγορίες δεδομένων που καλύπτει το σύστημα πρώτης γενιάς, το SIS II είναι σε θέση να διαχειρίζεται δακτυλικά αποτυπώματα, φωτογραφίες, αντίγραφα του ευρωπαϊκού εντάλματος σύλληψης, μηχανισμούς για την προστασία των συμφερόντων των προσώπων, των οποίων υποκλέπεται η ταυτότητα και συνδέσμους μεταξύ διαφόρων καταχωρήσεων. Για παράδειγμα, το SIS II είναι σε θέση να συνδέει τις καταχωρήσεις που αφορούν έναν καταζητούμενο για απαγωγή, το απαχθέν πρόσωπο και το όχημα που έχει χρησιμοποιηθεί για το έγκλημα αυτό. Οι κανόνες σχετικά με τα δικαιώματα πρόσβασης και τη διατήρηση των δεδομένων είναι οι ίδιοι με τους ισχύοντες για το σύστημα πρώτης γενιάς. Το SIS II που τέθηκε σε επιχειρησιακή λειτουργία την 09/04/2013, χρησιμοποιεί το s-TESTA, το ασφαλές σύστημα επικοινωνίας δεδομένων της Επιτροπής⁵ και εφαρμόζεται σε όλα τα Κράτη-μέλη, στην Ελβετία, στο Λιχτενστάιν, στη Νορβηγία και στην Ισλανδία.⁶

³ Έγγραφο του Συμβουλίου 5441/08, 30.1.2008· έγγραφο του Συμβουλίου 6162/10, 5.2.2010.

⁴ Βλ. σχετ.: Κανονισμός (ΕΚ) αριθ. 1986/2006, ΕΕ L 381 της 28.12.2006, σ. 1· Κανονισμός (ΕΚ) αριθ. 1987/2006, ΕΕ L 381 της 28.12.2006, σ. 4· Απόφαση 2007/533/ΔΕΥ, ΕΕ L 205 της 7.8.2007, σ. 63.

⁵ Ειδικότερα, το S-TESTA, (Secure Trans-European Services for Telematics between Administrations: «ασφαλείς διευρωπαϊκές υπηρεσίες τηλεματικής μεταξύ δημόσιων διοικήσεων») αποτελεί ένα δίκτυο επικοινωνίας δεδομένων που χρηματοδοτείται από την Επιτροπή και επιτρέπει την ασφαλή και κρυπτογραφημένη ανταλλαγή πληροφοριών μεταξύ των εθνικών διοικήσεων και των θεσμικών οργάνων, φορέων και οργανισμών της ΕΕ.

⁶ Το Ηνωμένο Βασίλειο και η Ιρλανδία συμμετέχουν στο SIS II, με εξαίρεση τις καταχωρίσεις που αφορούν υπηκόους τρίτων χωρών που χαρακτηρίζονται ως ανεπιθύμητοι.

2. Τα «εργαλεία» της Ευρωπόλ

Η Ευρωπόλ είναι η Ευρωπαϊκή Αστυνομική Υπηρεσία, η οποία συνεργάζεται με τα Κράτη – μέλη της Ε.Ε. μέσω των Εθνικών Μονάδων Ευρωπόλ (ENU) που έχουν ιδρυθεί και λειτουργούν σε καθένα από αυτά. Πιο συγκεκριμένα, τα Κράτη – μέλη τοποθετούν στις εγκαταστάσεις της Ευρωπόλ έναν Αστυνομικό Σύνδεσμο, ο οποίος διακινεί τις πληροφορίες από τον Οργανισμό προς την Εθνική Μονάδα και αντίστροφα, αλλά και προς και από τους άλλους Αστυνομικούς Συνδέσμους, ακόμη και χωρίς την ενημέρωση του Οργανισμού.

Οι πληροφορίες ανταλλάσσονται μέσω του προαναφερθέντος τριπτύχου (Οργανισμός-Σύνδεσμοι-Εθνικές Μονάδες) και αφορούν συγκεκριμένες μορφές σοβαρού και οργανωμένου εγκλήματος, όπως αυτές ορίζονται στο Παράρτημα 1 της Απόφασης Ευρωπόλ⁷, ενώ απαραίτητη προϋπόθεση είναι τα εγκλήματα αυτά να αποτελούν αντικείμενο έρευνας δύο ή περισσότερων Κρατών-μελών. Η Ευρωπόλ ασχολείται επίσης και με υποθέσεις τρομοκρατίας, χωρίς να είναι προαπαιτούμενη η προαναφερόμενη προϋπόθεση.

Για την εξασφάλιση ασφαλούς επικοινωνίας και μετάδοσης των δεδομένων, η Ευρωπόλ ανέπτυξε το σύστημα SIENA⁸, το οποίο αποτελεί και το εν ισχύ σύστημα ανταλλαγής αλληλογραφίας. Ενδεικτικά, για το 2011, τα Κράτη-μέλη χρησιμοποίησαν το SIENA για να ανταλλάξουν 222.000 μηνύματα, ενώ 53% των μηνυμάτων αυτών κοινοποιήθηκαν στην Ευρωπόλ⁹.

Ένα άλλο μέσο που αναπτύχθηκε από την Ευρωπόλ είναι το σύστημα EIS¹⁰. Το EIS είναι μία βάση δεδομένων, όπου οι Εθνικές Μονάδες Ευρωπόλ καταχωρούν στοιχεία υποθέσεων, οι οποίες βρίσκονται εν εξελίξει ή έχουν διαλευκανθεί και αφορούν τόσο σε άτομα, όσο και σε οχήματα. Περιέχει περίπου 183.000 πληροφορίες που παρέχουν τα κράτη μέλη για τη διασυννοριακή εγκληματικότητα, οι οποίες εμπίπτουν στο πεδίο της εντολής της Ευρωπόλ, τα

⁷ Απόφαση 2009/371/ΔΕΥ του Συμβουλίου της 6ης Απριλίου 2009 για την ίδρυση Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Ευρωπόλ), ΕΕ L 121/37, 15-5-2009.

⁸ Secure Information Exchange Network Application: «ασφαλής εφαρμογή δικτύου ανταλλαγής πληροφοριών».

⁹ COM(2012) 735 final: Ανακοίνωση της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο: Ενίσχυση της συνεργασίας για την επιβολή του νόμου στην Ε.Ε. – Το Ευρωπαϊκό Πρότυπο Ανταλλαγής Πληροφοριών, σελ. 6-7

¹⁰ Europol Information System (EIS).

εμπλεκόμενα άτομα (41.000) και άλλα συναφή δεδομένα. Συγκεκριμένα, η αναζήτηση στο EIS πραγματοποιείται στη βάση επιτυχούς/ μη επιτυχούς αναζήτησης («hit/no-hit»). Η Εθνική Μονάδα πραγματοποιεί δηλαδή αναζήτηση ενός προσώπου ή οχήματος στο σύστημα EIS κι εφόσον η αναζήτηση είναι επιτυχής (hit), τότε αιτείται την πληροφορία από το Κράτος-μέλος που την έχει καταχωρήσει.

Τα αρχεία δεδομένων εργασίας προς ανάλυση χρησιμοποιούνται από την Ευρωπόλ, προκειμένου να προβεί σε επιχειρησιακές αναλύσεις για την υποστήριξη διασυνοριακών ερευνών και κυρίως για την χάραξη στρατηγικής για την καταπολέμηση του εγκλήματος. Οι αναλύσεις αυτές πραγματοποιούνται για τον καθορισμό τόσο των εθνικών πολιτικών για την καταπολέμηση του εγκλήματος, όσο και των ευρωπαϊκών και είναι είτε τακτικές, όπως π.χ. η Ετήσια Έκθεση της Ευρωπόλ για το Οργανωμένο Έγκλημα (**O**rganized **C**rime **T**hreat **A**ssessment - OCTA), είτε «έκτακτες» κατόπιν αίτησης ενός Κ-μ ή της Ευρωπαϊκής Επιτροπής.

3. Τα «εργαλεία» της Ιντερπόλ

Ο Οργανισμός Διεθνούς Εγκληματολογικής Αστυνομίας (INTERPOL) είναι ο μεγαλύτερος οργανισμός αστυνομικής συνεργασίας. Συμβαλλόμενα μέρη είναι μέχρι σήμερα περί τα 190 Κράτη-μέλη, σε καθένα εκ των οποίων υφίσταται ένα Εθνικό Κεντρικό Γραφείο (ΕΚΓ) για την εξασφάλιση της επικοινωνίας με τη Γενική Γραμματεία του Οργανισμού στη Λυών, όσο και με τα Εθνικά Κεντρικά Γραφεία των άλλων Κρατών μελών. Τα ΕΚΓ της Ιντερπόλ λειτουργούν σε 24ωρη βάση και ανταλλάσσουν πληροφορίες με τη Γενική Γραμματεία της Ιντερπόλ, καθώς και μεταξύ τους, κάνοντας χρήση των εργαλείων του Οργανισμού¹¹.

Για τη διασφάλιση της επικοινωνίας, η Ιντερπόλ έχει αναπτύξει και λειτουργεί το σύστημα I-24/7, το οποίο είναι αντίστοιχο του SIS. Μέσω του I-24/7 διαβιβάζονται αιτήματα που αφορούν συνολικά το επιστητό του αστυνομικού έργου, συμπεριλαμβανομένων εξακριβώσεων ταξιδιωτικών εγγράφων, πινακίδων κυκλοφορίας, κ.α.. Παράλληλα, τα Κράτη-μέλη, μέσω των

¹¹ Το Εθνικό Κεντρικό Γραφείο Ιντερπόλ Αθήνας αποτελεί το 4^ο Τμήμα της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας του Αρχηγείου της Ελληνικής Αστυνομίας. Σημειώνεται ότι η Χώρα μας συμμετέχει στην Ιντερπόλ βάσει του Ν. 3640/1956 (ΦΕΚ 303 Α'/28.12.1956).

ΕΚΓ, αποστέλλουν αιτήματα στη Γενική Γραμματεία Ιντερπόλ για την έκδοση ανακοινώσεων/αγγελιών (Notices) με τις οποίες αιτούνται από τα άλλα Κράτη-μέλη τον εντοπισμό και τη σύλληψη ατόμων, οι οποίοι έχουν τελέσει αξιόποινες πράξεις ή σε βάρος των οποίων έχει ασκηθεί ποινική δίωξη για τέλεση εγκλημάτων και οι οποίοι εικάζεται ότι έχουν διαφύγει στο εξωτερικό (ερυθρές αγγελίες). Οι ερυθρές αγγελίες εκδίδονται βάσει εθνικού εντάλματος σύλληψης και αφορούν μόνο τον εντοπισμό και τη σύλληψη εγκληματιών και όχι την έκδοσή τους στην αιτούσα χώρα. Για την τελευταία περίπτωση, ισχύει η διαδικασία η οποία πραγματοποιείται μέσω της δικαστικής συνεργασίας και κυρίως μέσω της Ευρωπαϊκής Σύμβασης Έκδοσης¹², της Σύμβασης Έκδοσης της Οικονομικής Κοινότητας των Δυτικοαφρικανικών Κρατών (ECOWAS)¹³ και των Συμβάσεων που έχουν καταρτιστεί βάσει της Πρότυπης Σύμβασης των Ηνωμένων Εθνών για την Έκδοση¹⁴.

Άλλων ειδών αγγελίες (Notices) είναι οι μπλε, οι κίτρινες, οι μαύρες, οι πράσινες, οι πορτοκαλί και οι μωβ. Οι κίτρινες αγγελίες αφορούν τη συνδρομή στον εντοπισμό αγνοούμενων προσώπων (συμπεριλαμβανομένων των ανηλίκων) ή προσώπων που πάσχουν από άνοια ή αμνησία ή έχουν τραυματιστεί σοβαρά και δεν έχουν τις αισθήσεις τους και γενικά δεν είναι σε θέση να ταυτοποιήσουν τον εαυτό τους. Οι μπλε αγγελίες χρησιμοποιούνται για τη συλλογή περαιτέρω στοιχείων σχετικά με την ταυτότητα ενός προσώπου, τον τόπο εργασίας/κατοικίας του ή τις εγκληματικές του δραστηριότητες. Οι μαύρες αγγελίες χρησιμοποιούνται για την αναζήτηση πληροφοριών για

¹² European Convention on Extradition (CETS 024) signed in Paris on 13/12/1957, βλ. Το κείμενο [στον ιστοτόπο: http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=024&CM=8&CL=ENG](http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=024&CM=8&CL=ENG). Η σύμβαση αυτή κυρώθηκε στη χώρα μας με το Ν. 4165/1961 (ΦΕΚ 75/6.5.1961).

¹³ ECOWAS Convention of Extradition signed in Abuja on 6 August 1994 (https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=https://www.icpat.org/index.php/documentation-a-articles-mainmenu-97/doc_download/2F21-ecowas-extradition-document&ei=wQNAUvC_EYbcsgad8YDACw&usq=AFQjCNEGKOfnx6vgXb1WC1y0ciIFV54Q&sig=2=utqf62Ayxox7P9iaQom2og&bvm=bv.52434380.d.Yms). Η Ελλάδα δεν είναι Συμβαλλόμενο Μέρος.

¹⁴ UNODC Model Law on Extradition (http://www.icpat.org/index.php/documentation-a-articles-mainmenu-97/doc_download/50-unodc-model-law-on-extradition). Η Σύμβαση αυτή αποτελεί πρότυπο κειμένου που καταρτίστηκε το 2004 από τα Ηνωμένα Έθνη με σκοπό να χρησιμοποιείται από τα Κράτη ως μοντέλο σύναψης αντίστοιχων συμφωνιών. Το εν λόγω κείμενο συνοδεύουν τέσσερα εγχειρίδια, όπου επεξηγούνται οι διατάξεις του.

πτώματα που δεν έχει αναγνωρισθεί η ταυτότητά τους, ενώ οι πράσινες για την παροχή προειδοποιήσεων και πληροφοριών για άτομα που έχουν διαπράξει εγκλήματα και πιθανολογείται ότι θα επαναλάβουν τη διάπραξη τους σε άλλα κράτη. Οι πορτοκαλί αγγελίες εκδίδονται για την προειδοποίηση ενόψει ενός σοβαρού επικείμενου κινδύνου στη δημόσια ασφάλεια ενός κράτους και οι μωβ για την αναζήτηση πληροφοριών επί του τρόπου δράσης (modus operandi) εγκληματιών¹⁵.

Μια αγγελία εκδίδεται μόνον, όταν πληρούνται όλες οι νόμιμες προϋποθέσεις. Ειδικότερα, θα πρέπει να μην παραβιάζεται το άρθρο 3 του Κανονισμού της Ιντερπόλ¹⁶, βάσει του οποίου ο Οργανισμός απαγορεύεται να προβαίνει σε ενέργειες ή παρεμβάσεις πολιτικού, στρατιωτικού, θρησκευτικού ή φυλετικού χαρακτήρα, καθώς και να τηρούνται οι κανόνες επεξεργασίας που τίθενται στους Κανόνες Επεξεργασίας Δεδομένων της Ιντερπόλ¹⁷ σχετικά με τη νομιμότητα, την ποιότητα των πληροφοριών και την προστασία προσωπικών δεδομένων.

4. Λοιποί διάυλοι επικοινωνίας

Άλλοι διάυλοι περιλαμβάνουν Αξιωματικούς Συνδέσμους, οι οποίοι δραστηριοποιούνται σε διμερές επίπεδο. Συγκεκριμένα είναι εγκατεστημένοι σε άλλα Κράτη-μέλη και δραστηριοποιούνται κατά κανόνα για την αστυνομική συνεργασία σε μη επιχειρησιακά ζητήματα. Επίσης, λειτουργούν Κοινά Κέντρα Αστυνομικής και Τελωνειακής Συνεργασίας, τα οποία έχουν συσταθεί από γειτονικά Κράτη-μέλη για τη στήριξη της ανταλλαγής πληροφοριών καθώς και την επιχειρησιακή συνεργασία σε παραμεθόριες περιοχές.¹⁸

¹⁵ Ιστοσελίδα της Ιντερπόλ - <http://www.interpol.int/INTERPOL-expertise/Notices>

¹⁶ Interpol Constitution: <http://www.interpol.int/Media/Files/Legal-material/Reference-Documents/Constitution-and-General-Regulations>

¹⁷ Interpol's Rules on the Processing of Data: <http://www.interpol.int/Media/Files/Legal-material/Reference-Documents/INTERPOL%E2%80%99s-Rules-on-the-Processing-of-Data>

¹⁸ Στην Ελλάδα, τέτοιο Κέντρο υφίσταται στον Προμαχώνα Σερρών, στα ελληνοβουλγαρικά σύνορα. Ιδρύθηκε και λειτουργεί βάσει διακρατικής συμφωνίας, η οποία ενσωματώθηκε στην εθνική έννομη τάξη με το Ν. 3779/09.

B. Η Απόφαση 2008/615/ΔΕΥ (Prüm)

1. Προλεγόμενα

Όπως προαναφέρθηκε, η αστυνομική συνεργασία μέχρι και τα μέσα της δεκαετίας του έτους 2000 αφορούσε ουσιαστικά την ανταλλαγή στοιχείων επί προσώπων, οχημάτων και εγγράφων (κυρίως ταξιδιωτικών), κατόπιν σχετικού αιτήματος μιας χώρας. Τα δεδομένα όμως αλλάζουν ριζικά με την εισαγωγή μιας νέας αρχής που διέπει πλέον τη λειτουργία της αστυνομικής συνεργασίας στην Ε.Ε., της αρχής της διαθεσιμότητας. Ειδικότερα:

1.1. Η ανάδειξη της αρχής της διαθεσιμότητας (Principle of availability)

Με τη θεσμική αναγνώριση της αρχής της διαθεσιμότητας, όπως ορίστηκε στο Πρόγραμμα της Χάγης¹⁹, επιδιώκεται η διασφάλιση της δυνατότητας «ενός υπαλλήλου αρχής επιβολής του νόμου σε ένα Κράτος μέλος, ο οποίος χρειάζεται πληροφορίες (σε μια προ-δικαστική φάση²⁰) προκειμένου επιτελέσει το έργο του, να τις λάβει από ένα άλλο Κράτος μέλος και συγκεκριμένα από μια άλλη αρχή επιβολής του νόμου σε ένα άλλο Κράτος μέλος, η οποία κατέχει τις πληροφορίες και τις καθιστά διαθέσιμες για το σκοπό που αιτούνται»²¹. Η εν λόγω αρχή καθιερώθηκε αρχικά με τη Συνθήκη Prüm κι αργότερα με τις Αποφάσεις Prüm, τις οποίες θα δούμε παρακάτω.

Ποιος είναι όμως ο λόγος που εισήχθη αυτή η αρχή; Ήδη από τις αρχές του αιώνα που διανύουμε, καταδείχθηκε η αναγκαιότητα ανταλλαγής δεδομένων και πληροφοριών (συμπεριλαμβανομένων και «επεξεργασμένων πληροφοριών», υπό την αγγλική ορολογία «intelligence»), κυρίως στο πλαίσιο της αντιμετώπισης του οργανωμένου εγκλήματος, αλλά και της τρομοκρατίας, ιδίως μετά τα τρομοκρατικά χτυπήματα στους Δίδυμους Πύργους στη Νέα Υόρκη το 2001 και στο σιδηροδρομικό σταθμό της Μαδρίτης το 2004. Όπως γίνεται κατανοητό, η βασική προβληματική δεν αφορούσε τόσο τη συνήθη

¹⁹ ΕΕ C 53/1 “Το Πρόγραμμα της Χάγης: Ενίσχυση της ελευθερίας, της ασφάλειας και της δικαιοσύνης στην Ευρωπαϊκή Ένωση”, 03/03/2005, Κεφ. 2.1, σελ. 7

²⁰ Ο ανωτέρω όρος αποτελεί απόδοση στην ελληνική του όρου: “in the pre-trial phase”.

²¹ Βλ. σχετ. Sylvania KIERKEGAARD, From Prüm to the EU, Presentation at the *Computers, Privacy and Data Protection conference: Panel Session on Europol, Eurojust, Prüm and Beyond: New development in Justice and Home Affairs, 2009 (Brussels, 16-17 January)*, σελ. 3.

ανταλλαγή πληροφοριών αστυνομικού ενδιαφέροντος, η οποία έτσι κι αλλιώς πραγματοποιούνταν μέσω των υφιστάμενων διαύλων επικοινωνίας, αλλά περισσότερο τα αιτήματα για χρήση ειδικών ανακριτικών πράξεων, όπως η άρση απορρήτου επικοινωνιών κ.λπ., η νομοθετική πρόβλεψη των οποίων είχε πραγματοποιηθεί στη Σύμβαση του Παλέρμο και σταδιακά ενσωματώνονταν στις εθνικές νομοθεσίες των Κρατών.

Το ζήτημα που ανέκυψε ήταν ότι, στην πλειονότητα των Κρατών, η ανταλλαγή τέτοιων πληροφοριών απαιτούσε αίτημα δικαστικής συνδρομής, γεγονός που την καθιστούσε χρονοβόρα, περίπλοκη και προβληματική²², δεδομένου μάλιστα ότι τη συγκεκριμένη χρονική στιγμή μιλούσαμε ήδη για μία Ευρώπη, που ενόψει της ελεύθερης κυκλοφορίας προσώπων, είχε καταργήσει τους ελέγχους στα εσωτερικά σύνορα.

Για τους λόγους αυτούς, λοιπόν, το Ευρωπαϊκό Συμβούλιο της 25^{ης} Μαρτίου 2004 εισήγαγε την αρχή της διαθεσιμότητας των πληροφοριών, καλώντας την Ευρωπαϊκή Επιτροπή να στρέψει τις προσπάθειές της στην «απλοποίηση (simplify) της ανταλλαγής πληροφοριών και επεξεργασμένων πληροφοριών (information and intelligence) μεταξύ των αρχών επιβολής του νόμου των Κρατών – μελών [της Ε.Ε.]». Ανταποκρινόμενη στο κάλεσμα του Ευρωπαϊκού Συμβουλίου, η Επιτροπή εξέδωσε στις 16 Ιουνίου του ίδιου έτους την Ανακοίνωση 429/2004 υπό τον τίτλο: «Για την ενίσχυση της πρόσβασης στις πληροφορίες από τις αρχές επιβολής του νόμου». Στη συνέχεια ακολούθησε η Ανακοίνωση 490 του 2005²³, η οποία διελάμβανε τις προτάσεις για τους τρόπους υλοποίησης της απλοποίησης των πληροφοριών.

Τη νομοθετική πρωτοβουλία ανέλαβε το Λουξεμβούργο, που όντας η προεδρεύουσα χώρα στην Ε.Ε. το α' εξάμηνο του 2005, κατέθεσε το Μάρτιο του ίδιου έτους πρόταση για μια «αποτελεσματική ανταλλαγή πληροφοριών». Αν και δεν υπήρξε ρητή αναφορά στην αρχή της διαθεσιμότητας, η πρωτοβουλία του Λουξεμβούργου ουσιαστικά την υλοποιούσε, καθόσον είχε ως προφανή

²² Βλ. σχετ. Tony Bunyan, «The principle of availability», Δεκέμβριος 2006, Διαδικτυακό περιοδικό CILIP, Τεύχος 84 (σε <http://www.statewatch.org/analyses/no-59-p-of-a-art.pdf>), αλλά και Bigo Didier, Bruggeman Willy, Burgess Peter, Mitsilegas Valsamis, «The Principle of Information Availability», Μάρτιος 2007, διαδικτυακό περιοδικό Challenge:Liberty & Security, <http://www.libertysecurity.org/article1376.html>.

²³ COM(2005) 490 τελικό «Πρόταση Απόφασης – Πλαίσιο του Συμβουλίου για την ανταλλαγή πληροφοριών βάσει της αρχής της διαθεσιμότητας», 12.10.2005

στόχο τη δημιουργία – θεσμοθέτηση όσο το δυνατό περισσότερων κατηγοριών πληροφοριών²⁴ που είναι δυνατόν να ανταλλαχθούν με την ελάχιστη δυνατή προσπάθεια κι αν αυτό είναι εφικτό, με τους ελάχιστους περιορισμούς σε αδειοδοτήσεις και διαδικασίες, αν όχι χωρίς κανένα περιορισμό.²⁵

Μολονότι η ανωτέρω πρόταση δεν υιοθετήθηκε από το Συμβούλιο, έξι ακόμη Κράτη – μέλη της Ε.Ε. υποστήριξαν την πρόταση και κατάρτισαν στις 27 Μαΐου 2005 τη Συνθήκη Prüm²⁶, εκτός τότε του πλαισίου της Ε.Ε. Στην εν λόγω Συνθήκη περιλαμβάνεται η δημιουργία βάσεων γενετικών δεδομένων (DNA profiles) και οχημάτων (Vehicle registration), καθώς και η ανταλλαγή δεδομένων, βάσει αυτών, για λόγους ποινικής δίωξης.

