ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ - ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Διπλωματική Εργασία

του

Γιακουμή Ιωάννη

Θεσσαλονίκη, Ιούνιος 2019

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ - ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Γιακουμής Ιωάννης

Πτυχίο Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπουσα Καθηγήτρια
Ευγενία Αλεξανδροπούλου - Αιγυπτιάδου

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25/06/2019

Αλεξανδροπούλου Ευγενία	Μαυρίδης Ιωάννης	Γεωργιάδης Χρήστος
.....	.....	.....

Γιακουμής Ιωάννης

.....

Περίληψη

Ο βασικός σκοπός της παρούσας διπλωματικής εργασίας είναι να αναλύσει το νομικό πλαίσιο, τόσο σε Ευρωπαϊκό όσο και σε εθνικό επίπεδο, το οποίο σχετίζεται με την επεξεργασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Συν τοις άλλοις γίνεται αναφορά και σε πιθανούς κινδύνους για τα προσωπικά δεδομένα στο διαδίκτυο σε τεχνικό επίπεδο πέρα από το νομικό για ακόμα καλύτερη κατανόηση του εν λόγω ζητήματος από τον αναγνώστη και αναφέρεται η εξέλιξη του νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων στην Ευρώπη, από τις λεγόμενες ρυθμίσεις «πρώτης γενιάς» έως το σύγχρονο εθνικό κανονιστικό πλαίσιο και τις νομοθετικές πρωτοβουλίες της Ευρωπαϊκής Ένωσης. Συγκεκριμένα, η δομή της εργασίας είναι η εξής: στο πρώτο κεφάλαιο γίνεται μία σύντομη αναφορά στο υπό διερεύνηση θέμα και αναλύονται οι κίνδυνοι για τα προσωπικά δεδομένα στο διαδίκτυο και τα μέτρα ασφάλειας. Στο δεύτερο κεφάλαιο εξετάζεται το Ευρωπαϊκό νομοθετικό πλαίσιο και το τρίτο κεφάλαιο επικεντρώνεται στο Ελληνικό νομοθετικό πλαίσιο. Τέλος, η παρούσα διπλωματική εργασία καταλήγει με τα συμπεράσματα που προέκυψαν από την ανάλυση του υπό εξέταση ζητήματος.

Λέξεις Κλειδιά: *Ηλεκτρονικές επικοινωνίες, προσωπικά δεδομένα, Ευρωπαϊκή νομοθεσία, Ελληνικό νομοθετικό πλαίσιο*

Abstract

The main purpose of the current thesis is to analyze the legislative framework both on a European and on a national (Greek) level that is linked to the processing of personal data in the context of the e-communications. Furthermore, some potential risks, from the technical side, for the personal data are mentioned in order for the reader to be able to understand the subject better. Additionally, the current thesis examines the evolution of the legislative framework for the protection of private and personal data in Europe, from the so called “first generation” laws to the current legislative framework. More specifically, the structure of the thesis is as follows: the first chapter outlines shortly the under investigation subject and examines some risks for the personal data on the Internet. The second chapter analyses the European legislative framework and the third chapter focuses on the Greek legislation. Finally, the last part includes the main conclusions that were drawn by the analysis of the subject under investigation.

Keywords: *e-communications, personal data, European legislation, Greek legislative framework*

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια κα. Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία για τη σημαντική βοήθεια και καθοδήγηση κατά την εκπόνηση της παρούσας διπλωματικής εργασίας, καθώς επίσης και την οικογένεια μου, τους φίλους και τους συναδέλφους, για όλη τη στήριξη που μου παρείχαν από την έναρξη της συγγραφής μέχρι και την ολοκλήρωση της.

Περιεχόμενα

Κατάλογος Σχεδιαγραμμάτων/ Εικόνων

ΕΙΣΑΓΩΓΗ

Στο καινούριο περιβάλλον της τεχνολογίας της πληροφορίας, ο έλεγχος της πληροφορίας αλλά και η πρόσβαση σε αρκετές υπηρεσίες έχουν δημιουργήσει μία διαφορετική κοινωνική και οικονομική πραγματικότητα, η οποία χαρακτηρίζεται από την ταχύτατη ανάπτυξη των τηλεπικοινωνιακών δικτύων. Τα τηλεπικοινωνιακά δίκτυα άλλαξαν και μεταβλήθηκαν σε ψηφιακά μέσω των οποίων μεταδίδονται ταυτόχρονα ήχοι, εικόνες και δεδομένα και τα εν λόγω δίκτυα μέσα από την διαδικασία της σύγκλισης με τις τεχνολογίες πληροφορικής προκαλούν μία άνευ προηγουμένου εξέλιξη στον τρόπο διακίνησης, επεξεργασίας και αποθήκευσης της πληροφορίας. Στον σημερινό κόσμο της ψηφιακής τεχνολογίας ο τρόπος αντιμετώπισης των πληροφοριών, οι οποίες χαρακτηρίζονται ως προσωπικά δεδομένα, μεταβάλλεται συνεχώς. Οι ατομικές πληροφορίες μπορούν να αποθηκεύονται πλέον για απεριόριστο χρονικό διάστημα, σε μεγάλο αριθμό αντιτύπων και με πολύ χαμηλό κόστος, ενώ παράλληλα, η κάθε πληροφορία μπορεί να εξευρεθεί, να διοχετευθεί, να διανεμηθεί και επομένως, να αποκτήσει τεράστια οικονομική και στρατηγική σημασία, εάν χρησιμοποιηθεί ορθά.

Επομένως, όπως μπορεί να γίνει κατανοητό, η εξατομίκευση της πληροφορίας δίνει μεγάλο πλεονέκτημα σε όποιον την χρησιμοποιεί και μπορεί να την προσαρμόσει και να την κατευθύνει σε συγκεκριμένο αποδέκτη. Η σημασία της ψηφιακής τεχνολογίας στη διακίνηση της πληροφορίας επομένως, είναι μεγάλη, αφού επιτρέπει την ανάπτυξη μεθόδων marketing εξατομικευμένων και προσαρμοσμένων σε συγκεκριμένες ομάδες καταναλωτών. Με την πρόσβαση σε τέτοια δεδομένα προσωπικού χαρακτήρα, οι επιχειρήσεις και οι διάφοροι οργανισμοί μπορούν να αποκτούν τη δυνατότητα να πετυχαίνουν το σκοπό τους, ο οποίος συνδέεται με την στοχευμένη προώθηση των προϊόντων ή υπηρεσιών τους στους καταναλωτές. Ουσιαστικά με αυτή τη διαδικασία, η πληροφορία αποτελεί πλέον συναλλακτικό αγαθό με ιδιαίτερα μεγάλη αξία[1]. Συν τοις άλλοις, αξίζει να σημειωθεί ότι η οικονομία πλέον

[1] Μήτρου Λ. «Το δίκαιο στην Κοινωνία της Πληροφορίας», Σειρά : Δίκαιο Και Κοινωνία στον 21ο αιώνα, Εκδ Σάκκουλα, Αθήνα –Θεσσαλονίκη 2002, σελ.16 επ.

χαρακτηρίζεται από την ψηφιοποίηση των συναλλαγών, η οποία και μεταβάλλει τον τρόπο δημιουργίας, εμπορευματοποίησης και διανομής των προϊόντων και υπηρεσιών.

Φυσικά η μετατροπή αυτή του πολίτη σε «αντικείμενο» έχει και πολιτική σημασία πέρα από οικονομική. Η δυνατότητα καταγραφής της ιδιωτικής ζωής του ατόμου οδηγεί και σε άλλες πληροφορίες που αφορούν τις πολιτικές του πεποιθήσεις και δραστηριότητες. Επομένως, με αυτό τον τρόπο δίνεται η δυνατότητα να γίνει χρήση των προσωπικών του δεδομένων θέτοντας το άτομο στο στόχαστρο, είτε μίας πολιτικής διαφήμισης είτε των υπηρεσιών ασφαλείας μίας χώρας. Οι μεταβολές στις τεχνολογίες της πληροφορίας, που αλλάζουν με ταχύτατο ρυθμό, εντείνουν την ανησυχία ότι τα άτομα θα είναι συνεχώς εκτεθειμένα σε ανεπιθύμητη παρακολούθηση της ιδιωτικής τους ζωής χωρίς ουσιαστικές δυνατότητες προστασίας της[2]. Η διαδικασία επιβολής δικλείδων ασφαλείας, έτσι ώστε και η ιδιωτική ζωή των ατόμων να προστατεύεται αλλά και η ανάπτυξη της ψηφιακής οικονομίας να διασφαλίζεται, έχει καταστεί ένας σημαντικός σκοπός των σύγχρονων κοινωνιών και λόγω μίας σειράς εφαρμογών όπως το Facebook, το Instagram και το Twitter, τα οποία χρησιμοποιούνται από εκατομμύρια χρήστες στο διαδίκτυο[3].

Από τα ανωτέρω γίνεται αντιληπτό, ότι είναι προφανής η ανάγκη για μία όσο το δυνατό μεγαλύτερη και πιο οργανωμένη προσπάθεια σε διεθνές επίπεδο εγκαθίδρυσης υπερεθνικών νομικών κανόνων και νομοθετικού πλαισίου[4]. Για την αντιμετώπιση αυτής της κατάστασης το νομοθετικό πλαίσιο της κάθε χώρας σε διεθνές επίπεδο αλλάζει και προσαρμόζεται στα νέα τεχνολογικά δεδομένα, ώστε να μπορέσει να ισορροπήσει μεταξύ της ελεύθερης κυκλοφορίας πληροφοριών αλλά και της προστασίας τόσο του δημόσιου συμφέροντος όσο και του κάθε ατόμου ξεχωριστά[5]. Οι διεθνείς νομικές ρυθμίσεις σχετικά με την προστασία των προσωπικών δεδομένων συμβάλλουν στην όσο το δυνατόν ομοιόμορφη ενσωμάτωση και παραγωγή σχετικών ρυθμίσεων από τα διάφορα εθνικά δίκαια, τα οποία όμως διαμορφώνονται με τη σειρά τους σε εθνικό επίπεδο διαφορετικά, ώστε να ενσωματώνουν τις ανάγκες της εκάστοτε κοινωνίας.

[2] Tene. O. «Privacy, The New generations», International Data Privacy Law 2011
[3] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[4] Γεράρης Χ. «Τα προσωπικά δεδομένα και οι νέες προκλήσεις» ΔιΜΕΕ 2010
[5] Γεωργιάδη Γ. «Η σύναψη συμβάσεως μέσω διαδικτύου», Εκδ Αντ. Σάκκουλα, Αθήνα - Θεσσαλονίκη 2003

Όπως και σε άλλες χώρες, έτσι και στο χώρο της Ευρωπαϊκής Ένωσης, υπάρχει ένας κοινός σκοπός, ο οποίος είναι η εξασφάλιση της δυνατότητας των υποκειμένων της αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων να γνωρίζουν τις πληροφορίες που χρησιμοποιούν και επεξεργάζονται οι σχετικοί φορείς και κυρίως της δυνατότητας να ορίζουν τα ίδια τα υποκείμενα ποιες πληροφορίες θα διαθέσουν για επεξεργασία και σε ποιους[6]. Πέραν τούτου, ο καθορισμός ενός κανονιστικού πλαισίου που θα έχει ως στόχο να θέσει τις βάσεις και ορισμένους ρυθμιστικούς κανόνες αποδεκτούς και εφαρμόσιμους σε όλες τις χώρες της ΕΕ, είναι απαραίτητος για την καλύτερη προστασία των προσωπικών δεδομένων.

[6] Bygrave L. «Privacy in a Global Context-A Comparative Overview», Scandinavian Studies in Law, 2004

ΚΕΦΑΛΑΙΟ 1

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ, ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ

1.1 Προσωπικά δεδομένα[7] και κίνδυνοι στο Διαδίκτυο

Όπως έχει ήδη αναφερθεί παραπάνω, σχεδόν σε κάθε συναλλαγή ή πράξη που κάνει ένα άτομο μέσω του Διαδικτύου, δίνει ένα μέρος των προσωπικών του δεδομένων, τα οποία είναι ιδιαιτέρως σημαντικά για τον καθορισμό των προτιμήσεων του, αλλά και της προσωπικότητας του. Συνεπώς λοιπόν, γίνεται κατανοητό ότι υπάρχουν σημαντικά ζητήματα σχετικά με την ασφάλεια των εν λόγω δεδομένων, καθώς και την χρήση τους από τις διάφορες εταιρίες του Διαδικτύου όπως πχ. το Facebook.

Σε αυτό το σημείο είναι αναγκαίο να παρατεθεί ένας από τους πολλούς ορισμούς που υπάρχουν σχετικά με τα προσωπικά δεδομένα. Συγκεκριμένα, στο άρθρο 4 του Γενικού Κανονισμού Προστασίας Δεδομένων 2016/679(GDPR) δίδεται ο ακόλουθος ορισμός: «*δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.*

Παρόλο που τα προσωπικά δεδομένα έχουν ολοένα και μεγαλύτερη σημασία στη σημερινή εποχή της Κοινωνίας της Πληροφορίας, η ανάγκη προστασίας τους αλλά και οι διάφοροι κίνδυνοι που ελλοχεύουν δεν έχουν γίνει ακόμα κατανοητοί από την πλειονότητα των ανθρώπων. Ένας από τους λόγους της εν λόγω έλλειψης πλήρους κατανόησης των κινδύνων για τα προσωπικά δεδομένα είναι πιθανώς η μη κατανόηση ότι κίνδυνοι σχετικά με τα προσωπικά

[7] Βλέπε ενδεικτικά: Αλεξανδροπούλου- Αιγυπτιάδου Ε, «Προσωπικά Δεδομένα», Νομική Βιβλιοθήκη, 2016

δεδομένα υπάρχουν ακόμα και κατά τη διάρκεια απλών καθημερινών δραστηριοτήτων στο Διαδίκτυο. Η ανάγκη όμως προστασίας των εν λόγω δεδομένων έχει γίνει αντιληπτή, σε αντίθεση με ένα μεγάλο μέρος του πληθυσμού, από την πολιτεία η οποία έχει δημιουργήσει και ξεχωριστό νομικό πλαίσιο, στο οποίο υπάρχει ακριβής περιγραφή συγκεκριμένα για το είδος των πληροφοριών και προσωπικών στοιχείων, των οποίων μπορεί να γίνει χρήση από τρίτους. Συγκεκριμένα, το κράτος προστατεύει την ιδιωτικότητα του κάθε ατόμου ακόμα και όταν αυτή δεν αφορά τον πραγματικό κόσμο, αλλά και τον ψηφιακό μέσω των ψηφιακών αποτυπωμάτων του κάθε χρήστη, όπως είναι για παράδειγμα το ονοματεπώνυμο, οι φωτογραφίες, οι προτιμήσεις του χρήστη κτλ.

Για την κατανόηση όμως των διάφορων κινδύνων που καραδοκούν, είναι αναγκαίο να γίνει αναφορά και συζήτηση σχετικά με τα ίχνη που αφήνουν οι πράξεις ή συναλλαγές στο Διαδίκτυο. Συγκεκριμένα, με κάθε αποστολή ενός ηλεκτρονικού μηνύματος (e-mail) παρέχονται πληροφορίες στο εκάστοτε άτομο που λαμβάνει το e-mail. Σε περίπτωση που γίνει λάθος αυτές οι πληροφορίες που μπορεί να περιλαμβάνουν και κάποια προσωπικά δεδομένα, μπορούν σχετικά γρήγορα να σταλούν σε μεγάλο αριθμό ατόμων που δε θα έπρεπε να τα λάβουν. Αξίζει επίσης να τονιστεί, ότι οι διάφορες ομάδες συζητήσεων αποτελούν μία πιθανή πηγή ρίσκου σχετικά με τα προσωπικά δεδομένα των χρηστών που ανήκουν και δραστηριοποιούνται σε αυτές τις ομάδες, διότι το κάθε μέλος δεν έχει κάποιον περιορισμό ως προς τη συλλογή πληροφοριών και προσωπικών δεδομένων άλλων χρηστών από την εν λόγω ομάδα και τη διανομή τους. Σημαντικό είναι επίσης, να γνωρίζουν οι χρήστες του Διαδικτύου ότι κατά τη διάρκεια της χρήσης του αφήνουν ίχνη, τα οποία είναι σε μεγάλο βαθμό ανιχνεύσιμα. Συγκεκριμένα μέσω του φυλλομετρητή φαίνονται οι σελίδες που επισκέφτηκε ο χρήστης και μπορεί ακόμα και να παρέχονται πληροφορίες σχετικά με το e-mail του.

Επιπλέον, υπάρχουν και τα λεγόμενα «Cookies», μέσω των οποίων αρκετές ιστοσελίδες αποθηκεύουν στον υπολογιστή του χρήστη/επισκέπτη τα δεδομένα που αφορούν στην πλοήγηση του. Στην πραγματικότητα τα Cookies αποτελούν λίγες πληροφορίες όπως για παράδειγμα το όνομα του χρήστη, οι προτιμήσεις του, τα πράγματα που διάλεξε να αγοράσει κτλ[8]. Η πλειονότητα των (νόμιμων) διαδικτυακών εταιριών κάνει χρήση του εν λόγω εργαλείου, ώστε να μπορέσει να βελτιστοποιήσει τις υπηρεσίες της προς τους πελάτες/επισκέπτες της εκάστοτε

[8] Τανταλάκη Ν. «Κίνδυνοι και ασφάλεια στο διαδικτύο- δημιουργία κοινότητας πρακτικής για γονείς και μαθητές», Αριστοτέλειο Πανεπιστήμιο, 2010

σελίδας. Από την άλλη πλευρά όμως, υπάρχουν και διαδικτυακές εταιρίες που κάνουν παράνομη χρήση των Cookies με το να τα πουλάνε σε πολλές περιπτώσεις σε διαφημιστικές εταιρίες.

Επιπροσθέτως, σχετικά με τα ίχνη που αφήνει ο κάθε χρήστης στο Διαδίκτυο αξίζει να γίνει αναφορά στη χρήση των διαφόρων blogs (ιστολόγια), στα οποία γράφουν πολλά άτομα κυρίως νεαρής ηλικίας. Ο μεγάλος κίνδυνος της χρήσης ή της συμμετοχής στα εν λόγω blogs προκύπτει από το γεγονός ότι για να κάνει ένα άτομο εγγραφή και να μπορεί να συμμετάσχει σε αυτά χρειάζεται να δώσει κάποια από τα προσωπικά του στοιχεία όπως όνομα, το e-mail κτλ.

Πέραν των ανωτέρων όμως, αξίζει να γίνει αναφορά και στα στιγμιαία μηνύματα, όπως αυτά πραγματοποιούνται παραδείγματος χάριν μέσω του Facebook Messenger. Οι χρήστες οφείλουν να γνωρίζουν ότι η πλειονότητα των εταιριών (αν όχι όλες) μέσω των οποίων μεταδίδονται τα στιγμιαία μηνύματα, αποθηκεύουν τα προσωπικά δεδομένα και τις πληροφορίες που ανταλλάσσουν οι χρήστες μεταξύ τους. Όπως μπορεί να γίνει αντιληπτό τέτοιου είδους προσωπικά δεδομένα, αν δεν χρησιμοποιηθούν με ορθό τρόπο μπορούν να προκαλέσουν πρόβλημα στη ζωή του χρήστη είτε αυτό αφορά την επαγγελματική του ζωή είτε την προσωπική του.

Πέρα από τις γενικές πληροφορίες σχετικά με τα κοινωνικά δίκτυα, τα προσωπικά δεδομένα και τους κινδύνους που ελλοχεύουν, χρειάζεται να γίνει μία πιο λεπτομερής ανάλυση και παράθεση των βασικών κινδύνων που υπάρχουν στο διαδίκτυο και αντιμετωπίζουν οι περισσότεροι χρήστες του. Ορισμένες από τις βασικότερες κατηγορίες κινδύνων για τα προσωπικά δεδομένα είναι οι ακόλουθες:

Διαδικτυακοί Ιοί

Η διαδικασία αποστολής e-mail είναι ίσως η πλέον ευρέως διαδεδομένη μέθοδος ανταλλαγής πληροφοριών, ειδικά όταν πρόκειται για επιχειρήσεις και οργανισμούς. Τα βασικά πλεονεκτήματα της εν λόγω μεθόδου είναι η ταχύτητα μετάδοσης των πληροφοριών, αλλά και το γεγονός ότι έχει μηδενικό κόστος. Ακριβώς όμως για αυτό το λόγο τα e-mails είναι ο πιο συνηθισμένος τρόπος μετάδοσης των ιών[9]. Γενικά, οι ιοί στην αρχή όταν άρχισαν να δημιουργούνται είχαν ως βασικούς αποδέκτες προγραμματιστές, ενώ πλέον η φύση τους έχει

[9] Μαυρίδης Ι. «Ασφάλεια Πληροφοριών στο Διαδίκτυο», σελ. 21, ΣΕΑΒ, 2015

αλλάξει σημαντικά. Πλέον οι ιοί δημιουργούνται και αποσκοπούν στην υποκλοπή προσωπικών δεδομένων ή για άλλους εγκληματικούς σκοπούς ή ακόμα και για σκοπούς στρατιωτικής φύσεως, αν και η πιο διαδεδομένη χρήση των ιών είναι η κλοπή προσωπικών στοιχείων όπως π.χ. οι κωδικοί των καρτών. Ένας από τους πιο συνηθισμένους τρόπους μετάδοσης των ιών είναι μέσω αρχείων. Οι ιοί είναι στο αρχείο το οποίο κατεβάζει ο χρήστης από το Διαδίκτυο και με τη σειρά τους μολύνουν τον υπολογιστή του χρήστη, όταν αυτός ανοίγει το αρχείο ή αν διαβαστεί το e-mail που περιλαμβάνει το συγκεκριμένο αρχείο. Γενικά οι χρήστες οφείλουν να ανοίγουν e-mails και κυρίως να ανοίγουν ή να κατεβάζουν αρχεία μόνο από αξιόπιστες πηγές ή γνωστές διευθύνσεις e-mail και με μη ύποπτο θέμα. Όπως μπορεί να γίνει αντιληπτό, ακόμα και αν κάποιος χρήστης κάνει κάθε φορά ενδελεχή έλεγχο σχετικά με τα e-mails του είναι σημαντικό να έχει και κάποιο αποτελεσματικό αντιικό πρόγραμμα, το οποίο θα μπορεί να προστατεύει τον υπολογιστή[10].

Σκουλήκια (worms)

Με τον όρο worm νοείται ένα αυτόνομο πρόγραμμα που μπορεί να μεταπηδήσει από ένα σύστημα σε κάποιο άλλο. Αν και μοιάζουν με τους ιούς, εκ των πραγμάτων έχουν ορισμένες σημαντικές διαφορές. Συγκεκριμένα, ένα σκουλήκι για να πλήξει ένα σύστημα δεν είναι απαραίτητο να κάνει αλλαγή σε άλλο πρόγραμμα, διότι το ίδιο είναι πρόγραμμα που κάνει χρήση του Διαδικτύου και μέσω του οποίου εξαπλώνεται και αναζητεί εφαρμογές και συστήματα με ελλιπή προστασία, ώστε να μπορέσει να επεκταθεί ταχύτερα[11]. Η βασική διαφορά του σκουληκιού με τους ιούς, είναι ότι οι ιοί χρειάζονται την έγκριση ή τη συγκατάθεση του χρήστη, τον οποίον στοχεύουν, ώστε να μπορέσουν να τον πλήξουν. Τα σκουλήκια από την άλλη, δεν χρειάζονται καμία έγκριση ή συγκατάθεση, καθώς από τη στιγμή που θα ενεργοποιηθούνε, ψάχνουνε μόνα τους για κενά στα συστήματα ασφαλείας, εξαπλώνονται κτλ. Ένα από τα πιο διάσημα σκουλήκια ήταν το πρώτο που είχε εμφανιστεί το 1988 και είχε καταφέρει να εξαπλωθεί σημαντικά. Σε αυτό το σημείο είναι αναγκαίο να αναφερθεί, ότι το σκουλήκι πιθανότατα να μην το γνωρίζουν οι περισσότεροι χρήστες του Διαδικτύου, διότι δεν εμφανίζεται στους περισσότερους τόσο συχνά. Ο λόγος για τη μη συχνή του εμφάνιση, είναι

[10] Τανταλάκη Ν. «Κίνδυνοι και ασφάλεια στο διαδικτύο- δημιουργία κοινότητας πρακτικής για γονείς και μαθητές», Αριστοτέλειο Πανεπιστήμιο, 2010

[11] Μαυρίδης Ι. «Ασφάλεια Πληροφοριών στο Διαδίκτυο», σελ. 21, ΣΕΑΒ, 2015

κυρίως η δυσκολία της συγγραφής του, καθώς και πολλές φορές η μη συμβατότητα του με τα υπό απειλή υπολογιστικά συστήματα. Τέλος, ένα σκουλήκι μπορεί να βρίσκεται ακόμα και μέσα σε κάποιο script C++ ή σε ένα απλό αρχείο εκτέλεσης εντολών.

Δούρειοι ίπποι (Trojan)

Με τον όρο δούρειοι ίπποι (Trojan) χαρακτηρίζονται εκείνα τα προγράμματα που εκ πρώτης όψεως έχουν κάποιο όφελος για τους χρήστες, όμως εν τέλει ως απώτερο σκοπό έχουν την περάσουν από την ασφάλεια του υπολογιστή. Γενικά, οι Trojans είναι ευρέως διαδεδομένοι και εκμεταλλεύονται την απειρία πολλών χρηστών.

Ζόμπι (Zombies)

Τα Zombies είναι προγράμματα, τα οποία με κρυφό τρόπο μπαίνουν σε έναν υπολογιστή, ο οποίος είναι σε σύνδεση με το Διαδίκτυο και τον ελέγχουν, ώστε να τον χρησιμοποιήσουν για να προβούν σε επιθέσεις σε άλλους υπολογιστές που αποτελούν και τους πραγματικούς στόχους των εν λόγω προγραμμάτων. Η πλειοψηφία των στόχων τέτοιων προγραμμάτων είναι servers που έχουν πολλές συνδέσεις. Τέλος, τα εν λόγω προγράμματα μέσω αυτού του τρόπου καταφέρνουν να προχωρούν σε επιθέσεις μέσω των υπολογιστών άπειρων χρηστών και κρατάνε κρυφή την ταυτότητα των ατόμων που δημιούργησαν τα συγκεκριμένα προγράμματα.

Λαγοί (Rabbit programs)

Τα συγκεκριμένα προγράμματα αποτελούν ένα από τα παλαιότερα είδη προγραμματικής απειλής, αλλά όμως δεν αποσκοπούν κυρίως στην πρόκληση ζημιών σε διάφορα αρχεία, όπως τα άλλα προγράμματα που έχουν προαναφερθεί παραπάνω. Αντιθέτως, στοχεύουν στην αντιγραφή τους σε άπειρα ίδια προγράμματα και γενικά αποσκοπούν στο να επιβάλουν στον υπολογιστή να εκτελεί διάφορες εντολές χωρίς λόγο, απλά και μόνο για να μπορέσουν να χρησιμοποιήσουν το σύνολο των πόρων του με τελικό αποτέλεσμα τη διατάραξη της λειτουργίας του.

