ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»
Ακαδημαϊκό έτος 2022-2023

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Ελένης Βλιώρα
(Α.Μ.: 2106)

ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΕΔΙΟ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ: ΕΝ ΑΝΑΜΟΝΗ ΤΟΥ E-PRIVACY. Η ΠΡΟΒΟΛΗ ΤΟΥ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ

Επιβλέπουσα:
Αικατερίνα Παπανικολάου

Πειραιάς, Ιούνιος 2023

Ολοκληρώνοντας το πρόγραμμα μεταπτυχιακών σπουδών στο Πανεπιστήμιο Πειραιώς, θα ήθελα να ευχαριστήσω τους γονείς μου, Σπύρο Βλιώρα και Αθηνά Νικολογιάννη.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

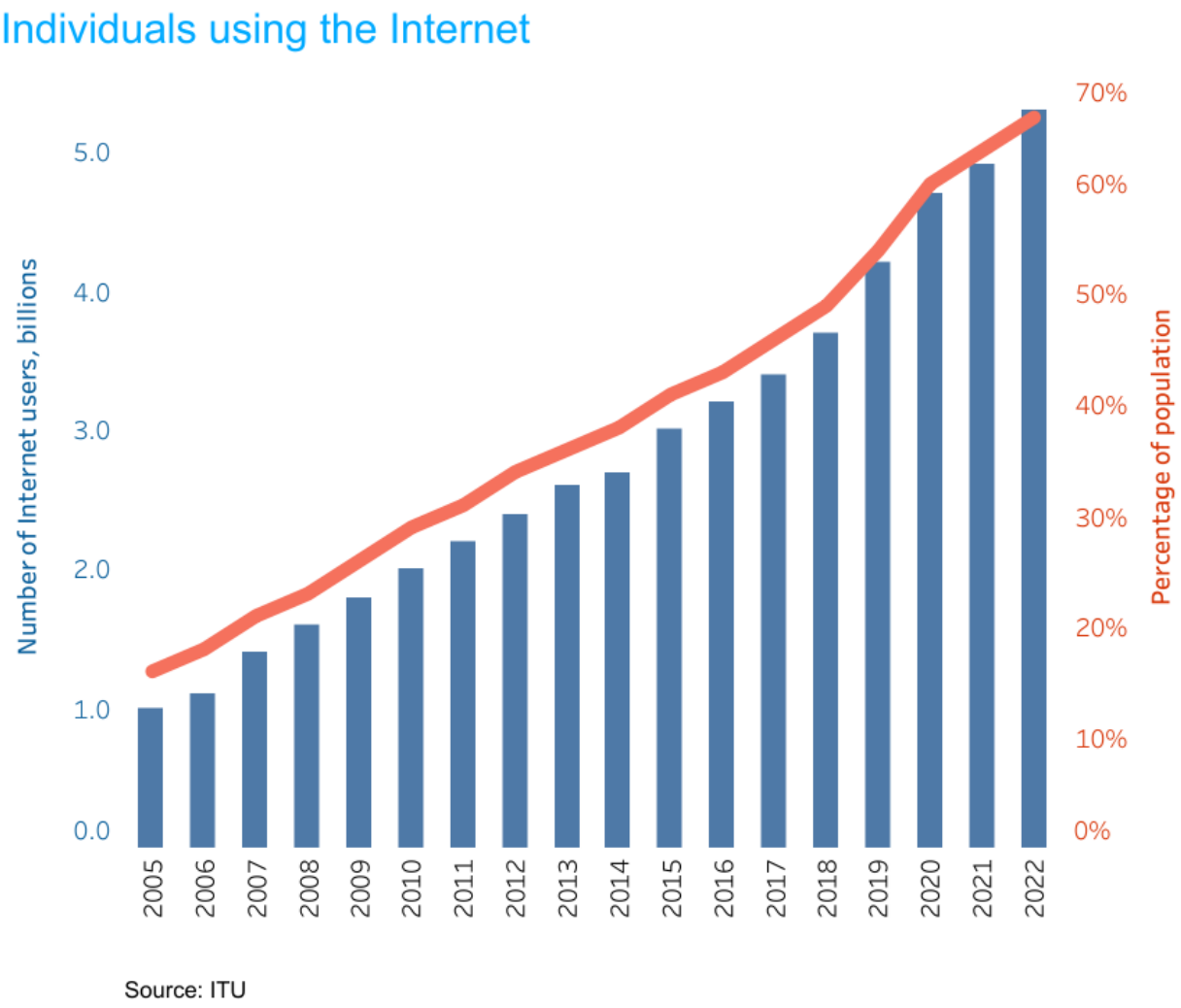
ΠΕΡΙΛΗΨΗ

Το παρόν εγχείρημα αναδεικνύει τα ζητήματα της προστασίας και της αξιοποίησης των δεδομένων που πηγάζουν από τις ηλεκτρονικές επικοινωνίες, υπό το πρίσμα της προσπάθειας επίτευξης ισορροπίας και εναρμόνισης συμφερόντων που παρουσιάζουν αντινομίες, όπως είναι η προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων έναντι της ανάπτυξης της καινοτομίας των τεχνολογικών προϊόντων και έναντι της επίτευξης υπέρτερων δημοσίων συμφερόντων, όπως η εθνική ασφάλεια και η αντιμετώπιση της βαριάς εγκληματικότητας. Πιο συγκεκριμένα, παρατίθεται το υφιστάμενο νομοθετικό πλαίσιο ως προς την προστασία των προσωπικών δεδομένων στο πεδίο των ηλεκτρονικών επικοινωνιών και, εν συνεχεία, επιχειρείται η παρουσίαση των βασικών σημείων της Πρότασης Κανονισμού *για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες).* Γίνεται αναφορά στα κρίσιμα σημεία στα οποία η Πρόταση Κανονισμού φιλοδοξεί να δώσει λύσεις, στα κενά που έχουν δημιουργηθεί λόγω της καθυστέρησης οριστικοποίησης του Κανονισμού, καθώς και στους λόγους για τους οποίους η ψήφιση του τελικού κειμένου δεν έχει πραγματοποιηθεί μέχρι σήμερα.

1. ΕΙΣΑΓΩΓΗ - ΟΙ ΕΠΙΚΟΙΝΩΝΙΕΣ ΣΗΜΕΡΑ

Ο τρόπος με τον οποίο επικοινωνούμε έχει αλλάξει άρδην τα τελευταία χρόνια. Οι παραδοσιακές μορφές επικοινωνίας, λόγω των ραγδαίως εξελισσόμενων τεχνολογικών μεταβολών, τείνουν να αντικαθίστανται από νέες υπηρεσίες βασιζόμενες στο Διαδίκτυο και σε δεδομένα.

Σύμφωνα με στατιστική έρευνα της Διεθνούς Ένωσης Τηλεπικοινωνιών[1], το 66% του παγκόσμιου πληθυσμού χρησιμοποιούν το Διαδίκτυο.



Έχουν αναπτυχθεί και χρησιμοποιούνται ευρέως οι λεγόμενες επιφυείς υπηρεσίες (OTT - Over the Top), οι οποίες περιλαμβάνουν μετάδοση και διανομή περιεχομένου (ήχος, βίντεο και άλλα αρχεία πολυμέσων μέσω του Διαδικτύου), που όμως δεν ελέγχονται από κάποιον χειριστή,

[1] Διεθνής Ένωση Τηλεπικοινωνιών https://www.itu.int/en/ITU-D/Statistics/Pages/about.aspx

παρακάμπτοντας τα τηλεπικοινωνιακά δίκτυα. Φαίνεται[2] πως δεν υφίσταται ένας καθιερωμένος ορισμός για αυτές τις υπηρεσίες· τέτοιες είναι οι εφαρμογές άμεσης ανταλλαγής μηνυμάτων μέσω Διαδικτύου και οι διάχυτες υπηρεσίες φωνής μέσω πρωτοκόλλου διαδικτύου VoIP (Voice over Internet Protocol), όπως για παράδειγμα το FaceTime, το WhatsApp, το Skype, το Messenger του Facebook, κ.ά.

Το Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών (BEREC), σε μία προσπάθεια αποσαφήνισης του όρου,[3] έχει υπογραμμίσει πως οτιδήποτε παρέχεται μέσω του δημόσιου Διαδικτύου συνιστά μία υπηρεσία OTT, όπως για παράδειγμα τα μέσα κοινωνικής δικτύωσης, οι ειδησεογραφικοί ιστότοποι, οι μηχανές αναζήτησης κ.ά.

Ακόμα, έχει αναδυθεί και η επικοινωνία μέσω του Διαδικτύου των Πραγμάτων (IoT, Internet of Things), με διασυνδεδεμένες συσκευές και μηχανές (machine to machine), μέσω των οποίων μεταφέρεται πληθώρα δεδομένων.

Στις μέρες μας λοιπόν γίνεται λόγος για "ηλεκτρονικές επικοινωνίες"[4], σε αντιδιαστολή με τον παλαιότερο όρο "τηλεπικοινωνίες", προσεγγίζοντας τον ορισμό των επικοινωνιών λειτουργικά, ώστε να περιλαμβάνονται, πλην των παραδοσιακών υπηρεσιών φωνητικής τηλεφωνίας, γραπτών μηνυμάτων (SMS) και ηλεκτρονικού ταχυδρομείου, και οι επιφυείς υπηρεσίες. Έναν τέτοιο ευρύ ορισμό των ηλεκτρονικών επικοινωνιών εμπεριέχει ο Ευρωπαϊκός Κώδικας ηλεκτρονικών επικοινωνιών[5], ο οποίος έχει θεσπίσει ανανεωμένες ρυθμίσεις που αφορούν τον τομέα των επικοινωνιών.

Οι παραπάνω μορφές επικοινωνίας παράγουν τέτοια πληθώρα πληροφοριών και συνακόλουθα συνεπάγονται τη μεταφορά τόσο μεγάλου όγκου δεδομένων προσωπικού

---

2 European Parliament - Directorate General for Internal Policies, Policy Department A Economic and Scientific Policy (2015) *Over-the-top (OTT) players: market dynamics and policy changes*, διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf

3 Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών (BEREC) (2016) BEREC Report on OTT services, διαθέσιμο εδώ: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-ott-services

4 Βλ. άρθρο 81 παρ. 4 του Ν.4070/2012

5 Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση)Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018L1972

χαρακτήρα, που, ευστόχως μπορούμε να πούμε ότι έχει τεθεί για τις συσκευές, όπως είναι τα smartphones, το ερώτημα "A Spy in your Pocket?[6]". Τα δεδομένα αυτά είναι τεράστιας αξίας τόσο για τις διωκτικές αρχές όσο και για τις ιδιωτικές εταιρείες και έχουν καταστήσει τη ρύθμιση της αξιοποίησής τους εξόχως πολύπλοκο ζήτημα.

Όλες αυτές οι νέες μορφές επικοινωνίας δεν διέπονται από το ισχύον ευρωπαϊκό νομοθετικό πλαίσιο για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, με αποτέλεσμα να έχει δημιουργηθεί κενό στο πλαίσιο προστασίας.

6 Nicola Green N. και Sean Smith (2003) *«A Spy in your Pocket»? The Regulation of Mobile Data in the UK, Surveillance and Society*, Vol. 1 No. 4 : Surveillance and Mobilities, διαθέσιμο εδώ: https://www.researchgate.net/publication/265007629_'A_Spy_in_your_Pocket'_The_Regulation_of_Mobile_Data_in_the_UK

2. ΤΟ ΔΙΚΑΙΩΜΑ ΤΗΣ ΑΠΟΡΡΗΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

2.1 Η επικοινωνία ως επιμέρους έκφανση της ιδιωτικότητας

2.1.1. Ευρωπαϊκά Κείμενα

Η επικοινωνία αποτελεί έκφανση της ιδιωτικής σφαίρας του ατόμου, η οποία ανάγεται σε ουσιώδες στοιχείο της ανθρώπινης προσωπικότητας[7]. Σε ευρωπαϊκό επίπεδο το δικαίωμα της απόρρητης επικοινωνίας προστατεύεται από τα θεμελιώδη κείμενα, ήτοι από το άρθρο 7 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ ("*Κάθε πρόσωπο έχει δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας του και των επικοινωνιών του*"), καθώς και από το άρθρο 8 της ΕΣΔΑ ("*1. Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του.*") Κατά πάγια νομολογία του ΕΔΔΑ, η ιδιωτική ζωή δεν μπορεί να ορισθεί εξαντλητικά, αποτελώντας ευρεία και δυναμική έννοια[8], με τις τέσσερις επιμέρους εκφάνσεις που αναφέρονται στο άρθρο 8 της ΕΣΔΑ, να αλληλοκαλύπτονται συχνά. Σε διεθνές επίπεδο, το δικαίωμα προστατεύεται από το άρθρο 17 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα και από το άρθρο 12 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα.

2.1.2. Συνταγματική κατοχύρωση

Στα καθ' ημάς, ο συντακτικός νομοθέτης έχει επιμερίσει το δικαίωμα της ιδιωτικότητας στο άρθρο 9 ("*...Η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη...")*, στο άρθρο 9Α ("*Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων...*") και στο άρθρο 19 ("*Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο...*"). Εντούτοις, εκ των ορισμών των ευρωπαϊκών κειμένων διαφαίνεται ότι το δικαίωμα στην ιδιωτική ζωή είναι ενιαίο[9].

---

7 Π. Δαγτόγλου (2012) *Συνταγματικό Δίκαιο, Ατομικά και Κοινωνικά Δικαιώματα*, 4η Έκδοση, Εκδόσεις Σάκκουλα, σελ. 269

8 Μ. Καραβίας σε Λ. Α. Σισιλιάνος (2013) *Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, Ερμηνεία κατ' άρθρο*, Νομική Βιβλιοθήκη, σελ. 312

9 ΕΔΔΑ (2022) *Guide on Article 8 of the Convention – Right to respect for private and family life*, διαθέσιμο εδώ: https://www.echr.coe.int/documents/guide_art_8_eng.pdf

Η συνταγματική διάταξη στο άρθρο 19 προστατεύει τον απόρρητο χαρακτήρα της επικοινωνίας, που σημαίνει ότι η επικοινωνία διεξάγεται εμπιστευτικά, σε συνθήκες οικειότητας, κάτι το οποίο ανάγεται στην προστασία της ιδιωτικής ζωής[10]. Μάλιστα, το απόρρητο της επικοινωνίας χαρακτηρίζεται από τη συνταγματική διάταξη με εμφατικό - πανηγυρικό τρόπο ως "απόλυτα απαραβίαστο", αν και στο αμέσως επόμενο εδάφιο το Σύνταγμα περιέχει επιφύλαξη νόμου για την κάμψη του κανόνα ("*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*.") Η συγκεκριμένη διατύπωση έχει συμβολικό χαρακτήρα και έχει τεθεί μεν για ιστορικούς λόγους, ωστόσο προσδίδει ιδιαίτερη βαρύτητα στο δικαίωμα της επικοινωνίας κατά τη στάθμισή του με άλλα θεμελιώδη δικαιώματα, με το πρώτο να υπέρκειται[11].

2.2 Ασφάλεια επικοινωνίας

Έχει υποστηριχθεί ότι το απόρρητο της επικοινωνίας διακρίνεται από την "ελευθερία της εμπιστευτικής επικοινωνίας[12]", άλλως το απαραβίαστο της επικοινωνίας, το να φτάσει η επικοινωνία ακέραια στον προορισμό της. Στο πλαίσιο αυτό αναδύεται η έννοια της ασφάλειας των επικοινωνιών.

Σύμφωνα με το άρθρο 2 παρ. 21 του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών, η ασφάλεια ορίζεται ως "*η ικανότητα δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών να ανθίστανται, σε δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των εν λόγω δικτύων και υπηρεσιών, των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω δικτύων ή υπηρεσιών ηλεκτρονικών επικοινωνιών*".

---

10 Τσακυράκης Σ. (1993) *Το απόρρητο της επικοινωνίας – Απόλυτα απαραβίαστο ή ευχή της έννομης τάξης;*, ΝοΒ, σελ. 995 επ.

11 Ν. Παπαδόπουλος (2008) *ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ - ΕΡΜΗΝΕΥΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΑΡΘΡΟΥ 19 ΤΟΥ ΣΥΝΤΑΓΜΑΤΟΣ ΤΗΣ ΕΛΛΑΔΑΣ*, Νομική Βιβλιοθήκη, σελ. 197

12 Καϊδατζής Α. (2007) *Τηλεπικοινωνιακό απόρρητο και ασφάλεια των επικοινωνιών. Παρατηρήσεις στη ΣΕ (ΕΑ) 456/2007*, ΕφημΔΔ, σελ. 440 επ.

Επομένως η ασφάλεια, ως ευρύτερη έννοια αφορά επιμέρους τομείς, ήτοι οι υπηρεσίες να είναι λειτουργικές (διαθεσιμότητα), να επιβεβαιώνεται η δηλούμενη ταυτότητα των χρηστών (αυθεντικότητα), να διασφαλίζεται ότι τα δεδομένα παραμένουν αμετάβλητα (ακεραιότητα) και να προστατεύονται οι επικοινωνίες και τα αποθηκευμένα δεδομένα από την υποκλοπή (απόρρητο). Υπό αυτό το πρίσμα, η ασφάλεια διακρίνεται : α) στην ασφάλεια του απορρήτου των πληροφοριών και των δεδομένων της επικοινωνίας, β) στην ασφάλεια των δεδομένων προσωπικού χαρακτήρα των χρηστών και συνδρομητών και γ) στη φυσική ασφάλεια των υποδομών.

Είναι άραγε δυνατόν να αντιμετωπίσουμε το ζήτημα της ασφάλειας των επικοινωνιών ξεχωριστά, απομονώνοντας την κάθε επιμέρους έκφανσή του; Για παράδειγμα, εάν η επικοινωνία δεν είναι ασφαλής, πώς θα επιτευχθεί το απόρρητο; Φαίνεται πως η απάντηση στο ερώτημα είναι αρνητική, καθώς όλες οι εκφάνσεις της ασφάλειας συναποτελούν στοιχεία μιας ελεύθερης επικοινωνίας[13]. Σχετικώς έχει λεχθεί[14] ότι το δικαίωμα του άρθρου 19 παρ. 1 του Συντάγματος κείται στο μεταίχμιο άλλων δικαιωμάτων που κατοχυρώνει το Σύνταγμα, όπως το δικαίωμα της ιδιωτικότητας του άρθρου 9, το δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας του άρθρου 5 παρ. 1, το δικαίωμα της ελευθερίας της γνώμης του άρθρου 14 παρ. 1 Σ, το δικαίωμα της ελεύθερης πρόσβασης στην πληροφόρηση του άρθρου 5Α και το δικαίωμα πληροφοριακής αυτοδιάθεσης του άρθρου 9Α και αποτελεί λογική προϋπόθεση για την ακώλυτη άσκησή τους.

2.3 Τι εμπίπτει στο πεδίο εφαρμογής της συνταγματικής διάταξης

2.3.1. Εσωτερικά και εξωτερικά στοιχεία επικοινωνίας

Η συνταγματική διάταξη προστατεύει τον απόρρητο χαρακτήρα της επικοινωνίας, χωρίς να κάνει αναφορά στον τρόπο διεξαγωγής της ή σε διακριτά στοιχεία αυτής. Επομένως, κάθε είδους επικοινωνία που τα μέρη της την εννοούν ως απόρρητη και εμπιστευτική εμπίπτει στο

---

13 Γρ. Τσόλιας (2008) *Η ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας σύμφωνα με τον Ν 3674/2008 (Παρουσίαση και ερμηνευτική προσέγγιση των διατάξεων)*, ΔΙΤΕ (π.ΔΙΜΕΕ) 3/2008

14 Γρ. Τσόλιας (2004) *Τα τηλεπικοινωνιακά δεδομένα υπό το πρίσμα του απορρήτου: προβληματισμοί ενόψει της ενσωμάτωσης της Οδηγίας 2002/58/ΕΚ*, ΔΙΤΕ (π. ΔΙΜΕΕ) 3/2004

πεδίο προστασίας.

Η αναφορά στη μη διάκριση των στοιχείων της επικοινωνίας είναι άξια λόγου στο παρόν σημείο, λόγω του διαχωρισμού που έχει γίνει σε θεωρητικό επίπεδο[15] μεταξύ εσωτερικών και εξωτερικών στοιχείων (η αλλιώς "μεταδεδομένων[16]") της επικοινωνίας. Ως εσωτερικά, κατ' αυτή τη διάκριση νοούνται τα στοιχεία του περιεχομένου της επικοινωνίας, δηλαδή το μεταδιδόμενο μήνυμα. Ως εξωτερικά νοούνται όλες οι περιστάσεις οι οποίες σχετίζονται με το επικοινωνιακό γεγονός, πλην του περιεχομένου της επικοινωνίας, όπως π.χ. τα επικοινωνούντα υποκείμενα, η γεωγραφική τους θέση, η διάρκεια της επικοινωνίας κλπ.

Το ζήτημα του εάν τα εξωτερικά στοιχεία της επικοινωνίας αποτελούν μέρος της προστασίας του απορρήτου της επικοινωνίας έχει προβληματίσει την επιστημονική κοινότητα. Στην Ελλάδα, για το εν λόγω θέμα έχει υπάρξει διαφωνία μεταξύ Εισαγγελικών, Δικαστικών και Ανεξάρτητων Αρχών:

2.3.2. Η θέση του Αρείου Πάγου

Το 2009 εξεδόθησαν Γνωμοδοτήσεις[17] από την Εισαγγελία του Αρείου Πάγου, σύμφωνα με τις οποίες α) οι επικοινωνίες που διεξάγονται μέσω Ίντερνετ δεν προστατεύονται από το απόρρητο των επικοινωνιών και β) στο προστατευτικό πεδίο εφαρμογής της συνταγματικής διάταξης του άρθρου 19 δεν εμπίπτουν τα εξωτερικά στοιχεία της επικοινωνίας και, επομένως, για την άρση αυτών δεν απαιτείται η τήρηση της διαδικασίας τού (τότε) Ν. 2225/1994. Το σκεπτικό αυτών των Γνωμοδοτήσεων κινήθηκε γύρω από την ανάγκη εξασφάλισης προανακριτικού υλικού, προκειμένου να αποφευχθεί ο κίνδυνος εξαφάνισης των ηλεκτρονικών ιχνών και, παρότι οι Γνωμοδοτήσεις δεν έχουν δεσμευτική ισχύ, έδωσαν το έναυσμα στις διωκτικές αρχές να απαιτούν από τους παρόχους επικοινωνιών την αποκάλυψη των εξωτερικών στοιχείων επικοινωνίας χωρίς καμία απολύτως εγγύηση. Τα ποινικά τμήματα του Αρείου Πάγου ενστερνιζόταν τη συγκεκριμένη άποψη, όπως εμφαίνεται και με σειρά σχετικών αποφάσεων

---

15 Ν. Λίβος (1997) *Η ποινική προστασία των συνδετικών δεδομένων των τηλεπικοινωνιών*, ΠοινΧρ, ΜΖ', σελ. 737 επ.

16 Θα αναλυθεί κατωτέρω.

17 Γνωμοδότηση υπ' αριθμ. 9/2009, Εισαγγελία ΑΠ, Γ. Σανιδάς Εισαγγελέας Αρείου Πάγου και Γνωμοδότηση υπ' αριθμ. 12/2009, Εισαγγελία ΑΠ, Ι. Σ. Τέντες Εισαγγελέας Αρείου Πάγου

που έχουν εκδοθεί[18]. Η Γνωμοδότηση 9/2009 μάλιστα κατέληξε στο συμπέρασμα ότι το ΠΔ 47/2005 (το οποίο, όπως θα δούμε στη συνέχεια εξειδικεύει τα της άρσης του απορρήτου) είναι αντισυνταγματικό στο μέτρο που επεκτείνει ρητώς το απόρρητο των επικοινωνιών στις επικοινωνίες μέσω Ίντερνετ και στα εξωτερικά στοιχεία της επικοινωνία.

2.3.3. Η θέση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

Η ΑΔΑΕ, ήδη από το 2005 με Γνωμοδότησή[19] της, είχε τοποθετηθεί επί του θέματος εκθέτοντας τους λόγους για τους οποίους τα εξωτερικά στοιχεία της επικοινωνίας εμπίπτουν στο προστατευτικό πεδίο του απορρήτου. Στο πλαίσιο απάντησης σε παρόχους επικοινωνιών οι οποίοι δέχονταν αιτήσεις αρχών για παροχή εξωτερικών στοιχείων επικοινωνίας χωρίς να τηρείται η νόμιμη διαδικασία άρσεως του απορρήτου, είχε γνωμοδοτήσει με σαφήνεια, παραθέτοντας την Ευρωπαϊκή νομοθεσία και νομολογία. Το 2002 τέθηκε σε ισχύ η Οδηγία e-Privacy (όπως θα δούμε αναλυτικά κατωτέρω), η οποία συμπεριέλαβε ρητώς τα εξωτερικά στοιχεία της επικοινωνίας στην έννοια του απορρήτου των επικοινωνιών. Αν και κατά το χρονικό διάστημα εκείνο η Οδηγία δεν είχε ενσωματωθεί ακόμα στην ελληνική έννομη τάξη, η τελευταία δεν έπαυε να δεσμεύεται από την νομολογία του ΕΔΔΑ, κατά την οποία τα εξωτερικά στοιχεία της επικοινωνίας αποτελούν αναπόσπαστο στοιχείο των επικοινωνιών.

2.3.4. Η θέση του Συμβουλίου της Επικρατείας (ΣτΕ)

Την αντίθετη άποψη από τον Άρειο Πάγο εξέφρασε το 2016 με απόφασή[20] του το Συμβούλιο της Επικρατείας, ερμηνεύοντας διασταλτικά τη διάταξη του άρθρου 19 παρ. 1 του Συντάγματος: Το απόρρητο "*εκτείνεται στο σύνολο του επικοινωνιακού γεγονότος, καλύπτει, δηλαδή, όχι μόνο το περιεχόμενο της επικοινωνίας (φωνή, κείμενο, εικόνα, ήχο, ιστοσελίδα κ.λπ.), αλλά και τα συναφώς παραγόμενα δεδομένα επικοινωνίας (εφεξής: «δεδομένα επικοινωνίας») που προσδιορίζουν τις συνθήκες επικοινωνίας και την εξατομικεύουν (όπως πληροφορίες για τον τόπο, το χρόνο, τη διάρκεια, τη μορφή και το είδος επικοινωνίας, στοιχεία προσδιοριστικά του*

---

18 Βλ. (ενδεικτικά) ΑΠ 711/2011, ΑΠ 203/2014

19 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (2005) *Γνωμοδότηση 1/2005 κατόπιν αιτήματος της εταιρείας «ΤΙΜ ΕΛΛΑΣ» αναφορικά με τη διαδικασία άρσεως του απορρήτου στις τηλεφωνικές επικοινωνίες*, διαθέσιμο εδώ: http://www.adae.gr/fileadmin/docs/nomoi/893-2005.pdf

20 ΣτΕ 1593/2016 (Τμήμα Δ')

μέσου με το οποίο διεξήχθη η επικοινωνία, στοιχεία ταυτότητας και διευθύνσεων επικοινωνούντων μερών κ.λπ.)". Θεωρήθηκε[21] ότι με τη συγκεκριμένη απόφαση οριοθετήθηκαν οι υποχρεώσεις των παρόχων των επικοινωνιών σχετικά με τη διαδικασία άρσεως του απορρήτου, οι οποίοι δεν επιτρέπεται να δίνουν πρόσβαση στα σχετικά δεδομένα χωρίς να έχει προηγηθεί η νόμιμη διαδικασία άρσεως του απορρήτου[22] και ότι η συγκεκριμένη πρακτική θεωρείται εσφαλμένη.

2.3.5. Η θέση των Ευρωπαϊκών Δικαστηρίων

Το ΕΔΔΑ είχε ήδη τοποθετηθεί επί του θέματος από το 1984 στην απόφαση[23] Malone κατά Ηνωμένου Βασιλείου: "*The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone".* Η προοδευτική για την τότε εποχή κρίση του ΕΔΔΑ στη συνέχεια επισφραγίστηκε με πληθώρα αποφάσεων που καθιστούν πάγια την νομολογία του σχετικά με την υπαγωγή των εξωτερικών στοιχείων της επικοινωνίας στο απόρρητο των επικοινωνιών. Στην απόφαση[24] Big Brother Watch κατά Ηνωμένου Βασιλείου το ΕΔΔΑ υπογράμμισε ότι, με την εξέλιξη των μέσων επικοινωνίας, το περιεχόμενο ενός μηνύματος μπορεί πλέον να αποκαλύπτει λιγότερες πληροφορίες για τα μέρη της επικοινωνίας από τα εξωτερικά στοιχεία της επικοινωνίας. Τα τελευταία δύνανται να σκιαγραφήσουν λεπτομερώς το προφίλ του επικοινωνούντος ατόμου, αποκαλύπτοντας την τοποθεσία των μερών, τα μέσα με τα οποία διαδόθηκε η επικοινωνία, τη ροή της περιήγησής τους στο Διαδίκτυο, με ποιους επικοινωνούν κ.ά. Το ΕΔΔΑ συναφώς κατέληξε στο συμπέρασμα ότι δεν είναι δυνατόν να υφίστανται διαφοροποιημένες εγγυήσεις σχετικά με την προστασία των εξωτερικών στοιχείων της επικοινωνίας σε σχέση με το περιεχόμενο αυτής[25]. Με πιο εμφατικό τρόπο το ΔΕΕ, στις συνεκδικασθείσες υποθέσεις του 2022 SpaceNet και Telekom Deutschland, έκανε λόγο στην αποκαλυπτικότητα των συναφών δεδομένων ως προς την

---

21 Γρ. Τσόλιας (2016) *Σημείωμα στην ΣτΕ 1593/2016- Η υπαγωγή των εξωτερικών στοιχείων της επικοινωνίας στην διαδικασία άρσης του απορρήτου και η διασφάλισή της από τους Παρόχους*, ΔΙΤΕ (π. ΔΙΜΕΕ) 4/2016

22 Βλ.ΣτΕ 1593/2016 (Τμήμα Δ') "δεν επιτρέπεται να παρέχουν δυνατότητα πρόσβασης στο περιεχόμενο και τα δεδομένα της επικοινωνίας ούτε να γνωστοποιούν σχετικά στοιχεία, παρά μόνο αν εκδοθεί, με τη διαδικασία που ορίζεται στο Ν. 2225/1994, διάταξη άρσης του απορρήτου"

23 Απόφαση ΕΔΔΑ (1984) *Malone v. the United Kingdom*

24 Απόφαση ΕΔΔΑ (2021) *Big Brothers Watch and others v. the UK.*, Βλ. κυρίως Σκέψεις 317 και 342

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

ιδιωτική ζωή των επικοινωνούντων:

"Τα δεδομένα κινήσεως και τα δεδομένα θέσεως μπορούν να αποκαλύψουν πληροφορίες σχετικά με σημαντικό αριθμό πτυχών της ιδιωτικής ζωής των υποκειμένων των δεδομένων, συμπεριλαμβανομένων ευαίσθητων πληροφοριών, όπως είναι ο γενετήσιος προσανατολισμός, τα πολιτικά φρονήματα, οι θρησκευτικές, φιλοσοφικές, κοινωνικές ή άλλες πεποιθήσεις, καθώς και η κατάσταση της υγείας, ενώ τα δεδομένα αυτά τυγχάνουν, επιπλέον, ειδικής προστασίας στο δίκαιο της Ένωσης. Στο σύνολό τους, τα εν λόγω δεδομένα μπορούν να καταστήσουν δυνατή τη συναγωγή ακριβέστατων συμπερασμάτων όσον αφορά την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα διατηρήθηκαν, όπως οι καθημερινές συνήθειες, οι μόνιμοι ή προσωρινοί τόποι διαμονής, οι καθημερινές ή άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις των συγκεκριμένων προσώπων και οι κοινωνικοί κύκλοι στους οποίους αυτά συχνάζουν. Ειδικότερα, τα δεδομένα αυτά παρέχουν τα μέσα για τον προσδιορισμό του προφίλ των υποκειμένων των δεδομένων, πληροφορία εξίσου ευαίσθητη, όσον αφορά το δικαίωμα στον σεβασμό της ιδιωτικής ζωής, με το ίδιο το περιεχόμενο των επικοινωνιών"[26].

