



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Χριστίνας Κακαλή (Α.Μ.: ΜΔΙ 2113)

ΤΑ ΜΕΤΑΔΕΔΟΜΕΝΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΩΣ ΔΙΑΣΤΑΣΗ ΤΟΥ
ΠΡΟΣΤΑΤΕΥΤΕΟΥ ΕΠΙΚΟΙΝΩΝΙΑΚΟΥ ΑΠΟΡΡΗΤΟΥ

Επιβλέπουσα:

Δρ. Αικατερίνα Παπανικολάου

Πειραιάς, Ιούνιος 2023

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ.....	5
ΕΙΣΑΓΩΓΗ.....	5
Α] ΤΑ ΜΕΤΑΔΕΔΟΜΕΝΑ ΕΠΙΚΟΙΝΩΝΙΑΣ (ΕΞΩΤΕΡΙΚΑ ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ)...	6
1. ΕΝΝΟΙΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΟΡΟΥ, ΤΑ ΣΤΟΙΧΕΙΑ ΠΟΥ ΤΑ ΣΥΝΘΕΤΟΥΝ, ΑΝΤΙΠΑΡΑΒΟΛΗ ΠΡΟΣ ΤΑ ΕΣΩΤΕΡΙΚΑ ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ.....	6
1.1 Εννοιολογική Προσέγγιση Μεταδεδομένων Επικοινωνίας.....	7
1.2 Στοιχεία Μεταδεδομένων Επικοινωνίας.....	9
1.3 Σύγκριση με εσωτερικά στοιχεία επικοινωνίας.....	12
2. Η ΙΔΙΑΙΤΕΡΗ ΣΗΜΑΣΙΑ ΠΟΥ ΑΠΟΚΤΟΥΝ ΣΤΗΝ ΨΗΦΙΑΚΑ ΠΡΟΗΓΜΕΝΗ ΚΟΙΝΩΝΙΑ ΚΑΙ Η ΑΝΑΓΚΗ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΧΑΡΑΚΤΗΡΑ ΤΟΥΣ.....	15
2.1 Η σημασία των μεταδεδομένων της επικοινωνίας στην ψηφιακά προηγμένη κοινωνία.....	15
2.1.1 Ορισμός και είδη μεταδεδομένων επικοινωνίας.....	15
2.1.2 Χρήσεις Μεταδεδομένων Επικοινωνίας.....	17
2.1.3 Κοινωνικές, οικονομικές και πολιτικές επιπτώσεις των μεταδεδομένων της επικοινωνίας.....	19
2.2 Η ανάγκη προστασίας του απόρρητου χαρακτήρα των μεταδεδομένων επικοινωνίας.....	21
2.2.1 Κίνδυνοι για το απόρρητο και τις αστικές ελευθερίες.....	21
2.2.2 Τεχνικά μέτρα για την προστασία της ιδιωτικής ζωής.....	22
2.2.3 Νομικά μέτρα για την προστασία της ιδιωτικής ζωής.....	23
2.2.4 Εξισορρόπηση απορρήτου και ασφάλειας.....	24
Β] ΔΙΚΑΙΩΜΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΕ ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ.....	26
1. ΚΑΤΟΧΥΡΩΣΗ ΤΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΗΝ ΕΘΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ- ΕΜΒΕΛΕΙΑ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ: Η ΠΡΟΒΛΗΜΑΤΙΚΗ ΤΩΝ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ.....	26
1.1 Άρθρο 19 Σύνταγμα.....	26
1.1.1 Απαραβίαστο Ιδιωτικότητα και Ελευθερία Επικοινωνίας.....	26
1.1.2 Εξαιρέσεις για την Εθνική Ασφάλεια και τα Σοβαρά Εγκλήματα.....	27
1.1.3 Ανεξάρτητη Αρχή για τη Διασφάλιση του Απορρήτου.....	28
1.1.4 Απαγόρευση αποδεικτικών στοιχείων που αποκτήθηκαν κατά παράβαση του άρθρου 19 και των συναφών άρθρων.....	28
1.2 Νόμος 2225/1994 – Νόμος 5002/2022.....	29

1.2.1 Σκοπός και σημασία της προστασίας του απορρήτου:.....	29
1.2.2 Ευρύ πεδίο προστασίας.....	29
1.2.3 Νομική αναγνώριση των δικαιωμάτων απορρήτου:.....	30
1.2.4 Περιορισμοί στην άρση του απορρήτου:.....	30
1.2.5 Νόμος 5002/2022 – Ορισμένοι Προβληματισμοί.....	31
1.3 Προεδρικό Διάταγμα 47/2005 & Νόμος 3471/2006 (Οδηγία 2002/58/EK).....	36
1.3.1 ΠΔ 47/2005: Προστασία του Απορρήτου των Επικοινωνιών	36
1.3.2 Νόμος 3471/2006: Προστασία των Θεμελιωδών Δικαιωμάτων στις Ηλεκτρονικές Επικοινωνίες- Συσχετισμός με τα δεδομένα προσωπικού χαρακτήρα	36
1.4 Νόμος 3917/2011 (Οδηγία 2006/24/EK)	38
1.5 Συμπερασματικές παρατηρήσεις /θέση της γράφουσας.....	40
2. Η ΕΠΙΧΕΙΡΗΜΑΤΟΛΟΓΙΑ ΠΕΡΙ ΤΗΣ ΥΠΑΓΩΓΗΣ ΤΩΝ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ.....	41
2.1 Γνωμοδότηση ΑΔΑΕ 1/2005	41
2.2 Γνωμοδότηση ΕισΑΠ 6/2008	42
2.3 ΑΠ 1421/2010.....	43
2.4 ΣτΕ 1593/2016	44
2.5 Βούλευμα ΠλημμΑθ 613/2016	45
3. Η ΕΠΙΧΕΙΡΗΜΑΤΟΛΟΓΙΑ ΠΕΡΙ ΤΗΣ ΜΗ ΥΠΑΓΩΓΗΣ ΤΩΝ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ	46
3.1 Γνωμοδοτήσεις ΕισΑΠ 9/2009, 12/2009 & 9/2011	46
3.2 ΑΠ 570/2006.....	48
3.3 ΑΠ 711/2011 & ΑΠ 78/2021	49
Γ] ΔΙΚΑΙΩΜΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΕ ΕΥΡΩΠΑΙΚΟ ΚΑΙ ΔΕΘΝΕΣ ΕΠΙΠΕΔΟ	50
1. ΚΑΤΟΧΥΡΩΣΗ ΤΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΗΝ ΕΝΩΣΙΑΚΗ ΚΑΙ ΔΙΕΘΝΗ ΕΝΝΟΜΗ ΤΑΞΗ- ΣΥΝΤΟΜΗ ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ	50
1.1 Άρθρο 8 Ε.Σ.Δ.Α.....	52
1.2 Άρθρο 7 -Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Χ.Θ.Δ.Ε.Ε.)	53
1.3 Άρθρο 12 -Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα & Άρθρο 17 - Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα	54
1.4 Οδηγία 97/66/EK, Οδηγία 2002/58/EK & Οδηγία 2006/24/EK.....	55
1.5 Κανονισμός e-Privacy.....	59

2. ΝΟΜΟΛΟΓΙΑΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΝΩΣΙΑΚΗΣ ΕΝΝΟΜΗΣ ΤΑΞΗΣ	60
2.1 Αποφάσεις Ε.Δ.Δ.Α.	60
2.1.1 Απόφαση Malone κατά Ηνωμένου Βασιλείου	60
2.1.2 Απόφαση Copland κατά Ηνωμένου Βασιλείου	62
2.1.3 Απόφαση Big Brother Watch κατά Ηνωμένου Βασιλείου	63
2.2 Αποφάσεις του Δ.Ε.Ε.	65
2.2.1 Απόφαση Digital Rights Ireland	65
2.2.2 Απόφαση Tele2 Sverige AB (C-203/2015) κατά Post-och telestyrelsen και Secretary of State for the Home Department (C-698/2015) κατά Tom Watson, Peter Brice, Geoffrey Lewis	67
2.2.3 Απόφαση La Quadrature du Net and Others κατά Premier ministre and Others	67
3. Αποφάσεις Διεθνών Δικαστηρίων	69
Δ. ΣΥΜΠΕΡΑΣΜΑΤΑ	71
ΒΙΒΛΙΟΓΡΑΦΙΑ	72

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική διερευνά τα ζητήματα που τίθενται στην εγχώρια, αλλά και ενωσιακή και διεθνή έννομη τάξη, αναφορικά με την προστασία του επικοινωνιακού απορρήτου και δη των μεταδεδομένων επικοινωνίας ως μέρος του επικοινωνιακού γεγονότος. Μέχρι πριν από κάποιες δεκαετίες ο διάλογος περί του προστατευτέου επικοινωνιακού απορρήτου αφορούσε κυρίως και περιοριζόταν στο καθαυτό περιεχόμενο της επικοινωνίας. Με την τεχνολογική πρόοδο και τη συστηματική επικράτηση των ψηφιακών μέσων στην ζωή των ατόμων γεννήθηκαν νέες προβληματικές και κίνδυνοι για το απόρρητο της επικοινωνίας και κατ'επέκταση για την ιδιωτική ζωή των ατόμων. Μέσα από μια σύντομη επισκόπηση της σχετικής νομοθεσίας και της δικαστηριακής πρακτικής γίνεται προσπάθεια να αναδειχθεί η σημασία που έχουν τα μεταδεδομένα και η ανάγκη για την προστασία του απορρήτου χαρακτήρα τους.

ΕΙΣΑΓΩΓΗ

Στη σημερινή ψηφιακή εποχή, τα μεταδεδομένα επικοινωνίας έχουν αναδειχθεί ως βασικό συστατικό του απορρήτου της επικοινωνίας. Τα μεταδεδομένα επικοινωνίας αναφέρονται στις εξωτερικές πτυχές της επικοινωνίας, συμπεριλαμβανομένων των πληροφοριών σχετικά με τον αποστολέα, τον παραλήπτη, την ημερομηνία, την ώρα, την τοποθεσία και τη διάρκεια της επικοινωνίας. Η συλλογή και η χρήση μεταδεδομένων επικοινωνίας έχουν εγείρει ανησυχίες σχετικά με παραβιάσεις του απορρήτου και την πιθανή κακή χρήση αυτών των σημείων δεδομένων. Οι μελετητές υποστήριξαν ότι τα μεταδεδομένα επικοινωνίας μπορούν να αποκαλύψουν σημαντικές ποσότητες ευαίσθητων πληροφοριών, συμπεριλαμβανομένων πολιτικών απόψεων, προσωπικών σχέσεων και ιατρικών καταστάσεων (Τσιφτόγλου, 2013). Η παρούσα διπλωματική εργασία στοχεύει να παράσχει μια ολοκληρωμένη ανάλυση των μεταδεδομένων της επικοινωνίας ως διάσταση του προστατευτέου απορρήτου της επικοινωνίας, εξετάζοντας τις νομικές προσεγγίσεις εντός της εθνικής, ενωσιακής και διεθνούς έννομης τάξης.

Η πρώτη ενότητα της διπλωματικής εστιάζει στην εννοιολογική προσέγγιση των μεταδεδομένων επικοινωνίας, αναδεικνύοντας τα στοιχεία που τα συνθέτουν και συγκρίνοντάς τα με τα εσωτερικά στοιχεία της επικοινωνίας. Τα μεταδεδομένα

επικοινωνίας διαδραματίζουν κρίσιμο ρόλο στην ψηφιακή επικοινωνία, επιτρέποντας τη μεταφορά πληροφοριών και τη δημιουργία συνδέσεων μεταξύ ατόμων και συσκευών.

Η δεύτερη ενότητα της παρούσας εξετάζει την κατοχύρωση του δικαιώματος στην προστασία του απορρήτου της επικοινωνίας στην εθνική έννομη τάξη. Η ανάγκη για νομική προστασία του απορρήτου της επικοινωνίας έχει γίνει πιο κρίσιμη με την αυξανόμενη εξάρτηση από την ψηφιακή επικοινωνία.

Η τρίτη ενότητα της παρούσας εστιάζει στην κατοχύρωση του δικαιώματος στην προστασία του απορρήτου της επικοινωνίας στην Ευρωπαϊκή Ένωση (ΕΕ) και τη διεθνή έννομη τάξη με μια σύντομη επισκόπηση του σχετικού νομοθετικού καθεστώτος, εξετάζοντας διάφορες αποφάσεις του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (Ε.Δ.Δ.Α.) και του Δικαστηρίου της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.), ενώ αναφορά γίνεται και στην απόφαση του Ανώτατου Αμερικανικού Δικαστηρίου Carpenter κατά Ηνωμένων Πολιτειών.

Η παρούσα στοχεύει στην παροχή μιας ολοκληρωμένης ανάλυσης των μεταδεδομένων επικοινωνίας ως διάσταση του προστατευτέο απορρήτου της επικοινωνίας, αναδεικνύοντας τις νομικές προσεγγίσεις εντός της εθνικής, ενωσιακής και διεθνούς έννομης τάξης. Η έρευνα επιδιώκει τελικά να συμβάλει στη συνεχιζόμενη συζήτηση για την προστασία του απορρήτου της επικοινωνίας στην ψηφιακή εποχή.

A] TA METADEDOMENA EPIKOINΩNΙΑΣ (ΕΞΩΤΕΡΙΚΑ ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ)

1. ΕΝΝΟΙΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΟΡΟΥ, ΤΑ ΣΤΟΙΧΕΙΑ ΠΟΥ ΤΑ ΣΥΝΘΕΤΟΥΝ, ΑΝΤΙΠΑΡΑΒΟΛΗ ΠΡΟΣ ΤΑ ΕΣΩΤΕΡΙΚΑ ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

Καθώς η χρήση της ψηφιακής επικοινωνίας συνεχίζει να αυξάνεται, αυξάνεται και η σημασία των μεταδεδομένων επικοινωνίας για την κατανόηση της συμπεριφοράς και των συνηθειών των ατόμων. Ως εκ τούτου, είναι ζωτικής σημασίας να έχουμε μια ολοκληρωμένη κατανόηση των μεταδεδομένων επικοινωνίας και τον πιθανό αντίκτυπό τους στο απόρρητο και την ασφάλεια στην ψηφιακή εποχή.

Ο όρος «μεταδεδομένα» τις προηγούμενες δεκαετίες χρησιμοποιούταν κυρίως ως αναφορά σχετική με τα αρχεία/εγγραφές των καταλόγων βιβλιοθηκών, τα δεδομένα λεξικών,

περιγραφές αρχείων σε συστήματα Γεωγραφικών Πληροφοριών, και λέξεις-κλειδιά που αποδίδονται σε ακαδημαϊκά άρθρα, ενώ στην ψηφιακή πλέον κοινωνική πραγματικότητα παραπέμπει σε αρχεία τηλεφωνικών κλήσεων, επικεφαλίδες email, αρχεία καταγραφής αναζήτησης στο Διαδίκτυο, τοποθεσίας GPS και data brokers (Mayernik, 2017).

1.1 Εννοιολογική Προσέγγιση Μεταδεδομένων Επικοινωνίας

Ο όρος «μεταδεδομένα επικοινωνίας», η χρήση του οποίου έγινε ευρέως διαδεδομένη τον αιώνα που διανύουμε λόγω της ραγδαίας τεχνολογικής και ψηφιακής προόδου σε συνδυασμό με τα διάφορα πολιτικά και κοινωνικά γεγονότα, εκκινώντας από το σκάνδαλο που ξέσπασε στο δυτικό κόσμο με τις αποκαλύψεις του Edward Snowden το έτος 2013 αναφορικά με τη μαζική ηλεκτρονική παρακολούθηση των πολιτών, μπορεί να ανευρεθεί ήδη από πολύ παλαιότερα. Στο πέρασμα των χρόνων, η έννοια αυτή διαπλάστηκε μάλλον κυρίως ακολουθώντας τις αλλαγές και τις εξελίξεις στον τομέα της τεχνολογίας και της πληροφορικής, «αναγκάζοντας» τη νομική της πτυχή να προσαρμοστεί αναλόγως. Η έννοια «μεταδεδομένα» επικοινωνίας συνήθως χρησιμοποιείται σε αντιδιαστολή προς το περιεχόμενο αυτής σε μια προσπάθεια διαχωρισμού των λεγόμενων εξωτερικών και εσωτερικών στοιχείων επικοινωνίας, διάκριση η οποία εντούτοις στη σημερινή ψηφιακή εποχή δεν είναι πάντοτε ευχερής και ίσως όχι ιδιαίτερα επιτυχημένη.

Ήδη από την ιστορία της αμερικανικής δικαστηριακής πρακτικής μπορούμε να εντοπίσουμε την τάση διαχωρισμού του περιεχόμενου της επικοινωνίας και των στοιχείων που παραδοσιακά εντάσσονται σε αυτό. Σε μια πρώτη απόπειρα την εποχή εκείνη που οι ηλεκτρονικοί υπολογιστές και τα κινητά τηλέφωνα δεν ήταν ακόμα γνωστά και οι επικοινωνίες διεξάγονταν μέσω ταχυδρομικών και ύστερα τηλεγραφικών υπηρεσιών, το Ανώτατο Δικαστήριο των ΗΠΑ στην υπόθεση *Ex parte Jackson* (1878) κλήθηκε να κρίνει περί του ζητήματος μέχρι ποιο βαθμό μπορούν οι αρμόδιες αρχές να εξετάσουν επιστολές, όπως προέβλεπε η τότε αμερικανική νομοθεσία, προς το σκοπό της πρόληψης και καταπολέμησης διακίνησης παράνομου υλικού. Το Δικαστήριο κατέληξε στο συμπέρασμα ότι οι αστυνομικές αρχές απαγορεύεται να λάβουν γνώση του εσωτερικού περιεχομένου μιας κλειστής επιστολής ή ενός πακέτου, δεν εμποδίζονται όμως να αντλήσουν πληροφορίες από τα εξωτερικά χαρακτηριστικά αυτών (αναγκαία δη τουλάχιστον τα στοιχεία αποστολέα και παραλήπτη) (Kift P. & Nissenbaum H., 2016). Έναν περίπου αιώνα αργότερα, το Δικαστήριο

στα πλαίσια της υπόθεσης Smith κατά Maryland (1979) και στην προσπάθεια ερμηνευτικής προσέγγισης της Τέταρτης Τροπολογίας του αμερικανικού συντάγματος, εμμένει στη διαπίστωση πως η νομική προστασία που επιφυλάσσει το αμερικανικό δίκαιο προς τα εκτός του περιεχόμενου της τηλεφωνικής επικοινωνίας στοιχεία, όπως είναι ο αριθμός τηλεφώνου, ο χρόνος και η διάρκεια της κλήσης, των οποίων κατ' ανάγκη λαμβάνει γνώση ο τηλεπικοινωνιακός πάροχος για την πραγματοποίηση της κλήσης υπολείπεται της νομικής προστασίας που προβλέπει η νομοθεσία για το περιεχόμενο της τηλεφωνικής επικοινωνίας (Ramirez, 2019). Σημειωτέον ότι η κρίση αυτή του αμερικανικού δικαστηρίου μεταβλήθηκε στη μεταγενέστερη απόφασή του επί της υπόθεσης Carpenter και την ανατροπή της λεγόμενης θεωρίας third-party doctrine (για την οποία θα γίνει λόγος στην οικεία ενότητα).

Οι μελετητές του επιστημονικού αυτού πεδίου επιχείρησαν να ανεύρουν έναν ορισμό για τα «μεταδεδομένα» χωρίς ωστόσο τελικά να είμαστε σε θέση με ασφάλεια να καταλήξουμε σε έναν και μόνο κοινά αποδεκτό ορισμό, μάλλον επειδή καθένας από αυτούς προσδίδει και κάποια σημαντική πληροφορία για τον καθορισμό της έννοιας των μεταδεδομένων. Μεταξύ άλλων, ως μεταδεδομένα ορίζονται «τα δεδομένα που παρέχουν πληροφορίες για άλλα δεδομένα». Για τον John Warren τα μεταδεδομένα χαρακτηρίζονται ως «*universe and DNA*» (Warren, 2015). Στην σχετικά πρόσφατη πρόταση του Ευρωπαϊκού Κανονισμού e-privacy τα μεταδεδομένα ηλεκτρονικών επικοινωνιών ορίζονται ως αυτά που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών για τους σκοπούς της μετάδοσης, της διανομής ή της ανταλλαγής περιεχομένου ηλεκτρονικών επικοινωνιών· συμπεριλαμβάνονται τα δεδομένα που χρησιμοποιούνται για την παρακολούθηση και την ταυτοποίηση της πηγής και του προορισμού μιας επικοινωνίας, τα δεδομένα τοποθεσίας της συσκευής που παράγονται στο πλαίσιο της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών και της ημερομηνίας, της ώρας, της διάρκειας και του είδους της επικοινωνίας (άρθρο 4 παράγραφος 3γ). Υπό το πρίσμα αυτό, τα μεταδεδομένα μπορούν να θεωρηθούν ως μια δομημένη πληροφορία που περιγράφει, εξηγεί, εντοπίζει και κάνει ευκολότερη την ανάκτηση και διαχείριση της πληροφορίας. Συνεπώς, τα μεταδεδομένα είναι άρρηκτα συνδεδεμένα με τη μετάδοση και την πραγματοποίηση του επικοινωνιακού γεγονότος αποκαλύπτοντας σημαντικές πτυχές αυτού, καθώς δυνάμει αυτών, στοιχεία, όπως η διάρκεια μιας κλήσης, η συχνότητα κλήσης ενός συγκεκριμένου αριθμού ή ο χρόνος αποστολής ενός mail, το μέσο (η συσκευή) που χρησιμοποιήθηκε, ο εντοπισμός της τοποθεσίας των συμμετεχόντων μερών και πολλά ακόμη, μπορούν να καταστούν γνωστά.

Γενικά, τα μεταδεδομένα διαδραματίζουν σημαντικό ρόλο στην ψηφιακή εποχή, όπου η ψηφιακή επικοινωνία είναι διαδεδομένη και πανταχού παρούσα. Τα μεταδεδομένα επικοινωνίας περιλαμβάνουν διάφορα στοιχεία, όπως είδαμε παραπάνω, συμπεριλαμβανομένων πληροφοριών σχετικά με τον αποστολέα, τον παραλήπτη, την ημερομηνία, την ώρα, την τοποθεσία και τη διάρκεια της επικοινωνίας. Οι πληροφορίες αποστολέα και παραλήπτη παρέχουν λεπτομέρειες σχετικά με τα μέρη που εμπλέκονται στην επικοινωνία. Οι πληροφορίες ημερομηνίας και ώρας παρέχουν λεπτομέρειες σχετικά με το χρονοδιάγραμμα της επικοινωνίας. Οι πληροφορίες τοποθεσίας παρέχουν λεπτομέρειες σχετικά με τη φυσική τοποθεσία του αποστολέα ή του παραλήπτη. Οι πληροφορίες διάρκειας παρέχουν λεπτομέρειες σχετικά με τη διάρκεια της επικοινωνίας.

Ωστόσο, πολλές χώρες δε διαθέτουν επαρκή νομική προστασία για τα μεταδεδομένα επικοινωνίας, καθιστώντας τα άτομα ευάλωτα σε παραβιάσεις του απορρήτου και πιθανή κατάχρηση των δεδομένων τους. Οι κυβερνήσεις και οι ιδιωτικές εταιρείες συχνά συλλέγουν και αναλύουν μεταδεδομένα επικοινωνίας για να αποκτήσουν γνώσεις για τις προτιμήσεις, τις συνήθειες και τα ενδιαφέροντα των ατόμων (Παπαδόπουλος, 2008). Αυτό έχει εγείρει ανησυχίες σχετικά με την πιθανή κακή χρήση των μεταδεδομένων επικοινωνίας, συμπεριλαμβανομένων των στοχευμένων διαφημίσεων, της κρατικής επιτήρησης και άλλων μορφών παραβιάσεων του απορρήτου.

1.2 Στοιχεία Μεταδεδομένων Επικοινωνίας

Τα μεταδεδομένα επικοινωνίας περιλαμβάνουν πολλά στοιχεία που παρέχουν πληροφορίες σχετικά με τις εξωτερικές πτυχές της επικοινωνίας. Σε αυτή την ενότητα, θα εξετάσουμε αυτά τα στοιχεία και τη σημασία τους.

Οι πληροφορίες αποστολέα και παραλήπτη παρέχουν λεπτομέρειες σχετικά με τα μέρη που εμπλέκονται στην επικοινωνία. Αυτές οι πληροφορίες είναι κρίσιμες για την κατανόηση του πλαισίου και του σκοπού της επικοινωνίας. Για παράδειγμα, μπορεί να παρέχονται πληροφορίες για τη σχέση μεταξύ του αποστολέα και του παραλήπτη, τους ρόλους τους και το είδος της επικοινωνίας. Οι ερευνητές έχουν επισημάνει τη σημασία των πληροφοριών αποστολέα και παραλήπτη για τον εντοπισμό και την ανάλυση των κοινωνικών δικτύων (Leskovec et al., 2008). Διαπίστωσαν ότι τα μεταδεδομένα επικοινωνίας μπορούν να παρέχουν πολύτιμες γνώσεις για τη δομή και τη δυναμική των κοινωνικών δικτύων.

Οι πληροφορίες ημερομηνίας και ώρας παρέχουν λεπτομέρειες σχετικά με το χρονοδιάγραμμα της επικοινωνίας. Αυτές οι πληροφορίες είναι απαραίτητες για την κατανόηση των χρονικών πτυχών της επικοινωνίας, συμπεριλαμβανομένων των προτύπων και των τάσεων. Για παράδειγμα, μπορεί να παρέχονται πληροφορίες για τη συχνότητα και τη διάρκεια της επικοινωνίας μεταξύ ατόμων ή ομάδων, πληροφορίες οι οποίες δύνανται να χρησιμοποιηθούν για να αναλυθούν τα πρότυπα επικοινωνίας και να προβλεφθεί η συμπεριφορά των ατόμων. Αναγκαία διαπίστωση τούτου είναι ότι τα μεταδεδομένα επικοινωνίας μπορούν να παρέχουν πολύτιμες γνώσεις για τη συμπεριφορά ατόμων και ομάδων.

Οι πληροφορίες τοποθεσίας παρέχουν λεπτομέρειες σχετικά με τη φυσική τοποθεσία του αποστολέα ή του παραλήπτη. Αυτές οι πληροφορίες είναι απαραίτητες για την κατανόηση των χωρικών πτυχών της επικοινωνίας. Για παράδειγμα, μπορεί να παρέχουν πληροφορίες για τη φυσική εγγύτητα ατόμων ή ομάδων, τα μοτίβα κινήσεών τους και τις αλληλεπιδράσεις τους με το περιβάλλον τους και οι πληροφορίες τοποθεσίας να χρησιμοποιηθούν για την ανάλυση της κοινωνικής συμπεριφοράς με τα μεταδεδομένα επικοινωνίας να μπορούν να παρέχουν πολύτιμες γνώσεις για την κοινωνική συμπεριφορά και τα πρότυπα κινητικότητας ατόμων και ομάδων.

Οι πληροφορίες διάρκειας παρέχουν λεπτομέρειες σχετικά με τη διάρκεια της επικοινωνίας. Αυτές οι πληροφορίες είναι απαραίτητες για την κατανόηση της έντασης και της έκτασης της επικοινωνίας. Για παράδειγμα, μπορεί να παρέχει μια εικόνα για την ποιότητα και τη σημασία της επικοινωνίας μεταξύ ατόμων ή ομάδων.

Ένα άλλο στοιχείο των μεταδεδομένων επικοινωνίας που παρέχει πολύτιμες πληροφορίες είναι το είδος της επικοινωνίας. Αυτό περιλαμβάνει πληροφορίες σχετικά με το μέσο που χρησιμοποιείται για την επικοινωνία, όπως email, μήνυμα κειμένου ή φωνητική κλήση. Μπορεί επίσης να περιλαμβάνει πληροφορίες σχετικά με το περιεχόμενο της επικοινωνίας, όπως τη γραμμή θέματος ή τις λέξεις-κλειδιά που χρησιμοποιούνται. Η φύση της αλληλεπίδρασης διαδραματίζει ζωτικό ρόλο στην κατανόηση των συνθηκών της επικοινωνίας, δεδομένου ότι διάφορες μορφές αλληλεπίδρασης μπορούν να παρουσιάσουν διαφορετικά πρότυπα, προσδοκίες και κοινωνικές αλληλεπιδράσεις.

Για παράδειγμα, ο τρόπος που επικοινωνούν οι άνθρωποι στις επίσημες επαγγελματικές συναντήσεις είναι πολύ διαφορετικός από τον τρόπο που επικοινωνούν σε μια περιστασιακή κοινωνική συγκέντρωση. Οι κανόνες, οι προσδοκίες και η κοινωνική δυναμική αλλάζουν σημαντικά. Σε μια επαγγελματική συνάντηση, οι άνθρωποι μπορεί να μιλούν πιο επίσημα, να χρησιμοποιούν συγκεκριμένη ορολογία και να ακολουθούν μια συγκεκριμένη ιεραρχία όταν μιλούν. Από την άλλη πλευρά, σε μια περιστασιακή κοινωνική συνάντηση, η χρησιμοποιούμενη γλώσσα θα ήταν πιο ανεπίσημη, θα υπήρχε λιγότερη ορολογία και οι άνθρωποι θα μιλούσαν ελεύθερα χωρίς αυστηρή τάξη ή ιεραρχία. Τα μεταδεδομένα από αυτούς τους δύο τύπους επικοινωνίας, όπως ο χρόνος, η συχνότητα και η διάρκεια των αλληλεπιδράσεων, μπορούν να παρέχουν πολύτιμες γνώσεις σε αυτά τα διαφορετικά πλαίσια.

Τέλος, τα μεταδεδομένα επικοινωνίας μπορούν επίσης να περιλαμβάνουν πληροφορίες σχετικά με τη συσκευή που χρησιμοποιείται για την επικοινωνία. Αυτό περιλαμβάνει πληροφορίες σχετικά με τη μάρκα και το μοντέλο της συσκευής, καθώς και πληροφορίες σχετικά με το λειτουργικό σύστημα και το λογισμικό που χρησιμοποιείται. Αυτές οι πληροφορίες μπορούν να παρέχουν πληροφορίες για τις τεχνολογικές δυνατότητες και προτιμήσεις ατόμων ή ομάδων.

Αυτά τα στοιχεία είναι κρίσιμα για την κατανόηση του πλαισίου, του σκοπού, των χρονικών και χωρικών πτυχών της επικοινωνίας. Χρησιμοποιώντας τα μεταδεδομένα επικοινωνίας καθίσταται δυνατή η απόκτηση γνώσεων σχετικά με τα κοινωνικά δίκτυα, τη συμπεριφορά, τα πρότυπα κινητικότητας και κατ' επέκταση η πρόβλεψη κοινωνικών αποτελεσμάτων.

Συνεπώς, τα μεταδεδομένα είναι μια πλούσια πηγή προσωπικών πληροφοριών για τους χρήστες - υποκείμενα, καθώς αποκαλύπτουν το «ποιος» (τα επικοινωνούντα μέρη), «πότε», πόσο καιρό και πόσο συχνά, (χρόνος, διάρκεια και συχνότητα), το «τι» (είδος επικοινωνίας, π.χ. τηλεφωνική κλήση, μήνυμα, e-mail), το «πώς» (η συσκευή επικοινωνίας που χρησιμοποιείται, π.χ. σταθερή τηλεφωνία, smartphone, tablet) και το «πού» (τοποθεσία των συσκευών που χρησιμοποιούνται) των μερών, που εμπλέκονται σε κάθε είδους επικοινωνία (Loideain, 2015).