Λογική βόμβα (Logic Bomb)

Το εν λόγω είδος απειλής είναι κώδικας προγράμματος που εισέρχεται σε ένα σύστημα και μετά από κάποια συγκεκριμένη χρονική στιγμή εκτελείται. Πρακτικά, αυτό το είδος απειλής είναι επί της ουσίας ένας ιός που λειτουργεί σε μεταγενέστερο χρόνο και με άγνωστα επιβλαβή αποτελέσματα στο σύστημα που έχει εισέλθει. Ορισμένες απειλές μπορούν να ακυρωθούν προτού αρχίσει η εκτέλεση τους μέσω ad hoc ανίχνευσης και άλλες μέσω τακτικών ελέγχων.

Πίσω πόρτες (back doors)

Το συγκεκριμένο είδος ηλεκτρονικής απειλής είναι ένας κώδικας ή κομμάτια ενός κώδικα που είναι γραμμένα σε λειτουργικά συστήματα, ώστε να παρέχουν πρόσβαση σε άλλα προγράμματα παρακάμπτοντας ουσιαστικά τις όποιες ασφαλιστικές δικλείδες. Πρακτικά, αποτελούν εσκεμμένα κενά ασφαλείας και το όνομα τους έχει δοθεί από τους διάφορους εισβολείς που τα χρησιμοποιούσαν για να αποκτήσουν πρόσβαση σε άλλα προγράμματα που είχαν παραβιαστεί, χωρίς όμως να απαιτείται από τους εισβολείς να επαναλάβουν τις ίδιες ενέργειες από την αρχή. Οι back doors πέρα από το ότι είναι ένα σημαντικό πρόβλημα που σχετίζεται με την προσπάθεια ορισμένων προγραμματιστών να εισβάλουν σε κάποιο άλλο πρόγραμμα με κακόβουλο σκοπό, αποτελούν και κίνδυνο σε περίπτωση που ξεχαστούν από τους ίδιους τους σχεδιαστές ενός προγράμματος και δεν διορθωθούν διότι μπορεί να ανιχνευτούν από άλλα άτομα και να χρησιμοποιηθούν με μη σύννομο τρόπο.

Παρόλο που υπάρχουν και άλλοι ηλεκτρονικοί κίνδυνοι σχετικά με τα προσωπικά δεδομένα, οι ανωτέρω είναι οι βασικότεροι και οι πιο ευρέως διαδεδομένοι και βοηθούν τον αναγνώστη να αντιληφθεί πρακτικά τους κινδύνους που υπάρχουν στο Διαδίκτυο. Αξίζει σε αυτό το σημείο να γίνει μία σύντομη αναφορά στην περίπτωση της διαρροής δεδομένων χρηστών του Facebook στην Cambridge Analytica που προκάλεσε σημαντικές πολιτικές αναταράξεις στις ΗΠΑ. Συγκεκριμένα, η εν λόγω εταιρία προσέφερε συμβουλευτικές υπηρεσίες στον (πλέον) πρόεδρο Trump και ταυτόχρονα συνεργαζόταν και με έναν ερευνητή που χρησιμοποίησε τα προσωπικά δεδομένα όσων χρηστών του Facebook απαντούσαν σε ένα ερωτηματολόγιο, για να σχεδιάσει έναν αλγόριθμο σχετικά με το προφίλ του κάθε χρήστη και των διαδικτυακών φίλων του σε συνδυασμό με τις εκλογικές τάσεις/αποτελέσματα. Το αποτέλεσμα ήταν να απαντήσουν στο εν λόγω ερωτηματολόγιο 270.000 άτομα και να χρησιμοποιηθούν τα στοιχεία 87.000.000 χρηστών

του Facebook στις ΗΠΑ στους οποίους η Cambridge Analytica έστειλε πολιτικά μηνύματα, αναλόγως με το προφίλ του καθενός χρήστη. Παρόλο που επίσημα δεν έγινε κάποια παραβίαση συστημάτων ή ασφαλείας, το εν λόγω γεγονός δείχνει πόσο εύκολα μπορεί να υπάρξει διαρροή και λανθασμένη χρήση ευαίσθητων προσωπικών δεδομένων με την άγνοια του εκάστοτε χρήστη.

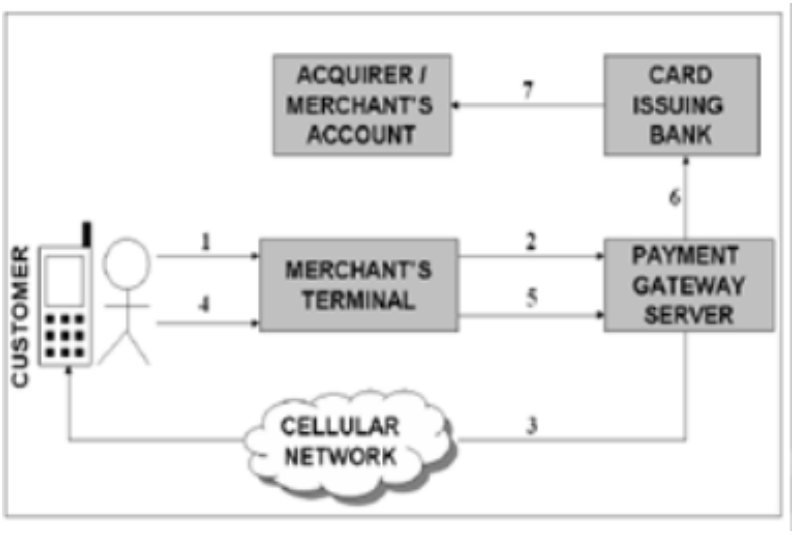
1.2 Ηλεκτρονικές συναλλαγές και ασφάλεια

Πέρα από ορισμένα γενικά στοιχεία για την ασφάλεια των προσωπικών δεδομένων στο Διαδίκτυο είναι αναγκαίο να αναλυθεί το ζήτημα των ηλεκτρονικών συναλλαγών και συγκεκριμένα, της ασφάλειας των προσωπικών δεδομένων που υπάρχουν και διακινούνται καθημερινά στις ηλεκτρονικές συναλλαγές.

Μία ηλεκτρονική συναλλαγή είναι παρόμοια με μία συναλλαγή με τηλέφωνο ή διά ζώσης, δηλαδή με φυσικό τρόπο[12]. Ουσιαστικά η διαδικασία είναι η ίδια σε μεγάλο βαθμό, διότι και στις ηλεκτρονικές συναλλαγές υπάρχει ένας πωλητής και ένας αγοραστής και σε πολλές περιπτώσεις παρεμβάλλονται ενδιάμεσα μέρη, όπως έμποροι, τράπεζες κ.ο.κ. Στην περίπτωση των ηλεκτρονικών συναλλαγών όμως, η όλη διαδικασία δεν γίνεται μέσω τηλεφώνου ή με φυσικό τρόπο στο κατάστημα που παρέχει τα προϊόντα, αλλά μέσω του Διαδικτύου και του ηλεκτρονικού υπολογιστή του εκάστοτε χρήστη[13]. Τα βασικά οφέλη του εν λόγω τρόπου συναλλαγών είναι το χαμηλό κόστος και η ευκολία χρήσης, διότι η ηλεκτρονική συναλλαγή μπορεί να γίνει όλη την ημέρα από πολλές διαφορετικές συσκευές (κινητό τηλέφωνο, υπολογιστής, φορητός υπολογιστής, tablet κτλ.). Από την άλλη όμως, τέτοιες συναλλαγές ενέχουν μεγάλους κινδύνους που σχετίζονται με την ασφάλεια των προσωπικών δεδομένων του χρήστη, τα οποία αυτός μοιράζεται με κάποιον οργανισμό στο Διαδίκτυο.

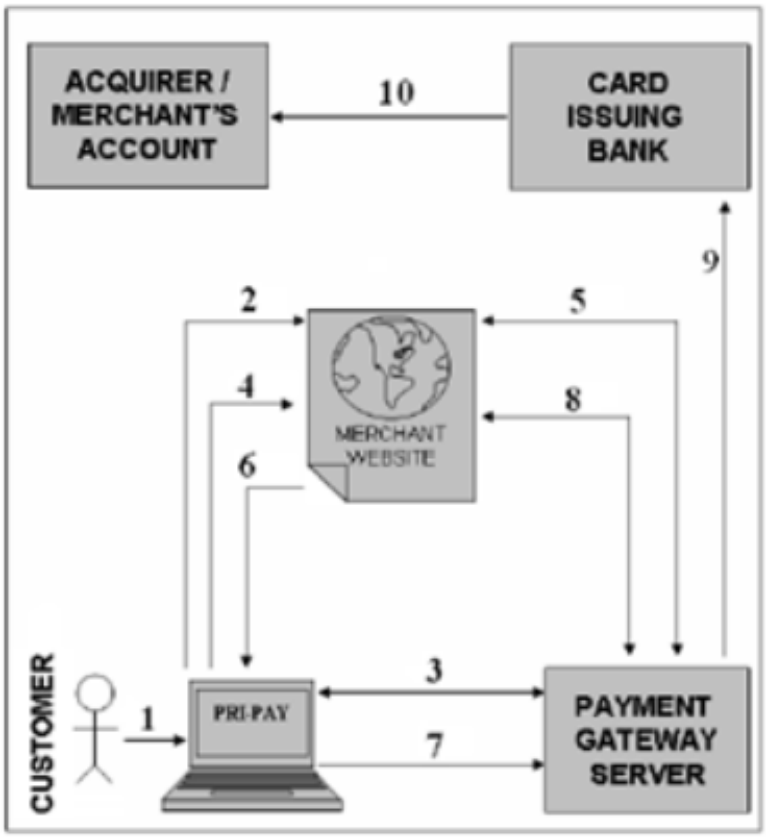
[12] Βλέπε σχεδιάγραμμα 1
[13] Βλέπε σχεδιάγραμμα 2

Σχεδιάγραμμα 1: Διαδικασία συναλλαγής με φυσικό τρόπο



Πηγή: Khandare (2013)

Σχεδιάγραμμα 2: Διαδικασία ηλεκτρονικής συναλλαγής



Πηγή: Khandare (2013)

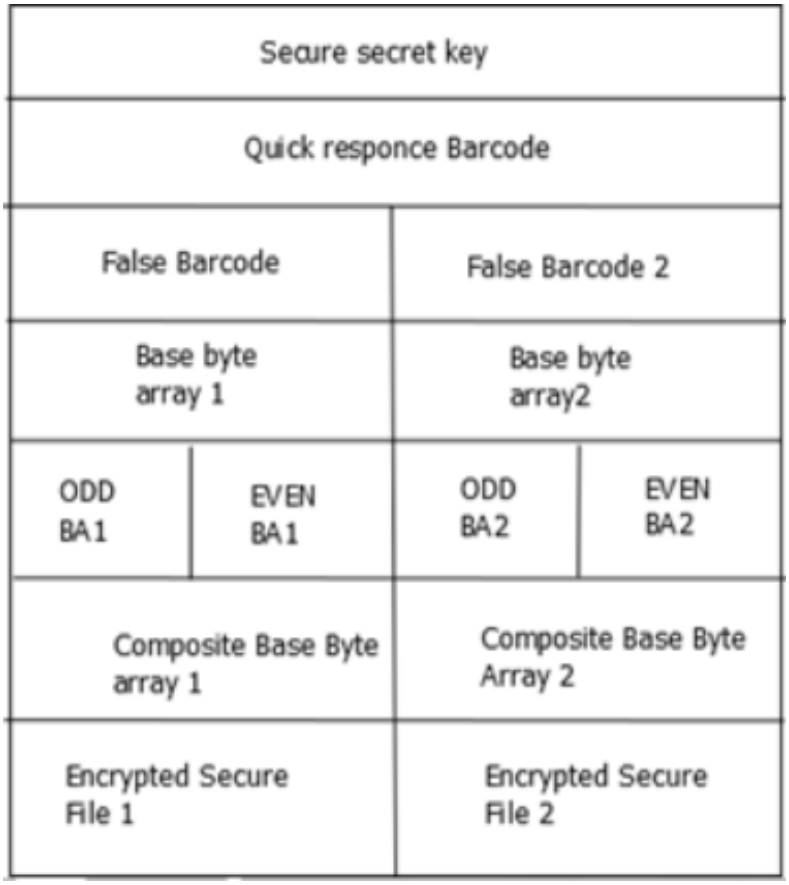
Συνεπώς λοιπόν, το βασικό στοιχείο κάθε ηλεκτρονικής συναλλαγής είναι η «ασφάλεια της μεταφοράς και διακίνησης ευαίσθητων δεδομένων» (sensitive data transfer secure- SDTS)[14]. Η SDTS συνδέεται άρρηκτα με την «ασφαλή ηλεκτρονική συναλλαγή» (Secure electronic transaction- SET) και με την κρυπτογραφία που βρίσκεται στα πρωτόκολλα με τα οποία διασφαλίζεται η ασφάλεια των ηλεκτρονικών συναλλαγών. Ένα βασικό εργαλείο για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές συναλλαγές είναι η επιβεβαίωση του χρήστη που επιθυμεί να κάνει μία συναλλαγή. Με αυτόν τον τρόπο μπορούν να αποφευχθούν περιπτώσεις που κάποιος τρίτος χρησιμοποιεί τους κωδικούς ενός χρήστη και προσπαθεί να κάνει συναλλαγές μέσω αυτού. Αν και υπάρχουν διάφοροι τρόποι επιβεβαίωσης του χρήστη,

[14] Βλέπε σχεδιάγραμμα 3

όπως ο απλός τρόπος που είναι κάποια ερώτηση σχετικά με κάτι προσωπικό που είχε ήδη προεπιλέξει ο χρήστης μέχρι και τη φωτογραφική επιβεβαίωση κάποιου κωδικού σε τραπεζικές συναλλαγές, εν τούτοις ο καλύτερος είναι ο βιομετρικός έλεγχος[15] για την επιβεβαίωση ενός χρήστη, ειδικά όταν η εν λόγω ηλεκτρονική συναλλαγή αφορά αντικείμενα ή υπηρεσίες αξίας.

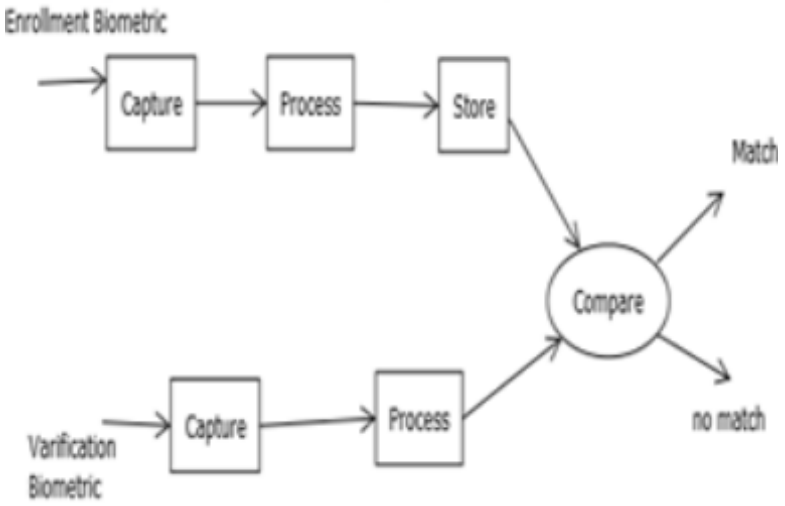
[15] Βλέπε σχεδιάγραμμα 4

Σχεδιάγραμμα 3: Απλοποιημένη μορφή της SDTS



Πηγή: Khandare (2013)

Σχεδιάγραμμα 4: Διαδικασία βιομετρικού ελέγχου και επιβεβαίωσης



Πηγή: Khandare (2013)

Παρόλο που οι ηλεκτρονικές συναλλαγές είναι πλέον μέρος της ζωής των περισσοτέρων ατόμων η ασφάλεια των προσωπικών δεδομένων σε αυτές ακόμα δεν είναι κάτι το αυτονόητο για τους περισσότερους ανθρώπους. Σε κάθε περίπτωση όμως χρειάζεται να γίνει κατανοητό ότι η ασφάλεια των προσωπικών δεδομένων και οι ηλεκτρονικές συναλλαγές είναι δύο πράγματα άρρηκτα συνδεδεμένα και τα οποία χρειάζονται το ένα το άλλο για να μπορούν λειτουργήσουν σωστά.

1.3 Ασφάλεια και προστασία- Firewall

Εφόσον λοιπόν, έχει γίνει αναλυτική συζήτηση τόσο σχετικά με τα προσωπικά δεδομένα όσο και με τους κινδύνους που σχετίζονται με αυτά και το Διαδίκτυο, τις ηλεκτρονικές συναλλαγές αλλά και τις τεχνικές ασφάλειας σε αυτές, χρειάζεται σε αυτό το σημείο να γίνει μία σύντομη αναφορά σε ορισμένα στοιχεία σχετικά με τη γενικότερη ασφάλεια και την προστασία στους ηλεκτρονικούς υπολογιστές. Συγκεκριμένα, ένας από τους πιο γνωστούς αμυντικούς μηχανισμούς ονομάζεται firewall και ουσιαστικά λειτουργεί συμπληρωματικά και συνεργατικά με τους υπόλοιπους μηχανισμούς ασφάλειας του εκάστοτε ηλεκτρονικού υπολογιστή. Ένα σύστημα firewall αποσκοπεί στον συνολικό έλεγχο, αλλά και στην καταγραφή όλων των προσπαθειών εισβολής ή απλά προσπέλασης στο σύστημα που βρίσκεται υπό προστασία ώστε

να μπορέσει με αυτούς τους ελέγχους να στέλνει τα διάφορα δεδομένα σε άλλη κατεύθυνση, αν χρειάζεται.

Πρακτικά, ένα σύστημα firewall αποτελεί ένα διαχωριστικό «φράχτη» μεταξύ του περισσότερο ασφαλούς δικτύου του υπολογιστή του εκάστοτε χρήστη και των διαφόρων δημόσιων δικτύων που δεν θεωρούνται τόσο ασφαλή. Συν τοις άλλοις, αξίζει να σημειωθεί ότι η βασική δυσκολία του εκάστοτε firewall αποτελεί η εύρεση και εφαρμογή των κριτηρίων, με βάση τα οποία γίνεται ο αποκλεισμός ή όχι ενός προγράμματος που προσπαθεί να προσπελάσει το υπό προστασία σύστημα. Εφόσον δεν υπάρχουν σαφείς οδηγίες/κατευθυντήριες γραμμές, τότε το firewall δεν μπορεί να λειτουργήσει αρκετά επαρκώς, όσο καλό και εάν είναι. Επομένως, τα firewalls που έχουν σαφείς οδηγίες και κατευθυντήριες γραμμές είναι αποτελεσματικά και αποτελούν την πρώτη γραμμή άμυνας και ασφάλειας του εκάστοτε υπολογιστή/ συστήματος. Χρειάζεται βέβαια σε αυτό το σημείο, να τονιστεί ότι η ύπαρξη ενός firewall δεν είναι η λύση σε κάθε πρόβλημα ασφαλείας του υπολογιστή και του δικτύου, καθώς επίσης ένα firewall δεν αποτελεί τη μοναδική μέθοδο ασφαλείας που μπορεί να χρησιμοποιηθεί. Επιπροσθέτως, είναι αναγκαίο να αναφερθεί ότι ένας επίδοξος αλλά ικανός εισβολέας μπορεί να βρει τρόπο να παρακάμψει ακόμα και το καλύτερο firewall. Πέραν τούτων, υπάρχουν και άλλα είδη από firewalls που χρησιμοποιούν τόσο τις δυνατότητες των proxy servers όσο και των inspection firewalls, αλλά αξίζει και να σημειωθεί ότι το μεγαλύτερο μέρος των firewalls έχουν υβριδική μορφή και χρησιμοποιούν περισσότερες από μία τεχνολογίες λόγω των θετικών στοιχείων της κάθε μίας.

Εφόσον έχουν συζητηθεί ορισμένα από τα βασικά στοιχεία των firewalls, χρειάζεται να αναφερθούν κάποια από τα βασικά είδη του συγκεκριμένου είδους προστασίας, τα οποία είναι τα ακόλουθα:

1. *Φιλτραρίσματος πακέτων(packet filter)*
2. *Εξέτασης κατάστασης (stateful inspection)*
3. *Επιπέδου κυκλώματος (circuit level-getaway)*
4. *Επιπέδου εφαρμογής (application level -gateway*

1) Packet filter

Το συγκεκριμένο είδος firewall δίνει τη δυνατότητα σε κάθε εισερχόμενο ή εξερχόμενο πρόγραμμα να περάσει προς το εσωτερικό δίκτυο και το Διαδίκτυο. Υπάρχει απαγόρευση της διέλευσης του, μόνο λόγω κάποιου ενεργοποιημένου κανόνα που χρησιμοποιεί ως βάση τον κανόνα του first fit basis. Ένα firewall της εν λόγω κατηγορίας δεν γνωρίζει τις δραστηριότητες των εφαρμογών, ενώ παράλληλα δεν ελέγχει την ταυτότητα των χρηστών, αλλά ούτε όμως και των διάφορων υπηρεσιών και προγραμμάτων που χρησιμοποιεί το εν λόγω υπό προστασία σύστημα. Πέραν των παραπάνω στοιχείων, το συγκεκριμένο είδος firewall καταγράφει μόνο τις πληροφορίες που παρέχονται από την IP διεύθυνση, δηλαδή παρέχει τον ελάχιστο βαθμό καταγραφής πληροφοριών.

2) Stateful inspection

Το συγκεκριμένο είδος firewall λειτουργεί με παρόμοιο τρόπο με το firewall της προηγούμενης κατηγορίας, αλλά με τη βασική διαφορά ότι διατηρεί αρχείο με τα προηγούμενα δεδομένα κατάστασης και τα συγκρίνει με ένα σύνολο ή μία ομάδα πακέτων. Σε περίπτωση που κάποιο πρόγραμμα καταφέρει να περάσει τον έλεγχο και εισέλθει στο σύστημα, τα δεδομένα του εισάγονται στην βάση δεδομένων του υπό εξέταση firewall. Συνεπώς, τα επόμενα παρόμοια προγράμματα επεξεργάζονται πιο γρήγορα από το υπό προστασία σύστημα , καθώς τα δεδομένα τους έχουν ήδη καταγραφεί με τρόπο παρόμοιο με το packet filter firewall.

3) Circuit level-getaway

Σε αντίθεση με το stateful inspection firewall που λειτουργούσε στο επίπεδο 3 του OSI, το circuit level-getaway firewall λειτουργεί στο επίπεδο 4, πραγματοποιώντας έλεγχο στην TCP επικεφαλίδα κάθε προγράμματος με βάση μια συγκεκριμένη ομάδα προκαθορισμένων κανόνων. Το εν λόγω firewall λειτουργεί με τον έλεγχο της δραστηριότητας μίας συνόδου του Διαδικτύου και η κάθε εφαρμογή αντιστοιχεί σε μία πόρτα. Συν τοις άλλοις, οι δυνατότητες καταγραφής γεγονότων μοιάζουν αρκετά με αυτές του packet filter firewall. Συνολικά, το συγκεκριμένο firewall λειτουργεί ως μία μοναδική αρχή ελέγχου, αφού ανοίγει πλήρως κάθε πρόγραμμα που επιχειρεί να εισέλθει στο υπό προστασία σύστημα διασφαλίζοντας έτσι μια μοναδική ασφαλή

ροή πληροφοριών, προστατεύει το υπό προστασία σύστημα από επιθέσεις κατακερματισμένων IP πακέτων.

4) Application level -gateway

Το συγκεκριμένο είδος firewall προχωράει ένα βήμα παραπέρα σε σχέση με τον έλεγχο των προγραμμάτων, αφού πραγματοποιεί ελέγχους στο επίπεδο 7 του OSI στην TCP επικεφαλίδα κάθε προγράμματος που προσπαθεί να εισέλθει στο υπό προστασία σύστημα με βάση μια συγκεκριμένη προκαθορισμένη ομάδα κανόνων, πραγματοποιώντας ταυτόχρονα έλεγχο της ροής των δεδομένων σε επίπεδο εφαρμογής. Παράλληλα, το εν λόγω είδος προστασίας έχει τη δυνατότητα να αναγνωρίζει εντολές των εφαρμογών και επιτρέπει ή απαγορεύει συγκεκριμένες εντολές, με αποτέλεσμα να προσφέρει ποιοτικό έλεγχο σχετικά με τη ροή των πληροφοριών στο σύστημα.

Αφού λοιπόν έγινε μία σύντομη αναφορά στα διάφορα είδη firewall που χρησιμοποιούνται συχνά, αξίζει να τονιστεί ότι ένα firewall μπορεί να έχει και άλλα οφέλη, όπως για παράδειγμα την απόκρυψη δικτύου (Network Address Translation - NAT). Σε αυτή την περίπτωση, το firewall είναι η μοναδική πύλη από και προς το υπό προστασία σύστημα, καθώς λαμβάνει μια IP διεύθυνση, η οποία είναι και η μόνη που είναι ορατή στο Διαδίκτυο, αποκρύπτοντας με αυτόν τον τρόπο τις εσωτερικές διευθύνσεις του δικτύου. Επιπροσθέτως, χρειάζεται να αναφερθεί και η επιπλέον υπηρεσία που προσφέρει η NAT, η οποία είναι η ανακατεύθυνση υπηρεσίας. Μέσω της συγκεκριμένης λειτουργίας προστατεύονται συγκεκριμένα τμήματα του συστήματος, τα οποία χρειάζονται μεγάλη προστασία από τους διάφορους επίδοξους εισβολείς. Για να γίνει κατανοητός ο συγκεκριμένος μηχανισμός ασφάλειας, αξίζει να αναφερθεί ένα σύντομο και πρακτικό παράδειγμα. Εάν ένα σύστημα έχει στο εσωτερικό του μία βάση δεδομένων, της οποίας τα στοιχεία και δεδομένα δεν πρέπει να είναι ανοιχτά σε χρήστες πέραν του εν λόγω συστήματος, τότε υπάρχει μία εικονική (virtual) βάση, η οποία παραμένει ανοιχτή στους εξωτερικούς χρήστες. Ταυτόχρονα, το firewall στέλνει τις αιτήσεις από την εικονική στην πραγματική βάση και το άμεσο αποτέλεσμα είναι η καλύτερη ασφάλεια και ο έλεγχος της εν λόγω βάσης δεδομένων.

Σε αυτό το σημείο αξίζει να αναφερθεί ότι όλες οι επιχειρήσεις που ασχολούνται με το ηλεκτρονικό εμπόριο και τις ηλεκτρονικές συναλλαγές έχουν υποχρέωση να προστατεύουν τα

προσωπικά δεδομένα των πελατών τους και να προβαίνουν σε ενέργειες, ώστε τα εν λόγω προσωπικά στοιχεία να μην είναι ανοιχτά και ευάλωτα σε μη εξουσιοδοτημένη προσπέλαση. Για αυτόν ακριβώς το λόγο τα firewalls χρησιμοποιούνται κατά κόρον από οργανισμούς που σχετίζονται με τις ηλεκτρονικές συναλλαγές, διότι μπορούν να ελέγχουν αποτελεσματικά την πρόσβαση στα συστήματα και τις βάσεις δεδομένων των εν λόγω οργανισμών και ουσιαστικά είναι ο πρώτος αμυντικός μηχανισμός απέναντι σε τυχόν εξωτερικές εισβολές. Επομένως, το συγκεκριμένο αμυντικό εργαλείο είναι ιδιαιτέρως χρήσιμο όσον αφορά τις ηλεκτρονικές συναλλαγές και την ασφάλεια των προσωπικών δεδομένων που διακινούνται στο Διαδίκτυο. Η αποτελεσματικότητα του αυξάνεται με τη διασύνδεση του στο Διαδίκτυο, πράγμα που συμβαίνει με όλες τις επιχειρήσεις ή τους οργανισμούς ηλεκτρονικών συναλλαγών, αφού έχουν συνεχώς τα συστήματα τους συνδεδεμένα με το Διαδίκτυο.