[26] Απόφαση ΔΕΕ (2022) *Bundesrepublik Deutschland κατά SpaceNet AG (C-793/19) και Telekom Deutschland GmbH (C-794/19)*, Σκέψη 61

3. ΤΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ

3.1 Η Οδηγία e-Privacy

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων[27] ("ΓΚΠΔ") που τέθηκε σε εφαρμογή τον Μάιο του 2018 δεν περιέχει εξειδικευμένες διατάξεις για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.

Το νομοθέτημα που υφίσταται στην ΕΕ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες είναι η Οδηγία 2002/58[28] «*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*» ("Οδηγία e-Privacy").

Οι απαρχές της Οδηγίας e-Privacy εντοπίζονται στην Οδηγία 97/66/ΕΚ[29], η οποία υποκινήθηκε από την υιοθέτηση της Οδηγίας 95/46/ΕΚ[30] για την προστασία των ατόμων έναντι της επεξεργασία προσωπικών δεδομένων (προγενέστερο νομοθετικό κείμενο του ΓΚΠΔ). Η Οδηγία 97/66/ΕΚ εμπεριείχε ρυθμίσεις για την επεξεργασία προσωπικών δεδομένων στις τηλεπικοινωνίες, αποτυπώνοντας στον τηλεπικοινωνιακό τομέα τις αρχές για την επεξεργασία δεδομένων που έθετε η Οδηγία 95/46[31]. Το πεδίο εφαρμογής της περιοριζόταν στις

---

27 Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex%3A32016R0679

28 Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, 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), διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058

29 Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A31997L0066

30 Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

31 Αιτιολογική Σκέψη 4 Οδηγία 2002/58

τεχνολογίες που χρησιμοποιούνταν τότε για την επικοινωνία, όπως η παραδοσιακή φωνητική τηλεφωνία.

Εντούτοις, η ανάπτυξη νέων τεχνολογιών στην αγορά των τηλεπικοινωνιών κατέστησε επιτακτική την επικαιροποίηση του νομοθετικού πλαισίου. Έτσι, η Οδηγία 97/66/ΕΚ αντικαταστάθηκε από την Οδηγία 2002/58, η οποία είναι εν ισχύ μέχρι και σήμερα.

Η Οδηγία e-Privacy έθεσε ένα ευρύτερο πλαίσιο προστασίας σχετικά με τα ζητήματα που άπτονται της ιδιωτικότητας και των προσωπικών δεδομένων κατά τη χρήση των ηλεκτρονικών επικοινωνιών, στοχεύοντας στην ελεύθερη ροή των προσωπικών δεδομένων, του εξοπλισμού και των υπηρεσιών ηλεκτρονικών επικοινωνιών και στην υιοθέτηση κοινών προτύπων στην ΕΕ για την προστασία αυτών των δεδομένων.[32] Αναγνωρίζοντας τις προκλήσεις για την ιδιωτικότητα των χρηστών που απορρέουν από τις αυξανόμενες δυνατότητες αποθήκευσης δεδομένων[33], η Οδηγία καθιέρωσε[34] την αρχή του απορρήτου των ηλεκτρονικών επικοινωνιών, επαυξάνοντας το πεδίο προστασίας του, με την επέκτασή του στα εξωτερικά στοιχεία της επικοινωνίας (“*όσο και των συναφών δεδομένων κινήσεως*”) και απαγόρευσε καταρχήν την αποθήκευση των επικοινωνιών και δεδομένων κινήσεως από άλλα πρόσωπα πέραν των χρηστών χωρίς τη συγκατάθεση τους.

3.1.1. Ο Ν. 3471/2006

Η Οδηγία e-Privacy ενσωματώθηκε στο εθνικό μας δίκαιο με τον Ν. 3471/2006[35], σκοπός του οποίου είναι “*η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών*”[36].

---

32 Άρθρο 1 Οδηγία 2002/58

33 Αιτ. Σκ 6 και 7 Οδηγίας

34 Με το άρθρο 5, παράγραφος 1

35 Νόμος 3471/2006 - ΦΕΚ 133/Α/28-6-2006 *Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997*

36 Άρθρο1 Νόμου 3471/2006

3.2. Η Οδηγία "Data Retention Directive" 2006/24

Άξια αναφοράς στο συγκεκριμένο πλαίσιο είναι η πρόσκαιρη ισχύς της Οδηγίας 2006/24[37], γνωστή ως "Data Retention Directive", η οποία θέσπισε "γενναιόδωρα" την διατήρηση από τους παρόχους των μεταδεδομένων επικοινωνίας *"για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων"*, στα οποία θα αποκτούν πρόσβαση οι αρμόδιες εθνικές διωκτικές αρχές. Το χρονικό πλαίσιο διατήρησης οριζόταν από έξι μήνες έως δύο χρόνια και το χαρακτηριστικό είναι πως δεν έθετε κάποιο κριτήριο για τη διάκριση ως προς τα υποκείμενα-στόχους, χωρίς να υφίσταται κάποια εύλογη υπόνοια εις βάρος τους. Προβλέφθηκε δηλαδή για το σύνολο του ευρωπαϊκού πληθυσμού, χωρίς να εξειδικεύει επαρκώς τα αντικειμενικά κριτήρια για μια τέτοια διατήρηση, δημιουργώντας ασαφές πλαίσιο για το ποια υποκείμενα θα μπορούσαν να υπαχθούν σε αυτό το μέτρο, αφού δεν προϋπέθετε την ενοχή κάποιου για αδίκημα. Μάλιστα, δεν εξαρτούσε την απόφαση περί διατήρησης των δεδομένων από την κρίση κάποιου ανεξάρτητου οργάνου. Σκοπός της Οδηγίας ήταν η καταπολέμηση της τρομοκρατίας και η πρόληψη του οργανωμένου εγκλήματος, ανάγκη που κατέστη επιτακτική εκείνη την περίοδο, ιδίως ύστερα από τις τρομοκρατικές επιθέσεις που σημειώθηκαν κατά το προγενέστερο χρονικό διάστημα[38].

Η Data Retention Directive προκάλεσε αντιδράσεις καθώς θεωρήθηκε ως προσπάθεια συστηματικής παρακολούθησης των πολιτών[39] και ακολούθησε έντονη κριτική συζήτηση ως προς την συμβατότητα με την ΕΣΔΑ και τον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ και συγκεκριμένα ως προς τη συνδρομή του κριτηρίου της αναγκαιότητας που θέτει το άρθρο 8 της ΕΣΔΑ. Εν τέλει, η Data Retention Directive, ύστερα από προδικαστικά ερωτήματα που έθεσε η Ιρλανδία και η Αυστρία στο ΔΕΕ, κρίθηκε με την απόφαση C-293/2012 Digital Rights Ireland, με αποτέλεσμα να ακυρωθεί και να κηρυχθεί ανίσχυρη, ως αποκλίνουσα από θεμελιώδεις διατάξεις του Χάρτη Θεμελιωδών Δικαιωμάτων. Το ΔΕΕ, επικαλούμενο τα άρθρα 7, 8 και 11 του Χάρτη Θεμελιωδών Δικαιωμάτων, κατέληξε στο συμπέρασμα ότι τα μέτρα της Οδηγίας

---

37 Οδηγία 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, διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32006L0024

38 Νέα Υόρκη το 2001, τη Μαδρίτη το 2004 και το Λονδίνο το 2005

39 Σπ. Τάσσης (2014) *ΔΕΕ -δύο θεμελιώδεις αποφάσεις για τα προσωπικά μας δεδομένα και τα ηλεκτρονικά δίκτυα: Απόφαση C-131/12 (Google) και συνεκδικαζόμενες C-293/12 και C-594/12 (νομιμότητα υποχρεωτικής διατήρησης τηλεπικοινωνιακών δεδομένων)*, ΔΙΤΕ (π. ΔΙΜΕΕ) 3/2014

συνιστούν σκληρές επεμβάσεις στα δικαιώματα των άρθρων αυτών. Πράγματι, τα διατηρούμενα δεδομένα στο σύνολό τους θα μπορούσαν να οδηγήσουν σε ιδιαίτερα συμπεράσματα όσον αφορά την ιδιωτική ζωή των υποκειμένων, τα οποία επιπρόσθετα θα επωμιζόταν το άγχος του αισθήματος της διαρκούς παρακολούθησης. Ναι μεν το Δικαστήριο αναγνώρισε την αξία των διατηρουμένων δεδομένων ως προς την καταπολέμηση της τρομοκρατίας και της βαριάς εγκληματικότητας — σκοποί γενικότερου συμφέροντος για την ΕΕ που ανάγονται στη δημόσια ασφάλεια, εντούτοις επεσήμανε ότι τίθεται ζήτημα ως προς το απολύτως αναγκαίο χαρακτήρα του μέτρου της Οδηγίας. Το γεγονός της μη οριοθέτησης προϋποθέσεων, κανόνων και εγγυήσεων του επιβαλλόμενου μέτρου οδήγησε στο συμπέρασμα ότι υπερβαίνει τα όρια που θέτει η αρχή της αναλογικότητας.

Μετά την ακύρωση της Οδηγίας, η διατήρηση των μεταδεδομένων εκ μέρους των παρόχων δεν είναι υποχρεωτική. Επανήλθε το προηγούμενο νομοθετικό καθεστώς της Οδηγίας 2002/58, η οποία στο άρθρο 15 παρ. 1 προβλέπει τη δυνατότητα των κρατών μελών να θεσπίζουν νομοθετικά μέτρα που περιορίζουν τα δικαιώματα που κατοχυρώνονται στην Οδηγία, τηρουμένων όμως των κανονιστικών απαιτήσεων του άρθρου 8 της ΕΣΔΑ, για τα οποία υφίσταται πλούσια νομολογία του ΕΔΔΑ.

3.2.1. Ο Ν. 3917/2011

Ωστόσο, η Οδηγία είχε ενσωματωθεί στο εθνικό μας δίκαιο με τον Ν. 3917/2011, ο οποίος ορίζει την διατήρηση των μεταδεδομένων επικοινωνίας επί 12 μήνες από την ημερομηνία της επικοινωνίας και απονέμει αρμοδιότητες ως προς την τήρηση των διατάξεών του στην ΑΔΑΕ και στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Ο νόμος αυτός εξακολουθεί να ισχύει στην ελληνική έννομη τάξη, παρά την ακύρωση της Οδηγίας 2006/24, με αποτέλεσμα να δημιουργείται ανακολουθία και ζήτημα ενότητας στη σχέση ενωσιακού και εθνικού δικαίου. Το 2014 συστήθηκε Νομοπαρασκευαστική Επιτροπή με στόχο την αναπροσαρμογή του ελληνικού κανονιστικού πλαισίου για τη διατήρηση των μεταδεδομένων επικοινωνίας. Ωστόσο, η τελευταία ουδέποτε υλοποίησε το έργο της.

3.3. Η Οδηγία "Cookies Directive" 2009/136

Η Οδηγία 2002/58 συμπληρώθηκε με την Οδηγία 2009/136[40], ενόψει των τεχνολογικών εξελίξεων στον τομέα των ηλεκτρονικών επικοινωνιών.
Η συμπεριφορά των χρηστών του διαδικτύου άρχισε να αλλάζει τον τρόπο λειτουργίας των διαδικτυακών διαφημίσεων, οπότε κατέστη αναγκαία η εισαγωγή ρυθμίσεων για την υποχρεωτική παροχή σαφούς και εκτενούς πληροφόρησης σχετικά με την *"αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό"*. Ακόμα[41], η Οδηγία 2009/136 εισήγαγε την απαίτηση της προηγούμενης συγκατάθεσης του συνδρομητή/χρήστη για την αποθήκευση πληροφοριών σχετικών με υλικό που χρησιμοποιούν οι χρήστες ή την απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες. Τέτοιες πληροφορίες είναι τα cookies, γι' αυτό και η Οδηγία 2009/136 είναι γνωστή και ως "Cookies Directive".

3.3.1. Ο Ν. 4070/2012

Οι διατάξεις της Οδηγίας 2009/136 ενσωματώθηκαν στην ελληνική έννομη τάξη με τον Ν. 4070/2012, ο οποίος τροποποίησε τον Ν. 3471/2006. Προβλέφθηκαν ρυθμίσεις σχετικές με τις τεχνολογίες όπως είναι τα cookies και συγκεκριμένα εισήχθη η απαίτηση της ειδικής συγκατάθεσης προκειμένου να εγκατασταθούν στον τερματικό εξοπλισμό του χρήστη τέτοιου είδους τεχνολογίες: *"Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του μετά από σαφή και εκτενή ενημέρωση"*[42].

---

40 Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 , για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32009L0136

41 Με προσθήκες που πραγματοποιήθηκαν στο στο άρθρο 5 παράγραφος 3 της Οδηγίας 2002/58, δυνάμει του άρθρου 2 της Οδηγίας 2009/136.

42 Με την προσθήκη που πραγματοποιήθηκε στο άρθρο 4 του ν. 3471/2006, δυνάμει του άρθρου170 του ν. 4070/2012.

4. ΑΡΧΕΣ ΚΑΙ ΝΟΜΙΜΟΙ ΛΟΓΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ

4.1. Νομοθετικές προβλέψεις

Οι κανόνες του ΓΚΠΔ ισχύουν για όλα τα ζητήματα που αφορούν την επεξεργασία προσωπικών δεδομένων, ωστόσο ο ΓΚΠΔ δεν εξειδικεύει τις αρχές και τους νόμιμους λόγους για την επεξεργασία των προσωπικών δεδομένων στο πεδίο των ηλεκτρονικών επικοινωνιών. Το πεδίο αυτό ρυθμίζει η Οδηγία e-Privacy όπως ισχύει με τις τροποποιήσεις της. Η Οδηγία e-Privacy είναι ειδική (lex specialis) ως προς τον ΓΚΠΔ, συμπληρώνοντάς[43] τον σε όσα ζητήματα δεν ρυθμίζονται από αυτόν.

Με βάση το ισχύον νομοθετικό πλαίσιο, όπως περιγράφηκε ανωτέρω, η επεξεργασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες είναι νόμιμη και επιτρέπεται τηρουμένων των αρχών που διέπουν την επεξεργασία των προσωπικών δεδομένων, οι οποίες καταγράφονται στο άρθρο 5 του ΓΚΠΔ.

Η Οδηγία e-Privacy δεν αποτυπώνει γενικές αρχές επεξεργασίας, παρά μόνο για την επεξεργασία δεδομένων κίνησης και θέσης, στο άρθρο 6, οι οποίοι έχουν αποτυπωθεί και στο άρθρο 6 του Ν. 3471/2006. Στο άρθρο 6 παρ. 1 της Οδηγίας αποτυπώνονται οι αρχές της αναγκαιότητας και της περιορισμένης διάρκειας της επεξεργασίας, οι οποίες αποτελούν εκφάνσεις της αρχής της αναλογικότητας. Αυτές επιτάσσουν τα δεδομένα "*να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας*".

Εντούτοις, ο εθνικός μας Ν.3471/2006 στο άρθρο 5 θεσπίζει γενικότερους κανόνες, αποτυπώνοντας τις γενικές αρχές επεξεργασίας των προσωπικών δεδομένων, προσαρμοσμένες στο πλαίσιο της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών[44].

Η πρώτη αρχή που καταγράφεται στην παρ. 1 του άρθρου 5 είναι αυτή του σκοπού: η επεξεργασία "*πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των*

[43] Άρθρο 1 παρ. 2 Οδηγίας 2002/58
[44] Αιτιολογική Έκθεση 3471/2006

σκοπών της". Στην παρ. 2 του άρθρου 5 αποτυπώνεται η αρχή της νομιμότητας της επεξεργασίας: η επεξεργασία είναι νόμιμη και επιτρέπεται όταν ο συνδρομητής/χρήστης έχει δώσει τη συγκατάθεσή του κατόπιν κατάλληλης ενημέρωσης (άρθρο 5 παρ. 2 α) και όταν η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης (άρθρο 5 παρ. 2 β). Στην παρ. 4 του άρθρου 5 αποτυπώνεται η αρχή της ελαχιστοποίησης των δεδομένων, με την απαίτηση για "*επεξεργασία όσο το δυνατόν λιγότερων δεδομένων*" κατά τον σχεδιασμό και την επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων.

4.2. Για ποιους λόγους επιτρέπεται η επεξεργασία

Ως γενικό κανόνα η Οδηγία e-Privacy θέτει το απόρρητο των επικοινωνιών, με την απαγόρευση της ακρόασης, υποκλοπής, αποθήκευσης ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης (Άρθρο 5 παρ. 1 Οδηγίας 2002/58). Ο κανόνας τίθεται με τις επιφυλάξεις (ενδεικτικά): α) της τεχνικής αποθήκευσης που είναι αναγκαία για τη διαβίβαση επικοινωνίας (Άρθρο 5 παρ. 1 Οδηγίας 2002/58), β) της καταγραφής συνδιαλέξεων και των συναφών δεδομένων κίνησης κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα (Άρθρο 5 παρ. 2 Οδηγίας 2002/58), γ) της τεχνικής φύσεως αποθήκευση ή πρόσβαση σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό διενέργεια ή η διευκόλυνση της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών την οποία έχει ζητήσει ρητά ο χρήστης (Άρθρο 5 παρ. 3 Οδηγίας 2002/58). δ) Όσον αφορά την "*εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας*", η επεξεργασία των δεδομένων κίνησης είναι επιτρεπτή μόνο εφόσον ο συνδρομητής/χρήστης έχει δώσει τη συγκατάθεσή του, δοθείσης της δυνατότητας να την ανακαλέσει οποτεδήποτε (άρθρο 6 παρ. 3 της Οδηγίας e-Privacy και άρθρο 6 παρ. 3 του Ν.3471/2006). ε) Ακόμα, η επεξεργασία των δεδομένων κίνησης είναι επιτρεπτή "για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων" (άρθρο 6 παρ. 2 της Οδηγίας e-Privacy και άρθρο 6 παρ. 2 του Ν.3471/2006).

Η Οδηγία e-Privacy, ως μέρος της συνολικής μεταρρύθμισης του κανονιστικού πλαισίου των ηλεκτρονικών επικοινωνιών που επιχειρήθηκε εκείνη την εποχή, στόχο είχε την εναρμόνιση κανόνων για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στο πλαίσιο

της δυναμικής εξέλιξης της σχετικής αγοράς. Σημείωσε αξιόλογη πρόοδο με την αναγνώριση των δυνατοτήτων επεξεργασίας των δεδομένων κίνησης και θέσης, προσπαθώντας να επιτύχει την αρμονική συνύπαρξη των συμφερόντων της αγοράς με αυτά των χρηστών-υποκειμένων των προσωπικών δεδομένων[45].

[45] Λ. Μήτρου (2004) *Η νέα Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*, ΔΙΤΕ (π. ΔΙΜΕΕ) 3/2004

5. ΚΑΝΟΝΙΣΜΟΣ E-PRIVACY

5.1. Στρατηγική Digital Single Market

Στο πλαίσιο της στρατηγικής Digital Single Market (Ψηφιακή Ενιαία Αγορά)[46] της ΕΕ, τον Μάιο του 2015, η Ευρωπαϊκή Επιτροπή ανακοίνωσε την πρόθεση εξασφάλισης υψηλού πεδίου προστασίας για τα δεδομένα προσωπικού χαρακτήρα, με την υλοποίηση του ΓΚΠΔ, και κατόπιν τούτου την επαναξιολόγηση του νομοθετικού πλαισίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

5.1.1. Ευρωπαϊκός Κώδικας Ηλεκτρονικών Επικοινωνιών

Υπό το πρίσμα της στρατηγικής αυτής, τον Οκτώβριο του 2016, η Ευρωπαϊκή Επιτροπή υπέβαλλε πρόταση Οδηγίας *"για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών"*[47], με στόχο την επανεξέταση και αναδιατύπωση τεσσάρων Οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορούσαν το κανονιστικό πλαίσιο των ηλεκτρονικών επικοινωνιών, σε ένα ενιαίο κείμενο. Ο Κώδικας υιοθετήθηκε[48] τον Δεκέμβριο του 2018.

Η Οδηγία e-Privacy δεν αποτέλεσε μέρος της πρότασης, για το λόγο ότι εκείνη την περίοδο βρισκόταν εν αναμονή η υιοθέτηση της εφαρμογής του ΓΚΠΔ, προς διασφάλιση κανονιστικής συνεκτικότητας. Ωστόσο, προετοίμασε πρόσφορο έδαφος για την αναθεώρηση και της Οδηγίας e-Privacy, καθώς συμπεριέλαβε στο πεδίο εφαρμογής της τους παρόχους OTT, λαμβανομένης υπόψη της επιτακτικής ανάγκης να αποτυπωθούν κανόνες που θα ανταποκρίνονται στις

---

46 Ευρωπαϊκή Επιτροπή (2015) *ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ Στρατηγική για την ψηφιακή ενιαία αγορά της Ευρώπης*, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A52015DC0192

47 Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση), διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52016PC0590

48 Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση)Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018L1972

τεχνολογικές εξελίξεις και θα έχουν ισχύ στους "νέους παίκτες" της αγοράς.

5.2. Πρόταση Κανονισμού e-Privacy

Αφού ψηφίστηκε ο ΓΚΠΔ τον Απρίλιο του 2016, τον Ιανουάριο του 2017 η Ευρωπαϊκή Επιτροπή υπέβαλλε Πρόταση Κανονισμού[49] "*για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες)*" (εφεξής η "Πρόταση Κανονισμού").

Πράγματι, σε συνάρτηση με τα ανωτέρω, η πρόταση Κανονισμού χρησιμοποιεί τους ορισμούς[50] του Κώδικα Ηλεκτρονικών Επικοινωνιών.

Έχει υποστηριχθεί[51] ότι, επειδή η Οδηγία e-Privacy χρησιμοποιεί τους ορισμούς των καταργούμενων οδηγιών που αντικαταστάθηκαν από τον Κώδικα Ηλεκτρονικών Επικοινωνιών, αυτό σημαίνει διεύρυνση του πεδίου εφαρμογής της, ώστε να ισχύει και για τους παρόχους ΟΤΤ. Ωστόσο, όπως αναφέρθηκε ανωτέρω, η Οδηγία e-Privacy δεν αποτέλεσε μέρος των καταργούμενων οδηγιών με τον Κώδικα Ηλεκτρονικών Επικοινωνιών, κάτι που διαφαίνεται και στα παραρτήματά του, όπου αναγράφονται αναλυτικά οι τροποποιήσεις που αυτός εισήγαγε. Όπως και να έχει, το μόνο σίγουρο είναι ότι υφίσταται ανακολουθία στο κανονιστικό πλαίσιο, η οποία θα συνεχίσει για όσο διάστημα δεν αναθεωρείται η Οδηγία e-Privacy.

Η Πρόταση Κανονισμού συνοδεύτηκε από δύο επιπλέον κείμενα της Ευρωπαϊκής Επιτροπής,

---

49 Πρόταση ΚΑΝΟΝΙΣΜΟΣ 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/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52017PC0010

50 των όρων «δίκτυο ηλεκτρονικών επικοινωνιών», «υπηρεσίες ηλεκτρονικών επικοινωνιών», «υπηρεσίες διαπροσωπικών επικοινωνιών», «υπηρεσίες διαπροσωπικών επικοινωνιών βάσει αριθμών», «υπηρεσίες διαπροσωπικών επικοινωνιών ανεξαρτήτως αριθμών», «τελικός χρήστης» και «κλήση», βλ. άρθρο 4 παρ. 1 β' της πρότασης Κανονισμού

51 R. Barcelo, M.Buckwell (2018) *New European Electronic Communications Code means the application of the ePrivacy Directive to OTTs,* iapp, διαθέσιμο εδώ: https://iapp.org/news/a/new-european-electronic-communications-code-means-the-application-of-the-eprivacy-directive-to-otts/

το εκ των υστέρων πρόγραμμα βελτίωσης της καταλληλότητας και της αποδοτικότητας του κανονιστικού πλαισίου της Οδηγίας e-Privacy («αξιολόγηση REFIT»)[52], και την εκτίμηση επιπτώσεων[53] που διενεργήθηκε παράλληλα προς την αξιολόγηση REFIT. Η αξιολόγηση κατέληξε στο ότι η Οδηγία e-Privacy δεν πέτυχε πλήρως τους στόχους της. Οι κανόνες της κρίθηκαν αναποτελεσματικοί ως προς την επίτευξη της προσδοκώμενης απαίτησης για προστασία της ιδιωτικής ζωής, απαίτηση τόσο των φυσικών όσο και των νομικών προσώπων. Στην αναποτελεσματικότητα αυτή θεωρήθηκε ότι έχει συντελέσει και ο κατακερματισμός στον τρόπο εφαρμογής της Οδηγίας από κάθε κράτος-μέλος. Ταυτόχρονα, αναδείχθηκε η προστιθέμενη αξία της ΕΕ στη ρύθμιση του εν λόγω τομέα, λόγω της διασυνοριακής φύσης της αγοράς των ηλεκτρονικών επικοινωνιών και εν γένει του Διαδικτύου, η οποία επιτάσσει ενιαία ρύθμιση σε επίπεδο ΕΕ. Ωστόσο, διαπιστώθηκε ότι οι στόχοι της Οδηγίας e-Privacy, ήτοι 1. η εξασφάλιση ισοδύναμου στην ΕΕ επιπέδου προστασίας του δικαιώματος της ιδιωτικής ζωής και της εμπιστευτικότητας όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών και 2. η διασφάλιση της ελεύθερης κυκλοφορίας στην ΕΕ των δεδομένων προσωπικού χαρακτήρα και του τερματικού εξοπλισμού, παραμένουν σχετικοί.

Κατά την εκτίμηση των επιπτώσεων κρίθηκε ότι υφίσταται περιθώριο για απλούστευση των κανόνων της Οδηγίας e-Privacy. Εξετάστηκαν πέντε επιλογές για την αναθεώρηση του νομοθετικού πλαισίου, διαβαθμισμένες, με την πρώτη επιλογή να αποτελείται από "soft law" μέτρα, μη νομοθετικά, που θα ενθαρρύνουν την αυτορρύθμιση του τομέα, τις υπόλοιπες τρεις να προτείνουν περιορισμένη/μέτρια/εκτεταμένη ενίσχυση του επιπέδου προστασίας του δικαιώματος της ιδιωτικής ζωής και της εμπιστευτικότητας και αντίστοιχη εναρμόνιση. Η πέμπτη επιλογή ήταν η κατάργηση της Οδηγίας e-Privacy, ώστε ο τομέας να ρυθμίζεται από τον ΓΚΠΔ. Η επιλογή που τελικά προτιμήθηκε ήταν η τρίτη, αυτή της μέτριας ενίσχυσης και εναρμόνισης.

---

52 Ευρωπαϊκή Επιτροπή (2017) *COMMISSION STAFF WORKING DOCUMENT Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC Accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0005

53 Ευρωπαϊκή Επιτροπή (2017) *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, διαθέσιμο εδώ: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications

5.2.1 Επιλογή νομικής πράξης: Κανονισμός

Ως νομική πράξη για την αντικατάσταση της Οδηγίας e-Privacy επιλέχθηκε ο Κανονισμός. Οι Κανονισμοί είναι δεσμευτικά νομοθετικά κείμενα και έχουν γενική ισχύ και άμεση εφαρμογή στα κράτη μέλη της ΕΕ, διασφαλίζοντας ένα ομοιόμορφο και οριζόντιο πλαίσιο προστασίας. Μάλιστα η συγκεκριμένη επιλογή επικροτήθηκε και από την Ομάδα Εργασίας του άρθρου 29[54], η οποία επεσήμανε ότι πέρα από τον κατακερματισμό των κανόνων, θα αποφευχθεί και η τυχόν ασάφεια για τις εποπτικές αρχές και τους οργανισμούς, αλλά και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων[55], που τόνισε την διασφάλιση ίσων όρων ανταγωνισμού για τους οργανισμούς.

5.2.2 Αλληλεπίδραση της Πρότασης Κανονισμού με τον ΓΚΠΔ

Ο ΓΚΠΔ, όπως είδαμε, δεν ρυθμίζει τα ζητήματα της προστασίας των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες. Προτάθηκε λοιπόν η υιοθέτηση Κανονισμού, ο οποίος θα είναι ειδικός (lex specialis) ως προς τον ΓΚΠΔ όσον αφορά τους κανόνες που σχετίζονται με προσωπικά δεδομένα, συμπληρώνοντάς τον, παράλληλα, σε όσα ζητήματα δεν ρυθμίζονται από αυτόν[56]. Γι' αυτό είναι σημαντικό να επιτευχθεί μεταξύ των δύο Κανονισμών συνοχή στο επίπεδο προστασίας των προσωπικών δεδομένων.