1.3 Σύγκριση με εσωτερικά στοιχεία επικοινωνίας

Ενώ τα μεταδεδομένα επικοινωνίας παρέχουν πολύτιμες πληροφορίες σχετικά με τις εξωτερικές πτυχές της επικοινωνίας, είναι σημαντικό να σημειωθεί ότι διαφέρουν από τις εσωτερικές πτυχές της επικοινωνίας. Οι εσωτερικές πτυχές της επικοινωνίας περιλαμβάνουν το περιεχόμενο, τον τόνο και το νόημα της επικοινωνίας. Αυτά τα στοιχεία είναι κρίσιμα για την κατανόηση του πλαισίου, του σκοπού και του περιεχομένου της επικοινωνίας.

Ωστόσο, ενώ οι εσωτερικές πτυχές της επικοινωνίας προστατεύονται από νόμους και κανονισμούς περί απορρήτου, δεν μπορούμε να πούμε το ίδιο για τα μεταδεδομένα επικοινωνίας. Σε πολλές δικαιοδοσίες, τα μεταδεδομένα επικοινωνίας δε θεωρούνται τόσο ευαίσθητα όσο το περιεχόμενο των επικοινωνιών και ως εκ τούτου υπόκεινται σε λιγότερη προστασία απορρήτου. Αυτό έχει οδηγήσει σε ανησυχίες σχετικά με την πιθανή κακή χρήση ή κακή διαχείριση των μεταδεδομένων επικοινωνίας από κυβερνήσεις, επιχειρήσεις και άλλες οντότητες.

Επιπροσθέτως, μια βασική διαφορά μεταξύ των μεταδεδομένων επικοινωνίας και των εσωτερικών πτυχών της επικοινωνίας είναι το επίπεδο ευκρίνειας. Οι ερευνητές έχουν χρησιμοποιήσει τις εσωτερικές πτυχές της επικοινωνίας για να αναλύσουν το συναίσθημα, τα συναισθήματα και την κοινωνική δυναμική (π.χ. Kramer et al., 2014· Schwartz et al., 2013) διαπιστώνοντας ότι οι εσωτερικές πτυχές της επικοινωνίας μπορούν να παρέχουν πολύτιμες γνώσεις για το συναίσθημα, τα συναισθήματα και την κοινωνική δυναμική των ατόμων και των ομάδων.

Μια άλλη διαφορά μεταξύ των μεταδεδομένων επικοινωνίας και των εσωτερικών πτυχών της επικοινωνίας είναι το επίπεδο υποκειμενικότητας. Ενώ τα μεταδεδομένα επικοινωνίας παρέχουν αντικειμενικές πληροφορίες για τις εξωτερικές πτυχές της επικοινωνίας, οι εσωτερικές πτυχές της επικοινωνίας είναι συχνά υποκειμενικές και ανοιχτές σε ερμηνεία. Αυτή η υποκειμενικότητα μπορεί να κάνει δύσκολη την ανάλυση και την ερμηνεία του περιεχομένου, του τόνου και του νοήματος της επικοινωνίας με ακρίβεια. Οι ερευνητές έχουν χρησιμοποιήσει τεχνικές επεξεργασίας φυσικής γλώσσας και μηχανικής μάθησης για να αναλύσουν τις εσωτερικές πτυχές της επικοινωνίας (π.χ. Jurafsky & Martin, 2023; Liu & Singh, 2004). Βρήκαν ότι αυτές οι τεχνικές μπορούν να βοηθήσουν να ξεπεραστεί η

υποκειμενικότητα των εσωτερικών πτυχών της επικοινωνίας και να παρέχουν πολύτιμες γνώσεις για το περιεχόμενο, τον τόνο και το νόημα της επικοινωνίας.

Αν και τα μεταδεδομένα και το περιεχόμενο είναι δύο διαφορετικές έννοιες, συχνά είναι δύσκολο να γίνει διάκριση μεταξύ των δύο, ειδικά σε ψηφιακά πλαίσια. Ακολουθεί μια σύντομη επισκόπηση του καθενός:

- **Μεταδεδομένα:** Αναφέρεται σε δεδομένα που περιγράφουν ή παρέχουν πληροφορίες για άλλα δεδομένα. Για παράδειγμα, στο πλαίσιο μιας ψηφιακής φωτογραφίας, τα μεταδεδομένα μπορεί να περιλαμβάνουν πληροφορίες σχετικά με την ημερομηνία και την ώρα λήψης της φωτογραφίας, τις ρυθμίσεις της κάμερας που χρησιμοποιήθηκαν και την τοποθεσία όπου τραβήχτηκε η φωτογραφία. Τα μεταδεδομένα συνήθως δεν είναι ορατά στο ίδιο το περιεχόμενο, αλλά είναι ενσωματωμένα σε αυτό ή αποθηκεύονται ξεχωριστά.
- **Περιεχόμενο:** Αναφέρεται στις πραγματικές πληροφορίες ή δεδομένα που μεταφέρονται. Στο πλαίσιο μιας ψηφιακής φωτογραφίας, το περιεχόμενο θα ήταν η ίδια η εικόνα - η οπτική πληροφορία που μεταφέρεται.

Παρά τις διαφορές μεταξύ των μεταδεδομένων επικοινωνίας και των εσωτερικών πτυχών της επικοινωνίας, συχνά συνδέονται στενά. Για παράδειγμα, τα μεταδεδομένα επικοινωνίας μπορούν να παρέχουν ενδείξεις σχετικά με το περιεχόμενο, τον τόνο και το νόημα της επικοινωνίας. Μπορεί επίσης να χρησιμοποιηθούν για την εξαγωγή προσωπικών πληροφοριών σχετικά με τα εμπλεκόμενα μέρη, όπως την ταυτότητα, τα ενδιαφέροντα και τις σχέσεις τους.

Ενώ τα μεταδεδομένα και το περιεχόμενο είναι διαφορετικές πτυχές των ψηφιακών πληροφοριών, είναι επίσης αλήθεια ότι είναι αλληλένδετα και μερικές φορές μπορεί να είναι δύσκολο να διακριθούν. Σε ορισμένες περιπτώσεις, τα μεταδεδομένα μπορούν να θεωρηθούν ως τύπος περιεχομένου, καθώς περιέχουν πληροφορίες που σχετίζονται με την κατανόηση και την ερμηνεία του ίδιου του περιεχομένου, καθότι ναι μεν δεν αποκαλύπτουν άμεσα το συγκεκριμένο περιεχόμενο ενός ψηφιακού αντικειμένου, μπορούν όμως και παρέχουν πολύτιμο πλαίσιο και πληροφορίες σχετικά με αυτό το περιεχόμενο. Για παράδειγμα, σε μια φωτογραφία, τα μεταδεδομένα μπορεί να περιλαμβάνουν πληροφορίες όπως ημερομηνία, ώρα, τοποθεσία, ρυθμίσεις κάμερας και άλλες τεχνικές λεπτομέρειες.

Αυτά τα μεταδεδομένα είναι σχετικά με την κατανόηση του πλαισίου και του νοήματος της ίδιας της φωτογραφίας. Ομοίως, σε ένα άρθρο επιστημονικής έρευνας, τα μεταδεδομένα όπως ο συγγραφέας, η ημερομηνία δημοσίευσης και οι λέξεις-κλειδιά μπορούν να παρέχουν σημαντικό πλαίσιο για την κατανόηση του περιεχομένου του άρθρου και ακόμα να αποκαλύψουν πληροφορίες σχετικά με τον συγγραφέα του, την ημερομηνία δημιουργίας του, το λογισμικό που χρησιμοποιήθηκε για τη δημιουργία του και πιθανώς τον σκοπό ή το κοινό για το οποίο προορίζεται.

Επιπλέον, τα μεταδεδομένα μπορούν να επηρεάσουν την ανιχνευσιμότητα και την προσβασιμότητα του ψηφιακού περιεχομένου. Οι μηχανές αναζήτησης και άλλα εργαλεία ανακάλυψης βασίζονται σε μεταδεδομένα για να βοηθήσουν τους χρήστες να βρουν και να αποκτήσουν πρόσβαση σε σχετικό περιεχόμενο.

Ως συνέπεια των ανωτέρω, τα μεταδεδομένα διαδραματίζουν σημαντικό ρόλο στην προστασία του απόρρητου. Αν και τα ίδια τα μεταδεδομένα μπορεί να μην περιέχουν ευαίσθητες ή ταυτοποιητικές πληροφορίες, μπορούν να παρέχουν ενδείξεις σχετικά με το περιεχόμενο των ψηφιακών αντικειμένων και τις δραστηριότητες των χρηστών που τα δημιούργησαν ή τα είχαν πρόσβαση. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για να συναχθούν προσωπικές ή ευαίσθητες πληροφορίες, ακόμη και αν αυτές οι πληροφορίες δεν αναφέρονται ρητά στο περιεχόμενο του ψηφιακού αντικειμένου.

Ακολουθούν ορισμένα παραδείγματα για το πώς τα μεταδεδομένα μπορούν να επηρεάσουν το απόρρητο:

1. Δεδομένα τοποθεσίας: Τα μεταδεδομένα που περιλαμβάνουν πληροφορίες τοποθεσίας μπορούν να αποκαλύψουν τις κινήσεις και τις δραστηριότητες ενός χρήστη, αποκαλύπτοντας ενδεχομένως ευαίσθητες πληροφορίες σχετικά με την προσωπική του ζωή ή συνήθειες.
2. Πρότυπα χρήσης: Τα μεταδεδομένα που παρακολουθούν μοτίβα χρήσης μπορούν να αποκαλύψουν προσωπικές προτιμήσεις και ενδιαφέροντα, αποκαλύπτοντας ενδεχομένως ευαίσθητες πληροφορίες σχετικά με τις πεποιθήσεις, την υγεία ή άλλα προσωπικά χαρακτηριστικά ενός χρήστη.

3. Πληροφορίες ταυτότητας: Τα μεταδεδομένα που περιλαμβάνουν πληροφορίες σχετικά με τον δημιουργό ή τον ιδιοκτήτη ενός ψηφιακού αντικειμένου μπορούν να χρησιμοποιηθούν για να συναχθούν προσωπικές ή ταυτοποιητικές πληροφορίες σχετικά με αυτό το άτομο.

4. Συνδέσεις δικτύου: Τα μεταδεδομένα που περιλαμβάνουν πληροφορίες σχετικά με συνδέσεις δικτύου ή μοτίβα επικοινωνίας μπορούν να χρησιμοποιηθούν για την εξαγωγή προσωπικών ή αναγνωριστικών πληροφοριών για άτομα ή ομάδες.

Συμπερασματικά, τα μεταδεδομένα επικοινωνίας και οι εσωτερικές πτυχές της επικοινωνίας είναι διαφορετικά αλλά στενά συνδεδεμένα στοιχεία επικοινωνίας. Ενώ οι εσωτερικές πτυχές της επικοινωνίας προστατεύονται από νόμους και κανονισμούς περί απορρήτου, τα μεταδεδομένα επικοινωνίας συχνά υπόκεινται σε λιγότερες προστασίες απορρήτου. Ωστόσο, καθώς τα μεταδεδομένα επικοινωνίας μπορούν να παρέχουν πολύτιμες πληροφορίες για το περιεχόμενο, τον τόνο και το νόημα των επικοινωνιών, είναι σημαντικό να προστατεύεται το απόρρητό τους και να διασφαλίζεται ότι δε γίνεται κατάχρηση ή κακή διαχείριση.

2. Η ΙΔΙΑΙΤΕΡΗ ΣΗΜΑΣΙΑ ΠΟΥ ΑΠΟΚΤΟΥΝ ΣΤΗΝ ΨΗΦΙΑΚΑ ΠΡΟΗΓΜΕΝΗ ΚΟΙΝΩΝΙΑ ΚΑΙ Η ΑΝΑΓΚΗ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΧΑΡΑΚΤΗΡΑ ΤΟΥΣ

2.1 Η σημασία των μεταδεδομένων της επικοινωνίας στην ψηφιακά προηγμένη κοινωνία

2.1.1 Ορισμός και είδη μεταδεδομένων επικοινωνίας

Τα μεταδεδομένα θα μπορούσαν να κατηγοριοποιηθούν σε διαφορετικούς τύπους με βάση τις πληροφορίες που παρέχουν (BasuMallick, 2022). Μερικές κοινές κατηγορίες μεταδεδομένων περιλαμβάνουν τα:

1. Περιγραφικά μεταδεδομένα: Αυτός ο τύπος μεταδεδομένων περιγράφει τα χαρακτηριστικά ενός πόρου, όπως ο τίτλος, ο συγγραφέας, η ημερομηνία δημιουργίας, το θέμα, οι λέξεις-κλειδιά κ.λπ. Χρησιμοποιείται για να βοηθήσει τους χρήστες να βρουν και να εντοπίσουν πόρους που ταιριάζουν με τις ανάγκες τους.

2. Δομικά μεταδεδομένα: Αυτός ο τύπος μεταδεδομένων περιγράφει την οργάνωση ενός πόρου, όπως ο πίνακας περιεχομένων, τα κεφάλαια, οι ενότητες και άλλα στοιχεία που συνθέτουν ένα έγγραφο ή αρχείο. Χρησιμοποιείται για να βοηθήσει τους χρήστες να πλοηγηθούν και να κατανοήσουν τη δομή του πόρου.

3. Διαχειριστικά (διοικητικά) μεταδεδομένα: Αυτός ο τύπος μεταδεδομένων παρέχει πληροφορίες σχετικά με τη διαχείριση ενός πόρου, όπως τη μορφή αρχείου, το μέγεθος, τα δικαιώματα πρόσβασης και την ιδιοκτησία. Χρησιμοποιείται για να βοηθήσει τους διαχειριστές να διαχειριστούν και να διατηρήσουν τον πόρο.

4. Μεταδεδομένα διατήρησης: Αυτός ο τύπος μεταδεδομένων παρέχει πληροφορίες σχετικά με τη μακροπρόθεσμη διατήρηση ενός πόρου, όπως η μορφή αρχείου, η τοποθεσία αποθήκευσης και το σχήμα μεταδεδομένων που χρησιμοποιείται. Χρησιμοποιείται για τη διασφάλιση της μακροπρόθεσμης προσβασιμότητας και χρηστικότητας του πόρου.

5. Μεταδεδομένα χρήσης: Αυτός ο τύπος μεταδεδομένων παρέχει πληροφορίες σχετικά με τον τρόπο χρήσης ενός πόρου, όπως τον αριθμό των λήψεων, τις προβολές ή τις αναφορές που έχει λάβει. Χρησιμοποιείται για τη μέτρηση του αντίκτυπου και της αξίας του πόρου.

6. Τεχνικά μεταδεδομένα: Αυτός ο τύπος μεταδεδομένων περιγράφει τα τεχνικά χαρακτηριστικά ενός πόρου, όπως η ανάλυση, ο χρωματικός χώρος και η μορφή συμπίεσης μιας εικόνας ή ενός αρχείου βίντεο. Χρησιμοποιείται για να διασφαλιστεί ότι ο πόρος μπορεί να εμφανιστεί σωστά και να έχει πρόσβαση από τους χρήστες.

Στις καθημερινές μας δραστηριότητες εμείς οι ίδιοι δημιουργούμε μεταδεδομένα. Ενδεικτικά, τα μεταδεδομένα που παράγονται ανάλογα με το είδος της δραστηριότητας είναι (Office of the Privacy Commissioner of Canada, 2014):

- Κατά την τηλεφωνική κλήση: ο τηλεφωνικός αριθμός επικοινωνούντων, ο μοναδικός αναγνωριστικός αριθμός των τηλεφωνικών συσκευών, ο χρόνος και η διάρκεια επικοινωνίας, η τοποθεσία των τερματικών συσκευών
- Κατά την αποστολή ενός email: το όνομα, η διεύθυνση ηλεκτρονικού ταχυδρομείου και η διεύθυνση IP αποστολέα, το όνομα, η διεύθυνση ηλεκτρονικού ταχυδρομείου παραλήπτη, η ημερομηνία και η ώρα, οι κεφαλίδες (headers) και οι μορφές κεφαλίδων (header formats), το θέμα, η κατάσταση email (αναγνωσμένο, μη αναγνωσμένο)

- Κατά την επικοινωνία με χρήση μέσων κοινωνικής δικτύωσης (social media): το όνομα και οι συναφείς αναγνωριστικές πληροφορίες που παρέχει ο χρήστης (κατοικία, ενδιαφέροντα, ημερομηνία γέννησης), το όνομα χρήστη και το μοναδικό αναγνωριστικό, η τοποθεσία και το μοναδικό αναγνωριστικό συσκευής, οι δραστηριότητες και οι ημερομηνίες αυτών
- Κατά την περιήγηση στο διαδίκτυο: οι ιστοσελίδες (domain names, χρόνος επίσκεψης), τα δεδομένα χρήστη και πιθανώς στοιχεία σύνδεσης χρήστη με λειτουργίες αυτόματης συμπλήρωσης, οι διευθύνσεις URL, η διεύθυνση IP του χρήστη, ο πάροχος υπηρεσιών Διαδικτύου, οι λεπτομέρειες υλικού συσκευής, το λειτουργικό σύστημα και η έκδοση προγράμματος περιήγησης του χρήστη, οι αναζητήσεις μέσω περιηγητή, καθώς και τα αυτοεγκαθιστώμενα αρχεία cookies.

Παρατηρώντας και μόνο τις κατηγορίες αυτές και το σύνολο των στοιχείων που μπορούμε να εξάγουμε στηριζόμενοι στα μεταδεδομένα θα λέγαμε με σχετική ασφάλεια ότι πράγματι τα μεταδεδομένα θα μπορούσαν να θεωρηθούν τύπος περιεχομένου. Η ολοένα αυξανόμενη χρήση των τεχνολογικών και ψηφιακών μέσων, αλλά και εν γένει η ψηφιοποίηση της κοινωνίας, έχουν ως σημαντική συνέπεια την αντιστοίχως αυξανόμενη «παραγωγή μεταδεδομένων», ενώ η τεχνολογική πρόοδος που σημειώνεται τις τελευταίες δεκαετίες επιτρέπει και διευκολύνει ιδιώτες και κυβερνήσεις ως την ανεύρεση, εξόρυξη, διατήρηση, ανάλυση και επεξεργασία αυτών μαζικά και σε τεράστια κλίμακα.

2.1.2 Χρήσεις Μεταδεδομένων Επικοινωνίας

Η χρήση μεταδεδομένων μπορεί να επιτρέψει στους παρόχους υπηρεσιών να προσφέρουν εξατομικευμένες υπηρεσίες και στοχευμένες διαφημίσεις στους πελάτες αναλύοντας τα πρότυπα επικοινωνίας και τη συμπεριφορά τους. Για παράδειγμα, τα μεταδεδομένα που σχετίζονται με τις δραστηριότητες περιήγησης στον ιστό ενός χρήστη μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός προφίλ των ενδιαφερόντων του, το οποίο στη συνέχεια μπορεί να χρησιμοποιηθεί για την προβολή στοχευμένων διαφημίσεων. Ομοίως, τα μεταδεδομένα που σχετίζονται με τις επικοινωνιακές δραστηριότητες ενός χρήστη μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός προφίλ της επικοινωνιακής του συμπεριφοράς, το οποίο στη συνέχεια μπορεί να χρησιμοποιηθεί για να του προσφέρει εξατομικευμένες υπηρεσίες όπως αποκλεισμός κλήσεων, προώθηση κλήσεων και φωνητικό ταχυδρομείο (Baltar & Brunet, 2012).

Εκτός από τις εμπορικές εφαρμογές τους, τα μεταδεδομένα μπορούν να χρησιμοποιηθούν για διάφορους άλλους σκοπούς, όπως η επιβολή του νόμου, η δημόσια υγεία και η ακαδημαϊκή έρευνα. Για παράδειγμα, τα μεταδεδομένα μπορούν να χρησιμοποιηθούν από τις υπηρεσίες επιβολής του νόμου για τη διερεύνηση εγκληματικών δραστηριοτήτων όπως η διακίνηση ναρκωτικών και η τρομοκρατία. Στη δημόσια υγεία, τα μεταδεδομένα μπορούν να χρησιμοποιηθούν για επιτήρηση ασθενειών, ανίχνευση εστίας ασθενειών και ιχνηλάτηση επαφών.

Τα μεταδεδομένα επικοινωνίας έχουν ένα ευρύ φάσμα χρήσεων σε διάφορους τομείς, συμπεριλαμβανομένων των επιχειρήσεων, του ακαδημαϊκού χώρου, της δημόσιας υγείας και της επιβολής του νόμου ενώ η χρήση μεταδεδομένων σε αυτούς τους τομείς έχει γίνει ολοένα και πιο διαδεδομένη τα τελευταία χρόνια λόγω της σημαντικής προόδου στην τεχνολογία επικοινωνίας και τις τεχνικές επεξεργασίας δεδομένων.

Στον επιχειρηματικό τομέα, τα μεταδεδομένα επικοινωνίας χρησιμοποιούνται συχνά για έρευνα αγοράς, δημιουργία προφίλ πελατών και ανίχνευση απάτης (Narayanan and Shmatikov, 2008). Οι εταιρείες μπορούν να χρησιμοποιήσουν μεταδεδομένα για να αναλύσουν τα πρότυπα επικοινωνίας των πελατών τους και να εντοπίσουν τάσεις και προτιμήσεις. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για την προσφορά εξατομικευμένων προϊόντων και υπηρεσιών στους πελάτες, τη βελτίωση της αφοσίωσης των πελατών και την αύξηση των πωλήσεων. Ο εντοπισμός απάτης είναι ένας άλλος τομέας όπου τα μεταδεδομένα χρησιμοποιούνται εκτενώς. Αναλύοντας τα πρότυπα επικοινωνίας των χρηστών, οι εταιρείες μπορούν να εντοπίσουν την ανώμαλη συμπεριφορά και να αποτρέψουν την απάτη πριν αυτή συμβεί.

Στον ακαδημαϊκό χώρο, τα μεταδεδομένα επικοινωνίας χρησιμοποιούνται για διάφορους ερευνητικούς σκοπούς, όπως ανάλυση κοινωνικών δικτύων, ανάλυση συναισθήματος και ανάλυση συμπεριφοράς επικοινωνίας (Baltar & Brunet, 2012). Η ανάλυση κοινωνικών δικτύων περιλαμβάνει την ανάλυση των κοινωνικών δομών και των σχέσεων μεταξύ ατόμων και ομάδων. Τα μεταδεδομένα επικοινωνίας μπορούν να χρησιμοποιηθούν για την κατασκευή γραφημάτων κοινωνικών δικτύων και την ανάλυση προτύπων επικοινωνίας μεταξύ ατόμων και ομάδων. Η ανάλυση συναισθημάτων περιλαμβάνει την ανάλυση του συναισθηματικού περιεχομένου της επικοινωνίας. Τα μεταδεδομένα μπορούν να

χρησιμοποιηθούν για τον εντοπισμό συναισθηματικών εκφράσεων στην επικοινωνία και την ανάλυση του συναισθήματος των μηνυμάτων. Η ανάλυση της συμπεριφοράς επικοινωνίας περιλαμβάνει την ανάλυση προτύπων επικοινωνίας, όπως οι χρόνοι απόκρισης, η διάρκεια των μηνυμάτων και η συχνότητα επικοινωνίας.

Στη δημόσια υγεία, τα μεταδεδομένα επικοινωνίας χρησιμοποιούνται για διάφορους σκοπούς, όπως η επιτήρηση ασθενειών, η ανίχνευση κρουσμάτων και η ανίχνευση επαφών (MD Matters, 2005). Αναλύοντας τα πρότυπα επικοινωνίας και τη συμπεριφορά, οι φορείς δημόσιας υγείας μπορούν να εντοπίσουν πιθανές εστίες ασθενειών και να λάβουν προληπτικά μέτρα για την πρόληψη της εξάπλωσης της νόσου. Η ανίχνευση επαφών περιλαμβάνει την αναγνώριση ατόμων που έχουν έρθει σε στενή επαφή με μολυσμένα άτομα. Τα μεταδεδομένα επικοινωνίας μπορούν να χρησιμοποιηθούν για τον εντοπισμό των προτύπων επικοινωνίας των μολυσμένων ατόμων και τον εντοπισμό των επαφών τους.

Στην επιβολή του νόμου, τα μεταδεδομένα επικοινωνίας χρησιμοποιούνται για ποινικές έρευνες, συλλογή πληροφοριών και πρόληψη τρομοκρατίας. Αναλύοντας τα πρότυπα επικοινωνίας των υπόπτων, οι υπηρεσίες επιβολής του νόμου μπορούν να εντοπίσουν πιθανές εγκληματικές δραστηριότητες και να αποτρέψουν την εμφάνισή τους. Η συλλογή πληροφοριών περιλαμβάνει τον εντοπισμό πιθανών απειλών για την ασφάλεια και τη συλλογή πληροφοριών για την αποτροπή τους.

2.1.3 Κοινωνικές, οικονομικές και πολιτικές επιπτώσεις των μεταδεδομένων της επικοινωνίας

Η χρήση μεταδεδομένων επικοινωνίας έχει σημαντικές κοινωνικές, οικονομικές και πολιτικές επιπτώσεις που εκτείνονται πέρα από τα εμπορικά και λειτουργικά οφέλη της. Τα μεταδεδομένα επικοινωνίας έχουν τη δυνατότητα να επηρεάσουν την κοινωνική δυναμική διαμορφώνοντας πρότυπα επικοινωνίας, τα οποία, με τη σειρά τους, μπορούν να επηρεάσουν τις κοινωνικές σχέσεις και τη δυναμική της ομάδας. Για παράδειγμα, τα μεταδεδομένα επικοινωνίας μπορούν να χρησιμοποιηθούν για την ανάλυση των προτύπων επικοινωνίας ατόμων και ομάδων και τον εντοπισμό σχέσεων και συσχετισμών που μπορεί να μην είναι εμφανείς από το περιεχόμενο της επικοινωνίας. Αυτό μπορεί να οδηγήσει στο σχηματισμό νέων κοινωνικών ομάδων και δικτύων, που μπορεί να έχουν εκτεταμένες επιπτώσεις στην κοινωνία.

Τα μεταδεδομένα επικοινωνίας έχουν επίσης σημαντικές οικονομικές επιπτώσεις. Αναλύοντας τα μεταδεδομένα επικοινωνίας, οι εταιρείες μπορούν να αποκτήσουν πολύτιμες γνώσεις για τη συμπεριφορά και τις προτιμήσεις των καταναλωτών, οι οποίες μπορούν να χρησιμοποιηθούν για την ανάπτυξη στοχευμένων καμπανιών μάρκετινγκ και την αύξηση των πωλήσεων. Ωστόσο, η χρήση μεταδεδομένων επικοινωνίας μπορεί επίσης να δημιουργήσει οικονομικές ανισότητες ευνοώντας εταιρείες με πιο σημαντικούς πόρους και δυνατότητες επεξεργασίας δεδομένων. Οι μικρές επιχειρήσεις και τα άτομα ενδέχεται να μην έχουν πρόσβαση στους ίδιους πόρους και τεχνικές επεξεργασίας δεδομένων, με αποτέλεσμα να βρίσκονται σε μειονεκτική θέση.

Η χρήση μεταδεδομένων επικοινωνίας έχει επίσης σημαντικές πολιτικές επιπτώσεις. Τα μεταδεδομένα επικοινωνίας μπορούν να χρησιμοποιηθούν για την παρακολούθηση των επικοινωνιακών δραστηριοτήτων ατόμων και ομάδων, οδηγώντας δυνητικά σε παραβιάσεις του απορρήτου και των πολιτικών ελευθεριών. Επιπλέον, τα μεταδεδομένα επικοινωνίας μπορούν να χρησιμοποιηθούν για να επηρεάσουν τον πολιτικό λόγο και την κοινή γνώμη στοχεύοντας άτομα με συγκεκριμένα μηνύματα και πληροφορίες. Αυτό μπορεί να έχει εκτεταμένες επιπτώσεις για τη δημοκρατία και τη λειτουργία της κοινωνίας.

Επιπλέον, η χρήση μεταδεδομένων επικοινωνίας μπορεί να επιδεινώσει τις υπάρχουσες ανισορροπίες ισχύος και ανισότητες στην κοινωνία. Άτομα ή ομάδες με πιο σημαντικούς πόρους ή πρόσβαση σε τεχνικές επεξεργασίας δεδομένων ενδέχεται να είναι σε θέση να εκμεταλλευτούν τα μεταδεδομένα επικοινωνίας για να αποκτήσουν αθέμιτο πλεονέκτημα έναντι άλλων. Αυτό μπορεί να δημιουργήσει έναν κύκλο ανισότητας που είναι δύσκολο να σπάσει.

Όπως αναφέρθηκε, η χρήση μεταδεδομένων επικοινωνίας έχει τη δυνατότητα να επηρεάσει την κοινωνική δυναμική, να δημιουργήσει οικονομικές ανισότητες και να επιδεινώσει τις ανισορροπίες και τις ανισότητες εξουσίας στην κοινωνία. Ως εκ τούτου η ανάγκη εξισορρόπησης των οφελών των μεταδεδομένων επικοινωνίας με τις πιθανές βλάβες και την προστασία της ιδιωτικής ζωής και των πολιτικών ελευθεριών είναι μια σημαντική πρόκληση που αντιμετωπίζουν οι υπεύθυνοι χάραξης πολιτικής, οι ρυθμιστικές αρχές και η κοινωνία γενικότερα.

2.2 Η ανάγκη προστασίας του απόρρητου χαρακτήρα των μεταδεδομένων επικοινωνίας

2.2.1 Κίνδυνοι για το απόρρητο και τις αστικές ελευθερίες

Η χρήση μεταδεδομένων επικοινωνίας εγείρει σημαντικές ανησυχίες για το απόρρητο και τις πολιτικές ελευθερίες. Τα μεταδεδομένα επικοινωνίας μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες για άτομα, όπως η τοποθεσία, οι επαφές και τα μοτίβα επικοινωνίας τους, τα οποία μπορούν να χρησιμοποιηθούν για την αναγνώριση και την παρακολούθηση ατόμων. Επιπλέον, τα μεταδεδομένα επικοινωνίας μπορούν να συνδυαστούν με άλλες πηγές πληροφοριών, όπως η δραστηριότητα των μέσων κοινωνικής δικτύωσης ή οι οικονομικές συναλλαγές, για τη δημιουργία ολοκληρωμένων προφίλ ατόμων (Solove, 2012).

Η συλλογή και η ανάλυση μεταδεδομένων επικοινωνίας από κυβερνήσεις και ιδιωτικές εταιρείες έχουν τη δυνατότητα να παραβιάζουν τα δικαιώματα ιδιωτικού απορρήτου και τις πολιτικές ελευθερίες των ατόμων. Οι κυβερνήσεις μπορούν να χρησιμοποιούν μεταδεδομένα επικοινωνίας για να παρακολουθούν τις επικοινωνιακές δραστηριότητες των ατόμων, γεγονός που ενδεχομένως οδηγεί σε παραβίαση των δικαιωμάτων των ατόμων στην ελευθερία του λόγου και του συνεταιρίζεσθαι. Επιπλέον, η χρήση μεταδεδομένων επικοινωνίας από ιδιωτικές εταιρείες μπορεί να έχει ως αποτέλεσμα τη συλλογή και αποθήκευση ευαίσθητων προσωπικών πληροφοριών χωρίς τη γνώση ή τη συναίνεση των ατόμων, οδηγώντας δυνητικά στην παραβίαση των δικαιωμάτων απορρήτου.

Επιπλέον, η χρήση μεταδεδομένων επικοινωνίας εγείρει σημαντικές ανησυχίες σχετικά με την ασφάλεια και την προστασία των δεδομένων. Τα μεταδεδομένα επικοινωνίας αποθηκεύονται συχνά σε διακομιστές και μεταδίδονται σε δίκτυα, καθιστώντας τα ευάλωτα σε μη εξουσιοδοτημένη πρόσβαση και κακή χρήση. Οι χάκερς ή άλλοι κακόβουλοι παράγοντες ενδέχεται να στοχεύουν μεταδεδομένα επικοινωνίας για το όφελος τους.