Πέρα από τα παραπάνω θετικά στοιχεία του firewall, χρειάζεται να αναφερθεί και η άποψη πολλών επικριτών της συγκεκριμένης μεθόδου προστασίας. Το επιχείρημα που χρησιμοποιείται εναντίον των firewalls αφορά τη δυσκολία που αυτά έχουν για τους χρήστες και επίσης ότι για να λειτουργήσουν σωστά χρειάζονται πολλές συνδέσεις. Επιπροσθέτως, τα firewalls κάνουν πιο δύσκολη και περίπλοκη την ελεύθερη πρόσβαση στο Διαδίκτυο, ενώ στην πραγματικότητα δεν παρέχουν απόλυτη ασφάλεια αλλά την αίσθηση απόλυτης ασφάλειας που μπορεί να έχει χειρότερα αποτελέσματα λόγω χαλάρωσης στα διάφορα μέτρα ασφαλείας. Παρόλο όμως όλα αυτά τα επιχειρήματα εναντίον των firewalls, η πλειονότητα των χρηστών συμφωνούν ότι αυτά είναι σημαντικά εργαλεία που βοηθούν στην ασφάλεια του εκάστοτε συστήματος, αλλά ποτέ δεν είναι σωστό να χαλαρώνουν οι υπόλοιποι μηχανισμοί ασφαλείας ενός συστήματος λόγω ύπαρξης των firewalls.

1.4 Ασφάλεια και προστασία- IDS (Intrusion Detection Systems)

Πέρα από το προαναφερθέν σύστημα ασφαλείας (firewall) υπάρχει μία ακόμη μέθοδος ασφαλείας που είναι ευρέως γνωστή και ονομάζεται σύστημα ανίχνευσης εισβολών (IDS). Η συγκεκριμένη μέθοδος αποσκοπεί στην ανίχνευση παράνομων δραστηριοτήτων που στοχεύουν στην απόκτηση και χρήση υπολογιστικών πόρων. Τα εν λόγω συστήματα βασίζονται σε διάφορες πληροφορίες από διαδικτυακές πηγές και έπειτα, τις αναλύουν και αναζητούν ενδείξεις εισβολής, προχωρώντας όμως και σε αναγκαίες ενέργειες για την προστασία του συστήματος

και αντιμετώπισης τυχόν εισβολών. Τόσο τα firewalls όσο και τα IDS είναι σίγουρα ένα σημαντικό αμυντικό εργαλείο της πολιτικής ασφάλειας των επιχειρήσεων που ασχολούνται με το ηλεκτρονικό εμπόριο και τις ηλεκτρονικές συναλλαγές.

Γενικά, τα IDS αυτοματοποιούν την διαδικασία ελέγχου, ανάλυσης, αναγνώρισης και αντίδρασης σε δραστηριότητες που μπορούν να θεωρηθούν ύποπτες για ενδεχόμενη εισβολή. Σε περίπτωση που το IDS προβαίνει στον έλεγχο αρχείων καταγραφής σε ένα συγκεκριμένο σύστημα ονομάζεται σύστημα ανίχνευσης εισβολής μεμονωμένου συστήματος και αξίζει να σημειωθεί ότι μία αποτελεσματική αρχιτεκτονική ασφαλείας περιέχει και τα απλά IDS αλλά και τα IDS που ελέγχουν τα αρχεία καταγραφής.

Όσο αφορά την εσωτερική δομή ενός IDS, είναι αναγκαίο να αναφερθεί ότι ένα απλό μοντέλο IDS έχει τη δυνατότητα να προσδιοριστεί από διαφορετικά μέρη, τα οποία εξαρτώνται μεταξύ τους. Χαρακτηριστικά, τέτοια μέρη μπορούν να είναι οι κατάλληλοι αισθητήρες για τη συλλογή δεδομένων, αλλά και η χρήση των γεγονότων για να ενημερωθεί καταλλήλως το προσωπικό. Σχετικά με την ανάλυση των δεδομένων που παίζει σημαντικό ρόλο σε κάθε σύστημα IDS, αξίζει επίσης να αναφερθεί ότι η αποθήκευση των δεδομένων, η αντίδραση σε πιθανές εισβολές και το γραφικό περιβάλλον για τον εκάστοτε χρήστη, μπορούν να λειτουργήσουν σε διαφορετικά συστήματα δείχνοντας όμως, το τελικό αποτέλεσμα του ελέγχου σε έναν κεντρικό διαχειριστή.

Βέβαια, παρόλο που τα IDS, όπως και τα firewalls αποτελούν ισχυρά εργαλεία για την ασφάλεια στους ηλεκτρονικούς υπολογιστές και τις ηλεκτρονικές συναλλαγές, εν τούτοις δεν είναι πανάκεια και δεν παρέχουν προστασία απέναντι σε κάθε πιθανή απειλή για το εκάστοτε σύστημα που χρήζει προστασίας.

ΚΕΦΑΛΑΙΟ 2

ΕΥΡΩΠΑΪΚΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

2.1 Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου

Μία από τις πρώτες νομοθετικές κινήσεις σε Ευρωπαϊκό επίπεδο για την προστασία των ανθρώπινων δικαιωμάτων έγινε με την Σύμβαση της Ρώμης για την «*προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών*», η οποία είχε ως σκοπό την ενίσχυση των δικαιωμάτων που αναφέρονταν στην «Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του Ο.Η.Ε»[16] και η οποία υπογράφτηκε την 4η Νοεμβρίου 1950 και τέθηκε σε ισχύ την 3η Σεπτεμβρίου 1953. Τελικά, κυρώθηκε από το ελληνικό κράτος με το Ν. 2329/1953 και το Ν.Δ 53/1974[17].

Σχετικά με την προστασία της ιδιωτικής ζωής αναφέρει το άρθρο 8 παρ.1 ότι κάθε πρόσωπο δικαιούται το σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. Συμπληρώνει την προστασία αυτή με τη δεύτερη παράγραφο, όπου ανάγει αυτή την προστασία σε υποχρέωση του κράτους και ειδικά, αναφέρει ότι δεν επιτρέπεται να υπάρξει επέμβαση δημοσίας αρχής κατά την άσκηση του δικαιώματος αυτού, εκτός εάν η επέμβαση προβλέπεται από νόμο και αποτελεί μέτρο το οποίο, σε μία δημοκρατική κοινωνία, είναι αναγκαίο για την εθνική ασφάλεια, τη δημόσια ασφάλεια, την οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων, την προστασία της υγείας ή της ηθικής, ή την προστασία των δικαιωμάτων και ελευθεριών άλλων[18].

Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (Ε.Σ.Δ.Α) αποτελεί το κύριο κείμενο αναφοράς όσον αφορά την προστασία των ανθρωπίνων δικαιωμάτων σε πανευρωπαϊκό

[16] http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

[17] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

[18] Καράκωστα Ι. «Η προστασία του ιδιωτικού βίου των προσώπων της επικαιρότητας από τη σκοπιά του συγκριτικού δικαίου» ΔΕΕ 1999 σελ.1229 επ.

επίπεδο[19] και αποτέλεσε ένα πρότυπο υπερεθνικής προστασίας των ανθρωπίνων δικαιωμάτων το οποίο οδήγησε στην υπογραφή της Αμερικανικής Σύμβασης Δικαιωμάτων του Ανθρώπου το 1969[20], του Αφρικανικού Χάρτη των Ανθρώπινων Δικαιωμάτων και των Δικαιωμάτων των Λαών το 1981[21] και του Αραβικού Χάρτη των Δικαιωμάτων του Ανθρώπου το 1994[22].

Η Ε.Σ.Δ.Α καθόρισε και έθεσε σε εφαρμογή την προστασία αυτή με την δημιουργία του ανάλογου δικαιοδοτικού μηχανισμού[23], του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου. Όπως επισημαίνεται, η κατοχύρωση από τη Σύμβαση όχι μόνο ουσιαστικών δικαιωμάτων, αλλά και του δικαιώματος του ατόμου να προσφεύγει στον δικαιοδοτικό της μηχανισμό, «*αποτελεί ένα αυθεντικά επαναστατικό μέτρο στη μεταπολεμική διεθνή κοινωνία, πρόκληση για μια επαναδιαπραγμάτευση, κάτω από τις νέες πολιτικοκοινωνικές πραγματικότητες, της θέσεως του ατόμου ως υποκειμένου του διεθνούς δικαίου*»[24].

2.2 Ευρωπαϊκά νομοθετήματα «πρώτης γενιάς»

Η πρώτη νομοθετική προσπάθεια σε ευρωπαϊκό επίπεδο για την προστασία των προσωπικών δεδομένων, έγινε στη Γερμανία το 1970, με τον νόμο για την προστασία των προσωπικών δεδομένων του κρατιδίου της Έσσης. Ο εν λόγω νόμος δημιούργησε για πρώτη φορά ανεξάρτητη ρυθμιστική αρχή και εξέφρασε τη ρυθμιστική λογική που υπήρχε στη Γερμανία, όπου η κανονιστική παρέμβαση ενός κράτους, η οποία έχει ως στόχο τη ρύθμιση συμπεριφορών πρέπει να υποστηρίζεται από ρυθμιστικές αρχές που θα προστατεύουν τα δικαιώματα των πολιτών έναντι του κράτους[25]. Επιπροσθέτως η Σουηδία ήταν και αυτή από τις πρωτοπόρες στην παραγωγή νομοθεσίας, όταν το 1973 εξέδωσε έναν νόμο για την προστασία των προσωπικών δεδομένων (Datalag) δημιουργώντας και αυτή μία εποπτεύουσα Αρχή για να επιβλέπει την

[19] Ματθία Σ. « Εισαγωγή στη Ευρωπαϊκή σύμβαση για τα δικαιώματα του ανθρώπου» ΕλλΔνη 1999 σελ. 729 επ.
[20] http://www.cidh.org/Basicos/English/Basic3.American%20Convention.html
[21] http://www.achpr.org/english/_info/charter_en.html
[22] http://www1.umn.edu/humanrts/instree/loas2005.html?msource=UNWDEC19001&tr=y&auid=333
[23] Μπακόπουλος Ι. «Ανθρώπινα Δικαιώματα στην Ευρωπαϊκή Έννομη Τάξη», ΕλλΔνη 2002 σελ. 54 επ.
[24] Περράκη Σ. « Διαστάσεις της διεθνούς προστασίας των δικαιωμάτων του ανθρώπου» τόμ. Α΄, Εκδ Αθήνα-Κομοτηνή 1991, σελ. 93 επ.
[25] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

αυτοματοποιημένη επεξεργασία δεδομένων είτε αυτή γίνεται από κρατικό είτε από ιδιωτικό φορέα[26].

2.3 Ευρωπαϊκά νομοθετήματα «δεύτερης γενιάς»

Μέσα στις συνθήκες ταχύτατων εξελίξεων στις τεχνολογίες πληροφορικής και επικοινωνιών, ήταν ξεκάθαρο ότι το άρθρο 8 της Ε.Σ.Δ.Α δεν επαρκούσε για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής, η οποία βρισκόταν σε περιβάλλον διακινδύνευσης[27]. Η επιθυμία για ένα σύγχρονο νομοθέτημα που να απαντά στην ανάγκη για καθορισμό των αρχών της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και των δικαιωμάτων των υποκειμένων της επεξεργασίας αυτής οδήγησε στη θέσπιση της Σύμβασης του Στρασβούργου[28]. Η εν λόγω σύμβαση 108/1981 «*για την προστασία των ατόμων από την αυτόματη επεξεργασία προσωπικών δεδομένων*» είναι το πρώτο διεθνές νομικά δεσμευτικό κείμενο για την προστασία προσωπικών δεδομένων[29]. Στο πρώτο άρθρο της ορίζεται ο σκοπός της σύμβασης που είναι η εξασφάλιση στην επικράτεια κάθε μέρους και για κάθε άτομο, ανεξαρτήτως της ιθαγένειας ή διαμονής του, του σεβασμού των δικαιωμάτων του και των θεμελιωδών ελευθεριών και ιδιαίτερα το δικαίωμα στην ιδιωτική ζωή, σε σχέση με την αυτόματη επεξεργασία προσωπικών δεδομένων που σχετίζονται με αυτό («προστασία δεδομένων»)»[30]. Η σύμβαση καθιέρωσε τις γενικές αρχές οι οποίες πρέπει να διέπουν την αυτόματη επεξεργασία των προσωπικών δεδομένων και αποτέλεσαν τον οδηγό για τη μετέπειτα παραγωγή νομοθετημάτων σε εθνικό και κοινοτικό επίπεδο, όπως η αρχή της νόμιμης συλλογής και επεξεργασίας, η αρχή του καθορισμένου και νόμιμου σκοπού της επεξεργασίας, η αρχή της αναγκαιότητας της επεξεργασίας, η αρχή της ακρίβειας των δεδομένων, η αρχή της χρονικά πεπερασμένης

[26] http://www.itkommissionen.se/dynamaster/file_archive/030121/991899fe86e3aecaa92d4e5730148f50/5.1%20%20Security%20and%20Vulnerability%20-%20S%F6ren%20%D6man.pdf
[27] Προοίμιο της Σύμβασης 108
[28] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[29] Νόμος 2068/1992. (ΦΕΚ Α' 118/9.7.1992), με τον οποίο επικυρώθηκε η σύμβαση
[30] http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

διατήρησης των δεδομένων[31]. Επί της ουσίας το άρθρο 5 της Σύμβασης 108 αναφέρει ότι τα δεδομένα θα πρέπει:

α) Να έχουν αποκτηθεί και να γίνεται η επεξεργασία τους με νόμιμο και θεμιτό τρόπο, δηλαδή είτε ότι τα υποκείμενα των δεδομένων θα πρέπει να συγκατατίθενται σε αυτή την επεξεργασία είτε ότι η σχετική νομοθεσία θα πρέπει να θέτει τις προϋποθέσεις και τους σκοπούς της συλλογής και της επεξεργασίας αυτής[32]

β) Να αποθηκεύονται και να φυλάσσονται μόνο για συγκεκριμένους και νόμιμους σκοπούς και να μην χρησιμοποιούνται με οποιονδήποτε τρόπο ασύμβατο προς τους σκοπούς αυτούς[33], έτσι ώστε να περιορίζεται η ποσότητα και τα είδη των επεξεργαζόμενων πληροφοριών

γ) να είναι επαρκή, σχετικά και όχι περισσότερα από όσα απαιτούνται ενόψει των σκοπών για τους οποίους φυλάσσονται[34]

δ) να είναι ακριβή και σε κάθε περίπτωση που αυτό θεωρείται αναγκαίο, να ενημερώνονται[35]

ε) τέλος, τα δεδομένα όχι μόνο πρέπει να είναι όσα χρειάζονται για την επίτευξη των σκοπών για τους οποίους και γίνεται η επεξεργασία τους, αλλά θα πρέπει να φυλάσσονται μόνο για το αναγκαίο χρονικό διάστημα που απαιτείται, έτσι ώστε πέραν αυτού να μην είναι δυνατός ο προσδιορισμός του υποκειμένου, το οποίο αφορούν.

Συν τοις άλλοις, λόγω του ότι η επεξεργασία προσωπικών δεδομένων μπορεί να αποκαλύψει φυλετική καταγωγή, πολιτικές και θρησκευτικές πεποιθήσεις και πληροφορίες σχετικές με την υγεία και τη σεξουαλική ζωή αλλά ακόμα και ποινικές καταδίκες, χρειάζεται να ληφθούν κάποιες δικλείδες ασφαλείας[36]. Η ίδια σύμβαση στο άρθρο 8 προέβλεψε μία σειρά βασικών δικαιωμάτων του υποκειμένου της επεξεργασίας, όπως το δικαίωμα της ενημέρωσης για τους

[31] http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
[32] Bignami F. «The Case for Tolerant Constitiuonal Patriotism: The right to Privacy Before the European Courts» ό.π. σελ.221
[33] Άρθρο 5 παρ.2 της Σύμβασης 108
[34] Άρθρο 5 παρ.3 της Σύμβασης 108
[35] Άρθρο 5 παρ.4 της Σύμβασης 108
[36] Άρθρο 6 της Σύμβασης 108

σκοπούς της τήρησης αρχείου δεδομένων και το δικαίωμα της διόρθωσης ή διαγραφής των δεδομένων αυτών[37].

2.4 Ευρωπαϊκά νομοθετήματα «τρίτης γενιάς»

Η προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Κοινότητα εκφράστηκε με την παρέμβαση στο χώρο του παράγωγου κοινοτικού δικαίου[38]. Συγκεκριμένα, το 1995 υιοθετήθηκε η κοινοτική οδηγία 95/46/ΕΚ ως ένα γενικό πλαίσιο προστασίας των προσωπικών δεδομένων βασισμένη στην κωδικοποίηση της Σύμβασης του Στρασβούργου του 1981 «*για την προστασία των ατόμων από την αυτόματη επεξεργασία προσωπικών δεδομέ*νων»[39]. Η νομική βάση της ήταν το άρθρο 100Α (πλέον άρθρο 95) της Συνθήκης της Ευρωπαϊκής Ένωσης, πλην όμως η διακήρυξη του χάρτη των θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης[40] από το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Επιτροπή το Δεκέμβριο του 2000 και ειδικότερα, το άρθρο 8 του Χάρτη αυτού που προβλέπει το δικαίωμα προστασίας των δεδομένων, έδωσε μεγαλύτερη έμφαση στη διάσταση «προστασία των θεμελιωδών δικαιωμάτων» της οδηγίας.

Με την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου η Ευρωπαϊκή Ένωση απέκτησε ένα από τα πιο συνεκτικά και αναλυτικά νομοθετικά κείμενα που επηρέασαν και επηρεάζουν παγκοσμίως τη διεθνή κανονιστική παραγωγή σε θέματα προστασίας προσωπικών δεδομένων[41]. Στόχος της εν λόγω οδηγίας υπήρξε η προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα[42], ως αναγκαία προϋπόθεση για την ομαλή λειτουργία της εσωτερικής αγοράς για

[37] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[38] Στάγκο Π.και Σαχπεκίδου Ε. «Δίκαιο των Ευρωπαικών Κοινοτήτων και της Ευρωπαικής Ένωσης», Εκδ Σάκκουλα Αθήνα- Θεσσαλονίκη 2000 σελ.197 επ.
[39] 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, ΕΕ L 281 της 23.11.1995, σελ. 31
[40] http://europa.eu.int/comm/justice_home/unit/charte/index_en.html
[41] 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, ΕΕ L 281 της 23.11.1995, σελ. 31
[42] Άρθρο 1 παρ.1 της Οδηγίας 95/46/ΕΚ

την οποία απαιτείται όχι μόνο η δυνατότητα κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών, αλλά και η προστασία των θεμελιωδών δικαιωμάτων του ατόμου με τρόπο ομοιόμορφο σε όλα τα Κράτη Μέλη[43]. Η προστασία αυτή θα μπορούσε να επιτευχθεί μόνο μέσω του καθορισμού κατευθυντήριων αρχών που προσδιορίζουν τη νομιμότητα της επεξεργασίας των προσωπικών δεδομένων. Το άρθρο 32 της οδηγίας έθεσε στα Κράτη Μέλη τριετή προθεσμία για τη προσαρμογή τους προς τους κανόνες αυτούς, τα οποία σύμφωνα με το άρθρο 249 (πρώην 189) δεσμεύονται για την άμεση και πλήρη εφαρμογή τους[44]. Η οδηγία σε συμφωνία με την Σύμβαση 108 περιέχει τις κατευθυντήριες αρχές για την επεξεργασία των προσωπικών δεδομένων[45].

Οι συγκεκριμένες κατευθυντήριες αρχές αφορούν τα ακόλουθα:

1. την ποιότητα των δεδομένων, δηλαδή τα δεδομένα προσωπικού χαρακτήρα που θα πρέπει συγκεκριμένα να αποτελούν αντικείμενο θεμιτής επεξεργασίας και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς, να είναι ακριβή και, αν χρειάζεται, ενημερωμένα[46]

2. τη νόμιμη επεξεργασία των δεδομένων: δηλαδή η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν μπορεί να γίνεται, παρά μόνο αν το άτομο, στο οποίο ανήκουν τα δεδομένα έχει κατά τρόπο αναμφισβήτητο δώσει τη συναίνεσή του ή αν η επεξεργασία είναι απαραίτητη σε συγκεκριμένα αναφερόμενες περιπτώσεις. Ειδικά, η ρύθμιση της προηγούμενης συγκατάθεσης αποτέλεσε και την σημαντικότερη ίσως νομοθετική παρέμβαση και ρύθμιση ιδιαίτερης σημασίας για τη διασφάλιση και επαύξηση της προστασίας δεδομένων με αντίκτυπο σε παγκόσμιο επίπεδο, καθώς έρχεται σε αντίθεση με το αμερικάνικο κανονιστικό πλαίσιο προστασίας των προσωπικών δεδομένων, όπου ισχύει η αρχή του opt-out, κατά την οποία τα υποκείμενα της επεξεργασίας έχουν τη δυνατότητα να αρνηθούν την χρήση των προσωπικών δεδομένων, εάν το επιθυμούν[47]

[43] Αιτιολογική σκέψη 3 της Οδηγίας 95/46/ΕΚ
[44] Λουκέρη Γ. «Εναρμόνιση του δικαίου της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση, ΝοΒ 1997 σελ. 547 επ.
[45] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[46] Άρθρο 6 παρ.1 της Οδηγίας 95/46/ΕΚ
[47] Bouckaert J., Degryse H. «Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies», 2005

Επιπροσθέτως, η εν λόγω οδηγία εισήγαγε την έννοια των ευαίσθητων προσωπικών δεδομένων ρυθμίζοντας ειδικές κατηγορίες για τις οποίες κατ' αρχήν απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως η φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε συνδικαλιστικές οργανώσεις και η υγεία και η σεξουαλική ζωή[48]. Ακολούθως, η αρχή του πληροφοριακού αυτοκαθορισμού υλοποιείται με την πρόβλεψη του δικαιώματος πρόσβασης των προσώπων αυτών στα δεδομένα[49], καθώς και την εισαγωγή του δικαιώματος στη διόρθωση, τη διαγραφή ή την απαγόρευση της πρόσβασης τρίτων στα δεδομένα, όπως και του δικαιώματος αντίταξης στην επεξεργασία δεδομένων[50]. Στην εν λόγω οδηγία αναπτύσσονται πολύ σημαντικές διατάξεις που προβλέπουν ότι επιτρέπονται οι μεταβιβάσεις δεδομένων προσωπικού χαρακτήρα από κράτος μέλος σε τρίτη χώρα, υπό την προϋπόθεση ότι αυτή η χώρα διαθέτει το κατάλληλο επίπεδο προστασίας[51]. Η συγκεκριμένη ρύθμιση χαρακτηρίζεται ως ιδιαίτερα σημαντική λόγω της ξεχωριστής βαρύτητας που δίνεται και της διασυνοριακής ροής δεδομένων προσωπικού χαρακτήρα ως μοχλό ανάπτυξης των διεθνών εμπορικών συναλλαγών[52].

2.5 Ευρωπαϊκός κανονισμός 2016/679

Γενικά, η έννοια της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα στην Ευρωπαϊκή Ένωση. Συγκεκριμένα το άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») και το άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) ορίζουν ότι, «*κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν*». Η οικονομική και κοινωνική ολοκλήρωση, η οποία προέκυψε από τη λειτουργία της εσωτερικής αγοράς, είχε ως αποτέλεσμα τη σημαντική αύξηση των διασυνοριακών ροών δεδομένων προσωπικού χαρακτήρα. Οι εθνικές αρχές των κρατών μελών καλούνται από το δίκαιο της Ένωσης να συνεργάζονται και να ανταλλάσσουν δεδομένα προσωπικού χαρακτήρα, προκειμένου να μπορούν να εκτελούν τις υποχρεώσεις τους.

[48] Άρθρο 8παρ.1 της Οδηγίας 95/46/ΕΚ
[49] Άρθρο 12 της Οδηγίας 95/46/ΕΚ
[50] Άρθρο 14 παρ.1 της Οδηγίας 95/46/ΕΚ
[51] Άρθρο 22 της Οδηγίας 95/46/ΕΚ
[52] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

Γενικότερα, οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Το εύρος της συλλογής και της ανταλλαγής δεδομένων προσωπικού χαρακτήρα αυξήθηκε σημαντικά. Η τεχνολογία, πλέον, επιτρέπει με πολύ μεγάλη ευκολία τη χρήση δεδομένων προσωπικού χαρακτήρα σε μια εκτεταμένη κλίμακα . Τα φυσικά πρόσωπα ολοένα και περισσότερο δημοσιοποιούν προσωπικές πληροφορίες και τις καθιστούν διαθέσιμες σε παγκόσμιο επίπεδο. Η τεχνολογία έχει επιφέρει αλλαγές τόσο στην οικονομία όσο και στην κοινωνική ζωή, ενώ καλείται να διευκολύνει περαιτέρω την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα, όχι μόνο εντός της Ένωσης, αλλά και τη διαβίβαση αυτών σε Τρίτες χώρες και Διεθνείς οργανισμούς, διασφαλίζοντας, παράλληλα, υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα. Όπως μπορεί να γίνει κατανοητό, οι εξελίξεις αυτές χρειάζονται ένα ισχυρό και πιο συνεκτικό πλαίσιο προστασίας των δεδομένων στην ΕΕ, υποστηριζόμενο από αυστηρή εφαρμογή της νομοθεσίας. Προς αυτή την κατεύθυνση, τον Απρίλιο του 2016 δημοσιεύθηκαν στην Επίσημη Εφημερίδα της ΕΕ τρεις ιδιαίτερα σημαντικές νομοθετικές πράξεις, οι οποίες στην ουσία αλλάζουν σταδιακά, αλλά και ριζικά το νομικό καθεστώς προστασίας δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση. Το συγκεκριμένο νέο αυτό νομοθετικό πλαίσιο σχηματίστηκε έπειτα από διαβουλεύσεις πολυετείς, με έντονο διάλογο από τα εμπλεκόμενα μέρη ενώ καθοριστικές για τη διαμόρφωση του νέου νομοθετικού πλαισίου, υπήρξαν οι επιρροές από τις τρομοκρατικές επιθέσεις στο Παρίσι και τις Βρυξέλλες.

Το νέο πλαίσιο προστασίας προσωπικών δεδομένων συνδιαμορφώνεται από 2 νέες κοινοτικές οδηγίες και έναν κανονισμό. Συγκεκριμένα, το νέο πλαίσιο προστασίας προσωπικών δεδομένων αποτελείται από:

1. Τον κανονισμό 2016/679[53] (*Γενικό Κανονισμό για την Προστασία Δεδομένων/General Data Protection Regulation)*

2. Την οδηγία 2016/680[54] σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Συν τοις άλλοις, η νέα αυτή

[53] https://eur-lex.europa.eu/legal-content/EL
[54] https://eur-lex.europa.eu/legal-content/EL

οδηγία περιλαμβάνει ένα νέο σύστημα κανόνων σχετικά με τις μεταφορές δεδομένων, ώστε να εξασφαλίζεται η «*ομαλότερη συνεργασία μεταξύ των δικαστικών και αστυνομικών αρχών*» των κρατών-μελών της Ευρωπαϊκής Ένωσης. Η οδηγία δεν αφορά μόνο στη διασυνοριακή μεταφορά δεδομένων εντός της ΕΕ, αλλά θεσπίζει για πρώτη φορά ελάχιστα πρότυπα για την επεξεργασία δεδομένων από τις αστυνομικές και δικαστικές αρχές στο εσωτερικό κάθε κράτους μέλους.