Η Πρόταση Κανονισμού περιέχει διατάξεις που αφορούν όχι μόνο την επεξεργασία προσωπικών δεδομένων, αλλά και την προστασία του απορρήτου των δεδομένων ηλεκτρονικών επικοινωνιών και των πληροφοριών που σχετίζονται με τον τερματικό εξοπλισμό, δηλαδή τη συσκευή του χρήστη. Καλύπτει επομένως ευρύτερο φάσμα δεδομένων από τον ΓΚΠΔ, καθώς αφορά και δεδομένα μη προσωπικού χαρακτήρα. Γι' αυτό και έχει λεχθεί[57] ότι χωρίς τον Κανονισμό e-Privacy, το ευρωπαϊκό νομοθετικό πλαίσιο προστασίας του

---

54 Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2017) *Γνώμη 01/2017 σχετικά με την πρόταση κανονισμού για τον κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (2002/58/ΕΚ)*, διαθέσιμη στο: https://www.lawspot.gr/sites/default/files/misc/misc_legal/wp247_el.pdf

55 Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2017) *Γνώμη 06/2017 για την Πρόταση Κανονισμού e-Privacy*, διαθέσιμη στο: https://service.betterregulation.com/document/289246

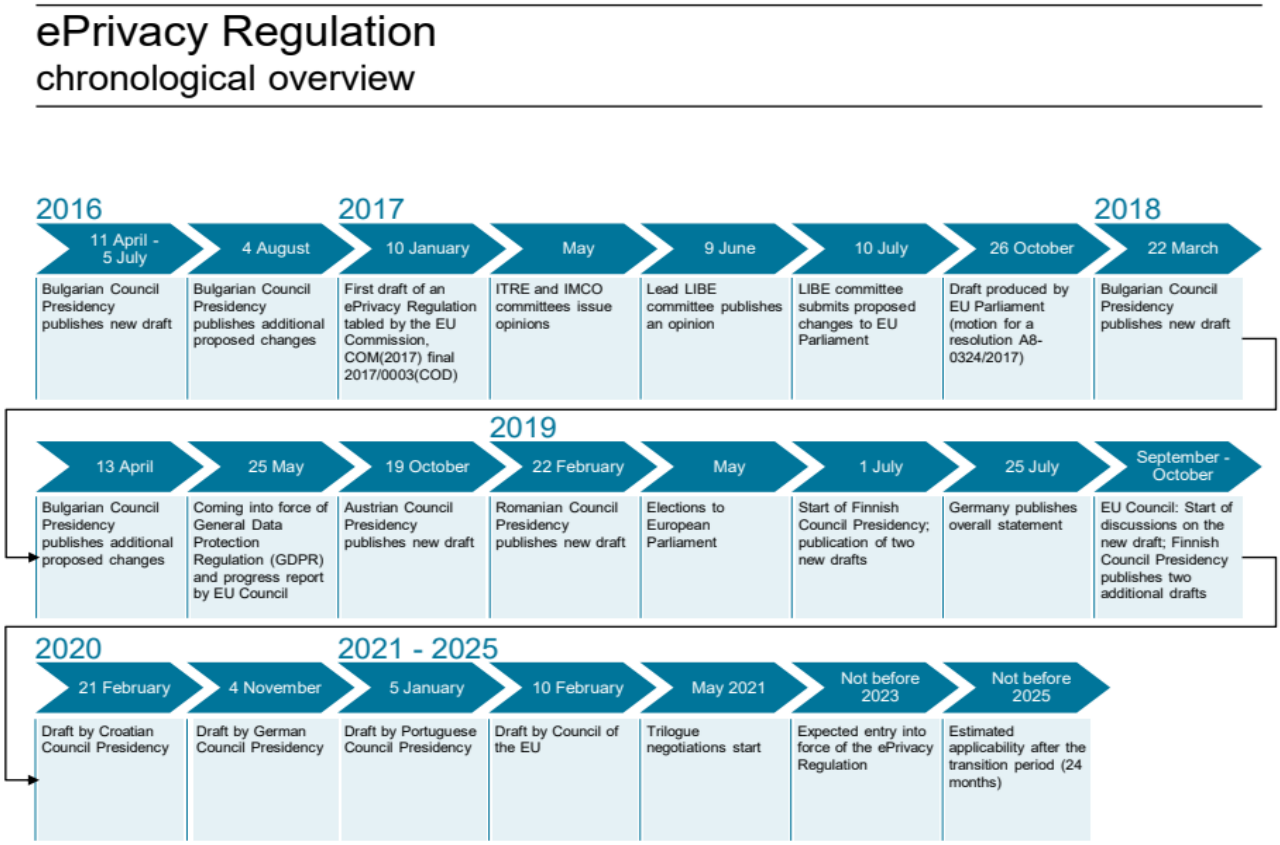
56 1.2 της Αιτιολογικής Έκθεσης της Πρότασης Κανονισμού

57 Giovanni Buttarelli (2017) *The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?*, 3 Eur. Data Prot. L. Rev. 155

απορρήτου και της προστασίας δεδομένων είναι ανολοκλήρωτο.

5.2.3 Η πορεία της Πρότασης Κανονισμού

Η Πρόταση Κανονισμού έχει επαναδιατυπωθεί πολλάκις από το 2017, περνώντας διαδοχικά από αρκετές Προεδρίες του Συμβουλίου της ΕΕ, κάθε μία από τις οποίες τροποποιούσε το κείμενο της Πρότασης.



Γράφημα χρονολογικής επισκόπησης της Πρότασης Κανονισμού, Πηγή: https://cms.law/

Είναι μάλιστα χαρακτηριστικό ότι κάθε Προεδρία με τις προτάσεις που υπέβαλλε υιοθετούσε αποκλίνουσες προσεγγίσεις ως προς τις ρυθμίσεις της Πρότασης Κανονισμού, με άλλες να χαρακτηρίζονται πιο προστατευτικές της ιδιωτικότητας και άλλες πιο φιλικές προς την ψηφιακή βιομηχανία.

Στο παρόν στάδιο η προτεινόμενη ενοποιημένη έκδοση της Πρότασης Κανονισμού της 10ης

Φεβρουαρίου 2021[58], που υιοθετήθηκε επί Πορτογαλικής Προεδρίας, βρίσκεται στο στάδιο των τριμερών διαπραγματεύσεων με το Ευρωπαϊκό Κοινοβούλιο και την Ευρωπαϊκή Επιτροπή, με στόχο την οριστικοποίηση του κειμένου και την ψήφισή του.

5.2.4 Στόχος της Πρότασης Κανονισμού

Είναι σημαντικό να αποσαφηνιστεί σε αυτό το σημείο αυτό ότι η Πρόταση Κανονισμού στοχεύει στην προστασία των θεμελιωδών δικαιωμάτων των φυσικών προσώπων, αυτών της ιδιωτικής ζωής και της προστασίας δεδομένων προσωπικού χαρακτήρα (άρθρο 1), και όχι στην προστασία της αγοράς των ηλεκτρονικών επικοινωνιών, κάτι που έχει επικροτηθεί από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων[59].

Φιλοδοξία της Πρότασης Κανονισμού είναι να αποκτήσουν τα υποκείμενα τον πλήρη έλεγχο των δεδομένων των επικοινωνιών τους και της ψηφιακής δραστηριότητάς τους, βελτιώνοντας την ασφάλεια και το απόρρητο των επικοινωνιών, καθορίζοντας σαφείς κανόνες για τις τεχνολογίες ιχνηλάτησης, όπως είναι τα cookies και εγκαθιδρύοντας διαφανείς διατάξεις[60]. Με απλά λόγια, στόχος είναι να αποκλείεται η μη εξουσιοδοτημένη πρόσβαση στις συσκευές των χρηστών και στα δεδομένα τους. Ωστόσο, παρά την εστίαση που γίνεται στην προστασία των δεδομένων των φυσικών προσώπων, οι οικονομικοί παράγοντες και τα οικονομικά συμφέροντα είναι αυτά που καθυστερούν την ψήφιση του Κανονισμού, όπως θα δούμε κατωτέρω.

5.2.5. Πεδίο εφαρμογής της Πρότασης Κανονισμού

Όπως αναφέρεται στην αιτιολογική σκέψη 1 της Πρότασης Κανονισμού, η νομοθετική κατοχύρωση του απόρρητου χαρακτήρα των επικοινωνιών περιλαμβάνει κάθε είδους ιδιωτική επικοινωνία, με όποιον τρόπο και αν διεξάγεται. Αυτή η παραδοχή, καίτοι αυτονόητη,

---

58 Πρόταση (10.01.2021) ΚΑΝΟΝΙΣΜΟΣ 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/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), διαθέσιμο εδώ: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

59 Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2017), ό.α.

60 "bring transparency to the often opaque world of personal data processing" Giovanni Buttarelli (2017), ό.α.

τοποθετείται στην κορυφή της Πρότασης Κανονισμού, καθώς λόγω του ολοένα εξελισσόμενου τεχνολογικού τοπίου στον τομέα των ηλεκτρονικών επικοινωνιών, έχουν δημιουργηθεί κενά στην προστασία που παρέχει η Οδηγία e-Privacy.

Ο Κανονισμός θα εφαρμόζεται σε όλες τις κατηγορίες των ηλεκτρονικών επικοινωνιών, τόσο στις παραδοσιακές μορφές ηλεκτρονικής επικοινωνίας, όπως αυτή των παρόχων τηλεφωνίας και ηλεκτρονικού ταχυδρομείου, όσο και στις επιφυείς υπηρεσίες, οι οποίες στην παρούσα φάση δεν υπόκεινται στο πεδίο εφαρμογής της Οδηγίας. Αυτές οι Over the Top (OTT) επικοινωνίες παρέχονται με την μεταφορά δεδομένων μέσω του διαδικτύου. Τέτοιες είναι οι εφαρμογές άμεσης ανταλλαγής μηνυμάτων μέσω διαδικτύου και οι διάχυτες υπηρεσίες φωνής μέσω πρωτοκόλλου διαδικτύου VoIP (Voice over Internet Protocol), όπως για παράδειγμα το FaceTime, το WhatsApp, το Skype, το Messenger του Facebook, κ.ά.

Ο Κανονισμός θα έχει εφαρμογή και σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό τελικών χρηστών καθώς και σε πληροφορίες σχετικές με αυτόν τον εξοπλισμό, όπως είναι για παράδειγμα τα δεδομένα τοποθεσίας που εκπέμπονται από τα smartphones. Ακόμα, ο Κανονισμός θα έχει εφαρμογή και στην επικοινωνία μέσω του Διαδικτύου των Πραγμάτων (IoT, Internet of Things), που διεξάγεται μέσω διασυνδεδεμένων συσκευών και μηχανών (machine to machine), οι οποίες συνήθως έχουν ενσωματωμένους αισθητήρες, αποθηκεύοντας και μεταφέροντας ποικίλες πληροφορίες που συχνά περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα. Η προστασία του απορρήτου των επικοινωνιών εκτείνεται και στις επικοινωνίες που διεξάγονται μέσω δημοσίως διαθέσιμων δικτύων, όπως hotspots πόλεων, καταστημάτων, αλλά όχι στα ιδιωτικά – κλειστά δίκτυα, όπως για παράδειγμα κάποιας εταιρείας.

Βλέπουμε λοιπόν ότι ο απόρρητος χαρακτήρας των επικοινωνιών πρέπει να διασφαλίζεται και να προστατεύεται ανεξαρτήτως του σκοπού της επικοινωνίας και ανεξαρτήτως της χρησιμοποιούμενης τεχνολογίας. Γι' αυτό και στο πεδίο εφαρμογής της Πρότασης Κανονισμού εμπίπτουν και οι παρεπόμενες υπηρεσίες που προσαρτώνται σε κάποια άλλη υπηρεσία, όπως είναι για παράδειγμα το chat σε ένα παιχνίδι[61].

Τοιουτοτρόπως, στο πεδίο εφαρμογής του Κανονισμού e-Privacy θα εμπίπτουν όλα τα δεδομένα

[61] Αιτιολογική Σκέψη 11αα

των ηλεκτρονικών επικοινωνιών, τόσο οι πληροφορίες του περιεχομένου της επικοινωνίας, όσο και τα μεταδεδομένα της επικοινωνίας. Σχετικά με τα τελευταία, έχει λεχθεί ότι έχουν "*διφυή υπόσταση*"[62], αφού όχι μόνο συνιστούν προσωπικά δεδομένα, αλλά και "*τηλεπικοινωνιακά δεδομένα*". Ο ορισμός των δεδομένων επικοινωνίας θα πρέπει λοιπόν να είναι ευρύς και ουδέτερος[63]. Αμφότερα περιεχόμενο και μεταδεδομένα μπορούν να οδηγήσουν στην αποκάλυψη ιδιαιτέρως προσωπικών ευαίσθητων πληροφοριών και εξαγωγή συμπερασμάτων για το υποκείμενο των δεδομένων. Ως εκ τούτου, αυτά θα πρέπει να είναι εμπιστευτικά (άρθρο 5), γενικώς απαγορευομένης κάθε παρεμβολής και επεξεργασίας, εκτός εάν επιτρέπεται βάσει των εξαιρέσεων που ορίζει ο ίδιος ο Κανονισμός.

Παρά την γενική απαγόρευση της επεξεργασίας, η Πρόταση Κανονισμού προβλέπει διευρυμένες δυνατότητες επεξεργασίας δεδομένων ηλεκτρονικών επικοινωνιών, οι οποίες δύνανται τα αποβούν χρήσιμες για το κοινωνικό σύνολο και τις επιχειρήσεις. Διαφαίνεται έτσι η ισορροπία που επιχειρείται να επιτευχθεί μεταξύ αφενός της προστασίας του απορρήτου της επικοινωνίας των χρηστών και αφετέρου της ανάπτυξης των καινοτόμων τεχνολογικών εφαρμογών.

Για παράδειγμα, η επεξεργασία των μεταδεδομένων επιτρέπεται για ανθρωπιστικούς σκοπούς, για την προστασία ζωτικών συμφερόντων, όπως σε περίπτωση επιδημιών ή κάποιας έκτακτης ανάγκης. Επίσης, επιτρέπεται για σκοπούς επιστημονικής έρευνας, καθώς και για στατιστικούς σκοπούς, με την διασφάλιση της κρυπτογράφησης ή της ψευδωνυμοποίησης των δεδομένων.

62 Γρ. Τσόλιας (2004), ό.α.

63 Όπως αναφέρει στην Εισαγωγική Σκέψη 14

6. ΚΑΝΟΝΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΟΥ ΘΕΤΕΙ Η ΠΡΟΤΑΣΗ ΚΑΝΟΝΙΣΜΟΥ E-PRIVACY

6.1. Η διατύπωση της γενικής απαγόρευσης επεξεργασίας - Άρθρο 5

Με αφετηρία τη δήλωση περί απαίτησης εμπιστευτικότητας των δεδομένων των ηλεκτρονικών επικοινωνιών, σε συνάφεια με τις επιταγές του άρθρου 7 του Χάρτη Θεμελιωδών Δικαιωμάτων[64], η Πρόταση Κανονισμού στο άρθρο 5 θέτει ως γενικό κανόνα την απαγόρευση της επεξεργασίας των δεδομένων των επικοινωνιών, με εξαίρεση τις περιπτώσεις επιτρεπόμενης επεξεργασίας που προβλέπονται στην ίδια την Πρόταση Κανονισμού.

Ιδίως εν όψει του γεγονότος ότι η ολοένα εξελισσόμενη τεχνολογία επιτρέπει ποικίλες δυνατότητες παρεμβολής στις επικοινωνίες[65], είναι σημαντικό να οριοθετηθούν κανόνες επεξεργασίας, κάτι που επιχειρεί η Πρόταση Κανονισμού.

Ωστόσο, παρά την διατύπωση της γενικής απαγόρευσης της επεξεργασίας, η Πρόταση Κανονισμού προβλέπει διευρυμένες δυνατότητες επεξεργασίας, ο σκοπός των οποίων προσδιορίζεται στα επόμενα άρθρα. Μάλιστα, στην αιτιολογική σκέψη 17 αναφέρει πως η επεξεργασία των μεταδεδομένων μπορεί να αποβεί χρήσιμη "*για επιχειρήσεις, καταναλωτές καθώς και για την κοινωνία ως σύνολο*". Για παράδειγμα, η επεξεργασία μεταδεδομένων για ανίχνευση της κίνησης σε διάφορες τοποθεσίες θα μπορούσε να συμβάλλει στην αναβάθμιση των υποδομών μέσων μετακίνησης. Στην ουσία εισάγονται περισσότερες - σε σχέση με το ισχύον καθεστώς - δυνατότητες επεξεργασίας για τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, με κύριο άξονα τη συγκατάθεση του τελικού χρήστη.

Η συγκατάθεση του τελικού χρήστη λοιπόν αποτελεί την κύρια νομική βάση επεξεργασίας της Πρότασης Κανονισμού. Στην αιτιολογική σκέψη 3 και στο άρθρο 4α ορίζει ότι ισχύει η έννοια της συγκατάθεσης κατά τα οριζόμενα στον ΓΚΠΔ, σύμφωνα με τον οποίο, προϋποθέσεις της έγκυρης συγκατάθεσης είναι να παρέχεται ρητά, με τρόπο αδιαμφισβήτητο, ειδικώς, εν πλήρει επιγνώσει, ελεύθερα, και να μπορεί να ανακληθεί ανά πάσα στιγμή.

---

64 Αιτιολογική Σκέψη 1

65 Βλ. Αιτιολογική Σκέψη 15

6.2 Επεξεργασία δεδομένων ηλεκτρονικών επικοινωνιών – Άρθρο 6

Το άρθρο 6 περιγράφει τις νομικές βάσεις επεξεργασίας των δεδομένων ηλεκτρονικών επικοινωνιών με τη μορφή γενικών κανόνων. Οι πάροχοι των υπηρεσιών ηλεκτρονικών επικοινωνιών μπορούν να επεξεργάζονται δεδομένα ηλεκτρονικών επικοινωνιών μόνο εάν είναι αναγκαίο για[66]: την παροχή μίας υπηρεσίας, για τους σκοπούς ασφάλειας των δικτύων και των υπηρεσιών καθώς και για τον εντοπισμό τεχνικών βαβλών ή κινδύνων ασφαλείας ή επιθέσεων στα δίκτυα, τις υπηρεσίες ή τον τερματικό εξοπλισμό των χρηστών, καθώς και για τη συμμόρφωση με νομική υποχρέωση στην οποία υπόκειται ο πάροχος. Διαφαίνεται η αρχή της αναγκαιότητας που θέτει η Πρόταση Κανονισμού, με την επεξεργασία να επιτρέπεται μόνο εφόσον κρίνεται αναγκαία προς την επίτευξη κάποιου σκοπού. Στην παρ. 2 διατυπώνονται και περαιτέρω γενικές αρχές επεξεργασίας, αυτή της συγκεκριμένης διάρκειας και η αρχή του σκοπού.

6.3 Επεξεργασία περιεχομένου ηλεκτρονικών επικοινωνιών - Άρθρο 6α

Το άρθρο 6α θέτει τις προϋποθέσεις της επιτρεπόμενης επεξεργασίας του περιεχομένου των ηλεκτρονικών επικοινωνιών, οι οποίες είναι οι εξής: Πρώτον, η περίπτωση που ο τελικός χρήστης έχει ζητήσει, παρέχοντας τη συγκατάθεσή του, την παροχή μίας υπηρεσίας για ιδιωτική χρήση και εφόσον δεν παραβιάζονται θεμελιώδη δικαιώματα άλλου προσώπου. Δεύτερον, η περίπτωση που ο τελικός χρήστης έχει δώσει τη συγκατάθεσή του στην επεξεργασία του περιεχομένου των επικοινωνιών του για κάποιον συγκεκριμένο σκοπό.

Το περιεχόμενο των ηλεκτρονικών επικοινωνιών μπορεί να αποκαλύψει άκρως ευαίσθητες πτυχές της ιδιωτικής ζωής, επομένως η διαφύλαξη της εμπιστευτικότητας αυτού είναι άρρηκτα συνδεδεμένη με τον σεβασμό της ιδιωτικής ζωής που προστατεύεται από το άρθρο 7 του Χάρτη Θεμελιωδών Δικαιωμάτων. Καθίσταται προφανές ότι οποιαδήποτε επεξεργασία του πρέπει να υπόκειται σε αυστηρούς κανόνες, προϋποθέσεις και εγγυήσεις[67]. Στη δεύτερη μάλιστα περίπτωση της επιτρεπόμενης επεξεργασίας απαιτείται η προηγούμενη διενέργεια εκτίμησης επιπτώσεων.

---

66 Άρθρο 6 παρ. 1

67 Βλ. Αιτιολογική Σκέψη 16α

6.4 Επεξεργασία μεταδεδομένων - Άρθρο 6β

Ενώ για την επεξεργασία του περιεχομένου των ηλεκτρονικών επικοινωνιών προβλέπονται μονάχα δύο περιπτώσεις, αντιθέτως για την επεξεργασία των μεταδεδομένων των ηλεκτρονικών επικοινωνιών η Πρόταση Κανονισμού στο άρθρο 6β απαριθμεί περισσότερες περιπτώσεις, οι οποίες μπορούμε να πούμε ότι κατά κύριο λόγο εξυπηρετούν συμφέροντα των παρόχων.

Η Πρόταση Κανονισμού υιοθετεί για τα εξωτερικά στοιχεία τον όρο "μεταδεδομένα", τα οποία ορίζει[68] ως "*τα δεδομένα 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*".

Όπως ακριβώς και το περιεχόμενο των ηλεκτρονικών επικοινωνιών, τα μεταδεδομένα μπορούν εξίσου να αποκαλύπτουν ευαίσθητες πτυχές της ιδιωτικής ζωής, αφού από αυτά απορρέει πληροφοριακό υλικό από το οποίο είναι δυνατό να εξαχθούν ιδιαιτέρως χρήσιμα πορίσματα και πληροφορίες σχετικά με την ιδιωτική ζωή των υποκειμένων της επικοινωνίας. Το ΔΕΕ μάλιστα στην απόφαση Tele2 Sverige AB (C-203/15)[69] έχει διατυπώσει την άποψη ότι τα μεταδεδομένα οδηγούν σε πληροφορίες ισοδύναμης αξίας με αυτές του περιεχομένου των επικοινωνιών.

Οι νομικές βάσεις επεξεργασίας των μεταδεδομένων σύμφωνα με το άρθρο 6β είναι οι ακόλουθες: Οι πάροχοι των υπηρεσιών ηλεκτρονικών επικοινωνιών μπορούν να επεξεργάζονται μεταδεδομένα ηλεκτρονικών επικοινωνιών μόνο εάν: α) η επεξεργασία είναι απαραίτητη για τους σκοπούς διαχείρισης ή βελτιστοποίησης του δικτύου ή για την επίτευξη

---

68 Άρθρο 4 παρ. 3 περ. γ'

69 Απόφαση ΔΕΕ (2016) *Tele2 Sverige AB (C-203/15)*, Σκέψη 99: "*…Τα δεδομένα αυτά παρέχουν τα μέσα για τον προσδιορισμό...του προφίλ των προσώπων περί των οποίων πρόκειται, πληροφορία εξίσου ευαίσθητη, υπό το πρίσμα του δικαιώματος του σεβασμού της ιδιωτικής ζωής, με το περιεχόμενο αυτό καθεαυτό των επικοινωνιών.*"

τεχνικών προδιαγραφών, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης υπηρεσιών ηλεκτρονικών επικοινωνιών, την τιμολόγηση ή τον εντοπισμό δόλιας/καταχρηστικής χρήσης των υπηρεσιών, γ) ο τελικός χρήστης έχει δώσει τη συγκατάθεσή του για την επίτευξη κάποιου συγκεκριμένου σκοπού, δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικών συμφερόντων φυσικών προσώπων, ε) η επεξεργασία μεταδεδομένων θέσης είναι απαραίτητη για επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς, υπό την προϋπόθεση ότι τα δεδομένα είναι ψευδωνυμοποιημένα, ο σκοπός δεν μπορεί να επιτευχθεί με ανωνυμοποιημένα δεδομένα, καθώς και ότι δεν χρησιμοποιούνται για να καθορίσουν τα χαρακτηριστικά του τελικού χρήστης ή για να σκιαγραφήσουν το προφίλ του, ζ) η επεξεργασία είναι απαραίτητη για επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς. Τα δεδομένα των δύο τελευταίων περιπτώσεων μπορούν να υπαχθούν σε επεξεργασία για την παραγωγή ευρωπαϊκών στατιστικών.

6.5 Επεξεργασία μεταδεδομένων για περαιτέρω σκοπούς - Άρθρο 6γ

Το άρθρο 6γ θέτει τις προϋποθέσεις υπό τις οποίες τα μεταδεδομένα μπορούν να τύχουν επεξεργασίας για σκοπούς διαφορετικούς από αυτούς για τους οποίους συλλέχθηκαν. Καταρχάς ο σκοπός της περαιτέρω επεξεργασίας θα πρέπει να είναι συμβατός με τον σκοπό για τον οποίο τα δεδομένα αρχικώς συλλέχθηκαν. Για την αξιολόγηση της συμβατότητας το κείμενο της Πρότασης Κανονισμού παραθέτει κάποια κριτήρια που πρέπει να ληφθούν υπόψη, τα οποία αντιστοίχως απαντώνται και στο κείμενο του ΓΚΠΔ[70] στο σημείο όπου ορίζονται οι προϋποθέσεις περαιτέρω επεξεργασίας. Ο πάροχος θα πρέπει να λαμβάνει υπόψη: τη σχέση μεταξύ των δύο σκοπών επεξεργασίας, το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα, με έμφαση τη σχέση μεταξύ του τελικού χρήστη και του παρόχου, τη φύση των δεδομένων και του σκοπού της περαιτέρω επεξεργασίας, ιδίως όταν θα μπορούσε να οδηγήσει σε αποκάλυψη ευαίσθητων προσωπικών δεδομένων, τις πιθανολογούμενες συνέπειες της περαιτέρω επεξεργασίας ως προς τους τελικούς χρήστες, καθώς και την ύπαρξη κατάλληλων μέτρων προστασίας. Πέρα από την συνδρομή κάποιου εκ των κριτηρίων, η Πρόταση Κανονισμού στην παρ. 2 θέτει περαιτέρω προϋποθέσεις οι οποίες απαιτείται τα τηρούνται προκειμένου να θεωρηθεί νόμιμη η περαιτέρω επεξεργασία των μεταδεδομένων. Θα πρέπει: η περαιτέρω επεξεργασία να μην είναι εφικτό να πραγματοποιηθεί με ανωνυμοποιημένα δεδομένα, να

[70] Στο άρθρο 6 παρ. 4

πραγματοποιείται με ψευδωνυμοποιημένα δεδομένα και τα δεδομένα να μην χρησιμοποιούνται για να καταρτίσουν το προφίλ του χρήστη.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων έχει σχολιάσει[71] ότι ορθότερη θα ήταν η προσέγγιση της γενικής απαγόρευσης επεξεργασίας, με πολύ περιορισμένες, ρητές εξαιρέσεις στην πρόταση της Ευρωπαϊκής Επιτροπής, εκφράζοντας την ανησυχία ότι ο έλεγχος συμβατότητας του περαιτέρω σκοπού επεξεργασίας ενέχει τον κίνδυνο της ανεξέλεγκτης υποκειμενικής κρίσης περί συμβατότητας από τους παρόχους, ώστε αυτοί να δικαιολογήσουν την επεξεργασία μεταδεδομένων.

6.6 Διατήρηση δεδομένων - Άρθρο 7

Στο άρθρο 7 προβλέπεται η διαγραφή ή ανωνυμοποίηση των μεταδεδομένων επικοινωνίας, όταν παύουν να είναι απαραίτητα για τον σκοπό μετάδοσης της επικοινωνίας. Ωστόσο, η πρόβλεψη τελεί υπό επιφύλαξη πολλών εκ των διατάξεων της Πρότασης Κανονισμού, όπως για παράδειγμα υπό την επιφύλαξη της επεξεργασίας για το σκοπό της συμμόρφωσης με νομική υποχρέωση στην οποία υπόκειται ο πάροχος, και της επεξεργασίας μεταδεδομένων θέσης είναι απαραίτητη για επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς.

Επίσης, στην παρ. 4 του άρθρου 7 προβλέπεται, εν είδει ανοικτής εξαίρεσης, η δυνατότητα των κρατών μελών ή της ΕΕ να θεσπίζουν νόμους για τη διατήρηση των μεταδεδομένων ως αναγκαίο μέτρο σε μία δημοκρατική κοινωνία για την διασφάλιση ειδικών δημόσιων συμφερόντων, όπως για σκοπούς εθνικής ασφάλειας, και σκοπούς πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων έχει εκφράσει προβληματισμούς[72] σχετικά με αυτή την ευρεία διατύπωση καθώς δεν θα πρέπει να νοηθεί ότι η Πρόταση Κανονισμού κανονικοποιεί μια γενική και χωρίς διακρίσεις διατήρηση μεταδεδομένων, η οποία δεν ευθυγραμμίζεται με την νομολογία του ΔΕΕ, τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ και την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου.

---

71 Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021) *Δήλωση 03/2021 σχετικά με τον κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*, διαθέσιμο εδώ: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_el

72 Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), ό.α.

Στο αρχικό σχέδιο της Επιτροπής του 2017 της Πρότασης Κανονισμού, στην Αιτιολογική Έκθεση υπήρχε ρητή αναφορά περί μη πρόβλεψης ειδικών διατάξεων που αφορούν τη διατήρηση των δεδομένων. Υπήρχε μονάχα το άρθρο 11 όπου τίθενται οι προϋποθέσεις για τον περιορισμό των δικαιωμάτων, κατά τα πρότυπα του Άρθρου 15 της Οδηγίας e-Privacy, με την ευθυγράμμιση ως προς τους σκοπούς με την αντίστοιχη διάταξη του Άρθρου 23 του ΓΚΠΔ.

6.7 Πληροφορίες τερματικού εξοπλισμού - Άρθρο 8

Στο άρθρο 8 τίθενται οι κανόνες προστασίας των πληροφοριών που σχετίζονται με τον τερματικό εξοπλισμό του τελικού χρήστη. Εύστοχα η Πρόταση Κανονισμού στην αιτιολογική σκέψη 20 εντάσσει τον τερματικό εξοπλισμό των χρηστών των δικτύων ηλεκτρονικών επικοινωνιών και κάθε πληροφορία που συνδέεται με τη χρήση του στην ιδιωτική σφαίρα του τελικού χρήστη[73]. Οι πληροφορίες αυτές εμπίπτουν στο επικοινωνιακό απόρρητο, επομένως η συλλογή και η κάθε είδους επεξεργασία τους πρέπει να διαδραματίζεται εντός οροθετημένων διαφανών κανόνων.

