



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του Δημητρίου Φάκα

Α.Μ. : 2051

**ΤΑ ΜΕΤΑΔΕΔΟΜΕΝΑ ΕΠΙΚΟΙΝΩΝΙΑΣ
ΩΣ ΣΤΟΙΧΕΙΟ ΤΟΥ ΕΠΙΚΟΙΝΩΝΙΑΚΟΥ ΑΠΟΡΡΗΤΟΥ**

Επιβλέποντες:

Δρ. Παπανικολάου Αικατερίνη, Δικηγόρος

Καθηγητής Γκρίτζαλης Στέφανος

Πειραιάς, Ιούνιος 2022

Στη Βασιλική και την Αντιγόνη
για την υπομονή και την αγάπη τους

Ευχαριστίες

Ολοκληρώνοντας την παρούσα διπλωματική εργασία, θέλω να ευχαριστήσω τον επιβλέποντα καθηγητή κύριο Γκρίτζαλη Στέφανο για τις στοχευμένες υποδείξεις χρήσιμου και κρίσιμου υλικού όσο και για την ευρύτητα των παρουσιάσεών του κατά τη διάρκεια όσο και μετά το πέρας των μαθημάτων.

Επιθυμώ επίσης να εκφράσω την ευγνωμοσύνη μου στην κυρία Παπανικολάου Αικατερίνη για την εμπιστοσύνη, την κατανόηση και την υποστήριξη κατά τη διάρκεια εκπόνησης της διπλωματικής εργασίας, αλλά και για τις ανοιχτές συζητήσεις μεταξύ νομικής επιστήμης, πολιτικής και τέχνης, που τόσο απλόχερα προσέφερε. Κυρίως, την ευχαριστώ για το παράδειγμά της.

Οφείλω να δηλώσω τη στήριξή μου και στους δύο επιβλέποντες καθηγητές μου για τις δημόσιες θέσεις που διατύπωσαν τον Απρίλιο του 2021 ενάντια στην εργαλειακή υπονόμηση του δικαιώματος ενημέρωσης σε σχέση με την άρση του επικοινωνιακού απορρήτου, η οποία επήλθε μάλιστα με σκόπιμη νομοθετική παρέμβαση.

Τέλος ευχαριστώ τη μητέρα μου και φιλόλογο Σπυριδούλα Κοταντάκη για την επιμέλεια του κειμένου, την τελική ευθύνη του οποίου φέρει ο γράφων και μόνο.

Περιεχόμενα

ΤΜΗΜΑ ΠΡΩΤΟ	8
Εισαγωγή	8
ΤΜΗΜΑ ΔΕΥΤΕΡΟ	14
A. Σκοπός	14
B. Μεθοδολογικές παρατηρήσεις	15
Περιορισμοί	16
ΤΜΗΜΑ ΤΡΙΤΟ	18
Δημιουργία και ιστορική εξέλιξη των μεταδεδομένων	18
Η αξία των ευρετηρίων της πρώιμης βιβλιοθηκονομίας	18
Από τις ανάγκες της βιβλιοθηκονομίας στις ανάγκες της ψηφιακής εποχής	19
Η στρατηγική αξία των μεταδεδομένων	21
ΤΜΗΜΑ ΤΕΤΑΡΤΟ	24
Ορισμός και κατηγορίες μεταδεδομένων	24
Ορισμός	24
Κατηγορίες μεταδεδομένων	25
ΤΜΗΜΑ ΠΕΜΠΤΟ	28
Ιστορικές επισημάνσεις	28
Σύντομη ιστορία των τρομοκρατικών επιθέσεων 2001-2005	28
Διακρατικός Ανταγωνισμός	29
Εξελίξεις στον τηλεπικοινωνιακό τομέα	32
ΤΜΗΜΑ ΕΚΤΟ	34
Τα μεταδεδομένα επικοινωνίας στο επίκεντρο της επικαιρότητας	34
Η υπόθεση Snowden	34
Έρευνα του Πανεπιστημίου Stanford	36
Η κατάθεση του καθηγητή E. Felten στην Αμερικανική Γερουσία	36
ΤΜΗΜΑ ΕΒΔΟΜΟ	39
The context is content	39
Υπόθεση εργασίας	39
Τεκμηρίωση	42
Σημειώσεις για τον πληροφοριακό πλούτο των μεταδεδομένων και του τρόπου ανάλυσης αυτών	44
Η αναπόφευκτη τομή επικοινωνιακού απορρήτου και δεδομένων προσωπικού χαρακτήρα	47
ΤΜΗΜΑ ΟΓΔΩΟ	49

Κατοχύρωση του απορρήτου της επικοινωνίας σε διεθνές επίπεδο	49
Κατοχύρωση του απορρήτου της επικοινωνίας σε ευρωπαϊκό επίπεδο – το ζήτημα των μεταδεδομένων επικοινωνίας	50
Κριτικές παρατηρήσεις	53
ΤΜΗΜΑ ΕΝΑΤΟ	54
Η ευρωπαϊκή νομολογία	54
Αποφάσεις του ΕΔΔΑ.....	54
Αποφάσεις του ΔΕΕ.....	55
ΤΜΗΜΑ ΔΕΚΑΤΟ	59
Συνοπτική αναφορά της εθνικής νομοθεσίας για την προστασία του απορρήτου και των μεταδεδομένων επικοινωνίας	59
Το άρθρο 19 του Συντάγματος	59
Ο ν.2225/1994	61
Ο ν.3783/2009	63
Το ΠΔ 47/2005.....	64
Ο ν.3471/2006	64
ΤΜΗΜΑ ΕΝΤΕΚΑΤΟ	67
Κριτική επισκόπηση της εθνικής νομοθεσίας σε σχέση με την προστασία των μεταδεδομένων επικοινωνίας	67
ΤΜΗΜΑ ΔΩΔΕΚΑΤΟ	73
Τα προβλήματα της διαδικασίας άρσης απορρήτου για λόγους εθνικής ασφάλειας αναφορικά με τα μεταδεδομένα επικοινωνίας	73
Γενική αξιολόγηση των ρυθμίσεων	73
Αξιολόγηση σε σχέση με τους κινδύνους που απορρέουν από την ανάλυση των μεταδεδομένων.....	74
Συμπληρωματικές παρατηρήσεις	77
ΤΜΗΜΑ ΔΕΚΑΤΟ ΤΡΙΤΟ	81
Απαγορεύσεις αποδεικτικής αξιοποίησης στοιχείων κατόπιν άρσης απορρήτου και το ζήτημα των μεταδεδομένων	81
ΤΜΗΜΑ ΔΕΚΑΤΟ ΤΕΤΑΡΤΟ	84
Η μαζική παρακολούθηση στη νομολογία του ΕΔΔΑ και τα προβλήματα της εθνικής νομοθεσίας και πρακτικής	84
Αντί επιλόγου	86

ΠΕΡΙΛΗΨΗ

Το συνταγματικά κατοχυρωμένο δικαίωμα στην απόρρητη επικοινωνία αποτελεί προϋπόθεση όσο και σημείο τομής για την άσκηση πολλών άλλων θεμελιωδών δικαιωμάτων. Λόγω ακριβώς της νευραλγικής του θέσης στη διεθνή αλλά και εθνική έννομη τάξη, τα ζητήματα που σχετίζονται με την προστασία του εκτείνονται από τον τεχνικό τρόπο λειτουργίας των σύγχρονων μέσων επικοινωνίας και καταλήγουν στο θεσμικό πλαίσιο και τον τρόπο εφαρμογής του.

Αναπόσπαστο τμήμα κάθε επικοινωνίας, πέραν του ίδιου του περιεχομένου, είναι το πλαίσιο της, το οποίο αποδίδεται με τον όρο μεταδεδομένα επικοινωνίας. Τα πρόσωπα των επικοινωνούντων, ο χρόνος, η διάρκεια, η γεωγραφική θέση είναι πληροφορίες που παράγονται από τα χρησιμοποιούμενα μέσα και συλλέγονται από τους παρόχους υπηρεσιών επικοινωνιών κατ' αρχήν για σκοπούς υλοποίησης μιας επικοινωνίας όσο και χρέωσής της.

Η ιστορία της δημιουργίας και αξιοποίησης μεταδεδομένων (στη γενική τους διάσταση) είναι παλαιά και αφορά τη διευκόλυνση γρήγορου εντοπισμού και οργάνωσης πληροφοριών. Στην εξέλιξη της ιστορίας, ακριβώς αυτή η ιδιότητά τους, μετατόπισε το ενδιαφέρον των υπηρεσιών ασφαλείας από τη χρήση παραδοσιακών μεθόδων παρακολούθησης (συνακρόαση), στην ανάλυση σημαντικού όγκου μεταδεδομένων επικοινωνίας.

Οι πληροφορίες αυτές είναι ιδιαίτερα αποκαλυπτικές τόσο σε σχέση με το περιεχόμενο αυτής όσο και σε σχέση με το προφίλ της ζωής των επικοινωνούντων, πορίσματα τα οποία έχουν επιβεβαιωθεί και σε ερευνητικό επίπεδο. Η διάκριση περιεχομένου και μεταδεδομένων στη σημερινή εποχή, θα πρέπει να θεωρείται πια ξεπερασμένη.

Η προστασία των μεταδεδομένων επικοινωνίας ως τμήμα του απορρήτου της επικοινωνίας, αναγνωρίζεται τόσο από την νομολογία όσο και τη νομοθεσία, σε ευρωπαϊκό και εθνικό επίπεδο, δίχως ωστόσο να απουσιάζουν και αντίθετες απόψεις.

Το εθνικό θεσμικό πλαίσιο για την άρση του απορρήτου όσο και ο τρόπος εφαρμογής του, προκαλούν σοβαρές ανησυχίες σε σχέση με την ικανοποιητική προστασία του δικαιώματος στην απόρρητη επικοινωνία. Συνεκτιμώντας τις ευρείες δυνατότητες εξαγωγής συμπερασμάτων από την ανάλυση μεταδεδομένων επικοινωνίας, φαίνεται να καταλείπονται σημαντικά ελλείματα και το εν γένει πλαίσιο προστασίας να έρχεται σε αντίθεση με τμήμα της νομολογίας του ΕΔΔΑ και του ΔΕΕ.

ΤΜΗΜΑ ΠΡΩΤΟ

Εισαγωγή

«Αν έχεις αρκετά μεταδεδομένα, στην πραγματικότητα δε χρειάζεσαι περιεχόμενο. Είναι κάπως ενοχλητικό το πόσο προβλέψιμοι είμαστε ως άνθρωποι»¹.

Οι ανθρώπινες κοινωνίες έχουν εγγεγραμμένη στον πυρήνα τους την έννοια και την πρακτική της επικοινωνίας. Η πραγμάτωση της προσωπικότητας, ανάπτυξη κοινωνικών δεσμών, η εκπαίδευση, η εργασία και κάθε ανθρώπινη δραστηριότητα προϋποθέτει τη δυνατότητα ελεύθερης πρόσληψης όσο και εξωτερίκευσης σκέψεων, συναισθημάτων, προθέσεων, πράξεων μέσα από ποικίλες μορφές επικοινωνίας. Κάθε μια περιλαμβάνει όχι απλά τα μηνύματα που ανταλλάσσουν τα μέρη, αλλά και το επικοινωνιακό πλαίσιο (context). Ακόμα και στο επίπεδο της ομιλίας, στοιχεία όπως ο χρόνος, ο τόπος, η απόσταση, η διάρκεια, τα νεύματα, οι μορφασμοί, η στάση του σώματος, ο αριθμός των συνομιλητών, συγκροτούν ένα πυκνό σημασιολογικό πλέγμα, το οποίο αλληλοεπιδρά με το μήνυμα ενώ δύναται να φέρει ακόμα και ένα ξεχωριστό πυρήνα σε σχέση με το ίδιο το περιεχόμενο της ομιλίας. Ανάλογες διαπιστώσεις ισχύουν και για τη γραφή. Τολμώντας να διατυπώσουμε ένα γενικό κανόνα καμία μορφή επικοινωνίας δε μπορεί να διαχωριστεί από το πλαίσιο της, το οποίο συγκροτεί μαζί με το περιεχόμενο έναν αδιάσπαστο corpus.

Το ελεύθερο της επικοινωνίας εν συνόλω αποτελεί *conditio sine qua non* για την πραγματική και αποτελεσματική άσκηση αυτής. Η ελευθερία αυτή προϋποθέτει οι επικοινωνούντες να εκφράζονται με την πεποίθηση ότι το περιεχόμενο όσο και οι συνθήκες της επικοινωνίας δεν επιτηρούνται και καθίστανται γνωστά μόνο σε όσους επιλέγουν οι ίδιοι. Καθότι η επικοινωνία εκτός από το ίδιο το μήνυμα εμπεριέχει και ταυτόχρονα αποκαλύπτει κάθε είδους σχέσεις (κοινωνικές, επαγγελματικές, πολιτικές κλπ), απόψεις, συνήθειες, πρακτικές και εν γένει πληροφορίες που δύναται να περιγράψουν πλήρως ένα πρόσωπο, η διασφάλιση της μυστικότητας, είναι αναγκαία ώστε η επικοινωνία να μην υπόκειται σε φίλτρα, προληπτικές αξιολογήσεις και αυτολογοκρισία εκ μέρους των επικοινωνούντων.

Στην εξέλιξη ιδίως της πρόσφατης ιστορίας, η απαίτηση αυτή μετασηματίστηκε και εισήλθε σε νέο πλαίσιο.

Η ανάπτυξη των σύγχρονων μέσων επικοινωνίας τις τελευταίες δεκαετίες και η ευρεία διάχυση των Τεχνολογιών Πληροφορικής και Επικοινωνιών, ήταν αποτέλεσμα των πολιτικών και κοινωνικών εξελίξεων που συνέβησαν κατά τη διάρκειά τους² και κυρίως μετά τη λήξη του Δευτέρου Παγκοσμίου Πολέμου. Η ψυχροπολεμική αντιπαράθεση με ποικίλες εκφάνσεις στη στρατιωτική τεχνολογία, τους υπολογιστές και τις επικοινωνίες³, ο ταξικός ανταγωνισμός και οι αλλαγές στη βιομηχανική παραγωγή για την αντιμετώπισή του, η βιομηχανοποίηση της πρωτογενούς παραγωγής και η εγκατάλειψη της υπαίθρου, η ως εκ τούτου επέκταση των μεγάλων πόλεων (και η αύξηση των αποστάσεων εντός αυτών) και εν γένει η αλλαγή του τρόπου οργάνωσης της καθημερινότητας για μεγάλες μάζες πληθυσμού, οδήγησαν στην αλλαγή του μοντέλου των επικοινωνιών.

Από τα τηλεφωνικά κέντρα και τα δημοσίως διαθέσιμα τηλέφωνα σε θαλάμους (κεντροποιημένη επικοινωνία) περάσαμε στη διάχυση των οικιακών τηλεφωνικών συσκευών σε ολόένα και μεγαλύτερο τμήμα του πληθυσμού και στη συνέχεια στην ταχύτατη διάδοση των συσκευών κινητής τηλεφωνίας (αποκεντρωμένη επικοινωνία). Η οριστική και καθολική επικράτηση των ατομικών συσκευών (σταθερής/κινητής τηλεφωνίας, προσωπικοί ηλεκτρονικοί υπολογιστές), η μείωση του κόστους (όσο και η διάδοση «δωρεάν» μέσω επικοινωνίας πχ δωρεάν υπηρεσίες email, instant messaging apps), η άμεση επικοινωνία χωρίς γεωγραφικούς περιορισμούς, οι δυνατότητες εμπλουτισμού της επικοινωνίας με επιπλέον περιεχόμενο πέραν της φωνής ή του κειμένου (φωτογραφίες, βίντεο, αρχεία κειμένων, υπερσύνδεσμοι κλπ) επιβεβαίωσαν τη συμβατότητά τους με τις οικονομικές και κοινωνικές εξελίξεις.

Αυτό που δεν έγινε από την αρχή ορατό στην διάρκεια αυτών των εξελίξεων, ήταν ότι η επικοινωνία, ανεξαρτήτως των χρησιμοποιούμενων μέσων, συνέχισε να ακολουθείται από το ίδιο της το πλαίσιο: ο τόπος, ο χρόνος, η διάρκεια, η ταυτότητα των επικοινωνούντων προσώπων ουδέποτε εξαφανίστηκε. Αντιθέτως, η πληροφοριακή αυτή σκιά ολόένα και μεγάλωνε. Πέραν των στοιχείων αναφορικά με τις τηλεφωνικές κλήσεις, με το πέρασμα στην εποχή του ψηφιακού υπολογιστή και του διαδικτύου, μια νέα κατηγορία πληροφοριών γεννήθηκε: τα ψηφιακά μεταδεδομένα.

Η δημιουργία του ηλεκτρονικού υπολογιστή, καθώς και η δημιουργία και έκρηξη των ψηφιακών αντικειμένων (digital objects), γέννησε την ανάγκη αναμφισβήτητης αναγνώρισης και ταξινόμησής τους, προκειμένου να είναι εφικτή η περαιτέρω χρήση τους. Τα ψηφιακά μεταδεδομένα χρησιμοποιούνται καταρχήν (αλλά όχι αποκλειστικά) για την αναγνώριση ψηφιακών αντικειμένων. Στο αχανές περιβάλλον της ψηφιακότητας όπου η προσέγγιση των ψηφιακών αντικειμένων διέρχεται αποκλειστικά μέσα από τη χρήση αντίστοιχων πληροφοριών που τα συνοδεύουν ή τα περιγράφουν, γρήγορα έγινε αντιληπτό ότι ένα από τα πρώτα και απαιτητικά καθήκοντα είναι η διασφάλιση της αναμφισβήτητης μοναδικότητάς τους. Όπως υποστηρίζει το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών σκοπός των μεταδεδομένων είναι «η διευκόλυνση της αναζήτησης, αξιολόγησης, απόκτησης και χρήσης πηγών»⁴.

Η λειτουργία των σύγχρονων μέσων επικοινωνίας και εν γένει των ψηφιακών μέσων βασίζεται και ταυτόχρονα παράγει σημαντικό όγκο ψηφιακών μεταδεδομένων. Οι συσκευές σταθερής και κινητής τηλεφωνίας, οι συσκευές GPS, οι εφαρμογές άμεσης επικοινωνίας (instant messaging applications πχ messenger, viber, signal, telegram κλπ), οι εφαρμογές τηλεδιάσκεψης (skype, Microsoft teams, Zoom, Goto Meeting κλπ), τα προγράμματα επεξεργασίας κειμένου, οι μηχανές αναζήτησης, οι περιηγητές, οι ιστότοποι, είναι καθημερινά παραδείγματα ψηφιακών μέσων και εφαρμογών, η λειτουργία των οποίων δε θα ήταν εφικτή υπό τη σημερινή τους εκδοχή, χωρίς την ύπαρξη μεταδεδομένων.

Κατά τη λειτουργία των ανωτέρω μέσων και εφαρμογών χρησιμοποιείται και ταυτόχρονα παράγεται κατ' αυτοματοποιημένο τρόπο και χωρίς την παρέμβαση των χρηστών, ένας σημαντικός αριθμός πληροφοριών, ο οποίος αφορά τον τρόπο, τις συνθήκες και τα χαρακτηριστικά της επικοινωνίας και επιπλέον τα χρησιμοποιούμενα μέσα, τα εμπλεκόμενα ή σχετιζόμενα ψηφιακά αντικείμενα, τα χρησιμοποιούμενα δίκτυα κλπ. Η «ανάγκη»⁵ γρήγορης και ακριβούς αναγνώρισης, ταξινόμησης, ανάσυρσης, συσχέτισης, αποθήκευσης και επεξεργασίας πληροφοριών προκειμένου να απαντηθεί ένα αίτημα⁶ από μια ψηφιακή μηχανή και εν γένει η διασφάλιση επικοινωνίας μεταξύ ψηφιακών μέσων, απαιτεί την χρήση μιας προκαθορισμένης γλώσσας, μηχανισμών και κανόνων. Η υλοποίηση των απαιτήσεων αυτών, διέρχεται σε σημαντικό βαθμό (και) μέσα από τη λειτουργία των μεταδεδομένων. Το σύνολο των πληροφοριών αυτών όμως, αφορά επικοινωνίες και συσκευές που χρησιμοποιούνται από πρόσωπα και δύναται να σχετιστεί με αυτά. Με άλλα λόγια οι πληροφορίες αυτές δεν είναι μόνο τεχνικές, αλλά ταυτόχρονα

και προσωπικές, διάκριση η οποία φθίνει ανάλογα με το πλαίσιο εξέτασης, τις τεχνικές δυνατότητες και τον όγκο τους, τα οποία στις μέρες μας είναι αρκούντως διαθέσιμα. Οι πληροφορίες αυτές περιγράφουν στενά προσδιορισμένες ανθρώπινες συμπεριφορές και σχέσεις και για το λόγο αυτό έχουν άμεση επίπτωση στην απόρρητη επικοινωνία⁷.

Το πέρασμα από την αναλογική (τηλεφωνική γραμμή χαλκού) στην ψηφιακή επικοινωνία (Ip-based communications) ανέδειξε την ειδικότερη τεχνική και όχι μόνο σημασία των εν γένει μεταδεδομένων επικοινωνίας ή των άλλως λεγομένων «εξωτερικών στοιχείων της επικοινωνίας»⁸. Τα μεταδεδομένα αυτά απέκτησαν χρήσεις που εκτείνονται σε ποικίλους τομείς, όπως στο εμπόριο, στη διαφήμιση, στην επιστημονική έρευνα, ενώ η χρήση τους έχει επεκταθεί μέχρι και σε στρατιωτικές επιχειρήσεις^{9 10}. Δεν είναι άγνωστο πια γεγονός ότι η χρήση τους στο πλαίσιο διερεύνησης και καταστολής ποινικών αδικημάτων συχνά εισέρχεται στα όρια της αξιοποίησής τους για ευρύτερους και συχνά προβληματικά απροσδιόριστους σκοπούς, υπό την επίκληση λόγων εθνικής ασφάλειας.

Η αναγνώριση της σημασίας και των χρήσεων των μεταδεδομένων επικοινωνίας δεν έχει καταστεί κοινή γνώση, για λόγους που καταρχήν (αλλά όχι μόνο) ανάγονται στο τεχνικό τους υπόβαθρο. Άλλωστε όταν τα μεταδεδομένα κάνουν τη δουλειά τους καλά σβήνουν στο παρασκήνιο σχεδόν σε σημείο να είναι αόρατα¹¹. Στο βαθμό που δεν υπάρχει εξοικείωση, είναι πράγματι δύσκολο να γίνουν αντιληπτά τα ευρύτερα αποτελέσματα της συλλογής και επεξεργασίας των μεταδεδομένων επικοινωνίας σε σχέση με τη συμπεριφορά προσώπων και ομάδων όσο και η νομική αξιολόγησή τους.

Επιπλέον δυσκολότερη, μέχρι στιγμής, είναι η πάγια αναγνώριση των μεταδεδομένων επικοινωνίας ως στοιχείο του απορρήτου στην εθνική νομολογία. Παρά τις πειστικές και συγκλίνουσες θέσεις της θεωρίας και μέρους της νομολογίας¹², ανώτεροι δικαστικοί λειτουργοί και ανώτατα δικαστήρια έχουν εκφράσει ρητά την αντίθεσή τους στην προστασία των μεταδεδομένων επικοινωνίας ως επικοινωνιακό απόρρητο¹³. Στη δημιουργία αυτής της ομιχλώδους κατάστασης συνέτεινε μάλλον και το γεγονός ότι γενικότερα, τα ζητήματα που σχετίζονται και επηρεάζουν το σκληρό πυρήνα των κρατικών εξουσιών, δεν συζητούνται με τη συχνότητα και τη λεπτομέρεια που τους αναλογεί.

Για παράδειγμα, η αρχικά αναφερθείσα ρήση του πρώην γενικού νομικού συμβούλου της NSA Stewart Baker, η οποία πυκνώνει με σχετική επάρκεια όσα θα έπρεπε καταρχήν να είναι κοινώς γνωστά σε σχέση με το αποτέλεσμα της λειτουργίας των μεταδεδομένων

επικοινωνίας, στην πραγματικότητα έχει λάβει δυσανάλογα μικρή δημοσιότητα όσο και σημασία.

Πέραν αυτών, παράγοντες όπως η διαχρονική υποβάθμιση των λειτουργιών και αρμοδιοτήτων από τη συνταγματικά προβλεπόμενη και αρμόδια Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (εφεξής ΑΔΑΕ)¹⁴, η μη ύπαρξη συχνών δημόσιων συζητήσεων για τη σχέση δικαίου και τεχνολογίας όσο και η προβληματική νομολογία, έχουν αποτρέψει¹⁵ τη συστηματική αντιμετώπιση των κινδύνων που συνδέονται με τη συλλογή, επεξεργασία και ανάλυση των μεταδεδομένων.

Στην παρούσα εργασία, πέραν της αναγκαίας συνοπτικής περιγραφής των λειτουργιών των μεταδεδομένων επικοινωνίας, επιχειρείται η περιγραφή του σχετικού νομοθετικού πλαισίου αναφορικά με τη συλλογή, διατήρηση και επεξεργασία μεταδεδομένων επικοινωνίας καθώς η κριτική ανάλυση της σχετικής εθνικής νομοθεσίας όσο και της νομοθεσίας περί άρσης του απορρήτου και των διαδικασιών που συγχέονται με αυτή.

Προκειμένου να γίνουν αντιληπτοί οι κίνδυνοι που απειλούν το απαραβίαστο του επικοινωνιακού απορρήτου (ευρύτερα: της ιδιωτικότητας) αλλά και τη λειτουργία των δημοκρατικών κοινωνιών,¹⁶ εξαιτίας των δυνατοτήτων που παρέχει η αξιοποίηση των μεταδεδομένων, κρίθηκε αναγκαία να παρατεθεί η ιστορία της δημιουργίας των μεταδεδομένων (στη γενική τους έννοια), γεγονότα που συνάπτονται με τη μετατόπιση του ενδιαφέροντος σε αυτό τον τομέα, πολιτικές εκτιμήσεις που συνάπτονται με τη δημιουργία της οικείας νομοθεσίας και το πλήθος των έντονα προσωπικών πληροφοριών που δύναται να αποκαλυφθεί μέσω της ανάλυσής τους.

Δεδομένου δε ότι η ροή των κάθε είδους πληροφοριών και επικοινωνιών διαχρονικά επιδιώκεται¹⁷ να οργανώνεται άμεσα ή έμμεσα από το κράτος και να επιτηρείται από αυτό, η κρατική εξουσία θα πρέπει να θεωρείται βασική πηγή διαρκούς διακινδύνευσης του απορρήτου της επικοινωνίας¹⁸. Προς τούτο εστιάζουμε στις υφιστάμενες διαδικαστικές εγγυήσεις άρσης του απορρήτου, περιγράφοντας τους κινδύνους που αναδεικνύονται. Στο πλαίσιο της σύγχρονης θεωρίας περί θετικών υποχρεώσεων του κράτους και της αρχής της αποτελεσματικής άσκησης των δικαιωμάτων¹⁹, είναι το κράτος που οφείλει να εκπληρώνει τις ουσιαστικές (νομοθετικές) όσο και διαδικαστικές (οργανωτικές) υποχρεώσεις, έτσι ώστε να εγγυάται την προστασία της απόρρητης επικοινωνίας. Τα ανωτέρω έχουν σημασία τόσο αυτοτελώς σε σχέση με το ανωτέρω δικαίωμα όσο και αναφορικά με τη σχέση που έχει με

άλλα θεμελιώδη δικαιώματα, καθώς βρίσκεται στο μεταίχμιο περισσοτέρων της μιας ατομικών ελευθεριών²⁰ και ειδικότερα με το δικαίωμα της ιδιωτικότητας, της ελεύθερης έκφρασης, του συνέρχεσθαι, του ασύλου της κατοικίας, της ελεύθερης ανάπτυξης της προσωπικότητας και άλλα.

Η προστασία που κατ' αρχήν αναγνωρίζει στα μεταδεδομένα επικοινωνίας η ευρωπαϊκή και εθνική νομοθεσία καθώς και η νομολογία²¹, συχνά έρχεται αντιμέτωπη με τη διαρκή εξέλιξη των μέσων επικοινωνίας, των τεχνολογιών ανάλυσης των μεταδεδομένων, τις διαρκώς αυξανόμενες αξιώσεις επιτήρησης των επικοινωνιών από τις δημόσιες αρχές και την καταστρατήγηση υπαρκτών νομοθετικών ελλειμάτων για την αντιμετώπιση πραγματικών, δυνητικών ή επικαλούμενων απειλών. Επομένως, είναι αναγκαία μια ρεαλιστική προσέγγιση, στη βάση των πραγματικών όσο και νομικών κινδύνων που απειλούν το απόρρητο της επικοινωνίας.

ΤΜΗΜΑ ΔΕΥΤΕΡΟ

Α. Σκοπός

Σκοπός της παρούσας διπλωματικής εργασίας είναι η απόδειξη των εξής θέσεων:

1. Τα μεταδεδομένα συνιστούν αναπόσπαστο στοιχείο του επικοινωνιακού απορρήτου, δεδομένου του πυκνού και πολυδιάστατου σημασιολογικού πλούτου τους σε σχέση με μεμονωμένα φυσικά πρόσωπα και ομάδες προσώπων, ενώ η διάκριση του επικοινωνιακού περιεχομένου και μεταδεδομένων επικοινωνίας είναι πια ξεπερασμένη.
2. Το ισχύον στη χώρα μας πλαίσιο όπως και οι διαφαινόμενες πρακτικές άρσης του απορρήτου για λόγους εθνικής ασφάλειας, αναφορικά με τα μεταδεδομένα, συνιστούν κίνδυνο για το δικαίωμα της απόρρητης επικοινωνίας, ερχόμενα σε αντίθεση και με τη νομολογία του ΕΔΔΑ και του ΔΕΕ.

B. Μεθοδολογικές παρατηρήσεις

Ένα μέρος της παρούσας εργασίας, έρχεται αντιμέτωπο με την απόσταση που χωρίζει τη νομική επιστήμη από έννοιες και αντικείμενα της πληροφορικής. Η γλώσσα και οι μηχανισμοί της νομικής σκέψης παρουσιάζουν μια ευλόγως αναμενόμενη επιστημονική ασυμμετρία σε σχέση με την πληροφορική.

Κατά την προσπάθεια εκπόνησης της παρούσας, διατηρήθηκαν οι τεχνικοί όροι κατά τον τρόπο που αξιοποιούνται από την επιστήμη της πληροφορικής, χωρίς να δημιουργηθεί κάποια απλουστευμένη γλώσσα²². Η επιλογή αυτή στηρίχθηκε στην ανάγκη διαφύλαξης της ακεραιότητας των εννοιών και της αποφυγής “μεταφράσεων” που θα συνεπάγοντο την υποχρέωση περαιτέρω οριοθετήσεων.

Αυτό που επιδιώκεται να αναδειχθεί μεταξύ άλλων, είναι η ανάγκη να αποφευχθεί η μηχανιστική και ανύποπτη χρήση όρων που περιγράφουν τεχνικές έννοιες (οι οποίες όλο και συχνότερα απαντώνται στη νομοθεσία και τη νομολογία) και να κατανοηθούν οι σημαντικές συνέπειές τους σε σχέση με το επικοινωνιακό απόρρητο.

Για παράδειγμα, ο όρος «εξωτερικά στοιχεία της επικοινωνίας» που απαντάται στη νομολογία του Αρείου Πάγου όσο και γνωμοδοτήσεις εκδοθείσες αναφορικά με το εύρος του επικοινωνιακού απορρήτου, επιχειρεί να υποδηλώσει μια σχέση αντίθεσης με το καθαυτό περιεχόμενο της επικοινωνίας και καταλήγει στην εσφαλμένη διάκρισή αυτών (εξωτερικών στοιχείων-περιεχομένου) όσο και στη μη προστασία των πρώτων. Μία από τις αιτίες (αν και όχι η μοναδική ή κύρια) είναι η παραγνώριση των πραγματικών δυνατοτήτων που παρέχει η ανάλυση των μεταδεδομένων.

Αυτό που επιχειρούμε να υπενθυμίσουμε είναι ότι οι όροι της πληροφορικής επιστήμης (κατ' ακρίβεια τα αντικείμενα που περιγράφονται από αυτούς τους όρους) συγκροτούν στο επίπεδο της νομικής σκέψης τη μείζονα πρόταση ενός δικανικού συλλογισμού. Δηλαδή, συγκροτούν τα πραγματικά περιστατικά, τα οποία καλούμαστε να υπάγουμε επιτυχώς στους οικείους κάθε φορά κανόνες.

Σε κάθε περίπτωση όμως, κατά την οποία τα πραγματικά περιστατικά:

α) είναι ελλιπή ή

β) γίνονται ελλιπώς ή εσφαλμένως κατανοητά, τόσο ως προς τη σημασία όσο και ως προς τη χρησιμότητα που έχουν για την οικεία επιστήμη ή

γ) παραποιούνται ως προς το πραγματικό περιεχόμενό τους

είναι βέβαιο ότι η υπαγωγή θα είναι εσφαλμένη.

Θα προκύψει δηλαδή είτε κατασκευή αποτελεσμάτων (fabrication) είτε παραποίηση τους (falsification)²³ και σε κάθε περίπτωση ο νομικός συλλογισμός θα είναι εσφαλμένος.

Στην περίπτωση μας, εάν τα μεταδεδομένα επικοινωνίας θεωρηθούν ως «τεχνικές» πληροφορίες μιας επικοινωνίας, εάν δεν συμπεριληφθούν στον ορισμό αυτής και δεν ληφθεί υπόψη ότι αποκαλύπτουν το περιεχόμενο της επικοινωνίας όσο και προσωπικά δεδομένα των επικοινωνούντων, τότε μοιραία²⁴ θα εξαιρούνται από το προστατευτικό πεδίο του δικαιώματος στην απόρρητη επικοινωνία και θα θεωρούνται νόμιμα αποδεικτικά μέσα, παρά τις σαφείς διατάξεις της εθνικής νομοθεσίας με τις οποίες αναμφίβολα προστατεύονται.

Πέραν των περιπτώσεων σκόπιμης απομείωσης της πραγματικής έντασης και έκτασης των τεχνολογικών εννοιών που χρησιμοποιούνται στο πεδίο της νομικής επιστήμης ή της παραποίησης του περιεχομένου τους²⁵ (για λόγους που εκφεύγουν της παρούσας), συχνότερα απαντάται η άγνοια σε σχέση με αυτές, η οποία ωστόσο έχει σημαντικά αποτελέσματα στον τρόπο εφαρμογής των οικείων κανόνων²⁶.

Στην περίπτωση μας, το πραγματικό περιεχόμενο και οι λειτουργίες των μεταδεδομένων επικοινωνίας, είναι κρίσιμο να εντοπιστούν και να αναλυθούν αρχικά στο πλαίσιο της επιστήμης της πληροφορικής και στη συνέχεια της νομικής, ώστε να αποφευχθεί, μεταξύ άλλων, ο κίνδυνος υποτίμησης των ευρύτατων χρήσεων και συνεπειών που έχουν σε σχέση με την ιδιωτικότητα και το απόρρητο των επικοινωνιών. Ο μύθος ότι συνιστούν απλώς “τεχνικές” πληροφορίες, πρέπει να καταρριφθεί.

Περιορισμοί

Η ανάλυση που γίνεται, στο πλαίσιο της παρούσας εργασίας, δεν αφορά και δεν περιλαμβάνει τη σημασία και την ανάλυση μεταδεδομένων, σε σχέση με σκοπούς εμπορικής προώθησης (marketing), διαχείρισης οργανισμών (management), επιστημονικής έρευνας, ιατρικής παρακολούθησης ή άλλους. Δεν περιλαμβάνει επίσης την ανάλυση

μεταδεδομένων που γίνονται σε διαδικασίες ψηφιακής εγκληματολογίας που διενεργούνται μετά από την κατάσχεση ψηφιακών πειστηρίων. Το ερευνητικό αντικείμενο θα περιοριστεί στα μεταδεδομένα επικοινωνίας, των οποίων η προστασία αίρεται κατά τη διαδικασία άρσης απορρήτου.

ΤΜΗΜΑ ΤΡΙΤΟ

Δημιουργία και ιστορική εξέλιξη των μεταδεδομένων

Γενικά η διοίκηση των πολλών δεν διαφέρει από τη διοίκηση των ολίγων. Είναι θέμα οργάνωσης.

Κι ο έλεγχος των πολλών δεν διαφέρει από τον έλεγχο των λίγων. Κι αυτό είναι θέμα σχηματισμών και σημάτων.²⁷

Τα ψηφιακά μεταδεδομένα (στη γενική τους διάσταση) δημιουργήθηκαν στο πλαίσιο διαδικασιών ψηφιοποίησης, προκειμένου να ενταθεί ο βαθμός αναγνώρισης, τυποποίησης, αλληλεπίδρασης και ελέγχου της ψηφιακής ή ψηφιοποιούμενης πληροφορίας. Τα ψηφιακά μεταδεδομένα υπηρετούν τις ανάγκες του ψηφιακού κόσμου, ως ο συνδετικός κρίκος μεταξύ δεδομένων και πληροφοριακών συστημάτων, τα οποία σε διαφορετική περίπτωση, θα συνδεόταν με πολύ μεγάλο κόπο και σε μεγάλο χρόνο, αν όχι καθόλου. Ωστόσο, οι βασικές λειτουργίες των μεταδεδομένων (στη γενική τους έννοια), δεν είναι επινόηση του 20ου αιώνα.