3. Στην παρούσα φάση, το σύνολο των τροποποιήσεων ολοκληρώνεται με την οδηγία 2016/681[55] (Passenger Name Record, εφεξής PNR), σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων. Τα κράτη μέλη θα πρέπει να ιδρύσουν ή να ορίσουν μια αρχή αρμόδια για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων, η οποία θα είναι αρμόδια για τη συλλογή και διαχείριση των δεδομένων PNR από τους αερομεταφορείς και τη μεταβίβασή τους στις αρχές (Μονάδα Στοιχείων Επιβατών ή ΜΣΕ). Οι πληροφορίες αυτές θα διατηρούνται σε βάση δεδομένων για περίοδο 5 ετών, αλλά μετά από 6 μήνες, όλα τα δεδομένα θα μένουν ανώνυμα με την κάλυψη των στοιχείων που μπορούν να χρησιμεύσουν στην άμεση ταυτοποίηση του επιβάτη, στον οποίο αναφέρονται (πχ. όνομα, διεύθυνση και στοιχεία επικοινωνίας). Τα κράτη μέλη θα μπορούν να συλλέγουν και να επεξεργάζονται δεδομένα PNR και από οικονομικούς φορείς που δεν είναι μεταφορείς, όπως ταξιδιωτικά γραφεία και διοργανωτές ταξιδιών που παρέχουν σχετιζόμενες με ταξίδια υπηρεσίες, συμπεριλαμβανομένων των κρατήσεων πτήσεων.

Όπως έχει αναφερθεί, ο εν λόγω κανονισμός αποτέλεσε προϊόν χρονοβόρων διαδικασιών και ισχυρών πιέσεων, οι οποίες διήρκησαν περισσότερο από τέσσερα χρόνια. Ο κανονισμός αυτός αντικαθιστά την ισχύουσα οδηγία (οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου) για την προστασία των δεδομένων, η οποία δεν ανταποκρινόταν επαρκώς στις ανάγκες μίας εποχής με smartphones, social media κτλ. Το διάστημα των 2 ετών που μεσολάβησε από την δημοσίευση μέχρι την εφαρμογή, αποτέλεσε περίοδο προσαρμογής για τα εμπλεκόμενα μέρη. Επί της ουσίας, πρόκειται για μια περίοδο κατά την οποία οι εταιρείες έπρεπε να εξασφαλίσουν ότι θα συμμορφώνονται με το νέο σύνολο κανόνων, ενώ οι εθνικές αρχές προστασίας δεδομένων, η ομάδα εργασίας του άρθρου 29 αλλά και ο Ευρωπαίος Επόπτης

[55] https://eur-lex.europa.eu/legal-content/EL

Προστασίας Δεδομένων ήταν υποχρεωμένοι να εκδίδουν και γνωμοδοτήσεις, προκειμένου να βοηθήσουν τα εμπλεκόμενα μέρη στο πλαίσιο της προετοιμασίας τους.

Όσο αφορά το αντικείμενο και τους στόχους, ο κανονισμός θεσπίζει κανόνες που αφορούν στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα (άρθρο 1, παρ.1). Σχετικά με τη δομή του, ο 679/2016 αποτελείται από 99 άρθρα και είναι ενιαίος για όλη την Ευρωπαϊκή Ένωση. Από την ημερομηνία εφαρμογής του (25/5/2018) καταργείται ρητά (άρθρο 94) η οδηγία 95/46/ΕΚ. Οι παραπομπές στην καταργούμενη οδηγία θεωρούνται παραπομπές στον παρόντα κανονισμό, ενώ οι παραπομπές στην ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συστάθηκε με το άρθρο 29 της οδηγίας 95/46/ΕΚ, θεωρούνται παραπομπές στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων που συστήνεται με τον παρόντα κανονισμό. Σχετικά με το Ελληνικό νομοθετικό πλαίσιο, τόσο το σχετικό νομοθετικό πλαίσιο Ν. 2472/97(ΦΕΚ Α' 50), στο οποίο είχε ενσωματωθεί η οδηγία 95/46/ΕΚ, καθώς και η πρόσφατη κωδικοποίηση των σχετικών διατάξεων που πραγματοποιήθηκε με το Π.Δ. 28/1 (ΦΕΚ-34 Α/23-3-15) θα αναγκαστούν να εναρμονιστούν σε όσα σημεία διαφοροποιούνται, έτσι ώστε να βρίσκονται σε πλήρη αρμονία με τον κανονισμό, ως υπερκείμενη πηγή δικαίου σε σχέση με τα δύο νομοθετήματα της ελληνικής έννομης τάξης.

Συν τοις άλλοις, από την ανάγνωση του Κανονισμού, και ιδιαίτερα από το άρθρο 2 προκύπτει με ευκολία ότι βασικό υποκείμενο προστασίας αποτελούν τα φυσικά πρόσωπα. Υπό αυτή την έννοια, ο Κανονισμός 679/2016 δεν καλύπτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν νομικά πρόσωπα και ιδίως επιχειρήσεις συσταθείσες ως νομικά πρόσωπα, συμπεριλαμβανομένων της επωνυμίας, του τύπου και των στοιχείων επικοινωνίας του νομικού προσώπου. Ο συγκεκριμένος κανονισμός δεν εφαρμόζεται σε ζητήματα προστασίας θεμελιωδών δικαιωμάτων και ελευθεριών - κυκλοφορία δεδομένων προσωπικού χαρακτήρα που σχετίζονται με δραστηριότητες που δεν υπάγονται στο πεδίο εφαρμογής του ενωσιακού δικαίου (άρθρο 2), όπως δραστηριότητες που αφορούν την εθνική ασφάλεια. Παράλληλα, ο κανονισμός δεν τυγχάνει εφαρμογής στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα κράτη μέλη, όταν αυτά εκτελούν δραστηριότητες συναφείς με την κοινή εξωτερική πολιτική και πολιτική ασφάλειας της Ένωσης. Εξαιρείται από την εφαρμογή του Κανονισμού, η προστασία

των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων. Τα θέματα αυτά ρυθμίζονται από ειδική ενωσιακή νομική πράξη.

Ο 679/2016 σκοπεύει επίσης να συμβάλλει στην επίτευξη ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης και μιας οικονομικής ένωσης, προς την κατεύθυνση της οικονομικής και κοινωνικής προόδου, στην ενίσχυση και σύγκλιση των οικονομιών εντός της εσωτερικής αγοράς και στην ευημερία των φυσικών προσώπων . Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα. Πρόκειται για έννομο αγαθό που η προστασία του δεν είναι δεδομένη και απόλυτη, αλλά σταθμίζεται με άλλα δικαιώματα , όπως το δικαίωμα της πληροφόρησης , της πρόσβασης σε αρχεία και έγγραφα κτλ.). Βασικό εργαλείο στην στάθμιση αυτή αποτελεί , η αρχή της αναλογικότητας.

Επιπροσθέτως, ορισμένα από τα βασικότερα σημεία του νέου κανονισμού επιγραμματικά είναι τα εξής:

1. *Δικαίωμα διαγραφής (δικαίωμα στη λήθη)*. Σύμφωνα με το άρθρο 17 του Κανονισμού, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν, χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους προβλεπόμενους στον Κανονισμό λόγους.

2. *Σαφής συγκατάθεση*. Σύμφωνα με το άρθρο 7 του Κανονισμού, τίθενται αυστηρές προϋποθέσεις αναφορικά με τη συγκατάθεση από το ενδιαφερόμενο πρόσωπο για την επεξεργασία των προσωπικών του δεδομένων, την οποία έχει δικαίωμα να ανακαλέσει ανά πάσα στιγμή. Παράλληλα, σύμφωνα με το άρθρο 8 , σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε παιδί, η επεξεργασία δεδομένων προσωπικού χαρακτήρα παιδιού είναι σύννομη ,εάν το παιδί είναι τουλάχιστον 16 χρονών. Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού. Τα κράτη μέλη δύνανται να προβλέπουν διά νόμου μικρότερη ηλικία για τους εν λόγω

σκοπούς, υπό την προϋπόθεση ότι η εν λόγω μικρότερη ηλικία δεν είναι κάτω από τα 13 έτη. Ο υπεύθυνος επεξεργασίας καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία . Το γενικό ενοχικό δίκαιο των κρατών μελών, περί των προϋποθέσεων , κατάρτισης ή συνεπειών μιας σύμβασης σε σχέση με ορισμένο παιδί, παραμένει σε ισχύ.

3. *Ανακοίνωση παραβίασης δεδομένων*. Σύμφωνα με το άρθρο 34 του Κανονισμού, όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.

4. *Σαφής και κατανοητή γλώσσα στις πολιτικές απορρήτου*. Σύμφωνα με το άρθρο 12 του Κανονισμού, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα, για να παρέχει στο υποκείμενο των δεδομένων κάθε απαιτούμενη από το νόμο πληροφορία σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη, ειδικά σε παιδιά.

5. *Αυστηρότερη εφαρμογή του νόμου και πρόστιμα στις επιχειρήσεις που τον παραβιάζουν*. Το άρθρο 83 του Κανονισμού προβλέπει τους γενικούς όρους επιβολής διοικητικών προστίμων. Υπό συγκεκριμένες προϋποθέσεις, ορισμένες παραβάσεις επισύρουν διοικητικά πρόστιμα έως και 20 εκατ. Ευρώ ή σε περίπτωση επιχειρήσεων, έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο. Ειδικά, για τους φορείς του δημοσίου, κεντρική θέση κατέχει η υποχρέωση ορισμού υπευθύνου για τη λήψη και την τήρηση των διαδικασιών και των μέτρων ασφαλείας των δεδομένων προσωπικού χαρακτήρα (DPO – Data Protection Officer) και επισημαίνεται πως η μη συμμόρφωση ενός Οργανισμού ή μίας Επιχείρησης προς τις επιταγές του νέου Κανονισμού μπορεί να επιφέρει ιδιαίτερα μεγάλα διοικητικά πρόστιμα.

6. *Δικαίωμα αποζημίωσης και ευθύνη*. Σύμφωνα με το άρθρο 82, κάθε πρόσωπο, το οποίο υπέστη υλική ή μη υλική ζημία, ως αποτέλεσμα παραβίασης του παρόντος κανονισμού

δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για τη ζημία που υπέστη.

Ως συμπέρασμα για τον εν λόγω κανονισμό θα μπορούσε να τονιστεί ότι ο επίκαιρος και επιτακτικός χαρακτήρας του νέου νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων έχει ενεργοποιήσει και την εσωτερική νομοθετική πρωτοβουλία. Προς την κατεύθυνση αυτή, στις 5 Μαρτίου 2018 έληξε η δημόσια διαβούλευση, κατόπιν νομοθετικής πρωτοβουλίας του Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, υπό τον τίτλο: «*Θέσπιση νομοθετικών μέτρων για την εφαρμογή του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) και ενσωμάτωση στην εθνική έννομη τάξη της Οδηγίας 2016/680/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου και συμπληρωματικές διατάξεις*». Μετά όμως την ανασύσταση της νομοπαρασκευαστικής Επιτροπής δεν έχει μέχρι σήμερα κατατεθεί στη βουλή το σχετικό νομοσχέδιο. Συνεπώς, δεν μπορεί να υπάρξει ασφαλές συμπέρασμα σχετικά με τη δυνατότητα της Ελλάδας να είναι έτοιμη να συμμορφωθεί στις ανάγκες του νέου αυτού νομοθετικού πλαισίου ή αν θα υπάρξουν πρακτικές δυσκολίες στην εφαρμογή του.

2.6 Η οδηγία 2002/58/ΕΚ για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες

Η κοινοτική οδηγία 2002/58 αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και ουσιαστικά αποτελεί μία οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Η ανάγκη της εν λόγω κοινοτικής οδηγίας προέκυψε από την ραγδαία ανάπτυξη

της τεχνολογίας στο χώρο των τηλεπικοινωνιών, αλλά και από την διαπίστωση της ύπαρξης κινδύνου των προσωπικών δεδομένων. Για αυτόν τον λόγο λοιπόν, προέκυψε η ανάγκη για μία ρύθμιση που θα συμπλήρωνε και θα εξειδίκευε την κοινοτική οδηγία 95/46/ΕΚ και έτσι, προέκυψε η οδηγία 97/66/ΕΚ που αποτελούσε εξειδίκευση της οδηγίας 95/46/ΕΚ σχετικά με την επεξεργασία των προσωπικών δεδομένων στις τηλεπικοινωνίες. Οι μεγάλες όμως αλλαγές στην τεχνολογία των επικοινωνιών, έδειξαν ότι ήταν αναγκαία η αντιμετώπιση των νέων απαιτήσεων που συνεπάγονται οι ψηφιακές τεχνολογίες στα δημόσια δίκτυα επικοινωνίας, σχετικά με την προστασία των προσωπικών δεδομένων και για αυτόν ακριβώς τον λόγο ξεκίνησε η αντικατάσταση του τότε υφιστάμενου νομικού πλαισίου για τις τηλεπικοινωνίες. Βασική στόχευση του νέου νομοθετικού πλαισίου ήταν η κατά το δυνατόν εναρμόνιση των κανονιστικών διατάξεων στα κράτη μέλη μέσω της κανονιστικής δράσης τόσο σε κοινοτικό, όσο και σε εθνικό επίπεδο.

Επομένως, το 2002 εκπονήθηκαν 5 κοινοτικές οδηγίες, οι οποίες ήταν οι ακόλουθες: η 2002/19/ΕΚ[56], η 2002/20/ΕΚ[57], η 2002/21/ΕΚ[58], η 2002/22/ΕΚ[59] και τέλος, η 2002/58/ΕΚ[60]. Εκ των πέντε που προαναφέρθηκαν, η σημαντικότερη για τον σκοπό και το πλαίσιο της παρούσας διπλωματικής εργασίας είναι η 2002/58/ΕΚ «*Για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών*», η οποία ήταν αναγκαία ως αντικατάσταση των «γερασμένων» κανόνων δικαίου που αφορούσαν τις νέες τεχνολογίες[61]. Η εν λόγω κοινοτική οδηγία ήταν μία κάθετη τομεακή ρύθμιση συμπληρωματική των διεθνών κειμένων και της 95/46/ΕΚ σε αντίθεση με την απορρύθμιση που

[56] Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (Οδηγία για την πρόσβαση) ΕΕ L 108 της 24.4.2002, σ. 7 έως 20

[57] Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (Οδηγία για την αδειοδότηση). ΕΕ L 108 της 24.4.2002, σ. 21 έως 32

[58] Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (Οδηγία πλαίσιο). ΕΕ L 108 της 24.4.2002, σ. 33 έως 50

[59] Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (Οδηγία καθολικής υπηρεσίας). ΕΕ L 108 της 24.4.2002, σ. 51 έως 77

[60] Μήτρου Λ. « Η νέα Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες» ΔιΜΕΕ 2004 σελ. 371

[61] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

παρατηρούνταν το ίδιο διάστημα στις Η.Π.Α.. Η βασική επιδίωξη του νομοθέτη σχετικά με την κοινοτική οδηγία 2002/58/ΕΚ, ήταν η διατύπωση τεχνολογικά ουδέτερων κανόνων μέσα σε περιβάλλον συνεχών τεχνολογικών εξελίξεων και για αυτόν ακριβώς τον λόγο, εάν εξεταστεί προσεκτικά η εν λόγω οδηγία, ο νομοθέτης δεν αναφέρεται σε «τηλεπικοινωνιακό τομέα» αλλά σε «ηλεκτρονικές επικοινωνίες».

Σύμφωνα με την 2002/58/ΕΚ, με τον όρο «δίκτυο ηλεκτρονικών επικοινωνιών» νοούνται τα συστήματα μετάδοσης, αλλά και ο εξοπλισμός μεταγωγής που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, συμπεριλαμβανομένων των δορυφορικών δικτύων, των σταθερών και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης[62].

Ο σκοπός της 2002/58/ΕΚ, όπως αναφέρεται στα αρχικά άρθρα της κοινοτικής οδηγίας, είναι η διασφάλιση του δικαιώματος στην ιδιωτική ζωή σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα με την προσπάθεια ταυτόχρονα, της εξασφάλισης της ελεύθερης κυκλοφορίας των εν λόγω δεδομένων, αλλά και των ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Κοινότητα. Ουσιαστικά, ο σκοπός της εν λόγω οδηγίας είναι παρόμοιος με εκείνον της 95/46/ΕΚ για την προστασία των προσωπικών δεδομένων, όπου η ανάγκη για εφαρμογή των βασικών στόχων των Ευρωπαϊκών Κοινοτήτων οδήγησε σε κανονιστικές ρυθμίσεις που θα διευκόλυναν την κυκλοφορία προσωπικών δεδομένων μεταξύ των κρατών μελών απαραίτητων για την εξασφάλιση της ελεύθερης κυκλοφορίας εμπορευμάτων, προσώπων, υπηρεσιών και κεφαλαίων με ταυτόχρονη προστασία τους.

Μεταξύ των άλλων, η εμπορική προώθηση ήταν ακόμα ένα ζήτημα σημαντικό που σχετιζόταν με την προστασία των προσωπικών δεδομένων. Συγκεκριμένα, η βασική αρχή που τέθηκε στην κοινοτική οδηγία 2002/58/ΕΚ ήταν ότι η χρησιμοποίηση αυτομάτων συστημάτων κλήσης (Fax, email) επιτρέπεται μόνο αφού προηγουμένως υπάρχει συγκατάθεση (opt-in) του συνδρομητή, όπως καθορίζεται στο άρθρο 13 της εν λόγω οδηγίας. Σχετικά με προστασία του απορρήτου, η 2002/58/ΕΚ εισάγει μια εξαίρεση με το άρθρο 15 παρ. 1. με το οποίο κάμπτεται η

[62] Άρθρο 2 α. της Οδηγίας 2002/21/ΕΚ

γενική αρχή της προστασίας του απορρήτου και των δεδομένων κίνησης και θέσης των πληροφοριών[63] και επίσης, δίνει τη δυνατότητα στα κράτη μέλη να περιορίζουν τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στα άρθρα 5 και 6, στο άρθρο 8 παράγραφοι 1 έως 4 και στο άρθρο 9 της ίδιας οδηγίας, αλλά και να λαμβάνουν νομοθετικά μέτρα για τη φύλαξη δεδομένων για ορισμένο χρονικό διάστημα.

[63] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

ΚΕΦΑΛΑΙΟ 3

ΕΛΛΗΝΙΚΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΧΩΡΟ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

3.1 Ηλεκτρονικές επικοινωνίες και ειδικές νομικές ρυθμίσεις

Το νομοθετικό πλαίσιο πάνω στο οποίο βασίζεται η προστασία των προσωπικών δεδομένων αλλά και του απορρήτου στις ηλεκτρονικές επικοινωνίες, είναι οι νόμοι 3471/2006[64], 3674/2008[65], 3917/2011[66], 4070/2012[67]. Ο 3471/2006 αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και ουσιαστικά, αποτέλεσε την ενσωμάτωση της κοινοτικής οδηγίας 2002/58/ΕΚ στο Ελληνικό νομοθετικό πλαίσιο. Ο 3674/2008 ενίσχυσε το πλαίσιο σχετικά με το απόρρητο στις τηλεφωνικές επικοινωνίες και με τη σειρά του ο νόμος 3917/2011 θέσπιζε πιο αυστηρά μέτρα σχετικά με τα δεδομένα που προκύπτουν από επεξεργασία με τη χρήση των ηλεκτρονικών επικοινωνιών. Τέλος, ο νόμος 4070/2012 αφορά την οργάνωση και λειτουργία των ηλεκτρονικών επικοινωνιών και ουσιαστικά αποτελεί ενσωμάτωση των κοινοτικών οδηγιών 2009/136/ΕΚ και 2009/140/ΕΚ και ο νόμος 4411/2016 αφορά την κύρωση της σύμβασης του Συμβουλίου της Ευρώπης για τα διάφορα εγκλήματα στο Διαδίκτυο, αλλά και την ποινικοποίηση των πράξεων με ρατσιστική χροιά που πραγματοποιούνται μέσω των ηλεκτρονικών επικοινωνιών[68].

[64] Ν. 3471/2006: «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του νόμου 2472/1997»
[65] Ν. 3674/2008: «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις»
[66] Ν. 3917/2011: «Διατήρηση δεδομένων που παράγονται ή υποβάλονται σε επεξεργασία σε συνάρτηση με την παροχή δαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»
[67] Ν. 4070/2012: «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις»
[68] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

Γενικότερα, σχετικά με το Ελληνικό νομοθετικό πλαίσιο, αξίζει να αναφερθεί ότι η Ελλάδα το 1999 είχε προχωρήσει στην ψήφιση του νόμου 2774/99 σχετικά με την «προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα» που ουσιαστικά αποτελούσε την ενσωμάτωση της κοινοτικής οδηγίας 97/66/ΕΚ στην Ελληνική νομοθεσία (Τουντόπουλος, 1999). Αργότερα η εν λόγω Ευρωπαϊκή οδηγία καταργήθηκε, διότι ήταν πλέον απαραίτητη η δημιουργία ενός καινούργιου νομοθετικού πλαισίου σχετικά με τα προσωπικά δεδομένα και την προστασία τους που να μπορεί να ανταποκρίνεται στις νέες ανάγκες της αγοράς και της τεχνολογίας, αλλά και της ανάγκης για προστασία που είχαν και ακόμα έχουν όλοι οι χρήστες των διαφόρων ηλεκτρονικών επικοινωνιών. Η κοινοτική οδηγία που ήρθε να αντικαταστήσει την 97/66/ΕΚ ήταν η 2002/58/ΕΚ για την προστασία της ιδιωτικότητας, αλλά και των δεδομένων με προσωπικό χαρακτήρα στις ηλεκτρονικές επικοινωνίες[69]. Στο Ελληνικό νομοθετικό πλαίσιο, η συγκεκριμένη αντικατάσταση έγινε με τον νόμο 3471/2006 που αντικατέστησε όλες τις διατάξεις του 2774/1999, ώστε να μπορέσει να ενσωματωθεί και η οδηγία 2002/58/ΕΚ (Αλεξανδροπούλου – Αιγυπτιάδου, 2008)[70]. Ο νόμος 3471/2006 στην πραγματικότητα προχώρησε ένα βήμα παραπέρα σχετικά με την προστασία των προσωπικών δεδομένων σε σύγκριση με την έως τότε Ελληνική νομοθεσία για το εν λόγω θέμα. Ο συγκεκριμένος νόμος θα μπορούσε να χαρακτηριστεί περισσότερο συμπληρωματικός και εξειδικευμένος σε σύγκριση πάντα με τον ν.2472/1997. Επί της ουσίας για τυχόν κενά ή διαφωνίες ή διαφορετικές ερμηνείες σχετικά με τη νομοθεσία για την προστασία των προσωπικών δεδομένων και τους παρόχους τηλεπικοινωνιών, η χρήση του 2472/1997 ήταν αναγκαία. Συν τοις άλλοις, ο 2472/1997 ισχύει και για την προστασία των προσωπικών δεδομένων σε ιδιωτικά δίκτυα, όπως αναφέρεται στην αιτιολογική έκθεση του νόμου 3471/2006. Πλέον εφαρμόζεται ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679 (GDPR) από 25/5/2018.

Σε αυτό το σημείο αξίζει να αναφερθεί ο σκοπός της ρύθμισης σχετικά με τις ηλεκτρονικές επικοινωνίες και την προστασία των προσωπικών δεδομένων όπως αναφέρεται στο πρώτο άρθρο του νόμου 3471/2006. Συγκεκριμένα, ο σκοπός του εν λόγω νομοθετικού πλαισίου είναι η «προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη

[69] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

[70] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών»[71]. Παρόμοια αναφορά και μέριμνα έχει και η οδηγία 2002/58/ΕΚ, στο πρώτο εδάφιο του πρώτου άρθρου, της οποίας αναφέρεται ως στόχος η «εναρμόνιση των διατάξεων των κρατών μελών προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Κοινότητα»[72]. Όπως μπορεί να γίνει κατανοητό, οι δύο ορισμοί που προαναφέρθηκαν διαφέρουν. Η διαφορά τους έγκειται στο γεγονός ότι στο πρώτο άρθρο της οδηγίας δεν υπάρχει αναφορά σχετικά με την προστασία των ηλεκτρονικών επικοινωνιών και του απορρήτου τους, σε αντίθεση με το Ελληνικό νομοθετικό πλαίσιο που την περιλαμβάνει[73]. Η Ευρωπαϊκή οδηγία όμως, αναφέρει στο προοίμιο της ότι το εν λόγω απόρρητο διασφαλίζεται σύμφωνα με τους διεθνείς κανόνες και τις διεθνείς πράξεις σχετικά με τα ανθρώπινα δικαιώματα, όπως αυτά προστατεύονται και με την Ευρωπαϊκή Σύμβαση για τα θεμελιώδη δικαιώματα του ανθρώπου[74].

Πέραν τούτων, ο Ελληνικός νόμος διαφέρει και σε ένα ακόμα σημαντικό σημείο σε σχέση με την οδηγία 2002/58/ΕΚ. Συγκεκριμένα, όπως αναφέρεται χαρακτηριστικά στο πρώτο άρθρο, η οδηγία 2002/58/ΕΚ αποσκοπεί και στην εξασφάλιση της ελεύθερης διακίνησης των προσωπικών δεδομένων, αλλά και των υπηρεσιών για τις ηλεκτρονικές υπηρεσίες στην Κοινότητα (Ευρωπαϊκή Ένωση)[75]. Όπως είναι γνωστό, η ελεύθερη διακίνηση ή κυκλοφορία αποτελεί ζωτικής σημασίας αρχή για την Ευρώπη, εξ ου και η αναφορά της συγκεκριμένης οδηγίας σε αυτήν. Σύμφωνα με τις αρχές που ισχύουν στην Ευρώπη, τα προσωπικά δεδομένα χρειάζεται να προστατεύονται, έτσι ώστε να μπορεί να προστατεύεται και ο διασυνοριακός ανταγωνισμός των Ευρωπαϊκών εταιριών και να ελαχιστοποιούνται τα όποια εμπόδια υπάρχουν στην εσωτερική αγορά των ηλεκτρονικών επικοινωνιών[76]. Η σημασία της ελεύθερης διακίνησης δεδομένων, ανθρώπων και ιδεών είναι ιδιαιτέρως σημαντική για την Ευρώπη λόγω κυρίως, της οικονομικής

[71] Ν. 3471/2006, άρθρο 1
[72] Ευρωπαϊκή οδηγία 2002/58/ΕΚ, άρθρο 1, εδάφιο α
[73] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[74] Ευρωπαϊκή οδηγία 2002/58/ΕΚ, αιτιολογική σκέψη 3
[75] Ευρωπαϊκή οδηγία 2002/58/ΕΚ, άρθρο 1, εδάφιο β
[76] Ευρωπαϊκή οδηγία 2002/58/ΕΚ, αιτιολογική σκέψη 8

της φύσεως και επομένως, «για την εγκαθίδρυση και λειτουργία της εσωτερικής αγοράς, στην οποία σύμφωνα με το άρθρο 7α της Συνθήκης, εξασφαλίζεται η ελεύθερη κυκλοφορία εμπορευμάτων, προσώπων, υπηρεσιών και κεφαλαίων, απαιτείται όχι μόνο η δυνατότητα κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών, αλλά και η προστασία των θεμελιωδών δικαιωμάτων του ατόμου»[77]. Επειδή όμως, το νομοθετικό πλαίσιο των διαφόρων κρατών μελών δεν είναι πάντα το ίδιο και έχει σημαντικές διαφορές, η ίδια η Κοινότητα μέσω των οργάνων της είναι αναγκασμένη να παρεμβαίνει, ώστε οι εκάστοτε διαφορετικές νομοθεσίες να προσεγγίζουν η μία την άλλη. Σε κάθε περίπτωση αξίζει να τονιστεί, ότι στην περίπτωση της Ελλάδας δεν είναι κατανοητή η παράλειψη μίας τόσο σημαντικής αρχής της Ευρώπης, όπως είναι η ελεύθερη διακίνηση των δεδομένων και ο περιορισμός του νομοθετικού πλαισίου μόνο στον τομέα της προστασίας των δεδομένων, χωρίς καμία αναφορά στην ελευθερία κυκλοφορίας των δεδομένων[78].