Η χρήση μεταδεδομένων επικοινωνίας έχει επίσης επιπτώσεις στην αυτονομία και την ελευθερία επιλογής των ατόμων. Αναλύοντας τα μεταδεδομένα επικοινωνίας, οι εταιρείες και οι κυβερνήσεις μπορούν να αποκτήσουν πολύτιμες γνώσεις για τη συμπεριφορά και τις προτιμήσεις των ατόμων, οδηγώντας ενδεχομένως στη δημιουργία στοχευμένων

μηνυμάτων ή παρεμβάσεων επηρεάζοντας με αυτόν τον τρόπο την αυτονομία και την ελευθερία επιλογής των ατόμων, οδηγώντας δυνητικά στη χειραγώγηση της συμπεριφοράς τους.

2.2.2 Τεχνικά μέτρα για την προστασία της ιδιωτικής ζωής

Για την προστασία του απορρήτου των μεταδεδομένων επικοινωνίας, έχουν προταθεί και εφαρμοστεί διάφορα τεχνικά μέτρα. Αυτά τα μέτρα αποσκοπούν στην πρόληψη της μη εξουσιοδοτημένης πρόσβασης στα μεταδεδομένα επικοινωνίας, στην προστασία της ασφάλειας και της ακεραιότητας των δεδομένων και στη βελτίωση του ελέγχου των χρηστών στα δεδομένα τους. Παρά τη χρησιμότητά τους διατυπώνονται επιφυλάξεις για την αποτελεσματικότητά τους στο σύνολο των περιπτώσεων που τίθενται ζητήματα προστασίας του απορρήτου, καθότι οι παραπάνω πρακτικές μπορούν να εφαρμοσθούν σε εξατομικευμένες ή κατηγορίες περιπτώσεων, χωρίς να μπορούν να συλλάβουν την καθολική ανάγκη προστασίας του απορρήτου των μεταδεδομένων.

Ένα τέτοιο μέτρο είναι η κρυπτογράφηση, η οποία μπορεί να χρησιμοποιηθεί για την προστασία της εμπιστευτικότητας και της ακεραιότητας των μεταδεδομένων επικοινωνίας. Η κρυπτογράφηση περιλαμβάνει τη μετατροπή του περιεχομένου ενός μηνύματος σε κωδικό που μπορεί να αποκρυπτογραφηθεί μόνο από τον προβλεπόμενο παραλήπτη. Αυτό καθιστά δύσκολη την πρόσβαση μη εξουσιοδοτημένων μερών στο περιεχόμενο ή στα μεταδεδομένα του μηνύματος. Η κρυπτογράφηση μπορεί να εφαρμοστεί σε διάφορα επίπεδα, συμπεριλαμβανομένης της κρυπτογράφησης από άκρο σε άκρο, η οποία κρυπτογραφεί το περιεχόμενο και τα μεταδεδομένα του μηνύματος από τον αποστολέα στον παραλήπτη και την ασφάλεια του επιπέδου μεταφοράς, η οποία κρυπτογραφεί την επικοινωνία μεταξύ του χρήστη και του παρόχου υπηρεσιών (Riebe et al., 2022).

Ένα άλλο τεχνικό μέτρο για την προστασία του απορρήτου είναι η ανωνυμοποίηση, η οποία περιλαμβάνει την αφαίρεση ή την απόκρυψη πληροφοριών αναγνώρισης από τα μεταδεδομένα επικοινωνίας. Η ανωνυμοποίηση μπορεί να επιτευχθεί μέσω διαφόρων μεθόδων, όπως η συνάθροιση, όπου τα δεδομένα συνδυάζονται με άλλα δεδομένα για την αφαίρεση πληροφοριών αναγνώρισης ή η γενίκευση, όπου τα δεδομένα τροποποιούνται για να αφαιρεθούν οι λεπτομέρειες αναγνώρισης.

Επιπλέον, μπορούν να χρησιμοποιηθούν τεχνικά μέτρα όπως ο έλεγχος πρόσβασης, τα τείχη προστασίας και τα συστήματα ανίχνευσης εισβολής για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στα μεταδεδομένα επικοινωνίας. Αυτά τα μέτρα αποσκοπούν στον περιορισμό της πρόσβασης στα μεταδεδομένα επικοινωνίας σε εξουσιοδοτημένους χρήστες και στην προστασία από μη εξουσιοδοτημένες προσπάθειες πρόσβασης ή τροποποίησης των δεδομένων. Επιπλέον, οι τεχνολογίες που βελτιώνουν το απόρρητο, όπως τα εικονικά ιδιωτικά δίκτυα (VPN) και το Tor, μπορούν να χρησιμοποιηθούν για την προστασία του απόρρητου των χρηστών αποκρύπτοντας τη διεύθυνση IP και την τοποθεσία τους (Liu & Singh, 2004).

2.2.3 Νομικά μέτρα για την προστασία της ιδιωτικής ζωής

Μπορούν επίσης να εφαρμοστούν νομικά μέτρα για την προστασία του απόρρητου των μεταδεδομένων επικοινωνίας που να στοχεύουν στη διασφάλιση της προστασίας των δικαιωμάτων ιδιωτικής ζωής και των πολιτικών ελευθεριών των ατόμων.

Ένα τέτοιο νομικό μέτρο είναι η νομοθεσία περί προστασίας δεδομένων, η οποία καθορίζει τις απαιτήσεις για τη συλλογή, αποθήκευση και χρήση προσωπικών δεδομένων, συμπεριλαμβανομένων των μεταδεδομένων επικοινωνίας. Η νομοθεσία περί προστασίας δεδομένων στοχεύει να διασφαλίσει ότι τα άτομα έχουν τον έλεγχο των προσωπικών τους δεδομένων και ότι χρησιμοποιούνται μόνο για νόμιμους σκοπούς. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) της Ευρωπαϊκής Ένωσης είναι ένα αξιοσημείωτο παράδειγμα νομοθεσίας για την προστασία δεδομένων που περιλαμβάνει διατάξεις για την προστασία των προσωπικών δεδομένων, συμπεριλαμβανομένων των μεταδεδομένων επικοινωνίας.

Ένα άλλο νομικό μέτρο για την προστασία του απόρρητου είναι η απαίτηση για τις εταιρείες και τις κυβερνήσεις να λαμβάνουν ενημερωμένη συναίνεση ατόμων πριν από τη συλλογή ή τη χρήση των μεταδεδομένων επικοινωνίας τους. Η ενημερωμένη συγκατάθεση σημαίνει ότι παρέχονται στα άτομα σαφείς και κατανοητές πληροφορίες σχετικά με τη συλλογή και τη χρήση των δεδομένων τους και έχουν τη δυνατότητα να επιλέξουν ελεύθερα και εθελοντικά εάν θα συναινέσουν στη συλλογή και χρήση των δεδομένων τους (Solove, 2013).

Επιπλέον, τα δικαστήρια και οι ρυθμιστικοί φορείς μπορούν να διαδραματίσουν σημαντικό ρόλο στην προστασία των δικαιωμάτων ιδιωτικής ζωής και των πολιτικών ελευθεριών των ατόμων όσον αφορά τα μεταδεδομένα επικοινωνίας. Οι δικαστικές αποφάσεις, όπως η απόφαση του Ανώτατου Δικαστηρίου των Η.Π.Α. στην υπόθεση Carpenter κατά Ηνωμένων Πολιτειών, έχουν αποδείξει ότι τα άτομα έχουν εύλογες προσδοκίες για το απόρρητο όσον αφορά τα δεδομένα τοποθεσίας τους και ότι η κυβέρνηση πρέπει να λάβει ένταλμα πριν αποκτήσει πρόσβαση σε αυτά τα δεδομένα. Οι ρυθμιστικοί φορείς, όπως οι αρχές προστασίας δεδομένων, μπορούν επίσης να επιβάλουν τη νομοθεσία για την προστασία δεδομένων και να διασφαλίσουν ότι τα δικαιώματα ιδιωτικού απορρήτου των ατόμων γίνονται σεβαστά από τις εταιρείες και τις κυβερνήσεις.

Επιπλέον, διεθνείς συμφωνίες και πρότυπα, όπως η Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων και το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα, αναγνωρίζουν το δικαίωμα των ατόμων στην ιδιωτική ζωή και μπορούν να παρέχουν ένα πλαίσιο για την προστασία των δικαιωμάτων της ιδιωτικής ζωής και των πολιτικών ελευθεριών σχετικά με τα μεταδεδομένα επικοινωνίας.

2.2.4 Εξισορρόπηση απορρήτου και ασφάλειας

Η εξισορρόπηση του απορρήτου και της ασφάλειας είναι μια σημαντική πρόκληση που αντιμετωπίζουν οι υπεύθυνοι χάραξης πολιτικής, οι ρυθμιστικές αρχές και η κοινωνία γενικότερα. Ενώ τα μεταδεδομένα επικοινωνίας μπορούν να παρέχουν πολύτιμες πληροφορίες για τα πρότυπα επικοινωνίας, μπορούν επίσης να χρησιμοποιηθούν για την παρακολούθηση και την επιτήρηση ατόμων, οδηγώντας σε πιθανές παραβιάσεις της ιδιωτικής ζωής και απειλές για τις πολιτικές ελευθερίες. Ταυτόχρονα, τα μεταδεδομένα επικοινωνίας μπορούν να είναι χρήσιμα για την καταπολέμηση του εγκλήματος και της τρομοκρατίας, καθιστώντας τα απαραίτητα για την εθνική ασφάλεια.

Μια προσέγγιση για την εξισορρόπηση των ανησυχιών για το απόρρητο και την ασφάλεια είναι η χρήση της ελαχιστοποίησης δεδομένων, η οποία περιλαμβάνει τον περιορισμό της συλλογής, χρήσης και διατήρησης των μεταδεδομένων επικοινωνίας μόνο σε ό,τι είναι απαραίτητο για νόμιμους σκοπούς. Η ελαχιστοποίηση δεδομένων αποσκοπεί στη μείωση του κινδύνου παραβίασης της ιδιωτικής ζωής και στην ενίσχυση του ελέγχου των ατόμων στα δεδομένα τους. Μια άλλη προσέγγιση είναι η χρήση της ανωνυμοποίησης δεδομένων ή

της ψευδωνυμοποίησης για την προστασία του απόρρητου των ατόμων, επιτρέποντας ταυτόχρονα την ανάλυση των προτύπων επικοινωνίας.

Επιπλέον, μπορούν να πραγματοποιηθούν αξιολογήσεις επιπτώσεων στο απόρρητο για την αξιολόγηση των πιθανών κινδύνων για το απόρρητο και τις πολιτικές ελευθερίες που σχετίζονται με τη συλλογή, τη χρήση και τη διατήρηση των μεταδεδομένων επικοινωνίας. Οι αξιολογήσεις επιπτώσεων στο απόρρητο μπορούν να βοηθήσουν στον εντοπισμό πιθανών παραβιάσεων της ιδιωτικής ζωής και να ενημερώσουν την ανάπτυξη κατάλληλων διασφαλίσεων και μέτρων για τον μετριασμό αυτών των κινδύνων.

Μια άλλη σημαντική πτυχή της εξισορρόπησης των ανησυχιών για το απόρρητο και την ασφάλεια είναι η διασφάλιση της ύπαρξης μηχανισμών εποπτείας και λογοδοσίας. Αυτοί οι μηχανισμοί μπορούν να περιλαμβάνουν ανεξάρτητους εποπτικούς φορείς, όπως επιτρόπους προστασίας της ιδιωτικής ζωής ή διαμεσολαβητές, που έχουν την εξουσία να ερευνούν και να επιβάλλουν την προστασία της ιδιωτικής ζωής. Επιπλέον, η διαφάνεια και η λογοδοσία μπορούν να βελτιωθούν μέσω της δημοσίευσης εκθέσεων διαφάνειας και της ανάπτυξης σαφών και κατανοητών πολιτικών και πρακτικών απόρρητου.

Συμπερασματικά, η εξισορρόπηση των ανησυχιών σχετικά με το απόρρητο και την ασφάλεια σχετικά με τα μεταδεδομένα επικοινωνίας είναι μια σύνθετη και διαρκής πρόκληση. Η ελαχιστοποίηση δεδομένων, η ανωνυμοποίηση δεδομένων, οι εκτιμήσεις επιπτώσεων στο απόρρητο, οι μηχανισμοί επίβλεψης και λογοδοσίας, καθώς και η διαφάνεια και η λογοδοσία μπορούν όλα να διαδραματίσουν ρόλο στην προστασία των δικαιωμάτων απόρρητου και των πολιτικών ελευθεριών των ατόμων, επιτρέποντας παράλληλα τη νόμιμη χρήση των μεταδεδομένων επικοινωνίας. Ωστόσο, η αποτελεσματικότητα αυτών των μέτρων εξαρτάται από την εφαρμογή και την επιβολή τους, και η συνεχής αξιολόγηση και προσαρμογή θα είναι απαραίτητη για την αντιμετώπιση νέων προκλήσεων και κινδύνων στην ψηφιακά προηγμένη κοινωνία.

Β] ΔΙΚΑΙΩΜΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΕ ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ

1. ΚΑΤΟΧΥΡΩΣΗ ΤΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΗΝ ΕΘΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ- ΕΜΒΕΛΕΙΑ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ: Η ΠΡΟΒΛΗΜΑΤΙΚΗ ΤΩΝ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ

1.1 Άρθρο 19 Σύνταγμα

Το άρθρο 19 του Ελληνικού Συντάγματος παρέχει ισχυρή προστασία για το απόρρητο των επιστολών και της ελεύθερης απάντησης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο αυτή διεξάγεται. Η συνταγματική διάταξη εγγυάται το απόλυτο απαραβίαστο του απορρήτου της επικοινωνίας, τονίζοντας τη σημασία της διασφάλισης των δικαιωμάτων των ατόμων στην ιδιωτική ζωή και την ελευθερία της επικοινωνίας. Το άρθρο αναγνωρίζει επίσης ότι ο νόμος ορίζει τις εγγυήσεις των δικαστικών αρχών και επιτρέπει εξαιρέσεις από το απόρρητο σε υποθέσεις που σχετίζονται με την εθνική ασφάλεια ή τη διερεύνηση ιδιαίτερα σοβαρών εγκλημάτων (Ελληνικό Σύνταγμα, άρθρο 19).

1.1.1 Απαρβίαστο Ιδιωτικότητα και Ελευθερία Επικοινωνίας

Το άρθρο 19, παράγραφος 1 του Ελληνικού Συντάγματος ορίζει ότι το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απολύτως απαραβίαστο. Αυτή η αρχή επιβεβαιώνει το θεμελιώδες δικαίωμα στην ιδιωτική ζωή, προστατεύοντας την εμπιστευτική επικοινωνία των ατόμων από μη εξουσιοδοτημένη παρέμβαση ή παρακολούθηση. Η διάταξη αναγνωρίζει την εγγενή αξία της ιδιωτικής ζωής και την ελευθερία έκφρασης χωρίς αδικαιολόγητη εισβολή (Ελληνικό Σύνταγμα, άρθρο 19). Το απαραβίαστο του απορρήτου της επικοινωνίας συνεπάγεται ότι τα άτομα έχουν το δικαίωμα να αναμένουν ότι οι επιστολές, οι επικοινωνίες και άλλες μορφές αλληλογραφίας τους θα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη. Υπογραμμίζει τη σημασία της διατήρησης του απορρήτου και της ακεραιότητας της ιδιωτικής επικοινωνίας (Παναγοπούλου, 2023).

Βασικά στοιχεία του άρθρου 19, άρρηκτα συνδεδεμένα μεταξύ τους, είναι: α) η ελευθερία της ανταπόκρισης ή επικοινωνίας και β) το απόρρητο της κάθε μορφής επικοινωνίας.

Αντικείμενο της συνταγματικής προστασίας είναι όχι το ίδιο το μήνυμα, αλλά το απόρρητο του μηνύματος αυτού (Δαδτόγλου, 2012), ενώ απόρρητο σημαίνει το απολύτως μυστικό ή εμπιστευτικό ως προς κάθε τρίτο πρόσωπο, πέραν του έτερου μέρους της επικοινωνίας (Τσόλιας, 2013). Η ανάγκη να συμπεριληφθεί κάθε είδος, μέσο και μορφή επικοινωνίας χωρίς περιορισμό, ακόμα και μελλοντικά μέσα επικοινωνίας, τα οποία οι τεχνολογικές εξελίξεις θα δημιουργούσαν, οδήγησαν στη διατύπωση της διάταξης με γενικό τρόπο.

Περαιτέρω, του συντακτικού νομοθέτη μη διακρίνοντας, στην έννοια της «επικοινωνίας» υπάγεται το επικοινωνιακό γεγονός σε όλη του την έκταση, ήτοι τόσο το περιεχόμενο αυτής όσο και τα στοιχεία που εξατομικεύουν τις περιστάσεις υπό τις οποίες λαμβάνει χώρα αυτή, δηλαδή τα μεταδεδομένα επικοινωνίας (Μαρκόπουλος, 2018/Δαγτόγλου, 2012). Άλλωστε, όπως ήδη αναφέρθηκε, στην ψηφιακή κοινωνική πραγματικότητα, η διάκριση μεταξύ εσωτερικών και εξωτερικών στοιχείων επικοινωνίας, ήτοι περιεχομένου και μεταδεδομένων, είναι δύσκολο να επιτευχθεί δεδομένης της σημασίας που αυτά έχουν για το απόρρητο και τη μυστικότητα καθότι είναι σε θέση να αποκαλύψουν ουσιώδεις προσωπικές και ευαίσθητες πληροφορίες σχετικά με τα άτομα. Το πλήρες εννοιολογικό περιεχόμενο της έννοιας της ελεύθερης επικοινωνίας προσδιορίζεται εξελικτικά ανάλογα της τεχνολογικής προόδου στον τομέα των ηλεκτρονικών επικοινωνιών και κυρίως του επιπέδου διακινδύνευσης, που συνεπάγεται η τεχνολογική εξέλιξη για την ιδιωτική ζωή, την ελεύθερη ανάπτυξη της προσωπικότητας και την ελευθερία της έκφρασης (Μαρκόπουλος, 2018), έχοντας ως συνέπεια η μη υπαγωγή τους στο προστατευτικό πεδίο της διάταξης να καθιστούσε την προστασία που επιφυλάσσει το σύνταγμα στο απόρρητο της επικοινωνίας - σχεδόν- κενή περιεχομένου.

1.1.2 Εξαιρέσεις για την Εθνική Ασφάλεια και τα Σοβαρά Εγκλήματα

Ενώ το άρθρο 19 εγγυάται το απολύτως απαραβίαστο του απορρήτου της επικοινωνίας, αναγνωρίζει ότι μπορούν να γίνουν εξαιρέσεις σε περιπτώσεις που σχετίζονται με την εθνική ασφάλεια ή τη διερεύνηση ιδιαίτερα σοβαρών εγκλημάτων. Το ελληνικό Σύνταγμα επιτρέπει περιορισμούς στο απόρρητο της επικοινωνίας όταν δικαιολογείται από επιτακτικούς λόγους εθνικής ασφάλειας ή κατά τη διερεύνηση ιδιαίτερα σοβαρών εγκλημάτων.

Αυτές οι εξαιρέσεις αναγνωρίζουν την ανάγκη εξισορρόπησης των δικαιωμάτων ιδιωτικής ζωής με τα νόμιμα συμφέροντα της εθνικής ασφάλειας και της πρόληψης του εγκλήματος. Αναγνωρίζει ότι υπό συγκεκριμένες συνθήκες, το κράτος μπορεί να χρειαστεί να παρακολουθεί ή να έχει πρόσβαση σε ιδιωτικές επικοινωνίες για την προστασία του δημόσιου συμφέροντος και τη διασφάλιση της δημόσιας ασφάλειας (Παναγοπούλου, 2023).

1.1.3 Ανεξάρτητη Αρχή για τη Διασφάλιση του Απορρήτου

Η παράγραφος 2 του άρθρου 19 ορίζει ότι ο νόμος ορίζει τη σύσταση, τη λειτουργία και τις αρμοδιότητες μιας ανεξάρτητης αρχής που έχει ως αποστολή τη διασφάλιση του απορρήτου της ιδιωτικής επικοινωνίας. Αυτή η διάταξη αναγνωρίζει τη σημασία της ύπαρξης ενός ανεξάρτητου φορέα υπεύθυνου για τη διατήρηση και την προστασία των δικαιωμάτων απορρήτου της επικοινωνίας. Στην ανεξάρτητη αρχή έχει ανατεθεί η διασφάλιση του απορρήτου της ιδιωτικής επικοινωνίας και η διασφάλιση ότι τυχόν περιορισμοί ή εξαιρέσεις εφαρμόζονται με νόμιμο και αναλογικό τρόπο. Ο ρόλος της είναι να παρέχει επίβλεψη, να αποτρέπει τις καταχρήσεις και να διατηρεί την ακεραιότητα του απορρήτου της επικοινωνίας (Παναγοπούλου, 2023).

1.1.4 Απαγόρευση αποδεικτικών στοιχείων που αποκτήθηκαν κατά παράβαση του άρθρου 19 και των συναφών άρθρων

Η παράγραφος 3 του άρθρου 19 τονίζει την απαγόρευση χρήσης αποδεικτικών στοιχείων που αποκτήθηκαν κατά παράβαση του άρθρου 19, καθώς και των άρθρων 9 και 9Α του ελληνικού Συντάγματος. Αυτή η διάταξη ενισχύει τη σημασία του σεβασμού των δικαιωμάτων απορρήτου της επικοινωνίας και διασφαλίζει ότι τα αποδεικτικά στοιχεία που αποκτήθηκαν παράνομα ή κατά παράβαση της προστασίας της ιδιωτικής ζωής θεωρούνται απαράδεκτα σε νομικές διαδικασίες. Η απαγόρευση χρησιμεύει ως διασφάλιση για την πρόληψη της εκμετάλλευσης των πληροφοριών που λαμβάνονται μέσω μη εξουσιοδοτημένης ή παράνομης παρέμβασης στο απόρρητο της επικοινωνίας. Υποστηρίζει την ακεραιότητα των νομικών διαδικασιών και διατηρεί τα δικαιώματα των ατόμων σε ένα δίκαιο νομικό σύστημα.

Επομένως, το άρθρο 19 του Ελληνικού Συντάγματος κατοχυρώνει το απόρρητο των επιστολών και την ελευθερία επικοινωνίας, επιβεβαιώνοντας το απαραβίαστο του

απορρήτου της επικοινωνίας. Επιτρέπει εξαιρέσεις σε περιπτώσεις εθνικής ασφάλειας ή σοβαρών εγκλημάτων, αλλά τονίζει την ανάγκη για νομικές εγγυήσεις και εποπτεία. Η απαγόρευση χρήσης αποδεικτικών στοιχείων που αποκτήθηκαν κατά παράβαση αυτού του άρθρου και των σχετικών διατάξεων ενισχύει περαιτέρω τη δέσμευση για την προστασία των δικαιωμάτων απορρήτου της επικοινωνίας και τη διασφάλιση μιας δίκαιης νομικής διαδικασίας .

1.2 Νόμος 2225/1994 – Νόμος 5002/2022

1.2.1 Σκοπός και σημασία της προστασίας του απορρήτου:

Ο εκτελεστικός του άρθρου 19 παρ. 1 του Συντάγματος Νόμος 2225/1994, γνωστός και ως Νόμος περί Απορρήτου των Επικοινωνιών, θεσπίστηκε για την προστασία του απορρήτου της επικοινωνίας εντός της ελληνικής έννομης τάξης. Αναγνωρίζοντας τη θεμελιώδη σημασία της ιδιωτικής ζωής, αυτός ο νόμος στοχεύει στη διασφάλιση της αυτονομίας, της αξιοπρέπειας και της προσωπικής ασφάλειας των ατόμων. Η προστασία του απορρήτου στην επικοινωνία διασφαλίζει ότι τα άτομα μπορούν ελεύθερα να εκφράζονται, να ανταλλάσσουν πληροφορίες και να συμμετέχουν σε ιδιωτικές συνομιλίες χωρίς φόβο μη εξουσιοδοτημένης εισβολής ή παρακολούθησης.

Με το άρθρο 5 του Ν. 5002/2022 με τον τίτλο «*Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*», καταργήθηκαν τα άρθρα 3, 4, 5 και 7 του Ν. 2225/1994 περί άρσης του απορρήτου, οι διατάξεις του οποίου πλέον εφαρμόζονται. Παρακάτω θα γίνει συνοπτική αναφορά στον μέχρι πρότινος εφαρμοζόμενο Ν. 2225/1994, οι διατάξεις και το πνεύμα του οποίου σε γενικό πλαίσιο διατηρήθηκαν χωρίς να εισέλθουμε σε λεπτομερή καταγραφή και σύγκριση των δύο νομοθετημάτων, καθότι εκφεύγει της παρούσης. . Εντούτοις, αποκτά ενδιαφέρον να γίνει μια εντελώς συνοπτική παρουσίαση ορισμένων επιλογών του νομοθέτη που με τη σειρά τους θέτουν προβληματισμούς σχετικά με το γενικό ρυθμιστικό πλαίσιο που αφορά την άρση του απορρήτου των επικοινωνιών.

1.2.2 Ευρύ πεδίο προστασίας

Ο Ν. 2225/1994 επεκτείνει την προστασία του σε διάφορες μορφές ηλεκτρονικών επικοινωνιών. Περιλαμβάνει παραδοσιακά μέσα όπως τα τηλεπικοινωνιακά δίκτυα,

συμπεριλαμβανομένων των τηλεφωνικών συνομιλιών και των μεταδόσεων φαξ. Επιπλέον, καλύπτει σύγχρονες μορφές επικοινωνίας, όπως επικοινωνίες μέσω email, πλατφόρμες άμεσων μηνυμάτων, δίκτυα μέσω κοινωνικής δικτύωσης και άλλες αναδυόμενες τεχνολογίες που διευκολύνουν τις ηλεκτρονικές αλληλεπιδράσεις.

1.2.3 Νομική αναγνώριση των δικαιωμάτων απορρήτου:

Η ιδιωτική ζωή είναι ένα θεμελιώδες δικαίωμα που είναι βαθιά ριζωμένο στις δημοκρατικές κοινωνίες. Ο Ν. 2225/1994 επιβεβαιώνει αυτό το δικαίωμα εντός της ελληνικής έννομης τάξης, αναγνωρίζοντας στα άτομα το δικαίωμα στην ιδιωτικότητα στις επικοινωνίες τους. Αναγνωρίζοντας το απόρρητο ως ακρογωνιαίο λίθο των δημοκρατικών αρχών, ο νόμος ενισχύει τη σημασία του σεβασμού της προσωπικής αυτονομίας των ατόμων και να τους επιτρέπει να ασκούν έλεγχο στις δικές τους πληροφορίες.

1.2.4 Περιορισμοί στην άρση του απορρήτου:

Ενώ το απόρρητο είναι υπέρτατο δικαίωμα, ο Ν. 2225/1994 αναγνωρίζει ότι εξαιρετικές περιστάσεις μπορεί να απαιτούν την άρση του απορρήτου. Στα άρθρα 3 έως 5, ο νόμος καθορίζει ειδικούς όρους και διαδικασίες που πρέπει να ακολουθούνται όταν κρίνονται αναγκαίες επιτρεπόμενες εξαιρέσεις, αυτές οι οποίες μπορεί να προκύψουν σε περιπτώσεις που σχετίζονται με την εθνική ασφάλεια, την πρόληψη και διερεύνηση ιδιαίτερα σοβαρών εγκλημάτων. Έτσι, λοιπόν, εξακολουθεί η προστασία του επικοινωνιακού απορρήτου να είναι ο κανόνας και μόνο στις εξαιρετικές περιπτώσεις και υπό τις προϋποθέσεις που ορίζονται, ο κανόνας αυτός δύναται να καμφθεί τηρουμένης της αρχής της αναλογικότητας που επιτάσσει τέτοιου είδους επεμβατικά και περιοριστικά του δικαιώματος μέτρα να εφαρμόζονται μόνο όταν είναι απολύτως αναγκαία, αφότου έχουν εξαντληθεί τα άλλα ηπιότερα μέσα για την ικανοποίηση του επιδιωκόμενου σκοπού, εν προκειμένω η καταπολέμηση και πρόληψη των περιοριστικά αναφερόμενων εγκλημάτων και η προάσπιση της εθνικής ασφάλειας.

Σημειωτέον ότι κατά το (καταργηθέν) άρθρο 5 παρ. 10 του Ν. 2225/1994: «Το περιεχόμενο της ανταπόκρισης η επικοινωνίας, το οποίο έγινε γνωστό λόγω της άρσης του απορρήτου, **καθώς και κάθε άλλο σχετικό με αυτή στοιχείο** απαγορεύεται, με ποινή ακυρότητας, να χρησιμοποιηθεί και να ληφθεί υπόψη ως άμεση ή έμμεση απόδειξη σε άλλη ποινική, πολιτική,

διοικητική και πειθαρχική δίκη και διοικητική διαδικασία για σκοπό διαφορετικό από εκείνον που είχε καθορισθεί με τη διάταξη.(...).

Κατά την πανηγυρική πλέον διατύπωση του Ν. 5002/2022, σύμφωνα με το άρθρο 4 παρ. 4 αναφορικά με την άρση απορρήτου που διατάσσεται για λόγους εθνικής ασφάλειας «Η διάταξη που επιβάλλει την άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας περιέχει: α) το όργανο που αιτείται την άρση, β) τον σκοπό της άρσης, γ) τα μέσα ανταπόκρισης ή επικοινωνίας στα οποία επιβάλλεται η άρση, **δ) το αντικείμενο της άρσης, δηλαδή τα εξωτερικά στοιχεία της επικοινωνίας ή και το περιεχόμενο αυτής,(...)**», ενώ σύμφωνα με το άρθρο 6 παρ. 4 αναφορικά με την άρση απορρήτου που διατάσσεται για τη διακρίβωση των εκεί αναφερόμενων εγκλημάτων: «Το βούλευμα ή η διάταξη που επιβάλλει την άρση του απορρήτου για διακρίβωση εγκλημάτων, περιλαμβάνει: α) την αστυνομική αρχή ή τον εισαγγελέα ή τον ανακριτή που ζητεί την άρση, β) την αξιόποινη πράξη, γ) τις σοβαρές ενδείξεις ενοχής σε βάρος του προσώπου κατά του οποίου διενεργείται η άρση, δ) την αιτιολογία επιβολής της άρσης, ιδίως την αδυναμία ή ιδιαίτερη δυσχέρεια διακρίβωσης του εγκλήματος με άλλο τρόπο, ε) τον σκοπό της άρσης, στ) τα μέσα ανταπόκρισης ή επικοινωνίας στα οποία επιβάλλεται η άρση, **ζ) το αντικείμενο της άρσης, δηλαδή τα εξωτερικά στοιχεία της επικοινωνίας ή και το περιεχόμενο αυτής,(...)**».

Καθίσταται απολύτως σαφές ότι τα εξωτερικά στοιχεία επικοινωνίας εμπίπτουν στο προστατευτέο περιεχόμενο του άρθρου 19 του Συντάγματος και για την άρση του απορρήτου αναγκαία πρέπει να πληρούνται οι προϋποθέσεις που τάσσει η νομοθεσία και να τηρηθεί η συγκεκριμένη διαδικασία που προβλέπεται, όμοια με αυτή που ακολουθείται για τις περιπτώσεις άρσης του απορρήτου του περιεχομένου της επικοινωνίας.