Η αξία των ευρετηρίων της πρώιμης βιβλιοθηκονομίας

Η χρήση «ευρετηριακών» πληροφοριών που βοηθούν στον εντοπισμό και τη διαχείριση περιεχομένου, ανάγεται πριν από αρκετούς αιώνες. Η χρήση αυτή βεβαίως, όπως και τα πρώτα «μεταδεδομένα», δεν είχαν ακριβώς το σημερινό χαρακτήρα και τις σημερινές δυνατότητες. Αφετηρία της δημιουργίας τους ήταν η ανάγκη διαχείρισης και χρήσης μεγάλου όγκου πληροφοριών ή αρχείων, που απαντώνταν αρχικά σε βιβλιοθήκες.

Οι πρώτοι βιβλιοθηκονόμοι δημιούργησαν ένα σύστημα ετικετών (tags) που περιείχαν συνήθως τον συγγραφέα, τον τίτλο, το θέμα και άλλες συναφείς πληροφορίες οι οποίες συνδέονταν με ετικέτες οι οποίες προσαρτώνταν στον εκάστοτε τίτλο, έτσι ώστε να υποβοηθούνται οι ερευνητές στη αναζήτηση του περιεχομένου που επιθυμούσαν²⁸.

Η πρώτη ευρύτερα αναγνωρισμένη πληροφορία σχετικά με τη δημιουργία βιβλιογραφικών «μεταδεδομένων», απαντάται αναφορικά με τη βιβλιοθήκη της Αλεξάνδρειας (280 π.Χ.),

στην οποία το προσωπικό της επισύναπτε μια μικρή ετικέτα που κρεμόταν στην άκρη κάθε πάπυρου και η οποία περιείχε το όνομα του συγγραφέα, τον τίτλο και το θέμα του παπύρου, ενώ παράλληλα δημιουργήθηκαν από τον Καλλίμαχο²⁹ οι «Πίνακες», ο πρώτος κατάλογος και σύστημα ταξινόμησης βιβλιοθήκης, όπου τα έργα παρετίθεντο κατά είδος, τίτλο, όνομα συγγραφέα, μαζί με κάποιες βιογραφικές πληροφορίες αναφορικά με αυτόν^{30 31}.

Παλαιότερες αναφορές ανάγονται στο 2500 π.Χ. και στην αρχαία πόλη Έμπλα³², όπου εντοπίστηκαν πήλινα πλακίδια, τοποθετημένα σε ράφι με την πρώτη γραμμή κάθε πλακιδίου να είναι ορατή για να επιτρέπεται η εύκολη ανάκτησή του περιεχομένου, ενώ μεταγενέστερα ευρήματα εντοπίζονται στην αυτοκρατορία των Χετταίων³³.

Η εφεύρεση της τυπογραφίας από το Γουτεμβέργιο το 15^ο αιώνα, πέραν των κοσμογονικών αλλαγών που επέφερε στη διάδοση της γνώσης, προκάλεσε και παράπλευρα θετικά αποτελέσματα στην οργάνωση των βιβλιοθηκών. Ο μεγάλος πια αριθμός των διαθέσιμων εκδόσεων όσο και η ευρύτατη θεματολογία, απαιτούσαν την αναζήτηση συστηματικών ταξινομικών λύσεων. Η βιβλιοθήκη Bodleian της Οξφόρδης κυκλοφόρησε για πρώτη φορά κατάλογο των περιεχομένων της, όπου μια σελίδα του καταλόγου αντιστοιχούσε στα περιεχόμενα ενός ραφιού της βιβλιοθήκης. Εν συνεχεία ο κατάλογος οργανώθηκε βάσει του ονόματος του συγγραφέα κάθε έκδοσης. Ωστόσο, αυτός ο τρόπος οργάνωσης δεν επέτρεπε στους αναγνώστες τον εύκολο εντοπισμό ενός βιβλίου. Άλλες προσπάθειες επίλυσης των ταξινομικών προβλημάτων (πχ του Thomas James) αντιμετώπισαν το λογικό πρόβλημα ότι κάποια βιβλία μπορούσαν να υπαχθούν σε περισσότερες της μιας κατηγορίες, ενώ παράλληλα ενείχαν ισχυρές δόσεις υποκειμενισμού των δημιουργών τους. Το πρόβλημα αυτό έπρεπε να αντιμετωπιστεί.

Από τις ανάγκες της βιβλιοθηκονομίας στις ανάγκες της ψηφιακής εποχής

Κατά τη διάρκεια του 19^{ου} αιώνα διαφάνηκε η αναμφισβήτητη ανάγκη για δημιουργία μιας σταθερής κωδικοποίησης των ταξινομικών κανόνων και διασώθηκαν σχετικές προσπάθειες.

Περί το 1876 ο Melville Louis Kossuth (Melvil) Dewey, δημιούργησε την πρώτη έκδοση του Δεκαδικού Συστήματος Ταξινόμησης Ντιούι (Dewey Decimal Classification-DDC). Το σύστημα συγκροτείται αρχικά από δέκα γενικές (θεματικές) τάξεις, εν συνεχεία κάθε μία από τις δέκα τάξεις υποδιαιρείται σε δέκα διαιρέσεις και τέλος κάθε διαίρεση υποδιαιρείται

σε δέκα τμήματα. Το σύστημα Dewey είναι από τα επικρατέστερα που χρησιμοποιούνται ακόμα και σήμερα σε βιβλιοθήκες.

Κατά τη διάρκεια του 20^{ου} αιώνα, η δημιουργία του ηλεκτρονικού υπολογιστή προκάλεσε νέες αλλαγές στις μεθόδους βιβλιογραφικής ταξινόμησης.

Στα τέλη της δεκαετίας του 1960, η Henriette Avram ανέπτυξε το MARC format (Machine Readable Cataloging), ένα διεθνές πρότυπο δεδομένων για βιβλιογραφικές πληροφορίες και πληροφορίες σχετικά με τις συλλογές σε βιβλιοθήκες. Αυτή η προσπάθεια, κατέστησε εφικτό την επεξεργασία των δεδομένων αυτών, μέσω υπολογιστή και τον ηλεκτρονικό διαμοιρασμό βιβλιογραφικών πληροφοριών μεταξύ βιβλιοθηκών. Το πρότυπο MARC ήταν το αποτέλεσμα της συνεργασίας της βιβλιοθηκονομίας και της επιστήμης των υπολογιστών, ενώ αξίζει να σημειωθεί ότι η Henriette Avram ξεκίνησε την καριέρα της και εργαζόταν ήδη από το 1952 στη γνωστή πια NSA. Η διαπλοκή αυτή ούτε είναι τυχαία ούτε πρέπει να μας ξαφνιάζει. Σύμφωνα με τον J. Agar, «η ψηφιοποίηση με τη χρήση ηλεκτρονικά αποθηκευμένων προγραμμάτων υπολογιστών, επιχειρήθηκε μόνο σε περιβάλλοντα όπου υπήρχαν ήδη υλικές και θεωρητικές υπολογιστικές πρακτικές και τεχνολογίες»³⁴.

Ωστόσο, το πρόβλημα με το πρότυπο MARC ήταν ότι δε μπορούσε να χρησιμοποιηθεί ως ευρύτερο πρότυπο για να περιγράψει τα διαρκώς αυξανόμενα και διαφοροποιούμενα ψηφιακά αντικείμενα που επρόκειτο να χρησιμοποιηθούν στον αχανή κόσμο των διασυνδεδεμένων υπολογιστών και (αργότερα) του διαδικτύου.

Παράλληλα, εμφανίστηκαν και άλλες κωδικοποιήσεις για την βιβλιοθηκονομική ταξινόμηση, όπως οι Anglo-American Catalog Rules (AACR), ο Resource Description and Access (RDA) (που αντικατέστησε τον AACR2), το BIBFRAME (Bibliographic Framework) κ.α.

Σχετικά πρόσφατη κατάληξη αλλά με πολύ ευρύτερες διαστάσεις από τη βιβλιοθηκονομία, αποτελεί το Resource Description Framework (RDF). Το RDF είναι ένα μοντέλο μεταδεδομένων, βελτιστοποιημένο για χρήση στο διαδίκτυο. Στο πλαίσιο του RDF κάθε κομμάτι πληροφορίας (πηγή) αποτελεί ξεχωριστή οντότητα, η οποία μπορεί να συσχετισθεί εύκολα με άλλες. Το RDF συνιστά μοντέλο οργάνωσης πληροφορίας που χρησιμοποιεί μοναδικά αναγνωριστικά, όπως το URI (Uniform Resource Identifier). Το URI επιτρέπει να εντοπιστεί μια πηγή πληροφορίας (source), ασχέτως της φυσικής της τοποθεσίας. Το URI είναι μοναδικό χαρακτηριστικό (unique identifier) και αποτρέπει τη δημιουργία σύγχυσης

μεταξύ διαφορετικών αντικειμένων (πηγών). Το URL (Uniform Resource Locator) είναι ένα URI το οποίο προσδιορίζει τη διεύθυνση, το σημείο μιας πηγής (πληροφορίας) και μας επιτρέπει να έχουμε πρόσβαση σε αυτή. Τόσο τα URIs όσο και τα URLs διαθέτουν δικούς τους συντακτικούς κανόνες. Η φαινομενικά μικρή διαφοροποίηση μεταξύ του URI και του URL ήταν μια από τις βασικές προϋποθέσεις για την ανάπτυξη του διαδικτύου στη μορφή που το γνωρίζουμε σήμερα. Η γνώση ενός URI είναι σχεδόν άνευ αξίας, αν στον αχανή κόσμο του διαδικτύου δεν είναι εξίσου γνωστή η διεύθυνση αυτής της πηγής, προκειμένου να αποκτηθεί πρόσβαση σε αυτή. Και βεβαίως, η ανακάλυψη αυτή³⁵, δηλαδή η σύνδεση ταυτοποιημένης πληροφορίας όσο και της τοποθεσίας της, απέκτησε ευρύτερες χρήσεις τα επόμενα χρόνια όπως θα δούμε στη συνέχεια.

Το 1995 στο Δουβλίνο του Οχάιο, επιστήμονες από τη βιβλιοθηκονομία, την επιστήμη της πληροφορικής κ.α., προσπαθώντας να βρουν το κατάλληλο πρότυπο για την περιγραφή φυσικών όσο και ψηφιακών αντικειμένων, αντί να επιχειρήσουν να μιμηθούν ή να εξελίξουν το πολύπλοκο σύστημα MARC, δημιούργησαν ένα νέο πρότυπο: το Dublin Core. Το πρότυπο αυτό αποτελείται από 15 ευρέως οριζόμενα στοιχεία, που είναι τα εξής: τίτλος, δημιουργός, θέμα, περιγραφή, εκδότης, συντελεστής, ημερομηνία, τύπος, μορφή (format), αναγνωριστικό, πηγή, γλώσσα, σχέση, ετικέτα, δικαιώματα. Το πρότυπο αυτό χρησιμοποιείται για την περιγραφή φυσικών ψηφιακών αντικειμένων όπως βίντεο, ήχο, εικόνες, κείμενο αλλά και πιο πολύπλοκων αντικειμένων, όπως ιστοσελίδες. Βασίζεται στις γλώσσες XML και RDF και εξαιτίας της απλότητάς του έχει καταστεί ίσως το πιο διαδεδομένο πρότυπο περιγραφικών μεταδεδομένων (descriptive metadata).

Η σημασία του Dublin Core έγκειται στο ότι κατέστη ένα ευρύτερα αναγνωρισμένο πρότυπο σε σχέση με την αποτελεσματική ανεύρεση πληροφοριών σε μεγάλα σύνολα δεδομένων (με εφαρμογές σε πολλούς τομείς) και ταυτόχρονα ανέδειξε τη σημασία της επίτευξης διαλειτουργικότητας (interoperability) μεταξύ των μεταδεδομένων. Διαμόρφωσε δηλαδή μια νέα αντίληψη για τις ευρύτερες χρήσεις και δυνατότητές τους.

Η στρατηγική αξία των μεταδεδομένων

Το ερώτημα το οποίο αβίαστα προκύπτει μετά την παράθεση των ανωτέρω στοιχείων είναι το εξής: για ποιο λόγο μας ενδιαφέρει η «ιστορία» των μεταδεδομένων; Πώς αυτή σχετίζεται με τις σημερινές εξελίξεις και χρήσεις τους;

Από την εποχή που ο εντοπισμός συγκεκριμένου αντικειμένου γινόταν αναγκαστικά με αναζήτηση σε ολόκληρο το περιεχόμενο ή σε καταλόγους που έβριθαν υποκειμενικών προσεγγίσεων, εισήλθαμε στην εποχή όπου αυτό κατέστη εφικτό με τη χρήση συγκεκριμένων, δομημένων (και εσχάτως ψηφιοποιημένων) οδοδεικτών, χωρίς την ανάγκη προσπέλασης ολόκληρου του περιεχομένου.

Όπως εύκολα γίνεται αντιληπτό, τα (κυρίως περιγραφικά) μεταδεδομένα δεν αποκαλύπτουν όλο το περιεχόμενο, σίγουρα όμως συνιστούν ένα ελάχιστο αλλά αναγκαίο τμήμα του, το οποίο είτε αυτοτελώς είτε σε συνδυασμό με άλλες πληροφορίες αποδεικνύεται εξαιρετικά αποτελεσματικό, ιδίως όταν ο όγκος είναι μεγάλος ή δύσκολα προσπελάσιμος.

Τα μεταδεδομένα δηλαδή, λειτουργούν ως ένας χάρτης εντοπισμού, οργάνωσης και μοναδικής αναγνώρισης πληροφοριών και φαίνεται να επιδρούν ως επιταχυντής σε διαδικασίες έρευνας και λήψης αποφάσεων, ενώ παράλληλα προσφέρουν δυνατότητες ελέγχου όσο και συσχέτισης του περιεχομένου.

Σε κάθε περίπτωση, η δημιουργία και χρήση των μεταδεδομένων, συνδέεται κατά διαχρονικό μάλλον τρόπο με τις εξής ανάγκες:

- τον έλεγχο, την εποπτεία και τη διαχείριση μεγάλου όγκου πληροφορίας
- τον εύκολο και γρήγορο εντοπισμό περιεχομένου
- την δημιουργία νέων συσχετίσεων μεταξύ των διαφορετικών περιεχομένων
- την ανταλλαγή, εμπλουτισμό και διαχείριση των αναγκών από τις οποίες πηγάζει η πληροφορία.

Οι ανάγκες αυτές, είναι προφανές ότι δεν είναι απλώς τεχνικές, αλλά βαθύτατα πολιτικές. Η συσσώρευση και επεξεργασία όγκου πληροφοριών ή γνώσεων, δε συνιστά τυχαίο γεγονός, αλλά συνδέεται και προϋποθέτει την ύπαρξη μηχανισμών διοίκησης ή και κοινωνικών δομών που είναι σε θέση να τα συλλέξουν, να τα οργανώσουν όσο και να τα εκμεταλλευτούν. Το γεγονός ότι πρώιμα συστήματα ταξινόμησης δημιουργήθηκαν πολλούς αιώνες πριν στην Αλεξάνδρεια και στην Έμπλα, δεν είναι καθόλου τυχαίο και συνδέεται με την πολιτική, οικονομική, εμπορική και πολιτιστική ισχύ τους. Πολιτικοί και κοινωνικοί

σχηματισμοί οι οποίοι συγκροτούν σώματα γνώσης και πληροφοριών, με διαφορετικούς τρόπους³⁶, είναι επόμενο να μην χρησιμοποιούν μεθόδους οργάνωσης με τη χρήση μεταδεδομένων. Με άλλα λόγια, τα μεταδεδομένα και εν γένει οι μηχανισμοί οργάνωσης πληροφοριών, είναι αναγκαία προϋπόθεση όσο και παράγωγο συγκεκριμένων ιστορικών, κοινωνικών και πολιτικών συνθηκών. Σε σχέση με αυτή τη θέση θα παρατεθούν περισσότερα στοιχεία στη συνέχεια.

ΤΜΗΜΑ ΤΕΤΑΡΤΟ

Ορισμός και κατηγορίες μεταδεδομένων

Ορισμός

Αναφορικά με το σύγχρονο ορισμό των μεταδεδομένων, έχουν διατυπωθεί αρκετές απόψεις.

Ο πιο διαδεδομένος αν και όχι σαφής ορισμός είναι ότι τα μεταδεδομένα είναι *“δεδομένα που παρέχουν πληροφορίες για άλλα δεδομένα”*. Σύμφωνα με τον Διεθνή Οργανισμό Τυποποίησης (ISO) και το πρότυπο 15489, τα μεταδεδομένα είναι *“δεδομένα που περιγράφουν περιεχόμενο, δομή αρχείων και τη διαχείρισή τους στο χρόνο.”* Σύμφωνα με το αμερικανικό υπουργείο άμυνας και το πρότυπο 5015.2, τα μεταδεδομένα περιγράφουν αποθηκευμένα δεδομένα: με άλλα λόγια δεδομένα που περιγράφουν τη δομή, τα στοιχεία των δεδομένων, τις αλληλεξαρτήσεις και άλλα χαρακτηριστικά ηλεκτρονικών αρχείων.

Ο αμερικανικός οργανισμός πληροφορικών και προτύπων (NISO) ορίζει τα μεταδεδομένα ως *δομημένες πληροφορίες που περιγράφουν, εξηγούν, τοποθετούν ή με άλλο τρόπο καθιστούν εύκολη την ανάκτηση, χρήση ή διαχείριση μιας πηγής πληροφοριών.*

Σύμφωνα με το ινστιτούτο Gartner τα μεταδεδομένα είναι *πληροφορίες που περιγράφουν διάφορες όψεις ενός πληροφοριακού αγαθού με σκοπό να βελτιώσουν την χρησιμότητά του καθ' όλο τον κύκλο ζωής του.*

Στην πρόταση του νέου 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*³⁷.

Στην παρούσα εργασία χρησιμοποιείται κυρίως ο όρος μεταδεδομένα, στον οποίο συμπεριλαμβάνονται³⁸:

- τα στοιχεία εισερχόμενων και απερχόμενων τηλεφωνικών κλήσεων³⁹ (Call detail Records -CDRs)
- τα δεδομένα κίνησης (traffic data) και τα δεδομένα θέσης (location data) στις ηλεκτρονικές επικοινωνίες

Κατηγορίες μεταδεδομένων

Τα μεταδεδομένα που τυγχάνουν συχνότερα επεξεργασίας στο πλαίσιο της επικοινωνίας (θέση τερματικών, χρόνος, διάρκεια, αναγνωριστικά επικοινωνούντων κλπ), χαρακτηρίζονται ως «περιγραφικά» (descriptive) μεταδεδομένα, αν και γενικότερα υφίστανται και άλλες κατηγορίες (structural, administrative, preservation metadata). Αυτό που έχει ωστόσο σημασία, στο πλαίσιο της απόρρητης επικοινωνίας, δεν είναι τόσο ο ορθός χαρακτηρισμός ή η ακρίβεια του ορισμού των μεταδεδομένων, όσο η πραγματική λειτουργία τους.

Κατά τη διάρκεια μιας επικοινωνίας και αναλόγως του χρησιμοποιούμενου μέσου, παράγονται διαφορετικές κατηγορίες μεταδεδομένων.

Ενδεικτικά παραδείγματα ανά είδος επικοινωνίας είναι τα εξής:

Τηλεφωνική επικοινωνία	<ul style="list-style-type: none"> • Τηλεφωνικός αριθμός επικοινωνούντων • Μοναδικός αναγνωριστικός αριθμός των τηλεφωνικών συσκευών • Χρόνος επικοινωνίας • Διάρκεια επικοινωνίας • Τοποθεσία των τερματικών συσκευών
Επικοινωνία μέσω email	<ul style="list-style-type: none"> • Όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου και διεύθυνση IP αποστολέα • Όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου παραλήπτη • Ημερομηνία και ώρα • Μοναδικό αναγνωριστικό email

	<ul style="list-style-type: none"> • Κωδικοποίηση μηνύματος • Κεφαλίδες (Headers) και μορφές κεφαλίδων (header formats) • Θέμα • Κατάσταση email (αναγνωσμένο, μη αναγνωσμένο) • Αίτημα αποδεικτικού ανάγνωσης (read receipt request)
<p>Επικοινωνία με χρήση μέσων κοινωνικής δικτύωσης (social media)</p>	<ul style="list-style-type: none"> • Όνομα και συναφείς αναγνωριστικές πληροφορίες που παρέχει ο χρήστης (πόλη, ενδιαφέροντα, ημ.γέννησης) • Όνομα χρήστη και μοναδικό αναγνωριστικό • URL • Τοποθεσία • Μοναδικό αναγνωριστικό συσκευής • Δραστηριότητες/ενέργειες και ημερομηνίες αυτών • Θέμα, τίτλος • Ετικέτες • Τύπος περιεχομένου
<p>Περιήγηση στο διαδίκτυο</p>	<ul style="list-style-type: none"> • Ιστοσελίδες (domain names, χρόνος επίσκεψης) • Αναζητήσεις μέσω περιηγητή • Αποτελέσματα • Στοιχεία σύνδεσης • Διεύθυνση ip • Πάροχος υπηρεσιών διαδικτύου • Έκδοση περιηγητή • Δεδομένα κρυφής μνήμης (cached data) • Πληροφορίες για το hardware

Χωρίς ο παραπάνω πίνακας να περιγράφει πλήρως τις κατηγορίες μεταδεδομένων, ιδίως αυτών που αναφέρονται στις ψηφιακές επικοινωνίες, εύκολα κανείς παρατηρεί το εξής: η

ψηφιακή επικοινωνία που βασίζεται σε πακέτα δεδομένων IP (ip packet data), στα οποία ενσωματώνονται τα μεταδεδομένα, είναι κατ' αρχήν συγκριτικά πλουσιότερη σε πληροφορίες κατ' αριθμό και είδος, σε σχέση με την τηλεφωνική επικοινωνία (και τα αντίστοιχα λεγόμενα Call Detail Records)⁴⁰. Και τούτο γιατί η ψηφιακή επικοινωνία περιλαμβάνει πολλά και διαφορετικά μέρη υλισμικού (hardware) όσο και λογισμικό (software), τόσο στα άκρα της (endpoints) όσο και στη διαδρομή της. Στο πλαίσιο αυτό γεννάται διαρκώς η ανάγκη τα πακέτα δεδομένων (όσο και τα ψηφιακά αντικείμενα που περιέχονται σε αυτά) να λαμβάνουν συγκεκριμένη μορφή, χαρακτηριστικά και ταυτότητα, να αναγνωρίζονται από το πρωτόκολλο επικοινωνίας και τους δρομολογητές (routers) ώστε να φθάνουν στον επιθυμητό προορισμό και να μπορούν να μετατραπούν σε κατανοητή πληροφορία. Η παρατήρηση αυτή αποκτά ιδιαίτερη σημασία υπό το φως της αύξησης του όγκου των ψηφιακών επικοινωνιών σε σχέση με την παραδοσιακή τηλεφωνία⁴¹.

Εξαρχής επίσης διαφαίνεται ότι πολλές από τις αναφερόμενες κατηγορίες υποδεικνύουν με άμεσο τρόπο το περιεχόμενο της επικοινωνίας (πχ οι επισκεφθείσες ιστοσελίδες, οι αναζητήσεις σε μηχανές αναζήτησης), ενώ άλλες έχουν ένα καταρχήν πιο «τεχνικό» χαρακτήρα. Παρά ταύτα, η αξία των εκάστοτε μεταδεδομένων επικοινωνίας δεν πρέπει να θεωρείται δεδομένη ή προκαθορισμένη, αλλά να κρίνεται κάθε φορά από το είδος και την έκταση των πληροφοριών που αποκαλύπτουν.

ΤΜΗΜΑ ΠΕΜΠΤΟ

Ιστορικές επισημάνσεις

*Φοβάμαι τη σημαία σας, πατέρες,
τα εμβλήματα στη φονική σας χλαίνη
κομήτες, μισοφέγγαρα κι αστέρες
το φθόνο σας που απόκοσμα βαθαίνει
και πυρπολεί τους άναρχους αιθέρες
το χέρι σας στο σχήμα του πολέμου
κι ό,τι σκιρτά στην ιαχή «λαέ μου»¹*

Η μετατόπιση του ενδιαφέροντος ιδίως (αλλά όχι μόνο) των υπηρεσιών ασφαλείας και των αστυνομικών αρχών στα μεταδεδομένα επικοινωνίας καθώς και η δημιουργία σχετικής ευρωπαϊκής νομοθεσίας, έχει πολύ συγκεκριμένη χρονική τοποθέτηση. Είναι δύσκολο να υποστηρίξει κανείς ότι οι εξελίξεις αυτές προέκυψαν σε συνθήκες τυχειότητας. Για το λόγο αυτό κρίνεται σκόπιμη η σύντομη παράθεση γεγονότων που σχετίζονται χρονικά όσο και πολιτικά με αυτές και φαίνεται να επέδρασαν αποφασιστικά στη λήψη των σχετικών αποφάσεων.

Σύντομη ιστορία των τρομοκρατικών επιθέσεων 2001-2005

Την 11^η Σεπτεμβρίου 2001, σημειώνεται ένα από τα πλέον κομβικά γεγονότα στη νεότερη ιστορία του δυτικού κόσμου, επικράτησε στη μνήμη⁴² ως «επίθεση στους δίδυμους πύργους» και αποδόθηκε στην ισλαμιστική οργάνωση Al-Qaeda και τον ηγέτη της Osama Bin Laden. Παρά τον καταιγισμό των γεγονότων που προκάλεσε και λόγω του ότι ο χρόνος που έχει παρέλθει από τότε δε συνιστά με κανένα τρόπο περίοδο μακράς διάρκειας⁴³ ώστε να δύναται να εξάγει κανείς συμπεράσματα υψηλής βεβαιότητας⁴⁴, η διατήρηση μιας επιφύλαξης σε σχέση με τις πλήρεις λεπτομέρειες αυτού του γεγονότος, θα ήταν απαραίτητη⁴⁵. Εκφεύγει από τη στοχοθεσία της παρούσας εργασίας η ανάλυση των γεγονότων αυτών. Ωστόσο, αυτό που έχει σημασία είναι ότι ενώ τα ερείπια των δίδυμων πύργων κυριολεκτικά έκαίγαν ακόμα⁴⁶, ενώ υπήρχαν χιλιάδες νεκροί, τραυματίες και αγνοούμενοι, στις 24/10/2001 ψηφίστηκε ο

¹ Καψάλης Διονύσης (1997), *Τετραλογία*, Υπό κλίμακα, Αγρα, Αθήνα, σελ.45

Patriot Act από τη Βουλή των Αντιπροσώπων και την επομένη ψηφίσθηκε και από τη Γερουσία⁴⁷. Βεβαίως, τον Ιούνιο του 2015 το Κογκρέσο ψήφισε το νόμο USA FREEDOM Act, με τον οποίο τερματίστηκε το πρόγραμμα συλλογής μεταδεδομένων μαζικής τηλεφωνίας της NSA, χωρίς ωστόσο να καταργηθεί η συλλογή μεταδεδομένων⁴⁸.

Στις 11/3/2004 στο κέντρο της Μαδρίτης εξερράγησαν ταυτόχρονα βόμβες σε 4 συρμούς τρένων, με αποτέλεσμα 190 νεκρούς και πολλούς τραυματίες. Οι αρχικές πιέσεις να αποδοθεί η επίθεση στην ETA⁴⁹, υποχώρησαν γρήγορα και οι κατηγορίες αποδόθηκαν (και πάλι) στην ισλαμιστική οργάνωση Al-Qaeda, της οποίας η εμπλοκή τελικά δεν αποδείχθηκε ποτέ, αλλά αντιθέτως προέκυψαν σοβαροί προβληματισμοί για πρόσωπα που ενεπλάκησαν σε αυτή⁵⁰. Στις 7/7/2005 μια ακόμη βομβιστική επίθεση γίνεται αυτή τη φορά στο Λονδίνο, ξανά σε συρμούς τρένων, με αποτέλεσμα 56 νεκρούς και εκατοντάδες τραυματίες⁵¹.

Κατά τη δεκαετία του 2000 και με αφορμή τα παραπάνω γεγονότα, ο «πόλεμος κατά της τρομοκρατίας» ιδεολογικοποιείται. Το δόγμα «είτε είστε μαζί μας είτε με τους τρομοκράτες»⁵², επικαλύπτει τις αντίθετες φωνές που υποστήριζαν ότι η άποψη αυτή όσο και το δίπολο «ελευθερία ή ασφάλεια» δε χωρούν σε δημοκρατικά οργανωμένες κοινωνίες. Ο φόβος που χτίζεται και διογκώνεται στις δυτικές κοινωνίες με τη συνδρομή των μέσων ενημέρωσης, αποκτά ευρύτερες χρήσεις στο εσωτερικό αυτών και καθοδηγείται για τη λήψη συγκεκριμένων αποφάσεων⁵³.

Διακρατικός Ανταγωνισμός

Η σειρά αυτή των γεγονότων δε δύναται από μόνη της να περιγράψει το ιστορικό προτσές που συνδέεται με αυτά. Ενδιαφέρον δε παρουσιάζει ότι εκδηλώθηκαν κατά τη διάρκεια της αλλαγής των συσχετισμών στον παγκόσμιο διακρατικό ανταγωνισμό, σε μια αξιοπερίεργη σύμπτωση γεγονότων και γεωπολιτικών σχεδιασμών.

Στα τέλη του 1991 διαλύεται η (από ετών βρισκόμενη σε σοβαρή κρίση) Σοβιετική Ένωση και δημιουργείται η Ρωσική Ομοσπονδία, αποτελούμενη από ομόσπονδα κρατίδια, ενώ οι πρώην σοβιετικές δημοκρατίες ακολουθούν μια ξεχωριστή πορεία η καθεμιά (άλλες στράφηκαν προς τη Δύση και άλλες παρέμειναν στη σφαίρα επιρροής της Ρωσικής Ομοσπονδίας). Τα κρατικά μορφώματα του ευρύτερου χώρου της πρώην Σοβιετικής Ένωσης αντιμετωπίζουν σοβαρά οικονομικά, πολιτικά και κοινωνικά προβλήματα, ενώ μόνο η στρατιωτική ισχύς

(συμπεριλαμβανομένου του πυρηνικού οπλοστασίου που κληρονόμησε από τη Σοβιετική Ένωση), φαίνεται να αποτρέπει ευρύτερες γεωπολιτικές αλλαγές στην Ευρασία. Οι ισορροπίες του έως τότε διπολικού κόσμου, διαλύονται.

Οι ΗΠΑ από το 1991 και μετά βρίσκονται πια ενώπιον ενός αρκετά ανοικτού γεωπολιτικού πεδίου ενώ οι νέες δυνάμεις που αναδύονται δεν είναι ακόμα σε θέση να λειτουργήσουν ως ισχυρά αντίβαρα (πχ Κίνα), πέραν και του γεγονότος ότι οι ΗΠΑ ασκούν σημαντική και ποικίλη επιρροή σε κάποιες από αυτές (πχ στα κράτη μέλη της Ευρωπαϊκής Κοινότητας). Παρά τις ποικίλες υποσχέσεις περί μη επέκτασης της Βορειοατλαντικής Συμμαχίας προς την Ανατολή, τη σφαίρα επιρροής και τις χώρες δορυφόρους της πρώην ΕΣΣΔ⁵⁴, οι οποίες δόθηκαν λίγο πριν όσο και μετά τη διάλυσή της, σταδιακά φαίνεται ότι επικράτησε το δόγμα Μπρεζίνσκι⁵⁵ και οι υποσχέσεις ανατράπηκαν στην πράξη^{56 57}. Πρω της 11ης Σεπτεμβρίου όσο και στη συνέχεια με μεγαλύτερη ένταση, οι ΗΠΑ και οι σύμμαχοί τους ακολουθούν στρατηγικές και πρακτικές επέκτασης της γεωπολιτικής, στρατιωτικής, οικονομικής όσο και πολιτικής επιρροής τους ανά τον πλανήτη με ταυτόχρονη άσκηση πίεσης⁵⁸ στο γεωγραφικό χώρο της πρώην ΕΣΣΔ.

Κατά τη δεκαετία του 1990 και του 2000, οι ΗΠΑ και οι σύμμαχοί τους χρησιμοποιούν στρατιωτικά μέσα και επεμβαίνουν σε αρκετές περιοχές του πλανήτη: το 1990 στον Περσικό Κόλπο (1ος πόλεμος στο Ιράκ), στην (πρώην) Γιουγκοσλαβία (1990-1999), στο Αφγανιστάν (2001-2021), στο Ιράκ (2ος πόλεμος 2003-2011) και σε άλλες. Αξίζει να σημειωθεί ότι οι περισσότερες από αυτές τις πολεμικές επιχειρήσεις γίνονται είτε σε περιοχές επιρροής της πρώην ΕΣΣΔ είτε σε περιοχές που έδιναν στρατηγικό πλεονέκτημα στην προσπάθεια περικύκλωσής της και ανασχεσης της ισχύος της. Ταυτόχρονα, από την αρχή της δεκαετίας του 2000 και μετά οι ΗΠΑ παρακολουθούν μάλλον με σχετική ανησυχία την αργή αλλά σταδιακή αποκατάσταση της οικονομικής, στρατιωτικής και (εν μέρει) γεωπολιτικής ισχύος της Ρωσικής Ομοσπονδίας⁵⁹ και την ανάπτυξη στενών εμπορικών και στρατιωτικών σχέσεων με την Κίνα.

Τα παραπάνω απέχουν πολύ από την πλήρη περιγραφή και εξήγηση των γεγονότων της δεκαετίας του 1990 και του 2000.

Ωστόσο το ερώτημα παραμένει: ποια μπορεί να είναι η σχέση των εξελίξεων αυτών με το ζήτημα των μεταδεδομένων επικοινωνίας; Η απάντηση δεν είναι εύκολη ή προφανής, σίγουρα δε μπορεί να εντοπιστεί εντός των ορίων της νομικής επιστήμης.

Για να υλοποιηθούν αυτά τα σχέδια ανάσχεσης ή και περικύκλωσης του μεγάλου γεωπολιτικού αντιπάλου των ΗΠΑ και των συμμάχων τους και να διεξαχθούν πολεμικές επιχειρήσεις οι οποίες θα ασκούσαν πίεση σε αυτόν, προϋπόθεση ήταν η συγκρότηση αρραγούς νομιμοποίησης σε σχέση με αυτά τόσο στο εσωτερικό των ίδιων των ΗΠΑ όσο και στο εσωτερικό των συμμάχων χωρών⁶⁰.

Η έναρξη ιδίως πολεμικών επιχειρήσεων (οι οποίες έχουν κόστος σε ανθρώπινες ζωές όσο και οικονομικό⁶¹), απαιτεί τη μείωση (αν όχι μηδενισμό) της πιθανότητας να προκύψουν εσωτερικές αντιθέσεις ή ανατρεπτικά της καθεστηκυίας τάξης γεγονότα. Ας μη διαφεύγει ότι στην ιστορική μνήμη των κρατών έχει εγγραφεί ότι οι πολεμικές επιχειρήσεις συναρτώνται με την ανάδυση επαναστατικών γεγονότων και διαδικασιών ⁶², κατά τρόπο που δεν είναι πάντα εύκολο να προβλεφθεί ή να αντιμετωπιστεί.

Η προετοιμασία των ΗΠΑ και των χωρών μελών του NATO για την πραγματοποίηση ενεργειών διαπλανητικής κυριαρχίας και περιορισμού των βασικών γεωπολιτικών, στρατιωτικών και οικονομικών ανταγωνιστών τους, επέτασσε, λοιπόν, την εξασφάλιση μιας επιτηρούμενης ειρήνης στο εσωτερικό τους, έτσι ώστε να αποτραπεί η πιθανότητα ξεσπάσματος εσωτερικών αναταραχών. Η παρακολούθηση και επιτήρηση των κάθε είδους επικοινωνιών αποτελεί τόσο ένα ουσιαστικό όσο και ένα συμβολικό μέσο, που λειτουργεί ως ένα βαθμό αποτρεπτικά για την ανάδυση τέτοιων γεγονότων, ενώ συμβάλλει στην αντιμετώπισή τους και τη διατήρηση του κοινωνικού ελέγχου. Σε αυτό το επίπεδο όμως, η αξιολόγηση του τί συνιστά εγκληματική απειλή και τί πολιτική διαφωνία, αποτελεί μια κρίση οριακού χαρακτήρα, η οποία εύκολα μπορεί να μετατοπιστεί προς τη μια ή την άλλη κατεύθυνση, δίχως να υπακούει σε αυστηρά νομικά κριτήρια. Η ιστορία βρίθει παραδειγμάτων εργαλειώδους ποινικοποίησης των αντιτιθέμενων στις κυρίαρχες απόψεις.

Παράλληλα, δεν πρέπει να διαφύγει της προσοχής ότι από τις αρχές της δεκαετίας του 1990 όσο και στη συνέχεια, οι οικονομίες του δυτικού κόσμου άρχισαν να εισέρχονται σε ένα διαρκώς εντεινόμενο περιβάλλον οικονομικών κρίσεων, το οποίο οι κυβερνήσεις επιχείρησαν να αντιμετωπίσουν με ποικίλα μέτρα. Η πλειονότητα αυτών συνεπάγετο τη μετάθεση των επιπτώσεων στους εργαζόμενους (άμεσες ή έμμεσες περικοπές μισθών, αύξηση φορολογίας, περιορισμός εργατικών δικαιωμάτων, δημιουργία εργαζομένων διαφορετικών ταχυτήτων, «εκμετάλλευση» αποθεματικών ασφαλιστικών ταμείων κ.α.). Οι

κοινωνικές εντάσεις που ήταν επόμενο να προκύψουν από αυτές τις επιλογές, έπρεπε να προληφθούν.

Σε αυτό το πυκνό ιστορικό συγκείμενο, λίγο μετά το 2000 τίθενται σε ισχύ νομοθετήματα τόσο στις ΗΠΑ (Patriot Act) όσο και στην Ευρώπη, μέσω των οποίων υποχωρεί σαφώς η προστασία της ιδιωτικότητας και του απορρήτου των επικοινωνιών και διευρύνονται οι εξουσίες των υπηρεσιών πληροφοριών.