Για να μπορέσει ο αναγνώστης να κατανοήσει καλύτερα τον νόμο 3471/2006, στον ίδιο τον νόμο, στο άρθρο 2, υπάρχουν οι απαραίτητοι ορισμοί. Συγκεκριμένα, από την οδηγία 2002/21/ΕΚ έγινε χρήση των όρων: «Υπηρεσίες ηλεκτρονικών επικοινωνιών», «Δίκτυο ηλεκτρονικών επικοινωνιών», «Δημόσιο δίκτυο επικοινωνιών», «Συνδρομητής», «Καταναλωτής», «Χρήστης» και «παροχή δικτύου ηλεκτρονικών υπηρεσιών»[79]. Πέραν όμως των προαναφερθέντων ορισμών, ο νόμος 3471/2006 περιλαμβάνει και τις παρακάτω έννοιες:

- *«Συνδρομητής»*: Κάθε φυσικό ή νομικό πρόσωπο, το οποίο έχει προχωρήσει στη σύναψη σύμβασης με φορέα παροχής διαθέσιμων υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των εν λόγω υπηρεσιών.
- *«Χρήστης»*: Κάθε φυσικό πρόσωπο που κάνει χρήση της διαθέσιμης υπηρεσίας ηλεκτρονικών υπηρεσιών για τους δικούς του σκοπούς, είτε επαγγελματικούς είτε προσωπικούς, χωρίς όμως να απαιτείται συνδρομή για την συγκεκριμένη υπηρεσία.

[77] Ευρωπαϊκή οδηγία 2002/58/ΕΚ, αιτιολογική σκέψη 3
[78] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[79] Ευρωπαϊκή οδηγία 2002/21/ΕΚ, άρθρο 2

- *«Δεδομένα κίνησης»*: Ως δεδομένα κίνησης ορίζονται τα δεδομένα που επεξεργάζονται για τη διαβίβαση μίας επικοινωνίας σε ένα δίκτυο ηλεκτρονικών επικοινωνιών. Η εν λόγω κατηγορία δεδομένων μπορεί να περιλαμβάνει διάφορα δεδομένα, όπως για παράδειγμα τη διεύθυνση ή την ταυτότητα της σύνδεσης ή ακόμη και τον τερματικό εξοπλισμό ενός χρήστη. Τα δεδομένα κίνησης αφορούν κυρίως συνδρομητές και ουσιαστικά περιέχουν δεδομένα με ιδιωτικές στιγμές των φυσικών προσώπων, υποβάλλονται σε επεξεργασία σε περίπτωση ανάγκης για την αποκατάσταση κάποιας σύνδεσης.
- «*Δεδομένα θέσης»*: Το συγκεκριμένο είδος δεδομένων χρησιμοποιείται για την γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μίας υπηρεσίας ηλεκτρονικών επικοινωνιών[80]. Τα εν λόγω δεδομένα περιέχουν και μπορούν να παρέχουν πληροφορίες σχετικά με το υψόμετρο, το μήκος και το πλάτος κάποιου τερματικού εξοπλισμού. Συν τοις άλλοις, μπορούν να παρέχουν πληροφορίες σχετικά με την κίνηση και κατεύθυνση του εν λόγω τερματικού με αρκετά μεγάλη ακρίβεια σχετικά με τη γεωγραφική του θέση. Τα δεδομένα όμως των κινητών δικτύων παρόλο που χρησιμοποιούν τη γεωγραφική θέση χρήστη και θα μπορούσαν να χαρακτηριστούν ως δεδομένα θέσης, εν τούτοις είναι δεδομένα κίνησης, σύμφωνα με το προοίμιο της οδηγίας 2002/58/ΕΚ, διότι αυτά τα δεδομένα υποβάλλονται σε επεξεργασία για τη μετάδοση των ηλεκτρονικών επικοινωνιών.
- *«Επικοινωνία»*: Η πληροφορία που μεταδίδεται εντός ορισμένων μερών με τη χρήση των ηλεκτρονικών επικοινωνιών. Σε αυτή την κατηγορία δεν ανήκουν τα δεδομένα που μεταβιβάζονται με ραδιοτηλεοπτικές υπηρεσίες μέσω των ηλεκτρονικών

[80] Ν. 3471/2006, άρθρο 2, παρ. 3

επικοινωνιών. Εξαίρεση αποτελούν οι πληροφορίες που μπορεί να αφορούν αναγνωρίσιμο χρήστη, ο οποίος τις λαμβάνει.

- *«Κλήση»*: Με τον όρο κλήση νοείται η σύνδεση που λαμβάνει χώρα μέσω τηλεφωνικής υπηρεσίας, η οποία επιτρέπει επικοινωνία σε αμφίδρομη κατεύθυνση[81].
- *«Υπηρεσία προστιθέμενης αξίας»*: Με τον όρο υπηρεσία προστιθέμενης αξίας νοείται κάθε υπηρεσία που υποχρεώνει την επεξεργασία είτε των δεδομένων θέσης είτε κίνησης εκτός εκείνων που χρειάζονται για τη μεταβίβαση ή χρέωση της επικοινωνίας. Γενικά, η κοινοτική οδηγία 2002/58/ΕΚ στο άρθρο 6 εισάγει την εν λόγω έννοια ως τεχνολογικά ουδέτερη και για αυτόν τον λόγο έχει ευρεία εφαρμογή σχετικά με την επεξεργασία δεδομένων. Σε αυτό το σημείο, αξίζει να αναφερθεί το έργο του Νούσκαλη (2003), στο οποίο ο συγγραφέας αναφέρει ότι η αόριστη αναφορά της Ευρωπαϊκής οδηγίας στον όρο των υπηρεσιών προστιθέμενης αξίας, τελικά ίσως να αποτελεί ένδειξη αδυναμίας σχετικά με την προστασία των δεδομένων κίνησης και εν τέλει αδυνατεί στην προστασία των προσωπικών δεδομένων και της ιδιωτικότητας.
- *«Ηλεκτρονικό ταχυδρομείο»:* Κάθε μήνυμα γραπτό, ηχητικό ή οπτικό που αποστέλλεται μέσω δικτύου επικοινωνιών και μπορεί να παραμένει αποθηκευμένο μέχρι να παραληφθεί από τον παραλήπτη.
- *«Υπηρεσίες ηλεκτρονικών επικοινωνιών»*: Οι κατά κύριο λόγο αμειβόμενες υπηρεσίες, των οποίων η παροχή αφορά τη μετάδοση σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικούς σκοπούς. Παρόλα αυτά, στις εν λόγω υπηρεσίες δεν περιλαμβάνονται οι υπηρεσίες

[81] Ευρωπαϊκή οδηγία 2009/136/ΕΚ, άρθρο 2, παρ. 2 εδάφιο α

παροχής ή ελέγχου περιεχομένου που μεταφέρονται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και οι υπηρεσίες που εμπίπτουν στην παράγραφο 2 του άρθρου 2 του προεδρικού διατάγματος 39/2001 και που δεν αφορούν τη μετάδοση σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών[82].

- *«Δημόσιο δίκτυο επικοινωνιών»:* Εκείνο το δίκτυο ηλεκτρονικών επικοινωνιών που χρησιμοποιείται, μερικώς ή στο σύνολο του, για την παροχή διαθεσίμων υπηρεσιών ηλεκτρονικών επικοινωνιών.
- «*Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών*»: Οι υπηρεσίες στις οποίες το κοινό έχει πρόσβαση.

Σύμφωνα με την Ελληνική νομοθεσία που ενσωμάτωσε την κοινοτική οδηγία 2002/58/ΕΚ, οι διατάξεις των άρθρων 1 έως 17 του νόμου εφαρμόζονται τόσο στην επεξεργασία προσωπικών δεδομένων, όσο και στο απόρρητο των επικοινωνιών. Επιπροσθέτως, η Ελληνική νομοθεσία ορίζει τις υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής του νόμου, δηλαδή διευκρινίζεται ότι οι σχετικές ρυθμίσεις εφαρμόζονται μόνο στα δημόσια δίκτυα ηλεκτρονικής επικοινωνίας δηλαδή στα δίκτυα ηλεκτρονικών επικοινωνιών, τα οποία χρησιμοποιούνται, εν μέρει ή εξ ολοκλήρου, για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών[83]. Επομένως, σχετικά με την επεξεργασία που πραγματοποιείται στο πλαίσιο μη διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών εφαρμόζεται η βασική νομοθεσία για την προστασία των προσωπικών δεδομένων[84]. Παραδείγματος χάριν, ο 3471/2006 δεν έχει εφαρμογή σε περιπτώσεις εσωτερικών τηλεφωνικών κέντρων, όπως είχε αποφασιστεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[85].

[82] Ν. 39/2001, άρθρο 2 παρ 2
[83] Ν. 3471/2006, άρθρο 2 παρ 10
[84] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[85] Απόφαση 60/2007 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία απάντησε σε σχετικό ερώτημα του ΑΣΕΠ για την νομιμότητα εγκατάστασης στο Γραφείο Εξυπηρέτησης Πολιτών καταγραφέα εισερχομένων κλήσεων στο εσωτερικό τηλεφωνικό κέντρο του ΑΣΕΠ, ο οποίος θα καταγράφει και το περιεχόμενο

Οι «Υπηρεσίες ηλεκτρονικών επικοινωνιών», όπως αναφέρθηκε παραπάνω, αποτελούνται από τις υπηρεσίες, των οποίων η παροχή συνίσταται, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις και όχι οι υπηρεσίες που περιλαμβάνουν υπηρεσίες παροχής ή ελέγχου περιεχομένου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και υπηρεσίες της Κοινωνίας της Πληροφορίας, όπως αυτές ορίζονται στην παράγραφο 2 του άρθρου 2 του π.δ. 39/2001 και που δεν αφορούν, εν όλω ή εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών[86]. Αυτό έχει σαν αποτέλεσμα ότι πρόσθετες υπηρεσίες ή υπηρεσίες που παρέχουν περιεχόμενο σε μία πύλη πρόσβασης ή σε έναν ιστοχώρο, να καλύπτονται μόνο από τη γενική νομοθεσία περί προστασίας των προσωπικών δεδομένων. Σημαίνει ακόμη ότι οι φορείς παροχής υπηρεσιών Διαδικτύου καλύπτονται από την τομεακή ρύθμιση, όταν λειτουργούν ως φορείς παροχής υπηρεσιών πρόσβασης και παρέχουν σύνδεση στο Διαδίκτυο και καλύπτονται μόνο από το Γενικό Κανονισμό Προστασίας Δεδομένων, όταν λειτουργούν ως φορείς παροχής περιεχομένου[87].

Συμπληρώνοντας το δεύτερο εδάφιο της πρώτης παραγράφου του άρθρου 3 ο ν.3471/2006, διευκρινίζεται στη δεύτερη παράγραφο του άρθρου 3 του ν. 3471/06 ότι «ο ν. 2472/97 και οι εκτελεστικοί του άρθρου 19 του Συντάγματος νόμοι, εφαρμόζονται για κάθε ζήτημα σχετικό με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, που δεν ρυθμίζεται ειδικότερα από τον παρόντα νόμο»[88]. Ο νόμος 3471/2006 είναι αναπόσπαστο κομμάτι της νομοθεσίας τόσο για την προστασία των προσωπικών δεδομένων όσο και του ρυθμιστικού πλαισίου των ηλεκτρονικών επικοινωνιών[89]. Συγκεκριμένα οι διατάξεις του ν. 3471/2006, όπως και του κατηργηθέντος ν. 2774/1999, αποτελούν συμπλήρωση και εξειδίκευση των γενικών ρυθμίσεων του ν. 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»,

---

της τηλεφωνικής συνδιάλεξης για την καλύτερη εξυπηρέτησή των πολιτών. Η σχετική απόφαση στην ιστοσελίδα της Αρχής www.dpa.gr

[86] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

[87] Χαρακτηριστικά παραδείγματα είναι τα περιεχόμενα που είναι σχετικά με ταινίες, ειδήσεις, on line παιχνίδια και γενικά περιεχόμενο που είναι δυναμικό δηλ. μεταβάλλεται και συνήθως προσφέρεται δωρεάν για να κάνει πιο ελκυστική μία ιστοσελίδα

[88] Ν. 3471/2006, άρθρο 3 παρ 2

[89] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

όπως ισχύει, στον τομέα των ηλεκτρονικών επικοινωνιών, ο οποίος συνεχίζει να ισχύει ως ο νόμος πλαίσιο για την προστασία των προσωπικών δεδομένων. Ενώ όσον αφορά την προστασία του απορρήτου των επικοινωνιών οι διατάξεις του 3471/06 συμπληρώνουν την προϋφιστάμενη σχετική νομοθεσία, όπως του 2225/94 «για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις», του 3115/03 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών», καθώς και τη νομοθεσία που έχει εκδοθεί κατ' εξουσιοδότηση των νομοθετημάτων αυτών και του προεδρικού διατάγματος 47/2005 «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλιση του»[90].

Συν τοις άλλοις, ο νόμος 3471/06 έχει εφαρμογή στις γραμμές συνδρομητών που συνδέονται με ψηφιακά κέντρα και μόνο όταν αυτό είναι τεχνικώς εφικτό, εφαρμόζεται και σε γραμμές συνδρομητών που συνδέονται με αναλογικά κέντρα, με την προϋπόθεση ότι δεν συνεπάγεται για τους παρόχους των υπηρεσιών αυτών δυσανάλογη οικονομική επιβάρυνση[91]. Μία παράγραφος που είναι ανάλογη του άρθρου 3 παρ.2 της Οδηγίας 2002/58/ΕΚ και η οποία φανερώνει τις πιέσεις των παρόχων, κατά την προετοιμασία της Οδηγίας 2002/58/ΕΚ, για διασφάλιση των οικονομικών τους συμφερόντων, η οποία υλοποιήθηκε με τη δυνατότητα τους να αποφασίζουν κατά βούληση πότε τους συμφέρει ή πότε δεν τους συμφέρει να προσφέρουν τις υπηρεσίες αυτές, ακυρώνοντας έτσι την υποχρέωση τους να παρέχουν τις υπηρεσίες του άρθρου 8 και 9 ατελώς. Για την διαπίστωση βέβαια και την εκτίμηση της δυνατότητας αυτής προβλέπεται ότι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) θα είναι αρμόδια να διαπιστώνει τις περιπτώσεις αυτές, όπου η σύνδεση με αναλογικά κέντρα είναι τεχνικώς αδύνατη ή απαιτεί δυσανάλογη επένδυση και η οποία θα πρέπει σε κάθε περίπτωση να ενημερώνει σχετικώς την Ευρωπαϊκή Επιτροπή[92]. Μία υποχρέωση που δεν προσφέρει πολλά από την στιγμή που αυτή η διάταξη δεν συνοδεύεται και από συγκεκριμένα μέτρα συμμόρφωσης

[90] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[91] Ν. 3471/2006, άρθρο 3 παρ 3 (α)
[92] Ν. 3471/2006, άρθρο 3 παρ 3 (β)

των παρόχων, όταν η Επιτροπή διαπιστώνει ότι οι λόγοι αυτοί δεν υφίστανται ή προβάλλονται προσχηματικά[93].

3.2 Νομικές υποχρεώσεις του παρόχου

Το σημαντικό στοιχείο, το οποίο χρειάζεται να λαμβάνεται υπόψη σχετικά με τις υποχρεώσεις του εκάστοτε παρόχου είναι η επεξεργασία των προσωπικών δεδομένων του χρήστη και το γεγονός ότι αυτό σημαίνει ότι ο εν λόγω πάροχος είναι ουσιαστικά ο υπεύθυνος επεξεργασίας σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων και επομένως, έχει υποχρέωση να τηρεί όλες τις αρχές επεξεργασίας των προσωπικών δεδομένων δηλαδή:

1. *Αρχή της νομιμότητας του σκοπού και του τρόπου επεξεργασίας*
2. *Αρχή της αναλογικότητας*
3. *Αρχή της ακρίβειας*
4. *Αρχή της χρονικής διάρκειας τήρησης των δεδομένων*

Συγκεκριμένα, στην υπό εξέταση ειδική νομοθεσία για τη ρύθμιση της επεξεργασίας προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, έχει όλες τις ανάλογες υποχρεώσεις, οι οποίες εξειδικεύονται στις βασικές αρχές επεξεργασίας, όπως στην αρχή αναλογικότητας και στην αρχή της καθορισμένης χρονικής τήρησης των δεδομένων.

3.2.1 Διασφάλιση αρχών επεξεργασίας δεδομένων

Για την καλύτερη κατανόηση της διασφάλισης των αρχών επεξεργασίας των δεδομένων, αξίζει να γίνει μία σύντομη αναφορά στην αρχή της αναλογικότητας. Σύμφωνα με την αρχή της αναλογικότητας, τα όποια δεδομένα που τίθενται υπό επεξεργασία οφείλουν να έχουν συνάφεια και να μην ξεπερνούν τον αριθμό που απαιτείται για την εν λόγω επεξεργασία[94]. Συν τοις άλλοις,

[93] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

[94] Ν. 3471/2006, άρθρο 5 παρ.6 «ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών

αξίζει να αναφερθεί το γεγονός ότι η συγκεκριμένη αρχή αφορά κυρίως τα δεδομένα. Παρακάτω, αναφέρονται χαρακτηριστικά ορισμένα σημεία στον νόμο 3471 που αφορούν την αρχή της αναλογικότητας:

1. Στον 3471 προσδιορίζονται τα όρια της αρχής του σκοπού και της αναλογικότητας και αναφέρεται ότι η επεξεργασία των προσωπικών δεδομένων, όπως τα δεδομένα κίνησης και θέσης, οφείλει να περιορίζεται στον αναγκαίο βαθμό και να μην ξεπερνάει τα όρια του σκοπού της[95].
2. Η εν λόγω αρχή εφαρμόζεται και στην έκτη παράγραφο του άρθρου 5 του 3471 που αναφέρεται στις υποχρεώσεις του παρόχου σχετικά με την επιλογή τεχνικών μέσων, αλλά και πληροφοριακών συστημάτων[96]. Επιπροσθέτως, ο νόμος 3471 αναφέρει για πρώτη φορά την αρχή της «εξοικονόμησης των δεδομένων»[97], η οποία μπορεί να εφαρμοστεί με τον σωστό σχεδιασμό των τεχνικών μέσων, αλλά και των πληροφοριακών συστημάτων, ώστε να μπορεί να πραγματοποιείται η επεξεργασία των προσωπικών δεδομένων στον ελάχιστο δυνατό βαθμό.
3. Η αρχή της αναλογικότητας είναι υποχρεωτική στους παρόχους σχετικά με την δημοσίευση σε είτε έντυπους είτε ηλεκτρονικούς καταλόγους συνδρομητών μόνο των προσωπικών δεδομένων που είναι αναγκαία για την αναγνώριση της ταυτότητας του συνδρομητή, εκτός όμως αν ο εν λόγω συνδρομητής έχει δώσει τη ρητή συγκατάθεσή του για τη δημοσίευση συμπληρωματικών προσωπικών δεδομένων[98]. Συνεπώς, για τα φυσικά πρόσωπα τα προσωπικά δεδομένα είναι το όνομα, το επώνυμο, το πατρώνυμο και η διεύθυνση, ενώ για τα νομικά πρόσωπα είναι η επωνυμία της επιχείρησης, η έδρα, η νομική μορφή και η διεύθυνση. Τόσο στα φυσικά πρόσωπα, όσο και στα νομικά, σε περίπτωση ρητής συγκατάθεσής τους, είναι δυνατή η δημοσίευση συμπληρωματικών του στοιχείων. Όπως γίνεται αντιληπτό, σε αυτό το σημείο το νομοθετικό πλαίσιο μέσω του 3471/2006 όσο και των επόμενων νόμων προσφέρει

επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα»

[95] Ν. 3471/2006, άρθρο 5 παρ. 1 και άρθρο 12 παρ. 3

[96] Ν. 3471/2006, άρθρο 5 παρ. 6

[97] Εισηγητική Έκθεση του ν.3471/2006

[98] Ν. 3471/2006, άρθρο 10 παρ. 2

στα νομικά πρόσωπα την ίδια προστασία με τα φυσικά που είναι συνδρομητές και χρήστες τέτοιων υπηρεσιών.

Το συγκεκριμένο νομοθετικό πλαίσιο είναι ένα σημαντικό βήμα, αφού προχωράει περαιτέρω στην προστασία των νομικών προσώπων τόσο σε σύγκριση νόμο 2774/1999, όσο και με την Οδηγία 2002/58/ΕΚ[99], η οποία δεν αναφέρεται ρητά στα νομικά πρόσωπα και στο δικαίωμα που αυτά έχουν για τη χρήση της συγκατάθεσης, με αποτέλεσμα να επιτρέπει στα κράτη μέλη να νομοθετήσουν, όπως επιθυμούν για το ζήτημα της συγκατάθεσης.[100]

Σε αυτό το σημείο αξίζει να τονιστούν οι δυσκολίες που προκύπτουν από την Οδηγία 2002/58/ΕΚ σχετικά με τα ακόλουθα ζητήματα:

- Επαλήθευση ότι κάποιο άτομο είναι όντως εκπρόσωπος κάποιου νομικού προσώπου και δεν δρα ως φυσικό
- Διασφάλιση ότι τα δικαιώματα του νομικού προσώπου θα ασκούνται από τον νόμιμο εκπρόσωπο του.

Επιπροσθέτως, στο άρθρο 16 του νόμου 3471/2006 αναφέρεται μία μεταβατική ρύθμιση για το περιεχόμενο των δημοσίων καταλόγων συνδρομητών που έχουν ήδη εκδοθεί.

Σύμφωνα με τον νόμο 3471, υπάρχει διάκριση για την μη υιοθέτηση του συστήματος προστασίας της προηγούμενης συγκατάθεσης σχετικά με την καταχώρηση δεδομένων σε καταλόγους συνδρομητών. Επί της ουσίας, δεν επεκτείνει την εν λόγω προστασία σε εκδόσεις καταλόγων, οι οποίοι έχουν ήδη διατεθεί στην αγορά, σε έντυπη ή μη δικτυακή ηλεκτρονική μορφή, πριν από την έναρξη του νόμου 3471. Σε αυτό το σημείο, αξίζει να τονιστεί ότι η λογική πίσω από αυτή την διάκριση ανάμεσα σε παλιούς και νέους συνδρομητές δεν είναι ξεκάθαρη, διότι ουσιαστικά δικαιολογεί αυτή τη μειωμένη προστασία, αφού οι συνδρομητές, των οποίων τα στοιχεία είναι τυπωμένα ή είναι συνδρομητές μέχρι την έναρξη του νόμου, μπορεί να ανέρχονται σε εκατομμύρια. Ακόμα και σήμερα, δεν είναι κατανοητή η συγκεκριμένη διάκριση,

[99] Παρ.4 της κοινοτικής οδηγίας 2002/58/ΕΚ
[100] Προίμιο της Οδηγίας 2002/58/ΕΚ, αιτιολογική σκέψη 45

αφού στην πραγματικότητα με την εν λόγω διάταξη ο νόμος απεμπολεί την συνολική φιλοσοφία της αυξημένης προστασίας των δικαιωμάτων των συνδρομητών και χρηστών[101].

Πέρα από την αρχή της αναλογικότητας, αξίζει να γίνει μία σύντομη αναφορά και στην αρχή της καθορισμένης χρονικής διάρκειας τήρησης των δεδομένων. Η συγκεκριμένη αρχή υποχρεώνει τη διατήρηση σε μορφή που να κάνει δυνατό τον προσδιορισμό της ταυτότητας των υποκειμένων τους, μόνο κατά τη διάρκεια της απαιτούμενης περιόδου για την εκτέλεση των σκοπών της συλλογής, αλλά και της επεξεργασίας τους[102]. Αναφορά της εν λόγω αρχής στις ηλεκτρονικές επικοινωνίες γίνεται στο άρθρο 6 του ν.3471/2006, όπου αναφέρεται ότι *«Επιτρέπεται η επεξεργασία δεδομένων θέσης, που αφορούν τους χρήστες ή συνδρομητές δικτύων ή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, για την παροχή υπηρεσίας προστιθέμενης αξίας, μόνον εφόσον αυτά καθίστανται ανώνυμα με την κατάλληλη κωδικοποίηση ή με τη ρητή συγκατάθεση του χρήστη ή του συνδρομητή, στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μίας υπηρεσίας προστιθέμενης αξίας»*[103].

Εφαρμογή σε επίπεδο νομοθετικού πλαισίου της αρχής της καθορισμένης χρονικής διάρκειας τήρησης των δεδομένων είναι η παράγραφος 1 του άρθρου 6 του νόμου 3471/2006, η οποία προβλέπει την καταστροφή των δεδομένων κίνησης με τη λήξη της επικοινωνίας. Επιπροσθέτως, στην πρώτη παράγραφο του άρθρου 6 της οδηγίας 2002/58/ΕΚ, όσο και του άρθρου 6 του 3471/2006 τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες και τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο ηλεκτρονικών επικοινωνιών, πρέπει να σβήνονται ή να γίνονται ανώνυμα[104], όταν δεν είναι πλέον απαραίτητα για το σκοπό της ολοκλήρωσης μιας επικοινωνίας.

Σχετικά με τον τρόπο με τον οποίο ολοκληρώνεται η επικοινωνία, θα πρέπει να εξεταστεί το προοίμιο της Οδηγίας 2002/58/ΕΚ όπου αναφέρεται, ότι η στιγμή της ολοκλήρωσης, βασίζεται στον τύπο υπηρεσίας ηλεκτρονικών επικοινωνιών που παρέχεται. Συν τοις άλλοις, ενδεικτικά αναφέρεται πως *«….για μια κλήση φωνητικής τηλεφωνίας η μετάδοση ολοκληρώνεται μόλις κάποιος από τους χρήστες περατώσει τη σύνδεση, για το ηλεκτρονικό ταχυδρομείο η μετάδοση*

[101] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[102] Αλεξανδροπούλου- Αιγυπτιάδου Ε, «Προσωπικά Δεδομένα», Εκδόσεις Αντ. Σάκκουλα, 2007
[103] Αλεξανδροπούλου- Αιγυπτιάδου Ε, «Προσωπικά Δεδομένα», Εκδόσεις Αντ. Σάκκουλα, 2007
[104] Όπως αναφέρεται στον Ν. 3471/2006 «με κατάλληλη κωδικοποίηση»

ολοκληρώνεται μόλις ο παραλήπτης λάβει το μήνυμα, συνήθως από τον εξυπηρετητή του οικείου παρόχου υπηρεσίας»[105]. Σχετικά με την κίνηση στο διαδίκτυο, η επικοινωνία τελειώνει αμέσως μόλις ο χρήστης αποκτήσει πρόσβαση στον ιστοχώρο τον οποίο αναζητούσε.