1.2.5 Νόμος 5002/2022 – Ορισμένοι Προβληματισμοί

Αναμφίβολα οι ρυθμίσεις της ελληνικής νομοθεσίας αναφορικά με την άρση του επικοινωνιακού απορρήτου έρχονταν επιτακτικής ανάγκης για εκσυγχρονισμό και βελτίωση προκειμένου να προσαρμοστούν στο νέο τεχνολογικό περιβάλλον των ηλεκτρονικών επικοινωνιών και να ανταποκριθούν στις υπερνομοθετικές εξελίξεις. Στον απόηχο των αποκαλύψεων της ύπαρξης και της λειτουργίας στην επικράτεια, αλλά υπό άγνωστο έλεγχο, κατασκοπευτικών λογισμικών, της (παράνομης) χρήσης λογισμικού spyware για σκοπούς παρακολούθησης δημοσιογράφων, πολιτικών προσώπων και υψηλόβαθμων

αξιωματικών του Ελληνικού Στρατού (Εθνική Επιτροπή για τα Δικαιώματα του Ανθρώπου, 2023), καθώς και των «επισυνδέσεων», δηλαδή άρσεων του απορρήτου από την ΕΥΠ για λόγους εθνικής ασφάλειας με διάταξης της τοποθετημένης εντός ΕΥΠ εισαγγελικής λειτουργού (Βενιζέλος, 2023), εισήχθη στη Βουλή και τελικά ψηφίστηκε ο πρόσφατος Ν. 5002/2022.

Ήδη από την κατάθεση του σχεδίου νόμου εντοπίστηκαν από πλήθος επιστημόνων του κλάδου δικαιοκρατικά ελλείματα, ενώ η ΑΔΑΕ επεσήμανε μια σειρά προβληματικών ρυθμίσεων. Κατόπιν της ψήφισης του νόμου, η έκδοση της Γνωμοδότησης του (πρώην) Εισαγγελέα του Αρείου Πάγου Ισιδώρου Ντογιάκου υπ' αριθμ. 1/2023 (για την οποία λόγος κατωτέρω) προκάλεσε έντονο διάλογο και θεωρήθηκε τέχνασμα για την παρεμπόδιση των ελέγχων της ΑΔΑΕ στους τηλεφωνικούς παρόχους κατόπιν καταγγελιών των πολιτών, καθότι, μεταξύ άλλων, ανέφερε ότι η ΑΔΑΕ δεν έχει αρμοδιότητα να διαχειρίζεται αιτήματα πολιτών που ζητούν να πληροφορηθούν εάν υπήρξε πράγματι παρακολούθηση των τηλεφώνων τους για λόγους εθνικής ασφάλειας ούτε μπορεί να απευθύνεται για αυτό σε τηλεφωνικούς παρόχους (Παπανικολάου, 2023).

Καίριο σημείο άξιο αναφοράς αποτελούν οι προβλέψεις του άρθρου 4 του Ν. 5002/2022 σχετικά με την άρση του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας. Την τελευταία αυτή έννοια -κατεξοχήν αόριστη νομική- ο νομοθέτης επιχειρεί να προσδιορίσει στο άρθρο 3 του Ν. 5002/2022 («(..)Λόγοι εθνικής ασφάλειας» είναι οι λόγοι που συνάπτονται με την προστασία των βασικών λειτουργιών του κράτους και των θεμελιωδών συμφερόντων των Ελλήνων πολιτών, όπως, ιδίως, λόγοι σχετικοί με την εθνική άμυνα, την εξωτερική πολιτική, την ενεργειακή ασφάλεια και την κυβερνοασφάλεια») υιοθετώντας μάλλον έναν ευρύ ορισμό που πιθανώς να μην είναι απόλυτα συμβατός με την πάγια νομολογία του ΕΔΔΑ, σύμφωνα με την οποία η εθνική νομοθεσία για τις μυστικές παρακολουθήσεις πρέπει να είναι επαρκώς σαφής ως προς τους όρους της, ώστε να παρέχει στους πολίτες επαρκείς ενδείξεις σχετικά με τις περιστάσεις υπό τις οποίες και τους όρους υπό τους οποίους οι δημόσιες αρχές είναι εξουσιοδοτημένες να αποφεύγουν τέτοια μέτρα (Συμεωνίδου-Καστανίδου, 2022, με τις εκεί παραπομπές).

Περαιτέρω, διατηρείται το παλιό 'σύστημα της έκδοσης εισαγγελικής διάταξης (και όχι ανάθεσης σε δικαστικό λειτουργό ή δικαστικό συμβούλιο) για άρση απορρήτου για λόγους

εθνικής ασφάλειας κατά βάση στον Εισαγγελέα της ΕΥΠ και του ΔΑΕΕΒ, για το οποίο (σύστημα) είχαν ήδη διατυπωθεί επιφυλάξεις εάν ανταποκρίνεται στις απαιτήσεις για ύπαρξη διαφάνειας και αποτελεσματικής προστασίας του δικαιώματος, ενώ εξακολουθούν να μην προβλέπονται ως αναγκαία στοιχεία της άνω διάταξης που επιβάλλει την άρση, το ονοματεπώνυμο του θιγόμενου (αφήνοντας περιθώριο για μαζικές παρακολουθήσεις πολιτών) και την αιτιολογία λήψης του μέτρου. Εντούτοις, ειδικά ενόψει της σοβαρότητας ενός τέτοιου μέτρου, η υποχρέωση εμπειριστατωμένης αιτιολόγησης της απόφασης αποτελεί εγγενές στοιχείο των αρχών του κράτους δικαίου και της δημοκρατίας, επιβάλλεται από τη συνταγματική αρχή της αναλογικότητας, αποτελεί το μέσο ελέγχου του οργάνου που εξέδωσε την απόφαση για το εάν ενήργησε εντός νομίμου πλαισίου της αρμοδιότητάς του ή εάν προέβη σε κατάχρηση εξουσίας, με αποτέλεσμα τελικά η αιτιολόγηση αυτή να συνιστά «εργαλείο» και απαραίτητη προϋπόθεση για την αποτελεσματική προστασία των δικαιωμάτων των πολιτών.

Συναφώς υψίστης σημασίας κρίνεται το δικαίωμα γνωστοποίησης στο θιγόμενο της λήψης εις βάρος του του μέτρου άρσης του απορρήτου της επικοινωνίας. Ειδικά δε για την περίπτωση που ελήφθη για λόγους προστασίας εθνικής ασφάλειας, η σχετική αρμοδιότητα της ΑΔΑΕ είχε καταργηθεί δυνάμει του Ν. 4790/2021 εγείροντας τότε ζητήματα συμβατότητας του τελευταίου με το σύνταγμα και το ευρωπαϊκό κεκτημένο όπως αποτυπώνεται στη νομολογία του ΕΔΔΑ (Παπανικολάου, 2023). Με την παράγραφο 7 του άρθρου 4 του Ν. 5002/2022 προβλέπεται η δυνατότητα γνωστοποίησης λήψεως του μέτρου κατόπιν υποβολής αιτήματος του θιγόμενου (ερωτάται ωστόσο πώς θα είναι σε θέση ο θιγόμενος να αντιληφθεί τυχόν τέτοιο ενδεχόμενο, ενόψει μυστικότητας του μέτρου) μετά την πάροδο τριών ετών από τη λήξη αυτού, με τη σχετική αρμοδιότητα για την ενημέρωση του θιγόμενου να ανατίθεται πλέον όχι στην ΑΔΑΕ, αλλά σε τριμελές όργανο αποτελούμενο από το διοικητή της ΕΥΠ (ή κατά περίπτωση το διευθυντή της ΔΑΕΕΒ), τον εισαγγελέα της ΕΥΠ (ή της ΔΑΕΕΒ) και τον πρόεδρο της ΑΔΑΕ. Έχει ασκηθεί κριτική σε αυτή τη νομοθετική επιλογή του τριμελούς οργάνου με τη συγκεκριμένη σύνθεση ως αποφασίζοντας την ενημέρωση. Κι αυτό διότι αφενός συμμετέχουν σε αυτό ταυτόχρονα ο ελέγχων (Πρόεδρος ΑΔΑΕ) και ο ελεγχόμενος (Διοικητής ΕΥΠ/Διευθυντής ΔΑΕΕΒ), αφετέρου, κατά πάγια νομολογία του ΕΔΔΑ, ένα από τα κριτήρια που συνεκτιμώνται κατά την αξιολόγηση ενός εθνικού κανονιστικού πλαισίου και για την κρίση περί της συμβατότητάς του με την ΕΣΔΑ είναι η ύπαρξη της πρόβλεψης, μετά τη λήξη της παρακολούθησης και υπό την προϋπόθεση

ότι δε διακυβεύεται πλέον ο σκοπός για τον οποίο διατάχθηκε η λήψη του μέτρου, ότι ο θιγόμενος ενημερώνεται από ανεξάρτητη αρχή με εχέγγυα ανεξαρτησίας ότι ελήφθη εις βάρος του ένα τέτοιο μέτρο (ΑΔΑΕ, 2022). Εν προκειμένω, συμμετέχοντας ο διοικητής και ο εισαγγελέας της ΕΥΠ (ή ο διευθυντής και ο εισαγγελέας της ΔΑΕΕΒ) στην έκδοση απόφασης περί γνωστοποίησης καλούνται να κρίνουν τις συνέπειες των δικών τους πράξεων (ή προκατόχων τους), καθότι αυτοί είναι αρμόδιοι για την απόφαση περί αναγκαιότητας ή μη λήψης του εν λόγω μέτρου. Είναι φανερό ότι μόνη αρμόδια θα πρέπει να είναι η ΑΔΑΕ, γιατί αυτή έχει ορίσει το Σύνταγμα ως ελέγχουσα ανεξάρτητη αρχή, η οποία ασφαλώς θα πρέπει να καλεί σε ακρόαση το διοικητή της ΕΥΠ (ή κατά περίπτωση διευθυντή της ΔΑΕΕΒ) πριν την ενημέρωση ώστε να διαπιστώσει εάν πράγματι δε διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε η λήψη του μέτρου. Επιπροσθέτως, αμφισβητήσεις έχουν διατυπωθεί ως προς τη σκοπιμότητα και την αναγκαιότητα ύπαρξης του (ελάχιστου) χρονικού όριο των τριών ετών από τη λήξη του μέτρου, μετά την πάροδο του οποίου ο πολίτης δύναται να ενημερωθεί, διότι φαίνεται να είναι άνευ λόγου ιδιαίτερα μεγάλο, ενώ ο θιγόμενος θα έπρεπε να ενημερώνεται ευθύς αμέσως με τη λήξη του μέτρου, εφόσον δε διακυβεύεται ο σκοπός της άρσης. Επιπρόσθετα, προκειμένου βέβαια το δικαίωμα της ενημέρωσης να αποκτήσει ουσιαστικό νόημα θα έπρεπε να γνωστοποιείται επιπλέον και ο λόγος για τον οποίο ελήφθη το μέτρο, στοιχείο που δεν προβλέπεται στο Ν. 5002/2022. Κι αυτό διότι χωρίς γνώση της αιτιολογίας, ο θιγόμενος δε θα είναι σε θέση να υπερασπιστεί αποτελεσματικά το δικαίωμά του έναντι τυχόν αδικαιολόγητης, καταχρηστικής και δυσανάλογης εις βάρος του χρήσης του μέτρου ούτε ο τυχόν έλεγχος από την αρμόδια αρχή ή το δικαστήριο λήψης ενός τέτοιου μέτρου μπορεί να είναι πλήρης. Φαίνεται, συνεπώς, να υπάρχει μια διαρκής αποδυνάμωση του δικαιώματος τούτου.

Στο πλαίσιο αυτό, η Γνωμοδότηση του (πρώην) Εισαγγελέα του Αρείου Πάγου υπ'αριθμ. 1/2023 υιοθέτησε το εξής επιχείρημα: εφόσον η ενημέρωση για τυχόν άρση του απορρήτου για λόγους εθνικής ασφάλειας μπορεί να γίνει εάν το ζητήσει ο θιγόμενος μόνον μετά την πάροδο τριετίας και εφόσον η σχετική αρμοδιότητα για την παροχή ενημέρωσης έχει πλέον ανατεθεί σε τριμελή επιτροπή συγκροτούμενη από δυο εισαγγελικούς λειτουργούς και τον πρόεδρο της ΑΔΑΕ, η ΑΔΑΕ δεν έχει πλέον την αρμοδιότητα να ασκεί ελέγχους επί των τηλεπικοινωνιακών παρόχων για την παρακολούθηση τηλεφωνικών επικοινωνιών με νόμιμη «επισύνδεση» (Βενιζέλος Ε., 2023). Χωρίς να υπεισέλθουμε στο ζήτημα περί αρμοδιότητας του Εισαγγελέα του Αρείου Πάγου να γνωμοδοτεί επί τέτοιας φύσης

υποθέσεις κατόπιν ιδιωτικής πρωτοβουλίας -εν προκειμένω το ερώτημα υπεβλήθη από τηλεπικοινωνιακό πάροχο (αναλυτικά επί του ζητήματος ενδεικτικά σε ΧρυσόγONO, Κ. (2023), «Το άρθρο 19 του Συντάγματος υπό τη σκιά του “Μεγάλου Αδερφού”. Ο ν. 5002/2022 και η 1/2023 γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου»), σημειώνεται επί του περιεχομένου της γνωμοδότησης ότι επιχειρείται ένα λογικό άλμα από τον Εισαγγελέα συγχέοντας δύο ρυθμίσεις-νόμους με μη διασταυρούμενα κανονιστικά πεδία: η εν λόγω ρύθμιση του Ν. 5002/2022 σχετικά με το ειδικότερο ζήτημα της ενημέρωσης ουδόλως περιορίζει τις γενικές αρμοδιότητες της ΑΔΑΕ που κατοχυρώνονται στο άρθρο 6 παρ. 1 του ειδικότερου, εκτελεστικού του άρθρου 19 παρ. 1 του Συντάγματος, Ν. 3115/2003 περί αυτεπάγγελτου ή κατόπιν καταγγελίας ελέγχου διενεργούμενου από την ΑΔΑΕ (Δήλωση του Προέδρου της ΑΔΑΕ Χρήστου Ράμμου, 2023). Η ελεγκτική αρμοδιότητα της ΑΔΑΕ απονέμεται σε αυτή απευθείας από το Σύνταγμα, η ερμηνεία των σχετικών με αυτή διατάξεων των τυπικών νόμων δε μπορεί παρά να είναι σύμφωνη με τις επιλογές του συντακτικού νομοθέτη. Σκοπός της συνταγματικής κατοχύρωσης των ανεξάρτητων αρχών είναι η ουσιαστική προστασία τους ώστε η έγκαιρη και αποτελεσματική δράση τους υπέρ των θεμελιωδών δικαιωμάτων των πολιτών να βρίσκεται στο απυρόβλητο έναντι του κοινού νόμου (Τασόπουλος, 2023). Εκτός δε του γεγονότος ότι ουδόλως προκύπτει πως ο νομοθέτης θέλησε έναν τέτοιο περιορισμό, δεν πρέπει να διαφεύγει της προσοχής ότι η αποτελεσματική άσκηση αυτών των γενικών αρμοδιοτήτων συνδέεται από την ημέρα που ιδρύθηκε η ΑΔΑΕ, κατά τρόπο άρρηκτο και πολυποίκιλο, με το συστηματικό έλεγχο των παρόχων και όλων των δημόσιων φορέων, στον τομέα διασφάλισης του απορρήτου των επικοινωνιών έλεγχο, ο οποίος δεν έχει ως μόνο σκοπό την ενημέρωση που προβλέπεται στην παράγραφο 7 του άρθρου 4 του Ν. 5002/2022 (Δήλωση του Προέδρου της ΑΔΑΕ Χρήστου Ράμμου, 2023).

Είναι πασιφανές ότι ο Ν. 5002/2022 επιχειρήσε να αντιμετωπίσει τα πριν της έκδοσής του ανακύπτοντα θέματα της ελληνικής κοινωνικής πραγματικότητας και πολιτικής που άπτονταν της εθνικής ασφάλειας, με τη διατήρηση σχεδόν αυτούσιων των διατάξεων του Ν. 2225/1994, δίχως τελικά τον επί της ουσίας εκσυγχρονισμό της νομοθεσίας στη νέα τεχνολογική πραγματικότητα.

1.3 Προεδρικό Διάταγμα 47/2005 & Νόμος 3471/2006 (Οδηγία 2002/58/EK)

1.3.1 ΠΔ 47/2005: Προστασία του Απορρήτου των Επικοινωνιών

Οι επιμέρους τεχνικές λεπτομέρειες και διαδικασίες άρσης του απορρήτου προσδιορίζονται από το Π.Δ. 47/2005 που εκδόθηκε σύμφωνα με την εξουσιοδότηση του άρθρου 8 Ν. 3115/2003. Με το ως άνω Π.Δ. δόθηκε νομοθετική λύση σε σειρά αμφισβητούμενων ζητημάτων, καθώς περιγράφηκαν σε αυτό αναλυτικά τα είδη και τα στοιχεία της επικοινωνίας, που υπάγονται στην προστασία του απορρήτου, μεταξύ των οποίων και τα εξωτερικά, στα οποία αναφέρεται η διαδικασία άρσης του απορρήτου σύμφωνα με το Νόμο 2225/1994 (Τσόλιας, 2005 / Τσόλιας, 2013) ως πληροφορίες που προσδιορίζουν τις περιστάσεις υπό τις οποίες διενεργείται η επικοινωνία και την εξατομικεύουν.

1.3.2 Νόμος 3471/2006: Προστασία των Θεμελιωδών Δικαιωμάτων στις Ηλεκτρονικές Επικοινωνίες- Συσχετισμός με τα δεδομένα προσωπικού χαρακτήρα

Ο Ν. 3471/2006, ο οποίος ενσωματώνει την Οδηγία 2002/58/EK, στοχεύει στην προστασία των θεμελιωδών δικαιωμάτων των ατόμων, ιδιαίτερα της ιδιωτικής ζωής, με τη θέσπιση κανονισμών για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στις ηλεκτρονικές επικοινωνίες. Ο νόμος διασταυρώνει την προστασία των προσωπικών δεδομένων με τη διασφάλιση του απορρήτου της επικοινωνίας, προβλέποντας στο άρθρο 4 παρ. 1 ότι οποιαδήποτε χρήση υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, προστατεύεται από το απόρρητο των επικοινωνιών, το οποίο μπορεί να αρθεί μόνο υπό τις προϋποθέσεις και τις διαδικασίες που καθορίζονται στο άρθρο 19 του Συντάγματος. Η θέση αυτή επιβεβαιώνεται στην Αιτιολογική Έκθεση που συνοδεύει το νόμο. Περαιτέρω, σύμφωνα με το άρθρο 2 παρ. 3 και 4 του νόμου, δίνονται οι ορισμοί των **δεδομένων κίνησης** (τα οποία είναι ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας κ.ά.) και των **δεδομένων θέσης** (που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη), τα οποία αποτελούν όλα τα προσωπικά στοιχεία των χρηστών, παρέχοντας έναν μη εξαντλητικό ορισμό και ενδεικτική απαρίθμηση των δεδομένων κίνησης και των δεδομένων τοποθεσίας, ευθυγραμμισμένος με τη διατύπωση της Οδηγίας 2002/58/EK. Στο άρθρο 6 παρ. 4 Ν. 3471/2006 προβλέπεται ειδική διαδικασία για τη

νόμιμη επεξεργασία τους - όπως επεξεργασία αυτών μόνον εφόσον αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση του συνδρομητή ή χρήστη, στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μίας υπηρεσίας προστιθέμενης αξίας.

Ο νόμος αναγνωρίζει ότι αυτές οι κατηγορίες δεδομένων, ενώ υποβάλλονται σε επεξεργασία κυρίως για σκοπούς μετάδοσης επικοινωνίας και χρέωσης υπηρεσιών, υπόκεινται σε προστασία της ιδιωτικής ζωής καθότι με βάση τις πληροφορίες αυτές είναι δυνατή η δημιουργία προφίλ ή πορτραίτων των χρηστών των δικτύων ηλεκτρονικής επικοινωνίας, αλλά και γενικότερα, η παρακολούθηση της σχετικής δραστηριότητας των συνδρομητών και χρηστών από την οποία μπορούν να εξαχθούν ποικίλα συμπεράσματα για τους σκοπούς της άμεσης προώθησης προϊόντων και υπηρεσιών, αλλά και για τους σκοπούς της αντεγκληματικής πολιτικής (Ιγγλεζάκης, 2021).

Στο σημείο αυτό αξίζει να σημειωθεί ότι οι διατάξεις για την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα δεν παρουσιάζουν αυτοτέλεια, αλλά εντάσσονται στο γενικότερο πλαίσιο των ρυθμίσεων του ΓΚΠΔ, τις διατάξεις του οποίου εξειδικεύει και συμπληρώνει ο εφαρμοστικός Νόμος 4624/2019 και οι διατάξεις του οποίου εφαρμόζονται για κάθε ζήτημα που δε ρυθμίζεται ειδικότερα από το Νόμο 3471/2006 (άρθρο 3 παρ. 2 αυτού). Η συσχέτιση προσωπικών δεδομένων διαδραματίζει σημαντικό ρόλο στην προστασία της ιδιωτικής ζωής, περιλαμβάνει τη σύνδεση ή τη συσχέτιση διαφορετικών τμημάτων πληροφοριών που σχετίζονται με ένα αναγνωρίσιμο άτομο, επιτρέποντας τη δημιουργία ολοκληρωμένων προφίλ. Αυτή η διαδικασία έχει αν μη τι άλλο επιπτώσεις στο απόρρητο και το απόλυτα απαραβίαστο αυτού.

Σε γενικά πλαίσια, ο ΓΚΠΔ ενισχύει τα δικαιώματα προστασίας δεδομένων και επιβάλλει υποχρεώσεις στους οργανισμούς που χειρίζονται προσωπικά δεδομένα. Εισάγει βασικές αρχές όπως η διαφάνεια (άρθρο 5), ο περιορισμός σκοπού (άρθρο 5), η ελαχιστοποίηση δεδομένων (άρθρο 5) και τα δικαιώματα των ατόμων για πρόσβαση, διόρθωση και διαγραφή των προσωπικών τους δεδομένων (άρθρα 15-17).

Ο ΓΚΠΔ ορίζει ότι ως προσωπικό δεδομένο νοείται κάθε πληροφορία που αναφέρεται σε ένα υποκείμενο δεδομένων, δηλ. ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ταυτοποιήσιμο δε πρόσωπο είναι αυτό του οποίου η ταυτότητα μπορεί να εξακριβωθεί με αναφορά, μεταξύ άλλων, σε δεδομένα θέσης ή επιγραμμικά αναγνωριστικά (άρθρο 4 περ.

1). Ρητά δε ορίζεται ότι η ταυτότητα ενός προσώπου μπορεί να εξακριβωθεί με αναφορά σε δεδομένα θέσης ή επιγραμμικά αναγνωριστικά, όπως είναι οι διευθύνσεις IP και τα αυτοεγκαθιστώμενα αρχεία cookies (που όπως εκτέθηκε ανωτέρω συνιστούν μεταδεδομένα επικοινωνίας) τα οποία μπορεί να χρησιμοποιούνται για τη δημιουργία προφίλ των υποκειμένων των δεδομένων και την ταυτοποίηση τους, όποτε θα πρέπει να θεωρούνται προσωπικά δεδομένα (Ιγγλεζάκης, 2021).

Η συσχέτιση προσωπικών δεδομένων έχει επιπτώσεις στο απόρρητο. Ενώ δίνει τη δυνατότητα στους οργανισμούς να παρέχουν εξατομικευμένες υπηρεσίες και στοχευμένες διαφημίσεις, εγείρονται ανησυχίες σχετικά με τον έλεγχο των ατόμων στα προσωπικά τους στοιχεία και την πιθανότητα δημιουργίας προφίλ και παρείσφρησης στην ιδιωτική ζωή. Η πλήρης συσχέτιση δεδομένων αυξάνει τον κίνδυνο παραβίασης δεδομένων, μη εξουσιοδοτημένης πρόσβασης και κλοπής ταυτότητας.

Για τον μετριασμό αυτών των κινδύνων και τη διασφάλιση της προστασίας της ιδιωτικής ζωής, οι οργανισμοί και οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να τηρούν βασικές αρχές και βέλτιστες πρακτικές. Αυτά περιλαμβάνουν την ελαχιστοποίηση δεδομένων με τη συλλογή και τη διατήρηση μόνο των απαραίτητων δεδομένων, την εφαρμογή αρχών απορρήτου μέσω σχεδιασμού κατά την ανάπτυξη συστημάτων και τεχνολογιών, τη λήψη ενημερωμένης συναίνεσης από άτομα πριν από τη συσχέτιση των δεδομένων τους, την εφαρμογή μέτρων ασφαλείας για τη διαφύλαξη των προσωπικών δεδομένων (άρθρο 32 ΓΚΠΔ) και τον σεβασμό των ατόμων δικαιώματα, όπως το δικαίωμα πρόσβασης, διόρθωσης και διαγραφής των προσωπικών τους δεδομένων (άρθρα 15-17 ΓΚΠΔ).

Με την τήρηση αυτών των αρχών και τη συμμόρφωση με τις σχετικές νομικές διατάξεις, οι οργανισμοί μπορούν να επιτύχουν μια ισορροπία μεταξύ των πλεονεκτημάτων της συσχέτισης δεδομένων και της προστασίας των δικαιωμάτων απορρήτου των ατόμων.

1.4 Νόμος 3917/2011 (Οδηγία 2006/24/EK)

Με το Ν. 3917/2011 ενσωματώθηκε στην εθνική έννομη τάξη η Οδηγία 2006/24/EK αναφορικά με την υποχρέωση των κρατών μελών να θεσπίσουν μέτρα προς το σκοπό διασφάλισης ότι τα δεδομένα κίνησης και θέσης διατηρούνται για συγκεκριμένο χρονικό διάστημα από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών ως αναγκαίο μέσο για την καταπολέμηση

σοβαρών εγκλημάτων. Ο νόμος δε ορίζει το χρονικό αυτό διάστημα σε ένα έτος και ως προς τα εγκλήματα παραπέμπει στον κατάλογο του Ν. 2225/1994 (πλέον Ν. 5002/2022).

Η οδηγία αναμφίβολα παρεμβατική ως αφορώσα όλους τους χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών καθιστώντας τους «υπόπτους», όλα τα μέσα επικοινωνιών, όλα τα δεδομένα κίνησης και θέσης, χωρίς να θεσπίζει σαφείς και ακριβείς κανόνες σχετικά με την έκταση της επέμβασης στα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας δεδομένων προσωπικού χαρακτήρα ακυρώθηκε με την απόφαση Digital Rights Ireland του Δ.Ε.Ε. στις υποθέσεις C-293/12 και C-594/12, το οποίο έκρινε ότι η οδηγία αντιβαίνει στην αρχή της αναλογικότητας. Παρά την κατάργηση της οδηγίας ο Ν. 3917/2011 ακόμα βρίσκεται τυπικά τουλάχιστον σε ισχύ.

Τέλος, ένα ακόμα επιχείρημα από την ελληνική νομοθεσία περί της υπαγωγής των μεταδεδωμένων επικοινωνίας στο πεδίο του προστατευτέου επικοινωνιακού απορρήτου αποτελεί η διάταξη του άρθρου 370Α του Ποινικού Κώδικα. Σύμφωνα με αυτό το άρθρο, οποιαδήποτε αθέμιτη παγίδευση ή παρέμβαση σε συσκευές, συνδέσεις, δίκτυα ή συστήματα υλικού και λογισμικού που χρησιμοποιούνται για την παροχή υπηρεσιών σταθερής ή κινητής τηλεφωνίας αποτελεί αξιόποιο αδίκημα όταν υπάρχει πρόθεση απόκτησης πληροφοριών ή καταγραφής του περιεχομένου τηλεφωνικών συνομιλιών μεταξύ τρίτων, καθώς και λεπτομερειών σχετικά με την τοποθεσία και την κίνηση τέτοιων επικοινωνιών. Η συμπερίληψη δεδομένων κίνησης και τοποθεσίας στο πεδίο εφαρμογής αυτής της ποινικής διάταξης είναι σημαντική, καθώς υπογραμμίζει την αναγνώριση αυτών των στοιχείων ως μέρος του προστατευόμενου περιεχομένου.

Από μια γρήγορη επισκόπηση περιοριζόμενη από τους σκοπούς και το αντικείμενο της παρούσας καθίσταται σαφές ότι η συνεχής αξιολόγηση και προσαρμογή των νόμων περί απορρήτου είναι ουσιαστικής σημασίας ως απάντηση στις τεχνολογικές εξελίξεις και τις κοινωνικές αλλαγές. Είναι απαραίτητες οι τακτικές αξιολογήσεις της νομοθεσίας, η ευθυγράμμιση με τα διεθνή πρότυπα και η παρακολούθηση των εξελισσόμενων προκλήσεων προστασίας της ιδιωτικής ζωής. Η δυναμική φύση των παραβιάσεων της ιδιωτικής ζωής στην ψηφιακή εποχή απαιτεί μια προληπτική προσέγγιση για την αποτελεσματική προστασία των δικαιωμάτων απορρήτου.

1.5 Συμπερασματικές παρατηρήσεις /θέση της γράφουσας

Συμπερασματικά, το ελληνικό νομικό πλαίσιο για την προστασία της ιδιωτικής ζωής στην επικοινωνία, όπως αποδεικνύεται από τη νομοθεσία, όπως ο Ν. 2225/1994, το Π.Δ. 47/2005, ο Ν. 3674/2008 και ο Ν. 3917/2011, αναδεικνύει τη σημασία της προάσπισης των προσώπων και του δικαιώματός τους στο σεβασμό του επικοινωνιακού απορρήτου. Ωστόσο, το ζήτημα των μεταδεδομένων θέτει σημαντικές προκλήσεις σε αυτό το πλαίσιο.

Τα μεταδεδομένα, τα οποία περιλαμβάνουν πληροφορίες σχετικά με συναλλαγές επικοινωνίας, όπως αρχεία καταγραφής κλήσεων, δεδομένα τοποθεσίας και μοτίβα κίνησης, μπορούν να αποκαλύψουν πολύτιμες πληροφορίες σχετικά με την ιδιωτική ζωή και τις δραστηριότητες των ατόμων. Παρά την αναγνώριση της σημασίας της προστασίας των μεταδεδομένων επικοινωνίας, οι υφιστάμενοι νόμοι είτε αφήνουν περιθώρια διαφορετικής ερμηνευτικής εκτίμησης είτε δεν παρέχουν σαφείς ορισμούς ή/και συγκεκριμένες κατευθυντήριες γραμμές σχετικά με το εύρος και τον χειρισμό των μεταδεδομένων στο πλαίσιο προστασίας του επικοινωνιακού απορρήτου.

Για παράδειγμα, βάσει του Ν. 3674/2008, οι πάροχοι τηλεφωνίας υποχρεούνται να υιοθετήσουν πολιτική ασφαλείας και να ορίσουν έναν υπεύθυνο ασφαλείας, αλλά ο νόμος δεν αντιμετωπίζει ρητά την επεξεργασία των μεταδεδομένων. Ομοίως, ο νόμος 3917/2011, ο οποίος μετέφερε την Οδηγία 2006/24/EK στο εθνικό δίκαιο, έχει καταστεί προβληματικός από την ακύρωση της ίδιας της οδηγίας. Αυτή η έλλειψη σαφήνειας και ευθυγράμμισης με τα διεθνή πρότυπα, όπως φαίνεται στην απόφαση Digital Rights Ireland, επιδεινώνει περαιτέρω τις προκλήσεις που σχετίζονται με τα μεταδεδομένα.

Η προβληματική φύση των μεταδεδομένων γίνεται εμφανής όταν εξετάζεται η πιθανότητα κατάχρησης ή κακής χρήσης τους. Χωρίς σαφείς κατευθυντήριες γραμμές, υπάρχει κίνδυνος μη εξουσιοδοτημένης πρόσβασης, παρακολούθησης ή χρήσης μεταδεδομένων για σκοπούς πέρα από αυτό που είναι απαραίτητο και αναλογικό. Αυτό μπορεί να οδηγήσει σε παραβιάσεις των δικαιωμάτων της ιδιωτικής ζωής, υπονομεύοντας τις θεμελιώδεις αρχές της αυτονομίας, της αξιοπρέπειας και της προσωπικής ασφάλειας.