Εξελίξεις στον τηλεπικοινωνιακό τομέα

Παράλληλα προς τις ανωτέρω ιστορικές παρατηρήσεις, προέκυψαν ενδιαφέρουσες εξελίξεις οι οποίες συνέτειναν στη στροφή κρατικών υπηρεσιών προς τη ανάλυση των μεταδεδομένων. Κατά τη διάρκεια της δεκαετίας του 1990 σημειώνεται η κατάργηση του κρατικού μονοπωλίου στις τηλεπικοινωνίες⁶³ και γίνεται επιτρεπτή η είσοδος ιδιωτικών εταιρειών για την παροχή τηλεπικοινωνιακών υπηρεσιών. Ως αποτέλεσμα, το κόστος μειώνεται σημαντικά και αυξάνονται τόσο οι συσκευές επικοινωνιών (τηλεφωνικές συσκευές, ηλεκτρονικοί υπολογιστές) όσο και οι χρήστες. Ταυτόχρονα αρχίζει η χρήση μεθόδων κρυπτογραφίας στις επικοινωνίες, ιδίως στις ηλεκτρονικές.

Ο μεγάλος και συνεχώς διογκούμενος αριθμός των πραγματοποιούμενων τηλεφωνικών κλήσεων όσο και κατά περίπτωση η χρήση μεθόδων κρυπτογραφίας, καθιστά σταδιακά αναποτελεσματική και κοστοβόρα για τις υπηρεσίες πληροφοριών την παρακολούθηση και καταγραφή του περιεχομένου μιας επικοινωνίας. Μέχρις εκείνη την ιστορική στιγμή και αναφορικά με το ζήτημα της απόκτησης πληροφοριών από μέσα επικοινωνίας, οι υπηρεσίες ασφαλείας είχαν βασιστεί για δεκαετίες στη συνακρόαση (υποκλοπή) τηλεφωνικών επικοινωνιών και κατά περίπτωση την προσπάθεια αποκρυπτογράφησης τυχόν διαβαθμισμένων κρυπτογραφημένων επικοινωνιών.

Το πληροφοριακό χάσμα (intelligence gap) που δημιουργήθηκε, δηλαδή το γεγονός ότι ο πολλαπλασιασμός του αριθμού των τηλεφωνικών επικοινωνιών όσο και η χρήση κρυπτογραφίας κατέστησε εκ των πραγμάτων αναποτελεσματικό το επί δεκαετίες χρησιμοποιούμενο μοντέλο συλλογής πληροφοριών που βασιζόταν στη συνακρόαση ⁶⁴, οδήγησε στην εξεύρεση τρόπων αξιοποίησης των μεταδεδομένων επικοινωνίας ως μέσο απόκτησης πληροφοριών.

Και όπως θα αναλυθεί στη συνέχεια, τα μεταδεδομένα επικοινωνίας είναι από τη φύση τους δομημένα, καθιστώντας ταχεία όσο και αποδοτική, τη δυνατότητα επεξεργασίας τους, ακόμα και όταν αυτά είναι σημαντικά ως όγκος δεδομένων. Παρά το γεγονός ότι η συνακρόαση τηλεφωνικών επικοινωνιών δεν εγκαταλείφθηκε εντελώς, η ανάλυση των μεταδεδομένων έδειξε σύντομα ότι μπορούσε να παράσχει περισσότερες, ακριβέστερες και πιο εκτεταμένες πληροφορίες για τα παρακολουθούμενα πρόσωπα (ή ομάδες προσώπων).

ΤΜΗΜΑ ΕΚΤΟ

Τα μεταδεδομένα επικοινωνίας στο επίκεντρο της επικαιρότητας

*Πέρασα με το κόκκινο τη διάβαση
Τα πάντα ούρλιαζαν: παράβαση, παράβαση
Ελεγξαν το αίμα μου και τα χαρτιά μου
Ήμουν πράγματι εγώ ο ίδιος το έγκλημά μου ²*

Η υπόθεση Snowden

Η συζήτηση για τη σημασία των μεταδεδομένων επικοινωνίας, προκλήθηκε κατά δραματικό τρόπο από τις ενέργειες του Edward Snowden. Υπηρετώντας από τη θέση του αναλυτή πληροφοριών στην Εθνική Υπηρεσία Ασφάλειας (National Security Agency) των ΗΠΑ, ανακάλυψε την ύπαρξη απόρρητων προγραμμάτων παγκόσμιας παρακολούθησης τηλεφωνικών επικοινωνιών (PRISM και Tempora), μέσω των οποίων συλλεγόταν και αναλυόταν πλήθος μεταδεδομένων, με τη συνεργασία τηλεπικοινωνιακών παρόχων και κυβερνήσεων.

Σύμφωνα με δήλωση του Snowden *“Τα μεταδεδομένα είναι αυτά που επιτρέπουν μια πραγματική απεριθωμένη κατανόηση, μια ακριβή καταγραφή όλων των ιδιωτικών δραστηριοτήτων στη ζωή μας. Δείχνουν τις σχέσεις μας, τους πολιτικούς μας δεσμούς και τις πραγματικές μας δραστηριότητες”* ⁶⁵.

Το 2013 ο E. Snowden προχώρησε στη δημοσιοποίηση απορρήτων εγγράφων μέσω της εφημερίδας Guardian ⁶⁶, όντας έκτοτε φυγάς κατηγορούμενος, μεταξύ άλλων για παραβίαση του νόμου περί κατασκοπείας.

Στις 6 Ιουνίου 2013 δημοσιεύθηκαν στην εφημερίδα Washington Post και στην Guardian τα πρώτα slides για το πρόγραμμα PRISM, απ’ όπου προέκυψε ότι η NSA είχε απευθείας πρόσβαση στους servers ορισμένων τεχνολογικών κολοσσών στις ΗΠΑ, όπως των εταιρειών Google, Microsoft, Apple, Skype, Yahoo!, Facebook και YouTube ⁶⁷. Οι αποκαλύψεις συνεχίστηκαν μέχρι το 2015.

² Λεοντάρης Βύρων (2017), *Ψυχοστασία, Ποιήματα 1949-2006*, Αθήνα, Ύψιλον, σελ.192

Η πραγματική έκταση των προγραμμάτων παρακολούθησης επικοινωνιών, τα περισσότερα των οποίων αφορούν στη συλλογή και ανάλυση μεταδεδομένων, είναι αδύνατο να παρατεθεί στην παρούσα εργασία. Τα προγράμματα αυτά ωστόσο μπορούν να καταταχθούν σε 4 μεγάλες κατηγορίες: συλλογής (collection programs), επεξεργασίας (processing programs), επίθεσης (attack programs), απομόνωσης (isolation programs)⁶⁸ και προγράμματα βάσης δεδομένων (database programs)⁶⁹. Αποτυπώνουν δε την χρησιμοποιούμενη από τη NSA τεχνολογία παρακολούθησης επικοινωνιών κατά το διάστημα 2010-2012. Αυτό που αξίζει να συγκρατήσει κανείς από τις ενέργειες και τα έγγραφα που δημοσιοποίησε ο Snowden είναι η επιβεβαίωση του γεγονότος ότι οι υπηρεσίες ασφαλείας μετατόπισαν το επιχειρησιακό τους μοντέλο από τη στοχευμένη παρακολούθηση που συνιστούσε τον παλαιότερο κανόνα, στην παρακολούθηση big data (big data surveillance).

Ακολούθησε μια αλυσίδα αποκαλύψεων, αναφορικά με άλλα προγράμματα παρακολούθησης καθώς και τη συνεργασία ιδιωτικών εταιρειών με την NSA, όπως και με επιχειρήσεις παρακολούθησης πολιτικών ηγετών ακόμα και εντός της Ευρωπαϊκής Ένωσης.

Σύντομα επιχειρήθηκε να αντιμετωπιστεί ο αντίκτυπος των δημοσιοποιηθέντων πληροφοριών. Οι δηλώσεις του τότε Αμερικανού Προέδρου Barack Obama ότι δεν καταγράφονται οι κλήσεις παρά μόνο μεταδεδομένα, επιχειρήσαν μάλλον να συσκοτίσουν παρά να διαλευκάνουν το τοπίο, καθώς αξιωματούχοι του Αμερικανικού κράτους το επόμενο διάστημα, αποκάλυψαν ότι τα μεταδεδομένα (επικοινωνίας) είναι απείρως πιο αποτελεσματικά, ακριβή και διεισδυτικά στο πλαίσιο διαδικασιών παρακολούθησης.

Ακόμα πιο επίσημη διάψευση των καθησυχαστικών δηλώσεων του τότε Αμερικανού Προέδρου, προήλθαν από την ίδια την NSA. Το Δεκέμβριο του 2014, κατά τη διάρκεια μιας συζήτησης στο Πανεπιστήμιο John Hopkins, ο πρώην διευθυντής της NSA, Michael Hayden, δήλωσε ότι η Αμερικανική Κυβέρνηση κυριολεκτικά σκοτώνει ανθρώπους βασιζόμενη στην ανάλυση μεταδεδομένων⁷⁰. Αντίστοιχες δηλώσεις έχουν κάνει και άλλοι αξιωματούχοι (της CIA⁷¹) διατυπώνοντας ρητά τη διαφωνία τους σε μια κάθετη διάκριση μεταξύ μεταδεδομένων και περιεχομένου.

Οι ενέργειες του E. Snowden τελικά συνέβαλαν στην αλλαγή της αντίληψης σε σχέση με τους κινδύνους που γεννά η επιτήρηση και ανάλυση του επικοινωνιακού πλαισίου.

Έρευνα του Πανεπιστημίου Stanford

Το Μάρτιο του 2014, στον απόηχο των προαναφερθέντων γεγονότων, το Πανεπιστήμιο του Stanford δημοσίευσε έρευνα που διενεργήθηκε σε δείγμα 546 εθελοντών αναφορικά με τις δυνατότητες εξαγωγής συμπερασμάτων με τη χρήση μεταδεδομένων επικοινωνίας⁷². Όπως θα δούμε στη συνέχεια αυτή δεν ήταν η μοναδική. Στο πλαίσιο αυτής, έγινε συλλογή και επεξεργασία του τηλεφωνικού αριθμού καλούντος και καλούμενου, του σειριακού αριθμού των εμπλεκόμενων τηλεφώνων, τη διάρκεια των κλήσεων και κατά περίπτωση του τόπου όπου βρισκόντουσαν τα επικοινωνούντα πρόσωπα κατά τη διάρκεια των κλήσεων⁷³.

Συνοπτικά, από την έρευνα προέκυψε ότι:

- τα μεταδεδομένα επικοινωνίας μπορούν να δώσουν πολλές λεπτομέρειες σχετικά με οικογενειακές, πολιτικές, επαγγελματικές, θρησκευτικές και σεξουαλικές σχέσεις
- δεν είναι τεχνικά δύσκολο να κλιμακωθούν αυτές οι ταυτοποιήσεις σε μεγαλύτερο πληθυσμό
- ένα μοτίβο κλήσεων αποκαλύπτει περισσότερα από μεμονωμένα αρχεία κλήσεων
- τα μεταδεδομένα του τηλεφώνου είναι αναμφισβήτητα ευαίσθητα, ακόμη και σε σχέση με ένα μικρό δείγμα πληθυσμού και με ένα μικρό χρονικό διάστημα (αναφοράς)

Το 2016 η έρευνα επαναλήφθηκε από τους ίδιους ερευνητές σε δείγμα 823 εθελοντών⁷⁴. Το συμπέρασμα της έρευνας ήταν ότι τα μεταδεδομένα των τηλεφώνων είναι εξαιρετικά ευαίσθητα, ιδίως όταν συσχετίζονται με ένα ευρύ φάσμα άμεσα διαθέσιμων πληροφοριών και ότι εξετάζοντας ένα μεγάλο δείγμα τηλεφωνικών συνδρομητών για μακρά περίοδο, είναι αναπόφευκτο ότι κάποιος από αυτούς θα αποκαλύψει ευαίσθητες πληροφορίες.

Η κατάθεση του καθηγητή E. Felten στην Αμερικανική Γερουσία

Στις 2 Οκτωβρίου 2013 ο Edward W. Felten, καθηγητής Πληροφορικής και Δημόσιων Υποθέσεων στο Πανεπιστήμιο του Princeton (ΗΠΑ), έδωσε κατάθεση στην Αμερικανική Γερουσία και ειδικότερα στην Επιτροπή Δικαστικής Ακρόασης του Νόμου περί παρακολούθησης των επικοινωνιών των αλλοδαπών υπηρεσιών πληροφοριών (Foreign Intelligence Surveillance Act – FISA)⁷⁵.

Από την συνοπτική αλλά εξαιρετικά πυκνή κατάθεση του E. Felten, δύναται να εξαχθούν τα εξής σημαντικά συμπεράσματα⁷⁶:

1. Τα μεταδεδομένα συνιστούν το διακομιστή μεσολάβησης (proxy) του περιεχομένου και μπορούν να το αποκαλύψουν.
2. Τα μεταδεδομένα μπορούν να δώσουν εκπληκτικές πληροφορίες για άτομα και ομάδες, ιδιαίτερα όταν συλλέγονται σε μεγάλες ποσότητες.
3. Τα μεταδεδομένα μπορούν να αποκαλύψουν κοινωνικές, πολιτικές και θρησκευτικές σχέσεις και να σχηματίσουν ένα κοινωνικό χάρτη (social graph), τόσο σε ατομικό όσο και συλλογικό επίπεδο.
4. Τα μεταδεδομένα είναι από τη φύση τους δομημένα δεδομένα (structured data), οργανώνονται με τρόπο που προσφέρεται για ανάλυση και μπορούν να αποφέρουν πολύ περισσότερες πληροφορίες σε μια δεδομένη προσπάθεια σε σχέση με το περιεχόμενο (content).
5. Το περιεχόμενο μιας επικοινωνίας (π.χ. μιας συνομιλίας), συνιστά μη δομημένο δεδομένο (unstructured) και απαιτεί σημαντικούς πόρους για την ανάλυσή του, λαμβανομένων υπόψη των ευρύτατων σημασιολογικών διαστάσεων του προφορικού λόγου.
6. Οι τεχνολογικές εξελίξεις στην ανάλυση πληροφοριών κατέστησαν τα μεταδεδομένα πλουσιότερα σε πληροφορίες απ' ό,τι στο παρελθόν. Είναι πια ευκολότερη και πιο αποδοτική η συλλογή, αποθήκευση και επεξεργασία μεγάλου όγκου αυτών.
7. Με τη χρήση εξελιγμένων υπολογιστικών εργαλείων, είναι πια εφικτή η αναγνώριση μοτίβων και σχέσεων, συμπεριλαμβανομένων προσωπικών πληροφοριών, συνηθειών και συμπεριφορών. Οι μεμονωμένες πληροφορίες, όταν εξετασθούν σ υ ν ο λ ι κ ά, μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες για την καθημερινή ζωή κάποιου προσώπου.
8. Η ισχύς της ανάλυσης των μεταδεδομένων αυξάνει με την κλίμακα των δεδομένων που συλλέγονται και αναλύονται.
9. Δεν υπάρχει πρακτικός τρόπος ώστε οι χρήστες να αποτρέψουν τη δημιουργία μεταδεδομένων τηλεφωνίας ή να τα σβήσουν στη συνέχεια. Ο μόνος τρόπος είναι να αποφύγουν τη δημιουργία αυτών των μεταδεδομένων, αποφεύγοντας την τηλεφωνική επικοινωνία⁷⁷.
10. Οι εφαρμογές ασφαλούς επικοινωνίας (ενδεικτικά: instant messaging apps όπως signal, telegram, what's up, υπηρεσίες κρυπτογραφημένων email πχ tutanota, preveil, virtu, protonmail κλπ) προστατεύουν μόνο το περιεχόμενο της επικοινωνίας (μέσω

κρυπτογράφησης), αλλά όχι τα μεταδεδομένα επικοινωνίας που παράγονται από αυτή. Η κρυπτογράφηση ενός μηνύματος email, προστατεύει το περιεχόμενό του, αλλά όχι τη διεύθυνση email αποστολέα ή του παραλήπτη, το χρόνο αποστολής και το μέγεθος αυτού⁷⁸.

Οι εκπληκτικές διαπιστώσεις του καθηγητή E.Felten, δε θα έπρεπε να προκαλούν αμηχανία. Τα εν γένει μεταδεδομένα επικοινωνίας, ήταν «εκ κατασκευής» προορισμένα να συντελέσουν σε αυτά τα αποτελέσματα. Η ίδια η μαθηματικοποιημένη (και κατά βάση ψηφιακή) επικοινωνία, είναι προορισμένη για την παραγωγή αυτών των αποτελεσμάτων. Η δημιουργία και κυρίως η επεξεργασία μεταδεδομένων επικοινωνίας (ιδίως με τη διαθέσιμη υπολογιστική ισχύ των τελευταίων δεκαετιών), είχε ως αποτέλεσμα τη μείωση της πληροφοριακής εντροπίας⁷⁹ σε σχέση με το περιεχόμενο των επικοινωνιών. Το παλαιό πρόβλημα του C. Shannon ότι τα μηνύματα συχνά έχουν νόημα, το οποίο αναφέρεται ή συσχετίζεται με φυσικές ή εννοιολογικές οντότητες, ξεπεράστηκε με την παράκαμψη (της ανάλυσης) του αχανούς σημασιολογικά περιεχομένου και την στροφή στη σημασία που έχουν τα επικοινωνιακά γεγονότα αφ' εαυτά⁸⁰. Φαίνεται λοιπόν ότι η στροφή στην ανάλυση μεταδεδομένων, ήταν εξαιρετικά αποτελεσματική όσο και επίκαιρη.

ΤΜΗΜΑ ΕΒΔΟΜΟ

The context is content ⁸¹

Η συζήτηση περί της ανάγκης προστασίας των μεταδεδομένων επικοινωνίας ως αναπόσπαστου τμήματος του απορρήτου, έχει ως αφετηρία την παραδοχή ότι η συλλογή και ανάλυσή τους, τόσο σε ατομικό επίπεδο όσο και σε συλλογικό, είναι δυνατό να οδηγεί σε ευρεία προσβολή ευρύτερων θεμελιωδών δικαιωμάτων και σε διατάραξη βασικών λειτουργιών μιας συντεταγμένης δημοκρατίας: οι συνέπειες δηλαδή είναι δυνατό να εκτείνονται πέρα από τον πυρήνα και τα όρια άσκησης του ίδιου του δικαιώματος της απόρρητης επικοινωνίας.

Έχοντας υπόψη τα βαρύνοντα και ιδιαίτερος συγκλονιστικά συμπεράσματα που προκύπτουν από την κατάθεση του καθηγητή E. Felten, είναι χρήσιμο να επεκτείνουμε τη σχετική προβληματική στα συμπεράσματα στα οποία δύναται να οδηγήσει η ανάλυση μεταδεδομένων επικοινωνίας.

Κατά τη διάρκεια των λίγων τελευταίων δεκαετιών, ο όγκος των (ψηφιακών κυρίως) δεδομένων αυξήθηκε πέρα από κάθε προηγούμενο⁸², ενώ παράλληλα έγινε εφικτή η ανάλυση μεγάλου όγκου δεδομένων (big data analytics) σε ελάχιστο χρονικό διάστημα, με την αύξηση της επεξεργαστικής ισχύος των ηλεκτρονικών υπολογιστών⁸³, την ευρεία χρήση αλγορίθμων και άλλων συναφώς χρησιμοποιούμενων τεχνολογιών⁸⁴.

Το data mining, δηλαδή η (επί το ακριβέστερο) διαδικασία εξαγωγής και ανακάλυψης μοτίβων (patterns) από μεγάλα σύνολα δεδομένων, άλλαξε τη σημασία των ίδιων των δεδομένων που τυγχάνουν επεξεργασίας. Κάθε φορά που είναι εφικτή η ανάλυση μιας σημαντικής «ποσότητας» δεδομένων με αναφορά σε συγκεκριμένο πρόσωπο ή πρόσωπα, είναι πια σχεδόν βέβαιο ότι τα εξαγόμενα συμπεράσματα σε σχέση με αυτά θα παρουσιάζουν υψηλό βαθμό διεισδυτικότητας καθώς και ακρίβειας.

Υπόθεση εργασίας

Με αναφορά σε μία και μόνο κατηγορία μεταδεδομένων, τη γεωγραφική θέση της τερματικής συσκευής, που συλλέγεται ήδη στο πλαίσιο της ισχύουσας νομοθεσίας⁸⁵, αξίζει να επιχειρήσει κανείς κάποιες περαιτέρω σκέψεις.

Η γεωγραφική θέση ενός τερματικού επικοινωνιακού εξοπλισμού, σε μια δεδομένη χρονική στιγμή, μπορεί να προσδιοριστεί με διάφορες μεθόδους και με υψηλή ακρίβεια⁸⁶. Σε ένα αφηρημένο επίπεδο⁸⁷ και υπό την αναγκαία προϋπόθεση ότι δεν υφίστανται και δεν αξιοποιούνται καθόλου άλλες διαθέσιμες πληροφορίες, το στοιχείο αυτό δε δύναται από μόνο του να αποκαλύψει κάτι περισσότερο από ένα γεωγραφικό σημείο ενός φυσικού προσώπου.

Ωστόσο, η εικόνα αλλάζει εντελώς, εάν προσθέσουμε στο σχετικό συλλογισμό τις εξής πληροφορίες⁸⁸:

- την αλλαγή (ή τη μη αλλαγή) της θέσης του χρήστη (είτε κατά τη διάρκεια της επικοινωνίας είτε όχι)
- τον τακτικό εντοπισμό μιας ή περισσότερων συγκεκριμένων θέσεων του χρήστη σε συγκεκριμένα γεωγραφικά σημεία
- τη συσχέτιση μιας ή περισσότερων θέσεων σε βάθος χρόνου με άλλες δημόσια διαθέσιμες πληροφορίες (ενδεικτικά: το είδος της περιοχής, του κτιρίου ή άλλου σημείου από το οποίο γίνεται η επικοινωνία, τις δραστηριότητες που αναπτύσσονται στην περιοχή, δημογραφικά/απογραφικά στοιχεία, στοιχεία εκλογικών αποτελεσμάτων κλπ)
- τη συσχέτιση μιας ή περισσότερων θέσεων σε βάθος χρόνου με ευαίσθητες ή διαβαθμισμένες πληροφορίες (περιοχή στην οποία εκδηλώθηκαν συγκεκριμένα γεγονότα, ενέργειες, δραστηριότητες ποινικής, πολιτικής ή άλλης αξιολόγησης)
- τη συσχέτιση μιας ή περισσότερων θέσεων σε βάθος χρόνου με άλλα μεταδεδομένα επικοινωνίας (το χρόνο επικοινωνίας, την ταυτότητα των επικοινωνούντων, τη διάρκεια και το είδος της επικοινωνίας, το μέγεθος του μηνύματος)

Συναξιολογώντας τις παραπάνω πληροφορίες, η γεωγραφική θέση μια τερματικής συσκευής επικοινωνίας είναι δυνατό να αποκαλύψει:

- τον πραγματικό τόπο κατοικίας, εργασίας και εν γένει δραστηριοποίησης ενός δεδομένου φυσικού προσώπου (ή ομάδας φυσικών προσώπων)
- τα καθημερινά ή τακτικά δρομολόγια προς οποιοδήποτε προορισμό (εργασία, διασκέδαση), το σκοπό και το μέσο μετακίνησης, συναφείς συνήθειες (στάσεις κλπ)
- τον πραγματικό τόπο ανάπτυξης προσωπικών ενασχολήσεων ενός δεδομένου φυσικού προσώπου (ή ομάδας φυσικών προσώπων) όπως αθλήματα, εξωτερικές δραστηριότητες, καλλιτεχνικές δραστηριότητες καθώς και το είδος αυτών,
- την ύπαρξη χρόνιων ή έκτακτων προβλημάτων υγείας (πχ γεωγραφική θέση σε νοσοκομείο ή τακτικές επισκέψεις σε ιατρούς-διαγνωστικά κέντρα) ενός δεδομένου φυσικού προσώπου (ή ομάδας φυσικών προσώπων)
- τις πολιτικές πεποιθήσεις (πχ γεωγραφική θέση σε σημείο και κατά χρόνο στον οποίο εκδηλώνεται μια πορεία διαμαρτυρίας, μια ακτιβιστική δράση, μια πολιτική εκδήλωση, το συνέδριο ενός κόμματος) ενός δεδομένου φυσικού προσώπου (ή ομάδας φυσικών προσώπων)
- τις θρησκευτικές πεποιθήσεις (πχ γεωγραφική θέση σε τόπους λατρείας) ενός δεδομένου φυσικού προσώπου (ή ομάδας φυσικών προσώπων)
- τις αγοραστικές και άλλες συνήθειες (πχ προτίμηση τρόπου διασκέδασης) ενός δεδομένου φυσικού προσώπου (ή ομάδας φυσικών προσώπων)
- τη συσχέτιση ενός φυσικού προσώπου (ή ομάδας φυσικών προσώπων) με άλλα πρόσωπα, το είδος και τη βάση της συσχέτισης (αν είναι τακτική ή τυχαία, αν αφορά μια δραστηριότητα ελεύθερου χρόνου, αν είναι ερωτικής φύσης ή άλλου χαρακτήρα, αν είναι στη βάση κάποιων κοινών πολιτικών απόψεων)
- εν γένει τον κοινωνικό χάρτη ενός φυσικού προσώπου ή ομάδων φυσικών προσώπων

Η περαιτέρω ανάλυση και συσχέτιση της γεωγραφικής θέσης με ακόμα πιο ακριβείς πληροφορίες, άλλες βάσεις δεδομένων (ή μεταδεδομένων) ή άλλα σχετιζόμενα μοτίβα συμπεριφοράς ή επικοινωνίας, είναι εφικτό να αποκαλύψει το ίδιο το περιεχόμενο της επικοινωνίας και κυρίως να σχηματίσει ένα ιδιαίτερος εξαντλητικό και διεισδυτικό προφίλ για συγκεκριμένο πρόσωπο ή ομάδες προσώπων. Καταρχήν, ακόμα και μόνη η γνώση ανωνυμοποιημένων πληροφοριών σε σχέση με τη θέση μιας τερματικής συσκευής, είναι δυνατό να οδηγήσει στην αναγνώριση του κατόχου της ⁸⁹. Δεν είναι παράλογο κατόπιν αυτών, ότι η γεωγραφική θέση θεωρείται το πιο σημαντικό μεταδεδομένο επικοινωνίας⁹⁰.

Αν σε αυτά συνεκτιμήσει κανείς άλλες διαθέσιμες τεχνικές ταυτοποίησης, συλλογής και ανάλυσης πληροφοριών, όπως:

- τη δυνατότητα να αναγνωριστεί μια συσκευή⁹¹ και να δημιουργηθεί ένα μοναδικό «δακτυλικό» αποτύπωμα αυτής (device fingerprint) απλώς και μόνο από τους ενσωματωμένους σε αυτό αισθητήρες (δίχως καν τη χρήση «σκληρών» μοναδικών αναγνωριστικών πχ του IMEI⁹²),

- τη συλλογή δεδομένων μέσα από cookies και ψηφιακούς ιχνηλάτες (trackers) και άλλες, γίνεται αντιληπτό ότι το επίπεδο των κινδύνων που συνεπάγεται η επεξεργασία των μεταδεδωμένων σε σχέση με το απόρρητο των (ψηφιακών κυρίως) επικοινωνιών όσο και την ιδιωτικότητα, είναι υψηλό.

Τεκμηρίωση

Σημαντικό τμήμα των παραπάνω εκτιμήσεων, δεν αποτελούν λογικές εκτιμήσεις, αλλά έχουν επιβεβαιωθεί και με ερευνητικά δεδομένα.

Ειδικότερα, έχει αποδειχθεί ότι η επεξεργασία των δεδομένων δικτύου κινητής τηλεφωνίας (mobile phone network data) μπορεί σε συλλογικό επίπεδο να αποκαλύψει για παράδειγμα:

- τον τόπο εργασίας και κατοικίας, την κινητικότητα ομάδων χρηστών (mobility estimation), τις χρήσεις γης σε μια δεδομένη περιοχή, την εκδήλωση γεγονότων και του χαρακτήρα αυτών⁹³,
- τη δομή των κοινωνικών δικτύων (social networks structure)⁹⁴
- τα ταξιδιωτικά μοτίβα και μοτίβα εισαγωγής ασθενειών σε μια συγκεκριμένη περιοχή⁹⁵
- τον προσδιορισμό μιας κοινότητας ενδιαφέροντος (community of interest)⁹⁶
- τη δομή και την ιεραρχία ενός οργανισμού⁹⁷
- τα χαρακτηριστικά μιας κοινότητας^{98, 99}
- τη σχέση μεταξύ τοποθεσίας φυσικών προσώπων και των επικοινωνιών τους¹⁰⁰
- τα οικονομικά χαρακτηριστικά μιας συγκεκριμένης περιοχής¹⁰¹
- τους κοινωνικούς δεσμούς¹⁰²

- την αποκάλυψη της δομής και της ιεραρχίας εγκληματικών δικτύων¹⁰³

ενώ σε ατομικό επίπεδο μπορεί:

- να οδηγήσει στην ταυτοποίηση μιας συγκεκριμένης συσκευής¹⁰⁴
- να οδηγήσει στην αναγνώριση της δραστηριότητας μιας συγκεκριμένης συσκευής^{105, 106}
- να οδηγήσει στην αναγνώριση του χρήστη μιας συσκευής ή ακόμα και μιας εφαρμογής^{107, 108}
- να οδηγήσει στο σχηματισμό προφίλ για ένα συγκεκριμένο χρήστη^{109, 110, 111}
- να οδηγήσει στην αναγνώριση της προσωπικότητας του χρήστη¹¹²
- να οδηγήσει στην ανακάλυψη του σεξουαλικού προσανατολισμού, της εθνικότητας¹¹³

Ακόμα πιο τολμηρές προσεγγίσεις σε σχέση με την ανάλυση μεταδεδομένων, αναφέρονται στη δυνατότητα όχι μόνο να αναλυθεί το παρελθόν, αλλά και να προβλεφθεί η μελλοντική συμπεριφορά ενός συγκεκριμένου προσώπου¹¹⁴. Η ανάλυση σημαντικού όγκου μεταδεδομένων σχηματίζει μοτίβα συμπεριφοράς τα οποία σχετιζόμενα με άλλες διαθέσιμες πληροφορίες μπορούν να αποκαλύψουν προθέσεις, σχέδια, μελλοντικές ανάγκες, φόβους και επιθυμίες¹¹⁵.

Εν γένει, η ανάλυση μεταδεδομένων επικοινωνίας, οδηγεί στην ανακάλυψη «μοτίβων ζωής» (Pattern-of-Life ή POL) και συνιστά τμήμα της σχετικής μεθόδου (POL Analytics)¹¹⁶.

Είναι φανερό ότι το πλήθος, η έκταση και το βάθος των συμπερασμάτων που μπορούν να εξαχθούν μέσω της ανάλυσης των μεταδεδομένων, δεν αποκαλύπτουν απλώς το περιεχόμενο των επικοινωνιών, αλλά ταυτόχρονα ένα πλήθος πληροφοριών που εντάσσονται στον πυρήνα της ιδιωτικότητας. Η διαθέσιμη τεχνολογία καθιστά δυνατή την πλήρη επιτήρηση προσώπων και ομάδων, σε βαθμό που τα καθιστά αντικείμενο μιας διαρκούς παρακολούθησης και ανάλυσης του συνόλου των βιοτικών γεγονότων που σχετίζονται με αυτά. Η πραγματικότητα αυτή δημιουργεί εξ αρχής μια σχέση υψηλής έντασης μεταξύ τεχνολογιών επικοινωνιών και των δικαιωμάτων απόρρητης επικοινωνίας και προστασίας δεδομένων προσωπικού χαρακτήρα, μετατοπίζοντας τη συζήτηση στο

θεσμικό πλαίσιο, στη λειτουργία του όσο και στα οργανωτικά και τεχνικά μέτρα που εφαρμόζουν οι πάροχοι υπηρεσιών τηλεφωνίας και ηλεκτρονικών επικοινωνιών.

Η μετατόπιση των υπηρεσιών ασφαλείας όσο και των διωκτικών αρχών στη συλλογή και ανάλυση μεταδεδομένων, μόνο τυχαία δεν ήταν.

Σημειώσεις για τον πληροφοριακό πλούτο των μεταδεδομένων και του τρόπου ανάλυσης αυτών

Δημιουργεί εύλογη απορία για ποιο λόγο τα μεταδεδομένα επικοινωνίας¹¹⁷ είναι τόσο πλούσια σε πληροφορίες και αποκαλυπτικά. Πέραν του γεγονότος ότι είναι δομημένα δεδομένα, τρία ακόμα χαρακτηριστικά συμβάλλουν σε αυτή την κατεύθυνση:

A) είναι πληροφορίες που δημιουργούνται/πυροδοτούνται από γεγονότα (event-triggered data¹¹⁸)¹¹⁹ σε ένα περιβάλλον προορισμένο να καταγράφει κάθε είδους ενέργεια ή συμβάν

B) είναι κατά βάση πληροφορίες ανθρώπινης συμπεριφοράς (behavioral data)

Γ) είναι πληροφορίες που μπορούν να τύχουν αλγοριθμικής ανάλυσης

A. Τα μεταδεδομένα επικοινωνίας παράγονται, συλλέγονται και καταχωρούνται με αυτοματοποιημένο τρόπο χωρίς κάποια επιπλέον ενέργεια απ' την πλευρά του χρήστη, χρησιμοποιώντας ένα τερματικό επικοινωνίας, με τρόπο που δε μπορεί να αποποιηθεί τη σχέση του σε σχέση με αυτά. Η ολοκληρωμένη πληκτρολόγηση ενός τηλεφωνικού αριθμού, η αποστολή ενός sms, η πληκτρολόγηση ενός URL στον browser, η αποστολή ενός email, χαρακτηρίζονται ως γεγονότα (events) τα οποία παράγονται από ένα συγκεκριμένο χρήστη (user-generated events). Δηλαδή, οι ενέργειες που συντελούν αποφασιστικά στην υλοποίηση μιας επικοινωνίας, αποκτούν συγκεκριμένο χαρακτήρα εντός της βάσης δεδομένων στην οποία καταχωρούνται και κατ' αυτό τον τρόπο καθίσταται διαθέσιμες προς ανάλυση.

B. Τα μεταδεδομένα επικοινωνίας μπορούν να καταταχθούν σε 3 επιπλέον υποκατηγορίες (σε σχέση με τις αρχικά αναφερθείσες):

1. σε αυτά που συνιστούν μοναδικά αναγνωριστικά (unique identifiers): ο αριθμός κλήσης, η διεύθυνση email, το όνομα χρήστη, η mac address κλπ
2. σε αυτά που αφορούν τις συνθήκες της επικοινωνίας: ημερομηνία, ώρα, τόπος, δίκτυο
3. σε αυτά που αφορούν το είδος ή το περιεχόμενο της επικοινωνίας: ετικέτες, κωδικοποίηση, μέγεθος
4. σε αυτά που περιγράφουν συγκεκριμένο είδος ενέργειας ενός ταυτοποιημένου (μοναδικά αναγνωρισμένου) χρήστη σε ένα δεδομένο μέσο επικοινωνίας

Γίνεται εύκολα αντιληπτό ότι η εξέταση των ανωτέρω πληροφοριών, τόσο μεμονωμένα καθώς και σε συνδυασμό μεταξύ τους, αποτυπώνει μεν τεχνικές κατ' αρχήν πληροφορίες, οι οποίες όμως αποκαλύπτουν συγκεκριμένη ανθρώπινη συμπεριφορά (επικοινωνιακή ή άλλη), αναγνωρισμένου προσώπου, υπό προσδιορισμένες συνθήκες (τόπος, χρόνος, διάρκεια, μέσο). Στο σημείο αυτό λοιπόν διασταυρώνονται τρεις πυλώνες πληροφοριών (ενέργεια, ταυτότητα προσώπου, συνθήκες) οι οποίες είναι καθοριστικής σημασίας για την περαιτέρω ανάλυση ενός επικοινωνιακού (ή άλλου) γεγονότος. Εάν σε αυτό το επίπεδο απουσίαζε κάποιος εκ των τριών πυλώνων, δε θα ήταν κατ' αρχήν (αλλά όχι και τελειωτικά) εφικτή η αποτύπωση συγκεκριμένης ανθρώπινης συμπεριφοράς.

Το στοιχείο όμως που διαφεύγει της προσοχής και αξίζει να συνεκτιμηθεί σε σχέση με τα ανωτέρω, είναι ότι στη σημερινή εποχή, η αλληλεπίδραση των ανθρώπων με τα μέσα επικοινωνίας (ιδίως τα ψηφιακά πχ κινητό τηλέφωνο, υπολογιστής):

1. είναι καθημερινή και αφορά όλες τις ώρες τις ημέρας¹²⁰.
2. αφορά τόσο το χρόνο εργασίας, όσο και τον ελεύθερο χρόνο.

Δηλαδή, η παραγωγή των μεταδεδομένων επικοινωνίας, συνδέεται ευθέως με όλες τις ενέργειες και τα βιοτικά γεγονότα ενός προσώπου καθ' όλη τη διάρκεια του χρόνου και όχι μόνο με όσες συνιστούν επικοινωνία εν στενή εννοία (πχ κλήση, αποστολή μηνύματος κλπ). Υπενθυμίζουμε ότι η γεωγραφική θέση μιας τερματικής συσκευής καταγράφεται ακόμα και όταν αυτή δε χρησιμοποιείται για σκοπούς επικοινωνίας.