Αξίζει όμως σε αυτό το σημείο να αναφερθούν και κάποιες εξαιρέσεις σχετικά με τα δεδομένα κίνησης. Ο νόμος 3471/2006 στο άρθρο 6 μεταφέροντας την δεύτερη παράγραφο του άρθρου 6 της 2002/58/ΕΚ επιτρέπει ουσιαστικά την επεξεργασία των δεδομένων κίνησης, ακόμα και μετά τη λήξη της επικοινωνίας, όταν αυτό είναι αναγκαίο[106] για τη χρέωση των συνδρομητών[107]. Ο φορέας παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούται να ενημερώσει τον συνδρομητή σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία, αλλά και σχετικά με τη διάρκεια της εν λόγω επεξεργασίας, η οποία επιτρέπεται μόνο έως το τέλος της περιόδου μέσα στην οποία μπορεί να αμφισβητηθεί ο λογαριασμός.

Σύμφωνα με την αιτιολογική σκέψη της καταργηθείσας Οδηγίας 97/66/ΕΚ, στο εν λόγω ζήτημα βοηθά ιδίως η ερμηνεία του άρθρου 6 παράγραφος 2, αναφέροντας ότι: *«...ότι τα δεδομένα που αφορούν συνδρομητές και υφίστανται επεξεργασία για την πραγματοποίηση κλήσεων περιέχουν πληροφορίες για την ιδιωτική ζωή των φυσικών προσώπων και αφορούν το σεβασμό του απορρήτου της αλληλογραφίας τους ή τα έννομα συμφέροντα νομικών προσώπων· ότι τα δεδομένα αυτά επιτρέπεται να αποθηκεύονται μόνο στο βαθμό που αυτό είναι απαραίτητο για την παροχή υπηρεσιών για τη χρέωση και την πληρωμή διασυνδέσεων, για περιορισμένο δε χρόνο· ότι κάθε άλλη επεξεργασία την οποία επιθυμεί να διενεργήσει ο φορέας παροχής της διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας για την εμπορική προώθηση των ιδίων του τηλεπικοινωνιακών υπηρεσιών επιτρέπεται μόνον εφόσον συμφωνεί με αυτήν ο συνδρομητής, βάσει ακριβών και πλήρων πληροφοριών που παρέχει ο φορέας παροχής της διαθέσιμης στο κοινό τηλεπικοινωνιακής υπηρεσίας σχετικά με τα είδη περαιτέρω επεξεργασίας που σκοπεύει να διενεργήσει»*.

Στη συνέχεια όπως αναφέρεται στο προοίμιο της 2002/58/ΕΚ : *«Τα δεδομένα αυτά επιτρέπεται να αποθηκεύονται μόνον εφόσον είναι απαραίτητο για την παροχή υπηρεσιών για τη*

[105] Οδηγία 2002/58, αιτιολογική σκέψη 27
[106] Ν. 3471/2006, άρθρο 6 παρ. 2
[107] Ν. 3471/2006, άρθρο 6 παρ. 2

χρέωση και την πληρωμή διασυνδέσεων και μόνο για περιορισμένο χρόνο»[108] Είναι επίσης ξεκάθαρο από τα όσα αναφέρονται στον νόμο, ότι τα δεδομένα που φυλάσσονται για λόγους που αφορούν τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων χρειάζεται να αποθηκεύονται μόνο για κάποια πεπερασμένη και περιορισμένη χρονική περίοδο και δεν επιτρέπεται να είναι συνηθισμένη η τήρησή τους για μακρές χρονικές περιόδους και πάντα εντός του πλαισίου της Οδηγίας 95/46/ΕΚ στην οποία αναφέρεται: *«ότι στόχος των εθνικών νομοθεσιών όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι η διασφάλιση της προστασίας των θεμελιωδών δικαιωμάτων και ιδίως της ιδιωτικής ζωής, όπως επίσης αναγνωρίζεται στο άρθρο 8 της ευρωπαϊκής σύμβασης περί προστασίας των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών καθώς και στις γενικές αρχές του κοινοτικού δικαίου· ότι, για το λόγο αυτό, η προσέγγιση των εν λόγω νομοθεσιών δεν πρέπει να Οδηγήσει στην εξασθένηση της προστασίας που εξασφαλίζουν αλλά, αντιθέτως, πρέπει να έχει ως στόχο την κατοχύρωση υψηλού επιπέδου προστασίας στην Κοινότητα»*[109]. Παρόλο αυτά, δεν προβλέπεται μία ενιαία ρύθμιση ως προς το χρονικό σημείο κατά το οποίο τελειώνει η περίοδος εντός της οποίας μπορεί να αμφισβητείται νομίμως ο λογαριασμός ή να επιδιώκεται η πληρωμή, αλλά αφήνεται στα διάφορα μέλη κράτη της Ε.Ε. να ρυθμίσουν ελεύθερα στην εσωτερική τους νομοθεσία για αυτό το ζήτημα[110].

Η ομάδα του άρθρου 29 είχε υποστηρίξει ότι η εφαρμογή της αρχής της αναλογικότητας και η ρύθμιση του άρθρου 6 παράγραφος 2 Οδηγίας 2002/58/ΕΚ, κατά την οποία τα δεδομένα κίνησης επιτρέπεται να υποβάλλονται σε επεξεργασία *«μόνο έως το τέλος της περιόδου εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή»* επιβάλλουν τα δεδομένα κίνησης να τηρούνται όσο είναι αναγκαίο για το διακανονισμό του λογαριασμού και τη διευθέτηση των διαφορών. Υπό κανονικές συνθήκες, αυτό θα σήμαινε ότι ως περίοδος αποθήκευσης θα ήταν το ανώτερο 3-6 μήνες για περιπτώσεις, κατά τις οποίες οι λογαριασμοί έχουν εξοφληθεί και δεν έχουν αμφισβητηθεί. Τονίζει ειδικότερα ότι η αποθήκευση των

[108] Οδηγία 2002/58/ΕΚ, αιτιολογική σκέψη 26
[109] Αιτιολογική σκέψη 10 της Οδηγίας 95/46/ΕΚ
[110] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

δεδομένων για μεγαλύτερο χρονικό διάστημα μπορεί να γίνει όταν υπάρχει αμφισβήτηση του ύψους του λογαριασμού, προκειμένου να διευκολυνθεί ο διακανονισμός του[111].

Συν τοις άλλοις, στις περιπτώσεις κατά τις οποίες ο λογαριασμός έχει εξοφληθεί, μπορεί να δικαιολογηθεί μία μεγαλύτερη διάρκεια αποθήκευσης για εξαιρετικές περιπτώσεις, όπου υπάρχουν σαφείς ενδείξεις ότι ο λογαριασμός πρόκειται να αμφισβητηθεί. Σε όλες αυτές τις περιπτώσεις, οι περίοδοι αποθήκευσης πρέπει να ορίζονται με βάση τα ιδιαίτερα χαρακτηριστικά κάθε περίπτωσης, έτσι ώστε να είναι δυνατή η διευθέτηση διαφορών. Αυτές οι μακρύτερες χρονικές περίοδοι δεν είναι δυνατόν να υπερβαίνουν σε διάρκεια τη μέγιστη χρονική περίοδο που προβλέπεται από την εθνική νομοθεσία. Η περίοδος της αναφοράς ξεκινά όταν τα δεδομένα κίνησης δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας[112].

Αξίζει σε αυτό το σημείο να αναφερθεί, και αυτό είναι λογικό, ότι η ακριβής στιγμή της ολοκλήρωσης της μετάδοσης μιας επικοινωνίας εξαρτάται από τον τύπο υπηρεσίας ηλεκτρονικών επικοινωνιών που παρέχεται. Στην περίπτωση που η παροχή της τηλεπικοινωνιακής υπηρεσίας είναι δωρεάν ή καλύπτεται από κάποιο πάγιο τέλος, κάτι που αποτελεί πρακτική, η οποία συνεχώς κερδίζει έδαφος, τότε είναι προφανές ότι δεν υπάρχει καμιά δικαιολογητική βάση από μέρους των παρόχων των υπηρεσιών αυτών για διατήρηση των δεδομένων κίνησης.

Η τελευταία παράγραφος του άρθρου 6 του νόμου 3471/2006 προβλέπει ότι σε κάθε περίπτωση οι προηγούμενες παράγραφοι του άρθρου που θέτουν το πλαίσιο για την διασφάλιση της προστασίας των δεδομένων κίνησης με την απάλειψη και ανωνυμοποίηση τους, την δυνατότητα επεξεργασίας τους μετά από συγκατάθεση του υποκειμένου και τον περιορισμό των αρμοδίων που εμπλέκονται στη διαδικασία επεξεργασίας ισχύουν, πάντα με την επιφύλαξη της δυνατότητας της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) να μπορεί να ενημερώνεται για τα δεδομένα κίνησης με σκοπό την επίλυση διαφορών, ιδίως σχετικά με τη διασύνδεση ή τη χρέωση.

[111] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[112] Οδηγία 2002/58/ΕΚ, άρθρο 6 παρ 1

Αντιστοίχως, η διάταξη 6 περιέχεται και στην Οδηγία 2002/58/ΕΚ κατά την οποία οι παράγραφοι 1, 2, 3 και 5 της Οδηγίας 2002/58/ΕΚ ισχύουν με την επιφύλαξη της δυνατότητας των αρμοδίων φορέων να ενημερώνονται για τα δεδομένα κίνησης σύμφωνα με την ισχύουσα νομοθεσία με σκοπό την επίλυση διαφορών, ιδίως σχετικά με τη διασύνδεση ή τη χρέωση.

Επιπροσθέτως, θα μπορούσε να υποστηριχθεί ότι η ρύθμιση της Ένωσης στην προσπάθεια να περιορίσει την προστασία των δεδομένων κίνησης για διαφορές σχετικές με τη διασύνδεση ή χρέωση δεν ήταν επιτυχημένη. Συγκεκριμένα, από την γενική έννοια των αρμοδίων φορέων και την αποφυγή ανάλυσης στο προοίμιο της Οδηγίας των πιθανών προβλημάτων στη διασύνδεση και την χρέωση που μπορεί να αποτελεί αφορμή για ανάλυση των δεδομένων κίνησης από αρμόδιους φορείς για λόγους άλλους από τους προβαλλόμενους, όπως της πρόληψης και καταστολής εγκλημάτων. Αυτό μπορεί να θεωρηθεί ως μία πρώτη προσπάθεια χρησιμοποίησης των δεδομένων αυτών κίνησης, έτσι ώστε να εφαρμοστεί η διατήρηση των δεδομένων άμεσα χωρίς περαιτέρω δικονομικές διατυπώσεις. Σε αυτή την κατεύθυνση της επιμήκυνσης του χρόνου τήρησης των δεδομένων κίνησης και θέσης για λόγους διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων κινείται τόσο η Οδηγία 2006/24/ΕΚ, όσο και ο νόμος 3917/2011[113].

Σε αυτό το σημείο είναι αναγκαίο να γίνει σύντομη αναφορά στην ανωνυμοποίηση των δεδομένων θέσης, όσο και στη χρονική διάρκεια της διατήρησης των δεδομένων. Η παράγραφος 3 του άρθρου 6 του νόμου 3471/2006 είναι ανάλογη έκφραση της αρχής της καθορισμένης χρονικής διάρκειας τήρησης των δεδομένων και επιτρέπει την επεξεργασία των δεδομένων θέσης που αφορούν τους χρήστες ή συνδρομητές δικτύων ή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, όταν αυτό είναι αναγκαίο για την παροχή υπηρεσίας προστιθέμενης αξίας[114] υπό την προϋπόθεση αυτά προηγουμένως να έχουν καταστεί ανώνυμα με την κατάλληλη κωδικοποίηση ή με τη ρητή συγκατάθεση του χρήστη ή του συνδρομητή, στην απαιτούμενη έκταση και την απαιτούμενη διάρκεια για την παροχή μίας υπηρεσίας προστιθέμενης αξίας. Δηλαδή μετά την παροχή της υπηρεσίας, ο πάροχος δεν μπορεί να

[113] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[114] Ν. 3471/2006, άρθρο 6 παρ. 3

αποθηκεύει τα δεδομένα θέσης των χρηστών, παρά κατ' εξαίρεση όταν αυτά αναγκαία για τη χρέωση και την πληρωμή της διασύνδεσης[115].

Πέρα από την ανωνυμοποίηση των δεδομένων θέσης, σημαντικό σημείο του νομοθετικού πλαισίου είναι η λήψη συγκατάθεσης. Η συγκατάθεση του υποκειμένου αποτελεί μία από τις πιο σημαντικές προϋποθέσεις της νομιμότητας της επεξεργασίας. Ο Γενικός Κανονισμός Προστασίας Δεδομένων ορίζει ως: *«συγκατάθεση» του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*.

Η συγκατάθεση του χρήστη ή συνδρομητή, είναι επί της ουσίας η κύρια έκφραση του θετικού περιεχομένου του δικαιώματος του πληροφοριακού αυτοκαθορισμού[116], προβλέποντας ότι η επεξεργασία επιτρέπεται μόνο αν ο χρήστης ή συνδρομητής έχει πρώτα δώσει τη συγκατάθεση του μετά από ενημέρωση για το είδος των δεδομένων, το σκοπό και την έκταση της επεξεργασίας, όπως και για τους αποδέκτες. Η μεγάλη σημασία του δικαιώματος της συγκατάθεσης φαίνεται και από την αναφορά που γίνεται στον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και συγκεκριμένα στο άρθρο Άρθρο 8 παρ. 2 που αναφέρει ότι: *«Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.»*[117]

Συν τοις άλλοις, η ελευθερία της συγκατάθεσης εξειδικεύεται και στο άρθρο 10 αρ. 4 εδ. 4 του νόμου 3471/2006, όπου αναφέρεται: *«Δεν επιτρέπεται στους φορείς παροχής υπηρεσιών δημοσίων καταλόγων να εξαρτούν την παροχή των υπηρεσιών δημοσίου καταλόγου από τη*

[115] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_el.pdf
[116] Γέροντα Α., « Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων», Αθήνα, 2002
[117] http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):EL:HTML

συγκατάθεση του συνδρομητή για τη διαβίβαση των δεδομένων για σκοπούς άλλους από αυτούς για τους οποίους έχουν συλλεγεί»[118].

Όταν γίνεται διαβίβαση των δεδομένων κίνησης σε παρόχους δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών από αντίστοιχο φορέα δεδομένων κίνησης, με σκοπό τη χρέωση των παρεχόμενων υπηρεσιών δεν χρειάζεται μεν η προηγούμενη συγκατάθεση του συνδρομητή/χρήστη, θα πρέπει όμως ο συνδρομητής ή ο χρήστης να έχει ενημερωθεί κατά την κατάρτιση της σύμβασης εγγράφως ότι οι φορείς παροχής δημοσίου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών θα μπορούν λαμβάνουν τα δεδομένα κίνησης[119].

Η λήψη συγκατάθεσης είναι υποχρεωτική και μετά από ενημέρωση, επαναλαμβάνεται και για τα δεδομένα θέσης[120], αφού απαιτείται από τους φορείς παροχής υπηρεσιών να ενημερώνουν τον χρήστη ή τον συνδρομητή, πριν από τη χορήγηση της συγκατάθεσής του για τα ακόλουθα:

1. Τον τύπο των δεδομένων θέσης που υποβάλλονται σε επεξεργασία
2. Τους σκοπούς
3. Τη διάρκεια της εν λόγω επεξεργασίας
4. Το ενδεχόμενο μετάδοσής τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας.

Ουσιαστικά, η ενημέρωση των χρηστών δεν είναι κάτι εύκολο εξαιτίας της περιορισμένης δυνατότητας μεταφοράς δεδομένων της τεχνολογίας ιδιαίτερα στις περιπτώσεις του κινητού τερματικού εξοπλισμού[121], καθώς η μεταφορά δεδομένων μπορεί να εμποδίζεται από δυσκολίες στη λήψη του εξοπλισμού.

Γενικότερα, η αρχή της συγκατάθεσης μπορεί να ανακληθεί σε οποιαδήποτε στιγμή απαιτείται[122] και αν ανακληθεί και τα δεδομένα έχουν εν τω μεταξύ χρησιμοποιηθεί ή ληφθεί από τρίτους, η ανάκληση ανακοινώνεται σε αυτούς με φροντίδα του υπεύθυνου επεξεργασίας[123].

---

[118] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[119] Άρθρο 5 παρ. 5 εδ γ. Νόμος 3471/2006
[120] Άρθρο 5 παρ.1 εδ α. Νόμος 3471/2006
[121] www.cs.helsinki.fi/n/Kraatika/Courses/F4fMC/WS2/Pitkaranta.pdf
[122] Άρθρο 5 παρ.5 εδ δ. Νόμος 3471/2006
[123] Άρθρο 5 παρ.5 εδ ε. Νόμος 3471/2006

Σχετικά με τον τρόπο και χρόνο ανάκλησης της δήλωσης συγκατάθεσης, ο νομοθέτης θέτει τον όρο «οποτεδήποτε» για τη δυνατότητα αυτή του χρήστη[124]. Επιπροσθέτως, ο νόμος εισάγει και τη ρητή απαγόρευση προς τους φορείς δημοσίου δικτύου ή/ και διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών να εξαρτούν την παροχή των υπηρεσιών αυτών προς τον συνδρομητή ή τον χρήστη από τη συγκατάθεσή του στην επεξεργασία των δεδομένων αυτών, όταν η επεξεργασία αυτή γίνεται για σκοπούς άλλους από εκείνους που εξυπηρετούν άμεσα την παροχή των υπηρεσιών που αφορούν τα άρθρα 1 έως 17 του νόμου[125].

Συγκεκριμένα, σχετικά με τα δεδομένα θέσης δηλαδή, τα δεδομένα που αποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη τόσο στον ελληνικό νόμο, όσο και στις Ευρωπαϊκές οδηγίες υπάρχει η πρόβλεψη για τη δυνατότητα χρήσης των δεδομένων θέσης για συγκεκριμένους σκοπούς, αφού επιτρέπεται η επεξεργασία των δεδομένων θέσης που αφορούν τους χρήστες δικτύων ή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, όταν αυτά τα δεδομένα είναι αναγκαία για την παροχή κάποιας υπηρεσίας προστιθέμενης αξίας[126]. Βέβαια, σε αυτή την περίπτωση πρέπει να υπάρχει η ρητή συγκατάθεση του χρήστη ή του συνδρομητή, μέσα στα πλαίσια της απαιτούμενης έκτασης και διάρκειας για την παροχή μίας υπηρεσίας προστιθέμενης αξίας[127].

Σχετικά με τον τύπο της συγκατάθεσης ειδικά για τις ηλεκτρονικές επικοινωνίες αναφέρεται ότι αυτή μπορεί να γίνει είτε εγγράφως σύμφωνα με το άρθρο 160 παρ. 1 του αστικού κώδικα, δηλαδή ιδιοχείρως υπογεγραμμένη είτε ηλεκτρονικά[128]. Η δυνατότητα της εξωτερίκευσης της δηλώσεως συγκατάθεσης διαζευκτικά με δύο τρόπους επιβάλλεται, καθώς ο παραδοσιακός έγγραφος τύπος δεν χρησιμοποιείται πλέον στις ηλεκτρονικές συναλλαγές, αφού χρειάζεται να εξασφαλίζεται ότι οι νομικές προϋποθέσεις που ισχύουν για τη διαδικασία σύναψης των συμβάσεων δεν παρακωλύουν τη χρήση των συμβάσεων που συνάπτονται με ηλεκτρονικά μέσα

[124] Χριστοδούλου Κ., «Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα», 2007
[125] Άρθρο 5 παρ.5 εδ ζ. Νόμος 3471/2006
[126] Άρθρο 6 παρ 3 Νόμος 3471/2006
[127] Αιτιολογική σκέψη 35 Οδηγίας 2002/58/ΕΚ
[128] Άρθρο 5 παρ.3 εδ α. Νόμος 3471/2006

ούτε αποστερούν τις συμβάσεις αυτές εννόμου αποτελέσματος ή ισχύος λόγω του ότι έχουν συναφθεί με ηλεκτρονικά μέσα[129].

Σε περίπτωση ηλεκτρονικής συγκατάθεσης, ο υπεύθυνος επεξεργασίας των δεδομένων πρέπει από τον νόμο να εξασφαλίζει τα ακόλουθα:

1 Ο χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωσή, του η οποία καταγράφεται με τεχνικά μέσα που προσφέρουν αυξημένη ασφάλεια

2 Η εν λόγω συγκατάθεση μπορεί να είναι συνέχεια προσβάσιμη στον χρήστη ή συνδρομητή και φυσικά μπορεί όποτε επιθυμεί να την ανακαλέσει.

Οι προϋποθέσεις της ηλεκτρονικής συγκατάθεσης ειδικότερα, είναι ο ασφαλής τεχνικά τρόπος και η άμεσα προσβάσιμη δήλωση. Σχετικά με την κατανόηση της έννοιας του ασφαλή τεχνικά τρόπου της δήλωσης του συνδρομητή, συναφές είναι το προεδρικό διάταγμα 150/2001, όπου στο παράρτημα ΙΙΙ γίνεται λόγος για *«απαιτήσεις για ασφαλείς διατάξεις δημιουργίας υπογραφής» οι οποίες και ταυτίζονται με την έννοια της «προηγμένης υπογραφής»* σύμφωνα και με το άρθρο 2 παρ.2 του π.δ. Συνεπώς, για τη συγκατάθεση αρκεί έγγραφο ασφαλές ως ασυμμετρικά κρυπτογραφημένο[130].

Ως άμεση πρόσβαση νοείται η δυνατότητα του συνδρομητή ή χρήστη να μπορεί ανά πάσα στιγμή στο μέλλον να αναζητεί και να ανατρέχει στη δήλωση του, η οποία με τη μορφή ηλεκτρονικού εγγράφου δεν θα μπορεί να μεταβληθεί παρά μόνο με τη διαδικασία της ανάκλησης[131]. Η αποθήκευση της δήλωσης συγκατάθεσης πρέπει να γίνεται σε σταθερό μέσο αποθήκευσης δεδομένων με την έννοια του άρθρου 2 της Οδηγίας 2002/65 δηλαδή σε *«κάθε μέσο που επιτρέπει στον καταναλωτή να αποθηκεύει πληροφορίες απευθυνόμενες προσωπικά σε*

[129] Άρθρο 9 της Οδηγίας 2000/31/ΕΚ
[130] Χριστοδούλου Κ., «Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα», 2007
[131] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

αυτόν, κατά τρόπο προσπελάσιμο για μελλοντική αναφορά επί χρονικό διάστημα επαρκές για τους σκοπούς που εξυπηρετούν οι πληροφορίες, και το οποίο επιτρέπει την ακριβή αναπαραγωγή»[132].

Σχετικά με τα δεδομένα θέσης μετά την λεπτομερή ενημέρωση τους οι εκάστοτε χρήστες μπορούν να δώσουν τη συγκατάθεση τους. Οι φορείς, στους οποίους πρέπει να απευθύνεται η συγκατάθεση είναι δύο:

- Ο φορέας εκμετάλλευσης ηλεκτρονικών επικοινωνιών που παρέχει την ζητηθείσα προστιθέμενη υπηρεσία
- Ο πάροχος της υπηρεσίας, ο οποίος πρέπει να λάβει τη συγκατάθεση του προσώπου στο οποίο αναφέρονται τα δεδομένα.

Σχετικά με τις ειδικές περιπτώσεις της υποχρέωσης για τη λήψη συγκατάθεσης τόσο με τον νόμο 3471/2006, όσο και με τους επόμενους νόμους[133], οι πάροχοι των αντίστοιχων υπηρεσιών αποκτούν την άδεια να δημοσιεύουν στους έντυπους ή ηλεκτρονικούς καταλόγους συνδρομητών μόνο τα δεδομένα προσωπικού χαρακτήρα που χρειάζονται για την αναγνώριση της ταυτότητας συγκεκριμένου συνδρομητή (όνομα, επώνυμο, πατρώνυμο, διεύθυνση), εκτός φυσικά, εάν ο συνδρομητής έχει δώσει τη ρητή συγκατάθεσή του για τη δημοσίευση συμπληρωματικών δεδομένων προσωπικού χαρακτήρα[134].

Επιπροσθέτως τόσο ο 3471/2006 στο άρθρο 11 μεταφέροντας το άρθρο 13 της ευρωπαϊκής Οδηγίας 2002/58/ΕΚ, όσο και ο 4070/2012 αναφέρονται στην αρχή της προηγούμενης συγκατάθεσης ως την προϋπόθεση για την πραγματοποίηση μη ζητηθεισών επικοινωνιών με τη χρησιμοποίηση αυτόματων συστημάτων κλήσης, όπως με τη χρήση συσκευών τηλεομοιοτυπίας είτε ηλεκτρονικού ταχυδρομείου και γενικότερα με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση που έχουν σαν σκοπό την απευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς. Συν τοις άλλοις, είναι χρήσιμο να αναφερθεί ότι με το άρθρο 16 του νόμου 3917/2011 επέρχεται αλλαγή του άρθρου 11, η οποία ισχύει από 01.09.2011[135]. Συγκεκριμένα οι λέξεις «με ή» της παρ.1 διαγράφονται. Έτσι με την πρώτη παράγραφο επιτρέπεται η πραγματοποίηση μη ζητηθεισών

[132] http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:271:0016:0024:EL:PDF
[133] Νόμος 4070/ 2012 και 4509/2017
[134] Άρθρο 10 παρ. 2 Νόμου 3471/2006
[135] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

επικοινωνιών με τη χρησιμοποίηση αυτόματων συστημάτων κλήσης, όπως με τη χρήση συσκευών τηλεομοιοτυπίας είτε ηλεκτρονικού ταχυδρομείου, και γενικότερα με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, χωρίς ανθρώπινη παρέμβαση, που έχουν σαν σκοπό την απευθείας εμπορική προώθηση προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς. Αντίστοιχα για τους αποδέκτες τηλεφωνικών κλήσεων, θα ισχύει το σύστημα της γενικής δήλωσης με υποχρέωση των παρόχων να καταρτίζουν διαθέσιμους στο κοινό ειδικούς καταλόγους των συνδρομητών που δεν επιθυμούν επικοινωνία[136]. Όπως αναφέρει και η εισηγητική έκθεση του 3917/2011, ο σκοπός αυτής της αντικατάστασης είναι να αρθεί η αντιφατικότητα στη γραμματική διατύπωση της πρώτης παραγράφου του άρθρου 11 του 3471/2006 με την οποία υιοθετήθηκε η παράλληλη εφαρμογή και του συστήματος συγκατάθεσης (opt – in) και του συστήματος γενικής δήλωσης (opt – out) της δεύτερης παραγράφου σε αντίθεση με την οδηγία 2002/58/ΕΚ που προβλέπει την επιλογή μεταξύ των δύο συστημάτων[137].