1.2. Η Απόφαση – Πλαίσιο 2006/960/ΔΕΥ (Σουηδική Πρωτοβουλία)

Παράλληλα όμως με την κατάρτιση της Συνθήκης Prüm, η Επιτροπή, κατόπιν σχετικής επιταγής του Προγράμματος της Χάγης (Κεφάλαιο III.2.1), επεξεργάστηκε ένα σχέδιο Απόφασης-Πλαίσιο για την εφαρμογή της αρχής της διαθεσιμότητας, που δημοσιοποιήθηκε με την προαναφερόμενη Ανακοίνωση 490 του 2005.

Η προτεινόμενη Απόφαση-Πλαίσιο, όπως άλλωστε αναφέρεται και στην αιτιολογική έκθεση²⁷ της Ανακοίνωσης της Επιτροπής, δεν αποτελεί τμήμα του κεκτημένου Σένγκεν, ούτε αποτελεί ανάπτυξή του. Αντιθέτως, εισάγει νέους κανόνες, βάσει των οποίων παρέχεται άμεση ηλεκτρονική πρόσβαση στις διαθέσιμες πληροφορίες και στα δεδομένα καταλόγου για πληροφορίες που δεν διατίθενται ηλεκτρονικά. Η πρόσβαση αυτή παρέχεται στις αρχές επιβολής του

²⁴ Στις κατηγορίες αυτές συμπεριλαμβάνονταν τόσο δεδομένα δακτυλικών αποτυπωμάτων και DNA, όσο και «διοικητικά δεδομένα», όπως στοιχεία αδειών οδήγησης, αδειών κυκλοφορίας οχημάτων, στοιχεία επιβατών αεροπορικών εταιριών, κ.α..

²⁵ Έγγραφο εργασίας 7416/05. Συγκεκριμένα διαλαμβανόταν ότι: «*The aim is obviously that as large a list of information categories as possible is exchangeable with as little effort as possible (ie: requiring a minimum of formalities, permissions, procedures, if any)*»

²⁶ Η Συνθήκη πήρε το όνομά της από τη γερμανική πόλη Prüm όπου και συνομολογήθηκε. Τα Συμβαλλόμενα Μέρη ήσαν η Γερμανία, η Ισπανία, η Γαλλία, το Λουξεμβούργο, η Ολλανδία, η Αυστρία και το Βέλγιο. Μέχρι το έτος 2008, όπου η Συνθήκη «κοινοτικοποιήθηκε» με την Απόφαση Prüm, που αναλύεται παρακάτω, στη Συνθήκη είχαν προσχωρήσει άλλα επτά Κ-μ, συμπεριλαμβανομένης και της γείτονός μας, Βουλγαρίας. Η Χώρα μας, αν και είχε εκδηλώσει πρόθεση συμμετοχής της μέσω του τότε Υπουργού Δημόσιας Τάξης, δεν προσχώρησε ποτέ στη Συνθήκη.

²⁷ COM(2005)490 final, ό.π., σελ. 2-3

νόμου των Κρατών-μελών και στους υπαλλήλους της Ευρωπόλ. Σχετικά λήφθησαν υπ' όψιν οι υφιστάμενες δυσκολίες στον τομέα της ανταλλαγής πληροφοριών και κυρίως η έλλειψη υποχρέωσης παροχής πληροφοριών (βάσει των υφιστάμενων διμερών και πολυμερών συμφωνιών), η παρέμβαση των εθνικών μονάδων ή κεντρικών σημείων επαφής (π.χ. Εθνική Μονάδα Ευρωπόλ), οι διαφορές στους όρους πρόσβασης και ανταλλαγής πληροφοριών, οι διακρίσεις μεταξύ αστυνομικής, τελωνειακής και δικαστικής συνεργασίας, οι αποκλίσεις στα πρότυπα προστασίας που εμποδίζουν την ανταλλαγή εμπιστευτικών πληροφοριών και η έλλειψη κοινών κανόνων για τον έλεγχο της νόμιμης χρήσης των πληροφοριών που λήφθηκαν από άλλο Κράτος-μέλος.

Κατ' ουσία, η πρόταση Απόφασης-Πλαίσιο υποχρεώνει τα Κράτη-μέλη να διασφαλίζουν ότι όλες οι πληροφορίες για την επιβολή του νόμου, ήτοι για την υλοποίηση, διευκόλυνση ή επιτάχυνση της πρόληψης, εξακρίβωσης ή διερεύνησης αξιόποινων πράξεων, οι οποίες ελέγχονται από τις αρχές που έχουν οριστεί για το σκοπό αυτό, διαβιβάζονται στις ισοδύναμες αρμόδιες αρχές άλλων Κρατών-μελών και στην Ευρωπόλ, εάν τούτο απαιτείται για την άσκηση των καθηκόντων τους. Οι διαθέσιμες πληροφορίες διαβιβάζονται είτε μέσω ηλεκτρονικής πρόσβασης είτε ηλεκτρονικά, κατόπιν αίτησης και μετά την επίτευξη αντιστοιχίας των αιτούμενων πληροφοριών και των δεδομένων καταλόγου που παρέχουν τα Κράτη-μέλη.

Παρότι όμως η πρόβλεψη για την ηλεκτρονική διαθεσιμότητα των πληροφοριών – η οποία ήταν και η μεγάλη καινοτομία – υπήρχε στην πρόταση της Επιτροπής (άρθρο 9), τούτη δεν ενσωματώθηκε στο τελικό κείμενο της Απόφασης-Πλαίσιο, προφανώς λόγω του ότι πολλά Κράτη-μέλη δεν είχαν τη δυνατότητα – ή και τη διάθεση – τη χρονική στιγμή εκείνη να διαθέσουν ηλεκτρονικά τα δεδομένα που είχαν αποθηκευμένα. Αυτό που παρέμεινε ωστόσο στο τελικό κείμενο ήταν οι προθεσμίες απάντησης (3 ώρες για τα κατεπείγοντα αιτήματα και 8 ώρες για τα επείγοντα), μέσω των οποίων επιταχύνονται ουσιαστικά οι χρόνοι απάντησης στα αιτήματα συνεργασίας.

Στη σχετική έκθεση του Συμβουλίου το Νοέμβριο του 2012 για την εφαρμογή της Απόφασης-Πλαίσιο²⁸ επισημάνθηκε ότι τέσσερα Κράτη-μέλη δεν

²⁸ Έγγραφο 14755/1/12 REV 1 JAI 683 DAPIX 123 CRIMORG 114 ENFOCUSTOM 99 ENFOPOL 317 COMIX 558 σχετικά με την εφαρμογή της Απόφασης 2006/960/ΔΕΥ, σελ. 3,5,6

έχουν ακόμα ενσωματώσει την Απόφαση-Πλαίσιο στην εθνική τους έννομη τάξη, παρά το γεγονός ότι η προθεσμία ενσωμάτωσης παρήλθε για περισσότερα από τέσσερα έτη²⁹. Περαιτέρω, παρατηρήθηκε ότι η αρχή της διαθεσιμότητας δεν τέθηκε στην πράξη σε ισχύ από πολλά Κράτη-μέλη, κυρίως λόγω της έλλειψης διάθεσης από τις δικαστικές αρχές να εφαρμόσουν τα χρονικά όρια απάντησης που θέτει η Απόφαση-Πλαίσιο³⁰.

2. Σκοπός και περιεχόμενο της Απόφασης 2008/615/ΔΕΥ

2.1. Γενικές παρατηρήσεις

Αν κι όπως επισημάνθηκε παραπάνω, τα Κράτη-μέλη φάνηκαν απρόθυμα να εφαρμόσουν τόσο την Απόφαση-Πλαίσιο 2006/960/ΔΕΥ, όσο και να συμμετάσχουν στη Συνθήκη Prüm, οι βασικές διατάξεις της τελευταίας³¹ (σχεδόν ολόκληρη και πλην κυρίως των sky marshals, των ένοπλων δηλαδή φρουρών σε πτήσεις αεροσκαφών πολιτικής αεροπορίας) «κοινοτικοποιήθηκαν» με τις Αποφάσεις 2008/615/ΔΕΥ, 2008/616/ΔΕΥ και 2008/617/ΔΕΥ, της 23^{ης} Ιουνίου 2008, οι οποίες είθισται να αποκαλούνται Αποφάσεις Prüm. Οι βασικές κανονιστικές διατάξεις βρίσκονται στην Απόφαση 615, ενώ οι Αποφάσεις 616 και 617 ορίζουν τεχνικές λεπτομέρειες εφαρμογής της, όπως π.χ. για τη συλλογή δεδομένων DNA, κ.λπ.

Η Απόφαση 2008/615/ΔΕΥ χωρίζεται κατά περιεχόμενο σε επτά κεφάλαια, στα οποία περιγράφονται αντίστοιχα οι γενικές πτυχές, η επιγραμμική πρόσβαση και οι αιτήσεις των επακόλουθων ενεργειών, οι ενέργειες κατά τα σημαντικά γεγονότα, τα μέτρα πρόληψης τρομοκρατικών

²⁹ Στην Ελλάδα, η Απόφαση – Πλαίσιο 2006/960/ΔΕΥ ενσωματώθηκε στην εθνική έννομη τάξη μόλις το Σεπτέμβριο του 2013 με το Π.Δ. 135/2009 (ΦΕΚ 209 Α'/30-9-13).

³⁰ Έγγραφο 14755/1/12, ό.π., σελ. 4

³¹ Δεν κοινοτικοποιήθηκαν οι διατάξεις για τους ένοπλους συνοδούς πτήσεων (sky marshals), καθώς και οι διατάξεις για την ανταλλαγή δεδομένων για θέματα ασύλου, οι οποίες ήδη τότε ενέπιπταν στο πεδίο του Α' Πυλώνα. Ειδικότερα, οι ένοπλοι συνοδοί (οι οποίοι ήταν ουσιαστικά απαίτηση των ΗΠΑ) αποτέλεσαν πεδίο δυναμικών αντιπαραθέσεων μεταξύ των σκανδιναβικών χωρών και των επτά συμβαλλόμενων μερών της Συνθήκης, κυρίως όσον αφορά τη συνεργασία κι έτσι δεν επιχειρήθηκε καν η εισαγωγή τους στο σχέδιο απόφασης. Περισσότερα επί της σχετικής προβληματικής σε Balzacq Thierry, Bigo Didier, Carrera Sergio and Guild Elspeth, Security and the Two-level Game: The Treaty of Prüm, the EU and the Management of Threats, Ιανουάριος 2006, Έκθεση για το Ευρωπαϊκό Κέντρο Σπουδών Πολιτικής (Centre for European Policy Studies, σελ. 10-11, <http://www.ceps.be/book/security-and-two-level-game-treaty-pr%C3%BCm-eu-and-management-threats>).

πράξεων, άλλες μορφές συνεργασίας, οι γενικές διατάξεις σχετικά με την προστασία προσωπικών δεδομένων, καθώς και οι τελικές διατάξεις.

Σκοπός της Απόφασης 2008/615/ΔΕΥ είναι η αναβάθμιση της διασυνοριακής συνεργασίας μεταξύ των κρατών μελών σε θέματα που καλύπτονται από τον τίτλο VI της ΣυνEE (Διατάξεις για την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις) και ιδίως στην ανταλλαγή πληροφοριών για τη διερεύνηση αξιόποινων πράξεων. Προς τούτο, περιέχει κανόνες στους ακόλουθους τομείς:

α) Όροι και διαδικασία αυτοματοποιημένης διαβίβασης προφίλ DNA, δεδομένων δακτυλικών αποτυπωμάτων και ορισμένων δεδομένων σχετικά με τις άδειες κυκλοφορίας οχημάτων (Κεφάλαιο 2),

β) Παροχή δεδομένων σχετικά με σημαντικά γεγονότα με διασυνοριακή διάσταση (Κεφάλαιο 3),

γ) Όροι παροχής πληροφοριών για την πρόληψη τρομοκρατικών πράξεων (Κεφάλαιο 4) και

δ) Όροι και διαδικασία αναβάθμισης της διασυνοριακής συνεργασίας μέσω διάφορων μέτρων (Κεφάλαιο 5).³²

2.2. Ανταλλαγή δεδομένων DNA, δακτυλικών αποτυπωμάτων και οχημάτων

Προκειμένου να επιτευχθεί επιγραμμική πρόσβαση στα δεδομένα, τα Κράτη-μέλη δημιουργούν και τηρούν εθνικά αρχεία DNA, η επεξεργασία των οποίων πραγματοποιείται σύμφωνα με τις εθνικές διατάξεις περί επεξεργασίας δεδομένων³³. Περαιτέρω, εξασφαλίζουν τη διαθεσιμότητα δεδομένων αναφοράς³⁴ τόσο από τα αρχεία δεδομένων DNA³⁵, όσο και από τα αρχεία για

³² Άρθρο 1 Απόφασης Prüm.

³³ Άρθρο 2 παρ. 1 Απόφασης Prüm.

³⁴ Σύμφωνα με την παρ. 2 του άρθρου 2 της Απόφασης Prüm, τα δεδομένα αναφοράς περιλαμβάνουν μόνο τα προφίλ DNA που έχουν καταρτιστεί από το μη κωδικοποιητικό τμήμα του DNA και αριθμό αναφοράς. Επίσης, σύμφωνα με το άρθρο 2 περ. γ' της Απόφασης 2008/616/ΔΕΥ του Συμβουλίου της 23^{ης} Ιουνίου 2008 για την εφαρμογή της Απόφασης Prüm, ως «προφίλ DNA» νοείται κωδικός αποτελούμενος από γράμματα ή αριθμούς, ο οποίος αντιστοιχεί σε σειρά χαρακτηριστικών ταυτοποίησης του μη κωδικοποιητικού τμήματος αναλυθέντος δείγματος ανθρώπινου DNA, λ.χ. της ιδιαίτερης μοριακής δομής στους διάφορους τόπους DNA (*loci*), ενώ, σύμφωνα με την περ. δ' του ίδιου άρθρου, ως «μη κωδικοποιητικό

τα εθνικά συστήματα αυτοματοποιημένης αναγνώρισης δακτυλικών αποτυπωμάτων³⁶. Επιπλέον, η Απόφαση ορίζει ρητά³⁷ πως τα δεδομένα αναφοράς δεν πρέπει να περιέχουν δεδομένα που να επιτρέπουν την άμεση αναγνώριση του προσώπου στο οποίο αναφέρονται, ενώ υφίσταται και υποχρέωση επισήμανσης δεδομένων αναφοράς DNA, τα οποία δεν αποδίδονται σε συγκεκριμένο πρόσωπο³⁸.

Τα Κράτη-μέλη ορίζουν σημεία επαφής³⁹ για την παροχή δεδομένων σχετικά με τα δεδομένα DNA και δακτυλικών αποτυπωμάτων, τα οποία παρέχουν στα εθνικά σημεία επαφής των λοιπών Κρατών μελών πρόσβαση στα δεδομένα αναφοράς με εξουσία διεξαγωγής αυτοματοποιημένων αναζητήσεων,⁴⁰ μέσω σύγκρισης⁴¹ των προφίλ DNA και μέσω των συστημάτων αναγνώρισης δακτυλικών αποτυπωμάτων.

Εάν διαπιστωθεί κατά την αναζήτηση είτε δεδομένων DNA, είτε δεδομένων δακτυλικών αποτυπωμάτων, η παροχή περαιτέρω δεδομένων προσωπικού χαρακτήρα και άλλων πληροφοριών σχετικά με τα δεδομένα αναφοράς, τούτη διέπεται από το δίκαιο του κράτους προς το οποίο απευθύνεται η αίτηση, δηλ. το κράτος στου οποίου τη βάση δεδομένων υφίσταται το πρόσωπο, συμπεριλαμβανομένων των κανόνων περί νομικής συνδρομής⁴².

τμήμα DNA» νοούνται περιοχές χρωμοσωμάτων που δεν είναι εκφρασμένες γενετικά, δηλαδή δεν είναι γνωστό αν καλύπτουν οποιεσδήποτε λειτουργικές ιδιότητες ενός οργανισμού.

³⁵ Άρθρο 2 παρ. 2 Απόφασης Prüm.

³⁶ Άρθρο 8 Απόφασης Prüm.

³⁷ Άρθρο 2 παρ. 2 εδ. γ' και άρθρο 8 εδ. γ' Απόφασης Prüm.

³⁸ Η περίπτωση αυτή αναφέρεται στα αταυτοποιητά προφίλ DNA τα οποία, σύμφωνα με την περ. ζ' του άρθρου 2 της Απόφασης 2008/616/ΔΕΥ, είναι προφίλ DNA που λαμβάνονται από ίχνη που έχουν συλλεγεί στο πλαίσιο έρευνας για αξιόποινες πράξεις και ανήκουν σε μη ταυτοποιημένα προς το παρόν πρόσωπα.

³⁹ Άρθρο 6 παρ. 1 και άρθρο 11 παρ. 1 Απόφασης Prüm.

⁴⁰ Σύμφωνα με την περ. β' του άρθρου 2 της Απόφασης 2008/616/ΔΕΥ, ως «αυτοματοποιημένη αναζήτηση» νοείται η διαδικασία επιγραμματικής πρόσβασης με την οποία μπορεί να συμβουλευτεί κανείς τις βάσεις δεδομένων ενός, περισσοτέρων ή όλων των κρατών μελών.

⁴¹ Σύμφωνα με την περ. α' του άρθρου 2 της Απόφασης 2008/616/ΔΕΥ, ως «αναζήτηση» και «σύγκριση» δεδομένων DNA και δακτυλικών αποτυπωμάτων νοούνται οι διαδικασίες με τις οποίες εξακριβώνεται κατά πόσον υπάρχει αντιστοιχία μεταξύ, αφενός, δεδομένων DNA ή δεδομένων σχετικών με δακτυλικά αποτυπώματα που έχουν κοινοποιηθεί από ένα κράτος μέλος και, αφετέρου, δεδομένων DNA ή δεδομένων σχετικών με δακτυλικά αποτυπώματα που έχουν αποθηκευτεί στις βάσεις δεδομένων ενός ή περισσοτέρων ή όλων των κρατών μελών.

⁴² Άρθρο 5 και άρθρο 10 Απόφασης Prüm.

Αντίστοιχα, όπως με τα δεδομένα DNA και δακτυλικών αποτυπωμάτων, τα Κράτη-μέλη παρέχουν πρόσβαση αυτοματοποιημένων αναζητήσεων σε δεδομένα σχετικά με άδειες κυκλοφορίας οχημάτων και συγκεκριμένα σε δεδομένα σχετικά με ιδιοκτήτες ή χρήστες και οχήματα. Οι αναζητήσεις διεξάγονται μόνο με πλήρες αριθμό αμαξώματος (αριθμό πλαισίου) ή πλήρη αριθμό άδειας κυκλοφορίας⁴³. Η αναζήτηση πραγματοποιείται, όπως και στην περίπτωση των δεδομένων DNA και δακτυλικών αποτυπωμάτων, σύμφωνα με το δίκαιο του αιτούντος κράτους, ενώ και στην περίπτωση αυτή ορίζεται εθνικό σημείο επαφής⁴⁴.

2.3. Ανταλλαγή δεδομένων στο πλαίσιο σημαντικών γεγονότων

Το Κεφάλαιο 3 της Απόφασης Prüm αναφέρεται στην παροχή δεδομένων προσωπικού χαρακτήρα ή μη, αυτοβούλως ή κατόπιν αιτήσεως, για τη διατήρηση της δημόσιας τάξης και ασφάλειας σε σημαντικά γεγονότα με διασυνοριακή διάσταση και ιδίως αθλητικές εκδηλώσεις ή συνόδους του Ευρωπαϊκού Συμβουλίου. Όσον αφορά την παροχή δεδομένων προσωπικού χαρακτήρα, τούτη πραγματοποιείται όταν από αμετάκλητες καταδικαστικές αποφάσεις ή άλλες αποφάσεις προκύπτουν εύλογες υπόνοιες ότι τα πρόσωπα αυτά θα διαπράξουν αξιόποινες πράξεις στο πλαίσιο των σημαντικών γεγονότων ή θα θέσουν σε κίνδυνο τη δημόσια τάξη και ασφάλεια, εφόσον η παροχή των δεδομένων αυτών επιτρέπεται από το εθνικό δίκαιο του παρέχοντος Κράτους-μέλους⁴⁵.

Στο σημείο αυτό, αξίζει να επισημανθεί ότι η έννοια της «δημόσιας τάξης και ασφάλειας», αν και αναφέρεται πολύ συχνά σε νομικά κείμενα, δεν είναι αποσαφηνισμένη. Κατά τον Ι. Μανωλεδάκη⁴⁶ η ασφάλεια εμφανίζει δύο βασικές όψεις: η μία αποτυπώνει την αποτελεσματική αντιμετώπιση των πολυποίκιλων διακινδυνεύσεων, ενώ η άλλη την εγγύηση των δικαιωμάτων των πολιτών. Στην πρώτη μπορεί να ενταχθεί και η ασφάλεια της ίδιας της πολιτείας, ως δημόσια

⁴³ Άρθρο 12 παρ. 1 Απόφασης Prüm.

⁴⁴ Άρθρο 12 παρ. 2 Απόφασης Prüm.

⁴⁵ Άρθρα 13 και 14 παρ. 1 Απόφασης Prüm.

⁴⁶ βλ. Ι. Μανωλεδάκη, Δημοκρατία-Ελευθερία-Ασφάλεια, το τρίπτυχο της ιδανικής πολιτείας, στον τιμητικό τόμο για τον ίδιο, Δημοκρατία-Ελευθερία-Ασφάλεια, Σάκκουλας, 2005, σελ. 60-61

ασφάλεια, δηλαδή ως προστασία των θεσμών και της κυριαρχίας μιας πολιτείας από εσωτερικές υπονομεύσεις (εσωτερική ασφάλεια) και εξωτερικές αμφισβητήσεις (εξωτερική ασφάλεια). Στο ίδιο πλαίσιο προστίθεται η επισήμανση της Α. Τάχου⁴⁷ πως η δημόσια ασφάλεια προσβλέπει στην εξασφάλιση της συμμόρφωσης του πολίτη προς τις επιταγές της δημόσιας τάξης, μέσω της οποίας το κράτος συντηρεί και διαφυλάσσει την ίδια του την ύπαρξη. Η μη ύπαρξη σαφούς ορισμού της έννοιας της «δημόσιας τάξης και ασφάλειας», όχι μόνο σε εθνικό, αλλά και σε ευρωπαϊκό επίπεδο, επιβεβαιώνεται κι από το ΔΕΚ στην απόφασή του στην υπόθεση REZGUIA ADOUI της 18/5/1982 (C-115/81 - απόσπασμά της αναπαράγεται στην ΑΠ 1067/1996), όπου σημειώνει πως το κοινοτικό δίκαιο δεν επιβάλλει στα Κράτη-μέλη μια ομοιόμορφη κλίμακα αξιών σε ό,τι αφορά την αξιολόγηση συμπεριφορών που θα μπορούσαν να θεωρηθούν ως αντίθετες προς της δημόσια τάξη. Το ΔΕΚ εκτιμά πως η προσφυγή από μια εθνική αρχή στην έννοια της δημόσιας τάξης προϋποθέτει την ύπαρξη μιας πραγματικής και επαρκώς σοβαρής απειλής που επηρεάζει ένα θεμελιώδες συμφέρον της κοινωνίας και απαιτεί να τηρείται η αρχή της αναλογικότητας.

Τα προαναφερόμενα δεδομένα προσωπικού χαρακτήρα τυγχάνουν επεξεργασίας μόνο για το συγκεκριμένο γεγονός, για το οποίο παρασχέθηκαν και διαγράφονται μόλις επιτευχθούν ή είναι πλέον αδύνατον να επιτευχθούν οι σκοποί για τους οποίους δόθηκαν ή, σε κάθε περίπτωση, το αργότερο εντός ενός έτους από τη λήψη τους⁴⁸. Εθνικά σημεία επαφής ορίζονται και σε αυτή την περίπτωση⁴⁹.

Αξιοπρόσεκτη είναι η διάταξη της παρ. 1 του άρθρου 14, η οποία παρουσιάζει και το μεγαλύτερο ενδιαφέρον. Σε όλα τα Κράτη-μέλη⁵⁰ υφίσταται νομικό πλαίσιο, στο οποίο προβλέπεται η ανταλλαγή πληροφοριών για οπαδούς ομάδων που έχουν στο παρελθόν καταδικαστεί για βίαιες πράξεις σε αθλητικούς χώρους, καθώς γίνεται κατανοητό ότι οι έννομες τάξεις έχουν αποδεχθεί πως, αν ένας οπαδός έχει προβεί σε έκνομες ενέργειες στο παρελθόν υποστηρίζοντας

⁴⁷ βλ. Α. Τάχου, Δίκαιο της δημόσιας τάξης, Σάκκουλας, 1990, σελ. 22

⁴⁸ Άρθρο 14 παρ. 2 Απόφασης Prüm.

⁴⁹ Άρθρο 15 Απόφασης Prüm.

⁵⁰ Για την εσωτερική μας έννομη τάξη βλ. ειδικότερα άρθρο 8 του Ν. 3708/2008 για την «Καταπολέμηση της βίας με αφορμή αθλητικές εκδηλώσεις και άλλες διατάξεις»

έναν αθλητικό σύλλογο, ενδεχομένως θα προβεί και σε ανάλογες ενέργειες στο μέλλον, όταν αγωνίζεται ο σύλλογος αυτός. Στην Απόφαση Prüm μάλιστα, παρατηρείται μία επέκταση του πεδίου εφαρμογής και σε άλλες περιπτώσεις που αφορούν τη συμμετοχή σε διαδηλώσεις, π.χ. σε συνόδους του Ευρωπαϊκού Συμβουλίου. Οι διατάξεις αυτές δέχονται κριτική από ένα μέρος της θεωρίας⁵¹, όπου υποστηρίζεται ότι πρόκειται περί ξεκάθαρης ποινικοποίησης του φρονήματος (κατά παράβαση του άρθρου 7 Συντ.) και κατά συνέπεια περί αντισυνταγματικών διατάξεων.

2.4. Μέτρα πρόληψης τρομοκρατικών πράξεων

Το 4^ο Κεφάλαιο της Απόφασης Prüm (άρθρο 16) αφορά στην παροχή δεδομένων προσωπικού χαρακτήρα, σε ατομικές περιπτώσεις, μέσω εθνικών σημείων επαφής (παρ. 3), κατόπιν αιτήσεως ή και αυτοβούλως, εφόσον αυτό απαιτείται από ειδικές περιστάσεις. Ειδικότερα, προς τούτο θα πρέπει να προκύπτουν εύλογες υπόνοιες ότι τα άτομα, στα οποία αναφέρονται τα δεδομένα, θα διαπράξουν αξιόποινες πράξεις σύμφωνα με τα άρθρα 1 – 3 της Απόφασης – Πλαίσιο 2002/475/ΔΕΥ του Συμβουλίου της 13^{ης} Ιουνίου 2002 για την καταπολέμηση της τρομοκρατίας. Τούτο σημαίνει πρακτικά ότι πρόκειται για υπόνοιες περί τέλεσης εγκλημάτων στο μέλλον.

Τα δεδομένα αυτά πρέπει να περιλαμβάνουν, σύμφωνα με την παράγραφο 2, ονοματεπώνυμο, ημερομηνία γέννησης και περιγραφή των περιστάσεων, υπό τις οποίες προκύπτουν οι εν λόγω εύλογες υπόνοιες. Η παροχή των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται, κατά την παρ. 4, σύμφωνα με το δίκαιο του παρέχοντος κράτους μέλους, το οποίο μπορεί να θέσει και όρους για τη χρήση τους, δεσμευτικούς για το παραλαμβάνον κράτος.

2.5. Κοινές Επιχειρήσεις

Στο Κεφαλαίο 5 υπό τον τίτλο «Άλλες μορφές συνεργασίας» καθορίζεται η δυνατότητα των κρατών μελών να διεξάγουν κοινές επιχειρήσεις και κοινές περιπολίες για την τήρηση της δημόσιας τάξης και ασφάλειας καθώς και για την πρόληψη αξιοποιήσιμων πράξεων, με τη συμμετοχή υπαλλήλων από άλλα Κράτη-

⁵¹ Βλ. ενδεικτικά Δ. Καλτσώνης, Βία στα γήπεδα, οργανωμένο έγκλημα και τρομοκρατία, Συλλογικός Τόμος Οπαδική Βία, εκδ. Νόβολι, 2010, σελ. 109-121

μέλη⁵². Βάσει της πρόβλεψης αυτής, τα Κράτη-μέλη μπορούν, σύμφωνα με το εθνικό τους δίκαιο, να διοργανώνουν κοινές επιχειρήσεις στο έδαφός τους και στο πλαίσιο αυτών να αναθέτουν εκτελεστικές εξουσίες σε υπαλλήλους άλλων κρατών μελών, ώστε να εκτελούν ενέργειες σύμφωνα με το δίκαιό τους (νοείται το δίκαιο του κράτους υποδοχής). Οι εν λόγω εκτελεστικές εξουσίες ασκούνται μόνον υπό την καθοδήγηση και – κατά κανόνα – παρουσία των υπαλλήλων του κράτους υποδοχής, ενώ το τελευταίο αναλαμβάνει και την ευθύνη για τις πράξεις τους ⁵³. Οι αποσπώμενοι υπάλληλοι δύνανται να φέρουν οπλισμό και άλλο εξοπλισμό (συμπεριλαμβανομένων οχημάτων) που επιτρέπεται να φέρουν στη χώρα τους, εφόσον τούτο επιτρέπεται από το δίκαιο του κράτους υποδοχής⁵⁴. Τα Κράτη-μέλη που διοργανώνουν και διεξάγουν τέτοιες κοινές επιχειρήσεις ρυθμίζουν με διμερείς συμφωνίες τις πρακτικές πτυχές της συνεργασίας τους και ενημερώνουν σχετικά το Συμβούλιο της Ε.Ε.⁵⁵

Κοινές επιχειρήσεις, υπό τη μορφή των παράλληλων ενεργειών κάθε κράτους μέλους στο έδαφός του, μπορούν να λάβουν χώρα και σε σχέση με μαζικές συγκεντρώσεις, καταστροφές και σοβαρά ατυχήματα. Στις περιπτώσεις αυτές, τα Κράτη-μέλη οφείλουν να ενημερώνουν τα άλλα Κράτη-μέλη για περιστατικά, τα οποία έχουν διασυννοριακό αντίκτυπο, προκειμένου να λάβουν τα απαραίτητα μέτρα αστυνόμευσης. Επίσης, στο πλαίσιο της αλληλεγγύης, δύνανται να αποσπούν το ένα στο άλλο, σύμφωνα πάντα με το εθνικό δίκαιο και κατ' αίτηση του κράτους υποδοχής, εμπειρογνώμονες, συμβούλους και υπαλλήλους, καθώς και να παρέχουν εξοπλισμό για την αντιμετώπιση των έκτακτων αυτών περιστατικών⁵⁶.

Τα άρθρα 20 έως 23 θεσπίζουν κανόνες ποινικής, αστικής και πειθαρχικής ευθύνης των αποσπώμενων υπαλλήλων. Επίσης προβλέπεται μια γενική ρήτρα παροχής από το κράτος υποδοχής συνδρομής στους αποσπώμενους υπαλλήλους, αντίστοιχης με αυτή που παρέχει στους δικούς του υπαλλήλους.

Αν και οι κοινές επιχειρήσεις του άρθρου 17 της Απόφασης Prüm δεν εμπίπτουν στην προβληματική της παρούσας εργασίας για την προστασία των

⁵² Άρθρο 17 παρ. 1 Απόφασης Prüm.

⁵³ Άρθρο 17 παρ. 2 και 3 Απόφασης Prüm.

⁵⁴ Άρθρο 19 Απόφασης Prüm.

⁵⁵ Άρθρο 17 παρ. 4 Απόφασης Prüm.

⁵⁶ Άρθρο 18 Απόφασης Prüm.

προσωπικών δεδομένων, δεν μπορεί να μην υπογραμμιστεί ότι οι σχετικές διατάξεις παρουσιάζουν ιδιαίτερο ενδιαφέρον. Μετά τη Σύμβαση Εφαρμογής της Συνθήκης Σένγκεν και ιδίως με τα άρθρα 40 και 41 αυτής, όπου περιγράφονται η διασυνοριακή καταδίωξη (hot pursuit) και η διασυνοριακή παρακολούθηση, οι κοινές επιχειρήσεις του άρθρου 17 της Απόφασης Prüm είναι ένα σημαντικό εργαλείο που δίνει τη δυνατότητα στα Κράτη-μέλη να διενεργούν αστυνομικές επιχειρήσεις σε έδαφος άλλου κράτους μέλους⁵⁷. Οι επιχειρήσεις διενεργούνται σαφώς βάσει του δικαίου του κράτους υποδοχής, αλλά η σημασία της διάταξης έγκειται προφανώς στην παραχώρηση εκτελεστικών εξουσιών σε υπηκόους άλλου κράτους μέλους. Τούτο αποτελεί συνέχεια των κοινών δράσεων που πραγματοποιούνται στο πλαίσιο της Frontex για την προστασία των συνόρων και κινείται στο πλαίσιο της ανάπτυξης ενός κοινού ευρωπαϊκού χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, όπου τα εθνικά σύνορα δεν αποτελούν όριο.

⁵⁷ Δυνατότητα επέμβασης στο έδαφος άλλου Κράτους-μέλους, υπό την ίδια λογική, παρέχει και το άρθρο 222 ΣΛΕΕ (Ρήτρα αλληλεγγύης) το οποίο προβλέπει τη χορήγηση εκτελεστικών αρμοδιοτήτων σε υπηκόους άλλου Κράτους-μέλους σε έκτακτη βάση και για την αντιμετώπιση συγκεκριμένου κινδύνου.

III. Προστασία προσωπικών δεδομένων στην Ε.Ε.

1. Επί των πρωτοβουλιών σε ευρωπαϊκό περιφερειακό επίπεδο

Ως γνωστόν, μέχρι και τη Συνθήκη του Άμστερνταμ και την εγκαθίδρυση του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, η προστασία των προσωπικών δεδομένων σε επίπεδο Ε.Ε. είχε αποτελέσει αντικείμενο νομικής πράξης στο πλαίσιο του τότε Α΄ Πυλώνα της Ένωσης, τον λεγόμενο Κοινοτικό, στον οποίο και καθορίζονταν κατά βάση οι οικονομικές πολιτικές της Ε.Ε. Το κύριο νομοθετικό κείμενο που καθόριζε την προστασία των προσωπικών δεδομένων ήταν η Οδηγία 95/46/ΕΚ, η οποία αποτέλεσε και τη βάση του ελληνικού νόμου 2472/1997.

Η Οδηγία 95/46 όμως, δεν ήταν το πρώτο κείμενο, με το οποίο επιχειρήθηκε να ορισθεί το καθεστώς προστασίας προσωπικών δεδομένων και δεν θα μπορούσε άλλωστε, ιδιαίτερα αν αναλογιστούμε ότι όλα τα προαναφερόμενα εργαλεία ανταλλαγής πληροφοριών αστυνομικής συνεργασίας προϋπήρχαν της Οδηγίας⁵⁸. Οι πρώτες προσπάθειες για τη θέσπιση νομοθεσίας σε ευρωπαϊκό περιφερειακό επίπεδο περί προστασίας προσωπικών δεδομένων χρονολογούνται στη δεκαετία του 1960⁵⁹, όπου οι «πρόγονοι» των υπολογιστών είχαν δείξει ότι μπορούν να απειλήσουν την ιδιωτικότητα, σε ένα, μέχρι τότε, άγνωστο βαθμό. Παρά το γεγονός ότι το δικαίωμα της ιδιωτικότητας είχε καθιερωθεί στις περισσότερες χώρες του δυτικού κόσμου, οι υπολογιστές έδωσαν τη δυνατότητα μαζικής αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων που ξεπερνούσε συχνά τα όρια μιας εθνικής νομοθεσίας⁶⁰, οδηγώντας έτσι τις χώρες της Ευρώπης να αναζητήσουν μια συνολική προσέγγιση. Η προσέγγιση αυτή αποτυπώθηκε στη Σύμβαση 108 του Συμβουλίου της Ευρώπης του 1981 για την αυτοματοποιημένη επεξεργασία

⁵⁸ Η Συνθήκη Σένγκεν χρονολογείται το 1985 και η Ιντερπόλ το 1964. Παράλληλα, η Ευρωπόλ, στην πρώτη της μορφή ως ΤΡΕVΙ δημιουργήθηκε τη δεκαετία του 80, ενώ ήδη από το 1990 λειτουργούσε ως ευρωπαϊκή Υπηρεσία καταπολέμησης των ναρκωτικών (European Drug Unit – EDU).

⁵⁹ Αναλυτικότερη αναφορά στην εξέλιξη της προστασίας των προσωπικών δεδομένων βλ. Σωτηρόπουλο Βασίλη, Η συνταγματική προστασία των προσωπικών δεδομένων, Σάκκουλας, 2006, σελ. 11.

⁶⁰ Paul de Hert, Vagelis Papakonstantinou, *The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for*, Διαδικτυακό περιοδικό Computer Law & Security Review, 2009, τ. 25, σ.403-414

προσωπικών δεδομένων κι εν συνεχεία στη Σύσταση 15 του 1987 της Επιτροπής Υπουργών. Τα κείμενα αυτά μάλιστα υπήρξαν πρωτοποριακά, ειδικότερα αν αναλογιστεί κανείς ότι κανένας άλλος διεθνής οργανισμός δεν κατάρτισε μέχρι σήμερα ανάλογο δεσμευτικό κείμενο.

Αξίζει στο σημείο αυτό να σημειωθεί η σημασία του ρόλου του Συμβουλίου της Ευρώπης στην προστασία των ανθρωπίνων δικαιωμάτων, της κοινοβουλευτικής δημοκρατίας και του κράτους δικαίου. Είναι γεγονός ότι μέχρι σήμερα, το Συμβούλιο της Ευρώπης έχει κατορθώσει να συντάξει μεγάλο αριθμό νομικά δεσμευτικών Ευρωπαϊκών Συμβάσεων, οι οποίες αποτελούν την βάση της μεταρρύθμισης και εναρμόνισης νομοθεσιών των κρατών μελών σε σειρά θεμάτων όπως τα ανθρώπινα δικαιώματα, η καταπολέμηση των βασανιστηρίων, η καταπολέμηση του οργανωμένου εγκλήματος, η προστασία των δεδομένων, η πολιτιστική συνεργασία και άλλοι τομείς. Επίσης, τα κείμενα αυτά έχουν αποτελέσει τη βάση για την κατάρτιση αντίστοιχων νομοθετημάτων σε επίπεδο Ευρωπαϊκής Ένωσης, με ενδεικτικό παράδειγμα τη Σύμβαση 108, η οποία αποτέλεσε τη βάση κατάρτισης της Οδηγίας 95/46/EK για την προστασία προσωπικών δεδομένων.

2. Τα κείμενα του Συμβουλίου της Ευρώπης επί της επιτασσόμενης προστασίας στον αστυνομικό τομέα

2.1. Κανονιστικό περιεχόμενο της Σύμβασης 108 του έτους 1981

Η Σύμβαση 108 του Συμβουλίου της Ευρώπης⁶¹ αποτελεί το πρώτο διεθνές νομικό κείμενο για την προστασία προσωπικών δεδομένων το οποίο τυγχάνει εφαρμογής και στον αστυνομικό τομέα, μιας και στο άρθρο 3 (πεδίο εφαρμογής) περιλαμβάνεται η αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων και στο δημόσιο τομέα. Η Σύμβαση έθεσε ορισμένες βασικές αρχές της προστασίας των προσωπικών δεδομένων, όπως την αρχή της θεμελίωσης της επεξεργασίας σε νόμο, την αρχή του σκοπού, της αναλογικότητας, της ακρίβειας των δεδομένων που συλλέγονται, καθώς και της διατήρησης των δεδομένων μόνο

⁶¹ Σύμβαση 108 του Συμβουλίου της Ευρώπης της 28^{ης} Ιανουαρίου 1981 «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα» (CETS 108) (www.conventions.coe.int). Η εν λόγω Σύμβαση κυρώθηκε με το Ν. 2068/1992 (ΦΕΚ 118/9-7-92) και τέθηκε σε ισχύ στη Χώρα μας την 01/12/1995 (ως εμφανίζεται στον πίνακα κυρώσεων της Σύμβασης στον προαναφερόμενο ιστότοπο).

για το αναγκαίο για την επίτευξη του σκοπού της επεξεργασίας χρονικό διάστημα⁶².

Παράλληλα, στις διατάξεις της ορίζονται ειδικές κατηγορίες προσωπικών πληροφοριών που δεν μπορούν να αποτελέσουν αντικείμενο αυτοματοποιημένης επεξεργασίας, στην περίπτωση που το εθνικό δίκαιο δεν παρέχει κατάλληλες εγγυήσεις⁶³, ενώ αναγνωρίζει δικαιώματα και στα πρόσωπα, στα οποία αναφέρονται τα δεδομένα⁶⁴. Συγκεκριμένα πρόκειται για την προστασία του ατόμου από αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ή προσβολές της τιμής και της υπόληψής του⁶⁵.

Περαιτέρω, μία από τις σημαντικότερες καινοτομίες που εισάγει η Σύμβαση είναι η πρόβλεψη δημιουργίας μίας ή περισσότερων ανεξάρτητων Αρχών για την εποπτεία των διατάξεων της Σύμβασης, ιδίως επί της διασυννοριακής ροής των πληροφοριών, η οποία γίνεται ελεύθερη με εξαιρέσεις για την προστασία πληροφοριών προσωπικού χαρακτήρα.

Η διασυννοριακή ροή πληροφοριών ρυθμίστηκε περαιτέρω με το Πρόσθετο Πρωτόκολλο στη Σύμβαση 108, το οποίο υιοθετήθηκε το έτος 2001⁶⁶. Μία από τις σημαντικότερες διατάξεις του Πρόσθετου Πρωτοκόλλου είναι η αυτή της παρ. 1 του άρθρου 2, με την οποία, για τη διαβίβαση προσωπικών δεδομένων σε τρίτα κράτη (δηλ. μη συμβαλλόμενα στη Σύμβαση 108), πρέπει να

⁶² Γνωμοδότηση 1/2009 ΑΠΔΠΧ, σελ. 12, ιστότοπος της Αρχής (<http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=149,197,97,16,81,229,57,90>)

⁶³ Άρθρο 6 της Σύμβασης.

⁶⁴ Άρθρο 8 και 9 της Σύμβασης.

⁶⁵ Βλ. σχετ. Γέροντα Α., «Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων», Αθήνα-Κομοτηνή, 2002, σελ. 101, 108

⁶⁶ Πρόσθετο Πρωτόκολλο στη Σύμβαση για την προστασία των ατόμων σχετικά με την αυτόματη επεξεργασία προσωπικών δεδομένων, αναφορικά με τις εποπτικές αρχές και τη διασυννοριακή ροή δεδομένων (CETS 181), 08/11/2001. Η Χώρα μας υπέγραψε μεν το εν λόγω Πρωτόκολλο, πλην όμως δεν έχει ακόμη ενσωματωθεί στην εθνική μας έννομη τάξη. Αν και η ΑΠΔΠΧ στη Γνωμοδότηση 1/2009 επισήμανε την αξία του Πρόσθετου Πρωτοκόλλου στην αναγνώριση της σημασίας ύπαρξης ανεξάρτητων εποπτικών αρχών για την αποτελεσματική προστασία των προσωπικών δεδομένων, από κάποιους δεν θεωρείται αναγκαία η κύρωσή του, δεδομένων αφενός μεν των αναφορών του Επεξηγηματικού Υπομνήματος της Σύμβασης 108 σε εποπτική αρχή (π.χ. για τις ειδικές κατηγορίες δεδομένων του άρθρου 8) κι αφετέρου του άρθρου 8 παρ. 3 του Χάρτη Θεμελιωδών Ελευθεριών της Ε.Ε. που αναφέρει τη λειτουργία ανεξάρτητης αρχής (βλ. Βασίλης Σωτηρόπουλος, 29/07/2009, ιστολόγιο E-Lawyer [elawyer.blogspot.gr/2009/07/blog-post_29.html]).

διασφαλίζεται από αυτά επαρκές επίπεδο προστασίας προσωπικών δεδομένων. Η διάταξη αυτή βέβαια φαίνεται έξοχη κι αργότερα μάλιστα συμπεριλήφθη και στο άρθρο 26 παρ. 4 της Οδηγίας 95/46/EK που θα αναλυθεί παρακάτω. Όμως δεν θεσμοθετήθηκε μηχανισμός, ο οποίος θα διασφαλίζει την επάρκεια της προστασίας προσωπικών δεδομένων στο τρίτο κράτος κι άρα επαφίεται στα Κράτη που είναι συμβαλλόμενα στη Σύμβαση να διαπιστώσουν τυχόν παραβίαση⁶⁷.

Επιπλέον, άξια μνείας είναι και η διάταξη της παρ. 2 του άρθρου 2 του Πρόσθετου Πρωτοκόλλου σχετικά με τις εξαιρέσεις διαβίβασης δεδομένων σε περιπτώσεις προστασίας ειδικών συμφερόντων του υποκειμένου των δεδομένων (π.χ. σε περιπτώσεις που δεν είναι σε θέση να ταυτοποιήσει τον εαυτό του λόγω αμνησίας) ή σε περιπτώσεις όπου υφίσταται υπέρτερο δημόσιο συμφέρον, εφόσον τούτα επιτρέπονται από την εθνική νομοθεσία του κράτους που διαβιβάζει τα δεδομένα. Η διάταξη αυτή αναπαράγεται κατ' ουσία πλέον στα περισσότερα κείμενα διεθνούς αστυνομικής συνεργασίας.

Σε γενικές γραμμές, η Σύμβαση 108 παρουσιάζει μία σημαντική προστιθέμενη αξία, ειδικότερα σε σχέση με την Ε.Ε., όπου δεν υπήρχε ανάλογο νομοθέτημα, με διαπυλωνικό μάλιστα χαρακτήρα. Ωστόσο, οι διατάξεις της θεωρούνται ήδη απαρχαιωμένες⁶⁸, δεδομένης της περαιτέρω ανάπτυξης της πληροφορικής και ήδη έχουν ξεκινήσει συζητήσεις για την αναθεώρησή της.

2.2. Περιεχόμενο της Σύστασης R (87) 15 της Επιτροπής Υπουργών

Η Σύσταση 15 της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης⁶⁹ έχει ως αντικείμενο την καθιέρωση κοινών ελάχιστων εγγυήσεων προστασίας των προσωπικών δεδομένων στο πλαίσιο της αστυνομικής συνεργασίας, αφορά

⁶⁷ Σε αντίθεση με το Πρόσθετο Πρωτόκολλο 181, η Οδηγία 95/46/EK αναθέτει το ρόλο της διευκρίνισης και έκδοσης απόφασης επάρκειας στην Ευρωπαϊκή Επιτροπή, η οποία καλείται να αποφανθεί, βάσει της διαδικασίας του άρθρου 31 παρ. 2 της Οδηγίας, ότι το τρίτο κράτος παρέχει επαρκείς εγγυήσεις για την προστασία προσωπικών δεδομένων.

⁶⁸ Ειδικότερα βλ. γνωμοδότηση ΕΕΠΔ, 2008/C110/01 για το σχέδιο πρότασης Απόφασης-Πλαίσιο για τη χρήση δεδομένων PNR, σελ. 6 και Paul De Hert, Rocco Bellanova, "Data Protection in the area of freedom, security and Justice: a system still to be fully developed?", Μάρτιος 2009, ιστότοπος: <http://www.fuslac.be/data1/publications/10/1425/8545.pdf>

⁶⁹ Το κείμενο της Σύστασης βρίσκεται στον ιστότοπο του Συμβουλίου της Ευρώπης (http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/organisedcrime/Rec_1987_15.pdf)

δε και στο πεδίο της Ε.Ε., στον τότε Γ΄ Πυλώνα. Οι αρχές που εμπεριέχονται στη Σύσταση αφορούν τη συλλογή, αποθήκευση, χρήση και ανταλλαγή προσωπικών δεδομένων για σκοπούς των αστυνομικών αρχών. Βάσει της Σύστασης, η συλλογή των δεδομένων (άρθρο 2) πρέπει να πραγματοποιείται στο βαθμό που είναι απαραίτητη για την πρόληψη πραγματικών κινδύνων ή την καταπολέμηση συγκεκριμένου ποινικού αδικήματος, ενώ η χρήση τους (άρθρο 4) πρέπει να περιορίζεται στους αστυνομικούς σκοπούς για τους οποίους συλλέχθηκαν και αποθηκεύτηκαν. Επίσης, προτείνεται η απαγόρευση της συλλογής δεδομένων προσώπων λόγω της εθνικής τους καταγωγής, των θρησκευτικών και πολιτικών πεποιθήσεων ή του σεξουαλικού τους προσανατολισμού (άρθρο 2), ενώ το εκτενέστερο κατά περιεχόμενο άρθρο της Σύστασης (άρθρο 5) αναφέρεται στην ανταλλαγή δεδομένων μεταξύ αστυνομικών αρχών ή στη διαβίβαση από αστυνομικές αρχές σε άλλες δημόσιες αρχές ή ιδιωτικούς φορείς.

Η Σύσταση 15 αποτελεί ένα εργαλείο για την κατανόηση της προστασίας των δεδομένων στο χώρο δικαιοσύνης και εσωτερικών υποθέσεων⁷⁰ και τη δημιουργία ενός ελάχιστου καθεστώτος προστασίας. Σε αρκετά μάλιστα κείμενα που ρυθμίζουν τη διαβίβαση και ανταλλαγή πληροφοριών αστυνομικού χαρακτήρα, όπως π.χ. στη Σύμβαση Ευρωπαϊκή⁷¹, γίνεται παραπομπή και στην εν λόγω Σύσταση σε συνδυασμό με τη Σύμβαση 108.

3. Κανονιστικό περιεχόμενο της Οδηγίας 95/46/ΕΚ

Αν και η Σύμβαση 108 κυρώθηκε το έτος 1992, η θέσπιση εσωτερικών ειδικών ρυθμίσεων για την προστασία προσωπικών δεδομένων δεν πραγματοποιήθηκε παρά με το Ν. 2472/97, με τον οποίο ενσωματώθηκε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24^{ης}

⁷⁰ Βλ. σχετ. Paul De Hert, Vagelis Papakonstantinou & Cornelia Riehle, "Data protection in the third pillar: cautious pessimism", *Crime, Rights and the EU*, [Justice] 2008, σελ. 142 (<http://www.vub.ac.be/LSTS/pub/Dehert/224.pdf>)

⁷¹ Η Σύμβαση για την ίδρυση Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Σύμβαση Ευρωπαϊκή) (ΟJ ΕΕ C 316, 27.11.1995) ενσωματώθηκε στην εθνική μας νομοθεσία με το Ν. 2605/98 (ΦΕΚ 88 Α΄/22-4-98). Στο άρθρο 14 της εν λόγω Σύμβασης, τα Κράτη-μέλη υποχρεούνται να λάβουν τα απαραίτητα εθνικά μέτρα για την επίτευξη ενός επιπέδου προστασίας της επεξεργασίας των αποθηκευμένων στα αρχεία τους δεδομένων, αλλά και σε αυτά που θα επεξεργαστούν, το οποίο να είναι τουλάχιστον ισοδύναμο με αυτό που απορρέει από τη Σύμβαση 108 και τη Σύσταση 15. Από τα προαναφερθέντα εμφανίζεται ότι αν και η Σύσταση 15 δεν έχει δεσμευτικό χαρακτήρα, όσον αφορά τα Κ-μ της Ε.Ε., η εφαρμογή της είναι υποχρεωτική.

Οκτωβρίου 1995 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Η ανωτέρω Οδηγία αποτελεί το κείμενο αναφοράς, σε ευρωπαϊκό επίπεδο, στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα. Θεσπίστηκε με σκοπό τη διασφάλιση, από τα Κράτη-μέλη, της προστασίας των θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενόψει της ελεύθερης κυκλοφορίας τους μεταξύ των Κρατών μελών στο πλαίσιο της ελεύθερης διακίνησης εμπορευμάτων, κεφαλαίων, κ.λπ., όπως ορίστηκε στη Συνθήκη του Μάαστριχτ.

Η Οδηγία θέτει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα ανά την Ευρωπαϊκή Ένωση. Προς το σκοπό αυτό, ορίζει τα όρια για τη συλλογή και τη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα και θέτει την υποχρέωση δημιουργίας, σε κάθε κράτος μέλος, ενός ανεξάρτητου εθνικού οργανισμού επιφορτισμένου με την προστασία των δεδομένων αυτών.

Η Οδηγία 95/46/EK εφαρμόζεται στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας με αυτοματοποιημένες διαδικασίες (π.χ. πληροφορική βάση δεδομένων πελατών) καθώς και στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο (παραδοσιακά αρχεία σε χαρτί). Δεν εφαρμόζεται στην επεξεργασία δεδομένων, η οποία πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων ή πραγματοποιείται για την άσκηση δραστηριοτήτων που δεν διέπονται από το (τότε) κοινοτικό δίκαιο, όπως η δημόσια ασφάλεια, η άμυνα ή η ασφάλεια του κράτους. Τούτο πρακτικά σημαίνει ότι η Οδηγία δεν είχε εφαρμογή στην αστυνομική και δικαστική συνεργασία (τότε Τίτλοι V και VI της Συνθήκης ΕΕ).

Στόχος της Οδηγίας είναι ο καθορισμός κατευθυντήριων αρχών που θα πρέπει να διέπουν τη νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Οι αρχές αυτές αφορούν:

- Την ποιότητα των δεδομένων: τα δεδομένα προσωπικού χαρακτήρα πρέπει συγκεκριμένα να αποτελούν αντικείμενο θεμιτής και ρητής

επεξεργασίας και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς. Θα πρέπει εξάλλου να είναι ακριβή και, αν χρειάζεται, ενημερωμένα·

- Τη νόμιμη επεξεργασία των δεδομένων: η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν μπορεί να γίνεται παρά μόνον, αν το υπ' όψιν άτομο έχει κατά τρόπο αναμφισβήτητο δώσει τη συναίνεσή του ή αν η επεξεργασία είναι απαραίτητη:
 - ο για την εκτέλεση σύμβασης, της οποίας το υπ' όψιν πρόσωπο αποτελεί συμβαλλόμενο μέρος,
 - ο για την τήρηση νομικής υποχρέωσης, στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας,
 - ο για τη διαφύλαξη ζωτικού συμφέροντος του υπ' όψιν προσώπου,
 - ο για την εκτέλεση αποστολής δημόσιου συμφέροντος,
 - ο για την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο της επεξεργασίας·
- Τις ειδικές κατηγορίες επεξεργασίας: θα πρέπει να απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία και την ερωτική ζωή. Η διάταξη αυτή συνοδεύεται από επιφυλάξεις που αφορούν, π.χ. την περίπτωση κατά την οποία η επεξεργασία είναι απαραίτητη για την υπεράσπιση των ζωτικών συμφερόντων του υπ' όψιν προσώπου ή για σκοπούς προληπτικής ιατρικής και ιατρικής διάγνωσης·
- Την ενημέρωση των ενδιαφερόμενων προσώπων σχετικά με την επεξεργασία δεδομένων: ορισμένες πληροφορίες (ταυτότητα του υπεύθυνου της επεξεργασίας, σκοπιμότητες της επεξεργασίας, παραλήπτες των δεδομένων κ.λπ.) θα πρέπει να παρέχονται από τον υπεύθυνο της επεξεργασίας στο πρόσωπο για το οποίο συλλέγει δεδομένα που το αφορούν·
- Το δικαίωμα πρόσβασης των προσώπων αυτών στα δεδομένα: κάθε σχετικό πρόσωπο θα πρέπει να έχει το δικαίωμα να επιτύχει από τον υπεύθυνο της επεξεργασίας:

- τη διαβεβαίωση ότι τα δεδομένα που το αφορούν γίνονται ή δεν γίνονται αντικείμενο επεξεργασίας και την κοινοποίηση των δεδομένων που αποτελούν το αντικείμενο επεξεργασίας,
- τη διόρθωση, τη διαγραφή ή την απαγόρευση της πρόσβασης στα δεδομένα, των οποίων η επεξεργασία δεν είναι σύμφωνη προς την παρούσα επεξεργασία - ιδίως σε ό,τι αφορά τον ατελή ή ανακριβή χαρακτήρα των δεδομένων - καθώς και την κοινοποίηση των τροποποιήσεων αυτών προς τρίτους, προς τους οποίους τα δεδομένα αυτά έχουν διαβιβασθεί.
- Τις εξαιρέσεις και τους περιορισμούς: αρχές σχετικά με την ποιότητα των δεδομένων, την πληροφόρηση του υπ' όψιν προσώπου, το δικαίωμα πρόσβασης και τη δημοσιότητα των επεξεργασιών δεδομένων μπορούν να έχουν περιορισμένη εμβέλεια ώστε να διαφυλαχθεί, μεταξύ άλλων, η κρατική ασφάλεια, η άμυνα, η δημόσια ασφάλεια, η ποινική δίωξη ποινικών παραβάσεων, ένα οικονομικό ή δημοσιονομικό σημαντικό συμφέρον ενός κράτους μέλους ή της ΕΕ ή η προστασία του εν λόγω προσώπου.
- Το δικαίωμα αντίταξης στην επεξεργασία δεδομένων: το υπ' όψιν πρόσωπο θα πρέπει να έχει το δικαίωμα να αντιταχθεί, για θεμιτούς λόγους, στην επεξεργασία δεδομένων που το αφορούν. Θα πρέπει επίσης να δύναται να αντιταχθεί, εφόσον το ζητήσει και δωρεάν, στην επεξεργασία δεδομένων που προβλέπεται για σκοπούς διερεύνησης. Θα πρέπει επίσης να ενημερώνεται πριν από τη διαβίβαση των δεδομένων σε τρίτους για σκοπούς έρευνας και θα πρέπει να του παρέχεται το δικαίωμα αντίταξης του στη διαβίβαση αυτή.
- Την εμπιστευτικότητα και την ασφάλεια της επεξεργασίας: κάθε πρόσωπο που ενεργεί υπό την εξουσία του υπευθύνου της επεξεργασίας ή εκείνη του υπεργολάβου, καθώς και ο ίδιος ο υπεργολάβος, που έχει πρόσβαση σε προσωπικά δεδομένα, δεν δύναται να τα επεξεργαστεί παρά μόνον κατόπιν εντολής του υπευθύνου επεξεργασίας. Εξάλλου, ο υπεύθυνος της επεξεργασίας θα πρέπει να εφαρμόζει τα ενδεδειγμένα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα έναντι τυχαίας ή

παράνομης καταστροφής, τυχαίας απώλειας, αλλοίωσης, διάδοσης ή πρόσβασης χωρίς άδεια·

- Την κοινοποίηση των αποτελεσμάτων της επεξεργασίας σε ελεγκτική αρχή: ο υπεύθυνος επεξεργασίας οφείλει να απευθύνει κοινοποίηση στην αρμόδια ελεγκτική αρχή πριν από την εκτέλεση μιας επεξεργασίας. Προηγούμενες εξετάσεις ως προς τους ενδεχόμενους κινδύνους έναντι των δικαιωμάτων και ελευθεριών των υπ' όψιν προσώπων θα πρέπει να γίνονται από την ελεγκτική αρχή μέχρι τη λήψη της κοινοποίησης. Η δημοσιότητα των αποτελεσμάτων της επεξεργασίας θα πρέπει να διασφαλίζεται και οι ελεγκτικές αρχές οφείλουν να τηρούν μητρώο των κοινοποιημένων αποτελεσμάτων επεξεργασίας.

Κάθε πρόσωπο θα πρέπει να έχει τη δυνατότητα νομικής προσφυγής, στην περίπτωση παραβίασης των δικαιωμάτων που εγγυώνται οι εθνικές διατάξεις, οι οποίες ισχύουν για τη σχετική επεξεργασία δεδομένων. Εξάλλου, τα άτομα που έχουν υποστεί βλάβη, λόγω μιας παράνομης επεξεργασίας των προσωπικών τους δεδομένων, έχουν το δικαίωμα να ζητήσουν αποκατάσταση της ζημίας που υπέστησαν.

Περαιτέρω, επιτρέπονται οι μεταβιβάσεις δεδομένων προσωπικού χαρακτήρα από κράτος μέλος σε τρίτη χώρα, υπό την προϋπόθεση ότι η τρίτη χώρα διαθέτει το κατάλληλο επίπεδο προστασίας. Αντίθετα, οι εν λόγω μεταβιβάσεις δεν μπορούν να πραγματοποιηθούν προς τρίτες χώρες, οι οποίες δεν διαθέτουν το κατάλληλο επίπεδο προστασίας, εκτός από συγκεκριμένες περιπτώσεις παρέκκλισης, οι οποίες απαριθμούνται περιοριστικά στην Οδηγία.

Σκοπός της Οδηγίας ήταν πρωτίστως η διευκόλυνση της εκπόνησης κωδίκων εθνικής και κοινοτικής συμπεριφοράς, οι οποίοι θα συνέβαλαν στην ομαλή εφαρμογή των κοινοτικών και εθνικών διατάξεων. Βάσει αυτής της Οδηγίας θεσπίστηκε στη Χώρα μας, όπως προαναφέρθηκε, ο Ν.2472/97 και κατά συνέπεια θεσμοθετήθηκε η ανεξάρτητη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Σε επίπεδο Ε.Ε., δημιουργήθηκε ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, στην οποία συμμετέχουν εκπρόσωποι των εθνικών αρχών ελέγχου, εκπρόσωποι

των ελεγκτικών αρχών των κοινοτικών θεσμικών οργάνων και οργανισμών και ένας εκπρόσωπος της Επιτροπής.⁷²

4. Κανονιστικό περιεχόμενο της Απόφασης – Πλαίσιο 2008/977/ΔΕΥ

Μετά τη Συνθήκη της Νίκαιας και την εγκαθίδρυση του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, κατέστη αναγκαίος ο καθορισμός ενός πλαισίου προστασίας των δεδομένων προσωπικού χαρακτήρα και στον Τρίτο Πυλώνα της Ε.Ε., ήτοι στην αστυνομική και δικαστική συνεργασία. Προς τούτο, το Συμβούλιο προχώρησε στην υιοθέτηση της Απόφασης – Πλαίσιο 2008/977/ΔΕΥ της 27^{ης} Νοεμβρίου 2008 «για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις». Επισημαίνεται ότι η προαναφερθείσα Οδηγία 95/46/ΕΚ εξαιρούσε τον τομέα της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις από το πεδίο εφαρμογής της.

Σκοπός της Απόφασης – Πλαίσιο είναι η διασφάλιση υψηλού επιπέδου προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, ιδίως δε του δικαιώματός τους για ιδιωτική ζωή έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις της Ε.Ε..

Η Απόφαση – Πλαίσιο, μολονότι συμπεριλαμβάνει τα δεδομένα που έχουν ανταλλαγεί τόσο μεταξύ των Κρατών-μελών, όσο και με τα ευρωπαϊκά όργανα (π.χ. Ευρωπόλ), εξαιρεί τα δεδομένα που έχουν ανταλλαγεί στο πλαίσιο εθνικής ασφάλειας (π.χ. συνεργασία Υπηρεσιών Πληροφοριών τύπου Ε.Υ.Π. και Δ.Α.Ε.Ε.Β.). Τούτο μάλιστα είχε προβλέψει και ο εθνικός μας νομοθέτης στο άρθρο 3, παρ. 2, περ. β του Ν.2472/1997.

Η Απόφαση – Πλαίσιο, αν και αναπαράγει στα περισσότερα σημεία της την Οδηγία 95/46/ΕΚ, εισάγει ορισμένες σημαντικές καινοτομίες στον τομέα της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις. Οι βασικότερες είναι οι ακόλουθες:

α) Το δικαίωμα ενημέρωσης και πρόσβασης του προσώπου στα δεδομένα που αφορούν το πρόσωπό του (άρθρα 16 και 17 αντίστοιχα). Τα δικαιώματα αυτά δύναται –όμως – να περιοριστούν για σκοπούς μη παρεμπόδισης επίσημων

⁷² Επεξεργασία δεδομένων προσωπικού χαρακτήρα στην Ε.Ε., ιστότοπος Ευρωπαϊκής Ένωσης (http://europa.eu/legislation_summaries/information_society/data_protection/l14012_el.htm)

ή νομικών ερευνών ή για την προστασία της δημόσιας ασφάλειας. Σε κάθε περίπτωση, το άτομο έχει δικαίωμα να ενημερωθεί από την αρχή, αν τηρήθηκαν όλοι οι όροι για τη διασφάλιση της χρήσης των δεδομένων του από τις αρχές.

β) Το δικαίωμα δικαστικής προσφυγής και αποζημίωσης (άρθρα 20 και 19 αντίστοιχα). Για πρώτη φορά θεσπίζεται στο πλαίσιο του τομέα αυτού το δικαίωμα ενός προσώπου να προσβάλει ενώπιον δικαστηρίου την αθέμιτη επεξεργασία των δεδομένων του και να ζητήσει αποζημίωση για τη βλάβη που υπέστη. Σε περίπτωση που στην εσωτερική νομοθεσία δεν προβλέπεται το εν λόγω δικαίωμα ή αρμόδια για την άσκησή του δικαστική αρχή, το Κράτος-μέλος υποχρεούται να συμμορφωθεί σχετικά, σύμφωνα με το άρθρο 20 της Απόφασης-Πλαίσιο.

γ) Την αναγνώριση αρμοδιότητας στις υφιστάμενες ανεξάρτητες αρχές (ή σε νέες αν επιθυμούν τα Κράτη-μέλη) που είχαν οριστεί βάσει της Οδηγίας του '95 να ασκούν έλεγχο και στις αστυνομικές και δικαστικές αρχές που τηρούν αρχεία προσωπικών δεδομένων (άρθρο 25). Οι ανεξάρτητες αρχές των Κρατών-μελών αναλαμβάνουν εξουσίες έρευνας των αρχείων των αστυνομικών και δικαστικών υπηρεσιών, προκειμένου να εξετάσουν, αν τηρούνται οι όροι προστασίας των προσωπικών δεδομένων. Επίσης, αναλαμβάνουν εξουσίες γνωμοδότησης προς τις αρχές για τη διαβίβαση ή μη δεδομένων προσωπικού χαρακτήρα σε άλλες χώρες, καθώς και εξουσίες παράστασης ενώπιον δικαστηρίου που υφίσταται ή έχει θεσμοθετηθεί βάσει του άρθρου 20 της Απόφασης – Πλαίσιο.

Τέλος, στο άρθρο 28 της Απόφασης – Πλαίσιο, προβλέπεται – κάτι που έχει ιδιαίτερη σημασία στην παρούσα εργασία – η εξαίρεση εφαρμογής των διατάξεών της για πράξεις που εκδόθηκαν στο πλαίσιο του Τρίτου Πυλώνα πριν από την εφαρμογή της (εξαίρεση των Αποφάσεων Prüm).

Συμπερασματικά αξίζει να τονιστεί ότι, αν και η Απόφαση – Πλαίσιο 2008/977/ΔΕΥ δεν έχει ακόμη ενσωματωθεί στην ελληνική έννομη τάξη (παρά την παρέλευση της προθεσμίας της 27^{ης} Νοεμβρίου 2010 που είχε θέσει το Συμβούλιο), αποτελεί μία εξαιρετικά σημαντική νομική πράξη για τον καθορισμό κανόνων προστασίας προσωπικών δεδομένων στον τομέα της αστυνομικής και δικαστικής συνεργασίας και έρχεται να καλύψει εν μέρει το κενό που άφηνε η Οδηγία 95/46/ΕΚ. Το πρόβλημα ενσωμάτωσης, ωστόσο, δεν ήταν μόνον

ελληνικό. Η Απόφαση – Πλαίσιο δεν ενσωματώθηκε από αρκετά Κράτη – μέλη, με αποτέλεσμα να είναι ήδη εν εξελίξει η διαβούλευση για την αντικατάσταση τόσο της Οδηγίας 95/46/ΕΚ, όσο και της Απόφασης – Πλαίσιο 2008/977/ΔΕΥ, με Κανονισμό και Οδηγία αντίστοιχα για την επίλυση των ζητημάτων ενσωμάτωσης, αλλά και για την επικαιροποίηση της νομικής προστασίας των δεδομένων προσωπικού χαρακτήρα.

5. Πρόταση Κανονισμού και Οδηγίας για την αναβάθμιση του καθεστώτος προστασίας προσωπικών δεδομένων στην Ε.Ε.

Με σκοπό την αναβάθμιση του καθεστώτος προστασίας προσωπικών δεδομένων στην Ε.Ε., στα τέλη του 2011, η Ευρωπαϊκή Επιτροπή κατέθεσε δύο προτάσεις, ένα σχέδιο Κανονισμού για την αντικατάσταση της Οδηγίας 46 και του Κανονισμού 45/2001 (για την προστασία προσωπικών δεδομένων από την επεξεργασία από Όργανα της Ε.Ε.) κι ένα σχέδιο Οδηγίας για την αντικατάσταση ουσιαστικά της Απόφασης-Πλαίσιο 977.

Η πρόταση της Επιτροπής, αν και δεν παρουσιάζει μεγάλες διαφοροποιήσεις από τα υφιστάμενα νομικά εργαλεία, φαίνεται να ενισχύει την αρχή της διαφάνειας, της πρόληψης και της υπευθυνότητας⁷³. Με το νέο Κανονισμό, κάθε επεξεργασία προσωπικών δεδομένων από Υπηρεσίες του δημόσιου τομέα θα πραγματοποιείται, εφόσον τούτο προβλέπεται σε νόμο. Επίσης, αίρεται η υφιστάμενη δυνατότητα επεξεργασίας με σκοπό την εξυπηρέτηση υπέρτερου έννομου συμφέροντος τρίτου και τούτη θα πραγματοποιείται βάσει των ισχυουσών δικονομικών διατάξεων. Παράλληλα, αναβαθμίζεται ο ρόλος των Αρχών προστασίας προσωπικών δεδομένων σε προληπτικό επίπεδο, αλλά κι ως βασικός μηχανισμός εξωδικαστικής προστασίας των προσφευγόντων.

Έχοντας υπ' όψιν ότι έχουν κατατεθεί περί τις 4000 προτάσεις τροπολογίας για τον Κανονισμό και περί τις 1200 για την Οδηγία, μόνον σε επίπεδο Ευρωπαϊκού Κοινοβουλίου⁷⁴, είναι δύσκολο να γίνει μία αποτίμηση του τελικού σχεδίου του «πακέτου» προστασίας προσωπικών δεδομένων. Μία ωστόσο αρχική αποτίμηση του Κανονισμού, όπως φαίνεται στην πρόταση της Επιτροπής, είναι θετική. Οι κύριες ανησυχίες αφορούν στην αναδιατύπωση των ορισμών των όρων «δεδομένα προσωπικού χαρακτήρα», «υπεύθυνος επεξεργασίας» και «εκτελών την επεξεργασία» (άρθρο 4), την μη παράθεση ορισμών για την «κατάρτιση προφίλ» (άρθρο 20) και την «παραβίαση

⁷³ Βλ. σχετ. Ζωή Καρδασιάδου, «Η εφαρμογή των αρχών της διαφάνειας, πρόληψης και υπευθυνότητας στο νέο νομοθετικό πλαίσιο», Εισήγηση στην επετειακή διημερίδα για τα 15 χρόνια λειτουργίας της ΑΠΔΠΧ, 24 Μαΐου 2013, σε Ενημερωτικό Δελτίο της ΑΔΠΧΠ (<http://www.dpa.gr/pls/portal/docs/page/apdpx/newsmain/informational/july2013.pdf>)

⁷⁴ Ενημέρωση από τον κ. Δ. Δρούτσα κατά την εισήγησή του στην προαναφερόμενη επετειακή διημερίδα.

προσωπικών δεδομένων» (άρθρο 31), καθώς και για το ότι το διάστημα των 24 ωρών, που προβλέπει ο Κανονισμός για την κοινοποίηση της παραβίασης στην Αρχή ελέγχου, είναι πολύ μικρό. Πρόσθετες ανησυχίες εκφράστηκαν για τις διατάξεις που αφορούν το δικαίωμα λήθης (άρθρο 17), τη φορητότητα των δεδομένων (άρθρο 18), την υποχρέωση τεκμηρίωσης (άρθρο 28) καθώς και για την ιεραρχική σχέση του Κανονισμού με το άρθρο 4(2) της Οδηγίας 2002/58/ΕΚ που φαίνεται να δημιουργεί νομική αβεβαιότητα⁷⁵.

Όσον αφορά το σχέδιο Οδηγίας και υπό την προαναφερθείσα επιφύλαξη, η γενική εκτίμηση είναι ότι δεν επιτυγχάνει τον εκπεφρασμένο στόχο για ένα υψηλό επίπεδο προστασίας. Οι κυριότερες αιτιάσεις εστιάζονται στην έλλειψη διατάξεων σχετικά με τον προσδιορισμό χρονικών ορίων, την αναθεώρηση και άλλες εγγυήσεις, όπως ο περιορισμός της χρήσης δεδομένων για σοβαρά αδικήματα κ.λπ., αλλά και στην έλλειψη κανόνα για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ των Κρατών-μελών της Ε.Ε⁷⁶. Περαιτέρω προβληματισμοί αφορούν στην έλλειψη υποχρέωσης των αρμόδιων αρχών να ενημερώνουν τον παραλήπτη ότι τα διαβιβασθέντα δεδομένα είναι εσφαλμένα ή ότι η διαβίβασή τους είναι παράνομη, καθώς και η έλλειψη σχετικής διάταξης για τη διαβίβαση δεδομένων σε ιδιώτες βάσει συγκεκριμένων προϋποθέσεων⁷⁷.

⁷⁵ Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Συμπεράσματα Δημόσιας Διαβούλευσης για το πακέτο προτάσεων για την προστασία των προσωπικών δεδομένων στην Ε.Ε., 20/8/2012, στον ιστότοπο του Γραφείου Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (<http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/8355008AD63C069CC2257A60003C9E4C?OpenDocument>). Οι προαναφερόμενες παρατηρήσεις υποστηρίχθηκαν και από την κα. Καρδασιάδου στην εισήγησή της στην επετειακή διημερίδα για τα 15 χρόνια λειτουργίας της ΑΠΔΠΧ, ό.π., αλλά και στη γνωμοδότηση 01/12 της Ομάδας Εργασίας του Άρθρου 29 για την προστασία των δεδομένων σχετικά με τις προτάσεις μεταρρύθμισης της προστασίας δεδομένων, 23/3/12, ιστότοπος της Ευρωπαϊκής Ένωσης (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_el.pdf), σελ. 5-6

⁷⁶ Γνωμοδότηση 01/12 της Ομάδας Εργασίας του Άρθρου 29, ό.π., σελ. 37. Κύριος προβληματισμός της Ομάδας Εργασίας είναι ότι το άρθρο 37 της πρότασης Οδηγίας, που προβλέπει την υποχρέωση του υπευθύνου επεξεργασίας να ενημερώνει τον παραλήπτη σχετικά με τυχόν περιορισμούς της επεξεργασίας και να λαμβάνει όλα τα εύλογα μέτρα για τη διασφάλιση της συμμόρφωσης με αυτούς, εφαρμόζεται μόνο στις διαβιβάσεις σε τρίτες χώρες. Σε αυτές τις περιπτώσεις, τα Κ-μ που λαμβάνουν τα δεδομένα πρέπει επίσης να υποχρεούνται να συμμορφώνονται με τυχόν περιορισμούς επεξεργασίας που επιβάλλονται από το διαβιβάζον Κ-μ. Η Ομάδα Εργασίας καταλήγει στη διαπίστωση ότι η πρότασης Οδηγίας αποτελεί ένα βήμα προς τα πίσω σε σχέση με την Απόφαση-Πλαίσιο 2008/977/ΔΕΥ.

⁷⁷ Γνωμοδότηση 01/12 της Ομάδας Εργασίας του Άρθρου 29, ό.π., σελ. 37.

Κατά την άποψή μου, ο βασικός προβληματισμός για το σχέδιο Οδηγίας αφορά καταρχάς το διαχωρισμό της από τον Κανονισμό και τη θέσπιση δύο νομικών πράξεων για την προστασία προσωπικών δεδομένων στην Ε.Ε., αντί ενός που ήταν και η αρχική πρόθεση της Επιτροπής. Ο διαχωρισμός των νομικών εργαλείων κατά το πεδίο εφαρμογής τους αποτελεί επιλογή του Συμβουλίου κι επαναφέρει ουσιαστικά τη λογική των Πυλώνων, όπου ο Κανονισμός θα αντικαταστήσει την Οδηγία 95/46/ΕΚ και θα αφορά την οικονομική ζωή και δραστηριότητα και η Οδηγία θα αντικαταστήσει – κυρίως – την Απόφαση-Πλαίσιο 2008/977/ΔΕΥ και θα αφορά την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις. Στη θέση του Συμβουλίου υποδηλώνεται ότι το καθεστώς προστασίας στις περιπτώσεις αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις θα πρέπει να είναι εκ των πραγμάτων μικρότερο, προκειμένου να καταστεί δυνατή – κάθε φορά – η στάθμιση μεταξύ της προστασίας των προσωπικών δεδομένων και της αναγκαιότητας καταπολέμησης των σοβαρών μορφών του εγκλήματος, ιδίως του οργανωμένου, αλλά και της τρομοκρατίας⁷⁸.

Εξετάζοντας την πρόταση Οδηγίας από τη σκοπιά των αρχών επιβολής του νόμου, παρατηρείται ότι με τις διατάξεις της θεσπίζονται επιπλέον γραφειοκρατικές διαδικασίες για αυτές (άρθρο 24), προκειμένου να επεξεργάζονται τα απαραίτητα δεδομένα και να επιτελέσουν το έργο τους και κατά συνέπεια συμπεραίνεται ότι ελλείπει η μέριμνα για την πρακτική διευκόλυνση επιβολής του νόμου. Επίσης, οι ρυθμίσεις που εισάγονται δημιουργούν αυξημένες υποχρεώσεις ενημέρωσης του υποκειμένου των δεδομένων, όπως επίσης και αυξημένο αριθμό πληροφοριών που πρέπει να δοθούν με αποτέλεσμα να δυσχεραίνεται το έργο των αρχών επιβολής του νόμου (άρθρο 11), λόγω της συνεπακόλουθης δυσχέρειας να διατηρηθεί το απόρρητο κρίσιμων πληροφοριών. Περαιτέρω, η διαγραφή δεδομένων (άρθρο 16) που συνάδει με το «δικαίωμα του υποκειμένου στη λήθη» θα έχει αρνητικές συνέπειες στην πληρότητα των ερευνών που ακολουθούν κατά την διερεύνηση εγκλημάτων και για το λόγο αυτό, προτείνεται να θεσπισθούν περισσότερες

⁷⁸ Σημειώνεται ότι αντίστοιχος διαχωρισμός στην αντιμετώπιση των δύο τομέων υπήρξε και στα προηγούμενα νομοθετήματα για την προστασία προσωπικών δεδομένων και το Συμβούλιο, σε αντίθεση με το Κοινοβούλιο, επιθυμούσε να παραμείνει.

εξαιρέσεις που θα διασφαλίζουν τη διατήρηση δεδομένων είτε για λόγους ελέγχου είτε για τήρηση αρχείου.

Τέλος, αξίζει να επισημανθεί ότι η κατάρτιση ενός πακέτου νομοθετημάτων (Κανονισμού και Οδηγίας) για την προστασία δεδομένων προσωπικού χαρακτήρα έχει δεχθεί επικρίσεις ως προς τη χρησιμότητά του⁷⁹. Οι επικρίσεις κυρίως αφορούσαν την άποψη ότι η πλήρης ομογενοποίηση των κανόνων προστασίας για όλους τομείς ενέχει τον κίνδυνο να αφεθούν αρρυθμιστα κάποια πεδία και κατά συνέπεια να επιτευχθεί τελικά χαμηλότερο επίπεδο προστασίας.

⁷⁹ Βλ. σχετ. Diana Alonso Blas, First Pillar and third Pillar: Need for a common approach on data protection?, Απρίλιος 2008, Ιστότοπος Πανεπιστημίου Εδιμβούργου, http://www2.law.ed.ac.uk/file_download/communities/92_article%20dab%20first%20pillar%20and%20third%20pillar%20april%202008.doc, σελ. 11-12

IV. Προστασία προσωπικών δεδομένων στα δίκτυα ανταλλαγής πληροφοριών αστυνομικής συνεργασίας σε ευρωπαϊκό και εθνικό επίπεδο

1. Προστασία προσωπικών δεδομένων στο Σύστημα Πληροφοριών Σένγκεν

Η προστασία προσωπικών δεδομένων και η ασφάλεια πληροφοριών στο πλαίσιο του Συστήματος Πληροφοριών Σένγκεν (SIS), ρυθμίζεται στα άρθρα 102 έως 118 της Σύμβασης Εφαρμογής της Συνθήκης Σένγκεν, η οποία ενσωματώθηκε στην εθνική έννομη τάξη με το Ν.2514/97 (ΦΕΚ 140 Α'/26-6-97).

Στα προαναφερόμενα άρθρα ορίζεται ότι τα προσωπικά δεδομένα επιτρέπεται να χρησιμοποιηθούν μόνο στο πλαίσιο της συγκεκριμένης έκδοσης σήματος για την οποία δόθηκαν, ήτοι για τους σκοπούς καταχώρησης που προβλέπονται στα άρθρα 95 έως 100 της Σύμβασης Εφαρμογής της Συμφωνίας Σένγκεν. Οι εν λόγω σκοποί καταχώρισης αφορούν:

α) Πρόσωπα των οποίων ζητείται η σύλληψη με σκοπό την εκτέλεση Ευρωπαϊκού Εντάλματος Σύλληψης (άρθρο 95 παρ. 1). Σημειώνεται ότι η σχετική διάταξη της Σύμβασης, όπως κυρώθηκε με το Ν. 2514/97, αναφέρεται μεν στην έκδοση, πλην όμως, με το άρθρο 38 εδ. ε' του Ν. 3251/04 «Ευρωπαϊκό Ένταλμα Σύλληψης, τροποποίηση του Ν. 2928/2001 για τις εγκληματικές οργανώσεις και άλλες διατάξεις», οι σχετικές αναφορές στην έκδοση έχουν αντικατασταθεί με την εκτέλεση Ευρωπαϊκών Ενταλμάτων Σύλληψης.

β) Αλλοδαπούς που καταχωρούνται σε αρχείο, βάσει εθνικής καταχώρησης, η οποία θεμελιώνεται σε αποφάσεις των αρμόδιων διοικητικών αρχών και δικαστηρίων, σύμφωνα με τους διαδικαστικούς κανόνες της εθνικής νομοθεσίας. Ως αιτιολογία στις εν λόγω αποφάσεις διαλαμβάνεται η απειλή της δημόσιας τάξης και ασφάλειας ή και της εθνικής ασφάλειας από την παρουσία ενός αλλοδαπού στην επικράτεια του κράτους (άρθρο 96).

γ) Πρόσωπα που έχουν εξαφανιστεί ή πρόσωπα που πρέπει να τεθούν υπό προσωρινή επιτήρηση για δική τους προστασία ή για την αποτροπή απειλών (άρθρο 97).

δ) Μάρτυρες ή πρόσωπα που κλητεύονται, προκειμένου να εμφανιστούν ενώπιον των δικαστικών αρχών για πράξεις ως προς τις οποίες έχει ασκηθεί σε βάρος τους ποινική δίωξη ή πρόσωπα, στα οποία πρέπει να επιδοθεί καταδικαστική απόφαση ή κλήση προς έκτιση ποινής στερητικής της ελευθερίας (άρθρο 98).

Τα προσωπικά δεδομένα που έχουν εισαχθεί στο SIS για τον εντοπισμό προσώπων μπορούν να διατηρηθούν μόνο για το χρονικό διάστημα που απαιτείται για την επίτευξη των σκοπών, για τους οποίους δόθηκαν και μέχρι τρία έτη κατ' ανώτατο όριο από την καταχώρησή τους στο σύστημα, πλην των δεδομένων που καταχωρούνται βάσει του άρθρου 99, τα οποία πρέπει να απαλείφονται μετά από ένα χρόνο (άρθρο 112 παρ. 1).

Από τις αναζητήσεις στο SIS προκύπτει «θετική απάντηση» («hit»), όταν τα αναζητούμενα στοιχεία αντιστοιχούν στη συγκεκριμένη καταχώριση. Εφόσον λάβουν θετική απάντηση, οι αρμόδιες αρχές δύνανται, μέσω του δικτύου των γραφείων SIRENE, να ζητήσουν συμπληρωματικές πληροφορίες σχετικά με τα υποκείμενα της καταχώρισης⁸⁰.

Τα Κράτη-μέλη πρέπει να θεσπίσουν εθνικούς κανόνες που προβλέπουν επίπεδο προστασίας των δεδομένων τουλάχιστον ισότιμο με το προβλεπόμενο στη Σύμβαση του Συμβουλίου της Ευρώπης του 1981 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα και στη Σύσταση της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης του 1987, για τη ρύθμιση της χρήσεως των δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα.⁸¹

Στην Ελλάδα, τα δικαιώματα που έχει το υποκείμενο των δικαιωμάτων, ήτοι τα δικαιώματα πρόσβασης και αντίρρησης, καθορίζονται από τα άρθρα 12 και 13 του Ν. 2472/97 αντίστοιχα. Όσον αφορά το Σύστημα Πληροφοριών Σένγκεν, τα δικαιώματα αυτά ασκούνται εγγράφως, με την αποστολή αίτησης,

⁸⁰ Το ελληνικό Εθνικό Γραφείο SIRENE αποτελεί το 3^ο Τμήμα της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας του Αρχηγείου της Ελληνικής Αστυνομίας του Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη.

⁸¹ Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, ό.π., και Σύσταση αριθ. R (87) 15 της 17ης Σεπτεμβρίου 1987, της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης, ό.π..

στον υπεύθυνο επεξεργασίας, ήτοι στο Εθνικό Γραφείο SIRENE του Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη.

Ο υπεύθυνος επεξεργασίας έχει υποχρέωση να απαντήσει εγγράφως εντός δεκαπέντε ημερών, ενώ σε αρνητική περίπτωση, το υποκείμενο των δικαιωμάτων δύναται να προσφύγει στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Το δικαίωμα πρόσβασης δύναται να περιοριστεί μόνο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, όπως ορίζει η παρ. 5 του άρθρου 12 του Ν.2472/97. Στην περίπτωση μη απάντησης επί του αιτήματος αντιρρήσεων εντός της προβλεπόμενης προθεσμίας ή εάν η απάντηση δεν είναι ικανοποιητική για το υποκείμενο των δεδομένων, τότε το τελευταίο μπορεί να προσφύγει ενώπιον της Αρχής, η οποία και θα κρίνει τελικά για τη νομιμότητα της καταχώρησης⁸².

Γίνεται κατανοητό ότι οι λόγοι εθνικής ασφάλειας και διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων είναι όροι ασαφείς και παραπέμπουν στη συλλογή και επεξεργασία πληροφοριών από την Εθνική Υπηρεσία Πληροφοριών και την Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας (Αντιτρομοκρατική) της Ελληνικής Αστυνομίας. Η Αρχή⁸³, εξετάζοντας σχετικό αίτημα, δέχθηκε ότι σκοπός της διάταξης της παρ. 5 του άρθρου 12 του Ν.2472/97 δεν είναι η εξαίρεση όλων των επεξεργασιών που διεξάγουν τα αρμόδια Υπουργεία και εντάσσονται στο πλαίσιο της προστασίας της εθνικής ασφάλειας, αλλά μόνον αυτών που μπορούν έστω και έμμεσα να τη βλάψουν. Το συμπέρασμα αυτό προκύπτει, κατά την Αρχή, από τη διατύπωση του Νόμου, ο οποίος δίδει δικαίωμα περιορισμού εν μέρει ή εν όλω της υποχρέωσης ενημέρωσης που έχουν τα αρμόδια Υπουργεία.

2. Προστασία προσωπικών δεδομένων στα εργαλεία της Ευρωπόλ

Η Ευρωπόλ μπορεί να επεξεργάζεται δεδομένα για να εξακριβώνει, κατά πόσον τα δεδομένα αυτά έχουν σχέση με την εκτέλεση των καθηκόντων της και δύναται να συμπεριληφθούν στο Σύστημα Πληροφοριών Ευρωπόλ, στα αρχεία δεδομένων εργασίας προς ανάλυση ή σε άλλα συστήματα επεξεργασίας

⁸² Ιστότοπος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (http://www.dpa.gr/portal/page?_pageid=33,126661&_dad=portal&_schema=PORTAL)

⁸³ Βλ. Ετήσια Έκθεση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σελ. 36 (σε http://www.dpa.gr/portal/page?_pageid=33,15424&_dad=portal&_schema=PORTAL)

δεδομένων προσωπικού χαρακτήρα που συγκροτούνται. Το Διοικητικό Συμβούλιο, έπειτα από πρόταση του Διευθυντή και αφού ζητήσει τη γνώμη της Κοινής Εποπτικής Αρχής, με απόφασή του καθορίζει τις προϋποθέσεις επεξεργασίας των δεδομένων αυτών, η οποία υποβάλλεται στο Συμβούλιο προς έγκριση⁸⁴.

Κατ' αρχάς, πέρα από τις ειδικές διατάξεις της οικείας Απόφασης περί της ίδρυσης της Ευρωπόλ και του κανονιστικού της πλαισίου, ισχύει για τη δράση της η υποχρέωση παροχής επιπέδου προστασίας των δεδομένων τουλάχιστον ισότιμου με το προβλεπόμενο στη σύμβαση του Συμβουλίου της Ευρώπης του 1981 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα και στη σύσταση της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης του 1987, για τη ρύθμιση της χρήσεως των δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα⁸⁵. Βεβαίως, κι όπως συνηθίζεται για τις Υπηρεσίες της Ένωσης, έχουν θεσπιστεί ειδικές ρυθμίσεις για την Ευρωπόλ (tailor-made), που αποτυπώνονται κυρίως στα άρθρα 27 έως 35 της Απόφασης Ευρωπόλ.

Ειδικότερα, τα δεδομένα προσωπικού χαρακτήρα που ανακτώνται από οποιοδήποτε εκ των αρχείων επεξεργασίας δεδομένων της Ευρωπόλ ή κοινοποιούνται με οποιοδήποτε άλλο κατάλληλο μέσο διαβιβάζονται ή χρησιμοποιούνται αποκλειστικά και μόνο από τις αρμόδιες αρχές των κρατών μελών με στόχο την πρόληψη και την καταπολέμηση αξιόποινων πράξεων που εμπίπτουν στην αρμοδιότητα της Ευρωπόλ, καθώς και για την πρόληψη και καταπολέμηση άλλων σοβαρών μορφών εγκληματικότητας. Η Ευρωπόλ χρησιμοποιεί τα δεδομένα μόνο για την άσκηση των καθηκόντων της⁸⁶. Ωστόσο, η χρήση των δεδομένων για άλλους σκοπούς ή από άλλες αρχές πλην των εθνικών αρμόδιων αρχών επιτρέπεται μόνον, αφού ζητηθεί η γνώμη του Κράτους-μέλους που διαβίβασε τα δεδομένα, στο μέτρο που τούτο επιτρέπεται με βάση την εθνική νομοθεσία του εν λόγω Κράτους-μέλους⁸⁷.

Άλλα μέτρα προστασίας των προσωπικών δεδομένων είναι: α) η θέσπιση από τη Ευρωπόλ σε συνεργασία με τα κράτη μέλη κατάλληλων μηχανισμών

⁸⁴ Άρ. 10 παρ. 4 Απόφασης Ευρωπόλ.

⁸⁵ Άρ. 27 Απόφασης Ευρωπόλ.

⁸⁶ Άρθρο 19 παρ. 1 Απόφασης Ευρωπόλ.

⁸⁷ Άρθρο 19 παρ. 2 Απόφασης Ευρωπόλ.

ελέγχου, οι οποίοι επιτρέπουν την επαλήθευση της νομιμότητας των ανακτήσεων από οποιοδήποτε εκ των αυτοματοποιημένων αρχείων δεδομένων της που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα⁸⁸, β) ο ορισμός υπευθύνου προστασίας δεδομένων ο οποίος, υπό καθεστώς ανεξαρτησίας, διασφαλίζει τη νομιμότητα και την τήρηση των ισχυουσών διατάξεων⁸⁹ και γ) το δικαίωμα πρόσβασης των υποκειμένων των δεδομένων με λήψη σε τακτά διαστήματα πληροφοριών σχετικά με το αν η Ευρωπόλ επεξεργάζεται προσωπικά του δεδομένα⁹⁰.

Περαιτέρω, κάθε Κράτος-μέλος ορίζει μια εθνική εποπτική αρχή⁹¹, αποστολή της οποίας είναι να ελέγχει, σύμφωνα με το εθνικό της δίκαιο και υπό καθεστώς ανεξαρτησίας, τη νομιμότητα κάθε καταχώρισης, ανάκτησης και κοινοποίησης στην Ευρωπόλ δεδομένων προσωπικού χαρακτήρα από το οικείο Κράτος-μέλος, καθώς επίσης να εξετάζει κατά πόσον μια τέτοια καταχώριση, ανάκτηση ή κοινοποίηση παραβιάζει τα δικαιώματα του υποκειμένου των δεδομένων. Για τον σκοπό αυτό, η εθνική εποπτική αρχή έχει πρόσβαση, στους χώρους της οικείας εθνικής μονάδας ή στους χώρους που χρησιμοποιούν οι αξιωματικοί-σύνδεσμοι, στα δεδομένα που έχουν εισαχθεί από το Κράτος-μέλος στο Σύστημα Πληροφοριών Ευρωπόλ ή σε οποιοδήποτε άλλο σύστημα, το οποίο έχει συγκροτηθεί από την Ευρωπόλ με σκοπό την επεξεργασία δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τις σχετικές εθνικές διαδικασίες⁹².

Κάθε πρόσωπο δικαιούται να ζητήσει από την εθνική εποπτική αρχή να διασφαλίσει τη νομιμότητα της καταχώρισης ή της κοινοποίησης στην Ευρωπόλ δεδομένων που το αφορούν υπό οιαδήποτε μορφή, καθώς και της πρόσβασης στα δεδομένα από μέρους του οικείου Κράτους-μέλους⁹³.

⁸⁸ Άρθρο 18 Απόφασης Ευρωπόλ.

⁸⁹ Άρθρο 28 Απόφασης Ευρωπόλ.

⁹⁰ Άρθρο 30 Απόφασης Ευρωπόλ.

⁹¹ Στο άρθρο 30 παρ. 2 Απόφασης Ευρωπόλ, αλλά και σε άλλα σημεία της Απόφασης (π.χ. αρ. 32 παρ. 2), καθιερώνεται υποχρέωση στα Κ-μ να ορίσουν μία ή περισσότερες ανεξάρτητες Αρχές, στις οποίες τα υποκείμενα των δικαιωμάτων θα απευθύνονται, προκειμένου αποκτήσουν πρόσβαση κ.λπ. στα δεδομένα που τα αφορούν. Στη Χώρα μας την αρμοδιότητα αυτή έχει αναλάβει η Αρχή Προστασίας Προσωπικών Δεδομένων, η οποία ασκεί το σχετικό έλεγχο και συνεργάζεται με την Κοινή Εποπτική Αρχή της Ευρωπόλ, βάσει της παρ. 1 του άρθρου 19 του Ν. 2472/97 (ιδίως των εδαφίων ιγ', ιδ' και ιε' της εν λόγω παραγράφου).

⁹² Άρθρο 33 παρ. 1 Απόφασης Ευρωπόλ.

⁹³ Άρθρο 33 παρ. 2 Απόφασης Ευρωπόλ.

Επίσης, στο πλαίσιο λειτουργίας της Ευρωπόλ, ιδρύθηκε ανεξάρτητη Κοινή Εποπτική Αρχή⁹⁴, η οποία έχει ως έργο να ελέγχει τις δραστηριότητες της Ευρωπόλ, προκειμένου να διασφαλίζει ότι η αποθήκευση, επεξεργασία και χρήση δεδομένων που κατέχει η Ευρωπόλ δεν παραβιάζουν τα δικαιώματα του οικείου φυσικού προσώπου, ενώ ελέγχει τη νομιμότητα της διαβίβασης δεδομένων προερχόμενων από την Ευρωπόλ. Η Ευρωπόλ από την πλευρά της οφείλει να παρέχει στην Κοινή Εποπτική Αρχή τις πληροφορίες που ζητεί, να της παραχωρεί πρόσβαση στο σύνολο των εγγράφων και των φακέλων με έγγραφα, καθώς και στα δεδομένα που είναι αποθηκευμένα στα αρχεία δεδομένων της· και σε όλους τους χώρους της να εφαρμόζει τις αποφάσεις που η Κοινή Εποπτική Αρχή εκδίδει επί προσφυγών. Επίσης, είναι αρμόδια να εξετάζει ζητήματα εφαρμογής και ερμηνείας σε σχέση με τις δραστηριότητες της Ευρωπόλ όσον αφορά την επεξεργασία και τη χρήση δεδομένων προσωπικού χαρακτήρα. Ανά τακτά χρονικά διαστήματα, η ανωτέρω Αρχή καταρτίζει εκθέσεις πεπραγμένων, οι οποίες διαβιβάζονται στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο⁹⁵.

Επίσης, εάν η Κοινή Εποπτική Αρχή διαπιστώσει παραβάσεις των διατάξεων της Απόφασης Ευρωπόλ κατά την αποθήκευση, επεξεργασία ή χρήση δεδομένων προσωπικού χαρακτήρα, απευθύνει τις αιτιάσεις που κρίνει αναγκαίες στο Διευθυντή και του τάσσει συγκεκριμένη προθεσμία για να απαντήσει. Ο Διευθυντής τηρεί ενήμερο το Διοικητικό Συμβούλιο σχετικά με την όλη διαδικασία. Σε περίπτωση που δεν μείνει ικανοποιημένη από την απάντηση του Διευθυντή στην αίτησή της, παραπέμπει το ζήτημα στο Διοικητικό Συμβούλιο (Management Board).

Τέλος, στο πλαίσιο της Ευρωπόλ έχει ιδρυθεί και λειτουργεί Γραφείο Προστασίας Προσωπικών Δεδομένων (Data Protection Office – DPO)⁹⁶ με επικεφαλής αξιωματούχο της Ευρωπόλ, ο οποίος διορίζεται από Διοικητικό

⁹⁴ Άρθρο 34 παρ. 2 Απόφασης Europol. Πρβλ. και Νίκου Παρασκευόπουλου, Οι πλειοψηφίες στο στόχαστρο. Τρομοκρατία και κράτος δικαίου, σελ. 43, όπου υποστηρίζει ότι «η Κοινή Εποπτική Αρχή δεν έχει καθαρά νομική σύνθεση, ούτε παρέχει ικανά εγγύα ανεξαρτησίας των μελών της.»

⁹⁵ Ιστοσελίδα της Κοινής Εποπτικής Αρχής της Ευρωπόλ (Europol Joint Supervisory Body) <http://europoljsb.consilium.europa.eu/about/tasks-of-the-jsb.aspx?lang=el>

⁹⁶ Data Protection Office, Europol, 2012, σελ. 27-31 https://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf

Συμβούλιο, κατόπιν πρότασης του Διευθυντή. Βασική αρμοδιότητα της εν λόγω υπηρεσίας είναι η διασφάλιση της νομιμότητας και της συμμόρφωσης των δράσεων του Οργανισμού με τα οριζόμενα στην Απόφαση Ευρωπόλ και στις λοιπές διατάξεις για την προστασία προσωπικών δεδομένων. Προς τούτο παρέχει καθοδήγηση και συμβουλές στο Τμήμα Επιχειρήσεων της Ευρωπόλ, ιδίως στις περιπτώσεις που εξετάζεται η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτα κράτη, ενώ γνωμοδοτεί κατά την κατάρτιση και διαπραγμάτευση των στρατηγικών και επιχειρησιακών συμφωνιών συνεργασίας του Οργανισμού. Έτσι, το εν λόγω Γραφείο, αν και οργανικά εντάσσεται – ως υπηρεσία – στον Οργανισμό, αποτελεί, σε συνεργασία με την Κοινή Εποπτική Αρχή, μία δικλείδα ασφαλείας στην προστασία προσωπικών δεδομένων.

Βέβαια, ο διορισμός προσωπικού της Ευρωπόλ στο Γραφείο Προστασίας Δεδομένων ήγειρε τις αντιδράσεις του Ευρωπαίου Επόπτη Προστασίας Προσωπικών Δεδομένων (EDPS), ο οποίος έθεσε θέμα ανεξαρτησίας του εν λόγω οργάνου. Στο σχέδιο Κανονισμού για τη συγχώνευση Ευρωπόλ – CEPOL⁹⁷ οι ανησυχίες του EDPS, όπως εκφράστηκαν και στη σχετική έκθεσή του⁹⁸, φαίνεται να επέφεραν θετικές τροποποιήσεις, καθώς το προσωπικό του εν λόγω Γραφείου θα ορίζεται με απόφαση του Διοικητικού Συμβουλίου (δηλ. από τα Κράτη-μέλη), ενώ για να αποδεσμευτεί θα ζητείται η σύμφωνη γνώμη του EDPS (άρθρο 44 Κανονισμού).

Ειδικότερα, όσον αφορά τα τρίτα κράτη, αυτά είναι υποχρεωμένα, πριν από την υπογραφή της επιχειρησιακής συμφωνίας με την Ευρωπόλ, να τροποποιήσουν το εθνικό τους δίκαιο, ενσωματώνοντας όλες τις διατάξεις για την προστασία προσωπικών δεδομένων που ισχύουν για τα κράτη μέλη της Ένωσης. Τη διασφάλιση της λήψης των μέτρων αυτών επιβεβαιώνει η Κοινή Εποπτική Αρχή⁹⁹, η εισήγηση της οποίας διαβιβάζεται μαζί με το σχέδιο επιχειρησιακής συμφωνίας στο Συμβούλιο προς έγκριση¹⁰⁰.

⁹⁷ COM(2013) 173 final «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον οργανισμό της Ευρωπαϊκής Ένωσης για τη συνεργασία και την κατάρτιση στον τομέα της επιβολής του νόμου (Ευρωπόλ) και για την κατάργηση των αποφάσεων 2009/371/ΔΕΥ και 2005/681/ΔΕΥ».

⁹⁸ Έγγραφο 10468/13 JAI 459 CATS 28 ENFOPOL 170 CODEC 1322 του Συμβουλίου, σημείο 147.

⁹⁹ Άρθρο 34 Απόφασης Ευρωπόλ.

3. Προστασία προσωπικών δεδομένων στα εργαλεία της Ιντερπόλ

Τα προσωπικά δεδομένα προστατεύονται καταρχάς από το Καταστατικό της Ιντερπόλ, όπου καθορίζεται (άρθρο 2 παρ. 1) ότι η συνεργασία μεταξύ των Κρατών μελών του Οργανισμού πραγματοποιείται με σεβασμό στις εθνικές νομοθεσίες και στο πνεύμα της Παγκόσμιας Δήλωσης για τα Ανθρώπινα Δικαιώματα του ΟΗΕ¹⁰¹, στο άρθρο 12 της οποίας προστατεύεται η ιδιωτικότητα από μη νόμιμη παρέμβαση.

Στο πλαίσιο του Οργανισμού έχει συσταθεί, βάσει του άρθρου 36 του Καταστατικού, ως ανεξάρτητο όργανο, μία Επιτροπή για τον έλεγχο των αρχείων της Ιντερπόλ (Commission for the Control of INTERPOL's Files – CCF), η λειτουργία της οποίας διέπεται από τους Κανόνες σχετικά με τον Έλεγχο των πληροφοριών και της πρόσβασης στα αρχεία της Ιντερπόλ¹⁰². Η Επιτροπή CCF αποτελείται από πέντε μέλη, τα οποία καθορίζονται με απόφαση της Γενικής Συνέλευσης του Οργανισμού για τριετή θητεία (άρθρα 2 και 3 RCI). Καθήκοντά της είναι η διασφάλιση της τήρησης των κανόνων χρήσης και επεξεργασίας των πληροφοριών και η παροχή συμβουλών στον Οργανισμό για κάθε πρόγραμμα, επιχείρηση ή σχέδιο κανόνων που συμπεριλαμβάνει την επεξεργασία προσωπικών δεδομένων (άρθρο 1 RCI). Παράλληλα, η Επιτροπή CCF είναι υπεύθυνη για την παραλαβή αιτημάτων πολιτών που επιθυμούν να ασκήσουν τα δικαιώματα πρόσβασης, διόρθωσης, και διαγραφής στα δεδομένα τους που έχουν καταχωρισθεί στα αρχεία της Ιντερπόλ (άρθρο 1 RCI, αλλά και άρθρο 18 του Κανονισμού της Ιντερπόλ για την επεξεργασία των δεδομένων).

¹⁰⁰ Άρθρο 23 παρ. 2 τελευταίο εδάφιο Απόφασης Ευρωπόλ, αλλά και Απόφαση 2009/934/ΔΕΥ του Συμβουλίου, της 30ής Νοεμβρίου 2009, για τη θέσπιση κανόνων εφαρμογής που διέπουν τις σχέσεις της Ευρωπόλ με τους εταίρους της, περιλαμβανομένης της ανταλλαγής δεδομένων προσωπικού χαρακτήρα και διαβαθμισμένων πληροφοριών (OJ L 325/6 // 11-12-09). Με το νέο σχέδιο Κανονισμού για τη συγχώνευση Ευρωπόλ – CEPOL και συγκεκριμένα με το άρθρο 31 αυτού, σε συνδυασμό με το άρθρο 218 ΣΛΕΕ, η Ευρωπόλ στερείται της δυνατότητας σύναψης επιχειρησιακών συμφωνιών, δυνατότητα η οποία μεταφέρεται στην Επιτροπή και στην Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης.

¹⁰¹ Universal Declaration of Human Rights, ιστότοπος Ηνωμένων Εθνών (<http://www.un.org/en/documents/udhr/index.shtml#a12>)

¹⁰² Rules relating to the Control of Information and Access to INTERPOL's Files (RCI), ιστότοπος Ιντερπόλ (<http://www.interpol.int/Media/Files/Legal-material/Reference-Documents/Rules-on-the-Control-of-Information-and-access-to-INTERPOL's-Files-RCI>)

Ειδικότερες ρυθμίσεις για την προστασία προσωπικών δεδομένων περιέχονται στα άρθρα του Κανονισμού της Ιντερπόλ για την επεξεργασία των δεδομένων¹⁰³ που δεσμεύει τη λειτουργία των Εθνικών Κεντρικών Γραφείων Ιντερπόλ και κατά συνέπεια και τη διαχείριση των πληροφοριών που διακινούνται μέσω αυτών, σε συνδυασμό πάντοτε με τις εθνικές νομοθεσίες προστασίας προσωπικών δεδομένων των Κράτη-μέλη του Οργανισμού.

Τα Εθνικά Κεντρικά Γραφεία είναι αρμόδια για τον έλεγχο της ποιότητας των πληροφοριών¹⁰⁴, ενώ και η Γενική Γραμματεία Ιντερπόλ οφείλει κι αυτή από την πλευρά της να ασκεί έναν έλεγχο της ποιότητας σε δεύτερο επίπεδο (άρθρο 12 παρ. 2 και 3). Περαιτέρω, η Γενική Γραμματεία οφείλει να διασφαλίζει τη διαφάνεια της επεξεργασίας των δεδομένων, τα οποία αποθηκεύονται στις βάσεις δεδομένων που διατηρεί, τηρώντας ενήμερη τόσο, την Επιτροπή Ελέγχου των Αρχείων της Ιντερπόλ για τις ενέργειές της, όσο και την Εκτελεστική Επιτροπή, τη Γενική Συνέλευση και τα Εθνικά Κεντρικά Γραφεία (άρθρο 13).

Απαραίτητες προϋποθέσεις για την καταχώρηση δεδομένων στις βάσεις δεδομένων της Ιντερπόλ είναι: α) η αναγραφή του σκοπού για τον οποίο συλλέχθηκαν, β) τα εν λόγω δεδομένα να είναι ακριβή και συναφή με το σκοπό συλλογής. Επίσης, θα πρέπει να αναφέρονται τυχόν ειδικοί περιορισμοί χρήσης τους (για αστυνομική ή/και για δικαστική χρήση), καθώς και τυχόν περιορισμοί στη χρήση τους από άλλες χώρες ή διεθνείς οργανισμούς (άρθρο 62). Η ευθύνη του ελέγχου των προϋποθέσεων καταχώρησης δεδομένων βαρύνει τα Εθνικά Κεντρικά Γραφεία Ιντερπόλ (άρθρο 63). Η χρήση των δεδομένων γίνεται μόνον για το σκοπό για τον οποίο συλλέχθηκαν (άρθρο 10). Κατ' εξαίρεση, στο πλαίσιο ποινικής διερεύνησης ενός εγκλήματος, η χρήση των δεδομένων μπορεί να πραγματοποιηθεί και για άλλους σκοπούς, εφόσον τούτοι συνάδουν με το

¹⁰³ INTERPOL's Rules on the Processing of Data, ιστότοπος Ιντερπόλ (<http://www.interpol.int/content/download/13042/90082/version/17/file/RTD%20ENGLISH.pdf>). Οι Κανόνες αναθεωρήθηκαν ομόφωνα κατά την 80^η Σύνοδο της Γενικής Συνέλευσης του Οργανισμού (03/11/2011), προκειμένου αναβαθμιστεί το καθεστώς προστασίας δεδομένων προσωπικού χαρακτήρα κατά τις ανταλλαγές πληροφοριών που πραγματοποιούνται μέσω του διαύλου που παρέχει ο Οργανισμός.

¹⁰⁴ Ως "ποιότητα των πληροφοριών" νοείται το σύνολο των χαρακτηριστικών που θα πρέπει να έχουν οι πληροφορίες, δηλαδή θα πρέπει να είναι ακριβείς, συναφείς, πρόσφορες, επικαιροποιημένες, κι όχι περισσότερες από όσο απαιτείται ενόψει των σκοπών που συλλέγονται.

πλαίσιο λειτουργίας της Ιντερπόλ και δεν είναι ασυμβίβαστοι με τον αρχικό σκοπό (άρθρο 63).

Η διατήρηση των δεδομένων στις βάσεις δεδομένων της Ιντερπόλ πραγματοποιείται για το απαραίτητο χρονικό διάστημα που απαιτεί η υλοποίηση του σκοπού για τον οποίο συλλέχθηκαν και διαγράφονται αυτόματα, με ευθύνη των Εθνικών Κεντρικών Γραφείων, με το πέρας του χρονικού διαστήματος αυτού. Τα δεδομένα μπορούν να διατηρηθούν και για ακόμη μεγαλύτερο χρονικό διάστημα, εφόσον ανακύπτει νέος σκοπός διατήρησής τους και επαρκής αιτιολόγηση από το Εθνικό Κεντρικό Γραφείο που τα διατηρεί (άρθρο 51). Σε κάθε περίπτωση, τα δεδομένα δεν μπορούν να διατηρηθούν για χρονικό διάστημα μεγαλύτερο των 10 ετών.

4. Προστασία προσωπικών δεδομένων στην Απόφαση Prüm

Η Απόφαση Prüm, δεδομένου ότι αφενός τέθηκε σε ισχύ την 23^η Ιουνίου 2008, ήτοι πέντε μήνες πριν την Απόφαση – Πλαίσιο 2008/977/ΔΕΥ, αφετέρου δεν υφίστατο νομικό πλαίσιο προστασίας προσωπικών δεδομένων στον τότε Τρίτο Πυλώνα, ήταν αναγκαίο να περιέχει διατάξεις για την προστασία προσωπικών δεδομένων¹⁰⁵. Οι εν λόγω διατάξεις περιέχονται στο Κεφάλαιο 6 της Απόφασης Prüm, στα άρθρα 24 – 32.

Στο άρθρο 24 ορίζονται οι έννοιες της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, της αυτοματοποιημένης διαδικασίας αναζήτησης, του χαρακτηρισμού και του κλειδώματος για τους σκοπούς της Απόφασης Prüm.

Η έννοια που δίδεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα¹⁰⁶ είναι σχεδόν όμοια με αυτή της Οδηγίας 95/46/ΕΚ, με τη διαφορά ότι συμπεριλαμβάνει την καταχώρηση δεδομένων προσωπικού χαρακτήρα, την ευθυγράμμιση, το συνδυασμό και την κοινοποίηση του κατά πόσο ήταν επιτυχής η αναζήτηση, επεκτείνοντας έτσι το πεδίο αναφοράς της επεξεργασίας. Ως «χαρακτηρισμός» νοείται η *επισήμανση των αποθηκευμένων δεδομένων προσωπικού χαρακτήρα χωρίς σκοπό να περιοριστεί η επεξεργασία τους στο μέλλον*, ενώ ως «κλείδωμα» νοείται η *επισήμανση των αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με σκοπό να περιοριστεί η επεξεργασία τους στο μέλλον*. Οι έννοιες του χαρακτηρισμού και του κλειδώματος δεν υπήρχαν στην Οδηγία 95/46/ΕΚ, αλλά έχουν συμπεριληφθεί στην Απόφαση – Πλαίσιο 2008/977/ΔΕΥ. Αντιθέτως, η έννοια της αυτοματοποιημένης διαδικασίας αναζήτησης η οποία νοείται ως *άμεση πρόσβαση στα αυτοματοποιημένα αρχεία άλλου φορέα, με πλήρως αυτοματοποιημένη ανταπόκριση στη διαδικασία αναζήτησης* δεν υπάρχει στα προαναφερόμενα κείμενα.

Στο άρθρο 25 καθορίζεται το επίπεδο προστασίας προσωπικών δεδομένων το οποίο πρέπει να τηρούν τα Κράτη-μέλη για την εφαρμογή της Απόφασης Prüm και καθορίζεται ως τουλάχιστον ισοδύναμο με αυτό που απορρέει από την Ευρωπαϊκή Σύμβαση του 1981 και από το πρόσθετο Πρωτόκολλο του 2001, λαμβάνοντας υπ' όψιν και τη σύσταση της Επιτροπής

¹⁰⁵ Προοίμιο Απόφασης Prüm παρ. 20.

¹⁰⁶ Παρατηρούμε ότι δεν καθορίζεται η έννοια των δεδομένων προσωπικού χαρακτήρα. Στην περίπτωση αυτή και δεδομένου ότι τότε δεν υπήρχε η Απόφαση – Πλαίσιο, θα πρέπει να θεωρηθεί ως ισχύον ο ορισμός που δίδεται από την Οδηγία του 1995.

Υπουργών του ΣτΕ του 1987¹⁰⁷. Η εν λόγω διάταξη έχει ουσιαστική εφαρμογή μόνο για τα Κράτη-μέλη που εισήλθαν στην Ε.Ε. μετά το 2001, καθώς τα προϋπάρχοντα κράτη, συμπεριλαμβανομένης και της Χώρας μας, έχουν ήδη εκπληρώσει τις προϋποθέσεις αυτές, θέτοντας σε ισχύ άλλες Συμβάσεις, όπως η Σύμβαση Ευρωπαϊκή, οι οποίες είχαν τα ίδια προαπαιτούμενα.

Απαραίτητη προϋπόθεση για την ενεργοποίηση της εν λόγω προστασίας των προσωπικών δεδομένων είναι φυσικά η έναρξη λειτουργίας της αυτοματοποιημένης ανταλλαγής των δεδομένων αυτών, όπως προβλέπεται στα άρθρα του Κεφαλαίου 1¹⁰⁸. Επίσης, από τις διατάξεις εξαιρούνται τα Κράτη-μέλη που εφαρμόζουν ήδη τη Σύμβαση Prüm, η οποία είχε δικές της διατάξεις περί προστασίας προσωπικών δεδομένων¹⁰⁹.

Στο άρθρο 26 καθορίζεται ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο για τους σκοπούς της Απόφασης. Για την επεξεργασία για άλλους σκοπούς απαιτείται προηγούμενη άδεια του παρέχοντος Κράτους-μέλους, σύμφωνα με το εθνικό του δίκαιο¹¹⁰. Η επεξεργασία δεδομένων DNA και δακτυλικών αποτυπωμάτων επιτρέπεται μόνο για να διαπιστωθεί, αν υφίσταται αντιστοιχία των συγκρινόμενων δεδομένων, για να προετοιμαστεί και να υποβληθεί αίτημα δικαστικής συνδρομής (αν υφίσταται αντιστοιχία) και για να πραγματοποιηθεί καταγραφή σύμφωνα με τους ειδικούς κανόνες του άρθρου 30. Μετά τη σύγκριση, τα δεδομένα διαγράφονται άμεσα, εκτός αν υφίσταται ζήτημα υποβολής αιτήματος δικαστικής συνδρομής ή καταγραφής¹¹¹.

Τα παραπάνω ισχύουν και για την παροχή δεδομένων σχετικά με τα οχήματα του άρθρου 12 της Απόφασης, με εξαίρεση ότι για αυτά δεν προβλέπεται η διατήρηση των στοιχείων προς σύγκριση για την υποβολή αιτήματος δικαστικής συνδρομής¹¹².

¹⁰⁷ Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα του Συμβουλίου της Ευρώπης, ό.π. και Σύσταση αριθ. R (87) 15 της 17ης Σεπτεμβρίου 1987 της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης, ό.π..

¹⁰⁸ Άρθρο 25 παρ. 2 Απόφασης Prüm.

¹⁰⁹ Άρθρο 25 παρ. 3 Απόφασης Prüm.

¹¹⁰ Άρθρο 26 παρ. 1 Απόφασης Prüm.

¹¹¹ Άρθρο 26 παρ. 2 Απόφασης Prüm.

¹¹² Άρθρο 26 παρ. 3 Απόφασης Prüm.

Στο άρθρο 27 ορίζεται ότι αρμόδιες αρχές για την επεξεργασία είναι οι αρχές, οι φορείς και τα δικαστήρια που θα επιτελέσουν το σκοπό της επεξεργασίας κατά το άρθρο 26, ενώ η παροχή των δεδομένων σε άλλες οντότητες (άρα και σε ιδιώτες) γίνεται μετά την προηγούμενη συναίνεση του παρέχοντος Κράτους-μέλους και σύμφωνα με το δίκαιο του λαμβάνοντος.

Οι ρυθμίσεις που αφορούν την ακρίβεια, την επικαιροποίηση και τη διάρκεια αποθήκευσης των δεδομένων προσωπικού χαρακτήρα απαντούν στο άρθρο 28. Η αρμοδιότητα για τις διαδικασίες αυτές εμπίπτει στα Κράτη-μέλη, τα οποία οφείλουν να διορθώσουν και να διαγράψουν δεδομένα που ήταν εσφαλμένα ή δεν θα έπρεπε να έχουν παρασχεθεί, κοινοποιώντας παράλληλα στο κράτος που τα διέθεσε¹¹³. Αν η ακρίβεια των δεδομένων αμφισβητείται από το πρόσωπο στο οποίο αναφέρονται και η ακρίβεια (ή η ανακρίβεια) αυτή δεν είναι δυνατόν να αποδειχθεί, τα δεδομένα επισημαίνονται σύμφωνα με το εθνικό δίκαιο του κράτους που τα διέθεσε και μετά από αίτηση του προσώπου που αναφέρονται τα δεδομένα. Η εν λόγω επισήμανση μπορεί να αφαιρεθεί μόνο με άδεια του προσώπου ή βάσει απόφασης του αρμόδιου δικαστηρίου ή της ανεξάρτητης Αρχής προστασίας δεδομένων και πάντοτε σύμφωνα με το εθνικό δίκαιο του κράτους που διέθεσε τα δεδομένα¹¹⁴.

Η τελευταία διάταξη προβλέπει βέβαια ότι ο καθ' ου τα δεδομένα δύναται να αμφισβητήσει την ακρίβεια των δεδομένων. Η όλη προβληματική εδώ έγκειται στο ότι, βάσει του εθνικού μας δικαίου (άρθρο 3 παρ. 2 σε συνδυασμό με το άρθρο 11 παρ. 1 Ν. 2472/97), δεν παρέχεται δικαίωμα ενημέρωσης στο πρόσωπο, τα στοιχεία του οποίου τυγχάνουν επεξεργασίας στο πλαίσιο διερεύνησης εγκλημάτων. Το ζήτημα όμως θα αναλυθεί εκτενέστερα στο επόμενο Κεφάλαιο καθώς αφορά όλα τα δίκτυα ανταλλαγής πληροφοριών κι όχι μόνον την Απόφαση Prüm.

Στα άρθρα 29 και 30 περιγράφονται οι τεχνικές διαδικασίες και τα μέτρα ασφαλείας που θα πρέπει να λάβουν τα Κράτη-μέλη για τη διασφάλιση των δεδομένων προσωπικού χαρακτήρα στις δομές που θα δημιουργήσουν.

Ιδιαίτερη σημασία έχει το άρθρο 31, με το οποίο κατοχυρώνεται **δικαίωμα ενημέρωσης και αποζημίωσης** των προσώπων που αναφέρονται τα

¹¹³ Άρθρο 28 παρ. 1 Απόφασης Prüm.

¹¹⁴ Άρθρο 28 παρ. 2 Απόφασης Prüm.

δεδομένα. Η διάταξη αυτή συνδυάζεται με το προαναφερόμενο άρθρο 28. Σύμφωνα λοιπόν με το άρθρο 31, το πρόσωπο, το οποίο αφορούν τα δεδομένα, λαμβάνει, κατόπιν αίτησής του την οποία υποβάλλει σύμφωνα με το εθνικό δίκαιο¹¹⁵, πληροφορίες σχετικά με τα δεδομένα, τα οποία υποβλήθηκαν σε επεξεργασία όσον αφορά τα προσωπικά του στοιχεία, την προέλευσή τους, τον αποδέκτη ή τις ομάδες αποδεκτών, τον επιδιωκόμενο σκοπό της επεξεργασίας και τη νομική βάση της επεξεργασίας (εφόσον απαιτείται από το εθνικό δίκαιο), ενώ δύναται να ζητήσει και τη διόρθωση ανακριβών στοιχείων ή τα διαγραφή δεδομένων που υποβλήθηκαν παράνομα¹¹⁶.

Επιπλέον, θεμελιώνεται υποχρέωση των κρατών μελών να εξασφαλίσουν τη δυνατότητα στον καθ' ου να ασκήσει **αποτελεσματικό ένδικο βοήθημα** ενώπιον ανεξάρτητου δικαστηρίου κατά την έννοια του άρθρου 6 παρ. 1 της ΕΣΔΑ περί δίκαιης δίκης ή ενώπιον ανεξάρτητης Αρχής κατά την έννοια του άρθρου 28 της Οδηγίας 95/46/EK. Συναφώς θα πρέπει να του παρασχεθεί η δυνατότητα να ζητήσει αποζημίωση ή άλλης μορφής ικανοποίηση, στην περίπτωση που παραβιάζονται τα δικαιώματά του αναφορικά με την προστασία δεδομένων και σύμφωνα με όσα ορίζονται από τις οικείες εθνικές διατάξεις για την προστασία προσωπικών δεδομένων¹¹⁷.

¹¹⁵ Βλ. την παραπάνω προβληματική

¹¹⁶ Άρθρο 31 παρ. 1 εδ. α' Απόφασης Prüm.

¹¹⁷ Άρθρο 31 παρ. 1 εδ. β' και γ' Απόφασης Prüm.

V. Δικαστική και εξωδικαστική προστασία

1. Θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων

Το πρόσωπο του οποίου τα δεδομένα επεξεργάζονται στο πλαίσιο μιας ανταλλαγής πληροφοριών μέσω ενός δικτύου ανταλλαγής πληροφοριών αστυνομικής συνεργασίας είναι φορέας μιας σειράς δικαιωμάτων, τα οποία προστατεύονται δικαστικά ή εξωδικαστικά, σύμφωνα με την κείμενη νομοθεσία. Ο Ν. 2472/92 καθιερώνει τέσσερα θεμελιώδη δικαιώματα του υποκειμένου των δικαιωμάτων και συγκεκριμένα: το δικαίωμα ενημέρωσης (άρθρο 11), το δικαίωμα πρόσβασης (άρθρο 12), το δικαίωμα αντίρρησης (άρθρο 13 και το δικαίωμα δικαστικής προστασίας (άρθρο 14).

1.1. Το δικαίωμα ενημέρωσης

Το δικαίωμα ενημέρωσης¹¹⁸ προστατεύεται αυτοτελώς και αποτελεί βασική προϋπόθεση για την άσκηση των δικαιωμάτων πρόσβασης και αντίρρησης που θα εξεταστούν παρακάτω. Με το δικαίωμα ενημέρωσης κατοχυρώνεται η γενική αρχή της πληροφορικής αυτοδιάθεσης του ατόμου (ως υποκειμένου των δικαιωμάτων), από την οποία απορρέει το ειδικότερο δικαίωμά του να γνωρίζει ποιος, τι, από πού και για ποιο σκοπό συγκεντρώνει (συλλέγει και διατηρεί) δεδομένα που το αφορούν.

Σύμφωνα με την παρ. 1 του Ν. 2472/97, ο υπεύθυνος επεξεργασίας οφείλει, κατά το στάδιο της συλλογής δεδομένων, να ενημερώνει με πρόσφορο και σαφή τρόπο το υποκείμενο για τα εξής τουλάχιστον στοιχεία: α) για την ταυτότητά του και την ταυτότητα του εκπροσώπου του, β) για το σκοπό της επεξεργασίας, γ) για τους αποδέκτες ή για τις κατηγορίες αποδεκτών των δεδομένων, δ) για την ύπαρξη του δικαιώματος πρόσβασης.

Η Αρχή απαιτεί η παραπάνω ενημέρωση να περιλαμβάνει¹¹⁹: α) το ονοματεπώνυμο, την ακριβή διεύθυνση και τον αριθμό τηλεφώνου του

¹¹⁸ Το δικαίωμα ενημέρωσης καθιερώνεται στο άρθρο 11 του Ν.2472/97, στα άρθρα 10 και 11 της Οδηγίας 95/46/EK και στο άρθρο 8 (α) της Σύμβασης 108. Ομοίως, καθιερώνεται στο άρθρο 16 της Απόφασης 2008/977/ΔΕΥ και στο άρθρο 31 της Απόφασης Prum, πλην όμως τα δύο τελευταία νομικά κείμενα δεν έχουν ακόμη ενσωματωθεί στην εθνική μας έννομη τάξη.

¹¹⁹ Άρθρο 1, παρ. 2 της υπ' αριθμ. 1/1999 (ΦΕΚ 555 Β'/6-5-1999) Κανονιστικής Πράξης της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Η εν λόγω Κανονιστική Πράξη

υπευθύνου επεξεργασίας ή του εκπροσώπου του, προς τον οποίο τον υποκείμενο δύναται να απευθυνθεί για να ασκήσει τα δικαιώματα πρόσβασης και αντίρρησης (άρθρα 12 και 13 αντίστοιχα), β) το σκοπό της επεξεργασίας κατά τρόπο κατανοητό και σαφή, γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων, δ) την ύπαρξη του δικαιώματος πρόσβασης, ε) την ύπαρξη του δικαιώματος αντίρρησης για τα δικαιώματα που αφορούν το υποκείμενο. Ομοίως, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει το υποκείμενο και για κάθε επιγενόμενη μεταβολή των παραπάνω στοιχείων που περιλαμβάνει η ενημέρωση¹²⁰.

1.2. Το δικαίωμα πρόσβασης

Το δικαίωμα πρόσβασης συνίσταται στο να γνωρίζει το υποκείμενο των δικαιωμάτων, αν δεδομένα που το αφορούν αποτέλεσαν ή αποτελούν αντικείμενο επεξεργασίας. Όπως και το δικαίωμα ενημέρωσης, το δικαίωμα πρόσβασης προστατεύεται αυτοτελώς¹²¹ κι ουσιαστικά αποτελεί τη βάση της προστασίας των δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι διασφαλίζει τον έλεγχο του υπευθύνου επεξεργασίας για τη σύννομη επεξεργασία και το δεσμό του υποκειμένου με τα δεδομένα που το αφορούν.

Σύμφωνα με την παράγραφο 2 του άρθρου 2 του Ν. 2472/97, το υποκείμενο των δεδομένων έχει δικαίωμα να ζητήσει και να λάβει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση, με τρόπο σαφή και κατανοητό, τις εξής πληροφορίες:

α) Όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και την προέλευσή τους.

β) Τους σκοπούς της επεξεργασίας και τους αποδέκτες ή τις κατηγορίες αποδεκτών.

αφορά τη ρύθμιση του τρόπου ενημέρωσης των υποκειμένων των δεδομένων από τον υπεύθυνο επεξεργασίας σύμφωνα με το άρθρο 11 του Ν.2472/97.

¹²⁰ Άρθρο 1, παρ. 3 της υπ' αριθμ. 1/1999 Κανονιστικής Πράξης της Αρχής, ό.π.

¹²¹ Το δικαίωμα πρόσβασης καθιερώνεται στο άρθρο 12 του Ν.2472/97, στο άρθρο 12 της Οδηγίας 95/46/EK και στο άρθρο 8 (β) της Σύμβασης 108. Ομοίως, καθιερώνεται στο άρθρο 17 της Απόφασης 2008/977/ΔΕΥ και στο άρθρο 31 της Απόφασης Prum, πλην όμως, όπως προαναφέρθηκε, τα δύο τελευταία νομικά κείμενα δεν έχουν ακόμη ενσωματωθεί στην εθνική μας έννομη τάξη.

γ) Την εξέλιξη της επεξεργασίας των δεδομένων για το χρονικό διάστημα από την προηγούμενη ενημέρωσή ή πληροφόρησή του. Από τη διατύπωση της διάταξης καθίσταται σαφές ότι το υποκείμενο των δεδομένων μπορεί να ασκήσει το δικαίωμα πρόσβασης περισσότερες από μία φορές και κατά συνέπεια να ενημερώνεται και να έχει τη δυνατότητα να προβάλλει αντιρρήσεις για την επεξεργασία των δεδομένων του, εάν μεταβληθούν ή αν αντιτίθεται στην επεξεργασία τους.

δ) Τη λογική της αυτοματοποιημένη επεξεργασίας. Στο Προοίμιο 41 της Οδηγίας 46 επισημαίνεται ότι το υποκείμενο των δεδομένων πρέπει να γνωρίζει τη λογική της αυτοματοποιημένης επεξεργασίας των δεδομένων του, εφόσον από αυτή παράγεται απόφαση σε βάρος του, βασιζόμενη αποκλειστικά σε αυτοματοποιημένη επεξεργασία που αξιολογεί ορισμένες πτυχές της προσωπικότητάς του, όπως π.χ. η διαγωγή του¹²².

ε) Κατά περίπτωση, τη διόρθωση, τη διαγραφή ή τη δέσμευση (κλειδώμα) των δεδομένων, των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του Ν.2472/97, ιδίως λόγω του ελλιπούς ή ανακριβούς χαρακτήρα των δεδομένων.

στ) Την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή δέσμευσης (κλειδώματος) που διενεργείται σύμφωνα με την περίπτωση (ε), εφόσον τούτο δεν είναι αδύνατον ή δεν προϋποθέτει δυσανάλογες προσπάθειες.

Η παρ. 5 του άρθρου 12 του Ν.2472/97 παρέχει, όμως, τη δυνατότητα στον υπεύθυνο επεξεργασίας να αιτηθεί στην Αρχή να αποφασίσει την άρση της υποχρέωσης πληροφόρησης του υποκειμένου των δεδομένων, συνολικά ή εν μέρει, εφόσον η επεξεργασία γίνεται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

1.3. Το δικαίωμα αντίρρησης

Το δικαίωμα αντίρρησης¹²³ συνίσταται στη δυνατότητα του υποκειμένου των δεδομένων να αντιταχθεί στην επεξεργασία των δεδομένων που το

¹²² Βλ. σχετ. Προοίμιο 41 και άρθρο 15 παρ. 1 της Οδηγίας 95/46/EK, ό.π.

¹²³ Το δικαίωμα αντίρρησης καθιερώνεται στο άρθρο 13 του Ν.2472/97, στα άρθρα 12 (β), (γ) και 14 (β) της Οδηγίας 95/46/EK και στο άρθρο 8 (γ) της Σύμβασης 108. Ομοίως,

αφορούν και να ζητήσει τη διόρθωση, συμπλήρωση, διευκρίνιση ή ακόμη και τη διαγραφή τους.

Πιο συγκεκριμένα, το υποκείμενο των δεδομένων έχει δικαίωμα να απευθύνει τις αντιρρήσεις του στον υπεύθυνο επεξεργασίας εγγράφως, ζητώντας από αυτόν να προβεί σε συγκεκριμένη/ες ενέργεια/ες, όπως η διόρθωση, δέσμευση, μη διαβίβαση ή διαγραφή των δεδομένων που το αφορούν. Ο υπεύθυνος επεξεργασίας υποχρεούται να απαντήσει εγγράφως εντός δεκαπέντε ημερών, ενημερώνοντας το υποκείμενο των δεδομένων για τις ενέργειες που έχει προβεί ή εάν απέρριψε το αίτημα, για τους λόγους για τους οποίους απερρίφθη. Σε περίπτωση απόρριψης του αιτήματος, ο υπεύθυνος επεξεργασίας οφείλει να κοινοποιήσει την απάντησή του στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Μη εμπρόθεσμη ή μη ικανοποιητική απάντηση του υπευθύνου επεξεργασίας, δίνει τη δυνατότητα στο υποκείμενο των δικαιωμάτων να προσφύγει στην Αρχή, ζητώντας της να εξετάσει το αίτημά του. Στην περίπτωση αυτή, η Αρχή εξετάζει την προσφυγή κι αν διαπιστώσει ότι οι αντιρρήσεις είναι εύλογες, ήτοι δεν τηρήθηκαν οι προϋποθέσεις του άρθρου 4 του Ν. 2472/97 που διέπουν τη νομιμότητα της επεξεργασίας, κι ότι συντρέχει κίνδυνος σοβαρής βλάβης από τη συνέχιση της επεξεργασίας, δύναται να επιβάλει την άμεση αναστολή της επεξεργασίας, μέχρι να εκδώσει οριστική απόφαση επί των αντιρρήσεων¹²⁴.

Από τα παραπάνω συμπεραίνεται ότι το δικαίωμα αντίρρησης υπόκειται σε περιορισμούς που επιτρέπουν τη στάθμιση των εκατέρωθεν συμφερόντων κατά την άσκηση του δικαιώματος. Σε κάθε περίπτωση, η Αρχή είναι αυτή που καλείται να συγκεράσει τα αντικρουόμενα συμφέροντα του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων¹²⁵.

καθιερώνεται στο άρθρο 18 της Απόφασης 2008/977/ΔΕΥ και στο άρθρο 31 της Απόφασης Prum, πλην όμως, όπως προαναφέρθηκε, τα δύο τελευταία νομικά κείμενα δεν έχουν ακόμη ενσωματωθεί στην εθνική μας έννομη τάξη.

¹²⁴ Σχετικά με το δικαίωμα αντίρρησης βλ. σχετ. Αλεξανδροπούλου-Αιγυπτιάδου Ε., Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου τους, Αρμ. 59(2005)137, σελ. 140-141.

¹²⁵ Βλ. σχετ. Αλεξανδροπούλου-Αιγυπτιάδου Ε., ό.π., σελ. 142

1.4. Το δικαίωμα δικαστικής προσφυγής

Το δικαίωμα δικαστικής προσφυγής καθιερώνεται στο άρθρο 14 του Ν. 2472/97 και συνίσταται στη δυνατότητα του υποκειμένου των δεδομένων να αιτηθεί ενώπιον του αρμοδίου δικαστηρίου την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, η οποία έχει ληφθεί από διοικητική αρχή, νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου, ένωση προσώπων ή φυσικό πρόσωπο, αποκλειστικά με αυτοματοποιημένη επεξεργασία των στοιχείων του.

Αρμόδιο δικαστήριο για την προσβολή της πράξης ή της απόφασης που θίγει το υποκείμενο των δεδομένων είναι το διοικητικό δικαστήριο, αν η πράξη ή απόφαση είναι διοικητική, ή το πολιτικό δικαστήριο, αν η πράξη ή απόφαση είναι ιδιωτική¹²⁶.

2. Κυρώσεις

Τα άρθρα 21 έως 23 του Ν. 2472/97 περιέχουν κυρώσεις που επιβάλλονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και τα αρμόδια δικαστήρια για παραβάσεις των ρυθμίσεων του Νόμου και κάθε άλλης διάταξης που προβλέπει την προστασία του προσώπου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι κυρώσεις είναι τριών ειδών: διοικητικές, ποινικές και αστικές.

2.1. Διοικητικές κυρώσεις

Σύμφωνα με το άρθρο 21 του Ν. 2472/97, η Αρχή επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους της τις ακόλουθες διοικητικές κυρώσεις:

- α) Προειδοποίηση, με αποκλειστική προθεσμία άρσης της παράβασης (άρθρο 21, παρ. 1, στοιχείο α').
- β) Πρόστιμο ποσού από τριακόσιες χιλιάδες (300.000) έως πενήντα εκατομμύρια (50.000.000) δραχμές¹²⁷ (άρθρο 21, παρ. 1, στοιχείο β').

¹²⁶ Βλ. σχετ. Αρμαμέντου/Σωτηροπούλου, Προσωπικά δεδομένα - Ερμηνεία Ν.2472/1997, Αθήνα-Θεσσαλονίκη 2005, άρθρο 14, αρ. 839.

¹²⁷ Πλέον τα ποσά που αναφέρονται σε δραχμές νοούνται σε ευρώ. Μάλιστα, οπουδήποτε σε κείμενα νόμου και κανονιστικές πράξεις προβλέπονται χρηματικά ποσά σε δραχμές, τα ποσά αυτά, μετά τη μετατροπή και στρογγυλοποίησή τους σε ευρώ, είναι δυνατόν να

γ) Προσωρινή ανάκληση άδειας (άρθρο 21, παρ. 1, στοιχείο γ').

δ) Οριστική ανάκληση άδειας (άρθρο 21, παρ. 1, στοιχείο δ').

ε) Καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή, επιστροφή ή κλείδωμα (δέσμευση) των σχετικών δεδομένων (άρθρο 21, παρ. 1, στοιχείο ε').

Οι διοικητικές κυρώσεις των εδαφίων γ' και δ' αναφέρονται στις άδειες που εκδίδει η Αρχή βάσει του νόμου κι είναι η άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων (άρθρο 7 παρ. 2), η άδεια ίδρυσης και λειτουργίας αρχείου συλλογής και προστασίας ευαίσθητων προσωπικών δεδομένων (άρθρο 7 παρ. 2), η άδεια διασύνδεσης αρχείων που περιέχουν ευαίσθητα δεδομένων (άρθρο 8 παρ. 3) και η άδεια διασυννοριακής διαβίβασης δεδομένων προσωπικού χαρακτήρα, που έχουν τύχει επεξεργασίας ή πρόκειται να τύχουν επεξεργασίας μετά τη διαβίβασή τους σε χώρα εκτός Ε.Ε. (άρθρο 9).

Οι διοικητικές κυρώσεις των στοιχείων β' έως ε' της παρ. 1 του άρθρου 21 του Ν.2472/97 επιβάλλονται μετά από ακρόαση του υπευθύνου επεξεργασίας ή του τυχόν εκπροσώπου του, όπως άλλωστε επιβάλλει το άρθρο 20 παρ. 2¹²⁸ του Συντάγματος κι είναι ανάλογες με τη βαρύτητα της καταλογιστέας παράβασης¹²⁹. Επίσης, οι κυρώσεις των στοιχείων γ' έως ε' επιβάλλονται σε περιπτώσεις ιδιαίτερα σοβαρής ή καθ' υποτροπή παράβασης και σωρευτικά με αυτές τις κυρώσεις, δύναται να επιβληθεί και πρόστιμο. Τέλος, εάν επιβληθεί η κύρωση του στοιχείου ε', υπεύθυνος για την καταστροφή του αρχείου είναι ο υπεύθυνος επεξεργασίας στον οποίο μπορεί να επιβληθεί και πρόστιμο για μη συμμόρφωση (άρθρο 21, παρ. 2).

2.2. Ποινικές κυρώσεις

Το άρθρο 22 του Ν.2472/97 προβλέπει ποινικές κυρώσεις αφενός για πράξεις και παραλείψεις επί των οποίων η Αρχή δεν έχει ακόμη αποφανθεί και αφετέρου για μη συμμόρφωση σε αποφάσεις της Αρχής¹³⁰. Ειδικότερα:

αναπροσαρμόζονται με Κ.Υ.Α. των Υπουργών Οικονομικών και των κατά περίπτωση αρμόδιων Υπουργών (βλ. σχετ. άρθρο 19 του Ν.2842/2000 [ΦΕΚ 207 Α'/27-9-2000]).

¹²⁸ Άρθρο 20 παρ. 2 Συντάγματος: «Το δικαίωμα της προηγούμενης ακρόασης του ενδιαφερομένου ισχύει για κάθε διοικητική ή μέτρο που λαμβάνεται σε βάρος των δικαιωμάτων ή των συμφερόντων του».

¹²⁹ Με την εν λόγω διάταξη εισάγεται η αρχή της αναλογικότητας, την οποία πρέπει να λαμβάνει υπ' όψιν της η Αρχή, όταν εφαρμόζει την παράγραφο 1 του άρθρου 21.

¹³⁰ Βλ. Εισηγητική Έκθεση του Ν. 2472/97, σελ. 506

2.2.1. Για πράξεις και παραλείψεις επί των οποίων η Αρχή δεν έχει ακόμη αποφανθεί

Με ποινές φυλάκισης ενός έως τρία έτη και με χρηματική ποινή ενός έως πέντε εκατομμυρίων δραχμών, τιμωρείται όποιος συστήνει, λειτουργεί ή μεταβάλλει τους όρους και της προϋποθέσεις χορήγησης άδειας δημιουργίας αρχείου συλλογής και επεξεργασίας ευαίσθητων προσωπικών δεδομένων, καθώς και όποιος προβαίνει σε διασύνδεση αρχείων χωρίς άδεια της Αρχής (άρθρο 22 παρ. 1 έως 3).

Επίσης, με ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή ενός έως δέκα εκατομμυρίων δραχμών (εκτός αν τιμωρείται βαρύτερα με άλλη διάταξη) τιμωρείται όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών, τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιοδήποτε τρόπο (άρθρο 22 παρ. 4).

Ποινή κάθειρξης έως δέκα ετών και χρηματική ποινή δύο έως δέκα εκατομμυρίων δραχμών απειλείται, όταν ο υπαίτιος των παραβάσεων που αναφέρονται στις δύο προηγούμενες παραγράφους είχε σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο οικονομικό όφελος ή να βλάψει κάποιον τρίτο (άρθρο 22 παρ. 6). Επίσης, ο υπαίτιος των πράξεων των δύο προηγούμενων παραγράφων τιμωρείται έστω κι αν τέλεσε τις πράξεις από αμέλεια.

Τέλος, ποινή κάθειρξης και χρηματική ποινή πέντε έως δέκα εκατομμυρίων δραχμών επιβάλλεται και στις περιπτώσεις που από τις παραπάνω πράξεις προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια.

2.2.2. Για μη συμμόρφωση σε αποφάσεις της Αρχής

Σύμφωνα με την παρ. 5 του άρθρου 22 του Ν. 2472/97, με ποινή φυλάκισης τουλάχιστον δύο ετών και με χρηματική ποινή ενός έως πέντε εκατομμυρίων δραχμών τιμωρείται ο υπεύθυνος επεξεργασίας που δεν έχει συμμορφωθεί με τις αποφάσεις της Αρχής που εκδίδονται για την ικανοποίηση

των δικαιωμάτων πρόσβασης και αντίρρησης, καθώς και με τις διοικητικές κυρώσεις του άρθρου 21 του νόμου σχετικά με την προσωρινή ή οριστική ανάκληση άδειας, ή την καταστροφή αρχείου ή τη διακοπή επεξεργασίας και καταστροφή, επιστροφή ή κλείδωμα των σχετικών δεδομένων. Με τις ίδιες ποινές τιμωρείται ο υπεύθυνος επεξεργασίας, εάν διαβιβάζει δεδομένα κατά παράβαση του άρθρου 9 του νόμου σχετικά με τη διασυννοριακή ροή δεδομένων, καθώς και αν δεν συμμορφώνεται προς δικαστική απόφαση κατά το άρθρο 14 (δικαίωμα δικαστικής προσφυγής). Σημειώνεται ότι οι πράξεις ή παραλείψεις του υπευθύνου επεξεργασίας τιμωρούνται έστω κι αν τελεστούν από αμέλεια. Επίσης, προβλέπεται κι εδώ επαύξηση των ποινών για τις περιπτώσεις πρόκλησης κινδύνου στη λειτουργία του δημοκρατικού πολιτεύματος ή στην εθνική ασφάλεια, αλλά και για τις περιπτώσεις που ο δράστης σκοπεύει τον παράνομο προσπορισμό ή τη βλάβη τρίτου.

2.3. Αστικές κυρώσεις

Στο άρθρο 23 του Ν. 2472/97 προβλέπονται αστικές κυρώσεις σε φυσικά ή νομικά πρόσωπα ιδιωτικού δικαίου που κατά παράβαση του νόμου προκαλούν περιουσιακή ή ηθική βλάβη στα υποκείμενα των δεδομένων. Η ευθύνη στοιχειοθετείται κι όταν ο υπόχρεος όφειλε να γνωρίζει την πιθανότητα ότι θα επέλθει βλάβη σε άλλον.

3. Ζητήματα πρακτικής αποτελεσματικότητας του νομοθετικού καθεστώτος των δικαιωμάτων κατά την επεξεργασία δεδομένων στα δίκτυα ανταλλαγής πληροφοριών στο πλαίσιο της αστυνομικής συνεργασίας

3.1. Προλεγόμενα

Στο προηγούμενο Κεφάλαιο παρουσιάστηκαν οι προβλέψεις των δικαιωμάτων του υποκειμένου των δεδομένων στους διαύλους διασυννοριακής αστυνομικής συνεργασίας, ενώ στα προηγούμενα δύο υποκεφάλαια αυτού του Κεφαλαίου αναφέρθηκε συνοπτικά το περιεχόμενο των δικαιωμάτων και οι προβλεπόμενες στο νόμο κυρώσεις.

Στο παρόν υποκεφάλαιο θα επιχειρηθεί η εξέταση του πως ακριβώς εφαρμόζονται τα δικαιώματα αυτά στην Ελλάδα και συγκεκριμένα στα

ισχύοντα δίκτυα ανταλλαγής πληροφοριών αστυνομικής συνεργασίας, ήτοι στο Σύστημα Πληροφοριών Σένγκεν, στα εργαλεία της Ευρωπόλ και στα εργαλεία της Ιντερπόλ.

Καταρχήν θα πρέπει να επισημανθούν τα εξής:

α) Τα δίκτυα ανταλλαγής πληροφοριών λειτουργούν μέσω ενός εθνικού γραφείου σε κάθε Χώρα που είναι συμβαλλόμενο μέρος στη συνθήκη ίδρυσής τους.

β) Τα εθνικά γραφεία επεξεργάζονται δεδομένα που λαμβάνουν από εθνικά γραφεία άλλων χωρών και τα διαβιβάζουν στις αρμόδιες αρχές επιβολής του νόμου της Χώρας. Επίσης, λαμβάνουν πληροφορίες που συλλέγουν και επεξεργάζονται οι αρχές επιβολής του νόμου της Χώρας και τις διαβιβάζουν στα εθνικά γραφεία άλλων χωρών.

γ) Σύμφωνα με το άρθρο 19, παρ. 1, εδ. ιε' του Ν. 2472/97, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ασκεί ανεξάρτητο έλεγχο στο εθνικό γραφείο SIRENE που εφαρμόζει τη Σύμβαση Εφαρμογής της Συνθήκης Σένγκεν και αρμοδιότητες εθνικής εποπτικής αρχής στην Εθνική Μονάδα Ευρωπόλ που εφαρμόζει την Απόφαση Ευρωπόλ¹³¹. Επίσης, - αν και δεν αναφέρεται ρητά στο νόμο - ασκεί αρμοδιότητες εποπτείας στο Εθνικό Κεντρικό Γραφείο Ιντερπόλ.

3.2. Εφαρμογή του δικαιώματος ενημέρωσης

Όπως αναφέρθηκε στο Κεφάλαιο IV, η εφαρμογή του δικαιώματος ενημέρωσης στο πλαίσιο των δικτύων αστυνομικής συνεργασίας είναι προβληματική. Η παρ. 2 του άρθρου 3 του Ν. 2472/97 εξαιρεί από το πεδίο εφαρμογής του νόμου την επεξεργασία δεδομένων από τις αστυνομικές και δικαστικές αρχές, όταν ενεργούν στο πλαίσιο της απονομής δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων, που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά ζωής, κατά της γενετήσιας ελευθερίας, της οικονομικής

¹³¹ Το στοιχείο ιε' αναφέρεται στη Σύμβαση Ευρωπόλ που κυρώθηκε με το Ν. 2605/1998, πλην όμως, η εν λόγω Σύμβαση έχει αντικατασταθεί με την Απόφαση 2009/371/ΔΕΥ (Απόφαση Ευρωπόλ). Μάλιστα εν εξελίξει βρίσκεται η κατάρτιση νέας νομικής πράξης σε ευρωπαϊκό επίπεδο για την αντικατάσταση της Απόφασης Ευρωπόλ, η οποία θα έχει τη μορφή Κανονισμού.

εκμετάλλευσης της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, καθώς και εγκλημάτων σε βάρος ανηλίκων θυμάτων. Στις περιπτώσεις αυτές, ουσιαστικά δηλαδή στην πλειονότητα κατασταλτικών ερευνών των αστυνομικών ή των δικαστικών αρχών, εφαρμόζονται οι ισχύουσες ουσιαστικές και δικονομικές ποινικές διατάξεις.

Η προαναφερόμενη διάταξη - εξαίρεση, η οποία προστέθηκε σχετικά πρόσφατα¹³² στο Ν. 2472/97, σε πρώτη ανάγνωση φαίνεται λογική, καθώς από την πλευρά των οργάνων επιβολής του νόμου θα ήταν αναποτελεσματική για τους σκοπούς τους η καθιέρωση απόλυτης υποχρέωσης να ενημερώνουν ένα πρόσωπο που ερευνούν π.χ. για λόγους συμμετοχής του σε κάποια μορφή οργανωμένου εγκλήματος, σχετικά με την συλλογή δεδομένων για αυτό. Μια προσεκτικότερη ματιά όμως αναδεικνύει ορισμένα κρίσιμα ζητήματα που προκύπτουν από τη διάταξη.

Καταρχάς, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, γνωμοδότησε¹³³ ότι η εν λόγω διάταξη έρχεται σε αντίθεση με το δικαίωμα πληροφοριακής αυτοδιάθεσης, όπως κατοχυρώνεται στο Σύνταγμα. Συγκεκριμένα, στο άρθρο 9Α του Συντάγματος ορίζεται ότι: «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». Από το γράμμα της συνταγματικής διάταξης προκύπτει ότι η ανάθεση του ελέγχου τήρησης των κανόνων προστασίας προσωπικών δεδομένων μπορεί να δοθεί μόνον σε ανεξάρτητη Αρχή κι επομένως, ο νομοθέτης δύναται μόνο να θεσπίσει τους απαραίτητους κανόνες για την ορθολογική και αποτελεσματική οργάνωση της Αρχής. Κατά συνέπεια, δεν είναι ορθή κατά την Αρχή η παραχώρηση της ελεγκτικής αρμοδιότητας για την προστασία προσωπικών δεδομένων στις εισαγγελικές αρχές κατά το χρονικό διάστημα διερεύνησης ποινικών πράξεων

¹³² Η προσθήκη της διάταξης πραγματοποιήθηκε με το άρθρο όγδοο του Ν.3625/2007 (ΦΕΚ 290 Α'/24.12.2007).

¹³³ Βλ. τη γνωμοδότηση 1/2009 της ΑΠΔΠΧ, www.dpa.gr.

και απονομής δικαιοσύνης σύμφωνα με τα προβλεπόμενα στο άρθρο 3 παρ. 2 εδ. β' του Ν. 2472/97.

Επιπροσθέτως, δυσχερές στον προσδιορισμό είναι τόσο το χρονικό διάστημα, όσο και το πεδίο εξαίρεσης που αφήνει το άρθρο 3 παρ. 2 εδ. β' του Ν. 2472/97. Καθόσον δεν είναι σαφές ποιο είναι το χρονικό διάστημα της απονομής δικαιοσύνης, θα μπορούσε εύκολα να θεωρηθεί ότι περιλαμβάνει μέχρι και την έκδοση αμετάκλητης δικαστικής απόφασης που σε περιπτώσεις σοβαρών εγκλημάτων δύναται να ξεπεράσει τα πέντε έτη. Περαιτέρω, η διάταξη θέτει ένα μεγάλο πεδίο εξαίρεσης, ορίζοντας ότι αφορά όλα τα εγκλήματα που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο¹³⁴.

3.3. Εφαρμογή του δικαιώματος πρόσβασης

Η εφαρμογή του δικαιώματος πρόσβασης στο Σύστημα Πληροφοριών Σένγκεν πραγματοποιείται σύμφωνα με τις διατάξεις του άρθρου 12 του Ν.2472/97 και του άρθρου 114 παρ. 2 του Ν. 2514/97. Το υποκείμενο των δεδομένων απευθύνει επιστολή στον υπεύθυνο επεξεργασίας ο οποίος για τη Χώρα μας είναι το Εθνικό Γραφείο SIRENE της Διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας του Αρχηγείου της Ελληνικής Αστυνομίας. Στην εν λόγω επιστολή αιτείται να του γνωστοποιηθούν ποια προσωπικά του δεδομένα τηρούνται στα αρχεία της Υπηρεσίας. Ο υπεύθυνος επεξεργασίας οφείλει να απαντήσει εγγράφως εντός δεκαπέντε (15) ημερών. Σε περίπτωση μη εμπρόθεσμης ή μη ικανοποιητικής απάντησης, το υποκείμενο των δεδομένων μπορεί να υποβάλλει καταγγελία στην Αρχή και να ζητήσει να εξεταστεί το αίτημά του.

Όσον αφορά την εφαρμογή του δικαιώματος στα εργαλεία της Ευρωπόλ, όπως αναλύθηκε στο Κεφάλαιο IV της παρούσας, η αρμοδιότητα του ελέγχου της νομιμότητας καταχώρησης των δεδομένων ανήκει στα Κράτη-μέλη (άρθρο 29 παρ. 1 σημ. (α) Απόφασης Ευρωπόλ), τα οποία παρέχουν τη δυνατότητα άσκησης του δικαιώματος πρόσβασης σύμφωνα με την εθνική τους νομοθεσία. Στην ευθύνη της Ευρωπόλ ανήκει η διασφάλιση της ασφάλειας των δεδομένων μετά τη λήψη τους από τα Κράτη-μέλη, καθώς και η περαιτέρω διαβίβασή τους σύμφωνα με τους όρους που θέτουν κάθε φορά τα Κράτη-μέλη.

¹³⁴ Η αναφορά σε εγκλήματα κατά της ζωής, της γενετήσιας αξιοπρέπειας, κ.λπ. είναι ενδεικτική.

Βάσει του άρθρου 30 της Απόφασης Ευρωπόλ, το υποκείμενο των δικαιωμάτων απευθύνει αίτημα πρόσβασης στην Ευρωπόλ, μέσω της Αρχής Προστασίας Προσωπικών Δεδομένων. Η Αρχή οφείλει να διαβιβάσει το αίτημα στην Ευρωπόλ χωρίς καθυστέρηση κι όχι αργότερα από ένα μήνα από τη λήψη του αιτήματος, ενώ η Ευρωπόλ οφείλει απάντησης ομοίως χωρίς καθυστέρηση κι όχι αργότερα από χρονικό διάστημα τριών μηνών από τη λήψη του αιτήματος.

Απλούστερη διαδικασία προβλέπεται για την εφαρμογή του δικαιώματος πρόσβασης στα εργαλεία της Ιντερπόλ. Το υποκείμενο των δεδομένων απευθύνει αίτημα πρόσβασης απευθείας στην Επιτροπή για τον έλεγχο των αρχείων της Ιντερπόλ (CCF), βάσει του άρθρου 9 των Κανόνων σχετικά με τον Έλεγχο των πληροφοριών και της πρόσβασης στα αρχεία της Ιντερπόλ. Η Επιτροπή CCF δεν έχει χρονικό όριο απάντησης και απαντά μόνον στο υποκείμενο των δεδομένων ή στο νομικό εκπρόσωπό του.

3.4. Εφαρμογή του δικαιώματος αντίρρησης

Στο Σύστημα Πληροφοριών Σένγκεν και στα εργαλεία της Ευρωπόλ, το δικαίωμα πρόσβασης ασκείται κατά τον ίδιο τρόπο με τον οποίο ασκείται και το δικαίωμα πρόσβασης. Στα εργαλεία της Ιντερπόλ όμως δεν αναφέρεται ρητά αντίστοιχο δικαίωμα, καθώς νοείται ότι τα στοιχεία επικαιροποιούνται με ευθύνη των Εθνικών Κεντρικών Γραφείων, όπως προαναφέρθηκε στο Κεφάλαιο 4 της παρούσας. Ωστόσο, σημειώνεται ότι με τη νεοεισαχθείσα διάταξη του άρθρου 21 παρ. 3 των Κανόνων Επεξεργασίας Δεδομένων του Οργανισμού η οποία ενεργοποιήθηκε την 01/07/2013, δίδεται η δυνατότητα στα Εθνικά Κεντρικά Γραφεία να συνάψουν συμφωνίες με εθνικές (εποπτικές) αρχές οι οποίες και θα έχουν πρόσβαση στα εργαλεία της Ιντερπόλ, προκειμένου ασκήσουν το εποπτικό τους έργο.

VI. Επίλογος

Δεν υπάρχει αμφιβολία ότι η καταπολέμηση του οργανωμένου εγκλήματος, της τρομοκρατίας και γενικά του διασυνοριακού εγκλήματος απαιτεί την ταχύτατη ανταλλαγή πληροφορίας μεταξύ των αρχών επιβολής του νόμου, με τη χρήση των εργαλείων που προσφέρει η τεχνολογία. Προς αυτή την κατεύθυνση καταδείχθηκε στο πλαίσιο της παρούσας εργασίας ότι κινήθηκαν τα Κράτη και η Ευρωπαϊκή Ένωση δημιουργώντας όλο και πιο σύγχρονες δομές, αλλά και εισάγοντας την αρχή της διαθεσιμότητας στη λογική αναμόρφωσης των συστημάτων. Το νέο σύστημα πληροφοριών Σένγκεν (SIS II), τα εργαλεία της Ευρωπόλ, αλλά και η Σουηδική Πρωτοβουλία και η Απόφαση Prüm παρέχουν δυνατότητες μείωσης του χρόνου ανταπόκρισης των υπηρεσιών επιβολής του νόμου, καθώς και ποιοτικότερης επεξεργασίας δεδομένων μέσω των αντιστοιχήσεων δεδομένων και των αναλύσεων που πραγματοποιούν.

Στον κυκεώνα όμως αυτόν των βάσεων δεδομένων και της αυτοματοποιημένης μεταφοράς πληροφοριών προβάλλει αναγκαία και η αναβάθμιση του νομικού πλαισίου για την προστασία προσωπικών δεδομένων, η οποία είναι γεγονός ότι παρουσίαζε/παρουσιάζει υστέρηση στο πλαίσιο του πρώην Τρίτου Πυλώνα. Είναι γεγονός ότι η Απόφαση-Πλαίσιο 2008/977/ΔΕΥ έχει περιορισμένο πεδίο εφαρμογής, καθώς εφαρμόζεται μόνον στη διασυνοριακή επεξεργασία δεδομένων και όχι σε δραστηριότητες επεξεργασίας των αστυνομικών και δικαστικών αρχών σε αμιγώς εθνικό επίπεδο. Επιπλέον, λόγω της φύσης και του περιεχομένου της, αφήνει μεγάλο περιθώριο αποκλίσεων στο εθνικό δίκαιο, όσον αφορά την εφαρμογή των διατάξεών της, ενώ δεν περιέχει κανέναν μηχανισμό ούτε προβλέπει κάποια συμβουλευτική ομάδα ανάλογη της ομάδας εργασίας του άρθρου 29, η οποία να στηρίζει την κοινή ερμηνεία των διατάξεών της. Επίσης, δεν προβλέπει οποιεσδήποτε εκτελεστικές εξουσίες για την Επιτροπή, ώστε να διασφαλίζεται κοινή προσέγγιση κατά την εφαρμογή της.

Από τη Συνθήκη της Λισσαβώνας κι έπειτα, η κατάσταση αυτή δείχνει να αλλάζει. Σε Ανακοίνωσή της¹³⁵, η Ευρωπαϊκή Επιτροπή κατέληξε στο

¹³⁵ Ανακοίνωση της Ευρωπαϊκής Επιτροπής με τίτλο «Συνολική προσέγγιση όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση», COM(2010)609 τελικό, 4 Νοεμβρίου 2010.

συμπέρασμα ότι η Ε.Ε. χρειάζεται μια συνολικότερη και συνεκτικότερη πολιτική σχετικά με το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Βάσει της Συνθήκης (άρθρο 16 ΣΛΕΕ), Συμβούλιο και Ευρωπαϊκό Κοινοβούλιο ανέλαβαν να θεσπίσουν κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στους τομείς της δικαστικής συνεργασίας σε ποινικές υποθέσεις και της αστυνομικής συνεργασίας, οι οποίοι να καλύπτουν τόσο τη διασυνοριακή όσο και την εγχώρια επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Η πρωτοβουλία αυτή για ένα «πακέτο» Κανονισμού και Οδηγίας για την προστασία προσωπικών δεδομένων βρίσκεται – μαζί με την παράνομη μετανάστευση – στο επίκεντρο των διαβουλεύσεων στην Ένωση, και αναμένεται να ολοκληρωθούν οι σχετικές εργασίες εντός του έτους 2014.

VII. Βιβλιογραφία

• Ελληνική βιβλιογραφία

- ✓ *Αρμαμέντος Π., Σωτηρόπουλος Β., Προσωπικά δεδομένα – Ερμηνεία Ν. 2472/1997, Αθήνα-Θεσσαλονίκη 2005.*
- ✓ *Γέροντας Α., «Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων», Αθήνα-Κομοτηνή, 2002.*
- ✓ *Καλτσώνης Δ, Βία στα γήπεδα, οργανωμένο έγκλημα και τρομοκρατία, Συλλογικός Τόμος Οπαδική Βία, εκδ. Νόβολι, 2010.*
- ✓ *Μανωλεδάκης Ι, Δημοκρατία-Ελευθερία-Ασφάλεια, το τρίπτυχο της ιδανικής πολιτείας, στον τιμητικό τόμο για τον ίδιο, Δημοκρατία-Ελευθερία-Ασφάλεια, Σάκκουλας, 2005.*
- ✓ *Μίτλεττον Φ., Δικαίωμα στον πληροφοριακό αυτοκαθορισμό και δημόσια τάξη: Ο ρόλος της Αρχής, σε: Π. Δόνος, Λ. Μήτρου, Φ. Μίτλεττον, Ευ. Παπακωνσταντίνου, Η Αρχή Προστασίας Προσωπικών Δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων, στον τόμο Δίκαιο και Κοινωνία στον 21^ο αιώνα, Αθήνα-Θεσσαλονίκη 2002.*
- ✓ *Παρασκευόπουλος Ν., Οι πλειοψηφίες στο στόχαστρο: Τρομοκρατία και κράτος δικαίου, Πατάκης, 2003 .*
- ✓ *Σωτηρόπουλος Β., Η συνταγματική προστασία των προσωπικών δεδομένων, Σάκκουλας, 2006.*
- ✓ *Τάχου Α., Δίκαιο της δημόσιας τάξης, Σάκκουλας, 1990.*

• Ελληνική αρθρογραφία

- ✓ *Αλεξανδροπούλου-Αιγυπτιάδου Ε., Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου τους, Αρμ. 59(2005)137.*
- ✓ *Σωτηρόπουλος Β., 29/07/2009, ιστολόγιο E-Lawyer [elawyer.blogspot.gr/2009/07/blog-post_29.html].*
- ✓ *Καρδασιάδου Ζ., «Η εφαρμογή των αρχών της διαφάνειας, πρόληψης και υπευθυνότητας στο νέο νομοθετικό πλαίσιο», Εισήγηση στην επετειακή διημερίδα για τα 15 χρόνια λειτουργίας της ΑΠΔΠΧ, 24 Μαΐου 2013, σε Ενημερωτικό Δελτίο της ΑΔΠΧΠ*

<http://www.dpa.gr/pls/portal/docs/page/apdpx/newsmain/informational/july2013.pdf>.

• **Ξένη αρθρογραφία**

- ✓ *Alonso Blas D., First Pillar and third Pillar: Need for a common a approach on data protection?, Απρίλιος 2008, Ιστότοπος Πανεπιστημίου Εδιμβούργου, http://www2.law.ed.ac.uk/file_download/communities/92_article%20dab%20first%20pillar%20and%20third%20pillar%20april%202008.doc.*
- ✓ *Balzacq T., Bigo D., Carrera S. and Guild E., Security and the Two-level Game: The Treaty of Prüm, the EU and the Management of Threats, Ιανουάριος 2006, Έκθεση για το Ευρωπαϊκό Κέντρο Σπουδών Πολιτικής (Centre for European Policy Studies), <http://www.ceps.be/book/security-and-two-level-game-treaty-pr%C3%BCm-eu-and-management-threats>.*
- ✓ *Bigo D., Bruggeman W., Burgess P., Mitsilegas V., «The Principle of Information Availability», Μάρτιος 2007, διαδικτυακό περιοδικό Challenge: Liberty & Security, <http://www.libertysecurity.org/article1376.html>.*
- ✓ *Bunyan T., «The principle of availability», Δεκέμβριος 2006, Διαδικτυακό περιοδικό CILIP, Τεύχος 84.*
- ✓ *De Hert P., Bellanova R., “Data Protection in the area of freedom, security and Justice: a system still to be fully developed?”, Μάρτιος 2009, ιστότοπος: <http://www.fusl.ac.be/data1/publications/10/1425/8545.pdf>*
- ✓ *De Hert P., Papakonstantinou V., The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for, Διαδικτυακό περιοδικό Computer Law & Security Review, 2009, τεύχος 25.*
- ✓ *De Hert P., Papakonstantinou V. & Riehle C., “Data protection in the third pillar: cautious pessimism”, Crime, Rights and the EU, [Justice] 2008, (<http://www.vub.ac.be/LSTS/pub/Dehert/224.pdf>)*
- ✓ *Kierkegaard S., From Prüm to the EU, Presentation at the Computers, Privacy and Data Protection conference: Panel Session on Europol, Eurojust, Prüm and Beyond: New development in Justice and Home Affairs, 2009 (Brussels, 16-17 January).*

• Επιλεγμένη Ελληνική Νομοθεσία

- ✓ Ν. 3640/1956 «περί συμμετοχής της Ελλάδος εις την Διεθνή Επιτροπήν Εγκληματολογικής Αστυνομίας» (ΦΕΚ 303 Α'/28.12.1956)
- ✓ Ν. 2068/1992 σχετικά με την «Κύρωση της Ευρωπαϊκής Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα», ΦΕΚ 118 Α'/9.7.92.
- ✓ Ν. 2472/1997 σχετικά με την «προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ΦΕΚ 50 Α'/10.4.97, όπως τροποποιήθηκε ιδίως με το άρθρο όγδοο του Ν. 3625/07 σχετικά με την «Κύρωση, εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία και άλλες διατάξεις», ΦΕΚ 290 Α', 24.12.2007.
- ✓ Ν.2514/97 «Κύρωση: 1) της Συμφωνίας μεταξύ των Κυβερνήσεων των Κρατών της Οικονομικής Ένωσης του Μπένελουξ, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και της Γαλλικής Δημοκρατίας σχετικά με τη σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα, 2) της Σύμβασης Εφαρμογής της ανωτέρω Συμφωνίας μεταξύ των ιδίων Κρατών – Μελών, 3) των Πρωτοκόλλων και των Συμφωνιών προσχώρησης στις παραπάνω Συμφωνίες: της Ιταλικής Δημοκρατίας, του Βασιλείου της Ισπανίας, της Δημοκρατίας της Πορτογαλίας, της Ελληνικής Δημοκρατίας, της Αυστριακής Δημοκρατίας, της Φινλανδικής Δημοκρατίας, του Βασιλείου της Δανίας και του Βασιλείου της Σουηδίας, μετά των τελικών πράξεων, πρακτικών, δηλώσεων και κοινών δηλώσεων αυτών» (ΦΕΚ 140 Α'/26-6-97).
- ✓ Ν. 3671/2008 σχετικά με την «Κύρωση της Συνθήκης της Λισσαβώνας που τροποποιεί τη Συνθήκη για την Ευρωπαϊκή Ένωση, τη Συνθήκη περί ιδρύσεως της Ευρωπαϊκής Κοινότητας και ορισμένες συναφείς πράξεις», ΦΕΚ 129 Α', 3.7.2008.

• Επιλεγμένη Ευρωπαϊκή Νομοθεσία

- ✓ Σύμβαση 108 του Συμβουλίου της Ευρώπης της 28^{ης} Ιανουαρίου 1981 «για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα» (CETS 108) και Πρόσθετο Πρωτόκολλο

στη Σύμβαση για την προστασία των ατόμων σχετικά με την αυτόματη επεξεργασία προσωπικών δεδομένων, αναφορικά με τις εποπτικές αρχές και τη διασυνοριακή ροή δεδομένων της 8^{ης} Νοεμβρίου 2001 (CETS 181).

- ✓ Σύμβαση Εφαρμογής της Συμφωνίας του Σένγκεν της 14ης Ιουνίου 1985 μεταξύ των κυβερνήσεων των κρατών της Οικονομικής Ένωσης Μπενελούξ, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και της Γαλλικής Δημοκρατίας, σχετικά με τη σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα, EE L 239 της 22.9.2000, σ. 19.
- ✓ Πράξη του Συμβουλίου της 26ης Ιουλίου 1995 για την κατάρτιση της σύμβασης για την ίδρυση Ευρωπαϊκής Αστυνομικής Υπηρεσίας (σύμβαση Eurropol) δυνάμει του άρθρου Κ.3 της συνθήκης για την Ευρωπαϊκή Ένωση, 95/C 316/01 της 27/11/1995.
- ✓ Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών, EE L 8 της 12.1. 01, σ. 1.
- ✓ Κανονισμός (ΕΚ) αριθ. 1986/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Δεκεμβρίου 2006 σχετικά με την πρόσβαση στο Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) των υπηρεσιών των κρατών μελών που είναι υπεύθυνες για την έκδοση αδειών κυκλοφορίας οχημάτων, EE L 381 της 28.12.2006, σ. 1.
- ✓ Κανονισμός (ΕΚ) αριθ. 1987/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Δεκεμβρίου 2006 σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II), EE L 381 της 28.12.2006, σ. 4.
- ✓ Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, EE L 281 της 23.11.1995, σ. 31.
- ✓ Απόφαση 2007/533/ΔΕΥ του Συμβουλίου της 12ης Ιουνίου 2007 σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II), EE L 205 της 7.8.2007, σ. 63.

- ✓ Απόφαση 2009/371/ΔΕΥ του Συμβουλίου της 6ης Απριλίου 2009 για την ίδρυση Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Ευρωπόλ), ΕΕ L 121/37 της 15.5.2009.
- ✓ Απόφαση-πλαίσιο 2006/960/ΔΕΥ του Συμβουλίου, της 18ης Δεκεμβρίου 2006, για την απλούστευση της ανταλλαγής πληροφοριών και στοιχείων μεταξύ των αρχών επιβολής του νόμου των κρατών μελών της Ευρωπαϊκής Ένωσης, ΕΕ L 386 της 29.12.2006, σ. 89.
- ✓ Απόφαση 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, ΕΕ L 210 της 6.8.2008, σελ. 1.
- ✓ Απόφαση 2008/616/ΔΕΥ του Συμβουλίου, της 23ης Ιουνίου 2008, 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, ΕΕ L 210 της 6.8.2008, σ. 12
- ✓ Απόφαση 2008/617/ΔΕΥ του Συμβουλίου, της 23ης Ιουνίου 2008, για τη βελτίωση της συνεργασίας σε καταστάσεις κρίσεως μεταξύ των ειδικών μονάδων επέμβασης των κρατών μελών της Ευρωπαϊκής Ένωσης, ΕΕ L 210 της 6.8.2008, σ. 73.
- ✓ Απόφαση-Πλαίσιο του Συμβουλίου, της 13ης Ιουνίου 2002, για την καταπολέμηση της τρομοκρατίας, ΕΕ L 164 της 22.6.2002, σ. 3.
- ✓ Απόφαση 2009/934/ΔΕΥ του Συμβουλίου της 30ής Νοεμβρίου 2009 για τη θέσπιση κανόνων εφαρμογής που διέπουν τις σχέσεις της Ευρωπόλ με τους εταίρους της, περιλαμβανομένης της ανταλλαγής δεδομένων προσωπικού χαρακτήρα και διαβαθμισμένων πληροφοριών, ΕΕ L 325 της 11.12.2009, σ.6.