Για την αντιμετώπιση των προκλήσεων των μεταδεδομένων το ελληνικό νομικό πλαίσιο έχει περιθώρια βελτίωσης και αναπροσαρμογής προς το σκοπό παροχής συγκεκριμένων

ορισμών, καθώς και κατευθυντήριων γραμμών και περιορισμών σχετικά με τη συλλογή, τη χρήση και τη διατήρηση των μεταδεδομένων. Αυτό μπορεί να περιλαμβάνει ευθυγράμμιση με διεθνή πρότυπα, όπως ο ΓΚΠΔ, ο οποίος προσφέρει ολοκληρωμένες διατάξεις για την προστασία των προσωπικών δεδομένων, συμπεριλαμβανομένων των μεταδεδομένων.

Επιπλέον, είναι σημαντικό να θεσπιστούν και εφαρμοσθούν δικλείδες ασφαλείας προκειμένου να εξασφαισθεί ότι η πρόσβαση, η χρήση και η επεξεργασία από ιδιώτες, εταιρείες και κυβερνήσεις θα γίνονται μόνο σύμφωνα με τις αρχές της αναγκαιότητας και της αναλογικότητας. Αυτό θα μπορούσε να περιλαμβάνει την εφαρμογή αυστηρών διαδικασιών εξουσιοδότησης, τη διενέργεια τακτικών ελέγχων και την επιβολή κυρώσεων για μη εξουσιοδοτημένη πρόσβαση ή κακή χρήση μεταδεδομένων.

Αντιμετωπίζοντας την προβληματική φύση των μεταδεδομένων στο νομικό πλαίσιο, η Ελλάδα μπορεί να προστατεύσει καλύτερα τα δικαιώματα της ιδιωτικής ζωής των ατόμων, να ενισχύσει την εμπιστοσύνη στα ψηφιακά συστήματα επικοινωνίας και να υποστηρίξει τις δημοκρατικές αξίες στην ψηφιακή εποχή. Είναι επιτακτική ανάγκη για τους νομοθέτες και τις ρυθμιστικές αρχές να αντιμετωπίσουν προληπτικά αυτές τις προκλήσεις και να διασφαλίσουν ότι το απόρρητο παραμένει θεμελιώδες δικαίωμα στο εξελισσόμενο τοπίο της ηλεκτρονικής επικοινωνίας.

2. Η ΕΠΙΧΕΙΡΗΜΑΤΟΛΟΓΙΑ ΠΕΡΙ ΤΗΣ ΥΠΑΓΩΓΗΣ ΤΩΝ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ

2.1 Γνωμοδότηση ΑΔΑΕ 1/2005

Η Γνωμοδότηση 1/2005 της ΑΔΑΕ παρέχει κατευθύνσεις αναφορικά με την ερμηνεία και την εφαρμογή των ουσιαστικών και διαδικαστικών προϋποθέσεων που τάσσει το άρθρο 19 του Συντάγματος και ο Ν. 2225/1994 περί άρσης του απορρήτου. Η γνωμοδότηση εκδόθηκε ύστερα από αναφορές των παρόχων υπηρεσιών κινητής τηλεφωνίας σύμφωνα με τις οποίες οι δικαστικές και ανακριτικές αρχές αιτούνταν την κοινοποίηση σε αυτές των στοιχείων επικοινωνίας των συνδρομητών των εν λόγω υπηρεσιών δίχως όμως την τήρηση της διαδικασίας για την άρση του απορρήτου ισχυριζόμενες ότι τα ανωτέρω στοιχεία (αναλυτική κατάσταση εισερχομένων και εξερχομένων κλήσεων, χρόνο συνδιάλεξης κλπ), «εξωτερικά

στοιχεία της επικοινωνίας» όπως η ΑΔΑΕ αναφέρει, υπάγονται στην έννοια των προσωπικών δεδομένων για τα οποία δε βρίσκει εφαρμογή η συνταγματική αυτή διάταξη.

Η γνωμοδότηση υποστηρίζει ότι ήδη ακόμα από τη διατύπωση της άνω συνταγματικής διάταξης, η οποία δε διακρίνει σε εσωτερικά και εξωτερικά στοιχεία αλλά κηρύττει το απόλυτα απαραβίαστο της ελεύθερης επικοινωνίας, καθώς και οι σχετικοί εθνικοί νόμοι που (έως κατά το χρόνο της γνωμοδότησης) είχαν εκδοθεί, στους οποίους κάνει ειδική μνεία, οι αποφάσεις της ίδιας της ανεξάρτητης αρχής, όπως και τα ενωσιακά νομοθετικά κείμενα δεν αφήνουν ουδέν περιθώριο αμφισβήτησης της υπαγωγής των εξωτερικών στοιχείων στο προστατευτικό πεδίο του επικοινωνιακού απορρήτου, διαπίστωση η οποία αποτυπώνεται στη δικαστηριακή πρακτική. Η ΑΔΑΕ καταλήγει ότι δε μπορεί παρά να προστατεύεται όλο το επικοινωνιακό γεγονός, τόσο το περιεχόμενο της επικοινωνίας, όσο και κάθε πληροφορία που προσδιορίζει τους όρους και τις περιστάσεις υπό τις οποίες αυτή διενεργείται.

Ως εκ τούτου η άρση του απορρήτου των λεγόμενων εξωτερικών στοιχείων της επικοινωνίας θα πρέπει να τηρεί αυστηρά τις διαδικασίες που περιγράφονται στον νόμο.

2.2 Γνωμοδότηση ΕισΑΠ 6/2008

Συναφής είναι η Γνωμοδότηση του τότε Εισαγγελέα του Αρείου Πάγου, Κ. Καρούτσου υπ' αριθμ. 6/2008, η οποία σχετίζεται με την εργαστηριακή επεξεργασία από τις ανακριτικές αρχές των αποθηκευμένων δεδομένων σε σκληρό δίσκο Η/Υ ή άλλο υλικό φορέα δεδομένων. Υποστηρίζεται ότι εάν αυτά τα αποθηκευμένα δεδομένα σχετίζονται με κάποια μορφή ανταπόκρισης ή επικοινωνίας, θα πρέπει να εμπίπτουν στη σφαίρα του απορρήτου, υπογραμμίζοντας την ανάγκη τήρησης των προϋποθέσεων και των διαδικασιών για την άρση του απορρήτου των επικοινωνιών, όπως περιγράφονται στους Ν. 2225/1994, Ν. 3115/2003 και Π.Δ. 47/2005.

Η γνώμη ευθυγραμμίζεται με την ιδέα ότι τα δεδομένα που είναι αποθηκευμένα σε σκληρό δίσκο Η/Υ ή άλλο υλικό φορέα δεδομένων συνυφασμένα με το γεγονός της επικοινωνίας συνιστούν μέρος της ιδιωτικής ζωής του προσώπου και του δικαιώματός του να διατηρούνται απόρρητα και εμπιστευτικά.

Ενώ η εν λόγω γνωμοδότηση παρέχει μια ερμηνεία της επεξεργασίας των αποθηκευμένων δεδομένων σε σχέση με την εμπιστευτικότητα, δεν κατέστησαν ιδιαίτερα εύληπτες οι έννοιες

του εύρους και ο ορισμός της «κάποιας μορφής απάντησης ή επικοινωνίας» δεδομένου ότι η γνωμοδότηση δεν παρέχει σαφή κριτήρια ή παραδείγματα για τον προσδιορισμό των τύπων αποθηκευμένων δεδομένων που θα εμπίπτουν σε αυτήν την κατηγορία. Καθώς η τεχνολογία εξελίσσεται, η διάκριση μεταξύ δεδομένων που σχετίζονται με την επικοινωνία και άλλων τύπων δεδομένων γίνεται θολή γεγονός που θα καταστήσει αναγκαία μια πιο διαφοροποιημένη προσέγγιση για τον προσδιορισμό της δυνατότητας εφαρμογής της προστασίας του απορρήτου στα αποθηκευμένα δεδομένα .

Σημειωτέον ότι η επίκληση της γνωμοδότησης στους Ν. 2225/1994, Ν. 3115/2003 και Π.Δ. 47/2005 εγείρει κάποια ερωτήματα σχετικά με την επάρκεια και τη συμβατότητα αυτών των νομικών πλαισίων για την αντιμετώπιση ζητημάτων απορρήτου στο πλαίσιο των αποθηκευμένων δεδομένων. Αυτοί οι νόμοι θεσπίστηκαν πριν από την ευρεία χρήση της ψηφιακής τεχνολογίας και ενδέχεται να μην καλύπτουν πλήρως τις πολυπλοκότητες και τις προκλήσεις που σχετίζονται με την αποθήκευση και την επεξεργασία ψηφιακών δεδομένων. Παράλληλα, η γνωμοδότηση αν και είναι άξια μνείας δεν εξετάζει ρητά το ζήτημα των μεταδεδομένων που επίσης μπορούν να παρέχουν σημαντικές πληροφορίες για την ιδιωτική ζωή των ατόμων.

2.3 ΑΠ 1421/2010

Στο πλαίσιο εκδίκασης ποινικής διαφοράς όπου ο κατηγορούμενος φερόταν ως δράστης του εγκλήματος της εξύβρισης ο Άρειος Πάγος επικύρωσε την απόφαση του εφετείου, το οποίο απέρριψε το αίτημα του συνηγόρου του αναφορικά με την αναζήτηση και προσκόμιση από τον τηλεπικοινωνιακό πάροχο καταλόγου των τηλεφωνικών κλήσεων των εμπλεκόμενων μερών προς απόδειξη των ισχυρισμών του πολιτικώς ενάγοντος. Κατά την κρίση του δικαστηρίου, ο κατάλογος των αριθμών τηλεφώνων θεωρείται στοιχείο που καλύπτεται από το επικοινωνιακό απόρρητο και για την άρση αυτού απαιτείται να συντρέχουν οι προϋποθέσεις του (ισχύοντος τότε) Ν. 2225/1994. Συνεπώς, καθότι το έγκλημα της εξύβρισης δεν υπαγόταν στον κατάλογο των εγκλημάτων για τη διακρίβωση των οποίων ο νόμος προβλέπει τη δυνατότητα άρσης του απορρήτου, το δικαστήριο απεφάνθη ότι δε μπορούσαν να γνωστοποιηθούν από τον πάροχο.

2.4 ΣτΕ 1593/2016

Η απόφαση αυτή τονίζει τη σημασία της τήρησης των συνταγματικών αρχών με το σκεπτικό ότι η αποτροπή πρόσβασης σε πληροφορίες επικοινωνίας είναι ζωτικής σημασίας για τη διασφάλιση των δικαιωμάτων απορρήτου. Η υπόθεση αφορούσε την επιβολή κυρώσεων από την ΑΔΑΕ στον τηλεπικοινωνιακό πάροχο διότι χωρίς να υπάρξει σχετική διάταξη γνωστοποίησε στις ανακριτικές αρχές κατάλογο με τα δεδομένα επικοινωνίας τηλεφωνικής σύνδεσης στα οποία περιλαμβάνονταν οι αριθμοί των κλήσεων, τα ονόματα και οι διευθύνσεις των επικοινωνούντων μερών, καθώς και η ημερομηνία, η διάρκεια και η χρέωση κάθε κλήσης.

Το δικαστήριο επεσήμανε ότι οι πάροχοι τηλεπικοινωνιακών υπηρεσιών έχουν την ευθύνη διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και ο Πάροχος δεν αποτελεί μια «δεξαμενή απόρρητων δεδομένων», η οποία «ξεκλειδώνεται» κάθε φορά που μια αρχή ζητάει πρόσβαση σε αυτά, επικαλούμενη την ιδιότητα της και μόνον ή το γεγονός της διενέργειας ποινικής έρευνας, αλλά αντιθέτως αποτελεί εγγυητή της διαδικασίας άρσης του απορρήτου, παράλληλα με την Α.Δ.Α.Ε., και οφείλει να αρνηθεί να χορηγήσει τα σχετικά δεδομένα, έχοντας την υποχρέωση να εξετάζει ακόμη και την τυπική νομιμότητα των σχετικών αιτημάτων, ενέργεια σύμφωνη με τις συνταγματικές και ευρωπαϊκές διατάξεις για την διασφάλιση του απορρήτου των επικοινωνιών (Τσόλιας, 2016).

Το ΣτΕ έκρινε ότι το απόρρητο της επικοινωνίας προστατεύεται έναντι πάντων καλύπτοντας στο σύνολό του το επικοινωνιακό γεγονός, δηλαδή όχι μόνο το περιεχόμενο της επικοινωνίας (φωνή, ιστοσελίδα κ.λπ.), αλλά και τα συναφώς παραγόμενα δεδομένα επικοινωνίας που προσδιορίζουν τις συνθήκες επικοινωνίας και την εξατομικεύουν (όπως πληροφορίες για τον τόπο, τον χρόνο, τη διάρκεια, στοιχεία ταυτότητας και διευθύνσεων επικοινωνούντων μερών κ.λπ.). Διαπίστωσε ότι από την επεξεργασία όλων τα ανωτέρω στοιχείων συντρέχει άμεσος κίνδυνος για τα άτομα να καταστούν γνωστές σε τρίτους πληροφορίες για αυτά, εντελώς προσωπικές και ιδιωτικές, που μπορούν να αφορούν ιδιαίτερες πτυχές της ζωής και της προσωπικότητάς τους επιτρέποντας κατά αυτόν τον τρόπο την εισβολή στα ιδιωτικά τους άδυτα. Το ΣτΕ επεσήμανε πως ενόψει του ότι ο συνταγματικός νομοθέτης εγγυάται ένα περιβάλλον ιδιαίτερα αυξημένης προστασίας της εμπιστευτικότητας κατά τη διεξαγωγή της επικοινωνίας και, συνακόλουθα, της ιδιωτικής

ζωής, η μη θεώρηση των δεδομένων της επικοινωνίας ως στοιχείο του προστατευτέου επικοινωνιακού απορρήτου είναι μάλλον «κοινωνικά επικίνδυνη».

Εν τέλει, το ΣτΕ κατέληξε στο συμπέρασμα ότι τα παρελθοντικά (αποθηκευμένα) δεδομένα κίνησης και θέσης στον τομέα των ηλεκτρονικών επικοινωνιών υπάγονται στην προστασία του απορρήτου ώστε η πρόσβαση και η χορήγησή τους από τους παρόχους προς τις αρμόδιες εισαγγελικές και ανακριτικές αρχές επιτρέπεται μόνο κατόπιν έκδοσης της σχετικής διάταξης περί άρσης του απορρήτου (Τσόλιας, 2017).

2.5 Βούλευμα ΠλημμΑΘ 613/2016

Το Συμβούλιο εξέτασε το ζήτημα αν εμπίπτουν ή όχι στην προστατευτική σφαίρα του απορρήτου της επικοινωνίας, ώστε αναλόγως να απαιτείται ή όχι για την εργαστηριακή επεξεργασία τους, ανεύρεση και τελικά νόμιμη χρήση αυτών σε δίκη, η διαδικασία άρσης του απορρήτου των επικοινωνιών, των αρχείων εκείνων, εν προκειμένω αρχείων πορνογραφίας ανηλίκων, που είναι αποθηκευμένα σε μια υπηρεσία αποθήκευσης στο νέφος (cloud storage), όπως dropbox, skydrive, google drive κτλ, με τα οποία ήταν συνδεδεμένοι υπολογιστές και κινητά τηλέφωνα υπόπτου για διακίνηση υλικού παιδικής πορνογραφίας.

Το Συμβούλιο (κατά τη γνώμη της πλειοψηφίας) διαπίστωσε ότι για την περίπτωση της νεφοϋπολογιστικής όπου τα δεδομένα αποθηκεύονται σε έναν απομακρυσμένο, εξωτερικό, σκληρό δίσκο, στον οποίο αυτά αποστέλλονται μέσω δικτύου, η αποστολή αυτών των δεδομένων στο νέφος συνιστά επικοινωνία και συνεπώς, τίθεται θέμα άρσης του απορρήτου της επικοινωνίας που προστατεύονται συνταγματικά βάσει του άρθρου 19 Συντ. Συνακόλουθα, αναφορικά με το στην παρούσα εξεταζόμενο ζήτημα των μεταδεδομένων επικοινωνίας, έγινε δεκτό ότι πρέπει να τηρηθεί η διαδικασία των άρθρων 4 παρ. 4 και 5 του Ν. 2225/1994 διατάσσοντας την άρση του απορρήτου των επικοινωνιών, κάνοντας ορισμένες επισημάνσεις (παραπέμποντας στο νομοθετικό καθεστώς των Ν. 2225/1994, Ν. 3917/2011, Ν. 3471/2006, Π.Δ. 47/2005): σε σχέση με το ζήτημα αν το απόρρητο καλύπτει τα εξωτερικά δεδομένα επικοινωνίας, διαπίστωσε ότι η κρατούσα άποψη δέχεται ότι τα εξωτερικά δεδομένα ταυτοποίησης προστατεύονται ως απόρρητη επικοινωνία κι αυτό διότι βρισκόμαστε αντιμέτωποι με την «τεχνολογική εξομοίωση των πληροφοριών που αφορούν το περιεχόμενο της επικοινωνίας με εκείνα που αναφέρονται στα εξωτερικά δεδομένα αυτής».

3. Η ΕΠΙΧΕΙΡΗΜΑΤΟΛΟΓΙΑ ΠΕΡΙ ΤΗΣ ΜΗ ΥΠΑΓΩΓΗΣ ΤΩΝ ΜΕΤΑΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ

3.1 Γνωμοδοτήσεις ΕισΑΠ 9/2009, 12/2009 & 9/2011

Στο πλαίσιο διερεύνησης από τις εισαγγελικές και ανακριτικές αρχές εγκλημάτων που σχετίζονταν με κακόβουλη/ενοχλητική επικοινωνία και σε απάντηση των ερωτημάτων που κατά καιρούς τέθηκαν από αυτές απευθυνόμενες προς τους εισαγγελείς του Αρείου Πάγου, εκδόθηκαν κατά σειρά σχετικές γνωμοδοτήσεις προκειμένου να απαντηθεί το κύριο ερώτημα του εάν οι πάροχοι τηλεπικοινωνιακών υπηρεσιών υποχρεούνται να παρέχουν στις ανακριτικές αρχές πληροφορίες αναφορικά με τα εξωτερικά στοιχεία επικοινωνίας των προσώπων που ενεργούν τηλεφωνικές κλήσεις εξυβριστικού κι απειλητικού χαρακτήρα.

Στις γνωμοδοτήσεις του 9/2009, 12/2009 και 9/2011, οι Εισαγγελείς του Αρείου Πάγου εξέφρασαν την άποψη ότι οι προστατευτικές διατάξεις του νόμου σχετικά με το απόρρητο των επικοινωνιών δεν επεκτείνονται α) στις επικοινωνίες μέσω διαδικτύου και β) στα εξωτερικά στοιχεία της επικοινωνίας οι οποίες εκδόθηκαν εξ αφορμής της αντιμετώπισης του ζητήματος πρόσβασης των προανακριτικών αρχών σε δεδομένα ταυτοποίησης κακόβουλων ή ενοχλητικών καλούντων, ασχολήθηκαν και με το ζήτημα των μεταδεδομένων επικοινωνίας, υποστηρίζοντας ότι ως απόρρητο της επικοινωνίας νοείται αυτό που προστατεύεται σύμφωνα με τις ποινικές διατάξεις χωρίς να ληφθεί υπόψη ούτε το τότε Ευρωπαϊκό νομοθετικό πλαίσιο ούτε όμως και η νομολογία του Ε.Δ.Δ.Α., με την οποία είχε λυθεί ad hoc το ζήτημα ήδη από το 1984 (Τσόλιας, 2013).

Αρχικά, στη Γνωμοδότηση 9/2009, ο τότε Εισαγγελέας του Αρείου Πάγου Γ. Σανιδάς, υποστήριξε ότι η επικοινωνία μέσω του Διαδικτύου είναι εξ ορισμού επικοινωνία σε δημοσιότητα, εκτός εάν έχει χρησιμοποιηθεί ειδική διαδικασία διαφύλαξης του απορρήτου. Τούτο π.χ. ισχύει όταν μέσω της ιστοσελίδας έχει δημιουργήσει κάποιος ένα απόρρητο προφίλ, στο οποίο θα έχει δικαίωμα πρόσβασης ο ίδιος και κάποιο ή κάποια συγκεκριμένα πρόσωπα που έχει επιλέξει και έχουν τα απαραίτητα «κλειδιά». Κατά συνέπεια, όταν μέσω του Διαδικτύου τελείται κάποιο έγκλημα, δεν απαιτείται να τηρηθούν οι διατάξεις περί άρσης απορρήτου για να εντοπιστούν τα ηλεκτρονικά ίχνη του προσώπου που το τέλεσε και τελικά και το ίδιο το πρόσωπο. Πηγαίνοντας ένα βήμα παραπέρα, η γνωμοδότηση υποστηρίζει ότι η προστασία που επιφυλάσσει το άρθρο 19 του Συντάγματος στο απόρρητο

της επικοινωνίας δεν εκτείνεται στα εξωτερικά στοιχεία της επικοινωνίας, διότι σε αντίθετη περίπτωση θεωρεί ότι θα ήταν αδύνατος ή ιδιαίτερος δυσχερής ο εντοπισμός των δραστών εγκλημάτων στις κρινόμενες εκεί υποθέσεις εγκλημάτων κακόβουλων κλήσεων, απειλητικών ή υβριστικών μηνυμάτων με συνέπεια την αδυναμία προστασίας των πολιτών. Κατά τα διαλαμβανόμενα στην ανωτέρω γνωμοδότηση, θεωρείται ότι το Π.Δ. 47/2005 με τις διατάξεις του οποίου επεκτάθηκε το απόρρητο των επικοινωνιών στις επικοινωνίες μέσω διαδικτύου και στα εξωτερικά στοιχεία της επικοινωνίας είναι ανίσχυρο κατά το σημείο αυτό, διότι αφενός έρχονται σε αντίθεση προς το άρθρο 19 του Συντάγματος, αφετέρου έχουν εκδοθεί καθ' υπέρβαση νομοθετικής εξουσιοδότησεως. Επιπροσθέτως, υποστηρίζεται αναφορικά με το άρθρο 4 του Ν. 3471/2006, ο οποίος ενσωμάτωσε την Οδηγία 2002/58/ΕΚ και ορίζει ότι τα δεδομένα κίνησης εντάσσονται στο απόρρητο των επικοινωνιών κατισχύει της διάταξης του άρθρου 19 του συντάγματος. Κατά συνέπεια, ο Εισαγγελέας διατύπωσε τη γνώμη ότι οι αρχές επιβολής του νόμου και οι εισαγγελείς έχουν το δικαίωμα να αναζητούν τα δεδομένα χρηστών αυτών των υπηρεσιών καθώς και τα εξωτερικά στοιχεία μιας επικοινωνίας ή τα ηλεκτρονικά ίχνη των χρηστών του διαδικτύου από τους αντίστοιχους παρόχους των υπηρεσιών χωρίς να τηρούν τις κατάλληλες νόμιμες διαδικασίες για την άρση του απορρήτου.

Παρόμοια ήταν η προσέγγιση που ακολουθήθηκε αργότερα στην Γνωμοδότηση 12/2009 του τότε Εισαγγελέα του Αρείου Πάγου Ι. Τέντε σχετικά με τη μη υπαγωγή των εξωτερικών στοιχείων της επικοινωνίας στην προστασία του απορρήτου σε περιπτώσεις επικοινωνιών όπου τελούνται εγκληματικές πράξεις, τις κακόβουλες κλήσεις (εξυβριστικές, απειλητικές). Θεωρεί, λοιπόν, ο Εισαγγελέας ότι κατόπιν παραγγελίας εισαγγελικού ή δικαστικού λειτουργού (και όχι αστυνομικού υπαλλήλου) τα εξωτερικά στοιχεία της κακόβουλης επικοινωνίας μπορούν να χορηγούνται από τους παρόχους των υπηρεσιών, καθότι στις περιπτώσεις αυτές δεν πρόκειται για επικοινωνία προστατευόμενη από το συνταγματικό απόρρητο εξαιτίας του εγκληματικού χαρακτήρα αυτής. Την ίδια άποψη ακολούθησε και η Γνωμοδότηση 9/2011 του τότε Εισαγγελέα του Αρείου Πάγου Α, Κατσιρώδη.

Οι παραπάνω θέσεις προκάλεσαν αντιδράσεις κι έχουν κατακριθεί εξαιτίας της μονοδιάστατης προσέγγισης και του παρωχημένου τρόπου που αντιλαμβάνονται τη φύση και τις ιδιότητες των εξωτερικών στοιχείων της επικοινωνίας, της ελλιπούς τεκμηρίωσης και της αγνόησης σειράς αποφάσεων του Ε.Δ.Δ.Α. και του Δ.Ε.Ε..

Αναμφίβολα, οι αντικρουόμενες ερμηνείες και πρακτικές που αφορούν το απόρρητο των διαδικτυακών επικοινωνιών έχουν θέσει σημαντικές προκλήσεις και ρυθμιστικούς κινδύνους για τους μεσάζοντες που λειτουργούν εντός του νομικού πλαισίου. Το σκεπτικό των παραπάνω γνωμοδοτήσεων έχει ακολουθήσει μεγάλο μέρος των δικαστικών αποφάσεων του Αρείου Πάγου, με το ζήτημα τελικά ακόμα να παραμένει αμφιλεγόμενο. Ενδεικτική παρουσίαση γίνεται παρακάτω.

3.2 ΑΠ 570/2006

Ο Άρειος Πάγος στο πλαίσιο εξέτασης της σχετικής αίτησης αναίρεσης του κατηγορούμενου για το έγκλημα της δωροδοκίας και της νομιμοποίησης εσόδων από εγκληματική δραστηριότητα για πρώτη φορά ασχολήθηκε και έκρινε ότι τα εξωτερικά στοιχεία επικοινωνίας δεν εντάσσονται στο προστατευτικό πεδίο της συνταγματικής διάταξης του άρθρου 19. Συγκεκριμένα, στην εν λόγω υπόθεση ο κατηγορούμενος υποστήριξε ότι το παραπεμπτικό βούλευμα του Συμβουλίου έπασχε απόλυτης ακυρότητας διότι, προκειμένου να στηρίξει την παραπεμπτική του κρίση, το Συμβούλιο έλαβε υπόψη παράνομο αποδεικτικό μέσο, ήτοι το έγγραφο του τηλεπικοινωνιακού παρόχου με το οποίο γνωστοποιούσε κατάλογο αριθμών κλήσεων που πραγματοποιήθηκαν και ελήφθησαν από την τηλεφωνική συσκευή του κατηγορούμενου, καθώς και τα ονόματα των συνδρομητών αυτών των τηλεφωνικών συνδέσεων χωρίς προηγουμένως να έχει τηρηθεί η διαδικασία για την άρση του απορρήτου των επικοινωνιών. Ο Άρειος Πάγος απέρριψε τον παραπάνω ισχυρισμό δεχόμενος χωρίς καμία αιτιολογία και υπό τη μορφή αξιώματος ότι *«το συνταγματικό απόρρητο καλύπτει μόνον το περιεχόμενο των τηλεφωνικών συνδιαλέξεων και όχι και τα εξωτερικά στοιχεία των επικοινωνιών»*. (Τσόλιας, 2013). Η συλλογιστική του δικαστηρίου για να καταλήξει στο συμπέρασμα αυτό δεν διατυπώνεται στην απόφασή του, η μόνη παραπομπή που γίνεται είναι στην υπ' αριθ. 38/2.12.1959 Γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου, η οποία αναφερόταν σε καταργημένο ήδη νομικό πλαίσιο και στο τότε άρθρο 20 του Συντάγματος, παραβλέποντας μάλλον, αφού δεν έκανε καμία παραπομπή, το ισχύον εθνικό και ενωσιακό νομοθετικό καθεστώς όπως είχε διαμορφωθεί από τους Ν. 2225/1994, Π.Δ. 47/2005, Ν. 3471/2006 και τις Οδηγίες 2002/58/ΕΚ και 2002/24/ΕΚ.

3.3 ΑΠ 711/2011 & ΑΠ 78/2021

Αντίστοιχη ήταν και η αντιμετώπιση του ζητήματος σε μεταγενέστερη ποινική υπόθεση του ανώτατου ακυρωτικού δικαστηρίου το οποίο έκρινε ότι «[Μ]ε την αναφερόμενη συνταγματική αρχή (ενν.19Σ) προστατεύεται το περιεχόμενο της επικοινωνίας και όχι η ύπαρξη αυτής και τα εξωτερικά της στοιχεία, δεν είναι δε ανεπίτρεπτη η αποκάλυψη και αναφορά του αριθμού και των στοιχείων του κατόχου των τηλεφωνικών συνδέσεων που κλήθηκαν από ορισμένη τηλεφωνική σύνδεση ή του αριθμού και των στοιχείων του κατόχου των τηλεφωνικών συνδέσεων από τις οποίες ο τελευταίος δέχθηκε τηλεφωνικές κλήσεις» και ως εκ τούτου διαπίστωσε ότι δεν υπάρχει απόλυτη ακυρότητα της διαδικασίας, συνιστάμενη στο ότι το δικαστήριο για την κήρυξη της ενοχής του αναιρεσείουτος έλαβε υπόψη του και αξιοποίησε παράνομα αποδεικτικά μέσα (έγγραφα εταιριών κινητής τηλεφωνίας στα οποία αποτυπώνονταν καταστάσεις εισερχομένων και εξερχομένων κλήσεων), καθώς δεν επήλθε παραβίαση της εκ του άρθρου 19 Συντ. αρχής του απορρήτου των επικοινωνιών, δεδομένου ότι τα ως άνω έγγραφα που αναγνώστηκαν δεν αποτελούσαν παράνομα αποδεικτικά μέσα, αλλά νόμιμα αποδεικτικά στοιχεία που αφορούσαν στα εξωτερικά στοιχεία τηλεφωνικών επικοινωνιών, όπως είναι τα ονοματεπώνυμα των συνδρομητών, καλούντων και καλουμένων, οι αριθμοί των τηλεφώνων και ο χρόνος και ο τόπος των συνδιαλέξεων και όχι το περιεχόμενο των τηλεφωνικών συνδιαλέξεων που προστατεύεται από το συνταγματικό απόρρητο, ενώ αμέσως κατωτέρω το δέχθηκε όλως αντιφατικώς ότι «τα εξωτερικά στοιχεία τηλεφωνικών επικοινωνιών (...) είχαν δε ληφθεί σύμφωνα με το νόμο, αφού είχε προηγηθεί η έκδοση των υπ' αριθμ. (...) διατάξεων του κ. Εισαγγελέα Πλημ/κών Αθηνών που είχαν εκδοθεί σύμφωνα με τις διατάξεις των άρθρων 4 και 6 του Ν. 2225/1994 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας κλπ, όπως είχε τροποποιηθεί με το άρθρο 12 του Ν. 3115.2003, οι οποίες είχαν επικυρωθεί με τα υπ' αριθμ. (...) και (...) βουλευμάτα του Συμβουλίου Πλημ/κών Αθηνών.»(Τσόλιας, 2013). Τη «γραμμή Σανιδά» ακολούθησε και η σχετικώς πρόσφατη απόφαση του Αρείου Πάγου υπ' αριθμ. 78/2021 με ευθεία αναφορά στις ανωτέρω γνωμοδοτήσεις των εισαγγελέων καταλήγοντας στο συμπέρασμα ότι « (...) με την προαναφερόμενη συνταγματική αρχή, προστατεύεται το περιεχόμενο της επικοινωνίας και όχι η ύπαρξη αυτής και τα εξωτερικά της στοιχεία, δεν είναι δε ανεπίτρεπτη η αποκάλυψη και αναφορά του αριθμού και των στοιχείων του κατόχου των τηλεφωνικών συνδέσεων που κλήθηκαν από ορισμένη τηλεφωνική σύνδεση ή του αριθμού και των στοιχείων του κατόχου των τηλεφωνικών συνδέσεων από τις οποίες ο τελευταίος δέχθηκε τηλεφωνικές κλήσεις. Στην

προκειμένη περίπτωση δε, τα ανωτέρω έγγραφα που αναγνώστηκαν, δεν αποτελούσαν παράνομα αποδεικτικά μέσα, αλλά νόμιμα αποδεικτικά στοιχεία που αφορούσαν τα εξωτερικά στοιχεία τηλεφωνικών επικοινωνιών, όπως είναι τα ονοματεπώνυμα των συνδρομητών, καλούντων και καλουμένων, οι αριθμοί των τηλεφώνων και ο χρόνος και ο τόπος των συνδιαλέξεων και όχι το περιεχόμενο των τηλεφωνικών συνδιαλέξεων που προστατεύεται από το Συνταγματικό απόρρητο.».

Τέλος, σημειώνεται ότι η ΑΔΑΕ με τις Γνωμοδοτήσεις της 3α/2002 και 79/2002 υπήγαγε τα τηλεπικοινωνιακά δεδομένα στην προστασία μόνο του 9ΑΣ, όχι του 19Σ, θεωρώντας ότι στην προστασία του απορρήτου υπάγεται μόνο το περιεχόμενο της επικοινωνίας, σε αντίθεση με τη μεταγενέστερη γνωμοδότησή της 1/2005, όπως ήδη ανωτέρω αναφέρθηκε.

Γ] ΔΙΚΑΙΩΜΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΕ ΕΥΡΩΠΑΙΚΟ ΚΑΙ ΔΕΘΝΕΣ ΕΠΙΠΕΔΟ

1. ΚΑΤΟΧΥΡΩΣΗ ΤΟΥ ΔΙΚΑΙΩΜΑΤΟΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΗΝ ΕΝΩΣΙΑΚΗ ΚΑΙ ΔΙΕΘΝΗ ΕΝΝΟΜΗ ΤΑΞΗ- ΣΥΝΤΟΜΗ ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ

Η προστασία του απορρήτου της επικοινωνίας είναι θεμελιώδης πτυχή των ατομικών δικαιωμάτων και έχει κερδίσει σημαντική προσοχή στην Ευρωπαϊκή Ένωση (ΕΕ) και στη διεθνή έννομη τάξη. Προς το σκοπό διαφύλαξης κάθε πτυχής της ιδιωτικότητας των ατόμων, το απόρρητο των ηλεκτρονικών επικοινωνιών δεν καλύπτει μόνο το περιεχόμενο των επικοινωνιών, αλλά και τα μεταδεδομένα, όπως για παράδειγμα πληροφορίες σχετικά με το ποιος επικοινωνήσε με ποιον, πότε και για πόσο χρόνο, καθώς και τα δεδομένα θέσης, όπως για παράδειγμα από πού έγινε η διαβίβαση των δεδομένων (Ευρωπαϊκή Ένωση, 2018).

Το άρθρο 8 της Ευρωπαϊκής Σύμβασης Ανθρωπίνων Δικαιωμάτων (Ε.Σ.Δ.Α.) διαδραματίζει κρίσιμο ρόλο στην προστασία του απορρήτου της επικοινωνίας αναγνωρίζοντας το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας. Θέτει τη βάση για τη διασφάλιση του απορρήτου της επικοινωνίας εντός της ΕΕ και είναι υψίστης σημασίας στις συζητήσεις σχετικά με τη νομιμότητα και τους περιορισμούς των μέτρων επιτήρησης.

Ομοίως, το άρθρο 7 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Χ.Θ.Δ.Ε.Ε.) προστατεύει το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, περιλαμβάνοντας το δικαίωμα στην προστασία του απορρήτου της επικοινωνίας εντός του νομικού πλαισίου της ΕΕ.

Η Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων και το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα περιλαμβάνουν το άρθρο 12 και το άρθρο 17, αντίστοιχα, που διασφαλίζουν το δικαίωμα στην ιδιωτική ζωή, συμπεριλαμβανομένου του απορρήτου της επικοινωνίας, στη διεθνή έννομη τάξη.

Σε μια προσπάθεια δημιουργίας ενός συνεκτικού και ολοκληρωμένου νομικού πλαισίου προστασίας του απορρήτου των επικοινωνιών σε συνδυασμό με την προστασία των δεδομένων προσωπικού χαρακτήρα, η ΕΕ έχει θεσπίσει οδηγίες όπως η Οδηγία 97/66/ΕΚ, η οποία εν συνεχεία αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, e-Privacy) και η Οδηγία 2006/24/ΕΚ αν και ακυρώθηκε αργότερα από το Δικαστήριο της Ευρωπαϊκής Ένωσης (Δ.Ε.Ε.), και οι οποίες αφορούν την προστασία της ιδιωτικής ζωής, την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διατήρηση δεδομένων στις ηλεκτρονικές επικοινωνίες. Περαιτέρω, ο προτεινόμενος κανονισμός e-Privacy στοχεύει να αντικαταστήσει την Οδηγία e-Privacy και να ενισχύσει την προστασία του απορρήτου της επικοινωνίας εντός της ΕΕ, αντιμετωπίζοντας τις αναδυόμενες προκλήσεις και ενισχύοντας τον έλεγχο των ατόμων στα προσωπικά τους δεδομένα.

Κατά πάγια δικαστηριακή πρακτική, τόσο το Δ.Ε.Ε. όσο και το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (Ε.Δ.Δ.Α.) αναγνωρίζουν την ιδιαίτερη φύση και αξία των μεταδεδομένων, τη δυναμική τους να αποκαλύψουν ιδιαίτερα ευαίσθητες πληροφορίες για τα πρόσωπα θέτοντας σε διακίνδυνευση τα δικαιώματα που απολαύουν εντός της ενωσιακής έννομης τάξης και την ιδιωτικότητά τους. Το απόρρητο σύμφωνα με την πλούσια ευρωπαϊκή νομολογία αφορά κάθε στοιχείο της επικοινωνίας, περιεχόμενο και μεταδεδομένα.

Σε αυτό το κεφάλαιο, θα διερευνήσουμε τα παραπάνω νομικά μέσα, οδηγίες και αποφάσεις για να κατανοήσουμε την καταχώριση και την προστασία του δικαιώματος στην ιδιωτική ζωή της επικοινωνίας στην ΕΕ και τη διεθνή έννομη τάξη.

1.1 Άρθρο 8 Ε.Σ.Δ.Α.

Το άρθρο 8 της Ε.Σ.Δ.Α. είναι μια θεμελιώδης διάταξη που προστατεύει το δικαίωμα στην ιδιωτική ζωή, συμπεριλαμβανομένου του απορρήτου της επικοινωνίας. Δηλώνει ότι ο καθένας έχει δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, του σπιτιού του και της αλληλογραφίας του.

Η σημασία του άρθρου 8 της Ε.Σ.Δ.Α. έγκειται στην αναγνώριση της ιδιωτικής ζωής ως θεμελιώδους ανθρώπινου δικαιώματος. Λειτουργεί ως ακρογωνιαίος λίθος για την προστασία του απορρήτου της επικοινωνίας και θεσπίζει ένα νομικό πλαίσιο που προστατεύει το απόρρητο των ατόμων στις επικοινωνίες τους. Το Ε.Δ.Δ.Α. έχει κρίνει σταθερά ότι το τηλεπικοινωνιακό απόρρητο αποτελεί επιμέρους διάσταση της ιδιωτικότητας και αυτή η διάταξη δεν εφαρμόζεται μόνο σε παραδοσιακές μορφές επικοινωνίας, όπως επιστολές και τηλεφωνικές συνομιλίες, αλλά επεκτείνεται και σε σύγχρονα μέσα επικοινωνίας, συμπεριλαμβανομένων των email, των μηνυμάτων κειμένου και των πλατφορμών μέσων κοινωνικής δικτύωσης.

Εν συντομία αναφέρεται ότι το Ε.Δ.Δ.Α. διαδραμάτισε κρίσιμο ρόλο στην ερμηνεία και τη διευκρίνιση του πεδίου εφαρμογής και των περιορισμών του άρθρου 8 Ε.Σ.Δ.Α. σε σχέση με το απόρρητο της επικοινωνίας κρίνοντας ότι οποιαδήποτε παρέμβαση στο απόρρητο της επικοινωνίας πρέπει να πληροί αυστηρές απαιτήσεις, συμπεριλαμβανομένης της ύπαρξης σαφών νομικών διατάξεων, επαρκών διασφαλίσεων και αποτελεσματικών ένδικων μέσων (εντελώς ενδεικτικά απόφαση Weber and Saravia κατά Γερμανίας).

Είναι σημαντικό να σημειωθεί ότι το άρθρο 8 Ε.Σ.Δ.Α. δεν είναι απόλυτο δικαίωμα και μπορεί να υπόκειται σε περιορισμούς. Το Ε.Δ.Δ.Α. έχει αναγνωρίσει ότι ορισμένα έννομα συμφέροντα, όπως η προστασία της εθνικής ασφάλειας ή η πρόληψη του εγκλήματος, μπορεί να δικαιολογούν παρεμβάσεις στο απόρρητο της επικοινωνίας διαμορφώνοντας μια σειρά κριτηρίων προκειμένου να καταγνώσει τη συμβατότητα ή μη των εκάστοτε εθνικών ρυθμίσεων ως προς τις απαιτήσεις της Ε.Σ.Δ.Α.. Ερμηνεύοντας το Δικαστήριο τα κριτήρια που εισάγει το άρθρο 8 παρ. 2 και τα οποία πρέπει να πληρούνται για να θεωρηθεί νόμιμος ο περιορισμός στο δικαίωμα της απόρρητης, ελεύθερης επικοινωνίας, τα κατηγοριοποιεί σε αδρές γραμμές ως ακολούθως: αρχικά, πρέπει ο περιορισμός να προβλέπεται στον νόμο, να ερείδεται δηλαδή, σε κανόνες δικαίου («basis in the domestic law»: ό,τι περιλαμβάνεται στις

πηγές του δικαίου, κατά την εγχώρια τάξη). Επιπροσθέτως, το Δικαστήριο εξετάζει σειρά παραμέτρων συναρτώμενων με την ποιότητα του κανονιστικού πλαισίου, υπό την έννοια του rule of law -ενδεικτικά: συμβατότητα με τις αρχές του κράτους δικαίου, ευχερής προσβασιμότητα και προβλεψιμότητα του κανόνα δικαίου, όπως επίσης και ένα πλέγμα ελάχιστων αναγκαίων εγγυήσεων που αφορούν, μεταξύ άλλων, τον κύκλο των πληττόμενων υποκειμένων, τη φύση της παραβατικής συμπεριφοράς, τις εύλογες υπόνοιες, την ορισμένη διάρκεια του μέτρου, την εποπτεία της διαδικασίας εκ μέρους ανεξάρτητου οργάνου κ.ο.κ. Όλα δε τα προηγούμενα τελούν υπό την αίρεση του αναγκαίου μέτρου, όπως αυτόπροσδιορίζεται από τα συγκείμενα της δημοκρατικής κοινωνίας (Παπανικολάου, 2020, με τις εκεί παραπομπές).

Η ερμηνεία και η εφαρμογή του άρθρου 8 της Ε.Σ.Δ.Α. συνεχίζουν να εξελίσσονται, καθώς αναδύονται νέες προκλήσεις και τεχνολογίες. Για παράδειγμα, στην υπόθεση Big Brother Watch and Others κατά Ηνωμένου Βασιλείου, όπως θα δούμε παρακάτω, το Ε.Δ.Δ.Α. εξέτασε τη συμβατότητα της μαζικής παρακολούθησης επικοινωνιών με το δικαίωμα στην ιδιωτική ζωή. Το Δικαστήριο τόνισε τη σημασία ύπαρξης επαρκών και αποτελεσματικών εγγυήσεων προκειμένου να διασφαλιστεί ότι η παρέμβαση στο απόρρητο της επικοινωνίας δεν είναι αυθαίρετη.

1.2 Άρθρο 7 -Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (Χ.Θ.Δ.Ε.Ε.)

Το άρθρο 7 του Χ.Θ.Δ.Ε.Ε. διαδραματίζει σημαντικό ρόλο στη διασφάλιση του δικαιώματος στην ιδιωτική ζωή, συμπεριλαμβανομένου του απορρήτου της επικοινωνίας, εντός του νομικού πλαισίου της ΕΕ. Αυτή η διάταξη κατοχυρώνει το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, του σπιτιού και των επικοινωνιών, συμπληρώνει και ενισχύει την προστασία που παρέχεται από το άρθρο 8 της Ε.Σ.Δ.Α. στο πλαίσιο της ΕΕ.

Το άρθρο 7 Χ.Θ.Δ.Ε.Ε. αναγνωρίζει τη θεμελιώδη φύση της ιδιωτικής ζωής ως εγγενή πτυχή της ανθρώπινης αξιοπρέπειας και αυτονομίας. Επιβεβαιώνει το δικαίωμα των ατόμων να διατηρούν τον έλεγχο των προσωπικών τους πληροφοριών και των επικοινωνιών τους, προστατεύοντάς τα από αδικαιολόγητη εισβολή ή παρέμβαση. Αυτό περιλαμβάνει την προστασία του απορρήτου των επικοινωνιών και τη διασφάλιση ότι τα άτομα μπορούν να

εκφραστούν ελεύθερα χωρίς φόβο αδικαιολόγητης παρακολούθησης ή εισβολής στην ιδιωτική τους ζωή.

Σημειωτέον ότι ο Χ.Θ.Δ.Ε.Ε. είναι νομικά δεσμευτικός για τα κράτη μέλη της ΕΕ και η ερμηνεία και η εφαρμογή του άρθρου 7 Χ.Θ.Δ.Ε.Ε. υπόκεινται στη δικαιοδοσία του Δ.Ε.Ε. Το Δ.Ε.Ε. διαδραμάτισε κρίσιμο ρόλο στη διασαφήνιση και την ενίσχυση της προστασίας του απορρήτου των επικοινωνιών βάσει του άρθρου 7 Χ.Θ.Δ.Ε.Ε. μέσω των αποφάσεών του.

Στην περίπτωση Digital Rights Ireland που εξετάζεται παρακάτω, το Δ.Ε.Ε. εξέδωσε μια απόφαση ορόσημο σχετικά με τη συμβατότητα της διατήρησης δεδομένων με το δικαίωμα στην ιδιωτική ζωή. Το Δικαστήριο τόνισε τη σημασία του δικαιώματος στην ιδιωτική ζωή στην ψηφιακή εποχή και έθεσε όρια στη διατήρηση και πρόσβαση στα δεδομένα επικοινωνίας των ατόμων, τονίζοντας την ανάγκη για επαρκείς διασφαλίσεις και αναλογικότητα σε τέτοια μέτρα.

Η νομολογία του Δ.Ε.Ε. σχετικά με το άρθρο 7 Χ.Θ.Δ.Ε.Ε. συμβάλλει στην εναρμόνιση και την προστασία του απορρήτου των επικοινωνιών εντός της ΕΕ. Αυτές οι αποφάσεις υπογραμμίζουν τη σημασία της επίτευξης ισορροπίας μεταξύ θεμιτών στόχων, όπως η εθνική ασφάλεια και η πρόληψη του εγκλήματος, και ο σεβασμός των δικαιωμάτων ιδιωτικής ζωής των ατόμων. Ενισχύουν την αντίληψη ότι οποιαδήποτε παρέμβαση στο απόρρητο της επικοινωνίας πρέπει να είναι απαραίτητη, αναλογική και να υπόκειται σε ισχυρές διασφαλίσεις για την προστασία των δικαιωμάτων και ελευθεριών που εγγυάται η ενωσιακή έννομη τάξη.

1.3 Άρθρο 12 -Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα & Άρθρο 17 - Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα

Το άρθρο 12 της Οικουμενικής Διακήρυξης των Ανθρωπίνων Δικαιωμάτων και το άρθρο 17 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα διαδραματίζουν σημαντικό ρόλο στην προάσπιση του δικαιώματος στην ιδιωτική ζωή, συμπεριλαμβανομένου του απορρήτου της επικοινωνίας, εντός της διεθνούς έννομης τάξης. Αυτές οι διατάξεις αναγνωρίζουν τη σημασία της ιδιωτικής ζωής ως θεμελιώδους ανθρώπινου δικαιώματος και παρέχουν τη βάση για την προστασία του απορρήτου της επικοινωνίας παγκοσμίως.

Το άρθρο 12 της Οικουμενικής Διακήρυξης των Ανθρωπίνων Δικαιωμάτων ορίζει ότι «*κανείς δεν πρέπει να υπόκειται σε αυθαίρετες παρεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, το σπίτι ή την αλληλογραφία του*». Επιβεβαιώνει το δικαίωμα των ατόμων να είναι απαλλαγμένα από αδικαιολόγητη εισβολή και παρέμβαση στην ιδιωτική τους ζωή, συμπεριλαμβανομένων των επικοινωνιών τους. Η διάταξη αυτή καθιερώνει την ιδιωτική ζωή ως εγγενή πτυχή της ανθρώπινης αξιοπρέπειας και αναγνωρίζει την ανάγκη προστασίας της.

Ομοίως, το άρθρο 17 του του Διεθνούς Συμφώνου εγγυάται το δικαίωμα στην ιδιωτική ζωή και το απαραβίαστο της αλληλογραφίας. Αναφέρει ότι «*κανείς δεν πρέπει να υποβληθεί σε αυθαίρετη ή παράνομη επέμβαση στην ιδιωτική του ζωή, την οικογένεια, το σπίτι ή την αλληλογραφία του*». Αυτή η διάταξη υπογραμμίζει περαιτέρω τη σημασία του απορρήτου στις προσωπικές επικοινωνίες και την ανάγκη αποτροπής μη εξουσιοδοτημένης πρόσβασης ή παρακολούθησης.

Τα δύο αυτά νομοθετικά κείμενα αποτελούν μέρος του διεθνούς νομικού πλαισίου και αντικατοπτρίζουν τη δέσμευση της διεθνούς κοινότητας να προστατεύσει τα δικαιώματα της ιδιωτικής ζωής, συμπεριλαμβανομένου του δικαιώματος στην προστασία του απορρήτου της επικοινωνίας. Αυτά τα μέσα αναγνωρίζουν ότι το απόρρητο της επικοινωνίας είναι απαραίτητο για τα άτομα να εκφράζονται ελεύθερα, να διατηρούν σχέσεις και να ασκούν τα δικαιώματά τους χωρίς φόβο παρακολούθησης ή εισβολής.

1.4 Οδηγία 97/66/ΕΚ, Οδηγία 2002/58/ΕΚ & Οδηγία 2006/24/ΕΚ

Οι Οδηγίες 97/66/ΕΚ και 2002/58/ΕΚ είναι καθοριστικής σημασίας για την καθιέρωση και τη ρύθμιση της προστασίας του απορρήτου των επικοινωνιών εντός της ΕΕ αντιμετωπίζοντας διάφορες πτυχές της ιδιωτικής ζωής, της επεξεργασίας προσωπικών δεδομένων και της διατήρησης δεδομένων στις ηλεκτρονικές επικοινωνίες.

Ήδη από πολύ νωρίς τα θεσμικά όργανα της ΕΕ είχαν τονίσει τα ζητήματα προσβολής της ιδιωτικότητας και τους κινδύνους για αυτή που συνεπάγεται η χρήση των ψηφιακών μέσων. Για παράδειγμα το Συμβούλιο της Ευρώπης το 1995 εξέδωσε Σύσταση για την προστασία των προσωπικών δεδομένων στον τομέα των τηλεπικοινωνιών, με ιδιαίτερη αναφορά στις τηλεφωνικές υπηρεσίες (ΣτΕ Επιτροπή Υπουργών Συμβούλιο της Ευρώπης, 1995).

Η Οδηγία 2002/58/EK θεσπίστηκε σε αντικατάσταση της Οδηγίας 97/66/EK και με στόχο την προσαρμογή της τελευταίας στις εξελίξεις των αγορών και των υπηρεσιών ηλεκτρονικών επικοινωνιών, εστιάζει ειδικά στην προστασία της ιδιωτικής ζωής και την επεξεργασία δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες. Συμπληρώνει και ενισχύει το γενικό πλαίσιο προστασίας δεδομένων που οριζόταν στην Οδηγία για την Προστασία Δεδομένων (Οδηγία 95/46/EK), πλέον στον Γενικό Κανονισμό για τη Προστασία Δεδομένων (ΓΚΠΔ), δίνοντας έμφαση στην προστασία του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

Η Οδηγία 2002/58/EK, όπως τροποποιήθηκε από την Οδηγία 2009/136/EK, εφαρμοζόμενη στις περιπτώσεις υπηρεσιών επικοινωνιών που παρέχονται σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών διακρίνει τρεις βασικές κατηγορίες δεδομένων, τα οποία δημιουργούνται κατά τη διάρκεια της επικοινωνίας: τα δεδομένα τα οποία συνιστούν το περιεχόμενο των μηνυμάτων που αποστέλλονται κατά τη διάρκεια της επικοινωνίας· τα εν λόγω δεδομένα είναι αυστηρώς εμπιστευτικά· τα δεδομένα που είναι αναγκαία για τη δημιουργία και τη διατήρηση της επικοινωνίας –γνωστά και ως μεταδεδομένα, τα οποία καλούνται «δεδομένα κίνησης» στην οδηγία– όπως πληροφορίες σχετικά με τους συμμετέχοντες στην επικοινωνία, το χρόνο και τη διάρκεια της επικοινωνίας· μεταξύ των μεταδεδομένων, υπάρχουν δεδομένα που αφορούν ειδικά τη θέση της συσκευής επικοινωνίας, γνωστά και ως δεδομένα θέσης. Τα εν λόγω δεδομένα αφορούν ταυτόχρονα και τη θέση των χρηστών των συσκευών επικοινωνίας και έχουν ιδιαίτερη σημασία για τους χρήστες συσκευών κινητής τηλεφωνίας (Ευρωπαϊκή Ένωση, 2018). Προς το σκοπό ενίσχυσης της προστασίας, η Οδηγία 2002/58/EK προβλέπει ως υποχρέωση των κρατών-μελών τη λήψη μέτρων που θα παρεμποδίζουν τη χωρία άδεια πρόσβαση στις επικοινωνίες στοχεύοντας στην προστασία του απορρήτου του περιεχόμενου, καθώς και κάθε δεδομένου που αναφέρεται στην επικοινωνία (προοίμιο 21), ορίζει δε ότι ο τερματικός εξοπλισμός των χρηστών και κάθε πληροφορία αποθηκευμένη σε αυτόν συνιστούν μέρος της ιδιωτικής ζωής (προοίμιο 24). Σύμφωνα με τους ορισμούς που δίνονται, τα δεδομένα θέσης αναφέρονται «στο γεωγραφικό πλάτος, το γεωγραφικό μήκος και το υψόμετρο του τερματικού εξοπλισμού του χρήστη, στην κατεύθυνση της κίνησής του, στο επίπεδο ακρίβειας των πληροφοριών περί της θέσης, στον προσδιορισμό της γεωγραφικής ζώνης του δικτύου στο οποίο βρίσκεται ο τερματικός εξοπλισμός σε μια δεδομένη χρονική στιγμή και στο χρόνο που καταγράφηκαν οι πληροφορίες περί της θέσης» (αιτιολογική σκέψη 14), ενώ τα δεδομένα κίνησης «(...) στη δρομολόγηση, τη

διάρκεια, το χρόνο ή το μέγεθος μιας επικοινωνίας, στο πρωτόκολλο που χρησιμοποιείται, στη θέση του τερματικού εξοπλισμού του πομπού ή του δέκτη, στο δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία, στην αρχή, το τέλος ή τη διάρκεια μιας σύνδεσης» (αιτιολογική σκέψη 15).

Τα δεδομένα αυτά έχουν για τον ενωσιακό νομοθέτη διττή υπόσταση: αποτελούν δεδομένα προσωπικού χαρακτήρα, καθώς και στοιχεία του απορρήτου της επικοινωνίας. Περαιτέρω, κατά το άρθρο 5 αυτής απαγορεύεται «(..) η ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια, σύμφωνα με το άρθρο 15 παράγραφος 1. ». Κατά παρέκκλιση τα ανωτέρω είναι ανεκτά οπότε και τα εθνικά δίκαια δικαιούνται να προβλέψουν εξαιρέσεις και να επιτρέψουν την άρση του απορρήτου των μεταδεδομένων επικοινωνίας κατά το άρθρο 15 παρ. 1 όταν «αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία για τη διαφύλαξη της εθνικής ασφάλειας (δηλαδή της ασφάλειας του κράτους), της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδειάς χρησιμοποίησης του συστήματος ηλεκτρονικών επικοινωνιών, όπως προβλέπεται στο άρθρο 13 παράγραφος 1 της οδηγίας 95/46/EK.».

Συναφώς η εν λόγω οδηγία ασχολείται με το ζήτημα της διατήρησης και επεξεργασίας μεταδεδομένων επικοινωνίας προβλέποντας ότι η διατήρηση και η επεξεργασία των μεταδεδομένων όλων των χρηστών που αφορούν τη χρέωση και τη μετάδοση της επικοινωνίας είναι επιτρεπτή, εφόσον οι πληροφορίες αυτές φυλάσσονται για τόσο διάστημα όσο απαιτείται για τη μετάδοση και την κίνηση και κατά τη διάρκεια της αποθήκευσης πληρούνται οι εγγυήσεις του απορρήτου και τα μεταδεδομένα απαλείφονται ή ανωνυμοποιούνται όταν δεν είναι απαραίτητα για αυτούς τους σκοπούς.

Μετά τις τρομοκρατικές επιθέσεις στη Νέα Υόρκη το 2001, τη Μαδρίτη το 2004 και το Λονδίνο το 2005, επιτακτική προέβλεπε η ανάγκη θέσπισης εξαιρετικών μέτρων για την αποτροπή παρόμοιων εγκληματικών πράξεων, σε επίπεδο ΕΕ. Σημαντική θεωρείται για το σκοπό αυτό η χρήση των δεδομένων των ηλεκτρονικών επικοινωνιών, καθώς από αυτά μπορούν οι διωκτικές αρχές να συναγάγουν χρήσιμα στοιχεία για τη διερεύνηση και δίωξη σοβαρών ποινικών αδικημάτων. Συγκεκριμένα τα μέτρα αυτά αφορούν τη διατήρηση δεδομένων

κίνησης και θέσης από τους παρόχους ηλεκτρονικών επικοινωνιών, στα οποία θα μπορούν να έχουν πρόσβαση οι δικτυικές αρχές. Μετά τα παραπάνω γεγονότα η διατήρηση δεδομένων επιβλήθηκε ως αναγκαιότητα και οδήγησε στη θέσπιση της Οδηγίας 2006/24/EK. (Ιγγλεζάκης, 2021).

Με την Οδηγία 2006/24/EK (Data Retention Directive) εισήχθη γενική υποχρέωση διατήρησης των δεδομένων ηλεκτρονικών επικοινωνιών σε όλα τα κράτη μέλη, σκοπός της οποίας είναι να καθίστανται αυτά διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων. Προστέθηκε στο άρθρ. 15 της Οδηγίας 2002/58/EK η παράγραφος 1α, που ορίζει ότι «η παράγραφος 1 δεν ισχύει για δεδομένα των οποίων τη διατήρηση προβλέπει ρητά η οδηγία 2006/24/EK για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών, όσον αφορά τους σκοπούς του άρθρου 1 § 1 της εν λόγω οδηγίας». Με αυτή επιβάλλεται τριπτή εξαίρεση (triple no-opt), τόσο έναντι των δύο επικοινωνούντων μερών, όσο και έναντι του παρόχου. Αντικείμενο της τριπτώς υποχρεωτικής επεξεργασίας («διατήρησης») δεν είναι βέβαια το περιεχόμενο της επικοινωνίας, αλλά τα λεγόμενα «εξωτερικά δεδομένα, ήτοι συγκεκριμένα όσα δεδομένα «κίνησης», αλλά και «θέσης της ηλεκτρονικής επικοινωνίας είναι αναγκαία για τον προσδιορισμό της πηγής, του προσορισμού της ημερομηνίας, της ώρας, της διάρκειας, του είδους και του εξοπλισμού της ηλεκτρονικής επικοινωνίας, καθώς και της θέσης αυτού.» (Χριστοδούλου, 2014).

Για την ακύρωση της οδηγίας με την απόφαση του Δ.Ε.Ε. στις συνεκδικασθείσες υποθέσεις C-293 και C-594/12 θα γίνει λόγος παρακάτω.

Σε γενικά πλαίσια μέσα από τη νομοθετική λειτουργία των ενωσιακών οργάνων διαφαίνεται η ανάγκη και η προσπάθεια δημιουργίας ενός ολοκληρωμένου νομικού πλαισίου για την προστασία του απορρήτου της επικοινωνίας εντός της ΕΕ. Σκοπός είναι η θέσπιση δικαιωμάτων, υποχρεώσεων και διασφαλίσεων που σχετίζονται με το απόρρητο στις ηλεκτρονικές επικοινωνίες, με στόχο την επίτευξη ισορροπίας μεταξύ των δικαιωμάτων ιδιωτικής ζωής και των έννομων δημόσιων συμφερόντων, όπως η εθνική ασφάλεια και η επιβολή του νόμου.

Μετά από εκκλήσεις για ένα πιο ισχυρό και εναρμονισμένο νομικό πλαίσιο για την προστασία του απορρήτου της επικοινωνίας εντός της ΕΕ, ως απάντηση σε αυτές τις ανησυχίες και για να ευθυγραμμιστεί με τον ΓΚΠΔ, η ΕΕ πρότεινε έναν νέο κανονισμό για την προστασία της ιδιωτικής ζωής ηλεκτρονικών δεδομένων που θα αντικαταστήσει την Οδηγία 2002/58/ΕΚ, τον Κανονισμό e-Privacy. Ο προτεινόμενος κανονισμός στοχεύει στην ενίσχυση της προστασίας της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες αντιμετωπίζοντας τις τεχνολογικές εξελίξεις και παρέχοντας σαφέστερους και πιο ολοκληρωμένους κανόνες για τη συναίνεση, τα μεταδεδομένα και το απόρρητο των επικοινωνιών.

1.5 Κανονισμός e-Privacy

Μετά την ψήφιση του ΓΚΔΠ η Ευρωπαϊκή Επιτροπή υπέβαλε πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) το λεγόμενο Κανονισμό e-Privacy, το τελικό σχέδιο του οποίου έγινε δεκτό από το Συμβούλιο της ΕΕ στις 10/02/2021.

Ο προτεινόμενος κανονισμός αντιπροσωπεύει μια σημαντική εξέλιξη στην προστασία του απορρήτου των επικοινωνιών εντός της ΕΕ. Αποσκοπεί στην αντικατάσταση της υφιστάμενης Οδηγίας 2002/58/ΕΚ και στη δημιουργία ενός πιο ολοκληρωμένου και εναρμονισμένου πλαισίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Ο κανονισμός φιλοδοξεί να αντιμετωπίσει τις εξελισσόμενες προκλήσεις που θέτουν οι ψηφιακές τεχνολογίες και να διασφαλίσει ότι τα δικαιώματα των ατόμων στην ιδιωτική ζωή τηρούνται στην ψηφιακή εποχή. Έρχεται ως *lex specialis* να εξειδικεύσει και να συμπληρώσει τον ΓΚΠΔ. Λόγω του χαρακτήρα του ως κανονισμού και όχι οδηγίας πρόκειται να έχει ευθεία εφαρμογή σε όλα τα κράτη μέλη της. Ο προτεινόμενος κανονισμός για το ηλεκτρονικό απόρρητο βασίζεται στα θεμέλια που θέτει η Οδηγία 2002/58/ΕΚ όμως οι διατάξεις του αποσκοπούν να ρυθμίσουν ζητήματα που αναφύονται στο πεδίο των ηλεκτρονικών επικοινωνιών αναφορικά με την προστασία απορρήτου και των δεδομένων επικοινωνιών των τελικών χρηστών κατά τρόπο ομοιόμορφο, συνεκτικό και υποχρεωτικό σε όλα τα κράτη μέλη της ΕΕ.

Περιεχόμενο επικοινωνίας και εξωτερικά στοιχεία επικοινωνίας βρίσκονται στην ίδια αξιακή κλίμακα και προστατεύονται από το απόρρητο, καθότι μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες που ανήκουν στην ιδιωτική σφαίρα του ατόμου και σχετίζονται με όλο το φάσμα της προσωπικότητάς του. Σύμφωνα με τον Κανονισμό, τα μεταδεδομένα περιλαμβάνουν τα δεδομένα τοποθεσίας της συσκευής που παράγονται στο πλαίσιο της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών και της ημερομηνίας, της ώρας, της διάρκειας και του είδους της επικοινωνίας. Ο όρος εξωτερικά στοιχεία επικοινωνίας απαλείφεται και αντικαθίσταται από τον όρο μεταδεδομένα επικοινωνίας, τα οποία συνιστούν από κοινού με το περιεχόμενό της τα δεδομένα ηλεκτρονικής επικοινωνίας, τα οποία απολαύουν την προστασία του απορρήτου (άρθρα 4 3^α,β,γ, 5,6) επιδιώκοντας έτσι τη μέγιστη ασφάλεια της εμπιστευτικότητας αυτών των πληροφοριών.

2. ΝΟΜΟΛΟΓΙΑΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΝΩΣΙΑΚΗΣ ΕΝΝΟΜΗΣ ΤΑΞΗΣ

2.1 Αποφάσεις Ε.Δ.Δ.Α.

Οι αποφάσεις του Ε.Δ.Δ.Α. ασκούν σημαντική επιρροή στην προστασία του απορρήτου της επικοινωνίας εντός του νομικού πλαισίου της ΕΕ. Το Ε.Δ.Δ.Α. ερμηνεύει τα δικαιώματα που κατοχυρώνονται βάσει της Ε.Σ.Δ.Α., συμπεριλαμβανομένου του δικαιώματος στην ιδιωτική ζωή βάσει του άρθρου 8 της Ε.Σ.Δ.Α.. Αρκετές αποφάσεις ορόσημα έχουν διαμορφώσει το νομικό τοπίο και έχουν δημιουργήσει σημαντικά προηγούμενα. Όπως αναφέρθηκε αν και η προστασία του απορρήτου των επικοινωνιών δεν περιλαμβάνεται ρητά στη γραμματική διατύπωση του άρθρου, κατά πάγια νομολογία, το τηλεπικοινωνιακό απόρρητο θεωρείται πτυχή της ιδιωτικότητας.

2.1.1 Απόφαση *Malone κατά Ηνωμένου Βασιλείου*

Στα πλαίσια των τηλεφωνικών παρακολουθήσεων το Ε.Δ.Δ.Α. ήδη από τη δεκαετία του 1980 εξετάζοντας την υπόθεση *Malone κατά του Ηνωμένου Βασιλείου* είχε δεχθεί ότι τα εξωτερικά στοιχεία της επικοινωνίας υπάγονται στην προστασία του απορρήτου της τηλεφωνικής επικοινωνίας κρίνοντας ότι υπήρξε διπλή παραβίαση του άρθρου 8 της Ε.Σ.Δ.Α. τόσο ως προς την υποκλοπή των τηλεφωνικών συνομιλιών όσο και ως προς την παράδοση στην αστυνομία των στοιχείων της συσκευής που είχε τοποθετηθεί στη συσκευή

του τηλεφώνου του προσφεύγοντος καταγράφοντας τους κληθέντες αριθμούς από τη συγκεκριμένη συσκευή, το χρόνο και τη διάρκεια της κλήσης. Ως προς την υποκλοπή των τηλεφωνικών επικοινωνιών, το Ε.Δ.Δ.Α. διατύπωσε τη θέση ότι η ύπαρξη νόμων και πρακτικής στην Αγγλία και την Ουαλία που καθιέρωναν σύστημα μυστικής παρακολούθησης των επικοινωνιών ισοδυναμεί καθαυτή με «επέμβαση» ανεξαρτήτως του εάν τέτοια μέτρα ελήφθησαν σε βάρος του προσφεύγοντος (παρ. 64). Αναλύοντας το περιεχόμενο του όρου «προβλέπονται υπό του νόμου» το Ε.Δ.Δ.Α. διατύπωσε τη θεώρηση ότι είναι απαραίτητος ο «νόμος» να είναι σαφής στους ορισμούς του, ώστε οι πολίτες να ξέρουν σε ποιες περιστάσεις και με ποιες προϋποθέσεις οι δημόσιες αρχές επιτρέπεται να «επεμβαίνουν» στο δικαίωμα σεβασμού της ιδιωτικής ζωής και της ανταπόκρισης ιδιαίτερα δε δεδομένου ότι τα μέτρα μυστικής παρακολούθησης δεν ελέγχονται από τον παρακολουθούμενο και το κοινό γενικά (Παπαδόπουλος, 2008). Ως προς το ζήτημα της καταγραφής (metering) η οποία με σύγχρονους όρους θα μπορούσε να αποδοθεί ως καταχώριση και αρχειακή αποθήκευση των προσδιοριστικών των περιστάσεων της επικοινωνίας, δεδομένων κίνησης και θέσης, έλκει την πρωτόλεια δικαστηριακή της πραγμάτευση από την εν λόγω απόφαση. Εν προκειμένω, το Δικαστήριο αντιδιέστειλε σε πρώτη φάση την υπό συζήτηση πρακτική προς την παρακολούθηση του εσωτερικού περιεχομένου των επικοινωνιών και συνακόλουθα την εξόρυξη των ουσιαστικών, ανταλλασσόμενων από τα μέρη πληροφοριών, η οποία είναι «ανεπιθύμητη και έκνομη σε μία δημοκρατική κοινωνία πλην εάν υφίσταται νόμιμος λόγος δικαιολόγησής της» (σκ.84). Δεν αρκέστηκε όμως σε μία τέτοια διακηρυκτική οριοθέτηση των εξωτερικών από τα εσωτερικά στοιχεία της επικοινωνίας τύπου *persona grata* και *non grata* σε μία δημοκρατική κοινωνία, αλλά έσπευσε στη συνέχεια να απορρίψει τον ισχυρισμό της βρετανικής κυβέρνησης περί της μη ένταξης της χρήσης των εξαγόμενων από τη συσκευή της μέτρησης πληροφοριών στον πυρήνα του άρθρου 8 Ε.Σ.Δ.Α., τονίζοντας ότι η χωρίς τη συγκατάθεση του υποκειμένου τροφοδότηση των αστυνομικών αρχών με τις πληροφορίες ανέρχεται εξίσου σε παρέμβαση επί του κατοχυρωμένου στη διάταξη δικαιώματος (Λαχανά, 2013). Για το Ε.Δ.Δ.Α. οι ενσωματωμένες στα εξωτερικά στοιχεία της επικοινωνίας πληροφορίες συνιστούν «αναπόσπαστο σύστοιχο των τηλεφωνικών επικοινωνιών» (σκ.64, 86επ.).

Με την απόφαση αυτή το Ε.Δ.Δ.Α. τόνισε την αναγκαιότητα ύπαρξης σαφούς και αποτελεσματικής εσωτερικής νομοθεσίας των κρατών που ρυθμίζουν τις παρεμβάσεις στη δικαιώματα των προσώπων και σταθμίζοντας την ανάγκη αντεγκληματικής πολιτικής και

του σεβασμού των ατομικών δικαιωμάτων απεφάνθη για την υπεροχή των δεύτερων διαπιστώνοντας τα ασαφή και αβέβαια όρια δράσης των βρετανικών αρχών επισημαίνοντας τον κίνδυνο καταχρηστικής άσκησης της εξουσίας τους. Ήταν σαφές για το Ε.Δ.Δ.Α. ότι οι πληροφορίες που δύνανται να εξαχθούν από τα εξωτερικά στοιχεία της επικοινωνίας όπως εν προκειμένω οι αριθμοί, οι κλήσεις, ο χρόνος και η διάρκεια αυτών ανάγονται στην προσωπική σφαίρα του ατόμου, είναι καθαρά ιδιωτικές και η οποιαδήποτε καταγραφή ή παρακολούθησή τους εν αγνοία και χωρίς τη συναίνεση του ατόμου δε μπορεί παρά να αντιτίθεται στο άρθρο 8 της Ε.Σ.Δ.Α..

2.1.2 Απόφαση *Copland* κατά *Ηνωμένου Βασιλείου*

Το Ε.Δ.Δ.Α. εμμένοντας στους βασικούς κανόνες που είχε διατυπώσει από την υπόθεση *Malone* έκρινε περαιτέρω στην *Απόφαση Copland κατά Ηνωμένου Βασιλείου* ότι οι ηλεκτρονικές επικοινωνίες του ατόμου (στις οποίες συγκαταλέγονται η πλοήγηση στο διαδίκτυο και η ηλεκτρονική αλληλογραφία) εμπίπτουν στην έννοια της προστασίας της ιδιωτικής ζωής, σύμφωνα με το άρθρο 8 της Ε.Σ.Δ.Α.. Διαπίστωσε επιπλέον ότι η χρήση διαδικτύου και η αποστολή mails ακόμα και στον εργασιακό χώρο υπάγονται στο προστατευτικό πεδίο της διάταξης. Πιστοί στο δόγμα της καθιερωμένης, δυναμικής και εξελικτικής ανάγνωσης της Σύμβασης ως «ζωντανού εργαλείου το οποίο χρήζει ερμηνείας υπό το φως των τρεχουσών συνθηκών», οι Ευρωπαίοι δικαστές προσάρμοσαν δικαιοπλαστικά το περιεχόμενο του άρθρου 8 παρ. 1 στους νέους πραγματολογικούς όρους διακινδύνευσης της προσωπικής αυτονομίας που αναδύονται μέσα από το παγκοσμιοποιημένο περιβάλλον της διαδικτυακής πραγματικότητας, διευρύνοντας την εμβέλειά του με την προσθήκη (ως «λογικά συναγόμενων») και των συναφών με τις περιηγήσεις στο Διαδίκτυο πληροφοριών καθώς και του ηλεκτρονικού ταχυδρομείου (σκ.41). Πλέον, όχι μόνο γίνεται στερεότυπη αναφορά στον ευρύτερο –έναντι των «συνδιαλέξεων»– όρο «επικοινωνίες», αλλά εκλαμβάνεται ως «αναντίλεκτο ότι όλες οι διεξαγόμενες μέσω ταχυδρομείου, τηλεφώνου ή e-mail επικοινωνίες [...] εμπίπτουν στις κατά το άρθρο 8 παρ. 1 έννοιες της “ιδιωτικής ζωής” και της “ανταπόκρισης”» (Λαχανά, 2013). Συνεπώς, η επιτήρηση και η αποθήκευση των σχετικών πληροφοριών συνιστούν επέμβαση στην ιδιωτικότητα του ατόμου.

2.1.3 Απόφαση Big Brother Watch κατά Ηνωμένου Βασιλείου

Η απόφαση Big Brother Watch κατά Ηνωμένου Βασιλείου αφορούσε τη συμβατότητα των δραστηριοτήτων μαζικής υποκλοπής και ανταλλαγής πληροφοριών στο πλαίσιο καταπολέμησης της τρομοκρατίας με τα δικαιώματα της ιδιωτικής ζωής. Η απόφαση τόνισε τη σημασία των διασφαλίσεων της ιδιωτικής ζωής, ιδιαίτερα στην ψηφιακή εποχή όπου οι προηγμένες τεχνολογίες επιτήρησης μπορούν να έχουν σημαντικές επιπτώσεις στο απόρρητο της επικοινωνίας. Μετά τις αποκαλύψεις του Edward Snowden, ήταν η πρώτη υπόθεση μαζικής παρακολούθησης που εξέτασε το Ε.Δ.Δ.Α. θίγοντας πληθώρα ζητημάτων αναφορικά με τη συμβατότητα τέτοιων πρακτικών με την Ε.Σ.Δ.Α. και σε ποια έκταση η υποκλοπή και η επεξεργασία των δεδομένων επικοινωνίας προσβάλλει την ιδιωτικότητα της ζωής του ατόμου.

Στην υπόθεση αυτή συγκεκριμένα το Δικαστήριο εξέτασε το σύστημα της μαζικής παρακολούθησης από τις κρατικές υπηρεσίες πληροφοριών του Ηνωμένου Βασιλείου των εξωτερικών ηλεκτρονικών (διαδικτυακών) επικοινωνιών, τη λήψη από τις βρετανικές υπηρεσίες πληροφοριών πληροφοριακού υλικού που αποτελεί προϊόν παρακολούθησης από αλλοδαπές αντίστοιχες υπηρεσίες, καθώς και τη δυνατότητα των κρατικών υπηρεσιών πληροφοριών να ζητούν από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να τους χορηγούν πληροφορίες τέτοιων επικοινωνιών.

Με μια μακροσκελή απόφαση το Ε.Δ.Δ.Α. εκκινεί από την παραδοχή ότι ενόψει της ραγδαίας τεχνολογικής προόδου και των κινδύνων που αυτή εγκυμονεί για τα κράτη, καθότι νέες μορφές τρομοκρατίας εμφανίζονται, αναγνωρίζοντας κατ' επέκταση ότι οι μαζικές παρακολουθήσεις μπορούν να συνιστούν «ένα πολύτιμο εργαλείο σε σχέση με την επίτευξη νόμιμων και θεμιτών στόχων δεδομένου ιδιαιτέρως του τρέχοντος επιπέδου απειλής τόσο τόσο στο επίπεδο της διεθνούς τρομοκρατίας όσο και στο επίπεδο της βαριάς εγκληματικότητας» (παρ. 386). Αντίστοιχα η πρακτική αυτή των κρατών θεωρείται εν γένει συμβατή με την Ε.Σ.Δ.Α. εφόσον πληρούνται οι προϋποθέσεις που έχει ήδη θέσει με προηγούμενη νομολογία του το Ε.Δ.Δ.Α. στις οποίες προστίθενται και κάποιες επιπλέον προς το σκοπό παροχής εγγυήσεων ότι τέτοιου είδους επεμβατικά μέτρα μπορούν να είναι ανεκτά από την έννομη τάξη.

Μεταξύ άλλων, το Ε.Δ.Δ.Α. εξέτασε τον ισχυρισμό της βρετανικής κυβέρνησης ότι το καθεστώς της μαζικής παρακολούθησης είναι συμβατό προς την Ε.Σ.Δ.Α. δεδομένου ότι διαφυλάσσει διαφορετική μεταχείριση αναφορικά με το περιεχόμενο των επικοινωνιών σε σχέση με τα μεταδεδομένα επικοινωνίας εκφράζοντας τη θέση των αρχών ότι το περιεχόμενο χρήζει μεγαλύτερης προστασίας από τα μεταδεδομένα λόγω μεγαλύτερης αξίας του. Το Δικαστήριο έθεσε τα δικά του κριτήρια, μη αποδεχόμενο αυτή τη συλλογιστική. Συγκεκριμένα, το Δικαστήριο επεσήμανε ορθώς ότι δεν υπάρχει κανένας απολύτως λόγος για την οποιαδήποτε διαφοροποίηση ως προς το πλέγμα εγγυήσεων που ισχύει για τις άνω κατηγορίες συλλεγόμενου υλικού, καθώς τα εξωτερικά στοιχεία επικοινωνίας μπορούν να είναι πιο αποκαλυπτικά, ακόμη και από το ίδιο το περιεχόμενό της, με αποτέλεσμα να μην είναι δυνατός ο χαρακτηρισμός της συλλογής τους ως λιγότερο επεμβατικός στην ιδιωτική ζωή του θιγόμενου προσώπου (Κουσουνή-Πανταζοπούλου, 2021). Εν προκειμένω, το Ε.Δ.Δ.Α. επανέλαβε προηγούμενες θέσεις του τονίζοντας την ιδιαίτερη σημασία που τα μεταδεδομένα επικοινωνίας μπορεί να έχουν για την ιδιωτικότητα του ατόμου, την εμπιστευτικότητα των πληροφοριών που μπορούν να παραχθούν από τα μεταδεδομένα και η αποκάλυψη των οποίων μπορεί κατά συνέπεια να προκαλέσει σοβαρές επεμβάσεις στην ιδιωτική τους σφαίρα ειδικότερα δε στις περιπτώσεις των μαζικών παρακολουθήσεων, οπότε τα μεταδεδομένα αυτά συλλέγονται μαζικά και σε μεγάλη κλίμακα.

Πέραν του αντικειμένου που εξετάζεται με την παρούσα εργασία δέον είναι να επισημανθεί για την εν λόγω υπόθεση ότι το Ε.Δ.Δ.Α. φαίνεται να αμβλύνει τις επιφυλάξεις του ως προς τη νομιμότητα των μαζικών παρακολουθήσεων αναγνωρίζοντας ότι πρόκειται για *«πολύτιμο εργαλείο σε σχέση με την επίτευξη νόμιμων και θεμιτών στόχων, δεδομένου ιδιαιτέρως του τρέχοντος επιπέδου απειλής τόσο στο επίπεδο της διεθνούς τρομοκρατίας, όσο και στο επίπεδο της βαριάς εγκληματικότητας»*. Στο σημείο αυτό διαφαίνεται υποχώρηση της κριτικής προσέγγισης του δικαστηρίου ως προς την πρακτική των διάχυτων, μη εξειδικευμένων παρακολουθήσεων. Οι λόγοι μολονότι ευχερώς ερμηνεύσιμοι, καθώς συνδέονται πρωτίστως, με τη διαρκή όξυνση της τρομοκρατικής απειλής, στις δυτικές κοινωνίες, δεν παύουν ωστόσο να προκαλούν ανησυχία ως προς την ακεραιότητα του δικαιώματος, στο παρόν και στο μέλλον (Παπανικολάου, 2020).

2.2 Αποφάσεις του Δ.Ε.Ε.

Αντίστοιχες σκέψεις μπορεί να βρει κανείς και στην νομολογία του Δ.Ε.Ε.. Ενδεικτικά παρακάτω αναφέρονται ορισμένες αποφάσεις του Δικαστηρίου κινούμενες γύρω από το ζήτημα που εξετάζεται στην παρούσα.

2.2.1 Απόφαση *Digital Rights Ireland*

Στις συνεκδικαζόμενες υποθέσεις C-293/12 και C-594/12, το Δ.Ε.Ε. με την απόφαση *Digital Rights Ireland Ltd* κλπ αξιολόγησε την Οδηγία 2006/24/EK και το νομικό πλαίσιο που έθεσε σχετικά με την υποχρεωτική διατήρηση των εξωτερικών στοιχείων της επικοινωνίας («δεδομένων κίνησης και θέσης») των χρηστών – συνδρομητών (data retention) για λόγους διακρίβωσης σοβαρών εγκλημάτων, την αντιμετώπιση της τρομοκρατίας και του οργανωμένου εγκλήματος καταλήγοντας να την κηρύσσει ανίσχυρη.

Συνοπτικά αξίζει να αναφερθούν ορισμένες θέσεις του Δ.Ε.Ε. οι οποίες αντικατοπτρίζουν το σκεπτικό του για τη σημασία που έχουν τα μεταδεδομένα επικοινωνίας και πως η πρόβλεψη τέτοιων μέτρων όπως αυτά που θέτει η οδηγία συνιστούν κατάφωρη επέμβαση στα θεμελιώδη δικαιώματα που καθιερώνει ο Χ.Θ.Δ.Ε.Ε. (ιδίως άρθρα 7, 8, 11 και 52).

Το Δ.Ε.Ε. επεσήμανε αρχικά ότι τα δεδομένα που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας «παρέχουν τη δυνατότητα, μεταξύ άλλων, διαπιστώσεως της ταυτότητας του προσώπου με το οποίο ο συνδρομητής ή ο εγγεγραμμένος χρήστης επικοινωνήσε, καθώς και του μέσου με το οποίο έγινε η επικοινωνία, καθώς και τη δυνατότητα προσδιορισμού του χρόνου της επικοινωνίας και της γεωγραφικής θέσεως από την οποία έλαβε χώρα η επικοινωνία αυτή. Επιπλέον, τα δεδομένα αυτά παρέχουν τη δυνατότητα να διαπιστωθεί η συχνότητα των επικοινωνιών του συνδρομητή ή του εγγεγραμμένου χρήστη με συγκεκριμένα πρόσωπα σε δεδομένη χρονική περίοδο» (αιτ. σκέψη 26), καθώς επίσης «(...) λαμβανόμενα στο σύνολό τους, παρέχουν τη δυνατότητα συναγωγής ιδιαιτέρως ακριβών συμπερασμάτων σε σχέση με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα έχουν διατηρηθεί, όπως είναι οι καθημερινές συνήθειες, οι μόνιμοι ή οι προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις των προσώπων αυτών και τα κοινωνικά περιβάλλοντα στα οποία τα πρόσωπα αυτά συχνάζουν.» (αιτ. σκ. 26). Το Δ.Ε.Ε. έκρινε ότι ένας σκοπός γενικού συμφέροντος, όσο θεμελιώδης και αν είναι, δεν μπορεί, αυτός

και μόνον, να προταθεί ως δικαιολογία για την προληπτική υποχρεωτική διατήρηση και τη μη διαγραφή από τους Παρόχους των εξωτερικών στοιχείων της επικοινωνίας για όλους ανεξαιρέτως τους πολίτες της ΕΕ χωρίς την ύπαρξη κάποιου στοιχείου που άμεσα ή έμμεσα να τους συνδέει με υπόνοιες τέλεσης εγκληματικών πράξεων. Με τον τρόπο αυτό, καθίστανται άπαντες «υπό αίρεση ύποπτοι» ώστε να παραβιάζεται αφενός, η αρχή της αναλογικότητας, αφετέρου, τα άρθρα 7, 8 και 52 παρ. 1 του Χάρτη Θεμελιωδών Δικαιωμάτων (Τσόλιας, 2017). Οι λόγοι που στηρίζουν το συμπέρασμα αυτό είναι οι εξής : η οδηγία αφορά αφενός το σύνολο των προσώπων που είναι χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών, ακόμα και πρόσωπα που δεν έχουν εμπλοκή με τα εγκλήματα, αφετέρου δεν περιορίζεται σε διατήρηση χρονικά ή τοπικά περιορισμένη, ούτε αφορά σε συγκεκριμένα πρόσωπα σε σχέση με τα οποία είναι αναγκαία η διατήρηση δεδομένων για τους σκοπούς της πρόληψης, διαπίστωσης ή δίωξης σοβαρών εγκλημάτων· περαιτέρω η οδηγία δεν οριοθετεί σαφώς ποια αδικήματα δύνανται να αποτελούν αντικείμενο έρευνας από τις εθνικές αρχές, ούτε προβλέπει ουσιαστικές και διαδικαστικές προϋποθέσεις για την πρόσβαση αυτών στα διατηρούμενα δεδομένα· και τέλος όσον αφορά τη διάρκεια της διατήρησης δεδομένων, ο καθορισμός της δεν στηρίζεται σε αντικειμενικά κριτήρια (Ιγγλεζάκης, 2021). Στην ίδια απόφαση του Δ.Ε.Ε. ρητά γίνεται αναφορά στη συναφή νομοθεσία της ΕΕ και την ερμηνεία της από το Δικαστήριο, όπου με τον πλέον κατηγορηματικό τρόπο γίνεται δεκτό ότι τα παρελθοντικά αποθηκευμένα στους Παρόχους «εξωτερικά στοιχεία της επικοινωνίας» (δεδομένα κίνησης και θέσης) υπάγονται στην προστασία του απορρήτου, καθώς και ότι η πρόσβαση στα διατηρούμενα δεδομένα από τις αρμόδιες εθνικές αρχές πρέπει να εξαρτάται από προηγούμενο έλεγχο πραγματοποιούμενο είτε από δικαστήριο είτε από ανεξάρτητη διοικητική αρχή (Τσόλιας, 2017).

Φαίνεται ότι κατέστη σαφές ότι τα μεταδεδομένα επικοινωνίας διατηρούν στο ενωσιακό δίκαιο και την ευρωπαϊκή πραγματικότητα εξέχουσα σημασία και η προστασία του απόρρητου χαρακτήρα τους πρέπει να λαμβάνει ιδιαίτερη προσοχή ενόψει της δυναμικής που έχουν για την κατασκευή «επικοινωνιακών πορτραίτων» όχι μόνο συγκεκριμένων προσώπων, αλλά και ολόκληρης της κοινωνίας, ιδιαίτερα στο ψηφιακό περιβάλλον το οποίο την επιτρέπει από τεχνικής άποψης. Η απόφαση αυτή θεωρείται ότι έχει πρακτική σπουδαιότητα διότι ορθώθηκαν φραγμοί στην κανονιστική ευχέρεια του ενωσιακού νομοθέτη να εισάγει περιορισμούς στην προστασία του απορρήτου της ελεύθερης επικοινωνίας για λόγους προάσπισης της δημόσιας ασφάλειας και καταστολής της σοβαρής

εγκληματικότητας (Λαχανά, 2014). Τέτοιου είδους περιορισμοί που εισάγουν παρέκκλιση από την αρχή του απορρήτου των επικοινωνιών και των συναφών δεδομένων πρέπει να ερμηνεύονται συσταλτικά και να υπακούν στη τιθέμενη από το δίκαιο αρχής της αναλογικότητας.

2.2.2 Απόφαση Tele2 Sverige AB (C-203/2015) κατά Post-och telestyrelsen και Secretary of State for the Home Department (C-698/2015) κατά Tom Watson, Peter Brice, Geoffrey Lewis

Αντίστοιχες με την ανωτέρω απόφαση ήταν και οι σκέψεις του Δ.Ε.Ε. που διατυπώθηκαν στις υποθέσεις C-203/2015 και C-698/2015 που αφορούσαν την ερμηνεία του άρθρου 15 παρ. 1 της Οδηγίας 2002/58, το οποίο μετά την κατάργηση της Οδηγίας 2004/26/EK αποτελεί τη νομική βάση στην ενωσιακή έννομη τάξη για τη διατήρηση των δεδομένων. Το Δ.Ε.Ε. κλήθηκε να κρίνει περί της νομιμότητας της εθνικής ρύθμισης της Σουηδίας και του Ηνωμένου Βασιλείου που προέβλεπε μια γενική υποχρέωση διατήρησης των δεδομένων, αφορώσα όλα τα πρόσωπα, όλα τα μέσα ηλεκτρονικής επικοινωνίας και όλα τα δεδομένα κίνησης, χωρίς περιορισμούς, διαφοροποιήσεις και εξαιρέσεις. Εν προκειμένω το Δ.Ε.Ε. εφάρμοσε τα ίδια κριτήρια με αυτά που εφαρμόστηκαν στην υπόθεση Digital Rights Ireland κρίνοντας ως επιβεβλημένη την υπαγωγή των αποθηκευμένων παρελθοντικών δεδομένων κίνησης και θέσης («εξωτερικών στοιχείων της επικοινωνίας») στην προστασία του απορρήτου (Τσόλιας, 2017). Το Δ.Ε.Ε. διαπίστωσε και πάλι ότι «τα μεταδεδομένα επικοινωνίας, λαμβανόμενα στο σύνολό τους, παρέχουν τη δυνατότητα συναγωγής ιδιαίτερως ακριβών συμπερασμάτων σε σχέση με την ιδιωτική ζωή των προσώπων, των οποίων τα δεδομένα έχουν διατηρηθεί, όπως είναι οι καθημερινές συνήθειες, οι μόνιμοι ή οι προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις των προσώπων αυτών και τα κοινωνικά περιβάλλοντα, στα οποία τα πρόσωπα αυτά συχνάζουν» (αιτ. σκ. 99).

2.2.3 Απόφαση La Quadrature du Net and Others κατά Premier ministre and Others

Μια άλλη σημαντική απόφαση του Δ.Ε.Ε. στον τομέα του απορρήτου της επικοινωνίας είναι η υπόθεση La Quadrature du Net and Others κατά Premier ministre and Others. Αυτή η υπόθεση αφορούσε τη συμβατότητα της εθνικής νομοθεσίας για τη γενική και αδιάκριτη διατήρηση δεδομένων κίνησης και τοποθεσίας με το άρθρο 15 παρ. 1 και 2 της Οδηγίας 2002/58/EK. Το Δ.Ε.Ε. κλήθηκε να κρίνει περί του ζητήματος εάν η υποχρέωση γενικής και

χωρίς διάκριση διατήρησης δεδομένων, συνιστά, στο πλαίσιο των συνεχιζόμενων σοβαρών απειλών για την εθνική ασφάλεια, επέμβαση η οποία δικαιολογείται από το δικαίωμα στην ασφάλεια και από τις απαιτήσεις εθνικής ασφάλειας, για τις οποίες είναι υπεύθυνα τα κράτη μέλη.

Το Δ.Ε.Ε. διαπίστωσε ότι τα επίμαχα δεδομένα «είναι αναγκαία για τον εντοπισμό της πηγής μιας επικοινωνίας και του προορισμού της, για τον καθορισμό της ημερομηνίας, της ώρας, της διάρκειας και του είδους της επικοινωνίας, για τον προσδιορισμό του χρησιμοποιούμενου υλικού επικοινωνίας, καθώς και για τον γεωγραφικό εντοπισμό του τερματικού εξοπλισμού και των επικοινωνιών, (...)» (αιτ. σκ. 82), επισημαίνοντας ότι τέτοιου είδους δεδομένα «μπορούν να αποκαλύψουν πληροφορίες σχετικά με σημαντικό αριθμό πτυχών της ιδιωτικής ζωής των υποκειμένων των δεδομένων, συμπεριλαμβανομένων ευαίσθητων πληροφοριών, όπως είναι ο γενετήσιος προσανατολισμός, τα πολιτικά φρονήματα, οι θρησκευτικές, φιλοσοφικές, κοινωνικές ή άλλες πεποιθήσεις, καθώς και η κατάσταση της υγείας, ενώ τα δεδομένα αυτά τυγχάνουν, επιπλέον, ειδικής προστασίας στο δίκαιο της Ένωσης. Στο σύνολό τους, τα εν λόγω δεδομένα παρέχουν τη δυνατότητα να συνάγονται με ιδιαίτερη ακρίβεια συμπεράσματα σε σχέση με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα έχουν διατηρηθεί, όπως είναι οι καθημερινές συνήθειες, οι μόνιμοι ή οι προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, (...) παρέχουν τα μέσα για τον προσδιορισμό του προφίλ των υποκειμένων των δεδομένων, πληροφορία η οποία, υπό το πρίσμα του δικαιώματος του σεβασμού της ιδιωτικής ζωής, είναι εξίσου ευαίσθητη με το περιεχόμενο αυτό καθεαυτό των επικοινωνιών» (αιτ. σκ. 117). Ενόψει της ιδιαίτερης φύσης των δεδομένων αυτών, της πληθώρας των πληροφοριών που μπορούν να εξαχθούν και αφορούν κάθε πτυχή της προσωπικής και ιδιωτικής ζωής των προσώπων, το δίκαιο της ΕΕ δε μπορεί παρά να επιφυλάσσει αντίστοιχα ιδιαίτερη προστασία του απορρήτου χαρακτήρα αυτών των δεδομένων, οπότε μια τέτοια υποχρέωση την οποία επιβάλλει ένα κράτος μέλος στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, βάσει εθνικής ρύθμισης, να διατηρούν τα δεδομένα κίνησης προκειμένου οι αρμόδιες εθνικές αρχές να έχουν πρόσβαση σε αυτά, εφόσον παρίσταται ανάγκη, συνιστά σοβαρή παρέμβαση στα δικαιώματα της ιδιωτικής ζωής και είναι επιτρεπτή μόνο εάν κρίνεται ως το απολύτως αναγκαίο μέτρο για την επίτευξη των επιδιωκόμενων με την ρύθμιση αυτή σκοπών και υπό την προϋπόθεση ότι υπόκειται σε αποτελεσματικές διασφαλίσεις και εγγυήσεις προκειμένου να αποφευχθεί οποιαδήποτε πιθανή κατάχρηση του εν λόγω επεμβατικού μέτρου.

Η απόφαση La Quadrature du Net επιβεβαίωσε τη δέσμευση του Δ.Ε.Ε. για την προστασία της ιδιωτικής ζωής στην ψηφιακή εποχή. Τόνισε τη σημασία ισχυρών διασφαλίσεων, συμπεριλαμβανομένης της προηγούμενης εξουσιοδότησης από ανεξάρτητο φορέα, της αναγκαιότητας διατήρησης δεδομένων για συγκεκριμένους σκοπούς και για περιορισμένο χρόνο και της διαθεσιμότητας αποτελεσματικών ένδικων μέσων κατά καταχρηστικών πρακτικών.

3. Αποφάσεις Διεθνών Δικαστηρίων

Carpenter κατά Ηνωμένων Πολιτειών 138 (2018)

Το απόρρητο της επικοινωνίας ως πτυχή της ιδιωτικότητας του ατόμου και η προστασία αυτού από την αυθαίρετη επέμβαση των κρατικών αρχών θεμελιώνεται στην αμερικανική έννομη τάξη με την Τέταρτη Τροπολογία του Αμερικανικού Συντάγματος, η οποία αναγνωρίζει το δικαίωμα των πολιτών στην ατομική ασφάλεια, στην ασφάλεια των οικιών τους, των εγγράφων τους και των αντικειμένων τους έναντι παράλογων ερευνών και κατασχέσεων, ότι τα παραπάνω είναι απαραβίαστα και εντάλματα έρευνας δεν εκδίδονται, εκτός εάν υπάρχει σοβαρός λόγος, κατόπιν ένορκης καταγγελίας ή συνοδευόμενα από αποδεικτικά στοιχεία, περιλαμβάνοντας ειδική περιγραφή του τόπου που πρόκειται να ερευνηθεί και των ατόμων ή των αντικειμένων που πρόκειται να συλληφθούν. Σχετική με το στην παρούσα εξεταζόμενο ζήτημα είναι η νομική θεωρία που αναπτύχθηκε και πλέον εφαρμόζεται από τα αμερικανικά δικαστήρια, γνωστή ως «third-party doctrine». Ήδη από το 1967 το Ανώτατο Αμερικανικό Δικαστήριο στην υπόθεση Katz κατά Ηνωμένων Πολιτειών έκρινε ότι ιδιωτικές πληροφορίες που το πρόσωπο οικειοθελώς κατέστησε γνωστές σε ένα τρίτο πρόσωπο δεν εμπίπτουν στην προστασία της Τέταρτης Τροπολογίας. Αργότερα, στην υπόθεση Ηνωμένων Πολιτειών κατά Miller (Geneva, 2021) το Ανώτατο Αμερικανικό Δικαστήριο έκρινε ότι ο τότε κατηγορούμενος για φορολογική απάτη δεν είχε «εύλογη προσδοκία» διατήρησης έναντι των κρατικών αρχών των τραπεζικών του αρχείων ως ιδιωτικών και απόρρητων, με την αιτιολογία ότι έχοντας αυτά γνωστοποιηθεί από τον ίδιο οικειοθελώς προς την τράπεζα, ο Miller έφερε τον κίνδυνο τα έγγραφα αυτά να καταστούν γνωστά και από τις κρατικές αρχές, επομένως για να λάβουν γνώση τα κρατικά όργανα δεν ήταν απαραίτητο να εκδοθεί το προβλεπόμενο από τη νομοθεσία ένταλμα αφού οι πληροφορίες αυτές θεωρήθηκαν ότι δεν υπάγονται στην προστασία της Τέταρτης

Τροπολογίας. Το Δικαστήριο εφαρμόζοντας πάλι τη θεωρία αυτή στην υπόθεση Smith κατά Maryland κατέληξε στην κρίση ότι τα κρατικά όργανα χωρίς την έκδοση εντάλματος μπορούν να αποκτήσουν πρόσβαση και να λάβουν γνώση των κληθέντων αριθμών από την τηλεφωνική συσκευή του κατηγορουμένου, καθώς αυτοί έχουν ήδη καταστεί γνωστοί στον πάροχο των τηλεπικοινωνιακών υπηρεσιών. Με το σκεπτικό αυτό περί ανυπαρξίας εύλογης προσδοκίας του θιγόμενου από το μέτρο να παραμείνουν ιδιωτικές και απόρρητες οι σχετικές πληροφορίες, το Δικαστήριο απέρριψε τον ισχυρισμό του κατηγορουμένου ότι η εγκατάσταση στο γραφείο του τηλεπικοινωνιακού παρόχου του κατηγορουμένου μιας συσκευής καταγραφής των κληθέντων από τη συσκευή του κατηγορουμένου τηλεφωνικών αριθμών που έγινε χωρίς ένταλμα συνιστά παραβίαση του συνταγματικού του δικαιώματος στην ιδιωτικότητα.

Με την πάροδο, ωστόσο, των χρόνων, την τεχνολογική πρόοδο που σημειώθηκε και έχοντας πλέον τα κινητά τηλέφωνα και δη τα έξυπνα τηλέφωνα καταστεί σχεδόν αναγκαία και πολύτιμα «εργαλεία» της καθημερινότητας των ατόμων, το Δικαστήριο προκειμένου να συμβαδίσει με τις εξελίξεις στην τεχνολογία και την ψηφιακή κοινωνική πραγματικότητα άρχισε να ακολουθεί μια κάπως διαφορετική προσέγγιση της θεωρίας αυτής αναφορικά με τις κρατικές έρευνες στις τηλεφωνικές συσκευές κάνοντας στάθμιση των συγκρουόμενων συμφερόντων. Αναγνωρίζοντας τη σημασία και το πλήθος των πληροφοριών που μπορούν να εξαχθούν από μια τηλεφωνική συσκευή και οι οποίες αφορούν μεταξύ άλλων τα μεταδεδομένα επικοινωνίας, το 2018, το Ανώτατο Δικαστήριο αντιμετώπισε και επανεξέτασε τη θεωρία αυτή στο πλαίσιο της υπόθεσης Carpenter κατά Ηνωμένων Πολιτειών. Οι κρατικές αρχές πέτυχαν την ταυτοποίηση ως εμπλεκόμενου και τη σύλληψη του τελευταίου που κατηγορούταν για διάπραξη ληστειών. Χρησιμοποιώντας τα μεταδεδομένα του κινητού τηλεφώνου ενός από τους συλληφθέντες (επονομαζόμενα «cell site location information- CSLI»), τα οποία ο τηλεπικοινωνιακός πάροχος διατηρούσε δυνάμει σχετικής νομοθεσίας για επαγγελματικούς σκοπούς, οι αστυνομικές αρχές κατάφεραν να ανεύρουν τους κληθέντες αριθμούς, την ημερομηνία, την ώρα και την τοποθεσία των συσκευών των συνδρομητών με βάση την εγγύτητα προς τους κοντινούς πύργους τηλεφωνίας, δίχως βέβαια την έκδοση εντάλματος.

Το Ανώτατο Αμερικανικό Δικαστήριο έχοντας αντιληφθεί την πλήρη επικράτηση των κινητών τηλεφώνων σε όλο το φάσμα της ζωής των ατόμων, το πλήθος και την αξία των

πληροφοριών που μπορούν να εξαχθούν από αυτά μέσω της παρακολούθησης και ανάλυσης των δεδομένων επικοινωνίας έκανε μια σημαντική υποχώρηση: αμφισβήτησε τον «οικειοθελή χαρακτήρα» της γνωστοποίησης προς τον τρίτο-πάροχο των δεδομένων αυτών και την ανυπαρξία εύλογης προσδοκίας περί μη αποκάλυψης αυτών στις κρατικές αρχές. Το Δικαστήριο τόνισε τη δυναμική της τεχνολογίας αυτής με τρόπο αυτόματο απλά και μόνο με τη χρήση του κινητού τηλεφώνου να αποκαλύπτει με ακρίβεια, σε τεράστια κλίμακα και σε βάθος χρόνου δεδομένα τοποθεσίας, τα οποία συνδυασμένα μεταξύ τους έχουν τη δυνατότητα να αποκαλύψουν πλήθος ευαίσθητων πληροφοριών για τη ζωή του προσώπου, μεταξύ αυτών πολιτικά και θρησκευτικά φρονήματα, το σεξουαλικό του προσανατολισμό κλπ. Το Δικαστήριο δέχτηκε ότι δεν αναιρείται η προσδοκία του προσώπου οι πληροφορίες αυτές να παραμένουν ιδιωτικές, ενώ λόγω της φύσης των πληροφοριών που μπορούν να εξαχθούν και του ιδιαίτερου αποκάλυπτικού χαρακτήρα τους για την ιδιωτική ζωή των ατόμων κατέληξε στο συμπέρασμα ότι τα πρόσωπα έχουν εύλογο και έννομο συμφέρον προστασίας της ιδιωτικότητας αυτών των πληροφοριών, το οποίο υπερτερεί του επιδιωκόμενου σκοπού (εν προκειμένω η εξιχνίαση των ληστειών) από την δημοσιοποίησή τους, απαιτώντας τελικά για την τελευταία την έκδοση σχετικού εντάλματος λόγω της προκαλούμενης ισχυρής επέμβασης στην ιδιωτική ζωή των ατόμων.

Δ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η δομημένη φύση των μεταδεδομένων επικοινωνίας καθιστά ιδιαίτερα εύκολη την επεξεργασία τους, ενώ η ραγδαία εξέλιξη της τεχνολογίας κατά τις τελευταίες δεκαετίες, η ψηφιακή εξόρυξη δεδομένων μέσω εξελιγμένων υπολογιστικών προγραμμάτων και η δυνατότητα συλλογής, αποθήκευσης κι επεξεργασίας τεράστιου όγκου δεδομένων προσωπικών επικοινωνιών, έχουν μεταβάλει άρδην την αξία και του ρόλου τους στην ψηφιακή πραγματικότητα. Τα μεταδεδομένα επικοινωνίας είναι σε θέση να αποκαλύψουν σημαντικές πληροφορίες για τα άτομα και τις ομάδες, ιδιαίτερα όταν συλλέγονται σε μεγάλες ποσότητες σε ολόκληρο τον πληθυσμό. Δεν είναι πλέον ασφαλές να υποθέσει κανείς ότι αυτές οι πληροφορίες "μη περιεχομένου" είναι λιγότερο αποκαλυπτικές ή λιγότερο ευαίσθητες από το περιεχόμενο που περιγράφουν (Felten, 2013). Ιδιαίτερα η εκτεταμένη χρήση των νέων τεχνολογιών σε κάθε πεδίο της ανθρώπινης δραστηριότητας σε παγκόσμιο επίπεδο έχει ως επακόλουθο την μαζική παραγωγή μεταδεδομένων, με την αξιοποίηση των οποίων είτε από κρατικούς φορείς είτε από ιδιώτες να καθίσταται δυνατή η

εξόρυξη μοτίβων συμπεριφοράς των ατόμων αλλά και ολόκληρου του πληθυσμού, καθώς και η δημιουργία των ψηφιακών προφίλ των ατόμων αποκαλύπτοντας στοιχεία για τις διαπροσωπικές τους σχέσεις, τα κοινωνικά και πολιτικά τους φρονήματα, τις προσωπικές ή τις θρησκευτικές τους προτιμήσεις.

Αυτή η διείσδυση σε τόσο ουσιώδεις και ευαίσθητες πληροφορίες της ιδιωτικής ζωής των προσώπων θέτει πολλά ερωτήματα, ακόμα δε περισσότερες και μεγαλύτερες ανησυχίες για το σεβασμό της ιδιωτικότητας και της ελεύθερης επικοινωνίας των προσώπων. Η ύπαρξη εξαιρέσεων εντός των νομικών πλαισίων, ιδίως εκείνων που σχετίζονται με την εθνική ασφάλεια και τα ιδιαίτερα σοβαρά εγκλήματα, υπογραμμίζει την εγγενή ένταση μεταξύ των δικαιωμάτων της ιδιωτικής ζωής και των νόμιμων συμφερόντων. Αν και είναι απαραίτητο να διασφαλιστεί η ιδιωτική ζωή των ατόμων, είναι εξίσου σημαντικό να αντιμετωπιστούν οι ανησυχίες που σχετίζονται με την εθνική ασφάλεια και τη διερεύνηση σοβαρών εγκλημάτων. Η επίτευξη ισορροπίας μεταξύ αυτών των ανταγωνιστικών συμφερόντων είναι ζωτικής σημασίας για να διασφαλιστεί ότι οι παραβιάσεις της ιδιωτικής ζωής είναι δικαιολογημένες, αναλογικές και υπόκεινται σε κατάλληλες διασφαλίσεις. Αυτή η λεπτή ισορροπία είναι ο ακρογωνιαίος λίθος ενός δίκαιου νομικού συστήματος που σέβεται τόσο τα ατομικά δικαιώματα όσο και τις κοινωνικές ανάγκες. Υπό τις συνθήκες αυτές σε διεθνές επίπεδο, ο ρόλος ενός ισχυρού νομικού πλαισίου και των αρχών που διασφαλίζουν το απόρρητο της επικοινωνίας παραμένει εξαιρετικά σημαντικός. Είναι αναγκαίο να αναγνωρίσουμε ότι η ταχεία πρόοδος της τεχνολογίας και η εμφάνιση νέων μορφών επικοινωνίας παρουσιάζουν συνεχείς προκλήσεις που απαιτούν συνεχή αξιολόγηση και προσαρμογή των νομικών πλαισίων. Το νομικό τοπίο πρέπει να συνεχίσει να ανταποκρίνεται σε αυτές τις αλλαγές για την αποτελεσματική προστασία των δικαιωμάτων απόρρητου της επικοινωνίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βενιζέλος, Ε. (2023), «Η σχέση εισαγγελικών αρχών και ανεξάρτητων αρχών - Σεβασμός ή παραβίαση των εγγυήσεων του κράτους δικαίου. Σχόλιο στην 1/2023 Γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου», Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης. Διαθέσιμο σε <https://www.constitutionalism.gr/i-sxesi-ton-eisafelikon-arxon-kai-anexartiton-arxon/>.

Δαγτόγλου, Π. (2012) *Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα*. Αθήνα: Εκδόσεις Σάκκουλας.

Ιγγλεζάκης, Ι. (2021) *Δίκαιο Πληροφορικής (Δ' Έκδοση)*. Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλας.

Ιγγλεζάκης, Ι. (2017), *Άρση απορρήτου όταν αντικείμενο έρευνας αποτελούν δεδομένα που είναι αποθηκευμένα στο νέφος (cloud storage)*. Διαθέσιμο σε https://informaticslaw.blogspot.com/2017/03/blog-post_18.html.

Κουσουνη-Πανταζοπούλου, Α. (2021), «Η νόμιμη (μαζική) παρακολούθηση των ηλεκτρονικών επικοινωνιών υπό το πρίσμα της νομολογίας του Ε.Δ.Δ.Α.. Σχόλιο στην από 25.5.2021 απόφαση Big Brothers Watch and others v. the UK». *ΔΙΤΕ (π. ΔΙΜΕΕ)*, (Τεύχος 3/2021).

Λαχανά, Κ.-Χ. (2013) «Quod ab initio non valet, in tractu temporis non convalescit: Νομική θεμελίωση της ασυμβατότητας της Οδηγίας 2006/24/ΕΚ προς το άρθρο 8 της Ε.Σ.Δ.Α. με αναγωγή στα νομολογιακά προηγούμενα (stare decisis) του Δικαστηρίου του Στρασβούργου». *Ποινική Δικαιοσύνη*, (Τεύχος 12/2013). Διαθέσιμο σε <https://www.constitutionalism.gr/lachana-odigia2006-24ek/>.

Λαχανά, Κ.-Χ. (2014) «Παρατηρήσεις στη Δ.Ε.Ε., συνεκδικαζόμενες υποθέσεις C-293/12 (Digital Rights Ireland Ltd.) και C-594/12 (Seitlinger κλπ.), Απόφαση της 8ης Απριλίου 2014», *Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης*. Διαθέσιμο σε <https://www.constitutionalism.gr/c-29312-digital-rights/>.

Νούσκαλης, Γ. (2020), «Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων (άρθρο 348 Α ΠΚ): Η νομολογιακή προσέγγιση κρίσιμων ζητημάτων ουσιαστικού και δικονομικού δικαίου», *ΕΠΙΘΕΩΡΗΣΗ ΔΙΚΑΙΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ*, (Τόμ. 1, Αρ. 1). Διαθέσιμο σε <https://ejournals.lib.auth.gr/infolawj/article/view/7783>.

Παναγοπούλου, Φ. (2023) *Σύνταγμα-Ερμηνεία κατ' άρθρο – Άρθρο 19*. Σε Βλαχόπουλο Σπ., Κοντιάδη Ξ., Τασόπουλο Γ., (επιμ.). Διαθέσιμο σε <https://www.syntagmawatch.gr/my-constitution/arthro-19/>.

Παπανικολάου, Α. (2023), «Γιατί μας αφορά όλους αυτό που συμβαίνει με την ΑΔΑΕ». Διαθέσιμο σε https://insidestory.gr/article/giati-mas-afora-oloys-ayto-poy-symbainei-me-tin-adae?token=EmrRK2guQI&fbclid=IwAR3j25uGAw_RhgYQtJgz9zkhE6c0Pvb5H8MfDz3zgn1J1nqMVzVtHr7x4Kg.

Παπανικολάου, Α.(2020), *Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*, Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης. Διαθέσιμο σε <https://www.constitutionalism.gr/2020-07-papanikolaou-aporito-epikinonias/>.

Παπαδόπουλος, Ν. (2008) *Προστασία του Απορρήτου της Επικοινωνίας, Ερμηνευτική Προσέγγιση του Αρθρου 19 του Συντάγματος της Ελλάδος*. Αθήνα: Νομική Βιβλιοθήκη.

Συμεωνίδου- Καστανίδου, Ε. (2022), «Το σχέδιο νόμου σχετικά με την άρση του απορρήτου των επικοινωνιών: κρίσιμες για τις θεμελιώδεις ελευθερίες «αστοχίες»», Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης. Διαθέσιμο σε <https://www.constitutionalism.gr/to-sxedio-nomou-sxetika-me-tin-arsis-tou-aporitou-ton-epikoinonion/>.

Τασόπουλος, Γ. (2023), «Πριονίζοντας τα συνταγματικά θεμέλια των συνταγματικών αρχών». Διαθέσιμο σε <https://www.syntagmawatch.gr/trending-issues/prionizontas-ta-syntagmatika-themelia-twn-anexarthtwn-arhwn/>.

Τσόλιας, Γ. (2023), «Το νομικό πλαίσιο άρσης του απορρήτου των ηλεκτρονικών επικοινωνιών για τη διακρίβωση εγκλημάτων σύμφωνα με τις διατάξεις του Ν 5002/2022 και η απολεσθείσα ευκαιρία εκσυγχρονισμού του». *Ποινική Δικαιοσύνη* (3/2023).

Τσόλιας, Γ. (2017) «Δ.Ε.Ε. υποθ. C-203/2015, C-698/2015 απόφ. της 21.12.2016 [Δεδομένα προσωπικού χαρακτήρα και ηλεκτρονικές επικοινωνίες]». *ΔΙΤΕ* (π. ΔΙΜΕΕ) (Τεύχος 1/2017).

Τσόλιας, Γ. (2017) «Εξελίξεις στον τομέα επιτήρησης των ηλεκτρονικών επικοινωνιών: από την ασφάλεια στην ελευθερία και τη διεύρυνση της προστατευόμενης επικοινωνίας (Εισαγωγικό Σημείωμα)». *Ποινική Δικαιοσύνη* (8- 9/2017).

Τσόλιας, Γ. (2016) «ΣτΕ 1593/2016 (Τμ. Δ') [Τηλεπικοινωνίες. Απόρρητο]». *ΔΙΤΕ* (π. ΔΙΜΕΕ), (Τεύχος 4/2016).

Τσόλιας, Γ. (2013) *Απόρρητο Ηλεκτρονικών Επικοινωνιών Ι - Συνταγματικό πλαίσιο προστασίας του απορρήτου στον τομέα των τηλεπικοινωνιών*. Σε Παύλου, Σ., Σάμιο, Θ. επιμ. Ειδικοί Ποινικοί Νόμοι. Αθήνα: Εκδόσεις Π.Ν. Σάκκουλας.

Τσόλιας, Γ. (2013) *Απόρρητο Ηλεκτρονικών Επικοινωνιών ΙΙΙ - Συνταγματικό πλαίσιο προστασίας του απορρήτου στον τομέα των τηλεπικοινωνιών*. Σε Παύλου, Σ., Σάμιο, Θ. επιμ. Ειδικοί Ποινικοί Νόμοι. Αθήνα: Εκδόσεις Π.Ν. Σάκκουλας.

Τσόλιας, Γ. (2005) «Προς ένα σύγχρονο νομικό πλαίσιο προστασίας του απορρήτου των επικοινωνιών (Παρουσίαση και σχολιασμός των διατάξεων του ΠΔ 47/2005)». *Ποινική Δικαιοσύνη*, (Τεύχος 7/2005).

Τσόλιας, Γ. (2006) «Η διατήρηση και επεξεργασία δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών σύμφωνα με την Οδηγία 2006/24/ΕΚ(Σύντομη ερμηνευτική προσέγγιση)». *ΔΙΤΕ (π. ΔΙΜΕΕ)*, (Τεύχος 3/2006).

Χριστοδούλου, Κ. (2014) «Το απόρρητο των ηλεκτρονικών επικοινωνιών μετά την βάσανο του Δ.Ε.Ε. – Η ακύρωση της Data Retention Directive και οι επιπτώσεις της στο εθνικό δίκαιο», *Constitutionalism – Όμιλος Αριστόβουλος Μάνεσης*, σελ. 3. Διαθέσιμο σε <https://www.constitutionalism.gr/christodoulou-aporritoepikoinonion%CE%B9%CE%BD/>.

Χρυσόγονος, Κ. (2023), «Το άρθρο 19 του Συντάγματος υπό τη σκιά του “Μεγάλου Αδερφού”. Ο ν. 5002/2022 και η 1/2023 γνωμοδότηση του Εισαγγελέα του Αρείου Πάγου». *Δικαιώματα του Ανθρώπου -Σάκκουλας* (τεύχος 95, έτος 2023).

Baltar F. & Brunet I. (2012) Social research 2.0: virtual snowball sampling method using Facebook, *Internet Research* 22 (1). Διαθέσιμο σε https://www.researchgate.net/publication/216554865_Social_Research_20_Virtual_Snowball_Sampling_Method_Using_Facebook

BasuMallick, C. (2022) «What is Metadata? Definition, Types, Uses, and Examples». Διαθέσιμο σε <https://www.spiceworks.com/tech/devops/articles/what-is-metadata/>.

Felten Edward W. (2013) United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act, 2/10/2013. Διαθέσιμο σε <https://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf>.

Jurafsky, D., & Martin, J. H. (2023). «An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition». Third Edition draft.

Kift P. & Nissenbaum H. (2016) «Metadata in Context –An Ontological and Normative Analysis of the NSA’s Bulk Telephony Metadata Collection Program», *I/S: A JOURNAL OF LAW AND POLICY*. Διαθέσιμο σε <https://www.semanticscholar.org/paper/Metadata-in-Context-An-Ontological-and-Normative-of-Kift-Nissenbaum/c8ada5c56be2a42ad5057d4483b6cabe4feefd57>.

Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014) «Experimental evidence of massive-scale emotional contagion through social networks.». *Proceedings of the National Academy of Sciences*. Διαθέσιμο σε https://www.researchgate.net/publication/262813340_Experimental_Evidence_of_Massive-Scale_Emotional_Contagion_Through_Social_Networks.

Landau, S. (2020) «Categorizing Uses of Communications Metadata: Systematizing Knowledge and Presenting a Path for Privacy.», *New Security Paradigms Workshop 2020 (NSPW '20)*, ACM. Διαθέσιμο σε <https://doi.org/10.1145/3442167.3442171>.

Leskovec, J., Backstrom, L., & Kleinberg, J. (2008). «Meme-tracking and the dynamics of the news cycle. In Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining». ACM. Διαθέσιμο σε <https://www.cs.cornell.edu/home/kleinber/kdd09-quotes.pdf>.

Liu, B., & Singh, P. (2004) «ConceptNet—a practical commonsense reasoning tool-kit.». *BT Technology Journal*, 22(4), 211-226.

Loideain, N.N. (2015) «EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era». *Cogitatio Media and Communication*, Τόμος 3 (Τεύχος 2). Διαθέσιμο σε https://www.mendeley.com/search/?query=EU+Law+and+Mass+Internet+Metadata+Surveillanc+in+the+Post-Snowden+Era&dgcid=md_homepage.

Mayernik, M. (2017) «Tracing the traces: The critical role of metadata within networked communications», *Journal of the Association for Information Science and Technology* 69(1).

MD Matters (2005) Developing Metadata to Organize Public Health Datasets. National Institutes of Health (.gov).

Montjoye, Y. -A., Radaelli, L., Singh, V.-K. & Pentland, Alex. (2015) «Unique in the shopping mall: On the reidentifiability of credit card metadata». *Science* (New York, N.Y.).

Narayanan A. και Shmatikov V. (2008) «Robust de-anonymization of large sparse datasets», *IEEE Symposium on Security and Privacy*. Διαθέσιμο σε https://www.researchgate.net/publication/4339941_Robust_De anonymization_of_Large_Sparse_Datasets.

Ramirez, G. (2019) «The Erosion of Smith v. Maryland», *Case Western Reserve Law Review*.

Riebe, T., Kühn, P., Imperatori, P., Reuter, C. (2022) « U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance», *European Journal for Security Research*.

Schwartz, H. A., Eichstaedt, J. C., Kern, M. L., Dziurzynski, L., Ramones, S. M., Agrawal, M., ... & Seligman, M. E. (2013) «Personality, gender, and age in the language of social media: The open-vocabulary approach.» *PloS One*. Διαθέσιμο σε https://www.researchgate.net/publication/257302212_Personality_Gender_and_Age_in_the_Language_of_Social_Media_The_Open-Vocabulary_Approach.

Solove, D. J. (2012) Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7).

Warren, J. (2015) «Zen and the Art of Metadata Maintenance», *Journal of Electronic Publishing*. Διαθέσιμο σε <https://mars.gmu.edu/handle/1920/9951>.

ΑΛΛΕΣ ΠΗΓΕΣ

Δελτίο Τύπου της ΑΔΑΕ σχετικά με το νομοσχέδιο για τις άρσεις του απορρήτου κλπ (21/11/2022). Διαθέσιμο σε <http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bfont-size3-colorreddeltio-typou-tis-adae-schetika-me-to-no/>.

Δήλωση του Προέδρου της ΑΔΑΕ Χρήστου Ράμμου για τη γνωμοδότηση 1/10879/10.1.2023 του Εισαγγελέως του Αρείου Πάγου κ. Ισιδώρου Ντογιάκου (10/1/2023). Διαθέσιμο σε <http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bdilosi-toy-proedroy-tis-adae-christoy-rammoy-gia-tin-g/>.

Εθνική Επιτροπή για τα Δικαιώματα του Ανθρώπου, (2023), «Έκθεση αναφοράς για το θεσμικό πλαίσιο ελέγχου των υπηρεσιών ασφαλείας και πληροφοριών». Διαθέσιμο σε <https://nchr.gr/ta-nea-mas/1654-ekthesi-anaforas-tis-eeda-gia-to-thesmiko-plaisio-elegxou-ton-ypiresion-asfaleias-kai-pliroforion.html>.

Εθνική Επιτροπή για τα Δικαιώματα του Ανθρώπου, (2022), «Σχετικά με το σχέδιο νόμου του Υπουργείου Δικαιοσύνης και του Υπουργού Επικρατείας, με τον τίτλο: «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών». Διαθέσιμο σε https://www.nchr.gr/images/pdf/apofaseis/protaseis_epi_nomoth_keimenwn/Simeioma_EEDA_Aporito_epikoinonion.pdf.

Ευρωπαϊκή Ένωση (2018), Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων. Διαθέσιμο σε <http://fra.europa.eu/el/publication/2020/egheiridio-shetika-me-tin-eyropaiki-nomothesia-gia-tin-prostasia-ton-prosopikon>.

Μαρκόπουλος, Ν. (2018) *Η συνταγματική προστασία των εξωτερικών στοιχείων της επικοινωνίας*, Πρακτικά Ημερίδας της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών με θέμα Απόρρητο Επικοινωνιών – Σύγχρονες Προκλήσεις. Αθήνα, 08-05-2018. Αθήνα: Α.Δ.Α.Ε

ΣτΕ Επιτροπή Υπουργών Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1995), Σύσταση Rec (95)4 σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των τηλεπικοινωνιακών υπηρεσιών, με ιδιαίτερη αναφορά στις τηλεφωνικές υπηρεσίες, 7 Φεβρουαρίου 1995.

Τσιφτσόγλου, Α. (2013) *Δημόσια ασφάλεια: θέτοντας όρια στο δικαίωμα του ιδιωτικού βίου*, Διδακτορική Διατριβή. Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ).

Office of the Privacy Commissioner of Canada (2014), *Metadata and Privacy A Technical and Legal Overview*.

NΟΜΟΘΕΣΙΑ

Ελληνικό Σύνταγμα

Νόμος 2225/1994 & Νόμος 5002/1994

Νόμος 3471/2006

Νόμος 3917/2011

Νόμος 4624/2019

Ποινικός Κώδικας

Προεδρικό Διάταγμα 47/2005

Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα

Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (Ε.Σ.Δ.Α.)

Οδηγία 95/46/ΕΚ

Οδηγία 97/66/ΕΚ

Οδηγία 2002/58/ΕΚ

Οδηγία 2006/24/ΕΚ

Οδηγία 2009/136/ΕΚ

Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων

Κανονισμός (ΕΕ) 2016/679 - Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (ΓΚΠΔ)

Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 10-02-2021 για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της Οδηγίας 2002/58/EK (Κανονισμός e-Privacy)

Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔ.Ε.Ε.)

ΝΟΜΟΛΟΓΙΑΚΑ ΚΕΙΜΕΝΑ- ΓΝΩΜΕΣ- ΓΝΩΜΟΔΟΤΗΣΕΙΣ

Γνωμοδοτήσεις Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) 3α/2008, 79/2002 & 1/2005

Γνωμοδοτήσεις Εισαγγελέων Αρείου Πάγου 6/2008, 9/2009, 12/2009, 9/2011 & 1/2023

Άρειος Πάγος 570/2006

Άρειος Πάγος 1421/2010

Άρειος Πάγος 711/2011

Άρειος Πάγος 78/2021

Πλημμελειοδικείο Αθηνών 613/2016

Συμβούλιο της Επικρατείας 1593/2016

Ανώτατο Δικαστήριο των Η.Π.Α., Ex Parte Jackson (1878)

Ανώτατο Δικαστήριο των Η.Π.Α., Katz κατά Ηνωμένων Πολιτειών (1967)

Ανώτατο Δικαστήριο των Η.Π.Α., Ηνωμένες Πολιτείες κατά Miller (1976)

Ανώτατο Δικαστήριο των Η.Π.Α., Smith κατά Maryland (1979)

Ανώτατο Δικαστήριο των Η.Π.Α., Carpenter κατά Ηνωμένων Πολιτειών

Δ.Ε.Ε., Digital Rights Ireland Ltd, Michael Seitlinger κλπ. κατά Minister for Communications κλπ, C-293/12 και C-594/12

Δ.Ε.Ε., La Quadrature du Net and Others κατά Premier Ministre and Others, C-511/18, C-512/18
και C-520/18

Δ.Ε.Ε., Tele2 Sverige AB κατά Post-och telestyrelsen και Secretary of State for the Home
Department κατά Tom Watson, Peter Brice, Geoffrey Lewis, C-203/2015 και C-698/2015

Ε.Δ.Δ.Α., Big Brothers Watch και άλλοι κατά Ηνωμένου Βασιλείου

Ε.Δ.Δ.Α., Copland κατά Ηνωμένου Βασιλείου

Ε.Δ.Δ.Α., Malone κατά Ηνωμένου Βασιλείου

Ε.Δ.Δ.Α., Weber και Saravia κατά Γερμανίας