Ο νόμος 2251/1994 για την προστασία των καταναλωτών, όπως τροποποιήθηκε με τον 3587/2007 προβλέπει ότι η χρησιμοποίηση των τεχνικών επικοινωνίας πρέπει να γίνεται, έτσι ώστε να μην προσβάλλεται η ιδιωτική ζωή του καταναλωτή[138]. Οι έννοιες όμως της απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και της προηγούμενης συγκατάθεσης χρήζουν ιδιαίτερης ανάλυσης στα πλαίσια του άρθρου 11 του 3471/2006 και γι' αυτό αξίζει να εξεταστούν οι προβληματισμοί που αναπτύχθηκαν γύρω από το ζήτημα στα πλαίσια της υιοθέτησης της Οδηγίας 2002/58/ΕΚ, για να μπορέσει ο αναγνώστης να καταλάβει τους σκοπούς του Έλληνα νομοθέτη[139].

Το πρώτο σημείο με το οποίο ασχολήθηκαν οι ειδικοί στην προστασία προσωπικών δεδομένων, ήταν η έννοια της απευθείας εμπορικής προώθησης. Σχετικά με την έννοια της απευθείας εμπορικής προώθησης ή άμεσης διαφήμισης, αναφορά υπάρχει στην οδηγία 95/46/ΕΚ. Συγκεκριμένα, στο προοίμιο[140] της οδηγίας γίνεται έμμεση αναφορά στην έννοια της

[136] Νόμος 3917/2011, άρθρο 16
[137] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[138] Νόμος 2251/1994 και τροποποίηση με το άρθρο 4 παρ.6 του νόμου 3587/2007
[139] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[140] Αιτιολογική παράγραφος 30 της Οδηγίας 95/46/ΕΚ

άμεσης διαφήμισης και ορίζεται ότι τα κράτη μέλη μπορούν να προσδιορίζουν τις προϋποθέσεις, με τις οποίες τα δεδομένα προσωπικού χαρακτήρα μπορούν να χρησιμοποιούνται και να ανακοινώνονται σε τρίτους, όταν αυτό γίνεται στα πλαίσια νόμιμης συνήθους δραστηριότητας στις επιχειρήσεις ή άλλους οργανισμούς και ότι επίσης, μπορούν να προσδιορίζουν τις προϋποθέσεις υπό τις οποίες μπορούν να ανακοινώνονται σε τρίτους τα δεδομένα προσωπικού χαρακτήρα για εμπορικούς ή διαφημιστικούς σκοπούς που επιδιώκονται είτε από εμπορικούς φορείς είτε από φιλανθρωπικά σωματεία ή άλλες οργανώσεις ή ενώσεις για παράδειγμα πολιτικού χαρακτήρα[141].

Σύμφωνα με την γνώμη της ομάδας εργασίας του άρθρου 29 το άρθρο 13 της Οδηγίας 2002/58/ΕΚ καλύπτει κάθε μορφή προώθησης των πωλήσεων, συμπεριλαμβανομένης της απευθείας εμπορικής προώθησης από φιλανθρωπικά σωματεία και οργανώσεις πολιτικού χαρακτήρα. Σε αυτό το σημείο αξίζει να σημειωθεί ότι ευρύς ορισμός έχει χρησιμοποιηθεί από την Ευρωπαϊκή Ομοσπονδία Απευθείας Εμπορικής Προώθησης (FEDMA) στον κώδικα πρακτικής για την χρήση προσωπικών δεδομένων στην απευθείας εμπορική προώθηση. Σύμφωνα με τον κώδικα, η απευθείας εμπορική προώθηση ως προς την επικοινωνία μπορεί να γίνει με οποιοδήποτε μέσο (που περιλαμβάνει, αλλά δεν περιορίζεται στο ταχυδρομείο, υπηρεσίες on-line κ.λπ.) οποιουδήποτε διαφημιστικού υλικού ή υλικού εμπορικής προώθησης και διενεργείται από τον αρμόδιο απευθείας εμπορικής προώθησης ή εξ ονόματός του και απευθύνεται σε συγκεκριμένα πρόσωπα[142].

Η επικέντρωση σε συγκεκριμένα πρόσωπα είναι αυτή που διαφοροποιεί την απλή διαφήμιση που απευθύνεται σε μεγάλο αριθμό ατόμων, από την άμεση εμπορική προώθηση. Πάντως, σύμφωνα με την παράγραφο 4 του άρθρου 11, η διαφήμιση προϊόντων και υπηρεσιών μέσω του ηλεκτρονικού ταχυδρομείου είναι δυνατόν να επιτρέπεται παρόλα αυτά αρκεί να ισχύουν τα ακόλουθα:

1. Να είναι σαφής και ευδιάκριτη η αναγραφή της ταυτότητας[143] του αποστολέα

[141] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[142] http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp77-annex_en.pdf
[143] Προοίμιο της οδηγίας 2001/58/ΕΚ

2. Να υπάρχει αντίστοιχη έγκυρη διεύθυνση, έτσι ώστε να μπορεί ο αποδέκτης του μηνύματος να τερματίζει, εάν το επιθυμεί, την επικοινωνία[144].

Στην Ευρωπαϊκή οδηγία στο άρθρο 13 παρ.4, αλλά και στον ελληνικό νόμο στο άρθρο 11 τίθεται σαν αρνητική προϋπόθεση η μη συγκάλυψη της ταυτότητας του αποστολέα κάποιου ηλεκτρονικού μηνύματος, του επονομαζόμενου και « spoofing»[145].

Πέρα από όλα τα παραπάνω, αξίζει να τονιστεί το ζήτημα της συγκατάθεσης στην άμεση διαφήμιση που είναι συναφές θέμα με την περίπτωση προηγούμενης συγκατάθεσης του υποκειμένου. Περιπτώσεις που ο πελάτης δίνει την προηγούμενη συγκατάθεσή του με την εγγραφή του σε ιστοσελίδα και αργότερα του ζητείται η επιβεβαίωση της εγγραφής, αλλά και της συγκατάθεσης του συνάδει μάλλον με τις διατάξεις της Οδηγίας. Μία απλή όμως ειδοποίηση με ένα μήνυμα ηλεκτρονικού ταχυδρομείου προς όλους τους αποδέκτες ζητώντας τους να δώσουν την συγκατάθεση τους για την αποδοχή «διαφημιστικών e-mails» δεν θα ήταν συμβατή με την Ευρωπαϊκή νομοθεσία, διότι δεν θεωρείται ότι ο πελάτης μπορεί να ενημερωθεί για την χρησιμοποίησή τους για άμεση εμπορική προώθηση με σαφή και ευκρινή τρόπο και να του δίνεται η ευκαιρία να αρνείται τη χρησιμοποίηση αυτή σύμφωνα με το άρθρο 13 παρ. 3 και αιτιολογική σκέψη 42 της Οδηγίας[146].

Συν τοις άλλοις, σε περίπτωση συγκατάθεσης με την ευκαιρία γενικής αποδοχής των όρων που διέπουν πιθανό κύριο συμβόλαιο, η συγκατάθεση πρέπει να συνάδει με τις επιταγές της Οδηγίας 95/46/ΕΚ δηλαδή της ελεύθερης, ρητής και εν πλήρει επιγνώσει συγκατάθεσης. Επιπροσθέτως, στην αιτιολογική σκέψη 17 αναφέρεται ότι η *«συγκατάθεση δύναται να παρέχεται με κάθε πρόσφορο τρόπο που επιτρέπει την ελεύθερη και ενημερωμένη έκφραση των επιθυμιών του χρήστη, όπως με τη συμπλήρωση τετραγωνιδίου κατά την επίσκεψη ιστοσελίδας του Διαδικτύου».*

Για να μην υπάρξει καμία σκιά ή παρανόηση στο ζήτημα της συγκατάθεσης, είναι αναγκαίο να αναφερθεί ότι η σιωπηρή συγκατάθεση δεν θεωρείται ότι είναι συμβατή με τους σκοπούς της

[144] Άρθρο 11 παρ. 1 ν.3471/2006 και 13 παρ.4 Οδηγίας 2002/58/ΕΚ
[145] Asscher, Lodewijk F., «Regulating Spam: Directive 2002/58 and Beyond», 2004
[146] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

οδηγίας 95/46 ειδικότερα με την απαίτηση να θεωρείται συγκατάθεση η μη αντίθεση στην αποστολή διαφημιστικών μηνυμάτων. Παράλληλα, η εμφάνιση στην ιστοσελίδα συμπληρωμένων τετραγωνιδίων δεν θεωρείται σύμφωνη με τις διατάξεις και συνεπώς, πρέπει οι εταιρίες να παρουσιάζουν τα τετραγωνίδια σαν κενά προς συμπλήρωση. Οι σκοποί της διαφήμισης πρέπει να αναφέροντα ρητά, με την έννοια ότι πρέπει να αναφέρεται ρητά το είδος των υπηρεσιών και των εμπορευμάτων που προσφέρονται στον χρήστη[147].

Η συγκατάθεση του χρήστη χρειάζεται και για την χρησιμοποίηση της διεύθυνσης επαφής του από τρίτα μέρη και ύστερα, πρέπει να αναφέρονται ρητά το είδος των υπηρεσιών και των εμπορευμάτων που προσφέρονται στον χρήστη από τα τρίτα μέρη, τα οποία ενδιαφέρονται να επικοινωνήσουν μέσω διαφημιστικών μηνυμάτων. Η κύρια αρχή της προηγούμενης συγκατάθεσης (opt in) ως βασικός λόγος νομιμοποίησης της εμπορικής προώθησης προϊόντων προβλέπεται και στον ελληνικό νόμο σχετικά με τις ενέργειες εμπορικής προώθησης[148]. Επιπλέον, η ξεκάθαρη συγκατάθεση ως θεμελιώδης κανόνας της επεξεργασίας των δεδομένων του υποκειμένου της επεξεργασίας αναφέρεται ξεκάθαρα και στο άρθρο 11 του νόμου 3471/06. Στο αναφερόμενο νομοθέτημα πραγματοποιείται αναφορά στις προϋποθέσεις της νόμιμης συλλογής και χρήσης στο πλαίσιο εμπορικής συναλλαγής των ηλεκτρονικών σημείων επαφής ενός χρήστη/συνδρομητή. Αξίζει σε αυτό το σημείο να αναφερθεί ότι η αιτιολογική έκθεση του 3471/06 τονίζει ότι τα ηλεκτρονικά σημεία επαφής, εκτός από τα μηνύματα του ηλεκτρονικού ταχυδρομείου, είναι και τα SMS και τα MMS αλλά και αντίστοιχης λειτουργίας μηνύματα[149].

3.3 Πρόσφατο νομικό πλαίσιο σχετικά με την ασφάλεια των ηλεκτρονικών επικοινωνιών και ΑΔΑΕ

Εφόσον έχει ήδη γίνει εκτενής αναφορά και συζήτηση για το αρχικό νομικό πλαίσιο για τις ηλεκτρονικές συναλλαγές που αποτελεί ουσιαστικά και τη βάση για τους επόμενους Ελληνικούς νόμους που ακολούθησαν, αξίζει να γίνει αναφορά και στους πρόσφατους νόμους που διέπουν την ασφάλεια των ηλεκτρονικών επικοινωνιών και των προσωπικών δεδομένων σε αυτές.

[147] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[148] Άρθρο 11 παρ. 1 Νόμος 3471/2006
[149] Αιτιολογική Έκθεση του άρθρου 4 Νόμος 3471/.2006

3.3.1 Νόμος 3674/2008

Με το νόμο 3674/2008 για την *«Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου των επικοινωνιών»*[150] η πολιτεία προσπάθησε να απαντήσει στα φαινόμενα εκτεταμένων υποκλοπών[151], όταν άγνωστοι εισήλθαν στα συστήματα λογισμικού του παρόχου και ενεργοποίησαν τα συστήματα συνακροάσεων, τα οποία λειτουργούν στην πλατφόρμα του λογισμικού του.

Το εν λόγω νέο νομοθετικό πλαίσιο[152] ρυθμίζει τα ζητήματα ασφάλειας των επικοινωνιών, καθορίζοντας ρητά δικαιώματα και υποχρεώσεις, οι οποίες συνάγονταν ερμηνευτικά από το προϋφιστάμενο δίκαιο[153]. Ο 3674/2008 εισάγει ουσιαστικά ένα σύστημα όπου από τη μία μεριά βρίσκεται ο πάροχος των υπηρεσιών ηλεκτρονικών υπηρεσιών που είναι υπεύθυνος για τη διασφάλιση του απορρήτου με τη λήψη των απαραίτητων τεχνικών και οργανωτικών μέτρων[154] και από την άλλη η ΑΔΑΕ[155], η οποία ορίζεται ως η Αρχή που αναλαμβάνει τον έλεγχο ασφαλείας των συστημάτων του παρόχου και του υπευθύνου ασφαλείας διασφάλισης του απορρήτου[156]. Συγκεκριμένα, ο πάροχος έχει την ευθύνη για την ασφάλεια των υπό την εποπτεία του χώρων, εγκαταστάσεων, συνδέσεων και των συστημάτων υλικού και λογισμικού. Όπως γίνεται αντιληπτό, το αποτέλεσμα αυτής της ευθύνης είναι η υποχρέωση να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα και να χρησιμοποιεί συστήματα υλικού και λογισμικού, τα οποία και θα διασφαλίζουν το απόρρητο της επικοινωνίας και θα επιτρέπουν την αποκάλυψη της παραβίασης ή απόπειρας παραβίασης του απορρήτου της επικοινωνίας[157].

Συν τοις άλλοις, υπάρχει η πρόβλεψη για την υποχρέωση του παρόχου να καταρτίζει και να εφαρμόζει ειδικό σχέδιο πολιτικής ασφάλειας ως προς τα μέσα, τις μεθόδους και τα μέτρα που

[150] Νόμος 3478/2008
[151] Αιτιολογική Έκθεση του ν. 3674/2008
[152] Αλεξανδροπούλου - Αιγυπτιάδου Ε., 2008, «Νομική διασφάλιση του απορρήτου των κινητών επικοινωνιών (Η ελληνική νομική ρύθμιση ενόψει και του Ν.3674/2008)», ΔιΜΕΕ 2008
[153] Τσόλιας Γ., 2008, «Η ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας σύμφωνα με το Ν. 3674/2008», ΔιΜΕΕ 2008
[154] Άρθρα 2, 3 του Ν. 3674/2008
[155] Οι αρμοδιότητες και η δομή της ΑΔΑΕ αναλύονται παρακάτω σε μεγαλύτερη λεπτομέρεια
[156] Άρθρα 3,4,5,6,7και 8 του Ν. 3674/2008
[157] Άρθρο 2 του Ν. 3674/2008

διασφαλίζουν το απόρρητο της επικοινωνίας[158], σχέδιο το οποίο οφείλει να ανατίθεται σε εξουσιοδοτούμενο στέλεχος, το οποίο ορίζεται ως υπεύθυνος διασφάλισης του απορρήτου[159]. Επιπροσθέτως, υπάρχει η υποχρέωση ενημέρωσης σε περίπτωση παραβίασης του απορρήτου ή ιδιαίτερου κινδύνου παραβίασης του απορρήτου της επικοινωνίας, όπου ο υπεύθυνος διασφάλισης του απορρήτου υποχρεούται να ενημερώνει αμελλητί τον πάροχο, την εισαγγελική αρχή, την ΑΔΑΕ και τους κατά περίπτωση θιγόμενους συνδρομητές, εγγράφως και σε περίπτωση αδυναμίας άμεσης επικοινωνίας με οποιοδήποτε άλλο πρόσφορο μέσο[160].

Ουσιαστικά με τον συγκεκριμένο νόμο, αναγνωρίζεται ότι το υπερατομικό έννομο αγαθό της ασφάλειας των επικοινωνιών βρίσκεται σε κίνδυνο κάθε φορά που λαμβάνει χώρα επίθεση στο σύστημα τηλεφωνικών επικοινωνιών (στις εγκαταστάσεις, στα δίκτυα, ή στο λογισμικό του συστήματος). Επί της ουσίας η εν λόγω επίθεση κάνει τις τηλεφωνικές επικοινωνίες ευάλωτες, εν όλω ή εν μέρει, με αποτέλεσμα τελικά να μη μπορεί να ασκείται ακωλύτως η θεμελιώδης ελευθερία που κατοχυρώνεται στο άρθρο 19 του Συντάγματος. Για αυτόν τον λόγο, εισάγεται με το νόμο[161] μία νέα διάταξη στον Ποινικό Κώδικα (το άρθρο 292Α) σύμφωνα με το οποίο, παρέχεται σε αυτήν ποινική προστασία αντίστοιχη σε βαρύτητα προς εκείνη που παρέχεται σε άλλα υπερατομικά έννομα αγαθά του 14ου Κεφαλαίου του Ειδικού Μέρους του Ποινικού Κώδικα, δηλαδή στην ασφάλεια των συγκοινωνιών και των κοινωφελών εγκαταστάσεων[162].

Με την εισαγωγή του άρθρου 10 επέρχονται στη βασική ποινική διάταξη του άρθρου 370Α του Ποινικού Κώδικα σημαντικές προσθήκες και βελτιώσεις που επιβάλλονται από διεθνή κανονιστικά κείμενα και έχουν καταστεί αναγκαίες από την πρόοδο της τεχνολογίας. Πιο ειδικά, το θεσπιζόμενο αξιόποινο των προβλεπόμενων στην παρ. 1 πράξεων διευρύνεται προς τις δύο ακόλουθες κατευθύνσεις:

- Αντικειμενικά, ούτως ώστε η πράξη της παγίδευσης ή παρέμβασης να μην αφορά, εφεξής, μόνο συσκευή ή τηλεφωνική σύνδεση αλλά και σύστημα υλικού ή λογισμικού που χρησιμοποιείται για την παροχή υπηρεσιών τηλεφωνίας

[158] Άρθρο 3 παρ. 1 του Ν. 3674/2008
[159] Άρθρο 3 παρ. 2 του Ν. 3674/2008
[160] Άρθρο 8 παρ. 1 του Ν. 3674/2008
[161] Άρθρο 9 του Ν. 3674/2008
[162] Αιτιολογική Έκθεση του ν. 3674/2008

- Το αξιόποινο διευρύνεται υποκειμενικά, διότι ορίζεται ότι είναι δυνατόν ο δράστης να πράττει με σκοπό όχι μόνον ο ίδιος, αλλά και άλλος να πληροφορηθεί ή να μαγνητοφωνήσει ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή τα στοιχεία θέσης και κίνησης της εν λόγω επικοινωνίας[163].

Πέρα από τις ανωτέρω όμως, αξίζει να τονιστεί ότι υπάρχουν και οι διοικητικές κυρώσεις[164] στον πάροχο υπηρεσιών τηλεφωνίας σε περίπτωση παραβάσεως από τα όργανά του ή το προσωπικό του των συγκεκριμένων υποχρεώσεων και τις οποίες ορίζει η ΑΔΑΕ, ενώ προβλέπεται και η αστική ευθύνη[165] εκείνου που κατά παράβαση του νόμου προκαλεί σε άλλον περιουσιακή ζημία ή ηθική βλάβη που είναι γνήσια αντικειμενική αδικοπρακτική ευθύνη, αφού για τη θεμελίωσή της δεν ενδιαφέρει η συνδρομή δόλου ή αμέλειας του δράστη[166].

3.3.2 Νόμος 3917/2011[167]

Σύμφωνα με την κοινοτική οδηγία 2002/58/ΕΚ, πριν την αναθεώρηση της από την 2006/24/ΕΚ υπήρχε η πρόβλεψη ότι τα κράτη μέλη θα μπορούσαν να λαμβάνουν νομοθετικά μέτρα για να περιορίζουν το δικαίωμα στο απόρρητο της επικοινωνίας για τη διαφύλαξη της εθνικής άμυνας, τη δημόσια ασφάλεια και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων[168]. Με τη σειρά του λοιπόν ο νόμος 3471/2006 ενσωμάτωσε την οδηγία 2002/58/ΕΚ, αλλά δεν επέβαλε στους παρόχους καμία υποχρέωση προληπτικής διατήρησης δεδομένων της επικοινωνίας. Αυτό είχε σαν αποτέλεσμα τα σχετικά δεδομένα να διατηρούνται από τους παρόχους και να τυγχάνουν επεξεργασίας μόνο για τους σκοπούς μετάδοσης και

[163] Αιτιολογική Έκθεση του ν. 3674/2008
[164] Άρθρο 11 του Ν. 3674/2008
[165] Άρθρο 12 του Ν. 3674/2008
[166] Αιτιολογική Έκθεση του ν. 3674/2008
[167] Νόμος 3917/2011 *«Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»*
[168] Άρθρο 15 παρ.1 Οδηγίας 2001/58/ΕΚ

χρέωσης της επικοινωνίας, ενώ υπήρχε η υποχρέωση να καταστρέφονται με τη λήξη αυτής και μέχρι το τέλος της περιόδου, εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή του[169].

Η οδηγία 2006/24/ΕΚ τροποποίησε την κοινοτική οδηγία 2002/58/ΕΚ και επομένως, η προαναφερθείσα δυνατότητα των κρατών μελών είναι πλέον υποχρεωτική. Με τη σειρά του ο νόμος 3917/2011 επιβάλλει τη διατήρηση ορισμένων δεδομένων, προκειμένου αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, σύμφωνα με τη διαδικασία, τις προϋποθέσεις και τους όρους πρόσβασης που ορίζονται στο Ελληνικό Σύνταγμα[170] Με τις διατάξεις του πρώτου κεφαλαίου του 3917/2011 ενσωματώνονται στην εθνική έννομη τάξη οι διατάξεις της οδηγίας 2006/24/ΕΚ, η οποία αποσκοπεί στην εναρμόνιση των διατάξεων των κρατών μελών, ώστε να διατηρούνται για ορισμένο διάστημα δεδομένα που παράγονται ή τυγχάνουν επεξεργασίας από τους παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων, με σκοπό τη διακρίβωση, διερεύνηση και δίωξη σοβαρών εγκλημάτων[171].

Συν τοις άλλοις, στο πρώτο άρθρο ορίζεται το βασικό αντικείμενο και το πεδίο εφαρμογής του πρώτου κεφαλαίου με το οποίο οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούνται να διατηρούν τα δεδομένα του άρθρου 5 που παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς, προκειμένου τα δεδομένα αυτά να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων, όπως αυτά ορίζονται στο άρθρο 4 του 2225/1994 (ΦΕΚ 121 Α΄)[172]. Πέραν των ανωτέρω, καθορίζεται ότι οι διατάξεις σχετικά με τη διατήρηση των δεδομένων εφαρμόζονται σε δεδομένα κίνησης ή θέσης, καθώς και σε δεδομένα αναγνώρισης του συνδρομητή ή του εγγεγραμμένου χρήστη, οποιουδήποτε φυσικού ή νομικού προσώπου και όχι στο περιεχόμενο των ηλεκτρονικών επικοινωνιών, καθώς

[169] Άρθρο 6 παρ. 2 ν 3471/2006
[170] Κατά το άρθρο 19 παρ. 1. του Συντάγματος
[171] Η επεξεργασία των στοιχείων αυτών από τις αρμόδιες αρχές αποτελεί εργαλείο στη μάχη κατά της τρομοκρατίας και της οργανωμένης εγκληματικότητας
[172] όπως αναφέρεται στο άρθρο 4 του ν.2225/1994

και στις πληροφορίες, στις οποίες η πρόσβαση πραγματοποιείται με τη χρήση δικτύου ηλεκτρονικών επικοινωνιών[173].

Όσο αφορά τις υποχρεώσεις παρόχων ως προς τη διατήρηση των δεδομένων[174] με το άρθρο 3 (παρ. 1 και 2) εισάγεται εξαίρεση στην αρχική απαγόρευση διατήρησης δεδομένων που απορρέει από τις διατάξεις του 3471/2006 και θεμελιώνεται η υποχρέωση των παρόχων για την διατήρηση των δεδομένων του άρθρου 5, ακόμα και των ανεπιτυχών κλήσεων, όταν αυτά παράγονται ή υποβάλλονται σε επεξεργασία από αυτούς κατά την παροχή των υπηρεσιών επικοινωνιών και επαναλαμβάνεται ρητώς η απαγόρευση διατήρησης δεδομένων που αποκαλύπτουν το περιεχόμενο της επικοινωνίας. Με τις συγκεκριμένες διατάξεις του άρθρου 5 καθορίζονται και οι κατηγορίες δεδομένων[175], τα οποία υποχρεούνται να διατηρούν οι πάροχοι και συγκεκριμένα:

1) Δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας

2) Δεδομένα αναγκαία για τον προσδιορισμό του προορισμού της επικοινωνίας[176]

3) Δεδομένα αναγκαία για τον προσδιορισμό της ημερομηνίας, ώρας και διάρκειας της επικοινωνίας

4) Δεδομένα αναγκαία για τον προσδιορισμό του είδους της επικοινωνίας[177]

5) Δεδομένα αναγκαία για τον προσδιορισμό του εξοπλισμού επικοινωνίας των χρηστών ή του φερομένου ως εξοπλισμού επικοινωνίας τους[178]

---

[173] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011

[174] Άρθρα 3 και 5 παρ. 2 της Οδηγίας 2006/24/ΕΚ

[175] Άρθρο 5 της Οδηγίας 2006/24/ΕΚ

[176] Όπως ο καλούμενος αριθμός ή αριθμοί (ο αριθμός ή οι αριθμοί τηλεφώνου που κλήθηκαν, τα ονοματεπώνυμα και οι διευθύνσεις των συνδρομητών ή εγγεγραμμένων χρηστών· και όσον αφορά τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω διαδικτύου, το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη και ο κωδικός ταυτότητας χρήστη του παραλήπτη της επικοινωνίας και ο κωδικός ταυτότητας χρήστη ή ο αριθμός τηλεφώνου του παραλήπτη διαδικτυακής τηλεφωνικής κλήσης·

[177] Όπως η χρησιμοποιηθείσα τηλεφωνική και διαδικτυακή υπηρεσία

[178] Όπως οι τηλεφωνικοί αριθμοί καλούντος και καλουμένου· όσον αφορά την κινητή τηλεφωνία: οι τηλεφωνικοί αριθμοί καλούντος και καλουμένου, η διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI) του καλούντος,η διεθνής ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI) του καλούντος,η IMSI του καλουμένου,η IMEI του καλουμένου

6) Δεδομένα αναγκαία για τον προσδιορισμό της θέσης του εξοπλισμού κινητής επικοινωνίας

Σύμφωνα με την αρχή της αναλογικότητας, το άρθρο 6 του νόμου 3917/2011, ορίζει ότι τα δεδομένα του άρθρου 5 παράγονται και αποθηκεύονται σε φυσικά μέσα, τα οποία βρίσκονται μέσα στα όρια της Ελληνικής Επικράτειας, προκειμένου να είναι ευχερής, άμεσος και αποτελεσματικός ο έλεγχος των αρμόδιων Αρχών για την ασφάλεια των δεδομένων εντός της οποίας και διατηρούνται για τους σκοπούς του νόμου[179]. Επιπροσθέτως, ως χρόνος διατήρησης ορίζεται το χρονικό διάστημα των δώδεκα μηνών από την ημερομηνία της επικοινωνίας, σύμφωνα με τις προϋποθέσεις που ορίζονται στα άρθρα 7 και 8 ενώ με την πάροδο του 12ου μήνα[180] τα δεδομένα πρέπει να καταστρέφονται με αυτοματοποιημένη διαδικασία από τον πάροχο[181]. Ειδικότερα, σχετικά με τα δεδομένα που διατηρούνται από τον πάροχο και για τα οποία ήρθη το απόρρητο για τη διακρίβωση ιδιαιτέρως σοβαρών εγκλημάτων καταστρέφονται ύστερα από γνωστοποίηση της σχετικής διάταξης της αρμόδιας αρχής, όταν παύσουν οι λόγοι για τους οποίους διατάχθηκε η πρόσβαση σ' αυτά[182].