Σκοπός του άρθρου 8 της Πρότασης Κανονισμού είναι να προστατεύσει τους χρήστες από τα εργαλεία ιχνηλάτησης που εισέρχονται και αποθηκεύονται στον τερματικό εξοπλισμό, όπως είναι για παράδειγμα τα cookies, η καταγραφή του αποτυπώματος ή άλλων αναγνωριστικών της συσκευής, όπως και άλλων δεδομένων που αποθηκεύονται σε συσκευές IoT, τα οποία δύνανται να αποθηκεύουν δεδομένα και να παρακολουθούν τη συμπεριφορά των χρηστών στο Διαδίκτυο.

Το κείμενο χαρακτηρίζεται από τεχνολογική ουδετερότητα, καθώς εντάσσει στο

[73] Πάντως ο τερματικός εξοπλισμός των χρηστών κι οι πληροφορίες που συνδέονται με αυτόν προστατεύονται ήδη από Οδηγία 2002/58, όπως έχει τροποποιηθεί από την Οδηγία 2009/136, η οποία εμπεριέχει σχετική διάταξη: Άρθρο 5 παρ. 3 "*Τα κράτη μέλη μεριμνούν ώστε η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία.*"

προστατευτικό πεδίο εφαρμογής του κάθε είδους πληροφορία που σχετίζεται με τον τερματικό εξοπλισμό, είτε πρόκειται για προσωπικά είτε για μη προσωπικά δεδομένα[74], καθώς και κάθε είδους δυνατότητα συλλογής/αποθήκευσης/επεξεργασίας αυτών των πληροφοριών.

Ωστόσο, παρά την πρόβλεψη στο άρθρο 8 του κανόνα της απαγόρευσης των δυνατοτήτων επεξεργασίας και αποθήκευσης τέτοιων πληροφοριών, προβλέπεται ευρεία λίστα επιτρεπόμενων εξαιρέσεων. Κάποιες από αυτές, όπως ο σκοπός της παροχής της υπηρεσίας και της λογισμικής αναβάθμισης έχουν τεχνικό πεδίο εφαρμογής. Ωστόσο, σκοπός του συγκεκριμένου άρθρου είναι η επίτευξη ισορροπίας μεταξύ αφενός της προστασίας της ιδιωτικότητας των τελικών χρηστών και αφετέρου της ανάγκης των εταιρειών να αναπτύσσουν τις υπηρεσίες τους μέσω της χρήσης cookies και άλλων ιχνηλατών που δεν κρίνονται παρεμβατικά. Η σημαντικότερη προβλεπόμενη εξαίρεση είναι αυτή της συγκατάθεσης του τελικού χρήστη[75].

Στο σημείο c της παρ. 1 του άρθρου 8 προβλέπεται ότι η επεξεργασία επιτρέπεται εφόσον πρόκειται για παροχή υπηρεσίας που ο τελικός χρήστης έχει αιτηθεί. Αντίστοιχη πρόβλεψη υπάρχει στο τελευταίο εδάφιο της παρ. 3 του άρθρου 5 της Οδηγίας 2002/58, με τη διαφορά ότι ενώ εκεί γίνεται αναφορά σε υπηρεσίες της κοινωνίας της πληροφορίας, η Πρόταση Κανονισμού κάνει λόγο για οποιαδήποτε υπηρεσία, διευρύνοντας εμφανώς το πεδίο εφαρμογής. Η Αιτιολογική Σκέψη 21αα της Πρότασης Κανονισμού δίνει ως παράδειγμα τέτοιων υπηρεσιών την ηλεκτρονική εφημερίδα που χρηματοδοτείται αποκλειστικά από διαφημίσεις. Σε μία τέτοια περίπτωση αυτή η υπηρεσία θα πρέπει να παρέχει στους τελικούς χρήστες σαφείς και ακριβείς πληροφορίες σχετικά με τα cookies και τις συναφείς τεχνολογίες που χρησιμοποιεί, στην τελική κρίση των οποίων απομένει να αποδεχθούν αυτή τη λειτουργία, δίνοντας ουσιαστικά τη συγκατάθεσή τους.

Στο σημείο g της παρ. 1 του άρθρου 8 προβλέπεται η δυνατότητα επεξεργασίας των πληροφοριών που σχετίζονται με τον τερματικό εξοπλισμό για σκοπούς διαφορετικούς από αυτούς για τους οποίους συλλέχθηκαν, παρέχοντας ακόμα περισσότερες δυνατότητες στους παρόχους, υπό την προϋπόθεση βέβαια οι δύο σκοποί να είναι συμβατοί[76]. Και εδώ η Πρόταση

[74] Αιτιολογική Σκέψη 20 τελευταίο εδάφιο
[75] Άρθρο 8 παρ. 1 β'
[76] Βλ. Αιτιολογική Σκέψη 20αα

Κανονισμού καταγράφει τα κριτήρια που πρέπει να λαμβάνονται υπόψη για την αξιολόγηση της συμβατότητας μεταξύ των σκοπών. Αυτά είναι: η σχέση μεταξύ των δύο σκοπών επεξεργασίας, το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα, με έμφαση τη σχέση μεταξύ του τελικού χρήστη και του παρόχου, η φύση των δεδομένων και του σκοπού της περαιτέρω επεξεργασίας, ιδίως όταν θα μπορούσε να οδηγήσει σε αποκάλυψη ευαίσθητων προσωπικών δεδομένων, οι πιθανολογούμενες συνέπειες της περαιτέρω επεξεργασίας ως προς τους τελικούς χρήστες, καθώς και η ύπαρξη κατάλληλων μέτρων προστασίας. Ένας συμβατός σκοπός όμως δεν οδηγεί άνευ ετέρου στην κατάφαση του επιτρεπτού της περαιτέρω επεξεργασίας, αφού η Πρόταση Κανονισμού θέτει περαιτέρω προϋποθέσεις, οι οποίες ουσιαστικά συνιστούν περιορισμούς. Περαιτέρω επεξεργασία, λοιπόν, επιτρέπεται, αφού κριθεί συμβατή, μόνο εφόσον: οι πληροφορίες διαγράφονται ή ανωνυμοποιούνται όταν παύουν να είναι απαραίτητες, η επεξεργασία περιορίζεται σε πληροφορίες που έχουν ψευδωνυμοποιηθεί, καθώς και καθώς και δεδομένου ότι οι πληροφορίες δεν χρησιμοποιούνται για να καθορίσουν τα χαρακτηριστικά του τελικού χρήστη ή για να σκιαγραφήσουν το προφίλ του.

Στο άρθρο 8 παρ. 2 η πρόταση Κανονισμού περιορίζει τις δυνατότητες συλλογής πληροφοριών που εκπέμπονται από τον τερματικό εξοπλισμό των χρηστών προκειμένου να συνδεθούν με άλλες συσκευές ή με εξοπλισμό δικτύου. Και πάλι βλέπουμε ότι η Πρόταση Κανονισμού θέτει γενικό κανόνα απαγόρευσης, με τις επιτρεπόμενες κατ' εξαίρεση περιπτώσεις να έπονται.

Αξιοσημείωτη είναι η αιτιολογική σκέψη 17 στην προηγούμενη εκδοχή της Πρότασης Κανονισμού (2017), η οποία ανέφερε ότι "*τα δεδομένα γεωγραφικής θέσης που δημιουργούνται εκτός του πλαισίου της παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών δεν θα πρέπει να θεωρούνται μεταδεδομένα*", συνδυαστικά με την προγενέστερη διατύπωση του άρθρου 8 παρ. 2β η οποία επέτρεπε την συλλογή πληροφοριών που εκπέμπονται από τερματικό εξοπλισμό, απλά και μόνο εφόσον ο υπεύθυνος για την επεξεργασία οργανισμός έχει ανακοινώσει ευδιακρίτως την συλλογή, τους σκοπούς για τους οποίους γίνεται και τον υπεύθυνο, χωρίς ωστόσο να παρέχει την δυνατότητα αντίρρησης στα υποκείμενα. Με αυτό το σχήμα θα δινόταν η δυνατότητα σε κάποιον οργανισμό να παρακολουθεί τις κινήσεις των υποκειμένων σε δημόσιους χώρους, μέσω της παρακολούθησης των συσκευών του. Δεν γινόταν μάλιστα διαχωρισμός μεταξύ των σκοπών αυτής της μη εξουσιοδοτημένης συλλογής, οι οποίοι ναι μεν μπορεί από τη μία να αφορούσαν μία απλή στατιστική καταμέτρηση, π.χ. της κίνησης σε μία

συγκεκριμένη περιοχή, όπως τους επιβάτες που βρίσκονται σε ένα αεροδρόμιο, ένα εμπορικό κέντρο, ή την μέτρηση της κίνησης στους δρόμους, ωστόσο από την άλλη θα μπορούσαν να οδηγήσουν σε μακροχρόνια παρακολούθηση και αναγνώριση των ατόμων που επισκέπτεται εξακολουθητικά ένα μέρος, με περαιτέρω "*πιο οχληρούς*" σκοπούς αποστολής "*εμπορικών μηνυμάτων σε τελικούς χρήστες, για παράδειγμα κατά την είσοδό τους σε κάποιο κατάστημα, με εξατομικευμένες προσφορές*"[77]. Παραγνωριζόταν έτσι το γεγονός ότι κάποιες από αυτές τις πρακτικές, όπως η εν αγνοία του υποκειμένου συλλογή δεδομένων με σκοπό τον εντοπισμό και την αναγνώριση της συσκευής συνεπάγονται υψηλό κίνδυνο για την ιδιωτική ζωή. Σε περιπτώσεις μάλιστα όπου η καταγραφή κινήσεων ανθρώπων γίνεται π.χ. σε νοσοκομεία ή σε εκκλησίες, εγείρεται ζήτημα ευαίσθητων προσωπικών δεδομένων[78]. Όπως αναφέρει η αξιολόγηση του Policy Department C του Ευρωπαϊκού Κοινοβουλίου για την Πρόταση Κανονισμού[79], αυτές οι πρακτικές μπορούν να δημιουργήσουν στους ανθρώπους το αίσθημα της διαρκούς παρακολούθησης, καθώς επίσης τονίζει ότι είναι δυσανάλογα περιοριστικό τα άτομα να αναγκάζονται να απενεργοποιούν τα κινητά τους τηλέφωνα, σε περίπτωση που δεν συναινούν σε αυτή την παρακολούθηση, χωρίς να παρέχεται καμία άλλη λύση, ήτοι δυνατότητα εξαίρεσης. Αυτή η πρακτική αντιβαίνει στους βασικούς στόχους της ΕΕ που εκφράζονται στον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών[80] για την συνδεσιμότητα και την ανεμπόδιστη πρόσβαση σε δίκτυα τηλεπικοινωνιών. Δεν θα πρέπει να λησμονούμε ότι στην αιτιολογική σκέψη 5 η Πρόταση Κανονισμού υπόσχεται ίσου επιπέδου προστασία με τον ΓΚΠΔ, ωστόσο εν προκειμένω υποβαθμιζόταν η παρεχόμενη προστασία, καθώς δεν λαμβανόταν υπόψη το δικαίωμα εναντίωσης του ΓΚΠΔ (άρθρο 21). Αυτή η ιδιαίτερη ανησυχία έχει επισημανθεί από την Ομάδα εργασίας του άρθρου 29[81], η οποία επιπρόσθετα επισημαίνει ότι η επιλογή αυτή δεν ισοδυναμεί με προστασία της ιδιωτικής ζωής "εξ ορισμού". Ανησυχίες εκφράστηκαν και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων[82] ο οποίος τόνισε ότι είναι δύσκολο να αντιληφθεί κανείς για ποιο λόγο αυτού του είδους τα δεδομένα θέσης να χρήζουν

---

77 Βλ. Αιτιολογική Σκέψη 25

78 Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2017), ό.α.

- 79 European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2017) *An assessment of the Commission's Proposal on Privacy and Electronic Communications*, διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

80 Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση), διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A52016PC0590

81 Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2017), ό.α.

82 Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2017), ό.α.

ασθενέστερης προστασίας.

Τα συγκεκριμένα χωρία άλλαξαν στην Πρόταση του 2021. Πλέον νομική βάση για τέτοιου είδους συλλογή δεδομένων αποτελεί η συγκατάθεση του χρήστη και η περίπτωση που είναι αναγκαία για στατιστικούς σκοπούς, με τις περαιτέρω απαιτήσεις η επεξεργασία να είναι περιορισμένη χρονικά στο μέτρο του αναγκαίου και τα δεδομένα να καθίστανται ανώνυμα ή να διαγράφονται όταν παύει η χρησιμότητά τους.

Στο σημείο αυτό κρίνεται σκόπιμο να αναφερθεί η κρίση της Ομάδας Εργασίας του Άρθρου 29 στη Γνώμη 1/2017, ότι θα πρέπει να αποφευχθεί η εισαγωγή "ανοιχτών" εξαιρέσεων επιτρεπόμενης επεξεργασίας, όπως προβλέπεται στο στ' του άρθρου 6 παρ. 1 του ΓΚΠΔ, με την επεξεργασία να επιτρέπεται "*για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος*", αφήνοντας ανοιχτό το πεδίο εφαρμογής του τι εμπίπτει στα έννομα συμφέροντα.

6.8 Κεφάλαιο 3 της Πρότασης Κανονισμού

Εισάγονται άρθρα που θεσπίζουν κανόνες που ισχύουν για την ταυτοποίηση των συνδρομητών, όπως η δυνατότητα ένδειξης της ταυτότητας και περιορισμού της αναγνώρισης της καλούσας γραμμής, εξαιρουμένων των περιπτώσεων κλήσεων έκτακτης ανάγκης, όπως επίσης και δυνατότητα αποκλεισμού συγκεκριμένων εισερχόμενων κλήσεων.

Στο άρθρο 16 παρ. 1 συνδυαστικά με την αιτιολογική σκέψη 33 διατυπώνεται η απαγόρευση της μη ζητηθείσας επικοινωνίας για σκοπούς άμεσης εμπορικής προώθησης χωρίς την προηγούμενη συγκατάθεση, εισάγοντας εύλογη εξαίρεση για υφιστάμενους πελάτες των οποίων τα στοιχεία επικοινωνίας κατέχουν λόγω της προηγούμενης σχέσης οι εταιρείες. Εισάγεται μάλιστα απαίτηση αυτές οι μη ζητηθείσες επικοινωνίες να παρουσιάζουν αναγνωριστικό της ταυτότητας του φορέα που τις διενεργεί.

7. ΠΕΡΙ COOKIES

7.1 Τι είναι τα cookies;

Ο ορισμός που δίνει η ΑΠΔΠΧ[83] είναι ο εξής: "*Τα cookies είναι μικρά αρχεία κειμένου με πληροφορίες, τα οποία αποθηκεύονται από τον διακομιστή (server) ενός ιστοτόπου στην τερματική συσκευή (υπολογιστής, κινητό τηλέφωνο κλπ.) ενός επισκέπτη/χρήστη κατά την πλοήγηση σε αυτόν. Ο ιστότοπος ανακτά τις εν λόγω πληροφορίες σε κάθε επίσκεψη προκειμένου να προσφέρει σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει σε αυτή (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, κ.λπ.)...Τα cookies μπορεί να εγκαθίστανται από τον ίδιο τον πάροχο της ιστοσελίδας που επισκέπτεται ο χρήστης (first party cookies) ή από άλλους μέσω του παρόχου της ιστοσελίδας (third party cookies) που επισκέπτεται ο χρήστης*".

7.2 Υφιστάμενο νομοθετικό πλαίσιο για τα cookies

Τα cookies διέπονται από την Οδηγία e-Privacy, όπως έχει τροποποιηθεί από την Οδηγία 2009/136. Ο ΓΚΠΔ, ως lex generalis περί προστασίας προσωπικών δεδομένων, δεν περιέχει διατάξεις σχετικές με τα cookies, παρά μόνο τη διαπίστωση στην Αιτιολογική Σκέψη 30 ότι: "*Τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων. Αυτά μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους*." Η Οδηγία e-Privacy, όπως έχει τροποποιηθεί από την Οδηγία 2009/136 προβλέπει ότι: "*η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη*

[83] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα *Τι είναι τα cookies*, διαθέσιμο εδώ: https://www.dpa.gr/index.php/el/cookies/plirofories/whatis_cookies

συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας. Τούτο δεν εμποδίζει οιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι απολύτως αναγκαία για να μπορεί ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει ζητήσει ρητά ο συνδρομητής ή ο χρήστης να παρέχει τη συγκεκριμένη υπηρεσία".

Αντίστοιχη διάταξη στην ελληνική έννομη τάξη ευρίσκεται στο άρθρο 4 του ν. 3471/2006, όπως έχει τροποποιηθεί δυνάμει του άρθρου 170 του ν. 4070/2012[84].

Η απαίτηση συγκατάθεσης του τελικού χρήστη, κατόπιν της εκτενούς ενημέρωσής του εισήχθη με την Cookies Directive. Η Οδηγία e-Privacy στην αρχική της μορφή επέτρεπε την "*αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό*" απλά και μόνο εφόσον "*παρέχονται στον συγκεκριμένο συνδρομητή ή χρήστη σαφείς και εκτεταμένες πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας, και ο υπεύθυνος ελέγχου των δεδομένων τού παρέχει το δικαίωμα να αρνείται την επεξεργασία αυτή".*

Αρχικά λοιπόν ίσχυε το "σύστημα opt-out", όπου για την εγκατάσταση των cookies δεν χρειαζόταν η συγκατάθεση του χρήστη, αρκεί να του παρεχόταν η εκ των υστέρων δυνατότητα να εναντιωθεί, σε αντιδιαστολή με το παρόν "σύστημα opt-in" που απαιτεί συγκατάθεση[85].

Το σύστημα αυτό δεν είναι άνευ εξαιρέσεων, αφού δεν χρειάζεται συγκατάθεση του χρήστη στις εξής δύο περιπτώσεις: προκειμένου αποκλειστικώς για τη "*διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών*" και την "*παροχή υπηρεσίας της*

---

84 *"Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει. Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής. Τα παραπάνω δεν εμποδίζουν την οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή η οποία είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής. Με πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) ορίζονται ειδικότερα οι τρόποι παροχής πληροφοριών και δήλωσης της συγκατάθεσης."*

85 Ε. Μαργαρίτης (2020) *ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ & ΠΡΟΣΤΑΣΙΑ ΚΑΤΑΝΑΛΩΤΗ*, NB, σελ. 84 επ.

κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής".

Η χρήση των cookies ωστόσο διέπεται και από τον ΓΚΠΔ, αφού η Οδηγία e-Privacy, ως προς τις προϋποθέσεις της συγκατάθεσης παραπέμπει στην οδηγία 95/46/ΕΚ, η οποία έχει αντικατασταθεί από τον ΓΚΠΔ. Επομένως, η συγκατάθεση πρέπει να έχει την ίδια έννοια με αυτή στον ΓΚΠΔ. Οι πάροχοι των ιστοσελίδων, με την έναρξη ισχύος του ΓΚΠΔ κλήθηκαν να μεταβάλλουν το μοντέλο λειτουργίας τους, αφού οι προϋποθέσεις την νόμιμης συγκατάθεσης αυστηροποιήθηκαν με τον ΓΚΠΔ σε σχέση με το προϊσχύον καθεστώς. Ο Κανονισμός e-Privacy θα προσφέρει συνοχή, καθώς στην παρούσα φάση ισχύει η Οδηγία e-Privacy, η ενσωμάτωση της οποίας στις εθνικές έννομες τάξεις κρίνεται κατακερματισμένη, παράλληλα με τον ΓΚΠΔ, ο οποίος έχει άμεση ισχύ σε όλα τα κράτη-μέλη.

7.3 Διάκριση cookies

Τα cookies στην εμπορική πρακτική διακρίνονται[86] σε "αυστηρώς απαραίτητα", "cookies επιδόσεων", "cookies λειτουργικότητας" και "cookies στόχευσης ή διαφήμισης".

Τα αυστηρώς απαραίτητα cookies είναι απολύτως αναγκαία για τη λειτουργία μιας ιστοσελίδας, και επιτρέπουν στον χρήστη να περιηγείται και να χρησιμοποιεί τις υπηρεσίες και τις λειτουργίες της. Όπως αναφέρει και η Πρόταση Κανονισμού στην Αιτιολογική Σκέψη 21, για την αποθήκευση αυτών των cookies δεν χρειάζεται η προηγούμενη συγκατάθεση του χρήστη, καθώς η χρήση τους συνεπάγεται περιορισμένη έως και καθόλου επέμβαση στην ιδιωτική ζωή. Τέτοια cookies είναι για παράδειγμα αυτά που χρησιμεύουν στο να θυμάται η ιστοσελίδα ποια προϊόντα πρόσθεσε ο χρήστης στο καλάθι αγορών κατά την περιήγησή του σε ένα e-shop.

Διαφορετικά είναι τα πράγματα για τις υπόλοιπες κατηγορίες cookies, πέραν των τεχνικώς απαραίτητων, για τις οποίες απαιτείται η προηγούμενη της εγκατάστασής τους συγκατάθεση του χρήστη, κατόπιν ενημέρωσής του. Οι λειτουργίες που επιτελούν τα cookies είναι άκρως

86 Βλ. Β. Καρκατζούνης (2019) *Cookies και προστασία δεδομένων προσωπικού χαρακτήρα*, ΔΙΤΕ (π. ΔΙΜΕΕ) 2/2019, όπου αναφέρεται ότι η συγκεκριμένη κατηγοριοποίηση που έχει γίνει από το Διεθνές Εμπορικό Επιμελητήριο του Ηνωμένου Βασιλείου (https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookiesguide_revnov.pdf) αποτελεί βάση κατανόησης των διάφορων ειδών cookies.

χρήσιμες, εκτός από τεχνικά, και εμπορικά για την βιωσιμότητα των ιστοτόπων. Η τεχνολογία των "ιχνηλατών" έχει προωθήσει την παγκοσμιοποιημένη "ψηφιακή αγορά"[87], όπως την ξέρουμε σήμερα. Όλοι αυτοί οι ιχνηλάτες όμως μπορούν να αποκτήσουν πρόσβαση και να συλλέξουν πληροφορίες του χρήστη που βρίσκονται στις συσκευές του, να παρακολουθήσουν τη δραστηριότητά του (tracking)[88]. Η Πρόταση Κανονισμού αναγνωρίζει τους κινδύνους που ενυπάρχουν στη λειτουργία αυτών των τεχνολογιών ως προς την ιδιωτική ζωή των χρηστών και σκοπεύει να θωρακίσει την προστασία της, αυστηροποιώντας το κανονιστικό πλαίσιο. Ο Κανονισμός e-Privacy αποσκοπεί να εξασφαλίσει ότι δεν θα εγκαθίσταται κανένας "ιχνηλάτης" στη συσκευή του χρήστη χωρίς τη συγκατάθεσή του, ανεξαρτήτως του εάν οδηγεί σε επεξεργασία προσωπικών δεδομένων[89], φιλοδοξώντας να αποκτήσει ο χρήστης τον έλεγχο του τερματικού του εξοπλισμού[90].

7.4 Cookies και διαφήμιση

Η Ομάδα Εργασίας του άρθρου 29 ήδη από το 2010 σε Γνώμη της[91] ανέλυσε το μοντέλο της συμπεριφορικής διαφήμισης στο Διαδίκτυο, το οποίο βασίζεται στην παρακολούθηση των χρηστών μέσω αναγνωριστικών στοιχείων που συνήθως αποτελούν προσωπικά δεδομένα, χρησιμοποιώντας τεχνολογίες παρακολούθησης όπως είναι τα cookies. Το μοντέλο αυτό στοχεύει στη δημιουργία προφίλ του χρήστη, ώστε να του προωθεί στη συνέχεια διαφημίσεις που ανταποκρίνονται στα ενδιαφέροντά του βάσει του προφίλ του. Στο μοντέλο της συμπεριφορικής διαφήμισης εμπλέκονται περισσότερα του ενός μέρη: Οι "εκδότες" των ιστοσελίδων συμβάλλονται με διαφημιστικά δίκτυα, εκμισθώνοντάς τους χώρο εντός της ιστοσελίδας προκειμένου να εμφανίζονται οι διαφημίσεις τους. Η ΟΕ 29 στη συγκεκριμένη γνώμη ανέδειξε νομικά ζητήματα που συνεπάγεται αυτό το "οικοσύστημα", ιδίως ως προς την

87 Μ. Σκόνδρα (2020) *Λήξη της προθεσμίας για τα Cookies: η συμμόρφωση που άργησε 8 χρόνια*, διαθέσιμο εδώ: www.gdprgroup.gr

88 Βλ. Αιτιολογική Σκέψη 20 Πρότασης Κανονισμού.

89 Τελευταίο εδάφιο Αιτιολογικής Σκέψης 20

90 Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018) *Δήλωση σχετικά με την αναθεώρηση του Κανονισμού για την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών (Κανονισμός ePrivacy) και τον αντίκτυπό της στην προστασία των φυσικών προσώπων όσον αφορά την ιδιωτικότητα και το απόρρητο των επικοινωνιών τους*, διαθέσιμη στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_el_0.pdf

91 Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2010) *Γνώμη 2/2010 σχετικά με την επιγραμμική συμπεριφορική διαφήμιση*, διαθέσιμο εδώ: https://www.dpa.gr/sites/default/files/2019-10/WP171_EL.PDF

επεξεργασία προσωπικών δεδομένων και την αλληλεπίδραση της Οδηγίας e-Privacy με την νομοθεσία περί προσωπικών δεδομένων.

Και ενώ από το συγκεκριμένο μοντέλο διαφήμισης τα εμπλεκόμενα μέρη αποκομίζουν τεράστια οικονομικά οφέλη, το οποίο έχει οδηγήσει στην ανάπτυξη της οικονομίας του Διαδικτύου, η ΟΕ 29 έχει επιστήσει την προσοχή στα ζητήματα προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων που προκύπτουν ως προς τους χρήστες του διαδικτύου, οι οποίοι όταν επισκέπτονται μία ιστοσελίδα ενδέχεται να μην έχουν στο νου τους όλο αυτό το μοντέλο και τις χρησιμοποιούμενες τεχνολογίες και πώς αυτές μπορούν να παρακολουθήσουν τη συμπεριφορά τους.

Η ψηφιακή διαφήμιση έχει εξελιχθεί έτι περαιτέρω. Από τα τέλη της δεκαετίας του 2000 βρισκόμαστε στην εποχή της επονομαζόμενης "προγραμματικής διαφήμισης", η οποία αποτελεί σήμερα μία από τις κύριες μορφές διαφήμισης στο Διαδίκτυο. Η ανάπτυξη της προγραμματικής διαφήμισης οφείλεται στην ελαχιστοποίηση του ανθρώπινου παράγοντα και στη χρησιμοποίηση νέων τεχνολογιών ("Adtech[92]") που αυτοματοποιούν όλη τη διαδικασία που "τρέχει" πίσω από τις διαφημίσεις. Συνδέεται επίσης με την ανάπτυξη της τεχνολογίας της real-time bidding (RTB), που επιτρέπει στους διαφημιζόμενους να αγοράζουν χώρο διαφήμισης μέσω αυτόματων δημοπρασιών σε πραγματικό χρόνο.

Καθόσον χάρη στην τεχνολογία η ψηφιακή διαφήμιση τείνει να γίνεται όλο και πιο περίπλοκη, είναι κεφαλαιώδους σημασίας να διαφυλάσσονται τα προσωπικά δεδομένα των χρηστών. Σε αυτό το πλαίσιο αναδεικνύεται η ανάγκη για διαφάνεια όσον αφορά την αποθήκευση πληροφοριών στον τερματικό εξοπλισμό του χρήστη. Οι υποχρεώσεις διαφάνειας αποτυπώνονται στο κείμενο της Οδηγίας e-Privacy "*ο χρήστης να έχει δώσει τη συγκατάθεσή του με βάση σαφείς και εκτενείς πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ, μεταξύ άλλων για το σκοπό της επεξεργασίας.*"

Αφ' ης στιγμής μέσω των cookies πραγματοποιείται επεξεργασία προσωπικών δεδομένων, η ψηφιακή διαφήμιση διέπεται τόσο από τις διατάξεις τόσο της Οδηγίας e-Privacy όσο και του ΓΚΠΔ. Στην Αιτιολογική Σκέψη 58 του ΓΚΠΔ γίνεται λόγος για την αρχή της διαφάνειας, η

[92] Β. Καρκατζούνης, Λ. Μήτρου (2020) *Online διαφήμιση και προστασία προσωπικών δεδομένων*, ΔΙΤΕ (π. ΔΙΜΕΕ) 1/2020

οποία "*έχει ιδιαίτερη σημασία σε περιπτώσεις στις οποίες η πληθώρα των συμμετεχόντων και η πολυπλοκότητα των χρησιμοποιούμενων τεχνολογιών καθιστούν δύσκολο για το υποκείμενο των δεδομένων να γνωρίζει και να κατανοεί εάν, από ποιον και για ποιο σκοπό συλλέγονται δεδομένα προσωπικού χαρακτήρα που το αφορούν, όπως στην περίπτωση επιγραμμικής διαφήμισης.*".

Πρέπει επομένως η ενημέρωση του χρήστη και η παροχή συγκατάθεσης εκ μέρους να λαμβάνουν χώρα τηρουμένων των "αυστηρών" προϋποθέσεων που θέτει ο ΓΚΠΔ.

Η πολυπλοκότητα του νομικού πλαισίου είναι εμφανής, καθώς εφαρμογή έχει τόσο η Οδηγία e-Privacy, η οποία έχει ενσωματωθεί διαφορετικά στις εθνικές έννομες τάξεις, όσο και ο ΓΚΠΔ, ο οποίος έχει άμεση ισχύ και εφαρμογή παντού.

Ένα άλλο ζήτημα που προκύπτει σχετικά με την ψηφιακή διαφήμιση που πραγματοποιείται μέσω της εγκατάστασης third party cookies είναι το ποιος θα παρέχει στον χρήστη τις απαιτούμενες πληροφορίες με βάση το άρθρο 5 παρ. 3 της Οδηγίας e-Privacy, όταν οι χρήστες επισκέπτονται μία ιστοσελίδα. Η ΟΕ 29 στη Γνώμη 2/2010 προσπάθησε να απαντήσει στο συγκεκριμένο ερώτημα: παρότι η υποχρέωση δεσμεύει εκείνον που τοποθετεί τα cookies και αποκτά πρόσβαση στις πληροφορίες χάρη στη χρήση των cookies, επομένως η συγκατάθεση του τελικού χρήστη θα έπρεπε να εξασφαλίζεται από τον πάροχο του διαφημιστικού δικτύου, εντούτοις, λόγω του ότι "οι *πάροχοι διαφημιστικών δικτύων είναι κατά κανόνα άορατοι για τους χρήστες*[93]", καταλήγει ότι ο εκδότης της ιστοσελίδας είναι αυτός που θα πρέπει παρέχει την ενημέρωση να εξασφαλίσει τελικά τη συγκατάθεση, αφού η όλη διάδραση γίνεται στην ιστοσελίδα του.

Στο ερώτημα εάν οι περί cookies κανόνες τηρούνται στην πράξη στις ελληνικές ιστοσελίδες, η απάντηση είναι μάλλον αρνητική. Η ελληνική ΑΠΔΠΧ, αφού διαπίστωσε "*σε ικανό βαθμό έλλειψη συμμόρφωσης των παρόχων υπηρεσιών της κοινωνίας της πληροφορίας στις ειδικές απαιτήσεις της νομοθεσίας για την επεξεργασία δεδομένων στις ηλεκτρονικές επικοινωνίες και του Γενικού Κανονισμού Προστασίας Δεδομένων όσον αφορά τη διαχείριση cookies και συναφών τεχνολογιών*" οδηγήθηκε το 2020 στην διατύπωση συστάσεων[94] για τους εκδότες των

[93] Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2010), ό.α.

[94] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2020) Συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες, διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythynon-

ιστοσελίδων που εμπεριέχουν πρακτικές οδηγίες σχετικά με την εφαρμογή των ως άνω υποχρεώσεων για τα cookies.

Με βάση το ισχύον πλαίσιο, η εγκατάσταση σε ιστοσελίδες των third party cookies δεν απαγορεύεται, αφού μάλιστα λαμβάνει χώρα στα πλαίσια της παροχής συγκατάθεσης εκ μέρους των χρηστών.

Όπως είδαμε, η συγκατάθεση πρέπει να έχει την ίδια έννοια με αυτή στον ΓΚΠΔ. Κατά τα οριζόμενα στον ΓΚΠΔ[95], για να θεωρηθεί έγκυρη η συγκατάθεση του υποκειμένου των δεδομένων, θα πρέπει να συντρέχουν οι εξής προϋποθέσεις: Το υποκείμενο θα πρέπει να ενημερώνεται σχετικά πριν δώσει τη συγκατάθεσή του, η οποία θα πρέπει να παρέχεται ελεύθερα, με σαφή θετική ενέργεια, συνιστώντας συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου υπέρ της επεξεργασίας των δεδομένων του και η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται. Ακόμα, ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει τη συγκατάθεση του υποκειμένου, καθώς και θα πρέπει να δίνεται η δυνατότητα στο υποκείμενο να ανακαλέσει ανά πάσα στιγμή τη συγκατάθεσή του.

Είναι αμφίβολο εάν πληρούνται όλες αυτές οι αυστηρές προϋποθέσεις της συγκατάθεσης στη ψηφιακή διαφήμιση. Ας εξετάσουμε την περίπτωση ενός μέσου χρήστη του Διαδικτύου. Όταν επισκέπτεται μία ιστοσελίδα ή κάνει χρήση μίας εφαρμογής, συνήθως βιάζεται να προχωρήσει στην ανάγνωση του περιεχομένου της / διάδραση με αυτό. Μάλιστα πολύ συχνά θα πατήσει "Συμφωνώ" στη χρήση cookies, απλά και μόνο για να εξαφανιστεί από την οθόνη του το cookie banner που έχει εμφανιστεί, ώστε να συνεχίσει ανενόχλητος την περιήγησή του. Πατώντας όμως "Συμφωνώ", είναι σχεδόν βέβαιο ότι ο χρήστης δεν γνωρίζει πού έχει δώσει τη συγκατάθεσή του, ούτε καν φαντάζεται πόσο μακριά θα φτάσουν τα προσωπικά του δεδομένα και από ποιον θα τύχουν επεξεργασίας.

Καθίσταται εμφανές ότι σε όλο αυτό το σχήμα δεν πληρούνται οι προϋποθέσεις περί έγκυρης συγκατάθεσης που απαιτεί ο ΓΚΠΔ. Ο Daniel J. Solove σε ένα άρθρο[96] του που παρουσιάζει

---

epexergasias-dedomenon-me-tin-eidiki

95 Άρθρο 7 και Αιτιολογική Σκέψη 32

96 Daniel J. Solove (2023), *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 Boston University Law Review (Forthcoming) GWU Legal Studies Research Paper No. 2023-23 GWU Law School

απερίφραστα τα πράγματα, χαρακτηρίζει την απόκτηση μιας πραγματικά έγκυρης συγκατάθεσης ως απελπιστικά δύσκολο έργο που παραμένει άπιαστο ιδανικό όνειρο για τους νόμους περί απορρήτου, οι οποίοι αρνούνται να δεχθούν αυτή την πραγματικότητα και αρκούνται στην "πλασματική" συγκατάθεση. Όσον αφορά τα αιτήματα συγκατάθεσης για cookies υπό τις προϋποθέσεις του ΓΚΠΔ, υπογραμμίζει ότι με το σύστημα opt-in οι οργανισμοί απλώς καλύπτονται ως προς την παροχή συγκατάθεσης, χωρίς αυτό να σημαίνει ότι οι χρήστες παρέχουν μία "ισχυρή" συγκατάθεση. Θεωρεί μάλιστα το σύστημα opt-in χειρότερο από το σύστημα opt-out, γιατί οι χρήστες θέλουν απλώς να διώξουν το ενοχλητικό cookie banner.

7.5 Τι προσπαθεί να αλλάξει ο Κανονισμός e-Privacy

Η Πρόταση Κανονισμού πολύ εύστοχα στην Αιτιολογική Σκέψη 20α αναγνωρίζει ότι η προστασία που προσφέρει η συγκατάθεση έχει υπονομευθεί, αφού οι χρήστες βομβαρδίζονται με αιτήματα παροχής συγκατάθεσης από τις ιστοσελίδες με αποτέλεσμα να παρέχουν τη συγκατάθεσή τους χωρίς καν να παρατηρούν σε τι συγκατατίθενται, με αποτέλεσμα την καταστρατήγηση της ουσίας των κανόνων της νομοθεσίας περί προσωπικών δεδομένων. Ως εκ τούτου, η Πρόταση Κανονισμού, στην προσπάθεια επίλυσης του ζητήματος, προκρίνει τρόπους για τη χορήγηση πραγματικής συγκατάθεσης:

7.5.1 Browser settings

Μία λύση είναι η δυνατότητα γενικευμένων ρυθμίσεων μέσω του φυλλομετρητή ή άλλης εφαρμογής λογισμικού, οι οποίες θα αφορούν στη χορήγηση συγκατάθεσης για τη χρήση cookies και θα είναι μάλιστα δεσμευτικές για τα τρίτα μέρη (π.χ. για έναν διαφημιστή). Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων[97] υποστηρίζει ότι αυτή η διάταξη θα πρέπει να εφαρμόζεται ρητώς και στα λειτουργικά συστήματα των έξυπνων τηλεφώνων, των tablet ή κάθε άλλου «user agent», ώστε να διασφαλίζεται ότι οι εφαρμογές επικοινωνιών μπορούν να

Public Law Research Paper

97 Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018) *Δήλωση σχετικά με την αναθεώρηση του Κανονισμού για την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών (Κανονισμός ePrivacy) και τον αντίκτυπό της στην προστασία των φυσικών προσώπων όσον αφορά την ιδιωτικότητα και το απόρρητο των επικοινωνιών τους*, διαθέσιμη στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_el_0.pdf

λαμβάνουν υπόψη τις επιλογές των χρηστών τους, ανεξάρτητα από τα χρησιμοποιούμενα τεχνικά μέσα.

7.5.2. Whitelisting

Η Πρόταση Κανονισμού ενθαρρύνει τους φυλλομετρητές να δημιουργούν λίστες διαδικτυακών τόπων (whitelistls) από τους οποίους θα γίνονται ή όχι δεκτά τα cookies, με στόχο την αποφυγή της επαναλαμβανόμενης συγκατάθεση που ο χρήστης καλείται να χορηγεί για τα cookies, άλλως το φαινόμενο της "κόπωσης συγκατάθεσης" ("consent fatigue"). Επισημαίνει βέβαια ότι μία ειδική δήλωση συγκατάθεσης εκ μέρους του χρήστη θα υπερισχύει των γενικών μέσω browser.

Σχετικά με τις γενικευμένες μέσω φυλλομετρητή ή άλλου λογισμικού ρυθμίσεις, έχουν εκφραστεί επιφυλάξεις από εκπροσώπους ψηφιακών υπηρεσιών[98] [99] [100], οι οποίοι πιστεύουν ότι η χρήση των ιστοτόπων και υπηρεσιών θα δυσχεραίνεται εάν πολλές επιλογές είναι εκ προεπιλογής απενεργοποιημένες, καθώς ο φυλλομετρητής δεν θα είναι σε θέση να ξεχωρίσει τις απαραίτητες τεχνολογίες για την λειτουργία μιας συγκεκριμένης υπηρεσίας. Οπότε, τελικά, οι χρήστες θα είναι αναγκασμένοι, προκειμένου να αξιοποιήσουν τις δυνατότητες μιας υπηρεσίας, είτε να ανάγονται συνεχώς στις γενικευμένες ρυθμίσεις για να τις τροποποιήσουν είτε θα τους εμφανίζονται και πάλι τα "ενοχλητικά" αιτήματα για συγκεκριμένη συγκατάθεση. Αυτό θα επιφέρει εκνευρισμό των χρηστών, καθώς και θα υπονομεύει το επιχειρηματικό μοντέλο των προγραμματιστών των ψηφιακών υπηρεσιών, αφού δεν θα μπορούν να καθορίσουν οι ίδιοι τους όρους υπό τους οποίους θέλουν να παρέχουν τις υπηρεσίες τους. Αλλά και με την εν λόγω πρακτική τίθεται εν αμφιβόλλω η εκπλήρωση της υποχρέωσης για τους υπευθύνους επεξεργασίας σχετικά με την χορήγηση των απαιτούμενων πληροφοριών στους χρήστες.

---

98 Interactive Advertising Bureau Europe - IAB Europe (2018) *Position on the proposed ePrivacy Regulation*, διαθέσιμο στο: https://iabeurope.eu/wp-content/uploads/2019/10/31.10.2018-IABEU-ePR_Position_Paper.pdf

99 Developers Alliance (2018) *Updated Position Paper on the Proposal for an E-Privacy Regulation*, διαθέσιμο στο: https://developersalliance.org/position-papers/

100 Centre for Information Policy Leadership (CIPL) (2021) *Comments by the Centre for Information Policy Leadership on the Draft E-Privacy Regulation for the Purpose of the Trilogue Discussions*, διαθέσιμο στο: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_draft_eprivacy_regulation__epr__for_the_epr_trilogues__29_sept_2021_.pdf

7.5.3 Cookie walls

Η Πρόταση Κανονισμού προβλέπει[101] ότι η πρόσβαση σε μια δωρεάν υπηρεσία μπορεί να εξαρτηθεί από την αποδοχή cookies, υπό την προϋπόθεση ότι ο πάροχος υπηρεσιών προσφέρει μια ισοδύναμη εναλλακτική επιλογή που δεν απαιτεί την αποδοχή των cookies. Για να θεωρείται νόμιμη η συγκεκριμένη πρακτική, η Πρόταση Κανονισμού αποδίδει ιδιαίτερη σημασία στην ύπαρξη "πραγματικής" εκ μέρους του χρήστη επιλογής ("genuine choise") όσον αφορά την αποδοχή των cookies. Θα πρέπει να δίδεται η δυνατότητα στο χρήστη να επιλέξει ανάμεσα στη συγκεκριμένη προσφορά και σε ισοδύναμη προσφορά του ίδιου παρόχου η οποία δεν προϋποθέτει τη χορήγηση συγκατάθεσης για τα cookies. Η Ομάδα Εργασίας του άρθρου 29[102] και πλέον το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ)[103], που χαρακτηρίζει αυτή την πρακτική του "όλα ή τίποτα" ως αθέμιτη από τη στιγμή που δεν προσφέρονται ισότιμες εναλλακτικές λύσεις, έχει εκφράσει την άποψη ότι θα πρέπει να απαγορεύεται η χρήση των cookie walls ή αλλιώς tracking walls. Έχει προτείνει μάλιστα τη ρητή συμπερίληψη της απαγόρευσης των cookie walls στην Πρόταση Κανονισμού, λαμβανομένης υπόψη της απαίτησης του ΓΚΠΔ για ελεύθερη συγκατάθεση που οδηγεί στο συμπέρασμα ότι αντίκειται στην ελεύθερη έννοια της συγκατάθεσης η εξαναγκαστική αποδοχή της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα ή των πληροφοριών που συνδέονται με τον τερματικό εξοπλισμό των τελικών χρηστών για την πρόσβαση σε μία υπηρεσία.

7.5.4 Κοινή χρήση δεδομένων με τρίτα μέρη

Σύμφωνα με την Πρόταση Κανονισμού, απαγορεύεται η κοινή χρήση των μεταδεδεδομένων επικοινωνιών και των δεδομένων τερματικού εξοπλισμού με τρίτα μέρη για περαιτέρω σκοπούς επεξεργασίας εάν δεν έχουν καταστεί ανώνυμα (άρθρο 6C παρ. 3 και άρθρο 8 παρ. 1 i).

Ως προς αυτό το σημείο της Πρότασης Κανονισμού έχει ασκηθεί έντονη κριτική και έχουν εκφραστεί[104] ανησυχίες από εκπροσώπους της ψηφιακής οικονομίας, καθώς αυτή η γενική

[101] Βλ Αιτιολογική Σκέψη 20αααα

[102] Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2017), ό.α.

[103] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021), ό.α.

[104] Developers Alliance (2018) *Updated Position Paper on the Proposal for an E-Privacy Regulation*, διαθέσιμο στο:

απαγόρευση έρχεται σε αντίθεση με τον τρόπο που λειτουργούν οι επιγραμμικές υπηρεσίες της σύγχρονης ψηφιακής οικονομίας. Αυτές προσφέρονται συνήθως άνευ αντιτίμου, ενώ για να εξασφαλίσουν τα κέρδη τους ζητούν την πρόσβαση στα δεδομένα των χρηστών τους, για την περαιτέρω αξιοποίησή τους. Ουσιαστικά το "αντίτιμο" που "πληρώνουμε" για να έχουμε πρόσβαση σε ιστοσελίδες/social media/εφαρμογές κ.ο.κ. ώστε να επωφελούμαστε από το περιεχόμενο που μας προσφέρουν, είναι τα δεδομένα μας. Περαιτέρω, το βασικότερο επιχειρηματικό μοντέλο αυτών των επιγραμμικών υπηρεσιών είναι η διαφήμιση. Η λειτουργία της online διαφήμισης είναι βασισμένη στην ομάδα τεχνολογιών των "ιχνηλατών[105]", όπως είναι τα cookies ή άλλες παρεμφερείς τεχνολογίες.

7.5.5 Αυτορρύθμιση της αγοράς

Η Google τον Αύγουστο του 2019 ανακοίνωσε[106] την πρωτοβουλία δημιουργίας ενός ασφαλούς για την ιδιωτικότητα των χρηστών στο Διαδίκτυο περιβάλλοντος, του "Privacy Sanbox", με στόχο την ανάπτυξη προτύπων και προσεγγίσεων διαφανών διαφημιστικών μοντέλων που θα ανταποκρίνονται στις προσδοκίες ιδιωτικότητας των χρηστών. Εντός αυτού του πλαισίου, επανήλθε με ανακοίνωσή της[107] στις αρχές του 2020 σχετικά με την πρόθεσή να πάψουν σταδιακά να υποστηρίζονται από το Chrome τα third-party cookies. Και άλλες εταιρείες ακολουθούν την ίδια τακτική. Το Firefox[108] της Mozilla το 2019 απέκλεισε τα third-party cookies από προεπιλογή, με το Safari[109] της Apple να ακολουθεί το παράδειγμα το 2020. Η Meta, επίσης, ανακοίνωσε[110] το 2021 ότι στοχεύει να απαγορεύσει στις πλατφόρμες της Facebook, Messenger,

https://developersalliance.org/position-papers/

105 Όπως τα έχει ονομάσει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο 25/02/2020 δελτίο τύπου "*Συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες*", διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythynon-epexergasias-dedomenon-me-tin-eidiki

106 Google Chrome (2019) *Building a more private web,* διαθέσιμο στο: https://www.blog.google/products/chrome/building-a-more-private-web/

107 Chromium Blog (2020) *Building a more private web: A path towards making third party cookies obsolete*, διαθέσιμο στο: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

108 Mozilla Firefox (2019) *Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default*, διαθέσιμο στο: https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

109 WebKit (2020) *Full Third-Party Cookie Blocking and More,* διαθέσιμο στο: https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

110 Forbes (2021) *Meta Will Soon Ban Targeting Ads Based On Sensitive Categories Including Religion And* Politics, διαθέσιμο στο: https://www.forbes.com/sites/martyswant/2021/11/09/meta-will-soon-ban-targeting-ads-based-on-sensitive-categories-including-religion-and-politics/?sh=2c0f9aa53b3d

Instagram και WhatsApp τις στοχευμένες διαφημίσεις που βασίζονται σε ευαίσθητες πληροφορίες.

8. ΠΕΡΙΟΡΙΣΜΟΣ ΔΙΚΑΙΩΜΑΤΟΣ ΤΗΣ ΑΠΟΡΡΗΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

8.1 Αρχή αναλογικότητας

Το δικαίωμα της απόρρητης επικοινωνίας δεν είναι απόλυτο. Αν και στο ελληνικό Σύνταγμα το δικαίωμα χαρακτηρίζεται ως "απολύτως" απαραβίαστο, παρά τη συμβολική βαρύτητα[111] που δίδεται, δεν σημαίνει κυριολεκτικά ότι υπερέχει[112] έναντι των υπολοίπων, συνταγματικώς κατοχυρωμένων, δικαιωμάτων. Κάθε φορά που συγκρούονται δύο δικαιώματα, επιβάλλεται να γίνεται προσπάθεια σταθμίσεως, προκειμένου να μην θίγεται ο πυρήνας κανενός εκ των συγκρουόμενων δικαιωμάτων. Αυτό επέρχεται διά της πρακτικής τους εναρμόνισης[113], μέσω της θεμελιώδους αρχής της αναλογικότητας. Σύμφωνα με την τελευταία, όταν λαμβάνεται κάποιο μέτρο που περιορίζει ένα δικαίωμα, θα πρέπει να είναι πρόσφορο, δηλαδή να μπορεί να επιφέρει τον σκοπό που επιδιώκει ("καταλληλότητα"), να είναι αναγκαίο ως προς τον επιδιωκόμενο σκοπό, ο οποίος δεν μπορεί να επιτευχθεί με κάποιο λιγότερο επαχθές μέτρο ("αναγκαιότητα") και, τέλος, να μην είναι δυσανάλογο ως προς τον σκοπό που επιδιώκει ("εν στενή εννοία αναλογικότητα").

8.2 Περιορισμός προστασίας του απορρήτου στα θεμελιώδη ευρωπαϊκά κείμενα

Ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ στο Άρθρο 52 προβλέπει ότι οι περιορισμοί στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον Χάρτη "*πρέπει να σέβονται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί μπορούν να τίθενται μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά στους στόχους γενικού ενδιαφέροντος που αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων. Στο βαθμό που ο Χάρτης περιλαμβάνει δικαιώματα που αντιστοιχούν σε δικαιώματα τα οποία διασφαλίζονται στην*

---

111 Α. Παπανικολάου (2020) *Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*, διαθέσιμο εδώ: https://www.constitutionalism.gr/2020-07-papanikolaou-aporito-epikinonias/

112 Βλ. Π. Δαγτόγλου (2012), ό.α. σελ. 95 "*Όλα τα συνταγματικώς κατοχυρωμένα δικαιώματα έχουν πάντως την ίδια τυπική ισχύ (δεν υπάρχουν δηλαδή "υπερέχοντα" και "υποδεέστερα" από νομικής απόψεως) και επομένως η τυχόν σύγκρουση δεν μπορεί να λυθεί με την αναφορά σε ιεραρχική κλίμακα ισχύος.*"

113 Βλ. Σπ. Βλαχόπουλος (2017) *ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ*, 1η Έκδοση, NB, σελ. 24-26

Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, η έννοια και η εμβέλειά τους είναι ίδιες με εκείνες που τους αποδίδει η εν λόγω Σύμβαση".

Συναφώς, το άρθρο 8 της ΕΣΔΑ στην παρ. 2 θέτει τις προϋποθέσεις υπό τις οποίες καθίσταται δυνατό να περιοριστεί με νόμιμο τρόπο το απόρρητο των επικοινωνιών, αποτυπώνοντας ουσιαστικά την αρχή της αναλογικότητας:

"*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 διά 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 άρση του απορρήτου χαρακτήρα της επικοινωνίας λοιπόν είναι νόμιμη εφόσον προβλέπεται από τον νόμο, επιδιώκει κάποιον από τους σκοπούς της διάταξης και εφόσον είναι αναγκαία στο πλαίσιο μιας δημοκρατικής κοινωνίας, για την επίτευξη των ανωτέρω σκοπών. Οι προϋποθέσεις αυτές είναι διατυπωμένες με ευρύ τρόπο, υποδεικνύοντας τις γενικές κατευθύνσεις υπό τις οποίες μπορεί να καμφθεί το δικαίωμα. Ωστόσο, υφίσταται πλούσια νομολογία του ΕΔΔΑ που εξειδικεύει αυτά τα κριτήρια.

8.3 Κριτήρια νομολογίας ΕΔΔΑ για τον περιορισμό της προστασίας του απορρήτου

Καταρχάς, ο περιορισμός πρέπει να προβλέπεται σε νόμο ("*in accordance with the law*"). Σύμφωνα με την πάγια νομολογία του ΕΔΔΑ[114], ο περιορισμός του δικαιώματος πρέπει να ερείδεται σε εθνικό νόμο, ο οποίος επιπροσθέτως πρέπει να έχει κάποια ποιοτικά χαρακτηριστικά: να είναι προσβάσιμος, προβλέψιμος και επαρκώς σαφής. Το κριτήριο της προσβασιμότητας επιτάσσει ο νόμος να είναι ευχερώς προσιτός και δημοσίως προσβάσιμος. Το κριτήριο της προβλεψιμότητας γενικά συνεπάγεται ότι πρέπει να παρέχονται επαρκείς ενδείξεις ως προς τις περιστάσεις υπό

[114] Βλ. Απόφαση ΕΔΔΑ (2010) *Kennedy v United Kingdom* παρ. 151, Απόφαση ΕΔΔΑ (2016) *Szabó and Vissy v. Hungary* παρ. 59, Απόφαση ΕΔΔΑ (2015) *Zakharov v. Russia* παρ. 228

τις οποίες θα περιοριστεί το δικαίωμα και ποιες θα είναι οι επακόλουθες συνέπειες[115]. Το ΕΔΔΑ ωστόσο έχει τονίσει ότι το κριτήριο της προβλεψιμότητας στον τομέα άρσης του απορρήτου των επικοινωνιών δεν είναι δυνατό να έχει την ίδια έννοια όπως σε άλλους τομείς. Λόγω της μυστικότητας του μέτρου, δεν μπορεί να σημαίνει ότι το άτομο θα είναι σε θέση να προβλέψει πότε οι επικοινωνίες του θα τύχουν παρακολούθησης, ώστε να προσαρμόσει αναλόγως τη συμπεριφορά του. Τοιουτοτρόπως, το ΕΔΔΑ[116] καταλήγει στο κριτήριο της επαρκούς σαφήνειας του νόμου. Η μυστική φύση του συγκεκριμένου τομέα και ενόψει του ότι οι τεχνολογίες που χρησιμοποιούνται για την άρση του απορρήτου ολοένα και εξελίσσονται, αποτελεί επιτακτική ανάγκη να υφίστανται κανόνες που ρυθμίζουν σαφώς και λεπτομερώς τις περιστάσεις και τις συνθήκες υπό τις οποίες μπορεί να επιβληθεί το συγκεκριμένο μέτρο[117].

Ο περιορισμός πρέπει να αποτελεί αναγκαίο μέτρο σε μία δημοκρατική κοινωνία επιδιώκοντας τους ειδικούς σκοπούς που παραθέτει το άρθρο. Δεδομένου ότι τα κράτη απολαύουν διακριτικής ευχέρειας ως προς τον τρόπο επιλογής των μέτρων προκειμένου να προστατεύσουν την εθνική τους ασφάλεια, αυτό δεν σημαίνει ότι οι εθνικές αρχές είναι σε θέση να καταχραστούν αυτή την εξουσία, παρακάμπτοντας τις προϋποθέσεις της Ευρωπαϊκής νομοθεσίας. Όπως εύστοχα έχει τονίσει το ΕΔΔΑ[118], υπάρχει ο κίνδυνος το σύστημα άρσης του απορρήτου να υπονομεύσει τη δημοκρατία, στην προσπάθεια υπεράσπισής της. Γι' αυτό, το ΕΔΔΑ έχει θεσπίσει μέσω της νομολογίας του κάποιες ελάχιστες εγγυήσεις που πρέπει να πληρούνται, προκειμένου να είναι σύννομη η διαδικασία άρσεως του απορρήτου, Αυτές οι εγγυήσεις περιλαμβάνουν: την ορισμένη χρονική διάρκεια του μέτρου[119], την υποχρέωση γνωστοποίησης του μέτρου μετά τη λήξη του στο θιγόμενο πρόσωπο[120], την εποπτεία της διαδικασίας από ανεξάρτητο όργανο[121], τον προσδιορισμό των θιγόμενων προσώπων, τη φύση της αξιόποινης συμπεριφοράς κ.ά.

8.4 Περιορισμός δικαιωμάτων Οδηγίας e-Privacy

115 Βλ. Απόφαση ΕΔΔΑ (2014) *Fernández Martínez v. Spain* παρ. 117
116 Απόφαση ΕΔΔΑ (2015) *Zakharov v. Russia* παρ. 229
117 Απόφαση ΕΔΔΑ (1990) *Kruslin v. France* παρ. 33
118 Απόφαση ΕΔΔΑ (2015) *Zakharov v. Russia* παρ. 232
119 Απόφαση ΕΔΔΑ (2016) *Szabó and Vissy v. Hungary* παρ. 74
120 Απόφαση ΕΔΔΑ (2006) *Weber and Saravia v. Germany* παρ. 135
121 Απόφαση ΕΔΔΑ (2015) *Zakharov v. Russia* παρ. 275

Εντός αυτού του πνεύματος, η Οδηγία e-Privacy περιέχει διάταξη κατά την οποία επιτρέπονται περιορισμοί των δικαιωμάτων που προβλέπει "*για τη διαφύλαξη 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*"[122], υπό τον όρο τήρησης της αρχής της αναλογικότητας ("*εφόσον ο περιορισμός αυτός αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία*").

8.5 Περιορισμός προστασίας του απορρήτου στην ελληνική έννομη τάξη

Ο κανόνας του άρθρου 19 παρ. 1 του Συντάγματος περί ελεύθερης επικοινωνίας δεν είναι άνευ εξαιρέσεων, αφού στο αμέσως επόμενο εδάφιο η συνταγματική διάταξη ορίζει τις εξαιρέσεις υπό τις οποίες καθίσταται επιτρεπτή η άρση του απορρήτου, με την τήρηση εγγυήσεων ώστε να τηρείται η αρχή της αναλογικότητας κατά τον περιορισμό του δικαιώματος[123]. Επιφυλάσσει αυτή την εξουσία μόνο στην δικαστική αρχή και μόνο για τους περιοριστικά αναφερόμενους λόγους της εθνικής ασφάλειας και της διακρίβωσης των ιδιαίτερα σοβαρών εγκλημάτων, υπό την επιφύλαξη νόμου. Ο εκτελεστικός νόμος, που υλοποιούσε μέχρι πρόσφατα την συνταγματική διάταξη ήταν ο Ν. 2225/1994, οι καίριες διατάξεις του οποίου περί άρσεως του απορρήτου[124] αντικαταστάθηκαν με τον Ν. 5002/2022, ο οποίος τέθηκε σε ισχύ προκειμένου να εκσυγχρονίσει την διαδικασία άρσεως του απορρήτου. Το Σύνταγμα επίσης ρητά στο άρθρο 19 παρ. 3 προβλέπει Ανεξάρτητη Αρχή για την διασφάλιση του απορρήτου των επικοινωνιών, εξοπλίζοντας έτσι την άσκηση του δικαιώματος με θεσμικές και οργανωτικές εγγυήσεις με στόχο την βέλτιστη πραγμάτωση του πυρήνα του δικαιώματος.

Στον Ν. 5002/2022 περιγράφεται (πλέον) η διαδικασία της άρσης του απορρήτου. Η εγχώρια επικαιρότητα του τελευταίου χρόνου, όπως θα δούμε παρακάτω, οδήγησαν στην αναδιαμόρφωση του νομοθετικού πλαισίου που αφορά την άρση του απορρήτου των επικοινωνιών. Τον Νοέμβριο του 2022 τέθηκε σε δημόσια διαβούλευση νομοθετική πρωτοβουλία με σκοπό "*τη θωράκιση και τον εκσυγχρονισμό της διαδικασίας άρσης του απορρήτου των επικοινωνιών σύμφωνα με το δεύτερο εδάφιο της παρ.1 του άρθρου 19 του Συντάγματος, τη βελτιστοποίηση της δράσης της Εθνικής Υπηρεσίας Πληροφοριών, την*

[122] Άρθρο 15 Οδηγίας e-Privacy
[123] Π. Δαγτόγλου (2012), ό.α., σελ. 299
[124] Τα άρθρα 3,4 και 5

προστασία του απορρήτου των επικοινωνιών από λογισμικά παρακολούθησης, την οργανική και λειτουργική αναβάθμιση του επιπέδου κυβερνοασφάλειας στη χώρα, και την αποτελεσματικότερη προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.[125]". Με την ψήφιση και θέση σε ισχύ του Νόμου 5002/2022 (ΦΕΚ Α 228/09.12.2022) καταργήθηκαν οι διατάξεις των άρθρων 3, 4, 5 και 7 του Ν. 2225/1994, όπου περιγραφόταν η διαδικασία άρσης του απορρήτου και επιχειρήθηκε η εξαντλητική της ρύθμιση στις διατάξεις του νέου νόμου.

Παρότι η επικαιρότητα στάθηκε αφορμή για την νέα αυτή νομοθετική πρωτοβουλία που αποφασίστηκε υπό πίεση, προκειμένου να προβλέψει ρυθμίσεις σχετικά με τα λογισμικά παρακολούθησης, ήταν ούτως ή άλλως επιτακτική η αναδιάρθρωση του οικείου νομοθετικού πλαισίου.

Ο Ν. 5002/2022 αποπειράθηκε να θεραπεύσει κάποιες αδυναμίες του προηγούμενου καθεστώτος.

- Προσπάθησε να οριοθετήσει την αόριστη νομική έννοια της "εθνικής ασφάλειας", συμπεριλαμβάνοντας στον ορισμό της παραδείγματα που συνιστούν λόγους εθνικής ασφάλειας. Αυτό κρίνεται θετικό αν αναλογιστούμε ότι η εθνική ασφάλεια μπορεί να χρησιμοποιηθεί ως πρόσχημα για να αρθεί το απόρρητο των επικοινωνιών. Ωστόσο, δεν εισήχθη στα υποχρεωτικά στοιχεία που πρέπει να περιλαμβάνει η διάταξη που διατάσσει άρση του απορρήτου για λόγους εθνικής ασφάλειας η απαίτηση παράθεσης ειδικής, συγκεκριμένης και εμπεριστατωμένης αιτιολογίας. Τα κράτη μέλη ναι μεν απολαύουν διακριτικής ευχέρειας ως προς τις δράσεις που αφορούν την προστασία της εθνικής ασφάλειας, η οποία θεωρείται ότι ανήκει στον "σκληρό πυρήνα[126]" του κράτους, ωστόσο, όπως αναφέρθηκε ανωτέρω, αυτό δεν μπορεί να οδηγεί σε κατάχρηση της ευχέρειας. Συναφώς, η έλλειψη της ανάγκης ύπαρξης αιτιολογίας έχει επικριθεί από την ΑΔΑΕ[127], αφού χωρίς αυτή δεν μπορούν να ελεγχθούν τα όρια της κρίσης και διακριτικής ευχέρειας του αποφασίζοντος οργάνου που εξέδωσε τη σχετική

[125] Άρθρο 1 του Ν. 5002/2022

[126] Απόφαση 867/2002 ΣτΕ Υπόθεση σκληρού πυρήνα κρατικών εξουσιών Σχολιασμός: Καραμπασιάδης Αριστείδης, διαθέσιμο στο: http://www.greeklaws.com/pubs/uploads/1585.pdf

[127] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (2022) Δελτίο Τύπου για το υπό διαβούλευση νομοσχέδιο του Ν. 5002/2022, διαθέσιμο στο: http://www.adae.gr/enimerosi/leptomereies/article/bfont-size3-colorredapantisi-toy-proedroy-tis-adae-se-dimo-1/

διάταξη, καθώς και η στάθμιση στην οποία προέβη με βάση τα κριτήρια της αρχής της αναλογικότητας και κατέληξε στην επιβολή του μέτρου.

- Επανέφερε το δικαίωμα για το υποκείμενο της παρακολούθησης να ενημερώνεται σχετικά με το επιβαλλόμενο εις βάρους μέτρο μετά την παύση της ισχύος της διάταξης άρσης του απορρήτου για λόγους εθνικής ασφάλειας[128]. Η δυνατότητα αυτή είχε καταργηθεί με τροποποίηση της παρ. 9 του άρθρου 5 του Ν. 2225/1994 με νόμο τον Μάρτιο του 2021 που αφορούσε κατεπείγουσες ρυθμίσεις για την πανδημία[129]. Το γεγονός αυτό είχε τότε προκαλέσει έντονη ακαδημαϊκή συζήτηση, ιδίως ως προς τη μη συμβατότητά του με τα κριτήρια του ΕΔΔΑ[130]. Ωστόσο, τίθεται εν αμφιβόλω η αποτελεσματικότητα του δικαιώματος αυτού, αφού ο Ν. 5002/2022 προβλέπει ότι θα γνωστοποιείται κατόπιν αιτήματος, τρία έτη μετά την παύση τη ισχύος της διάταξης και εφόσον "*δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε*" από τριμελές όργανο στο οποίο τα δύο από τα τρίτα πρόσωπα μετείχαν και στη διαδικασία αίτησης και έγκρισης του μέτρου της άρσης του απορρήτου. Το ομολογουμένως μεγάλο χρονικό διάστημα των τριών ετών σε συνδυασμό με το γεγονός ότι η γνωστοποίηση θα περιλαμβάνει ενημέρωση μόνο για την επιβολή του μέτρου και για τη διάρκειά του δεν κατατείνουν στην κατάφαση των δικαιωμάτων της αποτελεσματικής δικαστικής προσφυγής και της δίκαιας δίκης, τα οποία, σύμφωνα με την νομολογία του ΕΔΔΑ[131], συνδέονται άρρηκτα με το δικαίωμα

---

[128] Άρθρο 4 παρ. 7 του Ν. 5002/2022 *"Μετά την πάροδο τριών (3) ετών από την παύση της ισχύος της διάταξης άρσης του απορρήτου για λόγους εθνικής ασφάλειας γνωστοποιείται η επιβολή του περιοριστικού μέτρου στον θιγόμενο, υπό την προϋπόθεση ότι δεν διακυβεύεται ο σκοπός για τον οποίο αυτό διατάχθηκε. Για τη γνωστοποίηση του πρώτου εδαφίου υποβάλλεται σχετικό αίτημα στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), το οποίο διαβιβάζεται στην Ε.Υ.Π. και τη Δ.Α.Ε.Ε.Β.. Η άρση γνωστοποιείται μετά από απόφαση τριμελούς οργάνου, το οποίο αποφασίζει εντός προθεσμίας εξήντα (60) ημερών. Στην περίπτωση διενέργειας της άρσης από την Ε.Υ.Π., το όργανο αποτελείται από τον εισαγγελικό λειτουργό της παρ. 3 του άρθρου 5 του ν. 3649/2008, τον δεύτερο εισαγγελικό λειτουργό της παρ. 2 του άρθρου 4 του παρόντος και τον Πρόεδρο της Α.Δ.Α.Ε.. Στην περίπτωση διενέργειας της άρσης από τη Δ.Α.Ε.Ε.Β., το όργανο αποτελείται από τον εισαγγελικό λειτουργό της παρ. 3 του άρθρου 4 του ν. 2265/1994, τον δεύτερο εισαγγελικό λειτουργό της παρ. 2 του άρθρου 4 του παρόντος και τον Πρόεδρο της Α.Δ.Α.Ε.. Του οργάνου προεδρεύει ο ανώτερος ιεραρχικά ή, επί ομοιοβάθμων, ο αρχαιότερος εισαγγελικός λειτουργός. Το όργανο αποφασίζει κατά πλειοψηφία, με τήρηση απόρρητων συνοπτικών πρακτικών και καταγραφή της γνώμης της μειοψηφίας, εφόσον υφίσταται. Αν αποφασισθεί η ενημέρωση, ο θιγόμενος ενημερώνεται για την επιβολή του περιοριστικού μέτρου και για τη διάρκειά του. Δεν επιτρέπεται η υποβολή νέου αιτήματος πριν την πάροδο ενός (1) έτους από την υποβολή του προηγούμενου."*

[129] Με το άρθρο 87 του Ν. 4790/2021 (ΦΕΚ 48/Α/31-03-2021) "*Κατεπείγουσες ρυθμίσεις για την προστασία της δημόσιας υγείας από τις συνεχιζόμενες συνέπειες της πανδημίας του κορωνοϊού COVID-19, την ανάπτυξη, την κοινωνική προστασία και την επαναλειτουργία των δικαστηρίων και άλλα ζητήματα.*"

[130] Βλ. Χ. Ράμμος, Σ. Γκρίτζαλης, Α. Παπανικολάου (2021) *Αντίθεση του άρθρου 87 Ν. 4790/2021 προς τις εγγυήσεις της ΕΣΔΑ για διαφύλαξη του απορρήτου των επικοινωνιών*, διαθέσιμο στο: https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/

[131] Απόφαση ΕΔΔΑ (2015) *Zakharov v. Russia* παρ. 234

ενημέρωσης του υποκειμένου, ώστε το τελευταίο να είναι σε θέση να ελέγξει το επιβαλλόμενο εις βάρος του μέτρο της άρσης του απορρήτου.

Κατ' εξουσιοδότηση του προγενέστερου Ν. 2225/1994 έχει εκδοθεί το ΠΔ 47/2005[132], το οποίο εξειδικεύει πληρέστερα τις διαδικασίες και τις τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου. Η άρση του απορρήτου συνιστά μία ειδική ανακριτική πράξη για την οποία πρέπει να τηρείται η αρχή της αναλογικότητας, όπως προκύπτει από το άρθρο 1 του ΠΔ 47/2005, δηλαδή να γίνεται στάθμιση κάθε φορά μεταξύ της ελεύθερης επικοινωνίας και των σκοπών που επιδιώκει η άρση και αυτή να επιλέγεται ως η έσχατη λύση όταν τα προηγούμενα μέσα προς την επίτευξη των σκοπών δεν τελεσφόρησαν, και, επιπρόσθετα στο μέτρο και για όσο χρόνο κρίνεται απολύτως αναγκαίο.

8.6 Άρση απορρήτου στις σύγχρονες μορφές επικοινωνίας

8.6.1 Κρυπτογράφηση

Όπως είδαμε στην αρχή της παρούσας, στη σύγχρονη πραγματικότητα οι επικοινωνίες διεξάγονται μέσω εφαρμογών άμεσης ανταλλαγής μηνυμάτων, όπως είναι το WhatsApp, το Viber κλπ. Σε αντίθεση με τα SMS, τα οποία αποστέλλονται εντός δικτύου κινητής τηλεφωνίας, η επικοινωνία μέσω των εφαρμογών αυτών μεταδίδεται μέσω του Διαδικτύου. Οι προγραμματιστές αυτών των εφαρμογών, προκειμένου να προστατευτούν οι μεταδιδόμενες επικοινωνίες, έχουν αναπτύξει Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies –PETs), όπως για παράδειγμα η κρυπτογράφηση. Μάλιστα, αξίζει να σημειωθεί ότι η κρυπτογράφηση προκρίνεται από το κείμενο του ΓΚΠΔ[133] ως πολύ σημαντικό μέτρο ασφάλειας έναντι των κινδύνων που συνεπάγεται η επεξεργασία των προσωπικών δεδομένων.

Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για την προστασία δεδομένων τόσο σε κατάσταση ηρεμίας ("data at rest") όσο και κατά τη μετάδοσή τους ("data in transit")[134].

---

[132] Προεδρικό Διάταγμα 47/2005 - ΦΕΚ Α΄64/10-3-2005 *Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του*

[133] Αιτιολογική Σκέψη 83 και Άρθρο 32

[134] Information Commissioner's Office (ICO),What is encryption?, διαθέσιμο στο: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/what-is-encryption/

8.6.1.1 Κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας

Η κρυπτογράφηση δεδομένων σε κατάσταση ηρεμίας λειτουργεί[135] σε επίπεδο συσκευής, κρυπτογραφώντας δεδομένα που βρίσκονται σε μια φυσική συσκευή, όπως για παράδειγμα ένα laptop, ένα smartphone, μια μονάδα σκληρού δίσκου ή ένα USB. Για να αποκτήσει κάποιος πρόσβαση στα κρυπτογραφημένα δεδομένα της συσκευής πρέπει να είναι εξουσιοδοτημένος χρήστης που κατέχει το κλειδί αποκρυπτογράφησης. Αυτό το είδος κρυπτογράφησης προστατεύει τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση, καθώς και σε περίπτωση απώλειας ή κλοπής.

Μία μορφή κρυπτογράφησης δεδομένων σε κατάσταση ηρεμίας είναι η Full Disk Encryption (FDE)[136]. Το FDE κρυπτογραφεί το συνολικό περιεχόμενο της συσκευής, συμπεριλαμβανομένου του λειτουργικού συστήματος, των αρχείων του συστήματος και των δεδομένων του χρήστη. Για να αποκτήσει κάποιος πρόσβαση στη συσκευή, θα πρέπει να κατέχει το κλειδί αποκρυπτογράφησης, το οποίο συνήθως θα είναι ένας κωδικός πρόσβασης που ξεκλειδώνει την κρυπτογράφηση και δίνει πρόσβαση στα δεδομένα. Χωρίς το σωστό κλειδί αποκρυπτογράφησης, τα δεδομένα στο συσκευή είναι ουσιαστικά μη αναγνώσιμα.

8.6.1.2 Κρυπτογράφηση δεδομένων κατά τη μετάδοσή τους

Αντίθετα, η κρυπτογράφηση δεδομένων κατά τη μετάδοσή τους λειτουργεί[137] καθώς τα δεδομένα μεταδίδονται μέσω ενός δικτύου, όπως είναι το Διαδίκτυο. Όταν τα δεδομένα μεταδίδονται μέσω ενός δικτύου, αυτομάτως καθίστανται ευάλωτα σε κινδύνους υποκλοπών από χάκερ και άλλους εισβολείς. Η κρυπτογράφηση δεδομένων κατά τη μετάδοσή τους προστατεύει τα δεδομένα από αυτούς τους κινδύνους μετατρέποντας τα αρχικά δεδομένα σε μη αναγνώσιμη μορφή που μπορεί να αποκρυπτογραφηθεί μόνο από κάποιον που κατέχει το σωστό κλειδί αποκρυπτογράφησης. Επομένως αποτρέπει την υποκλοπή των δεδομένων και τη μη εξουσιοδοτημένη πρόσβαση σε αυτά, καθώς μεταδίδονται.

---

[135] Pratik Prakash Dixit (2018) Conceptualising Interaction between Cryptography and Law, 11 NUJS L. REV. 327, διαθέσιμο στο: http://nujslawreview.org/wp-content/uploads/2019/01/11.3-Pratik-Prakash-Dixit-CONCEPTUALISING-INTERACTION-BETWEEN-CRYPTOGRAPHY-AND-LAW.pdf

[136] Information Commissioner's Office (ICO), Encryption and data storage, διαθέσιμο στο: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/encryption-and-data-storage/

[137] WinZip Enterprise, Encrypting data in transit: What is it and why do you need to do it?, διαθέσιμο στο: https://winzip.com/blog/enterprise/encrypting-data-in-transit/

Αυτού του είδους η κρυπτογράφηση έχει πρακτική χρησιμότητα σε ευρύ φάσμα οργανισμών, για την προστασία ευαίσθητων πληροφοριών, όπως είναι για παράδειγμα οι κωδικοί πρόσβασης και οι κωδικοί πιστωτικών καρτών, διασφαλίζοντας το απόρρητό τους καθώς μεταδίδονται μέσω δικτύου.

8.6.1.3 Η κρυπτογράφηση στις επικοινωνίες

Η κρυπτογράφηση είναι ένα πολύ σημαντικό εργαλείο για την προστασία του απορρήτου των επικοινωνιών. Οι χρήστες έχουν συνδέσει τις σύγχρονες εφαρμογές επικοινωνίας με την ασφάλεια των επικοινωνιών τους, ακριβώς επειδή προσφέρουν κρυπτογραφημένη επικοινωνία. Πολλές εφαρμογές, όπως είναι για παράδειγμα το WhatsApp[138] και το Viber[139], χρησιμοποιούν την ειδικότερη μορφή κρυπτογράφησης δεδομένων κατά τη μετάδοσή τους, end-to-end encryption (E2EE). Στην E2EE[140], που στα ελληνικά ονομάζεται "κρυπτογράφηση από άκρο σε άκρο", το περιεχόμενο της επικοινωνίας κρυπτογραφείται στην πηγή του, δηλαδή στη συσκευή του αποστολέα πριν αποσταλεί και μπορεί να αποκρυπτογραφηθεί μόνο στη συσκευή του χρήστη, όταν παραληφθεί. Κατά την αποστολή ενός μηνύματος, η μετάδοση πραγματοποιείται ως εξής[141]: το μήνυμα φεύγει από τον Internet Service Provider (ISP) του αποστολέα, περνά από τον διακομιστή (server) της εφαρμογής και από τον ISP του παραλήπτη, και τέλος φθάνει στον παραλήπτη. Σε αυτή τη διαδρομή κανένας δεν μπορεί να διαβάσει το περιεχόμενο (plaintext) της επικοινωνίας, το οποίο βρίσκεται σε κρυπτογραφημένη μορφή κατά την μετάδοσή του. Τα κλειδιά της αποκρυπτογράφησης τα έχουν μόνο οι χρήστες (τα μέρη της επικοινωνίας), ενώ ούτε οι ISPs ούτε οι πάροχοι των υπηρεσιών επικοινωνίας (όπως είναι η WhatsApp) αποκτούν πρόσβαση στα κλειδιά.

Μπορούμε να πούμε ότι οι εφαρμογές IM συμφέρουν. Είναι ευρέως διαδεδομένες, παρέχονται δωρεάν, η χρήση τους είναι απλή και γρήγορη και διευκολύνουν τις ασφαλείς επικοινωνίες. Βέβαια, από την άλλη, λόγω της ευρείας χρησιμοποίησης των εφαρμογών αυτών και των δυνατοτήτων κρυπτογράφησης που προσφέρουν, μπορούν κάλλιστα να χρησιμοποιηθούν και με καταχρηστικό τρόπο. Η χρήση τους καθίσταται ένα ισχυρό εργαλείο στα χέρια των

[138] https://faq.whatsapp.com/820124435853543/?helpref=uf_share

[139] https://www.viber.com/en/security/

[140] Thiago Moraes (2020) *Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures*, European Data Protection Law Review (EDPL) 6, no. 1

[141] Wei Bai, Michael Pearson, Patrick Gage Kelley, Michelle L. Mazurek (2020) I*mproving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study*, IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)

εγκληματιών, προκειμένου να διευκολυνθεί η εγκληματική δραστηριότητα.

8.6.2 Άρση του απορρήτου των επικοινωνιών που διεξάγονται μέσω εφαρμογών επιφυών υπηρεσιών

Ανάγοντας το ζήτημα στα ελληνικά δεδομένα, το ΠΔ 47/2005, από νομικής πλευράς, υπάγει στην άρση του απορρήτου τις υπό συζήτηση μεθόδους επικοινωνίας και ορίζει ότι οι πάροχοι των υπηρεσιών είναι υποχρεωμένοι να ανταποκρίνονται στα αιτήματα των αρμοδίων αρχών και να συνεργάζονται μαζί τους, παρέχοντάς τους τα δεδομένα των επικοινωνιών, τα κλειδιά αποκρυπτογράφησης κλπ. Ωστόσο, όπως θα δούμε κατωτέρω, δεν είναι πάντα εύκολο να υλοποιηθούν αυτές οι δυνατότητες.

8.6.3 Πώς θα μπορούσαν οι αρχές επιβολής του νόμου να αποκτήσουν πρόσβαση στα κρυπτογραφημένα δεδομένα;

8.6.3.1 Εντολή άρσης της αποκρυπτογράφησης

Μία λύση είναι να διατάσσουν οι αρχές την άρση της αποκρυπτογράφησης. Ποιος όμως θα άρει την αποκρυπτογράφηση από τη στιγμή που οι επικοινωνίες μεταδίδονται μέσω του Διαδικτύου; Αναγκαστικά οι αρχές θα πρέπει να στραφούν στις ιδιωτικές εταιρείες – κατασκευαστές των εφαρμογών επικοινωνίας. Τίθεται το ζήτημα πώς οι αρχές θα εξαναγκάσουν ιδιωτικές εταιρείες να τους παρέχουν πρόσβαση στις επικοινωνίες των πελατών τους; Και ενώ παραδοσιακά οι νομοθεσίες επιβάλλουν τη συνδρομή του ιδιωτικού τομέα για την παρακολούθηση των επικοινωνιών, τις νόμιμες επισυνδέσεις, αυτή η πρακτική συνήθως αφορά τα δίκτυα κινητής τηλεφωνίας.

Όμως, το να εξαναγκάσεις μία ιδιωτική εταιρεία να "σπάσει" την κρυπτογράφηση των συστημάτων της είναι κάτι πολύ διαφορετικό. Καταρχάς, οι εταιρείες, προκειμένου να ανταποκριθούν σε κάτι τέτοιο, θα έπρεπε ουσιαστικά να αποδυναμώσουν[142] τα συστήματά τους, δημιουργώντας τρωτά σημεία που θα επέτρεπαν την παράκαμψη της κρυπτογράφησης. Τι θα κέρδιζε μία εταιρεία εάν το έκανε αυτό; Οι εταιρείες σχεδιάζουν τα προϊόντα τους με

[142] O. S. Kerr and B. Schneier (2017) *Encryption Workarounds*, 106 Georgetown Law Journal 989, διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

αυτές τις πολύ ισχυρές μεθόδους ασφαλείας, με σκοπό το κέρδος. Η αποδυνάμωση της κρυπτογράφησης θα έθετε σοβαρά ζητήματα ασφαλείας[143], τα οποία θα μπορούσαν να βλάψουν τη φήμη της εταιρείας και να οδηγήσουν σε απώλεια της εμπιστοσύνης των χρηστών, οι οποίοι βασίζονται σε αυτές τις εφαρμογές για να επικοινωνούν με ασφάλεια[144]. Εάν οι χρήστες γνώριζαν ότι η εταιρεία μπορεί να υποχρεωθεί να να αποδυναμώσει την κρυπτογράφηση και ουσιαστικά να αποκαλυφθούν οι επικοινωνίες τους, θα απομακρυνόταν από τη χρήση τους. Επιπρόσθετα, η αποδυνάμωση της κρυπτογράφησης θα μπορούσε να διευκολύνει τους χάκερ και άλλους κακόβουλους παράγοντες να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες, θέτοντας τους χρήστες σε κίνδυνο[145].

Αναδύεται και το πάρα πολύ σημαντικό ζήτημα της δικαιοδοσίας. Πώς για παράδειγμα οι αρχές της Ελλάδα θα εξανάγκαζαν τις αμερικανικές εταιρείες, προϊόντα των οποίων αποτελούν οι διαδεδομένες αυτές εφαρμογές, να τους δώσουν πρόσβαση στις επικοινωνίες χρηστών που διεξάγονται με κρυπτογράφηση;

Η ως άνω επιλογή έχει χαρακτηριστεί ως "*back door*"[146], καθώς πρόκειται περί κρυφού/μυστικού τρόπου αποφυγής των μέτρων ασφαλείας ενός συστήματος, με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο σύστημα ή στα δεδομένα. Μέσω μίας back door αποκτάται πρόσβαση στα κρυπτογραφημένα δεδομένα παρακάμπτοντας την κρυπτογράφηση[147] .

8.6.3.2 Εισαγωγή κλειδιού αποκρυπτογράφησης

Μία άλλη επιλογή είναι η "*front door*[148]", η οποία σημαίνει ότι οι αρχές αποκτούν πρόσβαση στις κρυπτογραφημένες επικοινωνίες των χρηστών μέσω των μέτρων ασφαλείας των συσκευών

---

[143] Milana Pisaric (2022) Communications encryption as an investigative obstacle, Journal of Criminology and Criminal Law (JCCL)

[144] The Crypto Blog, The Battle against Encryption: Government's Quest for Backdoor Access to Encrypted Communication Devices, διαθέσιμο στο: https://cryptoblog101.medium.com/the-battle-against-encryption-governments-quest-for-backdoor-access-to-encrypted-communication-5771dcb4f95

[145] Human Rights Watch (2017) Perils of Back Door Encryption Mandates, διαθέσιμο στο: https://www.hrw.org/news/2017/06/26/perils-back-door-encryption-mandates

[146] Donald L. Buresh (2021) *The Battle for Backdoors and Encryption Keys*, Journal of Current Scientific Research, Volume 1, Issue 3, διαθέσιμο στο: https://openaccesspub.org/current-scientific-research/article/1657

[147] Cloudwards.net, How Do Encryption Backdoors Work in 2023? Privacy vs Surveillanc, διαθέσιμο στο: https://www.cloudwards.net/encryption-backdoors/

[148] Council of the European Union From EU Counter-Terrorism Coordinator To Delegations (2020) Law enforcement and judicial aspects of encryption, διαθέσιμο στο: https://data.consilium.europa.eu/doc/document/ST-7675-2020-INIT/en/pdf

τους. Πώς θα μπορούσε να επιτευχθεί κάτι τέτοιο στις κρυπτογραφημένες με E2EE επικοινωνίες;

Καταρχάς, όπως είδαμε, οι εταιρείες συνήθως δεν διαθέτουν τα κλειδιά αποκρυπτογράφησης των χρηστών των εφαρμογών τους. Σε περίπτωση λοιπόν που διατάξουν οι διωκτικές αρχές την αποκρυπτογράφηση των επικοινωνιών, οι εταιρείες, ακόμα και σε περίπτωση που θα ήταν πρόθυμες να συνεισφέρουν, δεν θα ήταν πρακτικά σε θέση, αφού δεν διαθέτουν τα κλειδιά αποκρυπτογράφησης[149].

Εφόσον το ανωτέρω δεν είναι εφικτό, έχουν αναζητηθεί άλλοι τρόποι προκειμένου οι αρχές να "εισβάλλουν" στις συσκευές των χρηστών, "χακάροντας" τες. Αυτό θα μπορούσε να επιτευχθεί με την εκμετάλλευση τρωτών σημείων που υπάρχουν στις συσκευές[150].

Μία τεχνική είναι η "*zero-day vulnerability*" ("τρωτά σημεία ημέρας μηδέν")[151]. Αυτή εκμεταλλεύεται μια προηγουμένως άγνωστη ευπάθεια σε λογισμικό ή υλικό, η οποία μπορεί να μην έχει ανακαλυφθεί από τον προμηθευτή λογισμικού ή τους ερευνητές ασφαλείας και ως εκ τούτου, ενδέχεται να μην υπάρχει διαθέσιμη ενημέρωση κώδικα για την προστασία από την επίθεση. Μέχρι να ανακαλυφθεί από τους κατασκευαστές αυτή η ευπάθεια και να τη διορθώσουν μεσολαβεί ικανό χρονικό διάστημα ώστε οι χάκερς να κάνουν τη δουλειά τους.

Μία άλλη τεχνική είναι η επονομαζόμενη "*brute force*"[152] επίθεση, η οποία περιλαμβάνει τη δοκιμή όλων των πιθανών συνδυασμών χαρακτήρων, όπως γράμματα, αριθμοί και σύμβολα, για να βρεθεί ο κωδικός πρόσβασης, το κλειδί κρυπτογράφησης. Ουσιαστικά πρόκειται για τη δοκιμή κάθε πιθανού κλειδιού. Οι δοκιμές αυτές μπορούν να πραγματοποιηθούν χειροκίνητα, αλλά συχνά αυτοματοποιούνται χρησιμοποιώντας εξειδικευμένο λογισμικό ή σενάρια που μπορούν να δοκιμάσουν εκατομμύρια διαφορετικούς συνδυασμούς κωδικών πρόσβασης σε σύντομο χρονικό διάστημα.

---

149 Thiago Moraes (2020), ό.α.

150 Milana Pisaric (2022), ό.α.

151 U.K. Singh,C. Joshi, and D. Kanellopoulos (2019) *A framework for zero-day vulnerabilities detection and prioritization*, Journal of Information Security and Applications

152 O. S. Kerr and B. Schneier (2017), ό.α.

Ακόμα, υφίστανται τεχνικές που στοχεύουν στην παράκαμψη της κρυπτογράφησης Full Disk[153].

8.6.4 "*Going Dark*"

Όλες οι ως άνω πρακτικές δεν έχουν κριθεί αποτελεσματικές, λόγω της τεχνολογικής πολυπλοκότητας, με αποτέλεσμα οι διωκτικές αρχές να συναντούν εμπόδια στην προσπάθεια νόμιμης άρσης του απορρήτου. Το φαινόμενο αυτό είναι παγκοσμίως γνωστό ως "*Going Dark*"[154] και αναφέρεται στην αυξανόμενη πρόκληση που αντιμετωπίζουν οι διωκτικές αρχές όσον αφορά την πρόσβαση σε ψηφιακές πληροφορίες κατά τη διάρκεια ποινικών ερευνών λόγω της κρυπτογράφησης και άλλων μέτρων ασφαλείας που εμποδίζουν την πρόσβαση. Το πρόβλημα έγκειται στην έλλειψη τεχνολογικών μέσων εκ μέρους των διωκτικών αρχών, προκειμένου να αποκτήσουν πρόσβαση σε επικοινωνίες, έχοντας νόμιμη εξουσία να το κάνουν.

Η επίτευξη ισορροπίας μεταξύ αφενός του απορρήτου και της ασφάλειας των επικοινωνιών και αφετέρου της αποτελεσματικής εκτέλεσης των καθηκόντων των διωκτικών αρχών για την αντιμετώπιση της βαριάς εγκληματικότητας και των κινδύνων εθνικής ασφάλειας, αποτελεί τεράστια πρόκληση στο σύγχρονο τεχνολογικό περιβάλλον. Η εύρεση μιας μέσης λύσης που θα ικανοποιεί αμφότερες τις πλευρές απαιτεί προσεκτική εξέταση πολλαπλών παραγόντων, νομικών, τεχνικών και κοινωνικών, η οποία, προκειμένου να είναι αποτελεσματική, θα πρέπει να σέβεται τα θεμελιώδη ατομικά δικαιώματα και ελευθερίες.

Οι πάροχοι υπηρεσιών OTT δεν υπάγονται στο πεδίο εφαρμογής της Οδηγίας e-Privacy, σχετικά με τη δυνατότητα πρόβλεψης περιορισμών των δικαιωμάτων που αυτή προβλέπει, ζήτημα που αποπειράται να ρυθμιστεί με την υιοθέτηση της Πρότασης Κανονισμού e-Privacy.

Η παρ. 2 του Άρθρου 11 της Πρότασης Κανονισμού ορίζει ότι θα πρέπει να θεσπιστούν εκ μέρους των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών εσωτερικές διαδικασίες προκειμένου να ανταποκρίνονται σε αιτήματα πρόσβασης στα δεδομένα επικοινωνιών των

---

[153] Παραδείγματα τέτοιων τεχνικών στο: Thiago Moraes (2020), ό.α.

[154] James B. Comey (FBI) (2014) *Speeach at the Brookings Isnstitution, Going Dark: Are Technology, Privacy, and Public Sfety on a Collision Course?*, October 16,διαθέσιμο στο: https://www.americanrhetoric.com/speeches/jamescomeygoingdark.htm

τελικών χρηστών που υποβάλλουν οι αρμόδιες αρχές σύμφωνα με νομοθετικά μέτρα περιορισμών των δικαιωμάτων, σύμφωνα με την παρ. 1 του Άρθρου 11.

Ενόσω το πεδίο μένει αρρύθμιστο, το κενό που έχει δημιουργηθεί ελλείψει κανονιστικού πλαισίου, είναι γεγονός ότι έχει ανεξέλεγκτα ευνοήσει την ανάπτυξη παράνομων κατασκοπευτικών λογισμικών.

9. ΚΑΤΑΣΚΟΠΕΥΤΙΚΑ ΛΟΓΙΣΜΙΚΑ

9.1 Τι είναι τα κατασκοπευτικά λογισμικά[155]

Το κατασκοπευτικό λογισμικό εγκαθίσταται κρυφά στη συσκευή ενός χρήστη, χωρίς τη γνώση και τη συγκατάθεσή του, προκειμένου να παρακολουθεί τις δραστηριότητες της συσκευής, να συλλέγει πληροφορίες και να τις μεταδίδει σε έναν απομακρυσμένο διακομιστή, αυτού του ατόμου/οργανισμού που εγκατέστησε το κατασκοπευτικό λογισμικό.

Μπορεί να εγκατασταθεί σε μια συσκευή με διάφορους τρόπους, ανάλογα με τον συγκεκριμένο τύπο κατασκοπευτικού λογισμικού και τη συσκευή-στόχο. Μπορεί για παράδειγμα να εκμεταλλευτεί ευπάθειες του λογισμικού, να διαδοθεί από μολυσμένα αρχεία που βρίσκονται σε συνδέσμους ή λήψεις από κακόβουλους ιστότοπους ή σε συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου, να είναι προεγκατεστημένο από τον κατασκευαστή κ.ά.

Το κατασκοπευτικό λογισμικό παρακάμπτει τα μέτρα ασφαλείας της συσκευής, αποκτώντας πλήρη πρόσβαση στη συσκευή. Δεν είναι υπερβολή να λεχθεί ότι οι δυνατότητες που προσφέρει είναι ένα "όπλο" στα χέρια των διωκτικών αρχών, αν αναλογιστούμε ότι το περιεχόμενο ενός smartphone αντανακλά την προσωπικότητα του καθενός μας, αφού περιέχει πάρα πολλές πληροφορίες για τον χρήστη του, οι περισσότερες εκ των οποίων συνιστούν προσωπικά δεδομένα.

Η χρησιμοποίηση τέτοιων λογισμικών από τις διωκτικές αρχές/υπηρεσίες πληροφοριών που διαδραματίζεται κατά τρόπο ανεξέλεγκτο, χωρίς να υπόκειται σε νόμιμες προϋποθέσεις, είναι αναμφίβολα παράνομη. Ουδεμία σχέση έχει δε με τις νόμιμες επισυνδέσεις, την νόμιμη άρση του απορρήτου που διεξάγεται εντός του προβλεπόμενου νομοθετικού πλαισίου.

9.2. Χρήση παράνομων κατασκοπευτικών λογισμικών στην Ελλάδα

[155] European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2023), *The impact of Pegasus on fundamental rights and democratic processes*, διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EL.pdf

9.2.1 Παρελθοντικά γεγονότα

Στην Ελλάδα δεν είναι άγνωστες οι δυνατότητες χρήσης των κατασκοπευτικών λογισμικών. Προ εικοσαετίας σχεδόν, σύμφωνα με τον Απολογισμό Εταιρικής Υπευθυνότητας & Βιώσιμης Ανάπτυξης (Απρίλιος 2011- Μάρτιος 2012)[156] της εταιρείας Vodafone, "*Τον Μάρτιο του 2005, η Vodafone ενημερώθηκε για ένα περιστατικό ασφαλείας στο δίκτυό της. Λογισμικό ξένο προς το δίκτυο και ικανό να εκτελεί υποκλοπές εγκαταστάθηκε, χωρίς να το γνωρίζει η εταιρεία,σε λογισμικό δικτύου το οποίο δημιουργήθηκε, υποστηρίχθηκε και διατηρήθηκε από έναν εξωτερικό προμηθευτή.*" Η ΑΔΑΕ το 2006 συνέστησε Επιτροπή για να προβεί σε ελέγχους στις εγκαταστάσεις της Vodafone, κατόπιν των αποκαλύψεων των υποκλοπών και εξέδωσε Πορίσματα σχετικά με τη "*λειτουργία του παρείσακτου λογισμικού*"[157]. Το γεγονός αναδείχθηκε[158] σε ένα από τα μεγαλύτερα σκάνδαλα εκείνης της εποχής, καθώς παρακολουθήθηκαν παράνομα οι τηλεφωνικές επικοινωνίες μεγάλου αριθμού ατόμων του πολιτικού παρασκηνίου, ακόμα και του τότε πρωθυπουργού. Αξίζει μάλιστα να σημειωθεί ότι τα γεγονότα αυτά οδήγησαν στην θέσπιση του Ν. 3674/2008[159] "*Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις*" με τον οποίο ελήφθησαν πρόσθετα νομοθετικά μέτρα για την διασφάλιση του απορρήτου της επικοινωνίας και της ενίσχυσης του πλαισίου υποδομής του απορρήτου. Εντός αυτού του πλαισίου, εισήχθη στον Ποινικό Κώδικα η πρόβλεψη ποινικών κυρώσεων για την παραβίαση της ασφάλειας των επικοινωνιών, τροποποιήθηκε το άρθρο που αφορούσε την ποινική προστασία του απορρήτου ώστε εκτός από την παγίδευση ή παρέμβαση σε τηλεφωνική συσκευή ή σύνδεση, το αξιόποινο να επεκτείνεται και στο δίκτυο του Παρόχου, στο σύστημα υλικού ή λογισμικού του. Επίσης διευρύνθηκε το αξιόποινο της παραβίασης του απορρήτου και από πλημμέλημα αναβαθμίστηκε σε κακούργημα[160]. Οι συγκεκριμένες αναφορές σε αυτό το σημείο στόχο έχουν να αναδείξουν ότι δεν αποτελεί καινοφανές περιστατικό η επίσπευση της αυστηροποίησης της νομοθεσίας επ' αφορμή ενός γεγονότος που έλαβε μεγάλες διαστάσεις, δημιουργώντας

---

156 Διαθέσιμο στο https://www.vodafone.gr/

157 Περισσότερες πληροφορίες στην Έκθεση Πεπραγμένων Έτους 2006 της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, διαθέσιμο εδώ: http://www.adae.gr/fileadmin/docs/pepragmena/2006/KEFAL2.pdf

158 Για περισσότερες πληροφορίες, βλ. Η «άλωση» Vodafone από το λογισμικό των υποκλοπών, ΚΑΘΗΜΕΡΙΝΗ, 03.02.2006, διαθέσιμο στο: https://www.kathimerini.gr/politics/240962/i-alosi-vodafone-apo-to-logismiko-ton-ypoklopon/

159 Νόμος 3674/2008 - ΦΕΚ 136/Α/10-7-2008 *Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις*

160 Το 2019 ωστόσο με την τροποποίηση του ΠΚ το αδίκημα επαναφέρθηκε σε πλημμέλημα.

ανασφάλεια δικαίου, ιδίως ενόψει του ότι πρόκειται για ένα δικαίωμα που συνδέεται άρρηκτα με την ελευθερία της έκφρασης και συνακόλουθα με το δημοκρατικό πολίτευμα, όπως αναφέρθηκε ανωτέρω.

9.2.2 Σύγχρονα γεγονότα

Τον Ιούλιο του 2021 κυκλοφόρησε η είδηση[161] από το Citizen Lab του Πανεπιστημίου του Τορόντο, τη Διεθνή Αμνηστία και το Forbidden Stories ότι οι επικοινωνίες περίπου πενήντα χιλιάδων τηλεφωνικών αριθμών σε πολλές χώρες έτυχαν παρακολούθησης από παράνομο κατασκοπευτικό λογισμικό της Ισραηλινής εταιρείας NSO, το "Pegasus". Τα υποκείμενα των παρακολουθήσεων περιελάμβαναν, μεταξύ άλλων, δημοσιογράφους, υπέρμαχους των ανθρωπίνων δικαιωμάτων, πολιτικούς.

Παρόμοιο κατασκοπευτικό λογισμικό, το "Predator" χρησιμοποιήθηκε και στην Ελλάδα, όπως αποκαλύφθηκε από το Citizen Lab, για την παρακολούθηση των επικοινωνιών δημοσιογράφων και πολιτικών[162].

9.3 Πώς δουλεύει το λογισμικό Pegasus

Στην περιγραφή[163] της NSO για το προϊόν Pegasus, το οποίο υποστηρίζεται στα δημοφιλή λειτουργικά συστήματα BlackBerry, Android, iOS και Symbian, αναφέρεται ότι πρόκειται για μία επαναστατική λύση που, χρησιμοποιώντας τεχνολογίες αιχμής, διευκολύνει τις αρχές επιβολής του νόμου και τις υπηρεσίες πληροφοριών να εξάγουν εξ αποστάσεως κρυφά

---

161 Βλ. Forbidden Stories, *About the Pegasus Project*, διαθέσιμο στο: https://forbiddenstories.org/about-the-pegasus-project/, με συνεργάτες τους The Pegasus Project media partners: The Guardian, Le Monde, The Washington Post, Süddeutsche Zeitung, Die Zeit, Aristegui Noticias, Radio France, Proceso, OCCRP, Knack, Le Soir, Haaretz/TheMarker, The Wire, Daraj, Direkt36, PBS Frontline και με την τεχνική συνδρομή του Εργαστηρίου Ασφαλείας της Διεθνούς Αμνηστίας.

162 Για περισσότερες πληροφορίες, βλ. European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2023) *The use of Pegasus and equivalent surveillance spyware, The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware*, διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf Μάλιστα, στη σελ. 9 ανσφέρεται ότι στην Ελλάδα το Predator φαίνεται να χρησιμοποιήθηκε από την υπηρεσία πληροφοριών, ενώ το κράτος ισχυρίζεται ότι δεν αγόρασε το λογισμικό.

163 Pegasus – Product Description, διαθέσιμο στο: https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf

πολύτιμες πληροφορίες από σχεδόν οποιαδήποτε κινητή συσκευή. Πώς το κάνει αυτό; Παρακάμπτοντας κωδικούς πρόσβασης, ξεπερνώντας την κρυπτογράφηση, παρέχοντας απεριόριστη πρόσβαση στη συσκευή-στόχο για τη απομακρυσμένη συλλογή πληροφοριών, με την παρακολούθηση σε ζωντανό χρόνο των VoIP κλήσεων, παρακολουθώντας τις εφαρμογές (αυτές είναι μερικές από τις δυνατότητες που περιγράφονται). Και όλα αυτά διαδραματίζονται χωρίς να μεσολαβήσει κάποια ενέργεια του χρήστη της συσκευής, δηλαδή το Pegasus εγκαθίσταται χωρίς να το καταλάβει ο στόχος και επιτρέπει τις λεγόμενες "*zero-click attacks*" (*επιθέσεις χωρίς κλικ*). Ακόμα, αναφέρει ότι δεν αφήνει ίχνη στη συσκευή-στόχο. Μάλιστα, παρουσιάζεται ως λύση για την αντιμετώπιση της εγκληματικότητας και της τρομοκρατίας, ξεπερνώντας τα τεχνικά εμπόδια που έχουν θέσει οι σύγχρονες μορφές επικοινωνίας.

Το λογισμικό αυτό καθιστά τις συσκευές αντικείμενο παρακολούθησης εικοσιτέσσερις ώρες το εικοσιτετράωρο, παρέχοντας απεριόριστη πρόσβαση σε όλες τις πληροφορίες που βρίσκονται στη συσκευή. Δεν περιορίζεται όμως εκεί. Έχει πρόσβαση στην κάμερα και το μικρόφωνο της συσκευής, πράγμα που σημαίνει ότι μπορεί να παρακολουθήσει το περιρρέον περιβάλλον του στόχου σε πραγματικό χρόνο, βλέποντας και ακούγοντάς τον[164].

9.4 Οι επιπτώσεις των κατασκοπευτικών λογισμικών στην ιδιωτικότητα

Το Pegasus και τα παρεμφερή κατασκοπευτικά λογισμικά απέχουν πολύ από τα παραδοσιακά εργαλεία που χρησιμοποιούνται από τις διωκτικές αρχές, τις τηλεφωνικές επισυνδέσεις, οι οποίες διενεργούνται εντός ρυθμισμένου και ελεγχόμενου πλαισίου και με τη συνέργεια των τηλεπικοινωνιακών παρόχων. Τα κατασκοπευτικά λογισμικά, η χρήση των οποίων είναι αδιαφανής, επεκτείνουν την παρακολούθηση σε διάφορες πτυχές της ιδιωτικής ζωής του στόχου, εγείροντας ανησυχητικές επιπτώσεις.

Η υπό αυτές τις συνθήκες παρακολούθηση των επικοινωνιών συνιστά αναμφίβολα εξαιρετικά παρεμβατικό μέτρο στην ιδιωτικότητα. Απέχει μάλιστα πολύ από τα κριτήρια συμβατότητας με τις κανονιστικές προϋποθέσεις της ΕΣΔΑ, που έχει θέσει το ΕΔΔΑ (τα οποία αναλύθηκαν ανωτέρω). Το δικαίωμα στην ιδιωτική ζωή και η προστασία των προσωπικών δεδομένων από

[164] Λεπτομερέστερη περιγραφή στο: D. Pegg & S.Cutler (2021) *What is Pegasus spyware and how does it hack phones*, The Guardian, διαθέσιμο στο: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

παρεμβολές αποτελεί ακρογωνιαίο λίθο της ευρωπαϊκής έννομης τάξης. Περιορισμοί στο δικαίωμα της ελεύθερης επικοινωνίας, όπως είδαμε, καθίστανται κατ' εξαίρεση επιτρεπτοί μόνο εφόσον συντρέχουν εκείνες οι εξαιρετικού χαρακτήρα προϋποθέσεις για να αρθεί ο απόρρητος χαρακτήρας της ελεύθερης επικοινωνίας, οι οποίες αποτυπώνονται στα καταστατικά ευρωπαϊκά κείμενα.

Στο βαθμό που τα κατασκοπευτικά λογισμικά χρησιμοποιούνται πράγματι από τις διωκτικές αρχές και τις υπηρεσίες πληροφοριών για την αντιμετώπιση της βαριάς εγκληματικότητας και των κινδύνων για την εθνική ασφάλεια, δικαιολογείται καταρχάς ο περιορισμός του δικαιώματος της ελεύθερης επικοινωνίας. Δεν αρκεί όμως αυτό. Πρέπει να συντρέχουν όλα τα κριτήρια που έχουν διαπλαστεί από την νομολογία του ΕΔΔΑ, προκειμένου να καταγνωσθεί η συμβατότητα του μέτρου με τις απαιτήσεις της ΕΣΔΑ. Το ΕΔΔΑ έχει παρατηρήσει[165] ότι τα κράτη τείνουν, με στόχο την πρόληψη της τρομοκρατίας, να καταφεύγουν σε "*τεχνολογίες αιχμής*", προκειμένου να παρακολουθήσουν, ακόμα και μαζικά, τους στόχους οι οποίοι συνδέονται με κάποια υπόνοια. Οι εξελιγμένες τεχνολογικές δυνατότητες που προσφέρονται μπορούν να οδηγήσουν στην κατάρτιση λεπτομερούς προφίλ των υποκειμένων-στόχων. Γι' αυτό έχει τονίσει ότι εντός του πλαισίου αυτού πρέπει τα μέτρα που περιορίζουν την ελεύθερη επικοινωνία να συνοδεύονται από νομικές εγγυήσεις που διασφαλίζουν τον σεβασμό των θεμελιωδών δικαιωμάτων.

9.4.1 Κατασκοπευτικά λογισμικά και αρχή αναλογικότητας

Κατά πόσο τηρεί η διάχυτη παρακολούθηση μέσω των κατασκοπευτικών λογισμικών τις απαιτήσεις της αρχής της αναλογικότητας που τίθενται στην παρ. 2 του άρθρου 8 της ΕΣΔΑ; Καταρχάς, αναλογιζόμενοι απλά και μόνο την αλληλεπίδραση των ανθρώπων με τις ψηφιακές συσκευές τους στο πλαίσιο του ολοένα και ψηφιοποιούμενου περιβάλλοντος και τον όγκο των δεδομένων που υπάρχουν σε αυτές τις συσκευές, δύσκολα μπορούμε να καταλήξουμε στο συμπέρασμα ότι τα λογισμικά σαν το Pegasus πληρούν τις προϋποθέσεις της αναλογικότητας. Πιο αναλυτικά:

[165] Βλ. Απόφαση ΕΔΔΑ (2016) *Szabó and Vissy v. Hungary* παρ. 68

9.4.1.1 Είναι αναγκαίο το μέτρο;

Το ΕΔΔΑ ως προς το κριτήριο της αναγκαιότητας στο πλαίσιο χρησιμοποίησης τεχνολογιών αιχμής για τον περιορισμό του δικαιώματος, προϋποθέτει "*απόλυτη αναγκαιότητα*" ("*strict necessity*") για τη διαφύλαξη δημοκρατικών θεσμών, η οποία αφορά την απόκτηση μόνο των "*ζωτικής σημασίας πληροφοριών*" ("*obtaining of vital intelligence*")[166].

Εντούτοις, τα κατασκοπευτικά λογισμικά παρεισφρέουν στο σύνολο των πληροφοριών που σχετίζονται με τη συσκευή του στόχου. Εκτός από εκείνα τα δεδομένα της επικοινωνίας που κρίνονται αναγκαία, δίνεται πρόσβαση σε πληθώρα άσχετων πληροφοριών οι οποίες δεν ενδιαφέρουν τις αρχές. Μεταξύ αυτών ενδέχεται να βρίσκονται ακόμα και δεδομένα υγείας και άλλα είδη ειδικών κατηγοριών προσωπικών δεδομένων.

Αναδύεται και το ζήτημα της επέκτασης της παρακολούθησης επιπρόσθετων του στόχου ατόμων, αφού τα κατασκοπευτικά λογισμικά κάνουν χρήση κάμερας και μικροφώνου στο χώρο. Αναπόφευκτα η παρακολούθηση εκτείνεται στα μέλη της οικογένειάς του στόχου, στους συναδέλφους του στη δουλειά, ή σε όποιον τυγχάνει να βρίσκεται κοντά του.

Με αυτή τη διάχυτη επιτήρηση πλήττονται ουσιαστικά όλες οι εκφάνσεις της ιδιωτικής σφαίρα τους ατόμου, η ιδιωτική ζωή, η οικογενειακή ζωή, η κατοικία και η "αλληλογραφία"[167].

9.4.1.2 Οι επιπτώσεις των κατασκοπευτικών λογισμικών σε άλλα θεμελιώδη δικαιώματα

Μία μελέτη[168] του Θεματικού Τμήματος Δικαιωμάτων των Πολιτών και Συνταγματικών Υποθέσεων του Ευρωπαϊκού Κοινοβουλίου ανέδειξε την επιρροή των κατασκοπευτικών λογισμικών, πέραν του δικαιώματος της ιδιωτικής ζωής, και σε σειρά θεμελιωδών δικαιωμάτων τα οποία σχετίζονται με την θέση του ατόμου εντός της δημοκρατικής δομής της κοινωνίας. Θίγεται το δικαίωμα στην ελευθερία της έκφρασης όταν οι άνθρωποι, υπό τον φόβο ότι ενδέχεται οι επικοινωνίες τους να τύχουν παρακολούθησης, περιορίζουν την έκφραση των απόψεών τους κατά τις επικοινωνίες τους με άλλους ανθρώπους. Θίγεται με τον ίδιο τρόπο το

---

166 Βλ. Απόφαση ΕΔΔΑ (2016) *Szabó and Vissy v. Hungary* παρ. 73

167 Πρόκειται για τις τέσσερις επί μέρους εκφάνσεις της ιδιωτικής ζωής που αναφέρονται στο άρθρο 8 της ΕΣΔΑ.

168 European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2023), *The impact of Pegasus on fundamental rights and democratic processes*, διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EL.pdf

δικαίωμα "*να αναζητεί, να παίρνει και να διαδίδει πληροφορίες και ιδέες, με οποιοδήποτε μέσο έκφρασης*[169]".

Ο αντίκτυπος στα δικαιώματα αυτά καθίσταται πιο έντονος στην περίπτωση που ο στόχος είναι δημοσιογράφος ή πολιτικός, οι οποίοι ως εκ της ιδιότητάς τους διαδραματίζουν ενεργό ρόλο στη διατύπωση θέσεων και απόψεων στη δημόσια σφαίρα[170]. Κατ' επέκταση η μελέτη περιγράφει ακόμα τον τρόπο με τον οποίο επηρεάζεται το δικαίωμα του συνέρχεσθαι και του συνεταιρίζεσθαι όταν οι άνθρωποι, υπό τον φόβο της διαρκούς παρακολούθησης αποφεύγουν να συμμετάσχουν σε συναθροίσεις για ανταλλαγή πολιτικών και άλλων απόψεων. Η δημόσια σφαίρα στις δημοκρατικές κοινωνίες προϋποθέτει την ενεργή συμμετοχή των πολιτών, την οποία υποσκάπτουν τα κατασκοπευτικά λογισμικά.

Η χρήση τέτοιων λογισμικών δεν συνιστά επομένως το λιγότερο επαχθές μέτρο που θα μπορούσε να χρησιμοποιηθεί ως προς τον επιδιωκόμενο σκοπό.

9.4.1.3 Είναι κατάλληλο το μέτρο;

Το μέτρο είναι αναμφίβολα πρόσφορο να επιφέρει τον επιδιωκόμενο σκοπό της παρακολούθησης των επικοινωνιών του στόχου. Ωστόσο, κρίνεται καταχρηστικό λόγω των ευρειών δυνατοτήτων που προσφέρει.

9.4.1.4 Εν στενή εννοία αναλογικότητα

Εξετάζοντας και το τελευταίο στάδιο της αρχής της αναλογικότητας, αυτό της "εν στενή εννοία" αναλογικότητας, το μέτρο κρίνεται δυσανάλογο ως προς τον σκοπό που επιδιώκει, θίγοντας τον πυρήνα του δικαιώματος. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων έχει τονίσει[171] ότι το επίπεδο παρέμβασης στο δικαίωμα στην ιδιωτική ζωή είναι τόσο σοβαρό που στην πραγματικότητα το άτομο στερείται του δικαιώματος[172]. Το ΔΕΕ έχει επισημάνει ότι ένας

---

169 Άρθρο 19 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα

170 Βλ. σελ. 34 της μελέτης: "*Οι δημοσιογράφοι που κατασκοπεύονται μπορεί να μην είναι σε θέση να κάνουν ρεπορτάζ —από φόβο ότι οι εμπιστευτικές επαφές τους παρακολουθούνται, παραδείγματος χάριν, ή λόγω εμποδίων που συναντούν στο ερευνητικό τους έργο—ή μπορεί να απέχουν από τη δημοσίευση ερευνών φοβούμενοι ανεπιθύμητες ενέργειες που βασίζονται σε εμπιστευτικές πληροφορίες που συλλέγονται από τις συσκευές τους. Παρόμοιες εκτιμήσεις ισχύουν και για τους πολιτικούς, όταν εξετάζονται στο πλαίσιο του ρόλου τους ως συνεισφερόντων στη δημόσια επικοινωνιακή σφαίρα.*"

171 European Data Protection Supervisor (2022) *Preliminary Remarks on Modern Spyware*, διαθέσιμο εδώ: https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

172 Μάλιστα, έχει επισημάνει ότι η σωρεία των συλλεχθεισών πληροφοριών μέσω ενός τέτοιου

περιορισμός δεν μπορεί να οδηγήσει στο να "*καταστεί κανόνας η παρέκκλιση από την καταρχήν υποχρέωση διασφάλισης του απορρήτου των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων*"[173].

Εκ των ανωτέρω καθίσταται προφανές ότι δεν έχει εφαρμογή η αρχή της αναλογικότητας σε τέτοιου είδους χρήση των κατασκοπευτικών λογισμικών[174]. Η ανεξέλεγκτη χρήση των εργαλείων αυτών χωρίς να πλαισιώνεται από ένα αυστηρό ρυθμισμένο πλαίσιο περιορισμών και ελέγχου, δεν συμπλέει με το κανονιστικό πλαίσιο της ΕΕ και οδηγεί σε υπονόμευση των θεμελιωδών δικαιωμάτων και του δημοκρατικού θεσμού, αποτελώντας πηγή πρωτοφανών κινδύνων για την ιδιωτικότητα. Όχι αδίκως, έχει χαρακτηριστεί[175] ως το πιο ισχυρό εργαλείο hacking, συνιστώντας "*a real game-changer*[176]" στον τομέα των ψηφιακών παρακολουθήσεων.

9.5 Θα μπορούσαν να χρησιμοποιηθούν με νόμιμο τρόπο τα κατασκοπευτικά λογισμικά;

Το πρόβλημα με τα κατασκοπευτικά λογισμικά είναι ότι χρησιμοποιούνται μυστικά και αδιαφανώς. Η άνευ συγκατάθεσης του υποκειμένου εισβολή τέτοιων λογισμικών στη συσκευή του, ελλείψει νομοθετικού πλαισίου και απόφαση εκ μέρους δικαστικής αρχής είναι αναμφίβολα παράνομη.

Όσο το πεδίο μένει αρρύθμιστο, το "*Going Dark*" πρόβλημα θα συνεχίσει να διογκώνεται. Πράγματι, τα κατασκοπευτικά λογισμικά αποτελούν σπουδαίο εργαλείο στα χέρια των διωκτικών αρχών, οι οποίες δεν έχουν κανένα άλλο μέσο να αποκτήσουν πρόσβαση στις κρυπτογραφημένες επικοινωνίες. Το πρόβλημα έγκειται στην ανεξέλεγκτη χρήση τους και στις παρεισφρυτικές δυνατότητες τους, εξαιτίας των οποίων και τα έχουμε "δαιμονοποιήσει".

εργαλείου θέτει ζήτημα περιορισμού του δικαιώματος στη δίκαιη δίκη του Άρθρου 47 του Χάρτη Θεμελιωδών Δικαιωμάτων, λόγω της δυσχέρειας αξιοποίησης των σχετικών με την υπόθεση πληροφοριών.

173 Απόφαση ΔΕΕ (2020) *La Quadrature du Net and Others συνεκδικαζόμενες υποθέσεις C-511/18, C-512/18 ,και C-520/18*, παρ. 111

174 Βλ. Α. Παπανικολάου (2022) *Επικοινωνιακό απόρρητο: προβληματισμοί για τη διασφάλιση ενός κλασικού δικαιώματος στο πεδίο των σύγχρονων κατασκοπευτικών λογισμικών*, SyntagmaWatch, διαθέσιμο εδώ: https://www.syntagmawatch.gr/

175 European Data Protection Supervisor (2022) ό.α.

176 European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2022) *Pegasus and surveillance spyware*, διαθέσιμο εδώ: διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

Πώς θα μπορούσε να βρεθεί λύση στο πρόβλημα; Με την νομιμοποίηση των κατασκοπευτικών λογισμικών, υπάγοντας τα σε κανονιστικές προϋποθέσεις[177].
Η ιδέα της νομιμοποίησης της χρήσης των κατασκοπευτικών λογισμικών εκ μέρους των κρατών σαφώς και συνεπάγεται ένα σύμπλεγμα ζητημάτων. Ωστόσο, όπως δεν μπορεί να αποδυναμωθεί ο πυρήνας του δικαιώματος στην ιδιωτικότητα στο βωμό της εθνικής ασφάλειας και στην πρόληψη της εγκληματικότητας, έτσι δεν μπορεί να συμβεί και το αντίθετο. Δεν μπορούμε να παραγνωρίζουμε το γεγονός ότι μέσω των σύγχρονων επικοινωνιακών εφαρμογών η εγκληματικότητα καλπάζει ανενόχλητα. Τα καταστατικά κείμενα της ΕΕ προάγουν την ισόρροπη στάθμιση μεταξύ αφενός των σκοπών γενικού ενδιαφέροντος, όπως είναι η εθνική ασφάλεια και η εγκληματικότητα και αφετέρου των θεμελιωδών δικαιωμάτων, όπως είναι το δικαίωμα της ιδιωτικότητας και η επιμέρους έκφανση της επικοινωνίας. Εξάλλου και το ΔΕΕ[178] έχει τονίσει ότι "*τα δικαιώματα που κατοχυρώνονται στα άρθρα 7, 8 και 11 του Χάρτη δεν αποτελούν απόλυτα προνόμια, αλλά πρέπει να λαμβάνονται υπόψη σε σχέση με τη λειτουργία τους εντός της κοινωνίας*".

Η χρήση των κατασκοπευτικών λογισμικών ως μέτρο άρσης του απόρρητου χαρακτήρα της επικοινωνίας θα μπορούσε να προβλεφθεί με τη θέσπιση κανόνων, συνοδευόμενων από τα ποιοτικά χαρακτηριστικά της προσβασιμότητας, προβλεψιμότητας και επαρκούς σαφήνειας της νομολογίας του ΕΔΔΑ.

Την άποψη της ανάγκης νομοθετικής ρύθμισης του εμπορίου και της χρήσης των κατασκοπευτικών λογισμικών εξέφρασε το Ευρωπαϊκό Κοινοβούλιο[179] και, με το σκεπτικό ότι η διαδικασία κατάστρωσης νομοθεσίας είναι χρονοβόρα, διατύπωσε όρους, με τη μορφή συστάσεων υπό τους οποίους η χρήση τους θα μπορούσε να θεωρείται νόμιμη. Ένα νομικό

---

177 Βλ. Αικατερίνα Παπανικολάου (2022), ό.α.

178 Απόφαση ΔΕΕ (2022) *Bundesrepublik Deutschland κατά SpaceNet AG (C-793/19) και Telekom Deutschland GmbH (C-794/19)*, Σκέψη 63. Στη συγκεκριμένη υπόθεση βέβαια εξετάζεται το κατά πόσο μπορούν να θεσπιστούν εθνικά μέτρα για τη χωρίς διάκριση διατήρηση των δεδομένων κινήσεως θέσεως για την προληπτική καταπολέμηση της εγκληματικότητας και την πρόληψη των σοβαρών απειλών κατά της δημόσιας ασφάλειας. Πάντως το συμπέρασμα στο οποίο καταλήγει στη Σκέψη 65 είναι ότι "*πρέπει να πραγματοποιηθεί ο αναγκαίος συγκερασμός των διαφόρων εμπλεκομένων θεμιτών συμφερόντων και δικαιωμάτων και να θεσπισθεί νομικό πλαίσιο το οποίο θα καθιστά δυνατό τον εν λόγω συγκερασμό*".

179 Ευρωπαϊκό Κοινοβούλιο (2023) *Σχέδιο σύστασης του Ευρωπαϊκού Κοινοβουλίου προς το Συμβούλιο και την Επιτροπή σε συνέχεια της διερεύνησης καταγγελλόμενων παραβάσεων και περιπτώσεων κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης*, διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EL.html

πλαίσιο που θα επέτρεπε τη χρησιμοποίηση τέτοιων εργαλείων, τηρουμένων των εγγυήσεων της πάγιας νομολογίας του ΕΔΔΑ, θα έπρεπε απαραιτήτως να προβλέπει εγγυήσεις σχετικές με τη διαδικασία. Η υπαγωγή της κρίσης ως προς τη χρησιμοποίηση ενός τέτοιου μέτρου στην εκ των προτέρων ουσιαστική κρίση μίας ανεξάρτητης ή δικαστικής αρχής, η οποία θα εποπτεύεται και θα λογοδοτεί σε τρίτο, ανεξάρτητο όργανο, θα έλυνε το ζήτημα της αδιαφάνειας. Η φύση των σκοπών που θα υπηρετεί ένα τέτοιο μέτρο θα πρέπει να είναι αυστηρά προσδιορισμένοι, στοχεύοντας στην προστασία της εθνικής ασφάλειας και στην πρόληψη και καταπολέμηση της βαριάς εγκληματικότητας. Φυσικά για την κατάφαση της νομιμότητας του μέτρου θα πρέπει να πληρούνται οι απαιτήσεις της αρχής της αναλογικότητας. Η αρχή της αναλογικότητας συνεπάγεται τη χρησιμοποίηση του μέτρου κατ' εξαίρεση, μόνο εφόσον έχουν εξαντληθεί όλα τα υπόλοιπα, λιγότερο επεμβατικά προς την ιδιωτικότητα μέτρα και δεν επετεύχθη ο αυστηρά προσδιορισμένος επιδιωκόμενος σκοπός, ο οποίος μπορεί να επιτευχθεί μόνο με τη χρήση κατασκοπευτικού λογισμικού. Ακόμα, σημαίνει ότι το όφελος που επιδιώκεται υπερτερεί σε σχέση με την επέμβαση στην ιδιωτικότητα. Η άδεια της αρχής θα πρέπει να προσδιορίζει και περαιτέρω στοιχεία του μέτρου της παρακολούθησης, όπως είναι η χρονική διάρκειά του, η οποία δεν θα πρέπει να ξεπερνά το απολύτως αναγκαίο χρονικό διάστημα, τα άτομα που θα τύχουν παρακολούθησης, στο πρόσωπο των οποίων θα πρέπει να συντρέχει κάποια εύλογη υπόνοια, και το εύρος της πρόσβασης στη συσκευή του στόχου, η οποία δεν θα πρέπει να εκτείνεται σε δεδομένα τρίτων προσώπων, σε δεδομένα άσχετα ως προς τον επιδιωκόμενο σκοπό, καθώς και σε δεδομένα που προστατεύονται από κάποιο απόρρητο, π.χ. ιατρικό. Πολύ σημαντικό είναι και το να γνωστοποιηθεί στο υποκείμενο το μέτρο, με όλες τις λεπτομέρειες διεξαγωγής του, κατά τη λήξη του, προκειμένου να είναι σε θέση να ασκήσει τα προβλεπόμενα εκ του νόμου δικαιώματά του.

Με τη συνδρομή όλων των ανωτέρω περιγραφομένων προϋποθέσεων και θεσμικών αντιβάρων, τα κατασκοπευτικά λογισμικά θα μπορούσαν να λειτουργούν ελεγχόμενα εντός νομοθετικού πλαισίου, όπως συμβαίνει επί του παρόντος και με τις νόμιμες επισυνδέσεις.

Στην Ελλάδα πάντως ουδέποτε υπήρχε νόμος που να προβλέπει διαδικασία άρσης του απορρήτου διαφορετική από τις νόμιμες επισυνδέσεις. Ως εκ τούτου είναι βέβαιο ότι η χρήση κατασκοπευτικού λογισμικού έχει γίνει παρανόμως.

Με το άρθρο 13[180] του Ν. 5002/2022 προβλέπεται η δυνατότητα ρύθμισης με προεδρικό διάταγμα των προϋποθέσεων της νόμιμης χρησιμοποίησης λογισμικών παρακολούθησης εκ μέρους των αρχών. Στην ουσία με την πρόβλεψη αυτό ανοίγει ο δρόμος για να μπορούν οι κρατικές αρχές να παρακολουθούν τις επικοινωνίες, πέρα από τις νόμιμες επισυνδέσεις, και με λογισμικά παρακολούθησης τύπου Pegasus/Predator. Η Μη Κερδοσκοπική Οργάνωση Homo Digitalis[181] επέκρινε το συγκεκριμένο άρθρο, διατυπώνοντας την άποψη ότι μιας τέτοιας ρύθμισης θα πρέπει να έχει προηγηθεί διαφανής ανοιχτή διαβούλευση.

Το Ευρωπαϊκό Κοινοβούλιο, πάντως, στο σχέδιο συστάσεων[182] του, αφού διαπιστώνει ότι στην Ελλάδα υπήρξαν "*παραβάσεις και κακοδιοίκηση κατά την εφαρμογή του δικαίου της Ένωσης*", την καλεί να αναδιαμορφώσει το υφιστάμενο πλαίσιο.

[180] Άρθρο 13 Προμήθεια λογισμικών και συσκευών παρακολούθησης από το Δημόσιο. "*Με προεδρικό διάταγμα, που εκδίδεται εντός τριών (3) μηνών από την έναρξη ισχύος του παρόντος, μετά από πρόταση των Υπουργών Προστασίας του Πολίτη, Εθνικής Άμυνας, Δικαιοσύνης και Ψηφιακής Διακυβέρνησης, καθορίζονται οι προϋποθέσεις υπό τις οποίες είναι επιτρεπτή η σύναψη συμβάσεων εκ μέρους κρατικών δομών για την προμήθεια λογισμικών ή συσκευών παρακολούθησης του άρθρου 370ΣΤ του Ποινικού Κώδικα για την εκπλήρωση των σκοπών τους, καθώς και επιπρόσθετοι όροι της χρήσης τους*."

[181] Με επίκεντρο της δράσης της την υπεράσπιση των δικαιωμάτων των ανθρώπων που χρησιμοποιούν το Διαδίκτυο στην Ελλάδα. Περισσότερα εδώ: https://www.homodigitalis.gr/

[182] Ευρωπαϊκό Κοινοβούλιο (2023), ό.α.

ΕΠΙΛΟΓΟΣ

Οι ραγδαίοι ρυθμοί εξέλιξης της τεχνολογίας οδηγούν στην εμφάνιση πληθώρας ζητημάτων προς ρύθμιση. Η αέναη ανάγκη υπαγωγής πρωτοπόρων τεχνολογικών εννοιών και προϊόντων σε κανόνες, πέρα από το ότι προϋποθέτει αναμφίβολα διεπιστημονική προσέγγιση, επιδρά και σε διάφορα ηθικά, οικονομικά και κοινωνικά ζητήματα, καθιστώντας τη ρύθμιση της τεχνολογίας πολυδιάστατο ζήτημα που απαιτεί συνεργασία, διάλογο ειδικών διαφόρων τομέων και διαρκή προσαρμογή.

Το πεδίο που αποπειράται να ρυθμίσει ο Κανονισμός e-Privacy είναι ιδιαιτέρως καινοτόμο και ο ρόλος που καλείται να διαδραματίσει στη λειτουργία της σύγχρονης ψηφιακής οικονομίας είναι κεφαλαιώδους σημασίας[183]. Οι εταιρείες τεχνολογίας και επικοινωνιών αλλά και ο κλάδος της ψηφιακής διαφήμισης, όπως παρουσιάστηκε ανωτέρω, βασίζουν τη λειτουργία τους στη συλλογή και περαιτέρω αξιοποίηση προσωπικών δεδομένων. Οι νέοι κανόνες αποπειρώνται να ενισχύσουν την προστασία της ιδιωτικότητας των τελικών χρηστών, ρυθμίζοντας πιο αυστηρά τη χρήση των δεδομένων από τέτοιες εταιρείες. Τα επιχειρηματικά μοντέλα των επιγραμμικών υπηρεσιών φαίνεται να επηρεάζονται άμεσα από τις διατάξεις της Πρότασης Κανονισμού, καθώς αυτές τους υπάγουν σε αυστηρότερες κανονιστικές υποχρεώσεις, σε σχέση με το υφιστάμενο πλαίσιο.

Το επιθυμητό είναι να επιτευχθεί ισορροπία μεταξύ αφενός της προστασίας της ιδιωτικότητας και αφετέρου της ανάπτυξης της καινοτομίας των τεχνολογικών προϊόντων[184], συμφέροντα αντικρουόμενα και με τεράστια σημασία για την αγορά, εξ αυτού του λόγου άλλωστε δεν έχει ψηφιστεί ακόμα, αλλά διεξάγεται lobbying επί σχεδόν μία πενταετία, κατά το οποίο αντιδρούν έντονα εκπρόσωποι της ψηφιακής οικονομίας.

[183] Β. Καρκατζούνης, Λ. Μήτρου (2020), ό.α.

[184] Αυτός είναι άλλωστε και ο στόχος, σύμφωνα με την Πρόταση της Πορτογαλικής Προεδρίας. (https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf)

ΒΙΒΛΙΟΓΡΑΦΙΑ

- **ΕΛΛΗΝΙΚΑ ΒΙΒΛΙΑ**

1. Ν. Παπαδόπουλος (2008) *ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ - ΕΡΜΗΝΕΥΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΑΡΘΡΟΥ 19 ΤΟΥ ΣΥΝΤΑΓΜΑΤΟΣ ΤΗΣ ΕΛΛΑΔΑΣ*, Νομική Βιβλιοθήκη

2. Π. Δαγτόγλου (2012) *Συνταγματικό Δίκαιο, Ατομικά και Κοινωνικά Δικαιώματα*, 4η Έκδοση, Εκδόσεις Σάκκουλα

3. Μ. Καραβίας σε Λ. Α. Σισιλιάνος (2013) *Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, Ερμηνεία κατ᾽ άρθρο*, Νομική Βιβλιοθήκη

4. Σπ. Βλαχόπουλος (2017) *ΘΕΜΕΛΙΩΔΗ ΔΙΚΑΙΩΜΑΤΑ*, 1η Έκδοση, ΝΒ

5. Ε. Μαργαρίτης (2020) *ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ & ΠΡΟΣΤΑΣΙΑ ΚΑΤΑΝΑΛΩΤΗ*, ΝΒ

- **ΕΛΛΗΝΙΚΗ ΑΡΘΡΟΓΡΑΦΙΑ**

1. Τσακυράκης Σ. (1993) *Το απόρρητο της επικοινωνίας – Απόλυτα απαραβίαστο ή ευχή της έννομης τάξης;*, ΝοΒ

2. Ν. Λίβος (1997) *Η ποινική προστασία των συνδετικών δεδομένων των τηλεπικοινωνιών*, ΠοινΧρ, ΜΖ΄

3. Λ. Μήτρου (2004) *Η νέα Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*, ΔΙΤΕ (π. ΔΙΜΕΕ) 3/2004

4. Γρ. Τσόλιας (2004) *Τα τηλεπικοινωνιακά δεδομένα υπό το πρίσμα του απορρήτου: προβληματισμοί εν όψει της ενσωμάτωσης της Οδηγίας 2002/58/ΕΚ*, ΔΙΤΕ (π. ΔΙΜΕΕ) 3/2004

5. Καϊδατζής Α. (2007) *Τηλεπικοινωνιακό απόρρητο και ασφάλεια των επικοινωνιών. Παρατηρήσεις στη ΣΕ (ΕΑ) 456/2007*, ΕφημΔΔ

6. Γρ. Τσόλιας (2008) *Η ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας σύμφωναμε τον Ν 3674/2008 (Παρουσίαση και ερμηνευτική προσέγγιση των διατάξεων)*, ΔΙΤΕ (π.ΔΙΜΕΕ) 3/2008

7. Σπ. Τάσσης (2014) *ΔΕΕ -δύο θεμελιώδεις αποφάσεις για τα προσωπικά μας δεδομένα και*

τα ηλεκτρονικά δίκτυα: Απόφαση C-131/12 (Google) και συνεκδικαζόμενες C-293/12 και C-594/12 (νομιμότητα υποχρεωτικής διατήρησης τηλεπικοινωνιακών δεδομένων), ΔΙΤΕ (π. ΔΙΜΕΕ) 3/2014

8. Γρ. Τσόλιας (2016) *Σημείωμα στην ΣτΕ 1593/2016- Η υπαγωγή των εξωτερικών στοιχείων της επικοινωνίας στην διαδικασία άρσης του απορρήτου και η διασφάλισή της από τους Παρόχους*, ΔΙΤΕ (π. ΔΙΜΕΕ) 4/2016

9. Β. Καρκατζούνης (2019) *Cookies και προστασία δεδομένων προσωπικού χαρακτήρα*, ΔΙΤΕ (π. ΔΙΜΕΕ) 2/2019

10. Α. Παπανικολάου (2020) *Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*, διαθέσιμο εδώ: https://www.constitutionalism.gr/2020-07-papanikolaou-aporito-epikinonias/

11. Β. Καρκατζούνης, Λ. Μήτρου (2020) *Online διαφήμιση και προστασία προσωπικών δεδομένων*, ΔΙΤΕ (π. ΔΙΜΕΕ) 1/2020

12. Μ. Σκόνδρα (2020) *Λήξη της προθεσμίας για τα Cookies: η συμμόρφωση που άργησε 8 χρόνια*, διαθέσιμο εδώ: www.gdprgroup.gr

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

14. Χ. Ράμμος, Σ. Γκρίτζαλης, Α. Παπανικολάου (2021) *Αντίθεση του άρθρου 87 Ν. 4790/2021 προς τις εγγυήσεις της ΕΣΔΑ για διαφύλαξη του απορρήτου των επικοινωνιών*, διαθέσιμο στο: https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/

15. Α. Παπανικολάου (2022) *Επικοινωνιακό απόρρητο: προβληματισμοί για τη διασφάλιση ενός κλασικού δικαιώματος στο πεδίο των σύγχρονων κατασκοπευτικών λογισμικών*, SyntagmaWatch, διαθέσιμο εδώ: https://www.syntagmawatch.gr/

- **ΞΕΝΟΓΛΩΣΣΗ ΑΡΘΟΓΡΑΦΙΑ**

1. Nicola Green N. και Sean Smith (2003) *«A Spy in your Pocket»? The Regulation of Mobile Data in the UK, Surveillance and Society*, Vol. 1 No. 4 : Surveillance and Mobilities, διαθέσιμο εδώ: https://www.researchgate.net/publication/265007629_'A_Spy_in_your_Pocket'_The_Regula

tion_of_Mobile_Data_in_the_UK

2. James B. Comey (FBI) (2014) Speeach at the Brookings Isnstitution, Going Dark: Are Technology, Privacy, and Public Sfety on a Collision Course?, October 16, διαθέσιμο στο: https://www.americanrhetoric.com/speeches/jamescomeygoingdark.htm

3. Giovanni Buttarelli (2017) *The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?*, 3 Eur. Data Prot. L. Rev. 155

4. O. S. Kerr and B. Schneier (2017) *Encryption Workarounds*, 106 Georgetown Law Journal 989, διαθέσιμο στο: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

5. Pratik Prakash Dixit (2018) Conceptualising Interaction between Cryptography and Law, 11

6. NUJS L. REV. 327, διαθέσιμο στο: http://nujslawreview.org/wp-content/uploads/2019/01/11.3-Pratik-Prakash-Dixit-CONCEPTUALISING-INTERACTION-BETWEEN-CRYPTOGRAPHY-AND-LAW.pdf

7. U.K. Singh,C. Joshi, and D. Kanellopoulos (2019) A *framework for zero-day vulnerabilities detection and prioritization*, Journal of Information Security and Applications

8. Wei Bai, Michael Pearson, Patrick Gage Kelley, Michelle L. Mazurek (2020) *Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study*, IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)

9. Thiago Moraes (2020) *Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures,* European Data Protection Law Review (EDPL) 6, no. 1

10. Donald L. Buresh (2021) *The Battle for Backdoors and Encryption Keys*, Journal of Current Scientific Research, Volume 1, Issue 3, διαθέσιμο στο: https://openaccesspub.org/current-scientific-research/article/1657

11. D. Pegg & S.Cutler (2021) *What is Pegasus spyware and how does it hack phones,* The Guardian, διαθέσιμο στο: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

12. Milana Pisaric (2022) *Communications encryption as an investigative obstacle,* Journal of Criminology and Criminal Law (JCCL)

13. Daniel J. Solove (2023), *Murky Consent: An Approach to the Fictions of Consent in Privacy Law,* 104 Boston University Law Review (Forthcoming) GWU Legal Studies Research Paper No. 2023-23 GWU Law School Public Law Research Paper

- **ΔΗΜΟΣΙΕΥΣΕΙΣ ΤΗΣ ΕΥΡΩΠΑΙΚΗΣ ΕΝΩΣΗΣ**

1. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2010) Γνώμη 2/2010 σχετικά με την επιγραμμική συμπεριφορική διαφήμιση, διαθέσιμο εδώ: https://www.dpa.gr/sites/default/files/2019-10/WP171_EL.PDF

2. European Parliament - Directorate General for Internal Policies, Policy Department A Economic and Scientific Policy (2015) *Over-the-top (OTT) players: market dynamics and policy changes,* διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf

3. Ευρωπαϊκή Επιτροπή (2015) *ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ Στρατηγική για την ψηφιακή ενιαία αγορά της Ευρώπης,* διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A52015DC0192

4. Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών (BEREC) (2016) *BEREC Report on OTT services,* διαθέσιμο εδώ: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-ott-services

5. Ευρωπαϊκή Επιτροπή (2017) *COMMISSION STAFF WORKING DOCUMENT Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC Accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0005

6. Ευρωπαϊκή Επιτροπή (2017) *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, διαθέσιμο εδώ: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-

communications

7. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2017) *Γνώμη 01/2017 σχετικά με την πρόταση κανονισμού για τον κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (2002/58/ΕΚ)*, διαθέσιμη στο: https://www.lawspot.gr/sites/default/files/misc/misc_legal/wp247_el.pdf

8. Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2017) *Γνώμη 06/2017 για την Πρόταση Κανονισμού e-Privacy*, διαθέσιμη στο: https://service.betterregulation.com/document/289246

9. European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2017) *An assessment of the Commission's Proposal on Privacy and Electronic Communications,* διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

10. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2018) *Δήλωση σχετικά με την αναθεώρηση του Κανονισμού για την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών (Κανονισμός ePrivacy) και τον αντίκτυπό της στην προστασία των φυσικών προσώπων όσον αφορά την ιδιωτικότητα και το απόρρητο των επικοινωνιών τους*, διαθέσιμη στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_el_0.pdf

11. Council of the European Union From EU Counter-Terrorism Coordinator To Delegations (2020) Law enforcement and judicial aspects of encryption, διαθέσιμο στο: https://data.consilium.europa.eu/doc/document/ST-7675-2020-INIT/en/pdf

12. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021) *Δήλωση 03/2021 σχετικά με τον κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*, διαθέσιμη στο: https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_el.pdf

13. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2021) *Δήλωση 03/2021 σχετικά με τον κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες,* διαθέσιμο εδώ: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_el

14. Δήλωση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ) σχετικά με την

αναθεώρηση του Κανονισμού για την Προστασία της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών (Κανονισμός ePrivacy) και τον αντίκτυπό της στην προστασία των φυσικών προσώπων όσον αφορά την ιδιωτικότητα και το απόρρητο των επικοινωνιών τους, διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_el_0.pdf

15. European Data Protection Supervisor (2022) *Preliminary Remarks on Modern Spyware*, διαθέσιμο εδώ: https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

16. European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2022) *Pegasus and surveillance spyware*, διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

17. European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2023), *The impact of Pegasus on fundamental rights and democratic processes*, διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EL.pdf

18. European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate - General for Internal Policies (2023) *The use of Pegasus and equivalent surveillance spyware, The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware*, διαθέσιμο εδώ: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf

19. Ευρωπαϊκό Κοινοβούλιο (2023) *Σχέδιο σύστασης του Ευρωπαϊκού Κοινοβουλίου προς το Συμβούλιο και την Επιτροπή σε συνέχεια της διερεύνησης καταγγελλόμενων παραβάσεων και περιπτώσεων κακοδιοίκησης κατά την εφαρμογή της νομοθεσίας της Ένωσης σε σχέση με τη χρήση του λογισμικού Pegasus και αντίστοιχου κατασκοπευτικού λογισμικού παρακολούθησης*, διαθέσιμο στο: https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EL.html

- **ΙΣΤΟΤΟΠΟΙ**

1. https://www.homodigitalis.gr/
2. Information Commissioner's Office (ICO), Encryption and data storage, διαθέσιμο στο: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/encryption-and-data-storage/
3. Information Commissioner's Office (ICO),*What is encryption?*, διαθέσιμο στο: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/what-is-encryption/
4. WinZip Enterprise, *Encrypting data in transit: What is it and why do you need to do it?*, διαθέσιμο στο: https://winzip.com/blog/enterprise/encrypting-data-in-transit/
5. Cloudwards.net, *How Do Encryption Backdoors Work in 2023? Privacy vs Surveillanc*, διαθέσιμο στο: https://www.cloudwards.net/encryption-backdoors/
6. https://www.itu.int/en/ITU-D/Statistics/Pages/about.aspx
7. Human Rights Watch (2017) Perils of Back Door Encryption Mandates, διαθέσιμο στο: https://www.hrw.org/news/2017/06/26/perils-back-door-encryption-mandates
8. The Crypto Blog, The Battle against Encryption: Government's Quest for Backdoor Access to Encrypted Communication Devices, διαθέσιμο στο: https://cryptoblog101.medium.com/the-battle-against-encryption-governments-quest-for-backdoor-access-to-encrypted-communication-5771dcb4f95
9. R. Barcelo, M.Buckwell (2018) *New European Electronic Communications Code means the application of the ePrivacy Directive to OTTs,* iapp, διαθέσιμο εδώ: https://iapp.org/news/a/new-european-electronic-communications-code-means-the-application-of-the-eprivacy-directive-to-otts/
10. https://cms.law/
11. Interactive Advertising Bureau Europe - IAB Europe (2018) *Position on the proposed ePrivacy Regulation,* διαθέσιμο στο: https://iabeurope.eu/wp-content/uploads/2019/10/31.10.2018-IABEU-ePR_Position_Paper.pdf
12. Developers Alliance (2018) *Updated Position Paper on the Proposal for an E-Privacy Regulation,* διαθέσιμο στο: https://developersalliance.org/position-papers/
13. Centre for Information Policy Leadership (CIPL) (2021) *Comments by the Centre for Information Policy Leadership on the Draft E-Privacy Regulation for the Purpose of the Trilogue Discussions*,

διαθέσιμο στο: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_draft_eprivacy_regulation__epr__for_the_epr_trilogues__29_sept_2021_.pdf

14. Διεθνές Εμπορικό Επιμελητήριο του Ηνωμένου Βασιλείου https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookiesguide_revnov.pdf

15. ΚΑΘΗΜΕΡΙΝΉ (2006) *Η «άλωση» Vodafone από το λογισμικό των υποκλοπών*, διαθέσιμο στο: https://www.kathimerini.gr/politics/240962/i-alosi-vodafone-apo-to-logismiko-ton-ypoklopon/

16. Forbidden Stories *About the Pegasus Project*, διαθέσιμο στο: https://forbiddenstories.org/about-the-pegasus-project/

17. Pegasus – Product Description, διαθέσιμο στο: https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf

18. Google Chrome (2019) *Building a more private web,* διαθέσιμο στο: https://www.blog.google/products/chrome/building-a-more-private-web/

19. Mozilla Firefox (2019) *Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default*, διαθέσιμο στο: https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

20. Chromium Blog (2020) *Building a more private web: A path towards making third party cookies obsolete*, διαθέσιμο στο: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

21. WebKit (2020) *Full Third-Party Cookie Blocking and More,* διαθέσιμο στο: https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

22. Forbes (2021) *Meta Will Soon Ban Targeting Ads Based On Sensitive Categories Including Religion And* Politics, διαθέσιμο στο: https://www.forbes.com/sites/martyswant/2021/11/09/meta-will-soon-ban-targeting-ads-based-on-sensitive-categories-including-religion-and-politics/?sh=2c0f9aa53b3d

- **ΕΛΛΗΝΙΚΗ ΝΟΜΟΛΟΓΙΑ**

1. Απόφαση 867/2002 ΣτΕ Υπόθεση σκληρού πυρήνα κρατικών εξουσιών Σχολιασμός: Καραμπασιάδης Αριστείδης, διαθέσιμο στο: http://www.greeklaws.com/pubs/uploads/1585.pdf

2. Γνωμοδότηση υπ' αριθμ. 9/2009, Εισαγγελία ΑΠ, Γ. Σανιδάς Εισαγγελέας Αρείου Πάγου

3. Γνωμοδότηση υπ' αριθμ. 12/2009, Εισαγγελία ΑΠ, Ι. Σ. Τέντες Εισαγγελέας Αρείου Πάγου

4. Απόφαση ΑΠ 711/2011

5. Απόφαση ΑΠ 203/2014

6. Απόφαση ΣτΕ 1593/2016 (Τμήμα Δ')

- **ΞΕΝΟΓΛΩΣΣΗ ΝΟΜΟΛΟΓΙΑ**

1. Απόφαση ΕΔΔΑ (1984) *Malone v. the United Kingdom*

2. Απόφαση ΕΔΔΑ (1990) *Kruslin v. France*

3. Απόφαση ΕΔΔΑ (2006) *Weber and Saravia v. Germany*

4. Απόφαση ΕΔΔΑ (2010) *Kennedy v United Kingdom*

5. Απόφαση ΕΔΔΑ (2014) *Fernández Martínez v. Spain*

6. Απόφαση ΕΔΔΑ (2015) *Zakharov v. Russia*

7. Απόφαση ΕΔΔΑ (2016) *Szabó and Vissy v. Hungary*

8. Απόφαση ΔΕΕ (2016) *Tele2 Sverige AB (C-203/15)*

9. Απόφαση ΔΕΕ (2020) *La Quadrature du Net and Others συνεκδικαζόμενες υποθέσεις C-511/18, C-512/18 και C-520/18*

10. Απόφαση ΕΔΔΑ (2021) *Big Brothers Watch and others v. the UK.*

11. Απόφαση ΔΕΕ (2022) *Bundesrepublik Deutschland κατά SpaceNet AG (C-793/19) και Telekom Deutschland GmbH (C-794/19)*

12. ΕΔΔΑ (2022) *Guide on Article 8 of the Convention – Right to respect for private and family life,* διαθέσιμο εδώ: https://www.echr.coe.int/documents/guide_art_8_eng.pdf

- **ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ**

1. Προεδρικό Διάταγμα 47/2005 - ΦΕΚ Α΄64/10-3-2005 *Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη*

διασφάλισή του

2. Νόμος 3471/2006 - ΦΕΚ 133/Α/28-6-2006 *Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997*

3. Νόμος 3674/2008 - ΦΕΚ 136/Α/10-7-2008 *Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις.*

4. Νόμος 4070/2012 - ΦΕΚ Α' 82/10.04.2012 *Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*

5. Νόμος 4790/2021 - ΦΕΚ 48/Α/31-03-2021 *Κατεπείγουσες ρυθμίσεις για την προστασία της δημόσιας υγείας από τις συνεχιζόμενες συνέπειες της πανδημίας του κορωνοϊού COVID-19, την ανάπτυξη, την κοινωνική προστασία και την επαναλειτουργία των δικαστηρίων και άλλα ζητήματα*

6. Νόμος 5002/2022 - ΦΕΚ Α 228/9.12.2022 *Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*

- **ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ**

1. Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046
2. Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα, διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A31997L0066
3. Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, 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), διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058
4. Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης

Νοεμβρίου 2009 , για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32009L0136

5. Οδηγία 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, διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:32006L0024
6. Πρόταση (2017) ΚΑΝΟΝΙΣΜΟΣ 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/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52017PC0010
7. Πρόταση (10.01.2021) ΚΑΝΟΝΙΣΜΟΣ 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/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), διαθέσιμο εδώ: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf
8. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex%3A32016R0679
9. Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, 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)

10. Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση), διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:52016PC0590

11. Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση), διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32018L1972

- **ΚΕΙΜΕΝΑ ΑΝΕΞΑΡΤΗΤΩΝ ΕΛΛΗΝΙΚΩΝ ΑΡΧΩΝ**

1. Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (2005) *Γνωμοδότηση 1/2005 κατόπιν αιτήματος της εταιρείας «ΤΙΜ ΕΛΛΑΣ» αναφορικά με τη διαδικασία άρσεως του απορρήτου στις τηλεφωνικές επικοινωνίες*, διαθέσιμο εδώ: http://www.adae.gr/fileadmin/docs/nomoi/893-2005.pdf

2. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2020) *Συστάσεις για τη συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες*, διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-ti-symmorfosi-ypeythynon-epexergasias-dedomenon-me-tin-eidiki

3. Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (2006) *Έκθεση Πεπραγμένων Έτους 2006*, διαθέσιμο εδώ: http://www.adae.gr/fileadmin/docs/pepragmena/2006/KEFAL2.pdf

4. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα *Τι είναι τα cookies*, διαθέσιμο εδώ: https://www.dpa.gr/index.php/el/cookies/plirofories/whatis_cookies

5. Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (2022) Δελτίο Τύπου για το υπό διαβούλευση νομοσχέδιο του Ν. 5002/2022, διαθέσιμο στο: http://www.adae.gr/enimerosi/leptomereies/article/bfont-size3-colorredapantisi-toy-proedroy-tis-adae-se-dimo-1/

- **ΑΛΛΑ**

1. https://faq.whatsapp.com/820124435853543/?helpref=uf_share
2. https://www.viber.com/en/security/
3. https://www.vodafone.gr/