Γ. Η ύπαρξη ή η συγκέντρωση όλων των ανωτέρω πληροφοριών σε ένα σύνολο (πχ σε μια βάση δεδομένων), επιτρέπει την πλήρη αποτύπωση ενός επικοινωνιακού γεγονότος

αναφορικά με συγκεκριμένα πρόσωπα και σε δεύτερο επίπεδο την εξαγωγή συμπερασμάτων.

Ακόμα και η απάλειψη, η ανωνυμοποίηση ή η ψευδωνυμοποίηση κάποιων κατηγοριών από αυτές, δεν είναι ικανή συνθήκη σε σχέση με την αποτροπή ταυτοποίησης των επικοινωνούντων, του είδους ή ακόμα και του περιεχομένου της μεταξύ τους επικοινωνίας.

Και τούτο διότι:

1. είναι πιθανή η ύπαρξη δημόσιων (ή κατ' άλλο τρόπο) διαθέσιμων πληροφοριών σε σχέση με τους επικοινωνούντες, τη μεταξύ τους σχέση ή τα μέσα επικοινωνίας, οι οποίες επιτρέπουν τη «συμπλήρωση» των ελλειπόντων / ανωνυμοποιημένων / ψευδωνυμοποιημένων στοιχείων και την αποκατάσταση τυχόν κενών

2. είναι πιθανή η αξιοποίηση μοτίβων (patterns) σε σχέση με τους επικοινωνούντες τα οποία επιτρέπουν επίσης τη «συμπλήρωση» των ως άνω στοιχείων (είτε μοτίβα που έχουν δημιουργηθεί στο παρελθόν, είτε μοτίβα που δημιουργούνται από το συγκεκριμένο dataset), τα οποία προκύπτουν από αλγοριθμική ανάλυση.

Η αναγνώριση μοτίβων (pattern recognition) είναι η μια όψη της λειτουργίας των αλγορίθμων στο πλαίσιο της «εξόρυξης δεδομένων» (data mining). Η άλλη είναι η ανίχνευση ανωμαλιών (anomaly detection)¹²¹. Η αναγνώριση¹²² μοτίβων περιλαμβάνει την αυτοματοποιημένη αναγνώριση ομοιοτήτων, όμοιων συσχετισμών και κανονικοτήτων (regularities) σε ένα σύνολο δεδομένων, ενώ η ανίχνευση ανωμαλιών χαρακτηρίζει την αποτυχία υπαγωγής κάποιων δεδομένων, γεγονότων ή τάσεων έναντι ενός μοτίβου κανονικότητας, εντός του ίδιου πάντα συνόλου δεδομένων¹²³. Και οι δυο πλευρές της λειτουργίας των αλγορίθμων είναι προφανές ότι έχουν σημαντική επίδραση στην εξαγωγή συμπερασμάτων από ένα σύνολο μεταδεδομένων επικοινωνίας, αναφορικά με πρόσωπα ή ομάδες προσώπων. Όσο μεγαλύτερο είναι ένα τέτοιο σύνολο (σε σχέση με το χρονικό του βάθος, τις κατηγορίες πληροφοριών), τόσο περισσότερο θα είναι δυνατή η αναγνώριση διαφορετικού είδους μοτίβων με μικρότερο μάλιστα βαθμό αβεβαιότητας (εντροπίας)¹²⁴.

Οι παραπάνω σκέψεις μας οδηγούν στο συμπέρασμα ότι η μετάβαση από τα (εσφαλμένως αποκαλούμενα) «εξωτερικά στοιχεία της επικοινωνίας» στο ίδιο το περιεχόμενό της, εξαρτάται αποκλειστικά από:

α) τον όγκο των διαθέσιμων μεταδεδομένων αναφορικά με συγκεκριμένο πρόσωπο (ή πρόσωπα)^{125 126}

β) τον όγκο άλλων διαθέσιμων πληροφοριών με τα οποία αυτά μπορούν να συσχετιστούν

γ) τις τεχνικές δυνατότητες ανάλυσης μεταδεδομένων και συσχέτισης με άλλες διαθέσιμες πληροφορίες

Ο όγκος των διαθέσιμων μεταδεδομένων επικοινωνίας είναι εξαιρετικά μεγάλος λόγω του τρόπου λειτουργίας των σύγχρονων μέσων επικοινωνίας (ιδίως των ψηφιακών) και των προβλέψεων της νομοθεσίας σε σχέση με τη διατήρησή τους. Ο όγκος των λοιπών διαθέσιμων πληροφοριών και οι τεχνικές δυνατότητες ανάλυσης μεταδεδομένων, είναι στοιχεία γνωστά μόνο σε όσους προβαίνουν στις σχετικές έρευνες (πχ τις δημόσιες αρχές που επεξεργάζονται αιτήματα άρσης απορρήτου ή τους παρόχους επικοινωνιών¹²⁷).

Σε τεχνικό δηλαδή επίπεδο, ο τρόπος που είναι δομημένη η λειτουργία των τηλεφωνικών και ηλεκτρονικών επικοινωνιών, έχει ως αποτέλεσμα τη διαρκή και αδιάκριτη παραγωγή και συλλογή ποικίλων μεταδεδομένων επικοινωνίας, την παραγωγή σημαντικών, εκτεταμένων, διεισδυτικών, υψηλής ακρίβειας πληροφοριών αναφορικά με πρόσωπα και ομάδες, με τις προαναφερθείσες συνέπειες για την ιδιωτικότητα μεμονωμένων χρηστών όσο και ομάδων χρηστών, οι οποίες καταρχήν συλλέγονται και διατηρούνται από ιδιωτικούς φορείς (παρόχους επικοινωνιών).

Ως αποτέλεσμα, το απόρρητο της επικοινωνίας (όσο και η προστασία της ιδιωτικότητας) βρίσκεται διαρκώς σε κατάσταση διακινδύνευσης και η προστασία του εξαρτάται από τους παρόχους, την ποιότητα της νομοθεσίας, τον τρόπο εφαρμογής της και τις λοιπές ισχύουσες εγγυήσεις.

Η αναπόφευκτη τομή επικοινωνιακού απορρήτου και δεδομένων προσωπικού χαρακτήρα

Από τα παραπάνω καθίσταται φανερό ότι τα μεταδεδομένα επικοινωνίας, δε σχετίζονται αποκλειστικά με το απόρρητο των επικοινωνιών, αλλά συνιστούν ταυτόχρονα και δεδομένα προσωπικού χαρακτήρα. Το σύνολο των προαναφερθέντων πληροφοριών (και των πληροφοριών που συνάγονται από αυτά) συγκροτούν σε αρκετές περιπτώσεις ένα λεπτομερές μοτίβο ζωής ταυτοποιημένων ή ταυτοποιήσιμων φυσικών προσώπων και

υπάγονται ξεκάθαρα (και) στο προστατευτικό πεδίο της νομοθεσίας προστασίας δεδομένων προσωπικού χαρακτήρα. Η τομή αυτή αναδείχθηκε νομοθετικά με την Οδηγία 2002/58/ΕΚ¹²⁸ και σε εθνικό επίπεδο με το ν.3471/2006.

Το κρίσιμο σημείο σε σχέση με την προστασία των μεταδεδομένων επικοινωνίας, αφορά το πλαίσιο συλλογής και επεξεργασίας τους. Η έννοια του πλαισίου της συλλογής και επεξεργασίας (context) συνιστά μια ιδιαίτερη παράμετρο, η οποία αλληλοεπιδρά σε σχέση με την πιθανότητα, την έκταση και το είδος των κινδύνων και αυτό αναγνωρίζεται τόσο από τον ίδιο το Γενικό Κανονισμό Προστασίας Δεδομένων 679/2016/ΕΕ¹²⁹, όσο και από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (και παλαιότερα την Ομάδα Εργασίας του αρ.29)¹³⁰. Το πλαίσιο είναι μια γενική έννοια¹³¹ και περιλαμβάνει το σκοπό, το είδος και τα μέσα επεξεργασίας, τις κατηγορίες των υποκειμένων όσο και των δεδομένων καθώς και τα ιδιαίτερα χαρακτηριστικά του υπευθύνου επεξεργασίας. Τα στοιχεία αυτά προσδιορίζουν εν συνόλω τα πραγματικά όρια εντός των οποίων θα διεξαχθεί μια επεξεργασία και βεβαίως τα προσδιοριστικά στοιχεία των συναφών κινδύνων.

Λαμβάνοντας υπόψη την εκ μέρους των παρόχων συλλογή και διατήρηση σημαντικής έκτασης και όγκου μεταδεδομένων επικοινωνίας¹³² εκατομμυρίων ανθρώπων, το πλαίσιο αυτό διαμορφώνει ένα «μοναδικό σημείο αποτυχίας» (single point of failure¹³³) σε σχέση με το δικαίωμα προστασίας του απορρήτου της επικοινωνίας και το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών^{134 135}. Ο κίνδυνος ταυτόχρονης και καθολικής προσβολής των ανωτέρω δικαιωμάτων συγκεντρώνεται σε ένα σημείο¹³⁶ και η τυχόν αποτυχία των παρόχων να τα προστατεύσουν σε νομικό, οργανωτικό ή τεχνικό επίπεδο, συνεπάγεται την άμεση προσβολή του πυρήνα αυτών των δικαιωμάτων, καθώς δε μεσολαβεί κάποιο δεύτερο επίπεδο προστασίας. Ο κίνδυνος αυτός μάλιστα υπάρχει ήδη από το στάδιο της συλλογής και αυξάνει σε κάθε ένα από τα τυχόν επόμενα στάδια (στο στάδιο της διατήρησης, της επεξεργασίας, της χρήσης κλπ)¹³⁷. Η αναπόφευκτη τομή μεταξύ του απορρήτου της επικοινωνίας και δεδομένων προσωπικού χαρακτήρα, υποδηλώνει την ανάγκη συνολικής και συστηματικής προστασίας τους.

ΤΜΗΜΑ ΟΓΔΟΟ

Κατοχύρωση του απορρήτου της επικοινωνίας σε διεθνές επίπεδο

Αμέσως μετά τη λήξη του Β' Παγκοσμίου Πολέμου, επιχειρείται η επούλωση των πληγών αυτού και η δημιουργία μιας νέας διεθνούς «έννομης τάξης», η οποία έχει ως κύριο και κοινό χαρακτηριστικό την κατοχύρωση σειράς ανθρωπίνων δικαιωμάτων. Στο πλαίσιο αυτό, το δικαίωμα στην απόρρητη επικοινωνία κατοχυρώνεται με διάφορες διατυπώσεις σε σημαντικά νομικά κείμενα.

Στο άρθρο 12 της Οικουμενικής Διακήρυξης Δικαιωμάτων του Ανθρώπου (ΟΔΔΑ, 1948) ορίζεται ότι: *Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψής του. Κάθε άτομο έχει το δικαίωμα να το προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.* Παρότι ο όρος «correspondence» του αρχικού κειμένου αποδόθηκε στην ελληνική ως «αλληλογραφία», γίνεται δεκτό ότι αυτό αφορά όλες τις μορφές επικοινωνίας. Η άσκηση των δικαιώματος αυτού, τέθηκε υπό τη γενική επιφύλαξη του αρ.29 παρ.2 της ΟΔΔΑ.

Δύο χρόνια αργότερα, η κατοχύρωση του δικαιώματος του απορρήτου της επικοινωνίας έγινε πραγματικότητα και στο άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (1950), η οποία κατοχυρώθηκε στη χώρα μας με υπερνομοθετική ισχύ:

- 1. Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.*
- 2. Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.*

Η απόδοση του όρου correspondence γίνεται ξανά από τον Έλληνα μεταφραστή με τη χρήση της λέξης αλληλογραφία. Παρόλα αυτά, στη νομολογία του ΕΔΔΑ είναι πια αποδεκτό ότι ο όρος αυτός περιλαμβάνει κάθε μορφή επικοινωνίας. Κατωτέρω θα παρατεθούν

ενδιαφέρουσες νομολογιακές εξελίξεις αναφορικά με τη συλλογή μεταδεδομένων, όσο και τον τρόπο με τον οποίο το ΕΔΔΑ αξιολογεί την κρατική επέμβαση στο δικαίωμα αυτό.

Το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (ΔΣΑΠΔ, 1966¹³⁸) στο αρ.17, ακολούθησε τις διατυπώσεις της ΟΔΔΑ: *Κανείς δεν υπόκειται σε αυθαίρετες ή παράνομες παρενοχλήσεις της ιδιωτικής του ζωής, της οικογένειας, της κατοικίας ή της αλληλογραφίας του, ούτε σε παράνομες προσβολές της τιμής και της υπόληψής του. Κάθε πρόσωπο έχει δικαίωμα προστασίας από το νόμο έναντι τέτοιων παρενοχλήσεων ή προσβολών.*

Κατά το χρόνο που δημιουργήθηκαν και τέθηκαν σε εφαρμογή τα ανωτέρω νομοθετήματα, ήταν φανερό ότι η ανάγκη ειδικότερης προστασίας των μεταδεδομένων επικοινωνίας, δεν είχε τεθεί επί τάπητος.

Κατοχύρωση του απορρήτου της επικοινωνίας σε ευρωπαϊκό επίπεδο – το ζήτημα των μεταδεδομένων επικοινωνίας

Με τη Συνθήκη της Λισαβόνας, η οποία τέθηκε σε ισχύ από 1/12/2009, η Ένωση αναγνώρισε τα δικαιώματα, τις ελευθερίες και τις αρχές που περιέχονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕΕ) του 2000¹³⁹. Ο ΧΘΔΕΕ, ο οποίος κατά τον τρόπο αυτό κατέστη δεσμευτικό κείμενο, στο άρθρο 7 κατοχύρωσε το σεβασμό της ιδιωτικής και οικογενειακής ζωής, κάνοντας πια ρητή αναφορά σε επικοινωνίες και όχι σε αλληλογραφία.

Περαιτέρω, η Ευρωπαϊκή Κοινότητα με την Οδηγία 97/66/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και της προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα κατοχύρωσε ειδικότερα (στο άρθρο 5) την προστασία του επικοινωνιακού απορρήτου, επιβάλλοντας τη λήψη νομοθετικών μέτρων από τα κράτη μέλη, περιέλαβε διατάξεις για τα δεδομένα κίνησης και χρέωσης με τη ρητή επιφύλαξη (στο άρθρο 14) περιορισμού αυτού σε σχέση με σκοπούς διαφύλαξης της ασφάλειας του κράτους,

της εθνικής άμυνας, καθώς και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών παραβάσεων.

Η οδηγία αυτή καταργήθηκε και αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002 (γνωστή ως οδηγία e-privacy), σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

Η οδηγία καθιέρωσε το δικαίωμα στην ιδιωτική ζωή στον τομέα των ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των δεδομένων κίνησης, εξειδικεύοντας και συμπληρώνοντας την οδηγία 95/46/ΕΚ¹⁴⁰. Ειδικότερα, απαγόρευσε την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, υπό την επιφύλαξη του άρθρου 15 παράγραφος 1, δηλαδή επέτρεψε στα κράτη τη λήψη μέτρων διατήρησης των δεδομένων αυτών (κίνησης και θέσης) για περιορισμένο χρονικό διάστημα εφόσον αυτά αποτελούν αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία, δηλαδή υπό την επιφύλαξη της τήρησης της αρχής της αναλογικότητας. Ωστόσο, άφησε αρκετά ανοικτό το πεδίο της διατήρησης των δεδομένων, προβλέποντας την έννοια της τεχνικής αποθήκευσης, η οποία είναι αναγκαία για τη διαβίβαση επικοινωνίας.

Στο αρ.15 της οδηγίας προβλέφθηκε η δυνατότητα των κρατών μελών να λαμβάνουν νομοθετικά μέτρα που θα προβλέπουν τη φύλαξη δεδομένων για ορισμένο χρονικό διάστημα για τους σκοπούς διαφύλαξης της εθνικής ασφάλειας, της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδείας χρησιμοποίησης του συστήματος ηλεκτρονικών επικοινωνιών, εφόσον ο περιορισμός αυτός αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία.

Η οδηγία δεν κατέστησε σαφές στο κυρίως σώμα αυτής, ποιες τελικά συγκεκριμένες κατηγορίες δεδομένων περιλαμβάνονται στα δεδομένα κίνησης. Ωστόσο, στο αρ.14 της αιτιολογικής έκθεσης περιέλαβε ότι:

Τα δεδομένα θέσης μπορεί να 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

ενώ στο αρ.15 της αιτιολογικής έκθεσης περιέλαβε ότι:

Τα δεδομένα κίνησης μπορεί, μεταξύ άλλων, να αναφέρονται 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. Μπορεί επίσης να συνίστανται στο σχήμα με το οποίο η επικοινωνία μεταβιβάζεται από το δίκτυο.

Το 2006, στον απόηχο των τρομοκρατικών επιθέσεων στη Μαδρίτη και στο Λονδίνο¹⁴¹ και υπό την επιρροή του Προγράμματος της Χάγης¹⁴², τέθηκε σε ισχύ η οδηγία 2006/24/EK¹⁴³. Συνοπτικά, η οδηγία αυτή καθιέρωσε την υποχρέωση των κρατών- μελών να διατηρούν προληπτικά και υποχρεωτικά εκτεταμένες κατηγορίες μεταδεδομένων επικοινωνίας σε σχέση με την τηλεφωνία σταθερού δικτύου, την κινητή τηλεφωνία, την πρόσβαση στο Διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και τηλεφωνίας μέσω του Διαδικτύου, για χρονικό διάστημα από 6 μήνες έως 2 έτη, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων, όπως ορίζονται βάσει του εθνικού δικαίου των κρατών μελών. Η Οδηγία αυτή είχε ως αποτέλεσμα, τη δευτερεύουσα χρήση των δεδομένων αυτών, ερχόμενη σε αντίθεση από την αρχή του δεσμευτικά καθορισμένου και σαφούς σκοπού της επεξεργασίας¹⁴⁴, η οποία Οδηγία ωστόσο ακυρώθηκε από την απόφαση Digital Rights Ireland του ΔΕΕ¹⁴⁵.

Το 2017 υποβλήθηκε από την Ευρωπαϊκή Επιτροπή το σχέδιο Κανονισμού 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 για την

ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) ενώ στις 10-02-2021 ανακοινώθηκε η συμφωνία επ' αυτού, χωρίς ωστόσο ακόμα να έχει ψηφισθεί.

Στο σχέδιο Κανονισμού απαλείφεται η διάκριση μεταξύ περιεχομένου και δεδομένων κίνησης και θέσης, κυριαρχεί ο όρος μεταδεδομένα (αντί του όρου δεδομένα κίνησης/θέσης) ή δεδομένα ηλεκτρονικών επικοινωνιών, τα οποία εν συνόλω συγκαταλέγονται και προστατεύονται από το απόρρητο της επικοινωνίας. Το ενδιαφέρον στοιχείο είναι ότι ως προστατευόμενη επικοινωνία ορίζεται και αυτή που λαμβάνει χώρα μεταξύ συνδεδεμένων συσκευών όσο και μεταξύ μηχανών, υποδεικνύοντας ότι το διαδίκτυο των πραγμάτων (Internet of Things) δεν εξαιρείται από αυτή. Η ρύθμιση αυτή είναι ιδιαίτερα σημαντική καθώς ο αριθμός των συνδεδεμένων με το διαδίκτυο συσκευών παρουσιάζει αλματώδη αύξηση, ενώ παράγει πλήθος μεταδεδομένων, τα οποία σχετίζονται, ταυτοποιούν και αποκαλύπτουν πλήθος σημαντικών πληροφοριών για τους χρήστες τους.

Κριτικές παρατηρήσεις

Η ενωσιακή νομοθεσία (όσο και η εθνική όπως θα δούμε στη συνέχεια) αναφορικά με τη συλλογή μεταδεδομένων επικοινωνίας, δεν περιέχει διαβαθμίσεις και κριτήρια σε σχέση με τη συλλογή τους: εκτεταμένες και μάλιστα ενδεικτικώς (άρα όχι και οριστικώς) οριζόμενες κατηγορίες μεταδεδομένων συλλέγονται καθημερινά και αδιάλειπτα από τους παρόχους τηλεφωνικών υπηρεσιών και υπηρεσιών διαδικτύου, χωρίς ο χρήστης να μπορεί να το αποτρέψει¹⁴⁶. Δεν υφίστανται καν αναφορές σε τεχνικά μέτρα ώστε να μειώνεται το επικοινωνιακό αποτύπωμα των χρηστών¹⁴⁷.

Η απουσία τέτοιων μέτρων, υποδηλώνει το εξής ενδιαφέρον: ναι μεν ο καταρχήν σκοπός συλλογής και επεξεργασίας των μεταδεδομένων επικοινωνίας αφορά την πραγματοποίηση των επικοινωνιών και τη χρέωση των αντίστοιχων υπηρεσιών, αλλά τα μεταδεδομένα, με τις απεριόριστες δυνατότητες εξαγωγής συμπερασμάτων για πρόσωπα και ομάδες, παραμένουν διαθέσιμα και για άλλους σκοπούς, τελικά μεταξύ των οποίων και για σκοπούς ποινικής πρόληψης και καταστολής¹⁴⁸.

ΤΜΗΜΑ ΕΝΑΤΟ

Η ευρωπαϊκή νομολογία

Το ερώτημα της προστασίας των μεταδεδομένων επικοινωνίας ως στοιχείο του επικοινωνιακού απορρήτου, έχει τεθεί με emphaticό τρόπο στην ευρωπαϊκή νομολογία.

Αποφάσεις του ΕΔΔΑ

Το ΕΔΔΑ στην υπόθεση *Malone v. United Kingdom* (1984) αναγνώρισε παραβίαση του αρ.8 της ΕΣΔΑ διότι η λειτουργία του μηχανήματος παρακολούθησης (metering) είχε ως αποτέλεσμα την καταγραφή των κληθέντων τηλεφωνικών αριθμών, τα οποία συνιστούν αναπόσπαστο στοιχείο των τηλεφωνικών επικοινωνιών¹⁴⁹, καθιστώντας αναμφισβήτητη την ανάγκη προστασίας και αυτών των στοιχείων εντός του επικοινωνιακού απορρήτου¹⁵⁰.

Στην υπόθεση *Kopp v. Switzerland* (1994) (όσο και στην *Kruslin v. France* το 1990) διαπιστώνει κατά πάγιο τρόπο ότι η καταγραφή της συνομιλίας (το λεγόμενο tapping) όσο και άλλες μορφές παρακολούθησης των τηλεφωνικών συζητήσεων συνιστούν σημαντική επέμβαση στην ιδιωτική ζωή, ενώ απαιτεί την ύπαρξη σαφών και λεπτομερών κανόνων, ιδίως λόγω του ότι η σχετικώς διαθέσιμη τεχνολογία καθίσταται ολοένα και πιο εξελιγμένη¹⁵¹. Το Δικαστήριο δηλαδή είχε διαγνώσει όχι μόνο την ανάγκη προστασίας των «εξωτερικών» στοιχείων της επικοινωνίας αλλά και το ότι το απόρρητο της επικοινωνίας εν γένει είναι δυνατό να υπονομευθεί από το διαρκώς εξελισσόμενο επίπεδο των τεχνικών μέσων παρακολούθησης.

Στην υπόθεση *Copland v. The United Kingdom* (2007) το Δικαστήριο υπενθυμίζοντας όσα είχε πει στην υπόθεση *Malone* έκρινε ότι στοιχεία τηλεφωνικών επικοινωνιών (όπως οι τηλεφωνικοί αριθμοί, οι ημερομηνίες, η διάρκεια), στοιχεία υπηρεσιών ηλεκτρονικού ταχυδρομείου καθώς και της χρήσης του διαδικτύου, υπάγονται στην προστασία του αρ.8 της ΕΣΔΑ¹⁵² ενώ η συλλογή και αποθήκευσή τους συνιστά επέμβαση στο δικαίωμα ιδιωτικότητας.

Αποφάσεις του ΔΕΕ

Το ΔΕΕ στην υπόθεση Digital Rights Ireland κλπ¹⁵³ αξιολόγησε την Οδηγία 2006/24/EK¹⁵⁴ η οποία προέβλεπε την υποχρεωτική διατήρηση δεδομένων κίνησης και θέσης που αφορούν τον τομέα των ηλεκτρονικών επικοινωνιών, αναφορικά με τη συμβατότητά της με το Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Το Δικαστήριο υπενθύμισε αρχικά ότι το απόρρητο των δεδομένων κίνησης κατοχυρώνεται ήδη στην Οδηγία 2002/58. Εν συνεχεία, στις σκέψεις 26 και 27 τόνισε ότι τα δεδομένα που πρέπει να διατηρούν οι πάροχοι βάσει των αρ.3 και 5 της Οδηγίας 2006/24 είναι, μεταξύ άλλων, αυτά που είναι αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας και του προορισμού της, για τον προσδιορισμό της ημερομηνίας, της ώρας, της διάρκειας και του είδους της επικοινωνίας, του εξοπλισμού επικοινωνίας των χρηστών, καθώς και για τον προσδιορισμό της θέσεως του εξοπλισμού κινητής επικοινωνίας.

Έκρινε επιπλέον με τις ίδιες σκέψεις τα εξής σημαντικά:

1) ότι τα δεδομένα αυτά 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 όσο και τη δυνατότητα να διαπιστωθεί η συχνότητα των επικοινωνιών του συνδρομητή ή του εγγεγραμμένου χρήστη με συγκεκριμένα πρόσωπα σε δεδομένη χρονική περίοδο.

2) ότι τα δεδομένα αυτά, λαμβανόμενα στο σύνολό τους, παρέχουν τη δυνατότητα κυρίως συναγωγής συμπερασμάτων με ακρίβεια 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.

Στη σκέψη υπ' αριθμ 62 έκρινε ότι η πρόσβαση στα διατηρούμενα δεδομένα από τις αρμόδιες εθνικές αρχές δεν εξαρτάται από προηγούμενο έλεγχο πραγματοποιούμενο είτε από δικαστήριο είτε από ανεξάρτητη διοικητική αρχή με απόφαση η οποία έχει σκοπό να περιορίσει την πρόσβαση στα δεδομένα και την εν συνεχεία χρήση τους στον απολύτως αναγκαίο βαθμό,

προκειμένου να επιτευχθεί ο επιδιωκόμενος σκοπός, και εκδιδόμενη κατόπιν αιτιολογημένη αιτήσεως των αρχών αυτών υποβληθείσας στο πλαίσιο των διαδικασιών για την πρόληψη, τη διαπίστωση ή την ποινική δίωξη. Δηλαδή, εξάρτησε ευθέως την πρόσβαση των αρμοδίων αρχών σε αυτά τα δεδομένα από προηγούμενο έλεγχο δικαστηρίου ή ανεξάρτητης αρχής, με την έκδοση αιτιολογημένης απόφασης η οποία θα διασφαλίζει τη χρήση τους μόνο στον αναγκαίο βαθμό, τονίζοντας με εμφατικό τρόπο τις διαδικαστικές προϋποθέσεις και εγγυήσεις που οφείλουν τα κράτη να λαμβάνουν σε σχέση με αυτά τα δεδομένα.

Κατόπιν αυτών, έκρινε ανίσχυρη την Οδηγία 2006/24/EK διότι παρέκκλινε από το καθεστώς της προστασίας του δικαιώματος στον σεβασμό της ιδιωτικής ζωής, που καθιέρωναν οι οδηγίες 95/46 και 2002/58 και συνιστά επέμβαση στα θεμελιώδη δικαιώματα που καθιερώνουν τα άρθρα 7 και 8 του Χάρτη, η οποία μάλιστα έχει τεράστιο εύρος. Σημειωτέο ότι με την Οδηγία 2006/24/EK καταργούνται και η αρχή της αναλογικότητας που προέβλεπε η Οδηγία 2002/58, ενώ δεν προέβλεπε την καταστροφή των δεδομένων αυτών μετά την οριζόμενη διάρκεια διατήρησης¹⁵⁵. Εκτός αυτών, διαπίστωσε ότι η μη ενημέρωση των χρηστών σε σχέση με τη συλλογή και επεξεργασία αυτών των δεδομένων αυτών συντέεινε στη δημιουργία μιας αίσθησης ότι η ιδιωτική ζωή αποτελεί αντικείμενο διαρκούς παρακολούθησης, αναγνωρίζοντας δηλαδή έμμεσα την πρόκληση ενός φαινομένου αποθαρρυντικής επίδρασης (chilling effect) των πολιτών σε σχέση με την ακώλυτη άσκηση των δικαιωμάτων τους. Με την ακύρωση της Οδηγίας 2006/24, η ευρωπαϊκή έννομη τάξη επανήλθε στο καθεστώς που ίσχυε προηγουμένως, δηλαδή στην Οδηγία 2002/58 και στο αρ.15 παρ.1 αυτής.

Σημαντική επίσης είναι η απόφαση Tele 2 Sverige του ΔΕΕ¹⁵⁶. Στην υπόθεση αυτή κρίθηκε ότι αντιβαίνει προς τη διάταξη του άρθρου 15 παρ. 1 της Οδηγίας 2002/58 εθνική ρύθμιση, η οποία προς τον σκοπό καταπολεμήσεως του εγκλήματος, προβλέπει γενική και χωρίς διάκριση διατήρηση του συνόλου των δεδομένων κινήσεως και των δεδομένων θέσεως όλων των συνδρομητών και των εγγεγραμμένων χρηστών και αφορά όλα τα μέσα ηλεκτρονικής επικοινωνίας.

Τέλος, στην πρόσφατη απόφαση H.K. – Prokuratuur¹⁵⁷ το ΔΕΕ ερμηνεύοντας τις διατάξεις της Οδηγίας 2002/58 υπενθύμισε ότι το αρ.15 αυτής, υπό το πρίσμα των άρθρων 7, 8 και 11 καθώς και του άρθρου 52, παράγραφος 1, του Χάρτη, αντιτίθεται σε νομοθετικά μέτρα τα οποία

προβλέπουν, για τους σκοπούς αυτούς, προληπτικώς, τη γενικευμένη και χωρίς διάκριση διατήρηση των δεδομένων κίνησης και των δεδομένων θέσης¹⁵⁸.

Έκρινε επίσης ότι:

1. μόνον η καταπολέμηση του σοβαρού εγκλήματος και η πρόληψη σοβαρών απειλών κατά της δημόσιας ασφάλειας μπορούν να δικαιολογήσουν σοβαρές επεμβάσεις στα θεμελιώδη δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη, όπως αυτές από τις οποίες συνεπάγεται η διατήρηση των δεδομένων κίνησης και των δεδομένων θέσης, είτε αυτή είναι γενική και χωρίς διάκριση είτε στοχευμένη¹⁵⁹.

2. η επέμβαση στα θεμελιώδη δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη, την οποία συνεπάγεται η πρόσβαση δημόσιας αρχής σε σύνολο δεδομένων κίνησης ή δεδομένων θέσης, από τα οποία μπορούν να αντληθούν πληροφορίες σχετικά με τις επικοινωνίες που πραγματοποίησε χρήστης μέσου ηλεκτρονικής επικοινωνίας ή σχετικά με τον γεωγραφικό εντοπισμό του τερματικού εξοπλισμού τον οποίο χρησιμοποιεί, χαρακτηρίζεται σε κάθε περίπτωση σοβαρή, ανεξαρτήτως της διάρκειας του χρονικού διαστήματος για το οποίο έχει ζητηθεί η πρόσβαση στα εν λόγω δεδομένα και του όγκου ή του είδους των διαθέσιμων δεδομένων για το διάστημα αυτό, όταν [...] από το εν λόγω σύνολο δεδομένων μπορούν να συναχθούν ακριβή συμπεράσματα σχετικά με την ιδιωτική ζωή του οικείου προσώπου ή των οικείων προσώπων¹⁶⁰.

3. η σοβαρότητα της επέμβασης την οποία συνιστά η πρόσβαση εκτιμάται κατ' ανάγκην σε συνάρτηση με τον κίνδυνο που εν γένει συνδέεται με την κατηγορία των δεδομένων στα οποία ζητείται πρόσβαση για την ιδιωτική ζωή των οικείων προσώπων, χωρίς να έχει σημασία, αν οι πληροφορίες σχετικά με την ιδιωτική ζωή που απορρέουν από τα δεδομένα αυτά είναι ή όχι ευαίσθητες¹⁶¹.

Το ΔΕΕ δηλαδή συνδέει την πρόσβαση των δημοσίων αρχών σε δεδομένα κίνησης και θέσης μόνο με την ανάγκη καταπολέμησης της βαριάς εγκληματικότητας και των **σοβαρών** απειλών κατά της δημόσιας ασφάλειας και όχι έναντι κάθε απειλής. Επιπλέον, κρίνει κάθε πρόσβαση σε τέτοιο σύνολο δεδομένων ως αυτοτελώς σοβαρή επέμβαση, ανεξαρτήτως του διαστήματος πρόσβασης και του όγκου, διότι από αυτό είναι δυνατό να εξαχθούν ακριβή συμπεράσματα για τη ζωή ενός προσώπου. Υιοθετεί δε σε κάθε περίπτωση μια αναλογική εκτίμηση κινδύνου που συνεπάγεται η πρόσβαση για την ιδιωτική ζωή.

Δηλαδή, σύμφωνα με το ΔΕΕ, το αν νομίμως ζητούν πρόσβαση οι δημόσιες αρχές σε δεδομένα κίνησης και θέσης, εξαρτάται¹⁶² από τις σοβαρές συνέπειες και τον κίνδυνο που είναι δυνατό να έχει αυτή στην ιδιωτικότητα. Με άλλα λόγια, το είδος, η διάρκεια και η έκταση της πρόσβασης σε δεδομένα κίνησης και θέσης, πρέπει να σταθμίζονται με μεγάλη προσοχή, λόγω ακριβώς της δυνατότητας εξαγωγής πλήθους συμπερασμάτων για την ιδιωτική ζωή ενός προσώπου. Μια έρευνα από δημόσιες αρχές, δεν πρέπει να συνεπάγεται την κατάργηση κάθε έννοιας ιδιωτικότητας των ερευνόμενων προσώπων. Η κρίση αυτή είναι ιδιαίτερος χρήσιμη προς αντιπαραβολή σε σχέση με τα ισχύοντα σε εθνικό επίπεδο.

ΤΜΗΜΑ ΔΕΚΑΤΟ

Συνοπτική αναφορά της εθνικής νομοθεσίας για την προστασία του απορρήτου και των μεταδεδομένων επικοινωνίας

Το άρθρο 19 του Συντάγματος

Η προστασία του απορρήτου της επικοινωνίας κατοχυρώνεται ρητά στο αρ.19 του Συντάγματος¹⁶³, το οποίο ορίζει ότι:

- 1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.*
- 2. Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1.*
- 3. Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α.*

Η πρωτόλεια κατοχύρωση εντοπίζεται στο Σύνταγμα του 1844, στο οποίο εισήχθη ως επιρροή από ευρωπαϊκά συνταγματικά κείμενα¹⁶⁴, ενώ η ρητή κατοχύρωση γίνεται πανηγυρικά στο Σύνταγμα του 1864. Με τη συντακτική πράξη του 1974 επανήλθε σε ισχύ το Σύνταγμα του 1952 και ταυτόχρονα τροποποιήθηκε το αρ.20 στο οποίο (τότε) προβλεπόταν. Με το Ψήφισμα της 6ης Απριλίου 2001 της Ζ' Αναθεωρητικής Βουλής των Ελλήνων προστέθηκαν οι παράγραφοι 2 και 3 και έλαβε τη μορφή που διατηρεί μέχρι σήμερα.

Η σημερινή διατύπωση του δικαιώματος στην απόρρητη επικοινωνία είναι αρκετά ανοικτή και περιλαμβάνει με επιτυχημένα λακωνικό τρόπο κάθε μορφή επικοινωνίας και μέσο ανταλλαγής πληροφοριών και μηνυμάτων. Αξίζει μνείας ότι ο όρος «επικοινωνία» είναι ιδιαίτερα πυκνός και ευρύς, περιλαμβάνοντας αυτή που διεξάγεται μεταξύ δύο ή περισσότερων προσώπων (πχ τηλεφωνική) αλλά και τη μετάδοση μηνυμάτων, σκέψεων, προθέσεων, τα οποία δεν είναι κατ' αρχήν απαραίτητο να έχουν κάποιο άμεσο αποδέκτη

(ενώ πάντα ενδέχεται τελικά να καταλήξουν σε κάποιον). Δηλαδή, η συνταγματική προστασία καλύπτει τόσο την αμφίδρομη όσο και τη μονόδρομη επικοινωνία¹⁶⁵.

Το συνταγματικό αυτό δικαίωμα καλύπτει όλες τις μορφές επικοινωνίας, οι οποίες λόγω του τρόπου και των συνθηκών που διεξάγονται δημιουργούν την εύλογη πεποίθηση στους επικοινωνούντες ότι σε αυτή δε θα έχουν πρόσβαση τρίτοι, χωρίς την ανάγκη λήψης επιπλέον μέτρων¹⁶⁶, τα οποία ωστόσο εάν υφίστανται συνιστά μια επιπλέον απόδειξη του απόρρητου χαρακτήρα αυτής. Η πεποίθηση αυτή κατ' αρχήν αφορά το περιεχόμενο, αλλά η προστασία θα ήταν ανεπαρκής αν εξαντλούνταν σε αυτό.

Για να αναλογιστούμε τα όρια της συνταγματικής προστασίας, αξίζει να αναρωτηθούμε το εξής: θα πρέπει η πραγματοποίηση μιας αναπάντητης κλήσης ή η αποστολή μιας κενής επιστολής να καλύπτεται από το επικοινωνιακό απόρρητο; Δηλαδή, σε περιπτώσεις που η επικοινωνία είναι τυπικά μονόδρομη και παράγει μόνο μεταδεδομένα επικοινωνίας¹⁶⁷ και όχι περιεχόμενο, θα πρέπει αυτή να θεωρείται απόρρητη;

Κατεύθυνση στο ερώτημα μπορεί να δοθεί αν εξετάσει κανείς την αρνητική εκδοχή της απάντησης. Η απόρριψη της συνταγματικής προστασίας γι' αυτές τις περιπτώσεις, θα είχε ως αποτέλεσμα τον αδικαιολόγητα στενό προσδιορισμό της επικοινωνίας ως:

α) διαδικασία αποκλειστικής μετάδοσης περιεχομένου, το οποίο

β) πρέπει να φτάνει αναγκαστικά στο απευθυνόμενο πρόσωπο με επιτυχία.

Κατ' αυτό τον τρόπο η συνταγματική προστασία θα ετίθετο υπό την επιφύλαξη:

α) προληπτικού ελέγχου του περιεχομένου

β) σημασιολογικής και εν πολλοίς αυθαίρετης εκτίμησης σε σχέση με το τι συνιστά «περιεχόμενο» και

γ) της κατ' ανάγκη ολοκληρωμένης (σε τεχνικό επίπεδο) επικοινωνιακής διαδικασίας.

Η θέση αυτή δε μπορεί να γίνει αποδεκτή για λόγους εξόχως δικαιολογικής τάξης, ιδίως αν λάβει υπόψη κανείς και το γεγονός ότι τέτοιου είδους επικοινωνίες (αναπάντητες κλήσεις, κενές επιστολές) είναι δυνατό να έχουν μια προσυμφωνημένη σημασιολογική διάσταση για τους επικοινωνούντες¹⁶⁸. Περαιτέρω, μια τέτοια άποψη θα συνεπαγόταν ότι

μετά την ολοκλήρωση μιας επικοινωνίας, ο πάροχος των τηλεπικοινωνιακών υπηρεσιών θα μπορούσε να αναλύει τα μεταδεδομένα ελεύθερα καθώς και να παράσχει πρόσβαση ως προς αυτά σε τρίτους.

Είναι φανερό ότι ο αποκλεισμός της συνταγματικής προστασίας των μεταδεδομένων επικοινωνίας (είτε στο πλαίσιο μιας αμφίδρομης είτε στο πλαίσιο ακόμα και μιας κατ' αρχήν μονόδρομης επικοινωνίας), δε συνιστά προσέγγιση που μπορεί να επιδοκιμαστεί από τη συνταγματική τάξη.

Επιχείρημα μπορεί να αντληθεί επίσης από το γεγονός ότι κατά την εισαγωγή του σχετικού δικαιώματος στη συνταγματική έννομη τάξη έως και την τελευταία τροποποίησή του το 2001, ο συνταγματικός νομοθέτης ήταν γνώστης της τυπικής αυτής διάκρισης μεταξύ «εξωτερικών στοιχείων» και περιεχομένου. Εντούτοις, δεν προέβη στην αποτύπωσή της, στη σχετική συνταγματική διάταξη, αλλά αντιθέτως με ρητό τρόπο:

α) κατοχύρωσε την προστασία της επικοινωνίας με οποιοδήποτε τρόπο και αν αυτή γίνεται, και

β) διατήρησε το επίρρημα «απολύτως» αναφορικά με το απαραβίαστο του σχετικού δικαιώματος.

Παρά τα επιχειρήματα περί της ιστορικής χροιάς του σχετικού επιρρήματος¹⁶⁹, αυτό φαίνεται να συνιστά μια μάλλον επιτακτική υπενθύμιση προς τον εφαρμοστή του δικαίου, ότι κατά την εξέταση του δικαιώματος υφίσταται μαχητό τεκμήριο υπέρ του απόρρητου χαρακτήρα ενός επικοινωνιακού γεγονότος, όπως και αν αυτό εκδηλώνεται¹⁷⁰, ενώ οι περιπτώσεις άρσης αυτού, στο πλαίσιο του νόμου, θα πρέπει να συνοδεύονται από υψηλές εγγυήσεις. Στο συμπέρασμα αυτό είχε καταλήξει και μερίδα του νομικού κόσμου¹⁷¹ σε ανυποψίαστο χρόνο, ως προς τις ποικίλες δυνατότητες και συνέπειες της ανάλυσης των μεταδεδομένων.

Ο ν.2225/1994

Το απόρρητο των επικοινωνιών προστατεύεται από τον εκτελεστικό νόμο του αρ.19 Συντάγματος, ήτοι τον 2225/1994. Μέσω του ν.2225/1994 καθορίζονται οι περιπτώσεις αδικημάτων για τη διακρίβωση των οποίων είναι επιτρεπτό (αλλά όχι επιβαλλόμενο) να αρθεί το απόρρητο των επικοινωνιών καθώς και οι σχετικές διαδικαστικές εγγυήσεις.

Στο άρθρο 5 παρ.10 του ν.2225/1994 ορίζεται ότι:

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.

Παρά τη μη ρητή διατύπωση, είναι πρόδηλο¹⁷² ότι η διάταξη αυτή αναφέρεται στα μεταδεδομένα επικοινωνίας τα οποία γίνονται γνωστά (πέραν του περιεχομένου) λόγω της άρσης του απορρήτου. Κατά σαφή τρόπο¹⁷³, ο ν.2225/1994 ορίζει ότι η γνωστοποίηση (ενν. στις ανακριτικές αρχές) των μεταδεδομένων, διέρχεται αναγκαστικά μέσα από τη διαδικασία άρσης του απορρήτου, ενώ θέτει ταυτόχρονα και ποινή ακυρότητας σε περίπτωση που αυτά χρησιμοποιηθούν και ληφθούν υπόψη ως άμεση ή έμμεση απόδειξη σε άλλη δίκη¹⁷⁴.

Από τις διατυπώσεις του ν.2225/1994 συμπεραίνει κανείς ότι:

- α) εφόσον δε συντρέχει ανάγκη διακρίβωσης των απαριθμούμενων αδικημάτων ή
 - β) εφόσον η διακρίβωση των απαριθμούμενων αδικημάτων δεν απαιτεί την άρση του απορρήτου αλλά δύναται να επιτευχθεί με άλλα (κατά τεκμήριο ηπιότερα) μέσα
- ο κανόνας είναι η προστασία του επικοινωνιακού απορρήτου.

Η ερμηνεία αυτή είναι σύμφωνη με την αρχή της αναλογικότητας, η οποία επιτάσσει τη λήψη μόνο των εντελώς αναγκαίων μέτρων, που συνεπάγονται τη μικρότερη δυνατή προσβολή των απειλούμενων δικαιωμάτων.

Λαμβάνοντας υπόψη τις προαναφερθείσες εκτεταμένες δυνατότητες επέμβασης στην ιδιωτική ζωή ενός προσώπου και την αποκάλυψη πλήθους συμπερασμάτων σε σχέση με αυτό μέσα από την ανάλυση των μεταδεδομένων επικοινωνίας¹⁷⁵ και το γεγονός ότι τα μεταδεδομένα συνιστούν αναπόσπαστο στοιχείο του επικοινωνιακού απορρήτου, ο κανόνας (θα πρέπει να) είναι η προστασία του σε σχέση με αυτά και η κατά περίπτωση και μόνο άρση του όταν:

- α) συντρέχουν επαρκείς ενδείξεις τέλεσης ενός αδικήματος το οποίο περιλαμβάνεται στο αρ.4 του ν.2225/1994 και

β) η άρση σε σχέση με τα μεταδεδομένα επικοινωνίας είναι το μοναδικό μέσο σε σχέση με τη διακρίβωσή του, μη υπαρχόντων άλλων ηπιότερων

Ο ν.3783/2009

Ήδη από το άρθρο 1, στο οποίο αποτυπώνεται ο σκοπός του νόμου¹⁷⁶, διαφαίνεται η στενή σχέση του με το ζήτημα της αδιαμφισβήτητης ταυτοποίησης των χρηστών, οι οποίοι έκτοτε δεν είναι δυνατό να παραμένουν ανώνυμοι.

Στο αρ.2 παρ.7 ορίζονται τα στοιχεία ταυτοποίησης κινητού τερματικού στα περιλαμβάνονται αθροιστικά:

α) ο τηλεφωνικός αριθμός κλήσης του συνδρομητή,

β) η διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI),

γ) η διεθνής ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI),

δ) η ημερομηνία και ώρα της αρχικής ενεργοποίησης της υπηρεσίας,

ε) ο κωδικός θέσης (κωδικός ταυτότητας κυψέλης) από την οποία πραγματοποιήθηκε η ενεργοποίηση και

στ) η κάρτα ταυτότητας συνδρομητή (SIM, USIM ή άλλη αντίστοιχη) που περιέχει όλες τις πληροφορίες και τα δεδομένα που αφορούν τον συνδρομητή.

Τα «σκληρά» αυτά μεταδεδομένα επικοινωνίας (όσο και δεδομένα προσωπικού χαρακτήρα) είναι ικανά να ταυτοποιούν με μοναδικό τρόπο το συνδρομητή.

Το επιχείρημα υπέρ της συμπερίληψης των μεταδεδομένων στο προστατευτικό πλαίσιο του απορρήτου παρέχεται ευθέως από το αρ.3 παρ.2¹⁷⁷ όσο και από το αρ.5 παρ.2 ¹⁷⁸ του ν.3783/2009.

Με λίγα λόγια, ο νόμος όρισε ρητά ότι η πρόσβαση των δημοσίων αρχών σε στοιχεία που συνιστούν αναμφίβολα μεταδεδομένα επικοινωνίας, διέρχεται αναγκαστικά από τις διατάξεις του ν.2225/1994 και την τήρηση των προβλεπόμενων σε αυτόν διαδικασιών¹⁷⁹.

Το ΠΔ 47/2005

Η προστασία του απορρήτου των επικοινωνιών αποτυπώνεται και στο ΠΔ 47/2005 το οποίο καθορίζει τους όρους, τις διαδικασίες άρσης του απορρήτου και των οργανωτικών μεθόδων αυτής, έτσι ώστε να μη θίγεται η ιδιωτική ζωή και η προσωπικότητα του πολίτη, παρά μόνο στο μέτρο και για όσο χρονικό διάστημα είναι απολύτως αναγκαίο, χάριν της προστασίας της εθνικής ασφάλειας, της διακρίβωσης των εγκλημάτων που προβλέπονται στο άρθρο 4 του Ν. 2225/1994. Ήδη δηλαδή, από το σκοπό του νόμου γίνεται σαφές ότι ο κανόνας είναι η προστασία του απορρήτου, η οποία μάλιστα δεν εξαφανίζεται όταν συντρέχουν λόγοι άρσης του απορρήτου, αλλά υποχωρεί στο μέτρο και για όσο χρονικό διάστημα είναι απολύτως αναγκαίο. Η συνταγματική αρχή της αναλογικότητας τίθεται ήδη από την αρχή και κατά ρητό τρόπο από το νομοθέτη, καλώντας τον εφαρμοστή να ενεργήσει σταθμίσεις υψηλής ακρίβειας σε σχέση με την προστασία του απορρήτου και την επίτευξη των επιχειρησιακών στόχων μιας διαδικασίας άρσης απορρήτου.

Σε σχέση με το ζήτημα της προστασίας των μεταδεδομένων, το ΠΔ 47/2005 είναι σαφές: αφενός μεν περιγράφει αναλυτικά κατηγορίες μεταδεδομένων (όσο και προσωπικών δεδομένων) ανά μορφή επικοινωνίας, αφετέρου ορίζει ότι αυτά πρέπει να περιλαμβάνονται στην οικεία διάταξη που επιβάλλει την άρση του απορρήτου¹⁸⁰.

Παρουσιάζει ενδιαφέρον ότι το ΠΔ 47/2005 αποκαλύπτει κατ' ουσία αν όχι το σύνολο, τουλάχιστον τις περισσότερες κατηγορίες μεταδεδομένων επικοινωνίας τα οποία παράγονται ανά μορφή επικοινωνίας, υπολαμβάνοντας ότι αυτά συλλέγονται (ή είναι δυνατό να συλλέγονται) διαρκώς από τους παρόχους δικτύου επικοινωνιών και τους παρόχους υπηρεσιών επικοινωνιών.

Ο ν.3471/2006

Ο ν.3471/2006¹⁸¹ με τον οποίο ενσωματώθηκε η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου αποσκοπεί στην προστασία των θεμελιωδών δικαιωμάτων

των ατόμων, ιδίως της ιδιωτικής ζωής, τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

Στο νόμο αυτό τέμνεται η προστασία δεδομένων προσωπικού χαρακτήρα με τη διασφάλιση του απορρήτου των επικοινωνιών, ορίζοντας ότι η οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών καθώς και τα συναφή δεδομένων κίνησης και θέσης, προστατεύονται από το Απόρρητο των επικοινωνιών, του οποίου η άρση είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος, δηλαδή του ν.2225/1994. Η θέση αυτή άλλωστε επικυρώνεται και από την Αιτιολογική Έκθεση του νόμου¹⁸².

Ο νόμος προβαίνει σε ενδεικτικό και όχι περιοριστικό καθορισμό των δεδομένων κίνησης¹⁸³ ¹⁸⁴όσο και των δεδομένων θέσης¹⁸⁵. Η επιλογή αυτή, ακολουθεί μεν το λεκτικό της Οδηγίας 2002/58/EK, ωστόσο δεν κρίνεται επιτυχημένη, διότι ο καταρχήν σκοπός επεξεργασίας αυτών είναι η διαβίβαση των επικοινωνιών και η χρέωση των ζητούμενων υπηρεσιών. Με άλλα λόγια, τόσο η Οδηγία όσο και ο ν.3471/2006, δεν εξεδίκευσαν ποιες ακριβώς είναι οι α ν α γ κ α ί ε ς κατηγορίες μεταδεδομένων σε σχέση με τους δηλωθέντες σκοπούς, παρότι στο άρθρο 5 παρ.1,2 και στο αρ.6 παρ.2 του νόμου, μάλλον επιχειρήθηκε διαφυγή μέσω της αρχής της αναλογικότητας, μεταθέτοντας ωστόσο την ευθύνη στους παρόχους. Η επιλογή αυτή, θυμίζει τη λογική της αρχής της λογοδοσίας του μετέπειτα τεθέντος σε ισχύ ΓΚΠΔ 679/2016/EE. Ωστόσο κατά το χρόνο που τέθηκε σε ισχύ ο ν.3471/2006, η λογική της προστασίας δεδομένων προσωπικού χαρακτήρα ακολουθούσε μια πιο γραφειοκρατική λογική, την οποία κατά αξιοπερίεργο τρόπο δεν ακολούθησε ο νομοθέτης.

Αξίζει μνείας ότι πέραν των «κλασικών» περιπτώσεων προσβολής του επικοινωνιακού απορρήτου (ακρόαση, υποκλοπή), ο νόμος ρητά απαγορεύει και την επιτήρηση των συναφών δεδομένων κίνησης και θέσης. Παρότι δεν διευκρινίζεται ο όρος «επιτήρηση», η πυκνότητα του όρου διασφαλίζει ότι αυτός αφορά κάθε περίπτωση αθέμιτης παρακολούθησης, πρόσβασης (όσο και κατά λογική συνέπεια) και ανάλυσης αυτών.

Ο ν.3917/2011

Με το ν.3917/2011 μεταφέρθηκε στην εθνική έννομη τάξη η Οδηγία 2006/24/EK. Ωστόσο, όπως αναφέρθηκε η Οδηγία 2006/24/EK ακυρώθηκε με την απόφαση Digital Rights Ireland το 2014 όπως είδαμε ανωτέρω. Παρότι ο νόμος αυτός τυπικά ισχύει καθότι δεν έχει καταργηθεί ή αντικατασταθεί με νεότερο, βρίσκεται σε μια μετέωρη θέση. Από το 2014 συστήθηκε με απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, Ειδική Νομοπαρασκευαστική Επιτροπή με αντικείμενο την κατάργηση/τροποποίηση της εν λόγω νομοθεσίας. Η επιτροπή αυτή δεν ολοκλήρωσε ποτέ το έργο της. Συνεπώς, η πλέον ορθή νομική αντιμετώπιση του ζητήματος γίνεται με την εφαρμογή των ρυθμίσεων της Οδηγίας 2002/58/EK, όπως μάλιστα αυτή ερμηνεύεται από τα ευρωπαϊκά δικαστήρια.

Τέλος, θεμελίωση αναφορικά με την προστασία των «εξωτερικών» στοιχείων της επικοινωνίας μπορεί να αντληθεί επίσης και από το 370Α ΠΚ το οποίο ορίζει στην παρ.1 εδ. ά ότι:

Οποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλο τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών σταθερής ή κινητής τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή στοιχεία της θέσης και κίνησης της εν λόγω επικοινωνίας, τιμωρείται με φυλάκιση.

Δηλαδή, η καθ' οιονδήποτε τρόπο αθέμιτη παγίδευση ή παρέμβαση σε οποιοδήποτε τμήμα μιας τεχνολογικής υποδομής (τερματικό, σύνδεση, δίκτυο, λογισμικό, υλισμικό (hardware) με σκοπό ακόμα και την αποτύπωση στοιχείων θέσης ή κίνησης (πέραν δηλαδή της πληροφόρησης) συνιστά ποινικό αδίκημα. Η ποινική διάταξη είναι σημαντική διότι αφενός μεν αποτύπωσε με μεγάλη ακρίβεια το σύνολο των τεχνικών κατηγοριών που απαιτούνται στο πλαίσιο της επικοινωνίας, αφετέρου περιέλαβε ρητά στο προστατευτικό του περιεχόμενο και τα δεδομένα κίνησης και θέσης.

ΤΜΗΜΑ ΕΝΤΕΚΑΤΟ

Κριτική επισκόπηση της εθνικής νομοθεσίας σε σχέση με την προστασία των μεταδεδομένων επικοινωνίας

*καλό μου θήραμα
πες μου, σε παρακαλώ
τι 'ναι προτιμότερο από τα δυο;
να σε κυνηγάνε
ενώ έχει απαγορευτεί το κυνήγι;
ή να σε κυνηγάνε
ενώ επιτρέπεται;³*

Η εθνική νομοθεσία η οποία περιέχει διατάξεις που προστατεύουν τα μεταδεδομένα επικοινωνίας ως επικοινωνιακό απόρρητο, παρουσιάζει σημεία που προκαλούν προβληματισμό σε σχέση με επιμέρους διαστάσεις του ζητήματος.

1. Οι συλλεγόμενες κατηγορίες μεταδεδομένων επικοινωνίας (ιδίως δυνάμει του Π.Δ. 47/2005) ανά μέσο επικοινωνίας είναι ιδιαίτερα εκτεταμένες και σε κάθε περίπτωση φαίνεται να είναι το σύνολο των μεταδεδομένων που παράγονται ανά μέσο επικοινωνίας.

Προς τούτο συνηγορεί η διάταξη του αρ.4 παρ.3 του Π.Δ. 47/2005 η οποία ορίζει ότι:

Η παράθεση των στοιχείων επικοινωνίας της παραγράφου 1 είναι ενδεικτική. Η διάταξη άρσης απορρήτου δεν αποκλείεται να αναφέρεται και σε άλλα στοιχεία κατά είδος επικοινωνίας, κάθε φορά που η εξέλιξη της επιστήμης και της τεχνολογίας επιφέρει διεύρυνση του καταλόγου των στοιχείων αυτών.

Σε περίπτωση δηλαδή της εν γένει διαδικασίας άρσης απορρήτου, φαίνεται ότι η διάταξη δύναται να αναφερθεί και σε κατηγορίες στοιχείων επικοινωνίας (δηλαδή και μεταδεδομένων), οι οποίες δεν τίθενται ρητά στο Π.Δ. 47/2005.

³ Πρεβεδουράκης Γιώργος (2013), *Κλέφτικο*, Θεσσαλονίκη, Πανοπτικόν, σελ.25

Ωστόσο, ως έχει διαφανεί μέχρι τώρα, από την παράθεση των δυνατοτήτων των μεταδεδομένων επικοινωνίας, αρκεί η εξέταση μόνο ελάχιστων κατηγοριών από αυτά¹⁸⁶ προκειμένου να σχηματισθεί ένα πλήρες προφίλ ενεργειών, δηλώσεων, προθέσεων, συνηθειών και σχέσεων ενός ερευνώμενου προσώπου. Η επέκταση των κατηγοριών των υπό άρση μεταδεδομένων σε κάθε κατηγορία η οποία δύναται να προκύψει από την τεχνολογική πρόοδο, εγείρει ερωτήματα σχετικά με την αναλογικότητα της σχετικής ρύθμισης.

2. Ο νόμος 3471/2006 προβαίνει σε ενδεικτικό και όχι περιοριστικό καθορισμό των δεδομένων κίνησης^{187 188} όσο και των δεδομένων θέσης¹⁸⁹. Η επιλογή αυτή, ακολουθεί μεν το λεκτικό της Οδηγίας 2002/58/EK, ωστόσο δεν κρίνεται επιτυχημένη, διότι ο κατ' αρχήν σκοπός επεξεργασίας αυτών είναι η διαβίβαση των επικοινωνιών και η χρέωση των ζητούμενων υπηρεσιών. Με άλλα λόγια τόσο η Οδηγία όσο και ο ν.3471/2006 δεν εξειδίκευσαν ποιες ακριβώς είναι οι *α ν α γ κ α ί ε ς* κατηγορίες μεταδεδομένων σε σχέση με τους δηλωθέντες σκοπούς, παρότι στο άρθρο 5 παρ.1,2 και στο αρ.6 παρ.2 του νόμου, μάλλον επιχειρήθηκε διαφυγή μέσω της αρχής της αναλογικότητας, μεταθέτοντας έτσι την ευθύνη στους παρόχους. Η επιλογή αυτή, θυμίζει τη λογική της αρχής της λογοδοσίας του μετέπειτα τεθέντος σε ισχύ ΓΚΠΔ 679/2016/ΕΕ. Κατά το χρόνο που τέθηκε σε ισχύ ο ν.3471/2006, η λογική της προστασίας δεδομένων προσωπικού χαρακτήρα ακολουθούσε μια πιο γραφειοκρατική λογική, την οποία κατά αξιοπερίεργο τρόπο δεν ακολούθησε ο νομοθέτης.

3. Προβληματισμό επίσης δημιουργούν οι διατάξεις του ν.3471/2006 που αναφέρονται στην ανωνυμοποίηση δεδομένων κίνησης και θέσης.

Στο αρ.6 παρ.1 ορίζεται ότι:

Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον φορέα παροχής δημοσίου δικτύου ή και διαθέσιμες στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, με τη λήξη της επικοινωνίας καταστρέφονται ή καθίστανται ανώνυμα, με την επιφύλαξη του ν. 3917/2011 (Α`22)¹⁹⁰, καθώς και των παραγράφων 2 έως 6 του παρόντος άρθρου (ήτοι για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων, για την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας

Στο αρ.6 παρ.4 ορίζεται ότι:

*Επιτρέπεται η επεξεργασία δεδομένων που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του συνδρομητή ή χρήστη δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών για την παροχή υπηρεσίας προστιθέμενης αξίας, **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.*

Με τις διατάξεις αυτές τίθενται σημαντικά ζητήματα προστασίας του επικοινωνιακού απορρήτου.

Πέραν των περιπτώσεων επεξεργασίας των δεδομένων κίνησης (traffic data) για νόμιμους σκοπούς (χρέωσης, πληρωμής, εμπορικής προώθησης, υπηρεσιών προστιθέμενης αξίας), μετά την ολοκλήρωση της επικοινωνίας, καταλείπεται ευχέρεια στους παρόχους είτε να τα καταστρέψουν είτε να τα ανωνυμοποιήσουν. Ωστόσο, τα αποτελέσματα κάθε μιας εκ των επιλογών σε σχέση με την προστασία του επικοινωνιακού απορρήτου¹⁹¹ είναι εντελώς διαφορετικά: στην περίπτωση της καταστροφής, διασφαλίζεται πλήρως η προστασία του απορρήτου¹⁹², ενώ στην περίπτωση της ανωνυμοποίησης αυτών, αυτό δεν καθίσταται πάντα εφικτό.

Οι κίνδυνοι που προκαλούνται λόγω της φύσης, της ιεραρχίας, της σχέσης και της σημασιολογικής διάστασης των δεδομένων κίνησης είναι υψηλοί, διότι είναι δύσκολος έως απίθανος ο αποκλεισμός της πιθανότητας να αναγνωριστεί εκ νέου η ταυτότητα του συνδρομητή¹⁹³ ¹⁹⁴ ¹⁹⁵ και συνεπώς η δραστηριότητά του και εν γένει το προστατευτέο περιεχόμενο των ηλεκτρονικών επικοινωνιών του. Συμπληρωματικά πρέπει να ληφθεί υπόψη και η περίπτωση ανεπιτυχούς ανωνυμοποίησης. Δηλαδή, η επιλογή των παρόχων να ανωνυμοποιήσουν τα δεδομένα κίνησης, ενέχει σημαντικούς (και μάλλον μη αποδεκτούς) κινδύνους αναφορικά με την προστασία του επικοινωνιακού απορρήτου.

4. Ενδιαφέρον παρουσιάζει το γεγονός ότι η πρόσβαση στα ανωνυμοποιημένα δεδομένα κίνησης ή θέσης καθώς και η επιτήρηση αυτών, δεν προϋποθέτει την ενεργοποίηση των διατάξεων του ν.2225/1994. Γενικότερα, τα ανωνυμοποιημένα δεδομένα κίνησης ή θέσης κατ' αρχήν φαίνεται να μην τυγχάνουν προστασίας.

Ακολουθώντας το γράμμα του αρ.2 του ν.3471/2006 ο κύκλος ζωής (όσο και προστασίας) των δεδομένων κίνησης εξαντλείται μετά τη διαβίβαση μιας επικοινωνίας όσο και στο χρονικό διάστημα που απαιτείται για τη χρέωσή της¹⁹⁶. Με άλλα λόγια, ο προσδιορισμός των δεδομένων κίνησης βάσει των δηλωμένων σκοπών επεξεργασίας τους και όχι των πραγματικών σημασιολογικών περιεχομένων, δυνατοτήτων και διαστάσεών τους¹⁹⁷, καταλείπει ένα σημαντικό έλλειμμα προστασίας.

Ο νόμος 3471/2006 ορίζει διαφορετικά σε σχέση με τα δεδομένα θέσης. Και τούτο διότι ο ορισμός τους συνδέεται (επιτυχώς) με το αποτέλεσμα που προκύπτει από την επεξεργασία τους και είναι η υπόδειξη της γεωγραφικής θέσης του τερματικού εξοπλισμού του χρήστη μια διαθέσιμη στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. (Το αποτέλεσμα αυτό, όπως είδαμε ανωτέρω, είναι εφικτό ακόμα και στην περίπτωση της ανωνυμοποίησης των δεδομένων θέσης.)

Εν τούτοις, ο περιορισμός της προστασίας μόνο στα ανωνυμοποιημένα δεδομένα θέσης και όχι και στα ανωνυμοποιημένα δεδομένα κίνησης, δε μπορεί να γίνει αποδεκτός. Και οι δυο αυτές κατηγορίες δεδομένων, λόγω της ιδιάζουσας φύσης τους, του πληροφοριακού πλούτου τους και των διαθέσιμων μέσων ανάλυσής τους, είναι αναμφισβήτητα τμήμα του επικοινωνιακού απορρήτου. Ως εκ τούτου απαιτείται είτε μια νομοθετική μεταβολή, έτσι ώστε (και) τα ανωνυμοποιημένα δεδομένα κίνησης και θέσης να τυγχάνουν της ρητής προστασίας του απορρήτου, είτε μια υπερβολικά ευρεία ερμηνευτική προσέγγιση, στη βάση του τεκμηρίου υπέρ του απορρήτου και του *in dubio pro libertate*. Λαμβάνοντας υπόψη τις ισχυρές διαφωνίες ακόμα και σε σχέση με την προστασία των εν γένει (μη ανωνυμοποιημένων) μεταδεδομένων επικοινωνίας, σκόπιμη κρίνεται η υιοθέτηση της πρώτης εκδοχής.

Η ανησυχία πίσω από το ζήτημα της προστασίας των ανωνυμοποιημένων μεταδεδομένων είναι ότι εφόσον δεν καλύπτονται από την προστασία του επικοινωνιακού απορρήτου, δύνανται να παραχωρούνται από τους παρόχους σε άλλους ιδιωτικούς όσο και κρατικούς φορείς και υπηρεσίες, για σκοπούς επεξεργασίας οι οποίοι δεν τυγχάνουν δημοσιότητας και ελέγχου και μάλιστα για άγνωστο χρονικό διάστημα. Κατά τον τρόπο αυτό, είναι εφικτή η δημιουργία μιας γκριζας ζώνης σε σχέση με τα αποθηκευμένα ανωνυμοποιημένα δεδομένα κίνησης και θέσης, η οποία θα επιτρέπει την εξαγωγή πλήθους πληροφοριών και συμπερασμάτων για οποιοδήποτε χρήστη ή ομάδα χρηστών ηλεκτρονικών επικοινωνιών,

υπονομεύοντας ευθέως το απόρρητο των ηλεκτρονικών επικοινωνιών. Λαμβάνοντας υπόψη ότι ο εντοπισμός μιας τέτοιας διαδικασίας προϋποθέτει την πραγματοποίηση ελέγχων εκ μέρους της ΑΔΑΕ και της ΑΠΔΠΧ και την ύπαρξη σημαντικών πόρων σε αυτές¹⁹⁸, γίνεται αντιληπτό ότι οι κίνδυνοι προσβολής του επικοινωνιακού απορρήτου κατ' αυτό τον έμμεσο τρόπο είναι υψηλοί.

Σχετικά με την ανωτέρω διατυπωθείσα υπόθεση, αξίζει μνείας η υπ' αριθμ 4/2022 απόφαση της ΑΠΔΠΧ. Με την απόφαση αυτή η Αρχή επέβαλλε ίσως το υψηλότερο μέχρι σήμερα πρόστιμο σε πάροχο τηλεπικοινωνιακών υπηρεσιών για παραβίαση δεδομένων (μεγάλης κλίμακας) λόγω ελλιπών μέτρων ασφαλείας.

Το ενδιαφέρον ωστόσο στοιχείο που σχετίζεται με τα προαναφερθέντα, ανάγεται στον τρόπο με τον οποίο ο πάροχος αυτός τηρούσε τα δεδομένα κίνησης και θέσης. Παρά τους ισχυρισμούς περί ανωνυμοποίησης, ο πάροχος κατ' ουσία προέβαινε σε διατήρηση των δεδομένων αυτών υπό καθεστώς ψευδωνυμοποίησης¹⁹⁹ για την εξαγωγή στατιστικών συμπερασμάτων αξιοποιούμενα (κατά δήλωσή του) για το βέλτιστο σχεδιασμό του δικτύου κινητής τηλεφωνίας. Η Αρχή εκτίμησε ότι ακόμα και να είχε ληφθεί μέριμνα για την εφαρμογή της ορθής διαδικασίας ανωνυμοποίησης, θα έπρεπε να είχε εκτιμηθεί ταυτόχρονα και ο κίνδυνος επαναταυτοποίησης των χρηστών, λαμβάνοντας υπόψη όλα τα εύλογα μέσα που μπορεί να διαθέσει κάποιος ο οποίος θα έχει πρόσβαση στο εν λόγω αρχείο δεδομένων κίνησης και θέσης²⁰⁰. Δηλαδή, η Αρχή υπενθύμισε ότι τα ανωνυμοποιημένα δεδομένα κίνησης και θέσης, δε διασφαλίζουν ολοκληρωτικά την ανωνυμία, αλλά δύνανται να άγουν στην ταυτοποίηση ενός χρήστη.

Η αναφορά αυτή τίθεται σε σχέση με την ανωτέρω διατυπωθείσα υπόθεση και την τύχη των δεδομένων κίνησης και θέσης μετά την πάροδο του χρόνου διατήρησής τους. Επιβεβαιώνεται εμπράκτως²⁰¹ ότι τουλάχιστον ένας πάροχος τηλεφωνικών υπηρεσιών στη χώρα μας²⁰² ακολουθούσε προβληματικές πρακτικές σε σχέση με την προστασία των δεδομένων αυτών, οι οποίες φαίνεται να οδήγησαν στην προσβολή του επικοινωνιακού απορρήτου όσο και την προστασία δεδομένων προσωπικού χαρακτήρα, με συνέπειες άγνωστης ακόμα έκτασης.

5. Από τον σχεδιασμό της εθνικής νομοθεσίας που παρατέθηκε (συμπεριλαμβανομένης της νομοθεσίας που αφορά τη λειτουργία της ΑΔΑΕ), παρατηρείται η έντονη εμπλοκή των

τηλεπικοινωνιακών παρόχων όσον αφορά τους πραγματικούς όρους διασφάλισης αυτού, στο μέτρο που είναι υπεύθυνοι για τη συλλογή και διατήρηση αυτών.

Η ΑΔΑΕ ασκεί μεν τυπικώς τον έλεγχο των όρων της διαδικασίας άρσης του απορρήτου, χωρίς όμως να μπορεί να εξετάζει την κρίση των αρμόδιων δικαστικών αρχών²⁰³. Τούτο παρίσταται από συνταγματική άποψη λογικό²⁰⁴, ωστόσο καταλείπει ένα σημαντικό θεσμικό έλλειμμα ελέγχου. Δηλαδή, απουσιάζουν αποτελεσματικά θεσμικά αντίβαρα στην περίπτωση που η κρίση των αρμοδίων δικαστικών αρχών (Εισαγγελέα Εφετών, Δικαστικού Συμβουλίου) εμπεριέχει αποκλίσεις ή ακόμα και παραβιάσεις της νομοθεσίας περί άρσης του απορρήτου.

Οι πάροχοι είναι υπεύθυνοι για την υλοποίηση μιας διαδικασίας άρσης απορρήτου που αφορά μεταδεδομένα επικοινωνίας, καθώς αποφασίζουν αν θα τα χορηγήσουν ή όχι, έχοντας την υποχρέωση να εξετάζουν κατά πόσο (κατά το τυπικό σκέλος) πληρούνται οι απαιτήσεις του ν.2225/1994 σε σχέση με το περιεχόμενο των διατάξεων (ή των βουλευμάτων). Δηλαδή, αν και συνιστούν νομικά πρόσωπα ιδιωτικού δικαίου καταλήγουν να επιτελούν ένα εγγυητικό ρόλο²⁰⁵ σε σχέση με την προστασία του επικοινωνιακού απορρήτου, έχοντας άλλωστε προς τούτο ρητές εκ του νόμου υποχρεώσεις.

ΤΜΗΜΑ ΔΩΔΕΚΑΤΟ

Τα προβλήματα της διαδικασίας άρσης απορρήτου για λόγους εθνικής ασφάλειας αναφορικά με τα μεταδεδομένα επικοινωνίας

Λαμβανομένων υπόψη των δυνατοτήτων εξαγωγής πλήθους συμπερασμάτων για πρόσωπα και ομάδες προσώπων από την ανάλυση μεταδεδομένων επικοινωνίας, η υφιστάμενη διαδικασία άρσης απορρήτου, ιδίως δε υπό τον τρόπο που φαίνεται ότι εφαρμόζεται, προκαλεί σημαντικές ανησυχίες αναφορικά με την προστασία του απορρήτου και της ιδιωτικότητας, τόσο για το παρόν όσο και για το μέλλον. Αρχικά, είναι απαραίτητη η διατύπωση κάποιων διαπιστώσεων σε σχέση με τις αποφάσεις άρσης απορρήτου, των συνεπειών αυτών καθώς και πραγματολογικών δεδομένων.

Γενική αξιολόγηση των ρυθμίσεων

Η διάταξη (που επιβάλλει την άρση του απορρήτου για λόγους εθνικής ασφάλειας), παρουσιάζει τις εξής σημαντικές διαφορές από το βούλευμα (του δικαστικού συμβουλίου που επιβάλλει την άρση του απορρήτου για διακρίβωση εγκλημάτων): η ισχύς της διάταξης φαίνεται να μην έχει ανώτατο χρονικό όριο, επιπλέον δεν απαιτεί την παράθεση του ονόματος του προσώπου ή των προσώπων κατά των οποίων λαμβάνεται το μέτρο της άρσης και τέλος δεν απαιτείται η ύπαρξη αιτιολογίας σε αυτή.

Οι συνέπειες των συγκεκριμένων νομοθετικών επιλογών αναφορικά με τις διατάξεις άρσης απορρήτου για λόγους εθνικής ασφάλειας, είναι σημαντικές και παρατίθενται συνοπτικά ως εξής:

1. Καθίστανται αποδεκτές οι μαζικές παρακολουθήσεις, ενώ μια διάταξη μπορεί να αναφέρεται σε περισσότερους του ενός αριθμού συνδέσεων ή ατόμων για τα οποία διατάσσεται άρση του απορρήτου²⁰⁶.
2. Το χρονικό διάστημα της άρσης του απορρήτου δεν περιορίζεται.
3. Καταργείται έμπρακτα η δυνατότητα ελέγχου της ουσιαστικής νομιμότητας της άρσης απορρήτου και εν γένει η τήρηση της γενικής αρχής της λογοδοσίας, ιδίως σε περιπτώσεις προσχηματικών διώξεων.

4. Η λήψη απόφασης για την άρση του απορρήτου γίνεται άνευ αιτιολογίας και μάλιστα από μονοπρόσωπο όργανο.

Παρότι οι διαφορές των αποφάσεων για κάθε περίπτωση άρσης συμπληρώνονται από διαφορές και αναφορικά με την ακολουθούμενη διαδικασία²⁰⁷ και τα δικαιώματα των παρακολουθούμενων²⁰⁸, εκφεύγει της παρούσας εργασίας η ειδικότερη ανάλυσή τους.

Όσον αφορά δε τα πραγματικά στοιχεία σε σχέση με τις ακολουθούμενες διαδικασίες, υπενθυμίζουμε ότι από το 2004 έως 31/12/2020, η συντριπτική πλειονότητα περιπτώσεων άρσης απορρήτου αφορά τις περιπτώσεις που εμπίπτουν στην κατηγορία της εθνικής ασφάλειας. Μάλιστα, από το 2017 έως το τέλος του 2020 η αναλογία υπέρ των διατάξεων άρσης για λόγους εθνικής ασφάλειας κυμαίνεται από 70% έως 80% σε σχέση με τα βουλεύματα τα οποία κυμαίνονται από 30% έως 20% στο σύνολο των περιπτώσεων άρσης απορρήτου.

Αξιολόγηση σε σχέση με τους κινδύνους που απορρέουν από την ανάλυση των μεταδεδομένων

Ποια είναι η σημασία των ανωτέρω διαπιστώσεων σε σχέση με το ζήτημα της προστασίας των μεταδεδομένων επικοινωνίας;

Δεδομένης της ανυπαρξίας διαθέσιμων συγκεντρωτικών στοιχείων²⁰⁹ για τις λεπτομέρειες των αποφάσεων άρσης απορρήτου εν γένει, δυνατή είναι προς το παρόν μόνο η διατύπωση ενδεχομενικών παρατηρήσεων και η διαπίστωση πιθανολογούμενων κινδύνων.

1. Μια διάταξη άρσης απορρήτου για λόγους εθνικής ασφάλειας, αναφερόμενη σε μεταδεδομένα επικοινωνίας ενός προσώπου ή ομάδας προσώπων (γεγονός που όπως προαναφέραμε δεν αποκλείεται) και αναγόμενο στο παρελθόν (κατ' απώτατο όριο 12 μηνών²¹⁰) όσο και στο μέλλον (άνευ περιορισμού²¹¹), λόγω ακριβώς του μεγάλου (έως απροσδιόριστου) χρονικού εύρους, συνιστά ένα ιδιαίτερα επεμβατικό μέσο τόσο σε σχέση με το απόρρητο των επικοινωνιών όσο και σε σχέση με την ιδιωτικότητα του ερευνώμενου προσώπου ή ομάδας προσώπων²¹².

Όμως, η διενέργεια μιας έρευνας για τη διαπίστωση ύπαρξης παραγόντων που απειλούν την εθνική ασφάλεια, οφείλει να έχει συγκεκριμένο αντικείμενο (πρόσωπα, πράξεις). Εφόσον αυτά τα στοιχεία δεν εντοπίζονται εντός ενός δεδομένου και προκαθορισθέντος χρόνου²¹³, η άρση του απορρήτου θα έπρεπε είτε να παύει αυτοδικαίως είτε να παρατείνεται με ειδική αιτιολογία αναφορικά με το γιατί δεν ήταν εφικτή ή αποτελεσματική η ολοκλήρωση των ερευνών (ή σε ποιο βαθμό), ποιοι λόγοι καθιστούν αναγκαία τη συνέχισή της και για ποιο κατ' εκτίμηση χρονικό διάστημα.

Η επ' αόριστο συλλογή μεταδεδομένων επικοινωνίας για λόγους εθνικής ασφάλειας, μας οδηγεί στη διατύπωση τριών υποθέσεων:

α) οι αιτούντες όσο και αποφασίζοντες την άρση του απορρήτου, παρατείνουν την ύπαρξη (ή επιτρέπουν την επίταση) ενός ή περισσότερων κινδύνων για την εθνική ασφάλεια, επιτρέποντας στα ερευνώμενα πρόσωπα να συνεχίζουν τις εγκληματικές δραστηριότητές τους

β) η άρση του απορρήτου δεν έχει ως μοναδικό στόχο την αντιμετώπιση των απειλών της εθνικής ασφάλειας

γ) δεν υφίστανται λόγοι εθνικής ασφάλειας οι οποίοι οδήγησαν στην άρση του απορρήτου, αλλά άλλοι μη διακηρυγμένοι σκοποί, οι οποίοι υλοποιούνται παράνομα, καταχρηστικά και κυρίως ανέλεγκτα μέσα από την προβλεπόμενη διαδικασία

δ) η συλλογή μεταδεδομένων επικοινωνίας δε συνιστά ιδιαίτερα αποτελεσματικό μέσο για την αντιμετώπιση κινδύνων που άπτονται της εθνικής ασφάλειας και το επικοινωνικό απόρρητο αίρεται χωρίς ουσιαστικό λόγο.

Λαμβάνοντας υπόψη τα αρχικώς παρατεθέντα για τις ενέργειες και τα προγράμματα παρακολούθησης της NSA²¹⁴ όσο και τα ερευνητικά πορίσματα, η τέταρτη εκδοχή δε φαίνεται να έχει ισχυρή βάση.

Εάν, όμως, ισχύει οποιαδήποτε εκ των τριών άλλων υποθέσεων, τότε υφίσταται μείζον πολιτειακό ζήτημα, με ευρείες πολιτικές όσο και νομικές προεκτάσεις. Προς το παρόν, η αξιοπερίεργη διαδικαστική συσκότιση που αφορά τις διατάξεις άρσης απορρήτου για λόγους εθνικής ασφάλειας, δεν επιτρέπει την εξαγωγή βέβαιων συμπερασμάτων, πέραν του ότι οι διατάξεις της εθνικής νομοθεσίας προκαλούν σημαντική και υπέρμετρη παρέμβαση στο

απόρρητο της επικοινωνίας και την ιδιωτικότητα, ερχόμενες σε αντίθεση με τη νομολογία του ΔΕΕ και του ΕΔΔΑ.

2. Μια διάταξη άρσης απορρήτου που περιλαμβάνει κάθε κατηγορία μεταδεδομένων επικοινωνίας και δε συγκεκριμενοποιείται σε πρόσωπα αλλά αφορά μια γεωγραφική περιοχή, συνιστά μείζονα απειλή για το απόρρητο της επικοινωνίας όσο και την ιδιωτικότητα.

Εάν, δηλαδή, στα παραπάνω ανησυχητικά δεδομένα όσο και ερωτήματα, προσθέσει κανείς και την περίπτωση η άρση του απορρήτου με αντικείμενο τη συλλογή και ανάλυση μεταδεδομένων, να έχει ένα οριζόντιο χαρακτήρα με κριτήριο τη γεωγραφική θέση μιας τερματικής συσκευής, ο βαθμός επέμβασης στο δικαίωμα της απόρρητης επικοινωνίας είναι μη αποδεκτός.

Αναμφισβήτητα, η ανάλυση μεταδεδομένων επικοινωνίας σε μια συγκεκριμένη περιοχή, θα μπορούσε κατά περίπτωση να εισφέρει στον εντοπισμό στοιχείων για την τέλεση αδικημάτων που σχετίζονται με την εθνική ασφάλεια. Ωστόσο, το τίμημα μιας τέτοιας πρακτικής είναι ιδιαίτερα υψηλό, καθώς αυτομάτως προσδίδει το χαρακτηρισμό του de facto «υπόπτου» σε όσα πρόσωπα τυχαίνει να βρίσκονται στη συγκεκριμένη περιοχή κατά τη διάρκεια του διαστήματος της έρευνας.

Περαιτέρω, οι κίνδυνοι αξιοποίησης και ανάλυσης του ιδιαίτερος πλούσιου συλλεχθέντος υλικού για σκοπούς που δε σχετίζονται με το ερευνώμενο αντικείμενο είναι υψηλοί, ιδίως αν λάβει υπόψη κανείς τη μη ύπαρξη επιβεβαιωμένων εγγυήσεων περί του αντιθέτου. Το γεγονός ότι βρισκόμαστε στο πεδίο ανακριτικών ερευνών, αυτό δε σημαίνει ότι απεμπολείται κάθε σχετικό δικαίωμα των ερευνώμενων (ή παρεμπιπτόντως ερευνώμενων) προσώπων. Η εγχώρια συνταγματική όσο και η διεθνής έννομη τάξη, θέτει ως κανόνα το απόρρητο των επικοινωνιών, του οποίου η προστασία πρέπει να αίρεται στον απολύτως αναγκαίο βαθμό προκειμένου να εξυπηρετηθούν συγκεκριμένες ανάγκες διερεύνησης αδικημάτων ή προστασίας της εθνικής ασφάλειας. Η ανάλυση μεταδεδομένων επικοινωνίας μαζικής κλίμακας, από τη «φύση» της έχει απεριόριστες δυνατότητες και είναι εύκολο να διολισθήσει στην εξυπηρέτηση σκοπών που βρίσκονται εκτός των επιδιώξεων μιας δημοκρατικής έννομης τάξης. Προς τούτο, η χρήση τέτοιων πρακτικών θα πρέπει να συνιστά

την εξαίρεση και σε καμία περίπτωση τον κανόνα κατά την επιλογή των κατάλληλων ανακριτικών εργαλείων.

Συμπληρωματικές παρατηρήσεις

Τα παραπάνω ανησυχητικά ερωτήματα για την πραγματική προστασία των μεταδεδομένων επικοινωνίας και του απορρήτου στο πλαίσιο της εθνικής έννομης τάξης, δεν είναι τα μοναδικά. Η ίδια η έννοια και χρήση της εθνικής ασφάλειας, ο ρόλος του αρμοδίου εισαγγελικού λειτουργού και η έλλειψη διαδικαστικής συνοχής, συντείνουν στην επίταση των σχετικών κινδύνων.

1. Υποστηρίζεται ότι η έννοια της εθνικής ασφάλειας²¹⁵ παρουσιάζει δυσκολίες κατά τη συγκεκριμενοποίησή της, άποψη που κατ' αρχήν φαίνεται να έχει μια βάση. Οφείλουμε όμως να υπενθυμίσουμε ότι η άρση απορρήτου για λόγους εθνικής ασφάλειας δε γίνεται εν κενώ, αλλά συνιστά ειδική ανακριτική πράξη²¹⁶ έχουσα ως σκοπό τη συλλογή και τη διατήρηση των αποδείξεων για τη διερεύνηση της τέλεσης (ή απόπειρας τέλεσης) συγκεκριμένων ποινικών (ή στρατιωτικών ποινικών) αδικημάτων τα οποία δύναται να θέσουν σε διακινδύνευση το αγαθό αυτό²¹⁷.

Το παράδοξο όμως είναι η πλειονότητα των εγκλημάτων που σχετίζονται με την διακινδύνευση ή προσβολή της εθνικής ασφάλειας, περιγράφονται ήδη (!) στο αρ.4 παρ.1 του ν.2225/1994. Δηλαδή, η προστασία της εθνικής ασφάλειας δύναται να εξυπηρετηθεί από τη διαδικασία που ορίζεται για τη διακρίβωση αδικημάτων και η οποία κατά τεκμήριο παρέχει περισσότερα εχέγγυα δημοσίου ελέγχου όσο και τήρησης της αρχής της αναλογικότητας²¹⁸.

Προκύπτουν λοιπόν δύο εύλογα όσο και εξίσου ανησυχητικά ερωτήματα:

A. Για την έρευνα ποιων ακριβώς εγκλημάτων τα οποία σχετίζονται με τη διακινδύνευση ή προσβολή της εθνικής ασφάλειας (και τα οποία δεν περιλαμβάνονται στον κλειστό κατάλογο του αρ.4 παρ.1 του ν.2225/1994), εκδίδονται οι σχετικές διατάξεις ;

B. Αν όντως υφίστανται κάποια εγκλήματα που σχετίζονται με την εθνική ασφάλεια και δεν περιλαμβάνονται σε αυτόν τον κατάλογο, για ποιο λόγο αυτά δεν καθορίζονται ρητά;

Φαίνεται ότι η έννοια της εθνικής ασφάλειας, οι ρυθμίσεις και οι διαδικασίες που ακολουθούνται κατ' επίκλησή της παρέχουν μια προβληματικά ευρεία διακριτική ευχέρεια, τα όρια της οποίας δεν είναι εφικτό να ελεγχθούν με κανένα αποτελεσματικό τρόπο.

2. Πέραν των ζητημάτων που εγείρει η έννοια και οι χρήσεις της εθνικής ασφάλειας, εξίσου προβληματική είναι η αρμοδιότητα του Εισαγγελέα Εφετών σε σχέση με την έκδοση της σχετικής διάταξης για την άρση του απορρήτου.

Σύμφωνα με την παρ.2 του αρ.3 του ν.2225/1994:

2. Η αίτηση υποβάλλεται προς τον Εισαγγελέα Εφετών του τόπου της αιτούσας αρχής ή του τόπου όπου πρόκειται να επιβληθεί η άρση, εκτός αν στην αιτούσα αρχή, με βάση διάταξη νόμου και απόφαση του Ανωτάτου Δικαστικού Συμβουλίου έχει ήδη αποσπασθεί και υπηρετεί με αποκλειστική απασχόληση συγκεκριμένος εισαγγελικός λειτουργός, οπότε, στην περίπτωση αυτή, η ανωτέρω αίτηση υποβάλλεται σε αυτόν. Ο πιο πάνω, κατά περίπτωση, αρμόδιος εισαγγελικός λειτουργός αποφασίζει μέσα σε είκοσι τέσσερις (24) ώρες για την άρση ή όχι του απορρήτου με διάταξή του [...]

Ενώ σύμφωνα με τις παραγράφους 4 και 5 του άρθρου 22 Ν.4249/2014, οι οποίες προστέθηκαν με το άρθρο 231 παρ.4 Ν.4281/2014,ΦΕΚ Α 160/8.8.2014, ορίζεται ότι:

5. Ο εισαγγελικός λειτουργός της παρ. 3 του άρθρου 4 του ν. 2265/1994 (Α` 209), όπως η παράγραφος αυτή έχει τροποποιηθεί και ισχύει, εποπτεύει και το έργο της Διεύθυνσης Διαχείρισης και Ανάλυσης Πληροφοριών κατά την άσκηση των αρμοδιοτήτων της που σχετίζονται με τη συλλογή, επεξεργασία και αξιοποίηση πληροφοριών και στοιχείων

6. Σε εξαιρετικές περιπτώσεις κατά τη διάρκεια προκαταρκτικής εξέτασης ή προανάκρισης που ενεργείται στο πλαίσιο των αρμοδιοτήτων των Διευθύνσεων Διαχείρισης και Ανάλυσης Πληροφοριών και Αντιμετώπισης Ειδικών Εγκλημάτων Βίας εφαρμόζονται, αναλογικά, οι διατάξεις του άρθρου 6 του ν. 2713/1999 (Α` 89), όπως έχει τροποποιηθεί και ισχύει, καθώς και του άρθρου 3 του ν. 2225/1994 (Α` 121). Για την εφαρμογή των διατάξεων του προηγούμενου εδαφίου όπου στο άρθρο 6 του ν.2713/1999 αναφέρεται ο εισαγγελικός λειτουργός του άρθρου 3 του νόμου αυτού, νοείται ο εισαγγελικός λειτουργός της προηγούμενης παραγράφου του παρόντος άρθρου.

Από τα παραπάνω συνάγεται ότι για τις περιπτώσεις άρσης απορρήτου για λόγους εθνικής ασφάλειας, οι οποίες ζητούνται από τη Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών²¹⁹, αρμόδιος να αποφασίζει είναι ο Εισαγγελέας Εφετών, δηλαδή ο εποπτεύων το έργο της υπηρεσίας αυτής και στην οποία υπηρετεί με αποκλειστική απασχόληση. Δηλαδή, ο εποπτεύων το έργο μιας υπηρεσίας αποφασίζει για την άρση του απορρήτου στο πλαίσιο μιας έρευνας της ίδιας υπηρεσίας. Η ταύτιση αυτή δημιουργεί ζητήματα ανεξαρτησίας του συγκεκριμένου εισαγγελικού λειτουργού σε σχέση με τη λήψη απόφασης περί άρσης του απορρήτου (ιδίως αν συνεκτιμήσει κανείς ότι συνιστά και μονοπρόσωπο όργανο) και συνεπώς κινδύνου υπονόμησης του απαιτούμενου υψηλού επιπέδου προστασίας του δικαιώματος της απόρρητης επικοινωνίας, η οποία κατά τα λοιπά συνιστά τον (συνταγματικό μάλιστα) κανόνα.

Το συγκεκριμένο ζήτημα αναδείχθηκε από το ΔΕΕ στην υπόθεση C-746/18 και αντιμετωπίστηκε με εμφατικό τρόπο²²⁰. Το ΔΕΕ έκρινε ότι προκύπτει μια απαίτηση ανεξαρτησίας σε σχέση με την αρχή η οποία είναι επιφορτισμένη με τη διενέργεια του προηγούμενου ελέγχου σε σχέση με την άρση του απορρήτου. Ο έλεγχος αυτός επιβάλλει να έχει η αρχή αυτή την ιδιότητα τρίτου, σε σχέση με τον αιτούντα την πρόσβαση στα δεδομένα, ώστε να είναι σε θέση να ασκεί τον έλεγχο αυτό κατά τρόπο αντικειμενικό και αμερόληπτο χωρίς καμία εξωτερική επιρροή, τονίζοντας ότι επιβάλλεται η αρχή η οποία είναι επιφορτισμένη με αυτόν τον προηγούμενο έλεγχο να μην εμπλέκεται στη διεξαγωγή της συγκεκριμένης ποινικής έρευνας και να έχει ουδέτερη θέση έναντι των μετεχόντων στην ποινική δίκη.

3. Από τη νομοθεσία και την πρακτική που ισχύει σε σχέση με την εν γένει άρση του απορρήτου, αναδεικνύεται σημαντικό έλλειμμα σε σχέση με σημαντικές πτυχές αυτής. Επί παραδείγματι, τα εμπλεκόμενα όργανα και αρχές (Εισαγγελέας Εφετών, ΑΔΑΕ) δεν λαμβάνουν ενημέρωση που αφορά τα αποτελέσματα της διαταχθείσας άρσης απορρήτου²²¹, η οποία κατά τα λοιπά λαμβάνει χώρα για τη διερεύνηση συγκεκριμένων απειλών για την εθνική ασφάλεια ²²². Στο υποθετικό σενάριο κατά το οποίο οι διαδικασίες άρσης απορρήτου, σε σημαντικό ποσοστό, δεν οδηγούν στον εντοπισμό πράξεων και προσώπων, καταλείπεται εύλογα η αμφιβολία ότι αυτές δε γίνονται για το δηλωμένο σκοπό αλλά για άλλους και μάλιστα μη ανακοινωμένους. Με άλλα λόγια, η μη επαλήθευση της αναγκαιότητας και της

αποτελεσματικότητας των αιτούμενων άρσεων απορρήτου, τόσο σε κάθε περίπτωση όσο και συνολικά, δημιουργεί συνθήκες κατάχρησης των εν λόγω ανακριτικών πράξεων όσο και αδιαφάνειας σε σχέση με τη συνολική πρακτική.

ΤΜΗΜΑ ΔΕΚΑΤΟ ΤΡΙΤΟ

Απαγορεύσεις αποδεικτικής αξιοποίησης στοιχείων κατόπιν άρσης απορρήτου και το ζήτημα των μεταδεδομένων

Οι ανωτέρω παρατηρήσεις δε συνδέονται μόνο με το ζήτημα της προσβολής του επικοινωνιακού απορρήτου αλλά και με το ζήτημα της αξιοποίησης του συλλεχθέντος στο πλαίσιο μιας δίκης. Το Σύνταγμα στο αρ. 19 παρ.3 θέτει ρητή απαγόρευση χρήσης αποδεικτικών μέσων που συλλέχθηκαν κατά παράβαση συνολικά του άρθρου 19 του Συντάγματος, συμπεριλαμβάνοντας δηλαδή τον εκτελεστικό νόμο (εν προκειμένω το ν.2225/1994), το νόμο που ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες της ανεξάρτητης αρχής, τον διασφαλίζοντα το απόρρητο, δηλαδή της ΑΑΔΕ (ν.3115/2003) όσο και το ίδιο το δικαίωμα της απόρρητης επικοινωνίας.

Ειδικότερο προστατευτικό ρυθμιστικό περιεχόμενο περιέχουν οι παρ.9 εδάφιο β' και 10 του αρ.5 του ν.2225/1994, ορίζοντας κατ' ουσία ότι:

α) τα στοιχεία που είχαν συλλεγεί σε εκτέλεση της διάταξης για την άρση του απορρήτου σε περίπτωση διακρίβωσης εγκλημάτων, σύμφωνα με το άρθρο 4, επισυνάπτονται στη δικογραφία, αν συνιστούν αποδεικτικά μέσα για την ποινική δίωξη κατά την κρίση της αρχής η οποία εξέδωσε τη διάταξη και ότι

β) 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.

ενώ εξαιρετικά προβλέφθηκε στην παρ.10 εδάφιο β' ότι:

Κατ' εξαίρεση η αρχή που εξέδωσε τη διάταξη μπορεί κατά την αιτιολογημένη κρίση της, να επιτρέψει με νεότερη διάταξή της να χρησιμοποιηθούν και να ληφθούν υπόψη τα παραπάνω στοιχεία, αν χρησιμεύουν για τη διακρίβωση άλλου, ιδιαίτερος σοβαρού εγκλήματος από αυτά που αναφέρονται στην παρ. 1 του άρθρου 4 του παρόντος νόμου

Αντίστοιχη επιχειρηματολογία δύναται να εξαχθεί και από το άρθρο 254 ΚΠΔ, το οποίο περιορίζει τη χρήση των στοιχείων μόνο για συγκεκριμένα εγκλήματα και μάλιστα με την πρόβλεψη συγκεκριμένων εγγυήσεων.²²³

Οι ανωτέρω αποδεικτικές απαγορεύσεις σχετίζονται εντόνως με το ζήτημα της συλλογής και αξιοποίησης των μεταδεδομένων επικοινωνίας. Ιδίως στις περιπτώσεις της άρσης απορρήτου σε μια γεωγραφική περιοχή²²⁴ και λόγω ακριβώς του γενικευμένου χαρακτήρα αυτής, είναι πολύ πιθανό να συλλεχθούν στοιχεία σε σχέση με την τέλεση αδικημάτων μη περιλαμβανόμενα στον περιοριστικό κατάλογο του αρ.4 του ν.2225/1994. Επιπλέον αυτό είναι δυνατό να συμβεί και σε σχέση με πρόσωπα τα οποία δεν σχετίζονται καθόλου με τη διερεύνηση των απειλών κατά της εθνικής ασφάλειας. Η αποδοχή μιας τέτοιας πρακτικής, δηλαδή η ανακριτική αξιοποίηση στοιχείων που προέκυψαν παρεμπιπτόντως στο πλαίσιο άρσης απορρήτου για λόγους εθνικής ασφάλειας και δεν αφορούν την τέλεση των αδικημάτων που περιγράφονται στο αρ.4 του ν.2225/1994, θα οδηγούσε σε παραβίαση του αρ.19 παρ.3 του Συντάγματος και του ν.2225/1994. Επιπλέον δε, θα οδηγούσε στην δικαιολογικά μη αποδεκτή επέκταση των επιδιώξεων της ποινικής πρόληψης και καταστολής, κατά τρόπο που θα προσέκρουε ευθέως στον πυρήνα του δικαιώματος της απόρρητης επικοινωνίας. Την άποψη αυτή δυστυχώς μέρος της νομολογίας δε φαίνεται να ασπάζεται, προκρίνοντας την αποδεικτική αξιοποίησή τους²²⁵.

Για να γίνει πιο φανερός ο κίνδυνος που σχετίζεται με τα μεταδεδομένα επικοινωνίας, θα πρέπει να αναλογιστεί κανείς τη διαφορά μεταξύ της μεθόδου της συνακρόασης συγκεκριμένων επικοινωνιών συγκεκριμένων προσώπων και της μεθόδου της συλλογής και ανάλυσης μεταδεδομένων επικοινωνίας (συμπεριλαμβανομένων των στοιχείων τηλεφωνικών κλήσεων και των δεδομένων κίνησης και θέσης) είτε ενός προσώπου, είτε μια ολόκληρης γεωγραφικής περιοχής.

Στην πρώτη περίπτωση, η συνακρόαση τηλεφωνικών επικοινωνιών απαιτεί τη δέσμευση σημαντικών πόρων (εξοπλισμού, ανθρώπων, χρόνου), αφορά κατά βάση αδόμητα δεδομένα, βρίσκει τα όριά της στις ανθρώπινες ικανότητες ανάλυσης περιεχομένου επικοινωνιών²²⁶, ενώ καταλήγει στην άρση του επικοινωνιακού απορρήτου στοχευμένα και με αναφορά σε συγκεκριμένα πρόσωπα. Έχει δηλαδή μια πιο «αναλογική»²²⁷ προσέγγιση.

Στη δεύτερη περίπτωση, η συλλογή και ανάλυση μεταδεδομένων επικοινωνίας (είτε ενός προσώπου, είτε -πολύ περισσότερο- μιας ολόκληρης γεωγραφικής περιοχής) απαιτεί λιγότερους πόρους, βασίζεται στην ψηφιακή (και συχνά αλγοριθμική ανάλυση) και καταλήγει στη γενικευμένη άρση απορρήτου, κατά τρόπο οριζόντιο, ευρύ και γενικό, με

σημαντικά μεγαλύτερες δυνατότητες στόχευσης ομάδων και προσώπων σε ευρύτερα πεδία της ζωής τους (αν όχι σε όλα), ακολουθώντας μια ψηφιακή/αυτοματοποιημένη προσέγγιση.

Ενώ φαινομενικά η συνακρόαση φαίνεται εκ πρώτης όψης ως η πλέον σοβαρή και βάνανυση επέμβαση στο επικοινωνιακό απόρρητο, στην πραγματικότητα η ανάλυση των μεταδεδομένων επικοινωνίας δύναται να αφορά περισσότερους ανθρώπους και κυρίως να αφορά το σύνολο των δραστηριοτήτων, σχέσεων, πράξεων, συμπεριφορών τους, υπερβαίνοντας ακόμα και τις ανακριτικές επιδιώξεις της διαταχθείσας άρσης απορρήτου²²⁸.

Το ΔΕΕ στην υπόθεση C-746/18 H.K.Prokuratuur αναγνώρισε ξεκάθαρα αυτό τον κίνδυνο.

ΤΜΗΜΑ ΔΕΚΑΤΟ ΤΕΤΑΡΤΟ

Η μαζική παρακολούθηση στη νομολογία του ΕΔΔΑ και τα προβλήματα της εθνικής νομοθεσίας και πρακτικής

Αναφέρθηκε προηγουμένως ότι από τις διατάξεις του ν.2225/1994 προκύπτει ότι είναι επιτρεπτή η μαζική άρση απορρήτου των επικοινωνιών. Η νομολογία του ΕΔΔΑ δεν υποστηρίζει ότι μια τέτοια πρακτική είναι απαγορευμένη. Αντιθέτως, στην πρόσφατη νομολογία του διέγνωσε ότι οι μαζικές παρακολουθήσεις είναι ζωτικής σημασίας στην αντιμετώπιση απειλών εθνικής ασφάλειας²²⁹, επικαλούμενο την ικανότητα διαφυγής των τρομοκρατών από τα παραδοσιακά μέσα επιτήρησης και τη φύση του παγκόσμιου Διαδικτύου, η οποία καθιστά απρόβλεπτη τη διαδρομή μιας συγκεκριμένης επικοινωνίας²³⁰.

Σε κάθε περίπτωση, το ΕΔΔΑ έχει αναπτύξει ένα μίνιμουμ προϋποθέσεων-κριτηρίων για την κατάφαση στο ερώτημα της νομιμότητας των μαζικών παρακολουθήσεων προκειμένου να αξιολογήσει την αναλογικότητα των συναφών μέτρων σε εθνικό επίπεδο και οι διαδικασίες αυτές να είναι συμβατές με την ΕΣΔΑ ²³¹.

Μεταξύ άλλων είναι:

οι λόγοι για τους οποίους μπορεί να δοθεί άδεια για τη διενέργεια μαζικής παρακολούθησης

η διαδικασία που ακολουθείται για την παροχή της άδειας

οι διαδικασίες που ακολουθούνται ως προς την επιλογή, την εξέταση και τη χρήση του υλικού

τα όρια της διάρκειας

οι διαδικασίες του ελέγχου της συμμόρφωσης (και του εκ των υστέρων ελέγχου της συμμόρφωσης) με τις τεθείσες από αυτό εγγυήσεις ανεξάρτητης αρχής και οι εξουσίες της τελευταίας σε περίπτωση μη συμμόρφωσης.

Από την επισκόπηση των προαναφερθέντων, σε σχέση με τα εθνικώς ισχύοντα, φαίνεται ότι το ισχύον πλαίσιο και η πρακτική υπολείπονται καταφανώς του επιπέδου εγγυήσεων που αξιώνει το ΕΔΔΑ. Ειδικότερα:

1. Καθότι παραδοσιακά στις περιπτώσεις άρσης του απορρήτου, οι λόγοι εθνικής ασφάλειας υπερισχύουν σε σημαντικό βαθμό της διερεύνησης των αδικημάτων (δηλαδή φαίνεται να υπάρχει σημαντικός και διαρκής αριθμός εθνικών απειλών), θα έπρεπε οι συγκεκριμένοι λόγοι να καθίσταται ρητοί ανά περίπτωση (ανά διάταξη άρσης), χωρίς να αρκεί η ονομαστική αναφορά αυτών στη σχετική διάταξη του αρμοδίου Εισαγγελέα. Κάτι τέτοιο δε φαίνεται να συμβαίνει²³². Επιπλέον, καθότι δεν προβλέπεται η ύπαρξη αιτιολογίας, δεν παρέχεται καμία απόδειξη για τη συσχέτιση προσώπων ή ομάδας προσώπων με συγκεκριμένες πράξεις που τυγχάνουν διερεύνησης. Κατά τον τρόπο αυτό, οι λόγοι για τους οποίους μπορεί να εκδοθεί διάταξη άρσης απορρήτου είναι εκ των πραγμάτων αόριστοι.

2. Το ζήτημα του μονοπρόσωπου αποφασίζοντος οργάνου (Εισαγγελέα Εφετών) και των ζητημάτων ανεξαρτησίας που αναφέρονται προς το πρόσωπο, αναλύθηκαν ανωτέρω.

3. Δε φαίνεται να υφίστανται διαδικασίες ως προς την επιλογή, την εξέταση και τη χρήση του υλικού, ζητήματα που αντιμετωπίζονται από τις αστυνομικές αρχές.

4. Η χρονική διάρκεια των μέτρων αυτών είναι απροσδιόριστη, όπως προαναφέρθηκε.

5. Αναφορικά με τις διαδικασίες ελέγχου της συμμόρφωσης (και του εκ των υστέρων ελέγχου της συμμόρφωσης) με τις τεθείσες από αυτό εγγυήσεις από ανεξάρτητη αρχή και των εξουσιών της τελευταίας σε περίπτωση μη συμμόρφωσης, φαίνεται ότι η χώρα μας υπολείπεται σημαντικά. Παρότι η ΑΔΑΕ έχει αρμοδιότητες έρευνας, κατάσχεσης, επιβολής προστίμων, στο μείζον ζήτημα των διαδικασιών άρσης του απορρήτου, ελέγχει μόνο την τήρηση των όρων και της διαδικασίας, δηλαδή ασκεί τυπικό έλεγχο, χωρίς να δύναται να εξετάσει την κρίση των δικαστικών αρχών, δεν ενημερώνεται για τα αποτελέσματα των ληφθέντων μέτρων²³³.

Συνεπώς, το εθνικό πλαίσιο όσο και η μέχρι τώρα τηρούμενη πρακτική, δε φαίνεται να συμμορφώνεται με τα νομολογιακά κριτήρια του ΕΔΔΑ. Αντιθέτως, παρατηρείται μια υπερβολικά τυπολατρική και ταυτόχρονα ελαστική διαδικασία, η οποία επιτρέπει σοβαρές και εν πολλοίς ανέλεγκτες παρεμβάσεις στο δικαίωμα της απόρρητης επικοινωνίας.

Αντί επιλόγου

*Το αιώνιο πρόβλημα του νόμου είναι
ότι πάντα καταλήγει
στο ποιος κρατάει το ζύγι.
Μεμιάς όλες οι δικλείδες
έχουν τη χρησιμότητα μιας ομπρέλας όταν ρίχνει κεραυνούς
Η σιωπή για αυτό το ερώτημα
δεν ήτανε ποτέ τυχαία⁴*

Τα μεταδεδομένα επικοινωνίας συνιστούν ένα αναπόφευκτο παράγωγο κάθε είδους επικοινωνίας. Είτε σε μια απλή τηλεφωνική επικοινωνία, είτε σε μια ψηφιακή, η ίδια η επικοινωνία και τα σχετικώς χρησιμοποιούμενα μέσα (τερματικά, λογισμικό, δίκτυα), δημιουργούν ένα πλήθος πληροφοριών σε σχέση αυτή. Παρά την ύπαρξη διαφοροποιήσεων²³⁴ αναφορικά με τον πληροφοριακό πλούτο των εμπεριεχόμενων μεταδεδομένων, το βέβαιο είναι ότι σε κάθε περίπτωση αυτός είναι σημαντικός και ότι τα επικοινωνούντα πρόσωπα δύσκολα μπορούν να αποτρέψουν τη δημιουργία τους.

Ο πλούτος αυτός είναι δυνατό να αποκαλύψει, εκτός από το περιεχόμενο της επικοινωνίας, ένα πλήθος πληροφοριών σε σχέση με ομάδες προσώπων και πρόσωπα. Οι πληροφορίες αυτές έχουν ανησυχητικά μεγάλο εύρος όσο και βάθος και συνιστούν μια ευρεία επέμβαση στο δικαίωμα της απόρρητης επικοινωνίας όσο και της ιδιωτικότητας. Παρά το ότι η αρχική προσέγγιση των δικαιωμάτων αυτών είναι ατομοκεντρική, οι αναφερθείσες δυνατότητες ανάλυσης των μεταδεδομένων επικοινωνίας μοιραία μεταθέτουν τη συζήτηση για τους κινδύνους που εγκυμονούν και στο συλλογικό επίπεδο. Η παρακολούθηση ομάδων μπορεί να σχηματίσει ιδιαίτερα ακριβή συλλογικά προφίλ για τα πρόσωπα που τις απαρτίζουν και προφανώς ατομικά. Η έννοια της ιδιωτικότητας σε επίπεδο ομάδας (group-level privacy) έρχεται ολοένα και περισσότερο στο προσκήνιο²³⁵ για να αναδείξει πιθανούς τρόπους αντιμετώπισης των νέων αυτών κινδύνων.

⁴ Φάκας Π. Δημήτριος (2019), *Μικρά Νομικά*, αδημοσίευτο

Το επόμενο διάστημα με την επέκταση του Διαδικτύου των Πραγμάτων (Internet of Things-IoT), η «παραγωγή» μεταδεδομένων επικοινωνίας θα εκτιναχθεί σε ακόμα μεγαλύτερο βαθμό και θα θέσει επιπλέον ερωτήματα. Η επεξεργασία πληροφοριών που παράγονται από τη λειτουργία συνδεδεμένων στο διαδίκτυο συσκευών εγείρει νέα ζητήματα αναφορικά με την ταυτοποίηση των χρηστών τους, τη δημιουργία ακόμα πιο λεπτομερών προφίλ, τη διασύνδεση πληροφοριών από διαφορετικές συσκευές και άλλα²³⁶.

Η συλλογή μεγάλου βάθους και εύρους δημογραφικών όσο και στενά ατομικών πληροφοριών, θα έπρεπε να ανακατευθύνει τη σκέψη στο παρελθόν ανάλογων διαδικασιών, καθώς δεν είναι πρώτη φορά που συμβαίνουν. Η συγκέντρωση και αξιοποίηση τέτοιων πληροφοριών από ολοκληρωτικούς μηχανισμούς οδήγησε στην άσκηση ασφυκτικού ελέγχου και επιτήρηση επί στοχοποιημένων ομάδων πληθυσμού, με αποδεδειγμένα τραγικά αποτελέσματα ²³⁷. Υποτιμάται ότι η στροφή του μοντέλου συλλογής και ανάλυσης πληροφοριών από το περιεχόμενο των επικοινωνιών στα μεταδεδομένα, έχει τις ρίζες του σε γεωπολιτικές και μιλιταριστικές επιδιώξεις, σε ανάγκες των υπηρεσιών ασφαλείας και όχι σε κοινωνικές ανάγκες. "Συνέβη, επομένως μπορεί να ξανασυμβεί"²³⁸.

Αν και η εθνική νομοθεσία κατ' αρχήν προστατεύει τα μεταδεδομένα επικοινωνίας ως στοιχείο του απορρήτου της επικοινωνίας, η προστασία αυτή δεν εκτείνεται αποτελεσματικά απ' άκρο σε άκρο. Συγκεκριμένα θεσμικά και διαδικαστικά ελλείματα καθώς και η δυνατότητα αόριστης επίκλησης λόγων εθνικής ασφάλειας, επιτρέπουν σοβαρές επεμβάσεις σε σχέση με αυτά, δίχως την ύπαρξη επαρκών αντισταθμιστικών μηχανισμών ελέγχου και λογοδοσίας.

Οι διαδικασίες που άπτονται του πεδίου της απόρρητης επικοινωνίας και της προστασίας των μεταδεδομένων επικοινωνίας, απαιτούν νομική εγρήγορση όσο και εξοικείωση με τις διαθέσιμες τεχνολογίες επικοινωνιών, για τους ενδεικτικώς παρατιθέμενους ακόλουθους λόγους:

Α. Το επίπεδο συλλογής μεταδεδομένων επικοινωνίας, αναφορικά με τον αριθμό των προσώπων που αφορούν όσο και το είδος αυτών, φαίνεται να βρίσκεται σήμερα στο υψηλότερο δυνατό σημείο σε σχέση με κάθε άλλη προηγούμενη περίοδο. Η διάχυση ιδίως των ψηφιακών μέσων επικοινωνίας, τα οποία παράγουν περισσότερες κατηγορίες μεταδεδομένων έναντι των αναλογικών, έχει συμβάλει σε μια ποιοτική όσο και ποσοτική διαφορά σε σχέση με το παρελθόν.

Β. Η αύξηση της υπολογιστικής ισχύος όσο και οι συνεχώς εξελισσόμενες δυνατότητες της αλγοριθμικής επεξεργασίας δεδομένων μεγάλης κλίμακας, επιτρέπουν την ανάλυση μεταδεδομένων επικοινωνίας και τη δημιουργία ατομικών όσο και συλλογικών προφίλ, με υψηλό βαθμό ακρίβειας. Τα προφίλ αυτά, εκτός από το περιεχόμενο των επικοινωνιών μπορούν να αποτυπώσουν με λεπτομέρεια σχεδόν κάθε πτυχή της ανθρώπινης ζωής. Η παρέμβαση στο δικαίωμα της απόρρητης επικοινωνίας όσο και στην ιδιωτικότητα, είναι τεχνικά εφικτή σε ελάχιστο χρόνο.

Γ. Το δικαίωμα στην απόρρητη επικοινωνία είναι απολύτως απαραβίαστο, κατά ρητή μάλιστα συνταγματική πρόβλεψη. Ως εκ τούτου, οποιαδήποτε παρέμβαση σε αυτό θα πρέπει να συνιστά μια στενά οριοθετημένη εξαίρεση για τις προβλεπόμενες στο νόμο περιπτώσεις, υπό τον όρο ότι κάθε άλλο διαθέσιμο μέσο σε σχέση με τα επίδικα ερευνώμενα, απεδείχθη μη αποτελεσματικό.

Δ. Η ανάλυση μεταδεδομένων στο πλαίσιο οριακών ή καταχρηστικών διαδικασιών άρσης απορρήτου, δημιουργεί σημαντικές απειλές για την ίδια τη φύση του δημοκρατικού πολιτεύματος. Δεδομένου ότι το δικαίωμα στην απόρρητη επικοινωνία συμπλέκεται με την άσκηση αρκετών άλλων θεμελιωδών δικαιωμάτων, η διαρκής και εκτεταμένη επιτήρηση προσώπων και ομάδων για αόριστους ή προσχηματικούς λόγους, δημιουργεί συνθήκες ασφυκτικού ελέγχου, πίεσης, αυτοπεριορισμού και διάχυτου φόβου, κάμπτοντας τα δικαιοκρατικά θεμελιώδη, δηλαδή ότι η ελευθερία συνιστά τον κανόνα και όχι την εξαίρεση.

Οι θεσμικές όσο και διαδικαστικές εγγυήσεις της προστασίας των μεταδεδομένων επικοινωνίας, δε φαίνονται ικανές να ανακόψουν από μόνες τους τις διάχυτες τάσεις εξάπλωσης ενός σύγχρονου Πανοπτικού. Ωστόσο, η υποχώρηση σε σχέση με αυτές, δε μπορεί να συνιστά επιλογή μιας στοιχειωδώς δημοκρατικής πολιτείας. Ο εφαρμοστής του δικαίου δε δύναται να αξιοποιεί κάθε διαθέσιμη τεχνολογία, απλώς επειδή αυτό είναι εφικτό. Η μετάπτωση σε καθεστώτα αυταρχισμού, ανελευθερίας και καταπίεσης είναι πολύ πιο κοντά απ' όσο μπορεί να φαίνεται.

«Η οδός της ελευθερίας είναι δύσκολη και τραγική, διότι δεν υπάρχει τίποτε πιο υπεύθυνο, πιο ηρωικό και οδυνηρό από αυτή. Οι οδοί της αναγκαιότητας και του καταναγκασμού είναι ευκολότερες, λιγότερο τραγικές και ηρωικές»²³⁹.

¹ Baker Stewart, NSA General Counsel, Αναφέρεται στην απόφαση του Αμερικανικού Εφετείου στην υπόθεση 13-50572, 09/02/2020 UNITED STATES OF AMERICA v. BASAALY SAEED MOALIN, AKA Basal, AKA Muse Shekhnor Roble κλπ, βλ.σελ.20, διαθέσιμη στο [13-50572.pdf \(uscourts.gov\)](https://www.uscourts.gov/13-50572.pdf) ημερομηνία πρόσβασης 4/6/2022

² και όχι το αντίθετο όπως ευρύτερα εκτιμάται.

³ Η δημιουργία του internet ήταν αποτέλεσμα ενός ερευνητικού προγράμματος της DARPA και του Αμερικανικού Υπουργείου Άμυνας σε σχέση με τη δυνατότητα επιβίωσης των τηλεπικοινωνιών σε περίπτωση πυρηνικής επίθεσης από την τότε ΕΣΣΔ. Σχετική αναφορά μεταξύ πολλών στο Castells Manuel (2010) *The rise of the Network Society*, 2nd edition, UK, σελ.6

⁴ IEEE (2001), Draft Standard for Learning Object Metadata. Αναφορά στο Duval Erik (2001), *Metadata Standards: What, Who and Why*, Journal of Universal Computer Science, vol. 7, no. 7 (2001), 591-601, σελ. 591, διαθέσιμο στο [Duval E.pdf \(jucs.org\)](https://www.jucs.org/Duval_E.pdf), ημερομηνία πρόσβασης 4/6/2022

⁵ Ας σημειωθεί ωστόσο ότι οι παρατιθέμενες «ανάγκες», είναι απόρροια των ιστορικών διαδικασιών που συνέτειναν στην εξέλιξη των ηλεκτρονικών υπολογιστών κατά τη δεκαετία του 1950, της ψυχροπολεμικής αντιπαράθεσης όσο και του κοινωνικοοικονομικού μοντέλου που επικράτησε στο δυτικό κόσμο μετά το τέλος του ΒΠΠ.

⁶ Είναι το άλλως λεγόμενο request-response protocol στην επιστήμη της πληροφορικής

⁷ Το ίδιο ασφαλώς ισχύει και για τα μεταδεδομένα των τηλεφωνικών κλήσεων.

⁸ Όρος που όπως θα αναλυθεί στη συνέχεια είναι τουλάχιστον ανακριβής

⁹ Shane Harris (2014) How the NSA Became a Killing Machine, *The Daily Beast* (9-11-2014) διαθέσιμο στο <https://www.thedailybeast.com/how-the-nsa-became-a-killing-machine> ημ. πρόσβασης 4/6/2022

¹⁰ Hern Alex (2018) Fitness tracking app Strava gives away location of secret US army bases, *The Guardian* (28/1/2018) διαθέσιμο στο <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases> ημ.πρόσβασης 4/6/2022

¹¹ Pomerantz Jeffrey (2015) *Metadata*, MIT PRESS Essential Knowledge series (Cambridge), σελ.5

¹² Ενδεικτικά: ΑΠ 1448/2011, ΑΠ 1421/2010, ΣτΕ 1593/2016

¹³ Ενδεικτικά: Γνωμ ΕισΑΠ 9/2009, 9/2011, ΑΠ 78/2021, ΑΠ 689/2014, ΑΠ 203/2014

¹⁴ Όσο και της ΑΠΔΠΧ, των οποίων οι αρμοδιότητες σε σχέση με το ζήτημα της προστασίας των μεταδεδομένων είναι μάλλον διασταυρούμενες

¹⁵ Κατά συστηματικό τρόπο – τουλάχιστον κατά τη γνώμη του γράφοντος

¹⁶ Τουλάχιστον βάσει του καταστατικού τους χάρτη

¹⁷ και εν πολλοίς επιτυγχάνεται

¹⁸ Α. Παπανικολάου (2020) *Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*, διαθέσιμο στο [Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα - constitutionalism.gr](https://www.constitutionalism.gr) Ημ.πρόσβασης 4/6/2022

¹⁹ Θέση που έχει υιοθετήσει και το ΕΔΔΑ βλ.ενδεικτικά CASE OF ÖNER YILDIZ v. TURKEY, 30/11/2004, σκ.89,95

²⁰ Μάνεσης Α., *Συνταγματικά Δικαιώματα* (1982) Α Ατομικές ελευθερίες, 4^η έκδοση, Αθήνα – Θεσσαλονίκη, σελ.232

²¹ Με συχνές ωστόσο παραφωνίες

²² Πχ γλώσσα πίτζιν, βλ. Sismondo Sergio (2016) *Εισαγωγή στις Σπουδές Επιστήμης και Τεχνολογίας*, Αθήνα, Liberal Books, σελ.42

²³ National Academy of Sciences; National Academy of Engineering; Institute of Medicine; Committee on Science, Engineering, and Public Policy (2009) *On Being a Scientist: A Guide to Responsible Conduct in Research*, εκδ. The National Academies Press (Washington D.C.), διαθέσιμο στο <https://www.nap.edu/catalog/12192/on-being-a-scientist-a-guide-to-responsible-conduct-in> , σελ.34

²⁴ αλλά εσφαλμένα

²⁵ *Researchers who manipulate their data in ways that deceive others, even if the manipulation seems insignificant at the time, are violating both the basic values and widely accepted professional standards of science. Researchers draw*

conclusions based on their observations of nature. If data are altered to present a case that is stronger than the data warrant, researchers fail to fulfill all three of the obligations described at the beginning of this guide. They mislead their colleagues and potentially impede progress in their field or research. Βλ. υποσημ.25 *On Being a Scientist: A Guide to Responsible Conduct in Research*, National Academies Press σελ.27

²⁶ Είναι χαρακτηριστικό το παράδειγμα της νομικής αρθογραφίας όσο και της νομολογίας της άνοιξης και του καλοκαιριού του 2021, η οποία στην πλειονότητά της υποστήριζε σθεναρά την συνταγματικότητα των περιορισμών των δικαιωμάτων, όσο και τη νομιμότητα του υποχρεωτικού εμβολιασμού, αμφότερα στη βάση της εργαλειακής προσέγγισης της προστασίας της δημόσιας υγείας και της επίκλησης της πανδημίας. Υπήρξε εμφανής η διάθεση στρατευμένης χρήσης ιατρικών όρων και εννοιών (βλ. συζήτηση για την έννοια «κρούσμα»), η επιλεκτική χρήση αυτών, η επιδεικτική αγνόηση επιστημονικών ενστάσεων σε σχέση με τα παραπάνω, κατά τρόπο που προδίκαιζε τα αποτελέσματα των νομικών συλλογισμών.

²⁷ Σουν Τζου (2008) , *Η Τέχνη του Πολέμου* , Εκδόσεις Περίπλους, σελ.40

²⁸ Motta Dan (2018) *HISTORY OF THE WORLD: PART II... METADATA*, διαθέσιμο στο <https://discover.cobbtechnologies.com/blog/history-of-the-world-metadata> ημ.πρόσβασης 4/6/2022

²⁹ Πουητής, επιγραμματοποιός, 300 π.Χ.-240 π.Χ

³⁰ Pomerantz Jeffrey (2015) *Metadata*, σελ.6

³¹ Gartner Richard (2016) *Metadata, Shaping Knowledge from Antiquity to the Semantic Web*, Springer, UK , σελ.16

³² Η οποία συνιστούσε ένα από τα πρώτα βασίλεια της Συρίας και λειτούργησε ως σημαντικό κέντρο εμπορίου και πολιτισμού

³³ 1350 - 1295 π.Χ.

³⁴ Agar J. (2006), *What Difference Did Computers Make?*, *Social Studies of Science*, vol. 36, no. 6, 2006, pp. 869–907. Διαθέσιμο στο www.jstor.org/stable/25474487. ημ.πρόσβασης 4/6/2022, σελ.872

³⁵ Η σύλληψη της ιδέας αυτής αποδίδεται στο δημιουργό του διαδικτύου, Tim Berners-Lee.

³⁶ Πχ βασισμένοι στην προφορικότητα

³⁷ Πρόταση ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ 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 για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) COM(2017) 10 final, 2017/0003 (COD)

³⁸ Εκτός και αν γίνεται κάποια σχετική διάκριση

³⁹ Κατά την ορολογία του αρ.4 παρ.1 περιπτ. γ' του ΠΔ 47/2005

⁴⁰ Landau Susan (2020) *Categorizing Uses of Communications Metadata: Systematizing Knowledge and Presenting a Path for Privacy*. In *New Security Paradigms Workshop 2020 (NSPW '20)*, ACM, New York, NY, <https://doi.org/10.1145/3442167.3442171> 19 σελ. διαθέσιμο στο [Categorizing Uses of Communications Metadata: Systematizing Knowledge and Presenting a Path for Privacy \(acm.org\)](https://www.acm.org), σελ.4

⁴¹ Κετσιέτζης Κώστας (2022) *Το τέλος του «χρόνου ομιλίας»: Νέα εποχή στην κινητή τηλεφωνία* Money Review (εφημ. ΚΑΘΗΜΕΡΙΝΗ) 14/5/2022 διαθέσιμο στο <https://www.moneyreview.gr/business-and-finance/economy/77112/to-telos-toy-chronoy-omilias-nea-epochi-stin-kiniti-tilefonia/> ημ.πρόσβασης 4/6/2022

⁴² Για λόγους και μηχανισμούς μάλλον όχι τυχαίους

⁴³ “longue durée” κατά τον ιστορικό Fernand Paul Achille Braudel, ο οποίος διατύπωσε το περίφημο: «Ο βραχύς χρόνος είναι η πιο ιδιόρρυθμη, η πιο απατηλή διάρκεια». Braudel F. (1987) *Μελέτες για την Ιστορία*, ΕΜΝΕ ΜΝΗΜΩΝ, 2^η έκδοση, σελ.21

⁴⁴ Ο γράφων έχει τη θέση ότι ο ιστορικός κύκλος των γεγονότων στον οποίο εντάσσεται η επίθεση «στους δίδυμους πύργους» δεν έχει ακόμα κλείσει, διότι στην ουσία αποτέλεσε μια και μόνο (αναμφίβολα όμως σημαντική) στιγμή ενός εξελισσόμενου παγκόσμιου διακρατικού ανταγωνισμού, που ξεκίνησε μετά την διάλυση της Σοβιετικής Ένωσης και συνεχίζεται μέχρι σήμερα με ποικίλες μορφές. Εσχάτως δε ανοιχτά πολεμικές.

⁴⁵ Άλλωστε στις ΗΠΑ έχει αναπτυχθεί ισχυρός επιστημονικός αντίλογος στις κυρίαρχες απόψεις για πλειάδα ζητημάτων που σχετίζονται με τις «τεχνικές» διαστάσεις, προϋποθέσεις όσο και τα αποτελέσματα των πολλαπλών επιθέσεων που σημειώθηκαν εκείνη τη μέρα.

⁴⁶ Η φωτιά έσβησε στις 20/12/2001. (2001) *World Trade Center fires finally put out* CNN.COM 20/12/2001, διαθέσιμο στο [CNN.com - World Trade Center fires finally put out - December 20, 2001](https://www.cnn.com/2001/12/20/world.wtc.fire/index.html), Ημ.πρόσβασης 4/6/2022

⁴⁷ Ο νόμος ανήλθε σε 342 σελίδες τη στιγμή κατά την οποία ο μέσος όρος νομοθετημάτων το 2001 ανερχόταν στις 22 σελίδες περίπου. Παρά ταύτα η διαδικασία νομικής επεξεργασίας και ψήφισής του ολοκληρώθηκε σε χρόνο ρεκόρ. Είναι εύλογη η υπόθεση ότι ο νόμος είχε τύχει μακράς επεξεργασίας σε προγενέστερο χρόνο.

Βλ. σχετικά Hudson Jr David L. (2012) *PATRIOT ACT* <https://www.freedomforuminstitute.org/patriot-act> διαθέσιμο στο [Patriot Act | Freedom Forum Institute](https://www.freedomforuminstitute.org/patriot-act) ημ.πρόσβασης 4/6/2022.

Επίσης βλ. σχετικά *Are bills getting longer?* (2014) <https://govtracknews.wordpress.com/are-bills-getting-longer/> διαθέσιμο στο [Are bills getting longer? – GovTrack.us Site News \(wordpress.com\)](https://govtracknews.wordpress.com/are-bills-getting-longer/) (24/5/2014) ημ.πρόσβασης 4/6/2022

⁴⁸ Βάσει του USA FREEDOM ACT περιορίστηκε το εύρος των συλλεγόμενων δεδομένων και εισήχθησαν κάποιες δικλείδες διαφάνειας

⁴⁹ Αυτονομιστική οργάνωση Βάσκων, με πολιτική έκφραση το κόμμα Μπατασούνα, η οποία διαλύθηκε το 2018

⁵⁰ Δύο εκ των συνεργών της επίθεσης, αποδείχθηκε ότι ήταν πληροφοριοδότες της ισπανικής αστυνομίας (Guardia Civil).

Βλ. σχετικά Rubio Antonio (2006), “Los dos cómplices clave de los autores del 11-M eran confidentes policiales”, *Elmundo* (26/5/2006) διαθέσιμο στο [Los dos cómplices clave de los autores del 11-M eran confidentes policiales | elmundo.es](http://www.elmundo.es/2006/05/26/052601001_122.html) ημ.πρόσβασης 4/6/2022

⁵¹ Αξίζει ωστόσο να υπενθυμίσουμε ότι οι δύο από τους 4 βομβιστές ήταν υπό παρακολούθηση από τις βρετανικές υπηρεσίες πληροφοριών. Ωστόσο, παρά το ότι είχε προηγηθεί η 11 Σεπτεμβρίου, η βομβιστική επίθεση στη Μαδρίτη και οι υπηρεσίες ασφαλείας ήταν σε εγρήγορση, τελικά οι δράστες πέτυχαν το στόχο τους.

Βλ. σχετικά Batty David (2006) “Two 7/7 bombers were under surveillance” *The Guardian*, 11/5/2006 διαθέσιμο στο [Two 7/7 bombers were under surveillance | 7 July London attacks | The Guardian](https://www.theguardian.com/world/2006/05/11/two-7-7-bombers-were-under-surveillance) ημ.πρόσβασης 4/6/2022

Βλ. επίσης Gallagher Ryan (2018) “HOW LONDON’S 7/7 BOMBINGS LED TO “UNPRECEDENTED” SURVEILLANCE TACTICS” <https://theintercept.com/2018/03/13/how-london-7-7-bombings-led-to-unprecedented-surveillance-tactics/> διαθέσιμο στο [How London's 7/7 Bombings Led to "Unprecedented" Surveillance Tactics \(theintercept.com\)](https://theintercept.com/2018/03/13/how-london-7-7-bombings-led-to-unprecedented-surveillance-tactics/) ημ.πρόσβασης 4/6/2022

⁵² «Either you are with us, or you are with the terrorists», George W. Bush “Bush: 'You Are Either With Us, Or With the Terrorists' - 2001-09-21” (2009) *Voice of America*, 27/10/2009 <https://www.voanews.com/a/bush-6641197/549664.html> διαθέσιμο στο <https://www.voanews.com/a/bush-6641197/549664.html> ημ.πρόσβασης 4/6/2022

⁵³ *But the little secret here may be that the vagueness of the phrase was deliberately (or instinctively) calculated by its sponsors. Constant reference to a “war on terror” did accomplish one major objective: It stimulated the emergence of a culture of fear. Fear obscures reason, intensifies emotions and makes it easier for demagogic politicians to mobilize the public on behalf of the policies they want to pursue.* Από Brzezinski Zbigniew (2007), “Terrorized by 'War on Terror” *Washington Post*, 25/3/2007, διαθέσιμο στο <https://www.washingtonpost.com/wp-dyn/content/article/2007/03/23/AR2007032301613.html> ημ.πρόσβασης 4/6/2022

⁵⁴ Οι υποσχέσεις ήταν ρητές τόσο προφορικές όσο και γραπτές (στο πλαίσιο διαφόρων συμφωνιών), χωρίς ωστόσο να λάβουν ποτέ τη μορφή επίσημης Συνθήκης.

Ενδεικτικά βλ. Wintour Patrick (2022) “Russia’s belief in Nato ‘betrayal’ – and why it matters today” *The Guardian*, 12/1/2022, διαθέσιμο στο [Russia’s belief in Nato ‘betrayal’ – and why it matters today | Russia | The Guardian](https://www.theguardian.com/world/2022/jan/12/russia-belief-nato-betrayal), ημ.πρόσβασης 4/6/2022

Βλ. επίσης Protagon Team (2022) “Όταν το NATO (μπορεί να) εξαπάτησε την πρώην ΕΣΣΔ” *Protagon.gr* 13/1/2022 διαθέσιμο στο [Όταν το NATO \(μπορεί να\) εξαπάτησε την πρώην ΕΣΣΔ | Protagon.gr](https://www.protagon.gr/2022/01/13/otan-to-nato-μπορει-να-εξαπατησε-την-πρωην-εσση/) ημ.πρόσβασης 4/6/2022

⁵⁵ “Who controls Eurasia controls the world” Brzezinski Zbigniew (1997), *The Grand Chess Board*, New York Basic Books. Αναφέρεται στο Sabet, Amr G. E. “Geopolitics of a Changing World Order: US Strategy and the

Scramble for the Eurasian Heartland.” Contemporary Arab Affairs, vol. 8, no. 2, 2015, σελ.165. διαθέσιμο στο <https://www.jstor.org/stable/48600062>. ημ.πρόσβασης 4/6/2022

Η φράση αποτελεί «συνέχεια» των σχετικών απόψεων του Halford Mackinder (*Whoever rules the Eastern Europe will rule the Heartland, whoever rules the Heartland will rule the World Island, and whoever rules the World Island will rule the world*) αναφέρεται στο Sabet, Amr G. E. “Geopolitics of a Changing World Order: US Strategy and the Scramble for the Eurasian Heartland. Σελ.164

⁵⁶ Είσοδος χωρών Ανατολικής Ευρώπης στο NATO (Πηγή: [NATO - Βικιπαίδεια \(wikipedia.org\)](https://el.wikipedia.org/wiki/NATO) ημ.πρόσβασης 4/6/2022):

12 Μαρτίου 1999: Τσεχία, Ουγγαρία, Πολωνία

29 Μαρτίου 2004: Βουλγαρία, Εσθονία, Λετονία, Λιθουανία, Ρουμανία, Σλοβακία, Σλοβενία

1 Απριλίου 2009: Αλβανία, Κροατία

5 Ιουνίου 2017: Μαυροβούνιο

27 Μαρτίου 2020: Βόρεια Μακεδονία

⁵⁷ Μεσχαΐμερ Τζον (2022) Γιατί η Δύση έχει την ευθύνη για την κρίση στην Ουκρανία, *Καθημερινή* 20/3/2022 διαθέσιμο στο [Γιατί η Δύση έχει την ευθύνη για την κρίση στην Ουκρανία | Η ΚΑΘΗΜΕΡΙΝΗ \(kathimerini.gr\)](https://www.kathimerini.gr) ημ.πρόσβασης 4/6/2022

⁵⁸ Ως συνέχεια της «στρατηγικής της ανάσχεσης» του Τζωρτζ Κένναν

⁵⁹ Η συνέχεια του παγκόσμιου αυτού ανταγωνισμού συνεχίζει μέχρι τις ημέρες μας, με την ανατροπή της φιλορωσικής κυβέρνησης της Ουκρανίας του Βίκτορ Γιανούκοβιτς το 2014, τον εξοπλισμό και υποστήριξη νεοναζιστικών οργανώσεων, την ανακήρυξη των αυτόνομων περιοχών του Λουγκάνσκ και Ντονετσκ, την εισβολή του στρατού της Ρωσικής Ομοσπονδίας στην Κριμαία, τον εξοπλισμό του ουκρανικού στρατού και τη σφαγή 14.000 ουκρανών πολιτών-φίλα προσκεϊμένων στη Ρωσική Ομοσπονδία. Στις 24/2/2022 η Ρωσική Ομοσπονδία εισέβαλε στην Ουκρανία και ο πόλεμος συνεχίζεται μέχρι σήμερα, έχοντας αποκτήσει παγκόσμιες διαστάσεις, σε εμπορικό και (έμμεσα προς το παρόν) στρατιωτικό επίπεδο.

⁶⁰ Το ζήτημα είναι γνωστό ήδη από την «Ιστορία» του Θουκυδίδη, ενώ έχει επαναληφθεί και στο Περί Πολέμου του Κλαούζεβιτς (1999)

⁶¹ Ενδεικτικά το κόστος του πολέμου «κατά της τρομοκρατίας» (2001-2021) ανήλθε αναφορικά με τις ΗΠΑ σε 8 τρις δολάρια και προκάλεσε σχεδόν 1 εκατομμύριο νεκρούς.

Haltiwanger John (2021) “America’s 20-year war on terror has killed up to 929,000 people and cost over \$8 trillion: report” Insider 1/9/2021, insider.com διαθέσιμο στο <https://www.businessinsider.com/us-war-on-terror-deaths-cost-over-8-trillion-report-2021-8?r=US&IR=T> ημ.πρόσβασης 4/6/2022

⁶² Ενδεικτικά: η Παρισινή Κομμούνα ξεπήδησε κατά τη διάρκεια του γαλλοπρωσικού Πολέμου (1871), η Επανάσταση των Σοβιέτ (1917) ξέσπασε με το τέλος του ΑΠΠ, ενώ στη Γερμανία το 1918 ξέσπασε η Γερμανική ή Νοεμβριανή Επανάσταση

⁶³ Στις ΗΠΑ και στην Ευρώπη

⁶⁴ M. Hersh Seymour (1999) “The Intelligence Gap” *The New Yorker*, 28/11/1999 διαθέσιμο στο [The Intelligence Gap | The New Yorker](https://www.newyorker.com) ημ.πρόσβασης 4/6/2022

⁶⁵ “Metadata monitoring more intrusive than eavesdropping - Snowden and Greenwald” *Russia Today* (rt.com) 6/4/2014, διαθέσιμο στο <https://www.rt.com/news/snowden-greenwald-metadata-amnesty-757/> ημ.πρόσβασης 4/6/2022

⁶⁶ Greenwald Glenn (2013) “NSA collecting phone records of millions of Verizon customers dail” *The Guardian*, 6/6/2013, διαθέσιμο στο <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> ημ.πρόσβασης 4/6/2022

⁶⁷ (2013) “NSA slides explain the PRISM data-collection program” *The Washington Post*, 6/6/2013, διαθέσιμο στο <https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/> ημ.πρόσβασης 4/6/2022

Βλ.επίσης Greenwald Glenn και MacAskill Ewen “NSA Prism program taps in to user data of Apple, Google and others” *The Guardian*, 7/6/2013 διαθέσιμο στο [NSA Prism program taps in to user data of Apple, Google and others | US national security | The Guardian](https://www.theguardian.com/us-news/2013/jun/07/nsa-prism-program-taps-in-to-user-data-of-apple-google-and-others) ημ.πρόσβασης 4/6/2022

⁶⁸ Τα προγράμματα απομόνωσης ξεχωρίζουν ένα πρόσωπο, μια ομάδα, μια διαδικτυακή τοποθεσία ή συσκευή για εξειδικευμένη παρακολούθηση.

-
- ⁶⁹ Hu Margaret (2015) *“Taxonomy of the Snowden Disclosures Margaret Hu”* Washington and Lee University School of Law, Washington and Lee Law Review, vol.72, 2015, διαθέσιμο στο <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4477&context=wlulr> ημ.πρόσβασης 4/6/2022
- ⁷⁰ Ferran Lee (2014) *“Ex-NSA Chief: ‘We Kill People Based on Metadata’* ABC News, 12/5/2014, διαθέσιμο στο <https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata> Βλ. επίσης The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA (2014) βιντεοακουστικό υλικό διαθέσιμο στο https://m.youtube.com/watch?v=kV2HDM86XgI&feature=emb_title βλ. 18.04
- ⁷¹ «Δεν υπάρχει σαφής διάκριση μεταξύ μεταδεδομένων και περιεχομένου. Είναι περισσότερο μια συνέχεια» Ackerman Spencer (2014) *“NSA review panel casts doubt on bulk data collection claims”*, The Guardian, 14/1/2014, διαθέσιμο στο <https://www.theguardian.com/world/2014/jan/14/nsa-review-panel-senate-phone-data-terrorism> ημ.πρόσβασης 4/6/2022
- ⁷² Parker Clifton (2014) *“Stanford students show that phone record surveillance can yield vast amounts of information”* Stanford University (<https://www.stanford.edu/>) 12/3/2014 διαθέσιμο στο <https://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html> ημ.πρόσβασης 4/6/2022
- ⁷³ Mutchler Patrick και Mayer Jonathan (2014) *“MetaPhone: The Sensitivity of Telephone Metadata”* <http://webpolicy.org/> διαθέσιμο στο [MetaPhone: The Sensitivity of Telephone Metadata | Web Policy](http://webpolicy.org/meta-phone-the-sensitivity-of-telephone-metadata/) ημ.πρόσβασης 4/6/2022
- ⁷⁴ Mayer Jonathan και Mutchler Patrick και Mitchell John C. (2016) *“Evaluating the privacy properties of telephone metadata”* Proceedings of the National Academy of Sciences volume 113, pages 5536-5541, 2016, 10.1073/pnas.1508081113 διαθέσιμο στο <https://www.pnas.org/doi/full/10.1073/pnas.1508081113#sec-1> ημ.πρόσβασης 4/6/2022
- ⁷⁵ 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 στο <https://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf> ημ.πρόσβασης 4/6/2022
- ⁷⁶ Τα παραθέματα αποτελούν στο μεγαλύτερο βαθμό αποδόσεις τμημάτων της κατάθεσης
- ⁷⁷ Και χρησιμοποιώντας αποκλειστικά επικοινωνία μέσω διαδικτύου με τη χρήση εργαλείων που προσφέρουν ένα επίπεδο προστασίας της ιδιωτικότητας
- ⁷⁸ Και τα οποία αποθηκεύονται στις κεφαλίδες (headers) των emails
- ⁷⁹ Δηλ. του μέτρου αβεβαιότητας, βλ. περισσότερα για το ζήτημα Shannon C.E. (1948) *A Mathematical Theory of Communication* The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, Ιούλιος Οκτώβριος 1948, διαθέσιμο στο [shannon1948.dvi \(harvard.edu\)](http://www.harvard.edu/shannon1948.dvi) ημ.πρόσβασης 4/6/2022
- ⁸⁰ Ο λόγος που είναι εφικτή η σημασιολογική ανάλυση των μεταδεδομένων επικοινωνίας έτσι ώστε να παράγει τόσο ακριβή αποτελέσματα, εκφεύγει της παρούσας.
- ⁸¹ Clayton Newell Bryce και Tennis Joseph T. (2014) *Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs*, n iConference 2014 Proceedings (p. 345–355) doi 10.9776/14109, διαθέσιμο στο https://www.ideals.illinois.edu/bitstream/handle/2142/47299/109_ready.pdf?sequence=2 σελ.347
- ⁸² Αύξηση που συνεχίζεται βλ. ενδεικτικά για τα έτη από 2010-2025. *“Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025”* Statista Research Department, 23/5/2022, διαθέσιμο στο [Total data volume worldwide 2010-2025 | Statista](https://www.statista.com/statistics/1101111/volume-of-data-information-created-captured-copied-and-consumed-worldwide-from-2010-to-2025/) ημ.πρόσβασης 4/6/2022
- ⁸³ Διάσημος πια είναι ο Νόμος του Moore (1965) ο οποίος ισχυρίστηκε ότι ο αριθμός των τρανζίστορ σε ένα πυκνό ολοκληρωμένο κύκλωμα θα διπλασιάζεται κάθε χρόνο για τουλάχιστον μία δεκαετία από τότε. Στη συνέχεια αναθεώρησε την πρόβλεψή του, ορίζοντας το διάστημα που απαιτείται για τον διπλασιασμό των τρανζίστορ ενός πυκνού ολοκληρωμένου κυκλώματος στα δύο έτη. Βλ.ενδεικτικά 1965: *“MOORE’S LAW” PREDICTS THE FUTURE OF INTEGRATED CIRCUITS*, Computer History Museum (<https://computerhistory.org/>), διαθέσιμο στο [1965: “Moore’s Law” Predicts the Future of Integrated Circuits | The Silicon Engine | Computer History Museum](https://computerhistory.org/1965-moores-law-predicts-the-future-of-integrated-circuits/) ημ.πρόσβασης 4/6/2022
- ⁸⁴ Ενδεικτικά: Model fitting, Exploratory Data Analysis κλπ
- ⁸⁵ Όσο και με μη διαφανείς τρόπους από τους παρόχους διαδικτυακών υπηρεσιών
- ⁸⁶ Με τη μέθοδο του τριγωνισμού (βάσει της απόστασης από τους σταθμούς βάσης), με τη χρήση συστήματος GPS, μέσω του Cell-id, μέσω της ip address κ.α.

-
- ⁸⁷ Ιδίως κατά τον (κατ' αρχήν αναγκαία) αφηρημένο τρόπο με τον οποίο αναφέρεται η νομοθεσία στη γεωγραφική θέση
- ⁸⁸ Που είναι και η πλέον συχνά απαντώμενη περίπτωση
- ⁸⁹ "The way we move and the behaviour is so unique that four points are enough to identify 95% of people, Jason Palmer (2013) "Mobile location data 'present anonymity risk", BBC, 25/3/2013, διαθέσιμο στο <https://www.bbc.com/news/science-environment-21923360> ημ.πρόσβασης 4/6/2022
- ⁹⁰ [Location data is the most valuable communications metadata that mobile phones provide. It can be used to identify the user, where the user is and what the user is doing.] Susan Landau (2020) σελ.13
- ⁹¹ και κατ' επέκταση ο χρήστης
- ⁹² Hristo Bojinov και Michalevsky Yan και Nakibly Gabi και Boneh Dan (2014) "Mobile Device Identification via Sensor Fingerprinting," διαθέσιμο στο [1408.1416.pdf \(arxiv.org\)](https://arxiv.org/abs/1408.1416) ημ.πρόσβασης 4/6/2022
- ⁹³ Francesco Calabrese και Laura Ferrari και Vincent Blondel (2014) *Urban Sensing Using Mobile Phone Network Data: A Survey of Research*. ACM Computing Surveys. 47. 1-20. doi 10.1145/2655691 Διαθέσιμο στο <https://dl.acm.org/doi/abs/10.1145/2655691> Σελ.14-16
- ⁹⁴ Vincent D Blondel και Decuyper Adeline και Krings Gautier (2015) *A survey of results on mobile phone datasets analysis*, EPJ Data Science (2015) 4:10 DOI 10.1140/epjds/s13688-015-0046-0, διαθέσιμο στο [A survey of results on mobile phone datasets analysis \(springeropen.com\)](https://www.springeropen.com/article/10.1140/epjds/s13688-015-0046-0) ημ.πρόσβασης 4/6/2022
- ⁹⁵ Andrew Tatem και Qui Youliang και Smith David L. και Sabot Oliver και Ali Abdullah S. και Moonen Bruno (2009), "The use of mobile phone data for the estimation of the travel patterns and imported Plasmodium falciparum rates among Zanzibar residents," Malaria Journal, Vol. 8, Article number: 287 (2009) διαθέσιμο στο [Categorizing Uses of Communications Metadata: Systematizing Knowledge and Presenting a Path for Privacy \(acm.org\)](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2711000/)
- ⁹⁶ Corrina Cortes και Pregibon Daryl και Volinsky Chris, "Communities of Interest," IDA '01: Proceedings of the 4th International Conference on Advances in Intelligent Data Analysis, Σεπτέμβριος 2001, pp. 105-114 διαθέσιμο στο <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.23.8792&rep=rep1&type=pdf>
- ⁹⁷ Rowe Ryan και German Creamer και Shlomo Heshkop και Stolfo Salvatore, "Automated Social Hierarchy Detection through Email Network Analysis" Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 Workshop on Web Mining Social Network Analysis, pp. 109-117, διαθέσιμο στο <https://academiccommons.columbia.edu/doi/10.7916/D85T3T9Z/download> ημ.πρόσβασης 4/6/2022
- ⁹⁸ Eagle Nathan και Macy Michael και Claxton Rob. (2010). *Network Diversity and Economic Development*. Science (New York, N.Y.). 328. 1029-31. 10.1126/science.1186605. διαθέσιμο στο [Network Diversity and Economic Development \(researchgate.net\)](https://www.researchgate.net/publication/312211110)
- ⁹⁹ Blondel Vincent et.al (2015) *A survey of results on mobile phone datasets analysis*.
- ¹⁰⁰ Βλ. Blondel Vincent et.al (2015) *A survey of results on mobile phone datasets analysis*. σελ.15
- ¹⁰¹ Βλ. Blondel Vincent et.al (2015) *A survey of results on mobile phone datasets analysis*. σελ.18
- ¹⁰² Βλ. Blondel Vincent et.al (2015) *A survey of results on mobile phone datasets analysis*. σελ.33
- ¹⁰³ Ferrara Emilio και De Meo Pasquale και Catanese Salvatore και Fiumara Giacomo (2014), "Detecting criminal organizations in mobile phone networks" διαθέσιμο στο [1404.1295.pdf \(arxiv.org\)](https://arxiv.org/abs/1404.1295) ημ.πρόσβασης 4/6/2022
- ¹⁰⁴ Tadayoshi Kohno και Broido Andre και Claffy K.C.(2005), "Remote physical device fingerprinting" IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 2 (2005). Διαθέσιμο στο https://www.caida.org/catalog/papers/2005_fingerprinting/KohnoBroidoClaffy05-devicefingerprinting.pdf ημ.πρόσβασης 4/6/2022
- ¹⁰⁵ Karagiannis Thomas και Papagiannaka Konstantina και Faloutsos Michalis (2005), "BLINC: Multilevel Traffic Classification in the Dark", SIGCOMM'05, 22-26 Αυγούστου 2005, διαθέσιμο στο <http://www.cs.ucr.edu/~michalis/PAPERS/camera-BLINC.pdf> ημ.πρόσβασης 4/6/2022
- ¹⁰⁶ Wright Charles V. και Ballard Lucas και Monroe Fabian και Masso Gerald M.(2007) "Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?," Sixteenth USENIX Security Symposium, Αύγουστος 2007 διαθέσιμο στο https://www.usenix.org/legacy/events/sec07/tech/full_papers/wright/wright.pdf ημ.πρόσβασης 4/6/2022
- ¹⁰⁷ Chairunnunda Prima και Nam Pham και Urs Hengartner, "Privacy: Gone with the Typing! Identifying Web Users by their Typing Patterns," PETS 2011 , διαθέσιμο στο [cs858pets.dvi \(petsymposium.org\)](https://www.usenix.org/legacy/events/sec07/tech/full_papers/wright/wright.pdf) ημ.πρόσβασης 4/6/2022

-
- ¹⁰⁸ Rahat Masood και Zi Hao Zhao Benjamin και Jameel Asghar Hassan και Ali Kaafar Mohamed, “Touch and You’re Trapp(ck)ed: Quantifying the Uniqueness of Touch Gestures for Tracking” PETS 2018. Διαθέσιμο στο <https://petsymposium.org/2018/files/papers/issue2/popets-2018-0016.pdf>
- ¹⁰⁹ Zi Chu και Gianvecchio Steven και Wang Haining και Jajodia Sushil (2010) “Who is Tweeting on Twitter: Human, Bot, or Cyborg?,” Annual Computer Security Applications Conference (ACSAC) Δεκέμβριος 2010, διαθέσιμο στο <https://www.eecis.udel.edu/~hnw/paper/acsac10.pdf> ημ.πρόσβασης 4/6/2022
- ¹¹⁰ Huaxin Li και Xu Zheyu και Zhu Haojin και Ma Di και Li Shuan και Xing Kai (2016), “Demographics Inference Through Wi-Fi Network Traffic Analysis” INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications διαθέσιμο στο <https://nsec.sjtu.edu.cn/publications/2016/Demographics.pdf> ημ.πρόσβασης 4/6/2022
- ¹¹¹ Noah Apthorpe και Yuxing Huang Danny και Reisman Dillon και Narayanan Arvind και Feamster Nick (2019), “Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping”, Proceedings on Privacy Enhancing Technologies, διαθέσιμο στο <https://arxiv.org/pdf/1812.00955.pdf> ημ.πρόσβασης 4/6/2022
- ¹¹² De Montjoye Yves-Alexandre και Quoidbach Jordi και Robic Florent και Pentland Alex (Sandy), “Predicting Personality Using Novel Mobile Phone-Based Metrics” διαθέσιμο στο [Blank1.pdf\(mit.edu\)](Blank1.pdf(mit.edu)) ημ.πρόσβασης 4/6/2022
- ¹¹³ Conley Chris (2014) “Metadata: Piecing Together a Privacy Solution” διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573962 ημ.πρόσβασης 4/6/2022 σελ.6 και παραπομπές 12,15
- ¹¹⁴ In fact, mining metadata can not only expose sensitive information about the past, it can even allow an observer to predict future actions. For example, research has demonstrated that an individual’s future location and activities can be predicted by looking for patterns in his friends and associates’ location history. A security expert also warned that identifying phone calls from key executives at a company to or from a competitor, an attorney, or a brokerage can reveal the potential for a corporate takeover before any public announcement is made”. Από Conley Chris (2014) Metadata: Piecing Together a Privacy Solution, ACLU of California, διαθέσιμο στο <https://www.aclunc.org/publications/metadata-piecing-together-privacy-solution> ημ.πρόσβασης 4/6/2022
- ¹¹⁵ Αναφορικά με τις μηχανές αναζήτησης, βλ. Battelle John (2003), “The Database of Intentions”, διαθέσιμο στο https://battellemedia.com/archives/2003/11/the_database_of_intentions ημ.πρόσβασης 4/6/2022
- ¹¹⁶ Brownlee Lisa (2015) “The \$11 Trillion Internet Of Things, Big Data And Pattern Of Life (POL) Analytics” διαθέσιμο στο <https://www.forbes.com/sites/lisabrownlee/2015/07/10/the-11-trillion-internet-of-things-big-data-and-pattern-of-life-pol-analytics/> ημ.πρόσβασης 4/6/2022
- ¹¹⁷ Ίδιως και περισσότερα αυτά που παράγονται από ip-based επικοινωνίες
- ¹¹⁸ Zhao Ziliang και Shaw Shih-Lung και Xu Yang και Lu Feng και Chen Jie και Yin Ling (2016) “Understanding the bias of call detail records in human mobility research”, International Journal of Geographical Information Science, διαθέσιμο στο DOI: 10.1080/13658816.2015.1137298 ημ.πρόσβασης 4/6/2022 σελ.22
- ¹¹⁹ Ωστόσο κάποιες κατηγορίες μεταδεδομένων επικοινωνίας δε δημιουργούνται απευθείας από το χρήστη, αλλά είναι δυνατό να δημιουργηθούν από το ίδιο δίκτυο κατά τη διαδικασία μεταφοράς (transit) των πακέτων πληροφοριών, για κατ’ αρχήν τεχνικούς λόγους πχ για την εύρεση της πηγής και του προορισμού των πακέτων, τη μέτρηση της ταχύτητας κλπ. Ωστόσο, η αιτία που προκαλείται η αλυσίδα αυτή γεγονότων, εντοπίζεται σε μια ενέργεια του χρήστη.
- ¹²⁰ Ακόμα και κατά τη διάρκεια του ύπνου, το γεγονός της μη ύπαρξης επικοινωνιακών γεγονότων, έχει ποικίλες διαστάσεις.
- ¹²¹ Pasquinelli Matteo (2015) “Anomaly Detection: The Mathematization of the Abnormal in the Metadata Society”, διαθέσιμο στο <https://www.academia.edu/2573962/Anomaly-Detection-The-Mathematization-of-the-Abnormal-in-the-Metadata-Society-Matteo-Pasquinelli-Academia.edu> ημ. πρόσβασης 4/6/2022 σελ.6
- ¹²² Κατ’ ακρίβεια πρόκειται για δημιουργία μοτίβων, αλλά ακολουθείται ο χρησιμοποιούμενος επιστημονικός όρος
- ¹²³ Διαφεύγει της παρούσας, ωστόσο πρέπει να αναφερθεί ότι το είδος της συγκεκριμένης ανάλυσης παρότι παρίσταται αντικειμενικό, δε στερείται ούτε συγκεκριμένων ιδεολογικών επιρροών, ούτε αποτυχιών.
- ¹²⁴ Ωστόσο, το απόρρητο της επικοινωνίας αφορά τόσο τη μεμονωμένη επικοινωνία όσο και το σύνολο των επικοινωνιών ενός προσώπου ή μιας ομάδας προσώπων.

¹²⁵ *Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble..* δικαστική απόφαση U.S. v. Maynard διαθέσιμη στο <https://casetext.com/case/united-states-v-maynard-5>

¹²⁶ Αν και δεν είναι σπάνιες οι περιπτώσεις στις οποίες ακόμα και μικρότερος όγκος μεταδεδωμένων επικοινωνιών, μπορεί να αποκαλύψει το περιεχόμενό της. Η σκέψη αυτή έχει γίνει αποδεκτή και στη νομολογία του ΔΕΕ βλ. κατωτέρω.

¹²⁷ Βλ.αφ.7 παρ.7 ΠΔ 47/2005

¹²⁸ Βλ. κατωτέρω

¹²⁹ Βλ. ενδεικτικά Αιτιολογική Σκέψη 47, 51, 60,71, 76, 90 και αρ.24 παρ.1, αρ.25 παρ.1, αρ.32 παρ.1, αρ.35 παρ.1 ΓΚΠΔ 679/2016/ΕΕ

¹³⁰ Βλ. ενδεικτικά τις Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679. WP 248 αναθ. 01, έγγραφο το οποίο έχει υιοθετήσει και το ΕΣΠΔ.

¹³¹ Η οποία δεν έχει ερμηνευθεί ακόμα

¹³² Ακόμα και αν γίνεται εντός του πλαισίου της νομοθεσίας

¹³³ Single point of failure ή SPOF: συνιστά ένα λάθος κατά το σχεδιασμό ενός συστήματος και αφορά την ύπαρξη ενός σημείου το οποίο εφόσον αποτύχει στη λειτουργία του, θέτει σε κίνδυνο τη λειτουργία ολόκληρου του συστήματος.

¹³⁴ Η παρατήρηση αυτή αφορά τα αναφερόμενα δικαιώματα και όχι το τεχνικό σκέλος της προστασίας που ακολουθείται από τους παρόχους.

¹³⁵ Είναι προφανές ότι υφίστανται και άλλοι τρόποι προσβολής του επικοινωνιακού απορρήτου, ωστόσο αυτό που περιγράφεται αφορά αποκλειστικά το ζήτημα των μεταδεδωμένων επικοινωνιών που συλλέγονται από τους παρόχους.

¹³⁶ Δεν υιοθετείται δηλαδή μια διασπορά κινδύνου, προκειμένου αυτός να απομειωθεί.

¹³⁷ Ανάλογο σκεπτικό έχει διατυπώσει και το ΕΔΔΑ στην υπόθεση Big Brother Watch and others V. the UK βλ. σχετικά Γρ. Τσόλιας (2021) *Η νόμιμη (μαζική) παρακολούθηση των ηλεκτρονικών επικοινωνιών υπό το πρίσμα της νομολογίας του ΕΔΔΑ- Σχόλιο στην από 25.5.2021 απόφαση Big Brother Watch and others V. the UK*. ΔΙΜΕΕ 3/2021, σελ.393-394.

¹³⁸ Κυρώθηκε στην εθνική έννομη τάξη με το ν.2462/1997.

¹³⁹ Βλ.αρ.6 ΣΕΕ

¹⁴⁰ Η οποία καταργήθηκε από το 2018 με τον 679/2016/ΕΕ Γενικό Κανονισμό Προστασίας Δεδομένων

¹⁴¹ Οι οποίες μνημονεύονται ρητά στο σημείο 10 του Προοιμίου της Οδηγίας

¹⁴² Ευρωπαϊκό Συμβούλιο (2005) «*Ενίσχυση της Ελευθερίας, της Ασφάλειας και της Δικαιοσύνης στην Ευρωπαϊκή Ένωση*» διαθέσιμο στο [https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52005XG0303\(01\)&from=EL](https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52005XG0303(01)&from=EL) βλ. σημείο 2.2.

¹⁴³ ΟΔΗΓΙΑ 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ

¹⁴⁴ Σωτηρόπουλος Β. και Ταλίδου Ζ. (2006) «*Η προληπτική διατήρηση των τηλεπικοινωνιακών δεδομένων για σκοπούς καταπολέμησης του εγκλήματος (Οδηγία 2006/24/ΕΚ)*», ΔΙΜΕΕ, 2/2006, σελ. 181

¹⁴⁵ Βλ. κατωτέρω

¹⁴⁶ Εξαιρέσεις σημειώνονται μόνο σε σχέση με τα μεταδεδωμένα που αφορούν την περιήγηση στο διαδίκτυο, με τη χρήση Virtual Private Network (VPN) το οποίο αποκρύπτει τα δεδομένα κίνησης (traffic data) από τον πάροχο υπηρεσιών διαδικτύου, μέσω κρυπτογράφησης ή με τη χρήση ενός δικτύου Tor, κατά την οποία αποκρύπτεται η διεύθυνση ip και κρυπτογραφείται η κίνηση στο διαδίκτυο καθώς αυτή ανακατευθύνεται μέσω ενδιάμεσων servers προς τη σελίδα που επιθυμεί ο χρήστης. Άλλες υπηρεσίες όπως ο Tor Browser προσφέρουν επιπλέον τη δυνατότητα απόκρυψης του ιστορικού περιήγησης, καθιστώντας το χρήστη ανώνυμο, σε σημαντικό αλλά όχι απόλυτο βαθμό. Η χρήση vpn περιλαμβάνει σύνδεση σε ένα πάροχο vpn server (συγκεντρωτική προσέγγιση) -ο οποίος πάροχος μπορεί να έχει πρόσβαση στην κίνηση του χρήστη- και κρυπτογράφηση σε ένα μόνο επίπεδο.

Η χρήση του περιλαμβάνει κρυπτογράφηση σε πολλαπλά επίπεδα με τη χρήση πολλών και άγνωστων μεταξύ τους servers (αποκεντρωμένη προσέγγιση) και διαχωρισμό της ταυτότητας ενός χρήστη (της διεύθυνσης ip) από την κίνησή του στο διαδίκτυο.

¹⁴⁷ Για παράδειγμα, κάποιες κατηγορίες μεταδεδομένων οι οποίες εξαντλούν το σκοπό ύπαρξής τους (σε σχέση με την πραγματοποίηση της επικοινωνίας και τη χρέωση) λίγο μετά την ολοκλήρωση μιας επικοινωνίας, θα μπορούσαν να διαγράφονται αυτόματα ή να υφίσταται σε κάθε περίπτωση, ένας μικρότερος χρόνος διατήρησης, έτσι ώστε να μειωθούν οι κίνδυνοι προσβολής της ιδιωτικότητας. Θα μπορούσαν επίσης να χρησιμοποιούνται τεχνικές αλλοίωσης μοναδικών αναγνωριστικών μιας συσκευής ή των traffic data προκειμένου να μην αναγνωρίζεται διαρκώς ο χρήστης και να μην παρακολουθείται διαρκώς η κίνησή του στο διαδίκτυο.

¹⁴⁸ Στη χώρα μας δε, υπό τις προβληματικές διαδικασίες που ακολουθούνται για την άρση του απορρήτου βλ. κατωτέρω

¹⁴⁹ *The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone.* Απόφαση ΕΔΔΑ Malone V. United Kingdom, παρ.84

¹⁵⁰ Σημειώνεται ότι η χρησιμοποιούμενη συσκευή καταγραφής (metering) κατέγραφε επίσης το χρόνο και της διάρκειας της επικοινωνίας.

¹⁵¹ Παρ.72

¹⁵² Παρ. 44

¹⁵³ Συνεκδικαζόμενες υποθέσεις C-293/2012 και C-594/2012

¹⁵⁴ 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 δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/EK

¹⁵⁵ Βλ. Μπαντή-Μαρκούτη Βικτωρία (2015) «Μεταδεδομένα και Ηλεκτρονικές Επικοινωνίες: Η κατάργηση της Οδηγίας 2006/24 και η USA Freedom Act 2015» ΔΙΜΕΕ, 3/2015 σελ. 338, 341

¹⁵⁶ Συνεκδικασθείσες υποθέσεις C-2013/2015 και C-698/2015)

¹⁵⁷ Υπόθεση C-746/18

¹⁵⁸ Σκέψη υπ' αριθμ 30

¹⁵⁹ Σκέψη υπ' αριθμ 33

¹⁶⁰ Σκέψη υπ' αριθμ 39

¹⁶¹ Σκέψη υπ' αριθμ 40

¹⁶² πέραν της ύπαρξης λόγω καταπολέμησης βαριάς εγκληματικότητας και σοβαρών απειλών της δημόσιας ασφάλειας

¹⁶³ Ψήφισμα της 25ης Νοεμβρίου 2019 της Θ' Αναθεωρητικής Βουλής των Ελλήνων, που δημοσιεύθηκε στο Φ.Ε.Κ. 187/Α`/28.11.2019

¹⁶⁴ Ν. Παπαδόπουλος (2008) *Προστασία του Απορρήτου της Επικοινωνίας*, Αθήνα, Νομ. Βιβλιοθήκη σελ.120

¹⁶⁵ Ν. Παπαδόπουλος (2008) *Προστασία του Απορρήτου της Επικοινωνίας*, Αθήνα, Νομ. Βιβλιοθήκη σελ.170

¹⁶⁶ Πχ χρήση κρυπτογραφίας

¹⁶⁷ Εν προκειμένω: καλών, καλούμενος, χρόνος, τόπος (για τις τηλεφωνικές επικοινωνίες), αποστολέας, παραλήπτης, διεύθυνση, χρόνος (για τις επιστολές)

¹⁶⁸ Βλ. σχετικά Γρ. Τσόλιας (2009) Σημ. στην ΓνωμΕισΑπ 12/2009, ΔΙΜΕΕ 3/2009, σελ.396

¹⁶⁹ Σχετικά με αυτό βλ. ενδεικτικά Ν. Παπαδόπουλος (2008) *Προστασία του Απορρήτου της Επικοινωνίας*, Αθήνα, Νομ. Βιβλιοθήκη σελ.195 κ.επ.

¹⁷⁰ Εκτός και αν τα μέρη δεν επιθυμούσαν κατά αδιαμφισβήτητο τρόπο και συνθήκες να κρατήσουν την επικοινωνία απόρρητη

¹⁷¹ Ενδεικτικά Το απόρρητο της επικοινωνίας: Τσακυράκης Σ. (1993) «Απόλυτα απαραβίαστο ή ευχή της έννομης τάξης;» ΝοΒ 1993 σελ.998 και του ίδιου «Το απόρρητο της τηλεφωνικής επικοινωνίας – Η συνταγματική προστασία και η εφαρμογή της από τον ποινικό νομοθέτη και τα δικαστήρια» ΝοΒ 1995 σελ.512

¹⁷² Βλ. σχετικά Γρ. Τσόλιας (2009) σελ.396

¹⁷³ Αν και όχι νομοτεχνικά άρτιο

¹⁷⁴ Ωστόσο βάσει του εδαφίου β' της παρ.10 του αρ.5, ο κανόνας αυτός κάμπτεται χωρίς ωστόσο να παρέχονται εγγυήσεις αναλογικότητας. Δηλαδή ορίζεται ότι μπορεί να επιτραπεί να «χρησιμοποιηθούν και να ληφθούν υπόψη τα παραπάνω στοιχεία, αν χρησιμεύουν για τη διακρίβωση άλλου ιδιαίτερου σοβαρού εγκλήματος από αυτά που αναφέρονται στην παρ. 1 του άρθρου 4 ...». Δεν επαναλαμβάνεται δηλαδή η διαδικαστική εγγύηση του αρ.4 παρ.2 η οποία προβλέπει ότι: Η άρση στις περιπτώσεις αυτές είναι επιτρεπτή μόνο αν αιτιολογημένα το αρμόδιο δικαστικό συμβούλιο διαπιστώσει ότι η διερεύνηση της υπόθεσης ή η εξακρίβωση του τόπου διαμονής του κατηγορουμένου είναι αδύνατη ή ουσιωδώς δυσχερής χωρίς αυτήν.

¹⁷⁵ Οι οποίες είναι εφικτό να υπερβούν κατά πολύ τόσο το υπό έρευνα πρόσωπο όσο ακόμα και τις υπό έρευνες πράξεις του

¹⁷⁶ Σκοπός του νόμου είναι η ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας προπληρωμένου χρόνου ομιλίας, συνδρομητών με συμβόλαιο, ή άλλης μορφής κινητής τηλεπικοινωνίας, για λόγους εθνικής ασφάλειας και για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων ¹⁷⁷. Τα στοιχεία ταυτότητας του συνδρομητή μαζί με τα διαθέσιμα στοιχεία ταυτοποίησης του κινητού τερματικού τηρούνται από τον πάροχο υπό τους όρους της κείμενης νομοθεσίας περί προστασίας δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών. Απαγορεύεται η καταγραφή οποιωνδήποτε άλλων στοιχείων ταυτότητας του συνδρομητή, πέραν αυτών που ορίζονται περιοριστικά στον παρόντα νόμο.

¹⁷⁸ 2. Η πρόσβαση των δικτυικών αρχών στα τηρούμενα από τον πάροχο στοιχεία ταυτότητας συνδρομητή και ταυτοποίησης κινητού τερματικού επιτρέπεται υπό τους όρους του άρθρου 4 του ν. 2225/1994 (ΦΕΚ 121 Α), όπως αντικαταστάθηκε με το άρθρο 12 του ν. 3115/2003 (ΦΕΚ 47 Α) και του π.δ. 47/2005 (ΦΕΚ 64 Α).

¹⁷⁹ Βλ. σχετικά Τσόλιας Γρ. (2009) σελ.397

¹⁸⁰ Αρ.4 παρ.1, αρ.7 παρ.1 και 2 και αρ.8 παρ.9 περίπτωση β' ΠΔ 47/2005

¹⁸¹ Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997. ΦΕΚ Α 133/28.06.2006

¹⁸² Στο άρθρο 4 περιέχονται ρυθμίσεις για τη διασφάλιση του απορρήτου των επικοινωνιών, το οποίο επεκτείνεται ρητά και στα εξωτερικά στοιχεία της επικοινωνίας, τα δεδομένα κίνησης και θέσης. Σελ.1 Αιτιολογικής Έκθεσης στο σχέδιο νόμου Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997. Διαθέσιμη στο [p-dedom-eis \(hellenicparliament.gr\)](http://p-dedom-eis(hellenicparliament.gr))

¹⁸³ Δεδομένα κίνησης: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία.

¹⁸⁴ Ο όρος δεδομένα κίνησης αποδίδει στην ελληνική τον αγγλικό όρο “traffic data”

¹⁸⁵ Δεδομένα θέσης»: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μια διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών.»

¹⁸⁶ Από αυτά που παράγονται ήδη

¹⁸⁷ Δεδομένα κίνησης: τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία.

¹⁸⁸ Ο όρος δεδομένα κίνησης αποδίδει στην ελληνική τον αγγλικό όρο “traffic data”

¹⁸⁹ Δεδομένα θέσης»: τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μια διαθέσιμη στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.»

¹⁹⁰ Με τον νόμο αυτό ενσωματώθηκε 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 δημοσίων δικτύων επικοινωνιών, η οποία όμως κηρύχθηκε ανίσχυρη με την απόφαση ΔΕΕ Digital Rights Ireland της 8/4/2014 (Υποθέσεις C-293/2012 και C-594/2012).

¹⁹¹ όσο και των δεδομένων προσωπικού χαρακτήρα

¹⁹² Υπό την επιφύλαξη ότι η καταστροφή γίνεται με τεχνικές που δεν επιτρέπουν την ανάκτηση των δεδομένων αυτών

¹⁹³ [...]network data contains a variety of data types that make application of well-known anonymization methods difficult, if not impossible. Some fields in network data, like IP addresses, have a highly complex hierarchical ordering structure that often needs to be preserved after anonymization. Moreover, the relationship among different fields in network data is semantically rich, which means that the values taken by certain fields is dependent on their context with respect to other values within the data – both within the same row and within other rows – and these dependencies must be maintained in order for the data to be semantically meaningful.

The Challenges of Effectively Anonymizing Network Data. Scott E. Coull, Fabian Monrose, Michael K. Reiter, Michael Bailey

http://mdbailey.ece.illinois.edu/publications/catch09_anonymizing_final.pdf

¹⁹⁴ Montjoye Yves-Alexandre και Radaelli Laura και Singh Vivek και Pentland, Alex. (2015). “Unique in the shopping mall: On the reidentifiability of credit card metadata”. *Science* (New York, N.Y.) διαθέσιμο στο <https://www.science.org/doi/10.1126/science.1256297> ημ.πρόσβασης 4/6/2022

¹⁹⁵ Narayanan A. και Shmatikov V. (2008), “Robust de-anonymization of large sparse datasets” 2008 IEEE Symposium on Security and Privacy, (IEEE, New York, 2008) pp. 111-125 διαθέσιμο στο shmat_oak08netflix.pdf (utexas.edu) ημ.πρόσβασης 4/6/2022

¹⁹⁶ Συμπεριλαμβανομένου του χρόνου εντός του οποίου μπορεί να αμφισβητηθεί ο λογαριασμός

¹⁹⁷ Ταυτοποίηση χρήστη, αποκάλυψη δραστηριοτήτων του κλπ βλ. ανωτέρω

¹⁹⁸ Οι οποίοι διαχρονικά δεν υφίστανται

¹⁹⁹ Βλ. σελ.36 της υπ’ αριθμ 4/2022 ΑΠΔΠΧ. Ο πάροχος διατηρούσε το μυστικό κλειδί (salt) για 3 μήνες, έχοντας τη δυνατότητα να επαναταυτοποιήσει τα δεδομένα κίνησης και θέσης.

²⁰⁰ Βλ. υποσημείωση 12 της υπ’ αριθμ 4/2022 ΑΠΔΠΧ

²⁰¹ Αλλά δυστυχώς χωρίς τεχνικό έλεγχο από την πλευρά της ΑΠΔΠΧ, ο οποίος ίσως αναδείκνυε επιπλέον ευρήματα

²⁰² Και ο μεγαλύτερος βλ. Ηγουμενίδη Τέτη (2022) «Η μάχη για τα μερίδια στην αγορά τηλεφωνίας» Ναυτεμπορική 4/2/2022 διαθέσιμο στο <https://m.naftemporiki.gr/story/1828782/eett-i-ekseliksi-ton-meridion-agoras-ton-otevodafonewindkainova> ημ.πρόσβασης 4/6/2022

²⁰³ Αρ.6 παρ.1 περίπτ. στ’ ν.3115/2003

²⁰⁴ Στη βάση της διάκρισης των εξουσιών και της απαγόρευσης μεταβίβασης των αρμοδιοτήτων μιας εξουσίας σε άλλη

²⁰⁵ Τιντζογλίδου Νόπη (2010), «Ο εγγυητικός ρόλος των παρόχων στη διαδικασία άρσης του απορρήτου» *ΔιΜΕΕ*, 3/2010, σελ. 354

²⁰⁶ Βλ. ενδεικτικά την Έκθεση Πεπραγμένων της ΑΔΑΕ έτους 2020, σελ.59 EKTHESI_2020.pdf (<adae.gr>). Αντίστοιχες διατυπώσεις συναντά κανείς και σε εκθέσεις προηγούμενων ετών.

²⁰⁷ Α. Παπανικολάου (2020)

²⁰⁸ Βλ. ιδίως την εξόχως προβληματική διάταξη της παρ.1 άρθρου 87 Ν.4790/2021,ΦΕΚ Α 48/31.3.2021,που αντικατέστησε την παρ.9 του αρ.5 του ν.2225/1994, η οποία μάλιστα εφαρμόζεται αναδρομικά και για τις άρσεις του απορρήτου που έχουν λάβει χώρα έως τη δημοσίευση του Ν.4790/2021.

Σύμφωνα με δημοσιογραφική έρευνα, η νομοθετική τροποποίηση ήταν τουλάχιστον ευκαιριακή. Βλ. Λεοντόπουλος Νικόλας και Χονδρόγιαννος Θωδωρής (2022) «Εχθρός του Κράτους: Αποδεικνύουμε ότι η κυβέρνηση Μητσοτάκη παρακολουθούσε τον δημοσιογράφο Θανάση Κουκάκη Reporters United (<https://www.reportersunited.gr/>) 15/4/2022, διαθέσιμο στο <Εχθρός του Κράτους: Αποδεικνύουμε ότι η>

[κυβέρνηση Μητσοτάκη παρακολουθούσε τον δημοσιογράφο Θανάση Κουκάκη - R•U \(reportersunited.gr\)](http://reportersunited.gr) ημ.πρόσβασης 4/6/2022

²⁰⁹ Για παράδειγμα: ποιες κατηγορίες μεταδεδομένων αναλύονται με μεγαλύτερη συχνότητα,

²¹⁰ Βάσει του αρ.6 παρ.2 του ν.3471/2006

²¹¹ Αρ.5 παρ.6 ν.2225/1994

²¹² Βλ και παρατηρήσεις για την υπόθεση του ΔΕΕ C-746/18 H.K.Prokuratuur

²¹³ Για παράδειγμα εντός του απώτατου ορίου των 10 μηνών όπως ισχύει για τις περιπτώσεις διακρίβωσης εγκλημάτων

²¹⁴ Της οποίας οι σχεδιασμοί και ικανότητες δυσχερώς μπορούν να αμφισβητηθούν

²¹⁵ Η οποία συχνά συγκαλύπτει άλλες αξιολογήσεις ή επιδιώξεις

²¹⁶ Αρ.254 παρ.1 περίπτωση δ' ΚΠΑ

²¹⁷ Η μοναδική διαφορετική εκδοχή είναι η αξιοποίηση των στοιχείων που συλλέγονται κατά τη διαδικασία άρσης απορρήτου για την ενεργοποίηση του άρθρου 48 του Συντάγματος και τη θέση σε ισχύ του νόμου για την κατάσταση πολιορκίας. Ωστόσο, η πραγματικότητα των τελευταίων 18 ετών κατά τα οποία υπερισχύουν αδικαιολόγητα οι διατάξεις για την άρση του απορρήτου για λόγους εθνικής ασφάλειας και η μη ενεργοποίηση του αρ.48, υποδεικνύει ότι το συγκεκριμένο επιχείρημα στερείται βάσης.

²¹⁸ Αν και δε στερείται προβλημάτων

²¹⁹ Σύμφωνα με το αρ.27 του Π.Δ. 178/2014: *Η Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών (ΔΙ.Δ.Α.Π.) εδρεύει στην Αττική, έχει αρμοδιότητα σε όλη την επικράτεια και έχει ως αποστολή τη συγκέντρωση, ιδίως μέσω των περιφερειακών Υπηρεσιών της Ελληνικής Αστυνομίας, την αξιολόγηση, ταξινόμηση, ανάλυση και διάθεση επεξεργασμένων ή μη πληροφοριών, προς το σκοπό αντιμετώπισης κάθε μορφής εγκληματικότητας και ιδίως της τρομοκρατίας και του οργανωμένου εγκλήματος και συγκεκριμένα της πρόληψης, εξακρίβωσης ή διερεύνησης των αξιόποινων πράξεων που περιέχονται στην περίπτωση ε' του άρθρου 2 του π.δ. 135/2013,*

²²⁰ Τη σχετική κρίση επανέλαβε και στην υπόθεση C-746/18 H.K.Prokuratuur

²²¹ Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα, σελ.22

²²² Η τη διακρίβωση συγκεκριμένων αδικημάτων

²²³ Ήτοι ύπαρξη σοβαρών ενδείξεων τέλεσης των συγκεκριμένων πράξεων, διενέργεια των ανακριτικών πράξεων για το απολύτως αναγκαίο χρονικό διάστημα που απαιτείται για την επίτευξη του επιδιωκόμενου σκοπού και με βούλευμα που μεταξύ άλλων περιλαμβάνει την αδυναμία ή ιδιαίτερη δυσχέρεια διακρίβωσης του εγκλήματος με άλλο τρόπο και την απόλυτα αναγκαία χρονική διάρκεια της ανακριτικής πράξης.

²²⁴ Αλλά όχι αποκλειστικά. Παρόμοια προβλήματα δύνανται να προκύψουν και σε περιπτώσεις στοχευμένων άρσεων απορρήτου

²²⁵ ΑΠ 1014/2020 βλ. σχετικά και σχολιασμό σε Παρατηρήσεις στην ΑΠ (ποιν) 1014/2020

Κουκλουμπέρης Ν. (2021) Το ζήτημα της αξιοποίησης αποδεικτικών στοιχείων κατόπιν άρσης απορρήτου, ΠοινΔικ.8-9/2021 σελ.1246-1252

²²⁶ Και προϋποθέτει ένα πλήθος αναλυτικών ικανοτήτων, δυνατότητα προσέγγισης του σημασιολογικού κώδικα ή κώδικα συμπεριφοράς των παρακολουθούμενων και άλλες

²²⁷ Αναλογικής υπό την έννοια της αντιδιαστολής στην ψηφιακή.

²²⁸ Η συνακρόαση θα μπορούσε τηρουμένων των αναλογιών να παραλληλιστεί με τα όπλα ακριβείας, ενώ η μαζική ανάλυση μεταδεδομένων με τα όπλα διασποράς.

²²⁹ Big Brother Watch and others v. The United Kingdom, παρ.424

²³⁰ Επιχειρήματα που θέτουν ερωτήματα ως προς την πραγματική ανάγκη εν γένει προστασίας του απορρήτου. Δηλαδή, υπό αυτό το σκεπτικό, δε θα έπρεπε να υφίσταται απόρρητο της επικοινωνίας όταν γίνεται επίκληση λόγων εθνικής ασφάλειας.

²³¹ Βλ. σχετικά Τσόλιας Γρ. (2021) «Η νόμιμη (μαζική) παρακολούθηση των ηλεκτρονικών επικοινωνιών υπό το πρίσμα της νομολογίας του ΕΔΔΑ- Σχόλιο στην από 25.5.2021 απόφαση Big Brother Watch and others V. the UK., ΔΙΜΕΕ 3/2021», σελ.393 απ' όπου και το απόσπασμα που ακολουθεί

²³² Τα ίδια ισχύουν με εμφανέστερο τρόπο στις περιπτώσεις άρσης απορρήτου για διακρίβωση αδικημάτων, όπου λόγω των συνεχών αλλαγών στον ποινικό κώδικα και της παράθεσης μόνο του αριθμού των άρθρων αυτού στο αρ.4 του ν.2225/1994, δεν είναι πια βέβαιο για ποια ακριβώς αδικήματα επιτρέπεται η άρση απορρήτου

²³³ Α. Παπανικολάου (2020) Σελ.21 και επόμενες

²³⁴ Μεταξύ τηλεφωνικής και ψηφιακής επικοινωνίας όσο και μεταξύ των διαφόρων τύπων ψηφιακής επικοινωνίας

²³⁵ Distinguishing Group Privacy From Personal Privacy: The Effect of Group Inference Technologies on Privacy

Perceptions and Behaviors. JENNIFER JIYOUNG SUH, MIRIAM J. METZGER, SCOTT A. REID, AMR EL ABBADI, <https://par.nsf.gov/servlets/purl/10113167>

²³⁶ Jiyoung Suh Jennifer και Metzger Miriam J. και Reid Scott A. και El Abbadi Amr (2018) *Distinguishing Group Privacy From Personal Privacy: The Effect of Group Inference Technologies on Privacy Perceptions and Behaviors*. Proc. ACM Hum.-Comput. Interact. 2, CSCW, Article 168 (November 2018), 22 pages. <https://doi.org/10.1145/3274437> ημ.πρόσβασης 4/6/2022

²³⁷ Μιλάμε συγκεκριμένα για την απογραφή που έγινε από το ναζιστικό καθεστώς στη Γερμανία το 1939. Το Εθνικοσοσιαλιστικό Εργατικό Κόμμα Γερμανίας (το διαβόητο NSDAP), στο πλαίσιο της ναζιστικής πολιτικής και αμέσως μετά την άνοδό του στην εξουσία, αποφάσισε τη διεξαγωγή απογραφής σε όλο τον πληθυσμό. Η απογραφή έγινε το 1939 σε σύνολο σχεδόν 80 εκατομμυρίων ανθρώπων και μεταξύ των πληροφοριών που καταγράφονταν ήταν η ηλικία, το φύλο, η φυλή, το θρήσκευμα, ο τόπος διαμονής, η οικογενειακή κατάσταση κ.α. . Οι πληροφορίες αυτές αποθηκεύονταν σε διάτρητες κάρτες (punch-cards) και καταμετρούνταν με τη χρήση της μηχανής Hollerith, η οποία είχε αναπτυχθεί από την αμερικανική εταιρεία IBM και μέσω της θυγατρικής εταιρείας στη Γερμανία (της Dehomag), παρείχε στο ναζιστικό καθεστώς τεχνική υποστήριξη και μηχανικούς για τη λειτουργία των μηχανών αυτών. Παρά τα ποικίλα προβλήματα που αντιμετώπισε η διαδικασία αυτή, γεγονός είναι ότι συγκεντρώθηκαν εκτεταμένες και ακριβείς πληροφορίες για εκατομμύρια ανθρώπων και οι οποίες μπορούσαν να τύχουν ανάλυσης σε σχετικά μικρό χρονικό διάστημα, με έναν «αυτοματοποιημένο» τρόπο. Οι επιδιώξεις σε σχέση με τη συλλογή και ανάλυση πληροφοριών στο 3ο Ράιχ έφτασαν μέχρι την προσπάθεια δημιουργίας ενός μοναδικού αναγνωριστικού αριθμού (Personaleinzelerfassung) για κάθε άνθρωπο, μέσω του οποίου θα μπορούσε να επιτυγχάνεται η διαλειτουργικότητα των διαφορετικών αρχείων καθώς και ο εντοπισμός κάθε προσώπου.

Τα δεδομένα της απογραφής όσο και η λειτουργία των μηχανών Hollerith χρησιμοποιήθηκαν για τη δημιουργία του μητρώου Εβραίων που ζούσαν στη Γερμανία (και σε άλλες περιοχές που είχαν καταστεί μέρος του 3ου Ράιχ) και επιπλέον για τη δίωξη και τη σύλληψή τους. Απώτατος σκοπός αυτής της σύμπλεξης στατιστικής, τεχνολογίας, μεθόδων συλλογής πληροφοριών και ολοκληρωτικής πολιτικής, ήταν η υποστήριξη της λειτουργίας των στρατοπέδων συγκέντρωσης στο πλαίσιο της «τελικής λύσης».

Σχετικές πληροφορίες από Χαιρετάκης Μανώλης (2021) Η τεχνολογία, το Ολοκαύτωμα και η φρίκη, *Εφημερίδα των Συντακτών* 3/7/2021 διαθέσιμο στο https://www.efsyn.gr/nisides/300940_i-tehnologia-olokaytoma-kai-i-friki ημ.πρόσβασης 4/6/2022 και Δημοσιογραφική Ομάδα Ιός (2001) *Το διάτρητο παρελθόν της IBM*, 13/2/2001, διαθέσιμο στο <http://www.iospress.gr/mikro2001/mikro20010303.htm> ημ.πρόσβασης 4/6/2022

²³⁸ Λέβι Πρίμο (2000) *Αυτοί που βούλιαξαν και αυτοί που σώθηκαν*. Αθήνα, Άγρα, σελ.210

²³⁹ Μπερντιάεφ Νικολάϊ (2021), *Το νόημα της ιστορίας*, Αθήνα, Εναλλακτικές Εκδόσεις, σελ.285