Ακόμη , αξίζει να γίνει αναφορά στην πρώτη παράγραφο του άρθρου 7 του 3917/2011, όπως και στην οδηγία 2006/24/ΕΚ σχετικά με τις πρόσθετες ειδικές υποχρεώσεις στους παρόχους για την αποτελεσματική διαφύλαξη των δεδομένων που διατηρούν επί δώδεκα μήνες, όπως ότι:

α) τα διατηρούμενα δεδομένα πρέπει να είναι ίδιας ποιότητας και να έχουν την ίδια προστασία και ασφάλεια με τα δεδομένα που περιέχει το δίκτυο

β) θα πρέπει να λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων κατά τυχαίας ή παράνομης καταστροφής τους ή τυχαίας απώλειας, αλλοίωσης, μη εξουσιοδοτημένης ή παράνομης αποθήκευσης, επεξεργασίας, πρόσβασης ή αποκάλυψης

[179] Άρθρο 6 και 7 στοιχείο δ΄ της οδηγίας 2006/24/ΕΚ
[180] αιτιολογική έκθεση του νόμου 3917/2011
[181] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[182] Άρθρο 7 στοιχ. δ) της Οδηγίας 2006/24/ΕΚ

γ) υπάρχουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλισθεί ότι στα δεδομένα έχει πρόσβαση μόνον ειδικά εξουσιοδοτημένο προσωπικό[183].

Συν τοις άλλοις, με την παράγραφο 2 επιβάλλεται η υποχρέωση στους παρόχους να καταρτίζουν (σε εναρμόνιση με τα προβλεπόμενα στο άρθρο 3 του 3674/2008) ειδικό σχέδιο ασφάλειας για τα δεδομένα που διατηρούν.

Πέρα από τα ανωτέρω, υπάρχει και η πρόβλεψη ότι με κοινή πράξη τους[184], η Α.Δ.Α.Ε. και η Α.Π.Δ.Π.Χ. θα καθορίσουν κάθε θέμα σχετικό με τη διαδικασία και τον τρόπο εφαρμογής των διατάξεων του άρθρου 7 του 3917/2011. Σε συνέχεια του άρθρου 7, με το άρθρο 9 ορίζεται ότι η Α.Δ.Α.Ε. έχει τις αρμοδιότητες που προβλέπονται στο νόμο 3115/2003, καθώς τα διατηρούμενα δεδομένα του άρθρου 5, μαζί με το περιεχόμενο της επικοινωνίας, συνθέτουν, υπό ευρεία έννοια, την έννοια του απορρήτου της επικοινωνίας και η Α.Π.Δ.Π.Χ. έχει τις αρμοδιότητες, όπως αυτές προβλέπονται στο 2472/1997, διότι αυτά τα δεδομένα είναι και προσωπικά δεδομένα υπό την έννοια τόσο του 2472/1997, όσο και του 3471/2006. Σχετικά με την προστασία του χρήστη των ηλεκτρονικών επικοινωνιών[185] προβλέπονται οι ποινικές κυρώσεις για τα πρόσωπα, τα οποία κατά παράβαση των διατάξεων του πρώτου κεφαλαίου του 3917/2011 επεμβαίνουν στα διατηρούμενα δεδομένα με οποιονδήποτε τρόπο[186]. Όπως μπορεί να γίνει αντιληπτό, με την πρώτη και τη δεύτερη παράγραφο του άρθρου 11 διευρύνεται το αξιόποινο ως προς τον κύκλο των δραστών, επιδιώκεται η διασφάλιση της αυθεντικότητας των διατηρούμενων δεδομένων, αλλά και η προστασία των προσώπων από κακόβουλες επεμβάσεις, όπως και παράνομη χρήση των διατηρούμενων στοιχείων επικοινωνίας[187].

Σχετικά με τις διοικητικές κυρώσεις[188] του άρθρου 12 του υπό εξέταση νόμου 3917/2011[189], αυτές επιβάλλονται κάθε φορά που παραβιάζεται υποχρέωση που προβλέπεται στον 3917/2011 ή στις κανονιστικές πράξεις που εκδίδονται κατ' εξουσιοδότηση των διατάξεων του νόμου

[183] Άρθρο 7 παρ 1 νόμος 3917/2011
[184] Νόμος 3471/2006, άρθρο 13 παρ. ε
[185] Άρθρο 13 της οδηγίας 2006/24/ΕΚ
[186] Νόμος 3917/2011, άρθρο 11 παρ. α
[187] Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
[188] 1) Σύσταση για συμμόρφωση μέσα στα χρονικά όρια της τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης·2) πρόστιμο από 20.000 έως 5.000.000 ευρώ 3) οριστική ανάκληση του δικαιώματος παροχής υπηρεσιών
[189] Βλέπε άρθρο 13 της Ευρωπαϊκής οδηγίας 2006/24/ΕΚ

3917/2011 από τον νόμιμο εκπρόσωπο ή κάποιο μέλος της διοίκησης, τον υπεύθυνο ασφάλειας δεδομένων, κάποιον εργαζόμενο ή συνεργάτη του παρόχου, ανάλογα με τη βαρύτητα της παράβασης και αναλόγως με εάν συντρέχει περίπτωση υποτροπής[190]. Επιπροσθέτως, σύμφωνα με το άρθρο 12 παρ.3 του υπό συζήτηση νόμου, οι αποφάσεις με τις οποίες επιβάλλονται κυρώσεις υπόκεινται σε ουσιαστική προσφυγή ενώπιον του Διοικητικού Εφετείου Αθηνών, κατά των αποφάσεων δε του δικαστηρίου αυτού προβλέπεται αίτηση αναιρέσεως ενώπιον του Συμβουλίου της Επικρατείας, σύμφωνα με τις κείμενες διατάξεις. Τέλος, σχετικά με την αστική ευθύνη του υπόχρεου που δρα είτε ως νομικό είτε ως φυσικό πρόσωπο και κατά παράβαση των διατάξεων του 3917/2011 προκαλεί σε άλλον περιουσιακή ζημία ή ηθική βλάβη, αυτή συνίσταται σε πλήρη αποζημίωση ή χρηματική ικανοποίηση[191].

Θα πρέπει βέβαια στο σημείο αυτό να τονιστεί ότι μετά την ακύρωση της οδηγίας 2006/24/ΕΚ από το Δικαστήριο της Ευρωπαϊκής Ένωσης τίθεται το ζήτημα ισχύος του ν.3917/2011, άρα και των σχετικών υποχρεώσεων των παρόχων.

3.3.3 Νόμος 4070/2012

Ο νόμος του 2012 με τίτλο *«Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις»*[192], ουσιαστικά θεσπίστηκε για να καλύψει ορισμένα κενά στις ηλεκτρονικές επικοινωνίες, αλλά και να ενσωματώσει ορισμένες κοινοτικές οδηγίες. Συγκεκριμένα, με τον 4070/2012 ενσωματώνονται στο Ελληνικό νομοθετικό πλαίσιο οι Ευρωπαϊκές οδηγίες 2002/19/ΕΚ, 2002/20/ΕΚ, 2002/21/ΕΚ, 2002/22/ΕΚ και 2002/77/ΕΚ όπως τροποποιήθηκαν σύμφωνα με τις Οδηγίες 2009/136/ΕΚ και 2009/140/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[193]. Συν τοις άλλοις, ο εν λόγω νόμος αναφέρεται και σε συγκεκριμένα θέματα για τις αρμοδιότητες του Υπουργείου Μεταφορών σχετικά με τις ηλεκτρονικές επικοινωνίες[194]. Ένα ακόμα σημαντικό σημείο του εν λόγω νόμου είναι το άρθρο 20 σχετικά με τη διαχείριση του ραδιοφάσματος. Συγκεκριμένα, ο 4070/2012 εναρμονίζει το

[190] Εισηγητική Έκθεση νόμου 3917/2011
[191] Εισηγητική Έκθεση του νόμου 3917/2011
[192] Νόμος 4070/2012
[193] Νόμος 4070/2012, άρθρο 1 παρ. 1
[194] Νόμος 4070/2012, άρθρο 4

Ελληνικό νομοθετικό πλαίσιο με το Ευρωπαϊκό σχετικά με την εναρμόνιση του ραδιοφάσματος σε ολόκληρη την Ευρωπαϊκή Ένωση[195].

Στη συνέχεια ο 4070/2012 προχωράει και στην αναλυτική αναφορά σχετικά με την χορήγηση δικαιωμάτων χρήσης συχνοτήτων[196], αλλά και τη μεταβίβαση τους[197] μέσω της υιοθέτησης της κοινοτικής απόφασης 676/2002/ΕΚ. Ο συγκεκριμένος νόμος αναφέρεται επίσης και σε ένα ακόμα ζήτημα που δεν υπήρχε στους προηγούμενους, τη διαχείριση δορυφορικών τροχιών και συσχετισμένων συχνοτήτων[198]. Σε γενικές γραμμές μπορεί να υποστηριχθεί ότι ο εν λόγω νόμος δημιουργήθηκε για την υιοθέτηση ορισμένων Ευρωπαϊκών οδηγιών στο Ελληνικό νομοθετικό πλαίσιο.

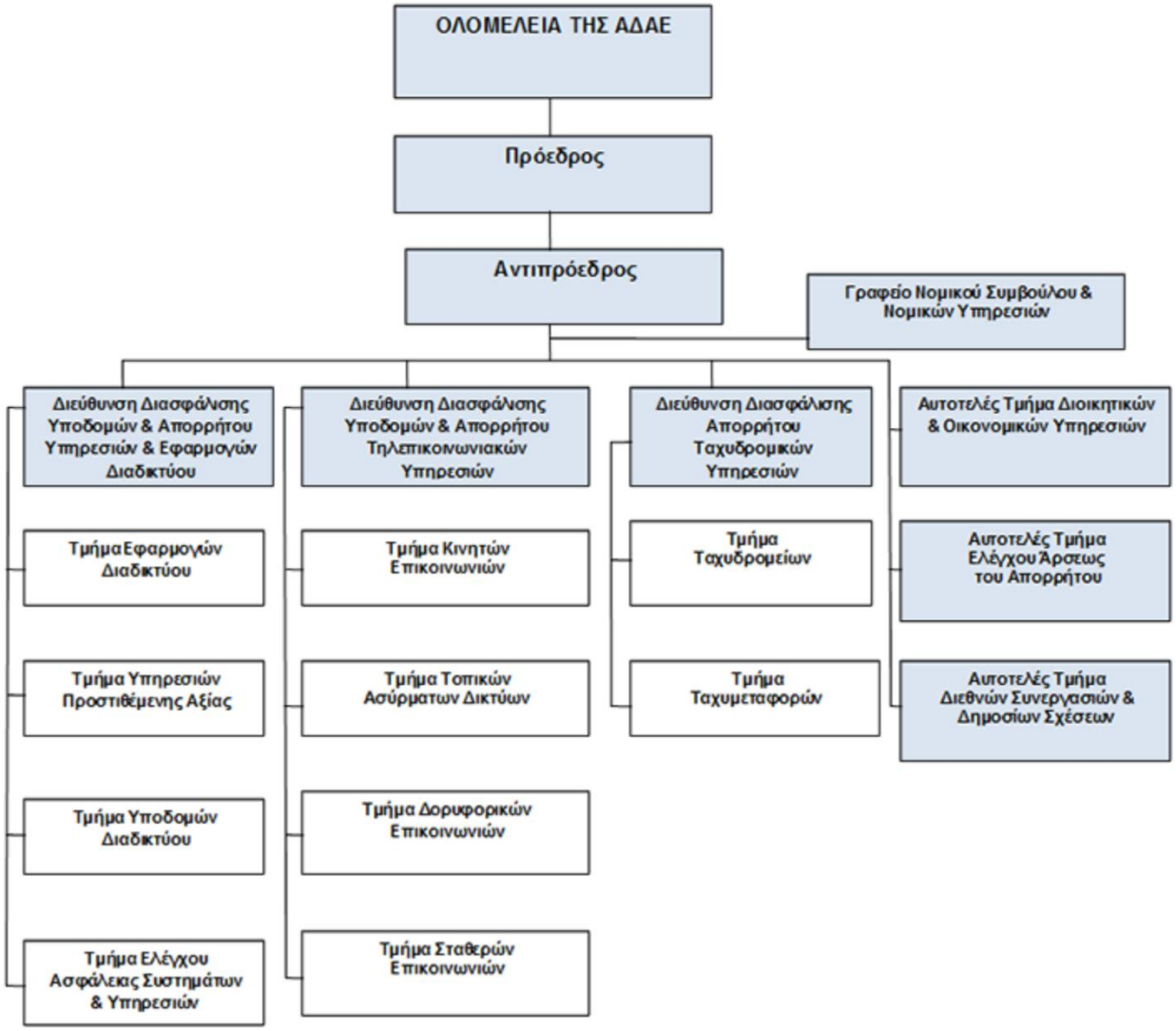
3.3.4 Γενικά στοιχεία για ΑΔΑΕ

Πέρα από τις λεπτομέρειες του νομοθετικού πλαισίου, αξίζει να γίνει μία σύντομη αναφορά στην ΑΔΑΕ, την Αρχή που έχει ως σκοπό την προστασία του απορρήτου επικοινωνιών. Συγκεκριμένα, η εν λόγω Αρχή συστάθηκε με το νόμο 3115/2003 άρθρο 1 και σύμφωνα με την παράγραφο 2 του άρθρου 19 του Συντάγματος και αποσκοπεί στο να προστατεύει το απόρρητο «των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο», όπως αναφέρεται χαρακτηριστικά και στην ιστοσελίδα της ΑΔΑΕ. Επιπροσθέτως, χρειάζεται να αναφερθεί ότι η ΑΔΑΕ είναι ανεξάρτητη με διοικητική αυτοτέλεια και με έδρα την πρωτεύουσα της Ελλάδας την Αθήνα παρόλο που έχει τη δυνατότητα να διατηρεί γραφεία και σε άλλα μέρη της χώρας. Η ΑΔΑΕ έχει την υποχρέωση να γνωστοποιεί τα πεπραγμένα της στο Προεδρείο της Βουλής, στον Υπουργό Δικαιοσύνης, μέσω του οποίου κοινοποιούνται οι αποφάσεις της ΑΔΑΕ, στα υπόλοιπα κόμματα της Βουλής των Ελλήνων αλλά και τέλος στο Ευρωπαϊκό Κοινοβούλιο. Συν τοις

[195] Νόμος 4070/2012, άρθρο 20
[196] Νόμος 4070/2012, άρθρο 21
[197] Νόμος 4070/2012, άρθρο 25
[198] Νόμος 4070/2012, άρθρο 31

άλλοις, αξίζει να σημειωθεί ότι η εν λόγω ανεξάρτητη Αρχή ελέγχεται κοινοβουλευτικά και σύμφωνα με τον εκάστοτε κανονισμό της Βουλής των Ελλήνων και η δομή της είναι όπως φαίνεται και στην παρακάτω εικόνα από την ιστοσελίδα της.

Σχεδιάγραμμα 5: Δομή ΑΔΑΕ



Πηγή: www.adae.gr

Πέρα από τα ανωτέρω, η ΑΔΑΕ έχει συγκεκριμένα τις παρακάτω αρμοδιότητες:

1. Έγκριση του ειδικού σχεδίου πολιτικής ασφάλειας και κάθε αναθεώρηση του[199]

2. Τοποθέτηση του υπευθύνου διασφάλισης του απορρήτου, ενώ υπάρχει η δυνατότητα να ζητήσει οποτεδήποτε, αυτεπαγγέλτως ή ύστερα από αίτημα της ΑΠΔΠΧ ή της ΕΕΤΤ ή άλλης

[199] Άρθρο 3 παρ 2 Ν. 3674/2008

δημόσιας αρχής, την αντικατάσταση του υπευθύνου διασφάλισης του απορρήτου εφόσον υπάρχει αιτιολογημένη απόφαση[200]

3. Δέχεται την γνωστοποίηση από τον πάροχο των μεθόδων κρυπτογράφησης[201]

4. Διεξαγωγή τακτικών και έκτακτων ελέγχων της υποδομής των συστημάτων υλικού και λογισμικού που βρίσκονται υπό την εποπτεία του παρόχου, για την τήρηση των διατάξεων της κείμενης νομοθεσίας για την προστασία του απορρήτου της επικοινωνίας[202]

5. Στις πρώτες δέκα ημέρες κάθε τετράμηνου ο Πρόεδρος της ΑΔΑΕ λαμβάνει δήλωση από τον πάροχο ή τον νόμιμο εκπρόσωπο αυτού και τον υπεύθυνο διασφάλισης του απορρήτου, στην οποία αναφέρονται οι διατάξεις και τα βουλεύματα για την άρση του απορρήτου, καθώς και οι Αρχές που είχαν υποβάλει το εν λόγω αίτημα[203]

6. Ο υπεύθυνος ασφαλείας υποχρεώνεται να ενημερώνει την ΑΔΑΕ άμεσα, εφόσον υπάρχει περίπτωση παραβίασης του απορρήτου ή ιδιαίτερου κινδύνου παραβίασης του απορρήτου της επικοινωνίας

7. Επιβολή των κυρώσεων του άρθρου 11με απόφαση της ύστερα από προηγούμενη κλήση του ενδιαφερομένου για παροχή εξηγήσεων[204].

[200] Άρθρο 3 παρ 2 Ν. 3674/2008
[201] Άρθρο 5 παρ 2 Ν. 3674/2008
[202] Άρθρο 6 παρ 1 Ν. 3674/2008
[203] Άρθρο 7 Ν. 3674/2008
[204] Άρθρο 11 Ν. 3674/2008

ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως έγινε αντιληπτό από την εν λόγω εργασία, τα τελευταία χρόνια γίνεται προσπάθεια σε παγκόσμιο επίπεδο για την προστασία των προσωπικών δεδομένων λόγω της αλματώδους εξέλιξης της τεχνολογίας των πληροφοριών. Το νομικό πλαίσιο τόσο σε εθνικό, όσο και σε διεθνές επίπεδο, δείχνει την προσπάθεια προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής ως ανθρωπίνων δικαιωμάτων και την αναγωγή τους σε συνταγματικά προστατευμένα αγαθά. Η έννοια της ιδιωτικής ζωής όμως, έχει αλλάξει σημαντικά τις τελευταίες δεκαετίες και ειδικά από την εισαγωγή του διαδικτύου που είχε ως άμεσο αποτέλεσμα την παγκοσμιοποιημένη κοινωνία. Πλέον, κάθε άτομο που δραστηριοποιείται στο Διαδίκτυο παρέχει καθημερινά προσωπικές πληροφορίες είτε χρησιμοποιώντας κυβερνητικές υπηρεσίες είτε σε φιλικές και συγγενικές συναναστροφές. Στις μέρες μας, είναι ξεκάθαρο ότι τα άτομα επιθυμούν και επιτρέπουν να μοιράζονται τις πληροφορίες που τα αφορούν με πολύ μεγαλύτερη ευκολία συγκριτικά με το παρελθόν.

Όσον αφορά την προστασία των προσωπικών δεδομένων, η επικαιροποίηση του νομοθετικού πλαισίου, ώστε να μπορεί να ακολουθεί τις ανάγκες των ατόμων και την πραγματικότητα, είναι πλέον επιτακτική. Προς την κατεύθυνση αυτή, έχει αρχίσει να εφαρμόζεται από τις 25/5/2018 ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679(GDPR) σε ευρωπαϊκό πλαίσιο. Ωστόσο, στη χώρα μας μετά την ανασύσταση της νομοπαρασκευαστικής Επιτροπής, δεν έχει κατατεθεί ακόμη στη βουλή το σχετικό νομοσχέδιο. Μένει λοιπόν, να φανεί στην πράξη η δυνατότητα της Ελλάδας να συμμορφωθεί στις ανάγκες του νέου κανονισμού.

Εστιάζοντας στον τομέα των ηλεκτρονικών επικοινωνιών, χρειάζεται να σημειωθεί η παραδοχή ότι τα τελευταία χρόνια τόσο σε Ευρωπαϊκό επίπεδο, όσο και σε εθνικό έχουν γίνει σημαντικές προσπάθειες για τη βελτίωση του νομοθετικού πλαισίου σχετικά με την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες. Ωστόσο, το μέλλον και η πρακτική εφαρμογή του κανονιστικού πλαισίου θα δείξει το βαθμό επιτυχίας του προς την κατεύθυνση της διασφάλισης του απορρήτου των ηλεκτρονικών επικοινωνιών και των προσωπικών δεδομένων σε αυτές. Πρέπει να σημειωθεί τέλος, ότι η ενίσχυση της προστασίας των προσωπικών

δεδομένων στις ηλεκτρονικές επικοινωνίες αναμένεται με την ψήφιση του σχετικού κανονισμού που θα αντικαταστήσει την Οδηγία 2002/58/ΕΚ[205].

Καταλήγοντας, το συμπέρασμα της παρούσας ανάλυσης είναι ότι οι νέες τεχνολογίες έχουν φέρει στην επιφάνεια την ανάγκη ύπαρξης ισχυρού νομικού πλαισίου για την προστασία του απορρήτου των προσωπικών δεδομένων τόσο σε εθνικό αλλά κυρίως σε Ευρωπαϊκό επίπεδο. Παρόλο που η Ευρωπαϊκή Ένωση έχει ήδη θεσπίσει σημαντικές νομοθετικές πρωτοβουλίες, εν τούτοις η σημερινή κοινωνία και τεχνολογία κινούνται με ταχύτατους ρυθμούς και αυτό το γεγονός οδηγεί σε πιθανά κενά στο νομοθετικό πλαίσιο των χωρών μελών της Ε.Ε.

[205] Βλέπε: Proposal for e-privacy regulation, διαθέσιμο στο *https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation*

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική

- Αλεξανδροπούλου- Αιγυπτιάδου Ε, «Προσωπικά Δεδομένα», Νομική Βιβλιοθήκη, 2016
- Αλεξανδροπούλου-Αιγυπτιάδου Ε. «Νομική διασφάλιση του απορρήτου των κινητών επικοινωνιών», ΔiΜΕΕ, 2008, σελ.446 επ.
- Αλεξανδροπούλου-Αιγυπτιάδου Ε. «Προσωπικά Δεδομένα», Εκδ. Αντ. Σάκκουλα Αθήνα –Κομοτηνή 2007
- Γεράρης Χ. «Τα προσωπικά δεδομένα και οι νέες προκλήσεις», ΔiΜΕΕ, 2010, σελ. 42 επ.
- Γέροντας Α. « Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων», Εκδ. Αντ. Σάκκουλα, Αθήνα 2002
- Γεωργιάδης Γ. «Η σύναψη συμβάσεως μέσω διαδικτύου», Εκδ. Αντ. Σάκκουλα, Αθήνα – Κομοτηνή 2003
- Καράκωστας Ι. «Προστασία της Ιδιωτικότητας στην κοινωνία της πληροφορίας», ΔιΜΕΕ, 2004 σελ.55 επ.
- Κίτσος Π. «Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011
- Λουκέρης Γ. « Εναρμόνιση της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα στην Ευρωπαική Ένωση», ΝοΒ, 1997, σελ. 547επ.
- Ματθίας Σ. « Εισαγωγή στη σύμβαση για τα δικαιώματα του ανθρώπου» ΕλλΔνη, 1999, σελ. 729 επ
- Μαυρίδης Ι. «Ασφάλεια Πληροφοριών στο Διαδίκτυο», σελ. 21, ΣΕΑΒ, 2015
- Μήτρου Λ. «Το δίκαιο στην Κοινωνία της Πληροφορίας», Σειρά : Δίκαιο Και Κοινωνία στον 21ο αιώνα, Εκδ. Σάκκουλα, Αθήνα –Θεσσαλονίκη 2002, σελ.16 επ.
- Μπακόπουλος Ι. «Ανθρώπινα Δικαιώματα στην Ευρωπαϊκή Έννομη Τάξη», ΕλλΔνη, 2002, σελ. 54
- Περράκης Σ. « Διαστάσεις της διεθνούς προστασίας των δικαιωμάτων του ανθρώπου,» τόμ. Α΄, Εκδ. Σάκκουλα Αθήνα- Κομοτηνή 1991

- Στάγκος Π., Σαχπεκίδου Ε. «Δίκαιο των Ευρωπαικών Κοινοτήτων και της Ευρωπαικής Ένωσης», Εκδ. Σάκκουλα Αθήνα-Θεσσαλονίκη 2000, σελ.197 επ.
- Σωτηρόπουλος Β.,Ταλίδου Ζ. «Η προληπτική διατήρηση των τηλεπικοινωνιακών δεδομένων για σκοπούς καταπολέμησης του εγκλήματος (Οδηγία 2006/24/ΕΚ), ΔiΜΕΕ, 2006, σελ. 181επ.
- Τανταλάκη Ν. «Κίνδυνοι και ασφάλεια στο διαδικτύο- δημιουργία κοινότητας πρακτικής για γονείς και μαθητές», Αριστοτέλειο Πανεπιστήμιο, 2010
- Τσόλιας Γ. «Η ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας σύμφωνα με το Ν. 3674/2008», ΔιΜΕΕ, 2008, σελ. 334 επ.
- Χριστοδούλου Κ. «Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα», Πραγματείες Αστικού Δικαίου, Εκδ. Αντ. Ν. Σάκκουλα Αθήνα-Κομοτηνή 2007

Ξενόγλωσση

- Asscher, Lodewijk F., «Regulating Spam: Directive 2002/58 and Beyond" (http://ssrn.com/abstract=607183)
- Bignami Francesca, «The Case for Tolerant Constitiuonal Patriotism: The right to Privacy Before the European Courts» Cornell International Law Journal, 2008 σελ. 219 επ.
- Bouckaert J., Degryse H. «Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies»,2005, http://weis2006.econinfosec.org/docs/34.pdf
- Bygrave L.«Privacy in a Global Context-A Comparative Overview», Scandinavian Studies in Law, 2004, σελ.319 επ. σε folk.uio.no/lee/publications/ Privacy%20in%20global%20context.pdf
- Nikhil Khandare, Meshram B. B. « Security of Online Electronic Transactions», Mumbai 2013, Veermata JijabaiTechnological Institute
- Tene O. «Privacy The New generations», International Data Privacy Law, 2011, σελ. 15 επ

Ιστοσελίδες

http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

http://www.cidh.org/Basicos/English/Basic3.American%20Convention.html

http://www.achpr.org/english/_info/charter_en.html

http://www1.umn.edu/humanrts/instree/loas2005.html?msource=UNWDEC19001&tr=y&auid=333

www.itlaw.uom.gr

http://www.itkommissionen.se/dynamaster/file_archive/030121/991899fe86e3aecaa92d4e5730148f 50/5.1%20%20Security%20and%20Vulnerability%20-%20S%F6ren%20%D6man.pdf

http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

www.adae.gr

http://europa.eu.int/comm/justice_home/unit/charte/index_en.html

https://eur-lex.europa.eu/legal-content/EL

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_el.pdf

www.cs.helsinki.fi/n/Kraatika/Courses/F4fMC/WS2/Pitkaranta.pdf

https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation