Κατευθυντήριες γραμμές 2/2023 σχετικά με το τεχνικό πεδίο εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

Έκδοση 2.0

Εκδόθηκε στις 7 Οκτωβρίου 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Ιστορικό έκδοσης

Έκδοση 1.0	14 Νοεμβρίου 2023	Έγκριση κατευθυντήριων γραμμών για δημόσια διαβούλευση
Έκδοση 2.0	7 Οκτωβρίου 2024	Έγκριση κατευθυντήριων γραμμών μετά από δημόσια διαβούλευση

Περίληψη

Στις παρούσες κατευθυντήριες γραμμές, το ΕΣΠΔ εξετάζει την εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες σε διάφορες τεχνικές λύσεις. Οι παρούσες κατευθυντήριες γραμμές βασίζονται στη γνώμη 9/2014 της ομάδας εργασίας του άρθρου 29 σχετικά με την εφαρμογή της οδηγίας 2002/58/ΕΚ (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) στην αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος και αποσκοπούν στην παροχή σαφούς κατανόησης των τεχνικών λειτουργιών που καλύπτονται από το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Η εμφάνιση νέων μεθόδων ιχνηλάτησης τόσο για την αντικατάσταση των υφιστάμενων εργαλείων ιχνηλάτησης (για παράδειγμα, τα cookies, λόγω της διακοπής υποστήριξης για cookies τρίτων από ορισμένους πωλητές φυλλομετρητών) όσο και για τη δημιουργία νέων επιχειρηματικών μοντέλων αποτελεί μείζον ζήτημα προστασίας δεδομένων. Παρόλο που η εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες είναι καλά εδραιωμένη και η εν λόγω διάταξη εφαρμόζεται για ορισμένες τεχνολογίες ιχνηλάτησης, όπως τα cookies, χρειάζεται να αντιμετωπιστούν οι ασάφειες που σχετίζονται με την εφαρμογή της εν λόγω διάταξης στα αναδυόμενα εργαλεία ιχνηλάτησης.

Οι κατευθυντήριες γραμμές προσδιορίζουν τρία βασικά στοιχεία για την εφαρμογή του άρθρου 5 παράγραφος 3, της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (τμήμα 2.1), ήτοι τις «πληροφορίες», τον «τερματικό εξοπλισμό συνδρομητή ή χρήστη» καθώς και την «απόκτηση πρόσβασης» και «αποθήκευση πληροφοριών και αποθηκευμένες πληροφορίες». Οι κατευθυντήριες γραμμές παρέχουν περαιτέρω λεπτομερή ανάλυση κάθε στοιχείου (τμήμα 2.2-2.6).

Στο τμήμα 3, η ανάλυση αυτή εφαρμόζεται σε έναν μη εξαντλητικό κατάλογο περιπτώσεων χρήσης οι οποίες αντιπροσωπεύουν κοινές τεχνικές, και συγκεκριμένα:

- την ιχνηλάτηση μέσω URL και εικονοστοιχείων
- την τοπική επεξεργασία
- την ιχνηλάτηση με βάση μόνο τη διεύθυνση IP
- τις διακοπτόμενες και διαμεσολαβούμενες αναφορές στο διαδίκτυο των πραγμάτων (IoT)
- το μοναδικό αναγνωριστικό

Πίνακας περιεχομένων

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Έχοντας υπόψη το άρθρο 70 παράγραφος 1 στοιχείο ε) του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (εφεξής «ΓΚΠΔ»),

έχοντας υπόψη τη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο και ιδίως το παράρτημα XI και το πρωτόκολλο 37 αυτής, όπως τροποποιήθηκαν με την απόφαση της Μικτής Επιτροπής του ΕΟΧ αριθ. 154/2018 της 6ης Ιουλίου 2018,[1]

Έχοντας υπόψη το άρθρο 15 παράγραφος 3 της οδηγίας 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, όπως τροποποιήθηκε με την οδηγία 2009/136/ΕΚ (εφεξής «οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες» ή «ePD»),

Έχοντας υπόψη το άρθρο 12 και το άρθρο 22 του εσωτερικού κανονισμού του

ΕΞΕΔΩΣΕ ΤΙΣ ΑΚΟΛΟΥΘΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

1 ΕΙΣΑΓΩΓΗ

1. Σύμφωνα με το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, «*η αποθήκευση πληροφοριών, ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες, στον τερματικό εξοπλισμό συνδρομητή ή χρήστη*» επιτρέπεται μόνο με βάση τη συγκατάθεση ή την αναγκαιότητα για τους συγκεκριμένους σκοπούς που ορίζονται στο εν λόγω άρθρο. Όπως υπενθυμίζεται στην αιτιολογική σκέψη 24 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[2], στόχος της εν λόγω διάταξης είναι η προστασία του τερματικού εξοπλισμού των χρηστών, καθώς συνιστά μέρος της ιδιωτικής ζωής των χρηστών. Από τη διατύπωση του άρθρου προκύπτει ότι το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες δεν εφαρμόζεται αποκλειστικά στα cookies, αλλά και σε «παρόμοιες τεχνολογίες». Ωστόσο, επί του παρόντος δεν υπάρχει πλήρης κατάλογος των τεχνικών πράξεων που διέπονται από το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

[1] Οι αναφορές στα «κράτη μέλη» στο παρόν έγγραφο θα πρέπει να νοούνται ως αναφορές στα «κράτη μέλη του ΕΟΧ».

[2] «Ο τερματικός εξοπλισμός των χρηστών δικτύων ηλεκτρονικών επικοινωνιών και κάθε πληροφορία που αποθηκεύεται στον εξοπλισμό αυτόν συνιστούν μέρος της ιδιωτικής ζωής των χρηστών η οποία χρήζει προστασίας δυνάμει της ευρωπαϊκής σύμβασης για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών. Τα επιλεγόμενα κατασκοπευτικά λογισμικά, δικτυακοί «κοριοί», (web bugs) κρυφά αναγνωριστικά στοιχεία και άλλες παρόμοιες διατάξεις μπορούν να εισέλθουν στο τερματικό του χρήστη εν αγνοία του με σκοπό την πρόσβαση σε πληροφορίες, την αποθήκευση αθέατων πληροφοριών ή την ανίχνευση των δραστηριοτήτων του χρήστη, και συνιστούν ενδεχόμενη σοβαρή παραβίαση της ιδιωτικής ζωής του χρήστη. Η χρησιμοποίηση τέτοιων διατάξεων θα πρέπει να επιτρέπεται μόνο για θεμιτούς σκοπούς και εφόσον το γνωρίζουν οι αφορώμενοι χρήστες.».

2. Στη γνώμη 9/2014 της ομάδας εργασίας του άρθρου 29 (εφεξής «WP29») σχετικά με την εφαρμογή της οδηγίας 2002/58/ΕΚ (για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) στην αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος (εφεξής «γνώμη 9/2014 της ομάδας εργασίας του άρθρου 29») έχει ήδη διευκρινιστεί ότι το ψηφιακό αποτύπωμα εμπίπτει στο τεχνικό πεδίο εφαρμογής του άρθρου 5 παράγραφος 3[3] της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, αλλά λόγω των νέων εξελίξεων στις τεχνολογίες απαιτείται περαιτέρω καθοδήγηση όσον αφορά τις τεχνικές ιχνηλάτησης που παρατηρούνται σήμερα. Το τεχνικό τοπίο έχει εξελιχθεί την τελευταία δεκαετία, με την αυξανόμενη χρήση αναγνωριστικών ενσωματωμένων σε λειτουργικά συστήματα, καθώς και με τη δημιουργία νέων εργαλείων που επιτρέπουν την αποθήκευση πληροφοριών σε τερματικό εξοπλισμό.

3. Οι ασάφειες σχετικά με το πεδίο εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες έχουν δημιουργήσει κίνητρα για την εφαρμογή εναλλακτικών λύσεων με στόχο την παρακολούθηση των χρηστών του διαδικτύου και έχουν οδηγήσει σε μια τάση καταστρατήγησης των νομικών υποχρεώσεων που προβλέπονται στο άρθρο 5 παράγραφος 3 της εν λόγω οδηγίας. Όλες αυτές οι καταστάσεις εγείρουν ανησυχίες και απαιτούν συμπληρωματική ανάλυση για τη συμπλήρωση της προηγούμενης καθοδήγησης του ΕΣΠΔ.

4. Σκοπός των κατευθυντήριων γραμμών είναι η διενέργεια τεχνικής ανάλυσης σχετικά με το πεδίο εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, δηλαδή η διασάφηση του τι καλύπτεται τεχνικά από τη φράση «*η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη*». Οι παρούσες κατευθυντήριες γραμμές δεν εξετάζουν τις περιστάσεις υπό τις οποίες μια πράξη επεξεργασίας μπορεί να εμπίπτει στις εξαιρέσεις από την απαίτηση συγκατάθεσης που προβλέπεται στην οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[4], καθώς οι περιστάσεις αυτές θα πρέπει να αναλύονται κατά περίπτωση, λαμβάνοντας υπόψη τη σχετική μεταφορά στο εθνικό δίκαιο και τις οδηγίες που εκδίδουν οι εθνικές αρμόδιες αρχές.

5. Ένας μη εξαντλητικός κατάλογος συγκεκριμένων περιπτώσεων χρήσης θα αναλυθεί στο τελευταίο μέρος των παρουσών κατευθυντήριων γραμμών.

2 ΑΝΑΛΥΣΗ

2.1 Βασικά στοιχεία για την εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

6. Το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες εφαρμόζεται εάν:

   a. **ΚΡΙΤΗΡΙΟ Α:** οι εκτελούμενες πράξεις αφορούν «*πληροφορίες*». Θα πρέπει να σημειωθεί ότι ο όρος που χρησιμοποιείται δεν είναι «δεδομένα προσωπικού χαρακτήρα», αλλά «πληροφορίες».

[3] Γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29, σ. 11.

[4] Όπως ορίζεται στο άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες: «*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.*»

b. **ΚΡΙΤΗΡΙΟ Β:** οι εκτελούμενες πράξεις αφορούν τον «*τερματικό εξοπλισμό*» ενός συνδρομητή ή χρήστη (Β.1), γεγονός που συνεπάγεται την ανάγκη αξιολόγησης της έννοιας *«δημόσιο δίκτυο επικοινωνιών»* (Β.2).

c. **ΚΡΙΤΗΡΙΟ Γ** οι εκτελούμενες πράξεις συνιστούν πράγματι «*αποθήκευση*» (Γ.1) ή «*απόκτηση πρόσβασης*» (Γ.2). Οι δύο αυτές έννοιες μπορούν να εξεταστούν ανεξάρτητα, όπως υπενθυμίζεται στη γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29: *«Η χρήση των λέξεων "αποθήκευση ή πρόσβαση" υποδεικνύει ότι η αποθήκευση και η πρόσβαση δεν χρειάζεται να πραγματοποιούνται στο πλαίσιο της ίδιας επικοινωνίας ούτε να διενεργούνται από το ίδιο ενδιαφερόμενο μέρος*[5]*».*

Για λόγους αναγνωσιμότητας, η οντότητα που αποκτά πρόσβαση σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό του χρήστη θα αναφέρεται στο εξής ως «οντότητα πρόσβασης».

2.2 Έννοια της «πληροφορίας» - Κριτήριο Α

7. Όπως διατυπώνεται στο ΚΡΙΤΗΡΙΟ Α, το παρόν τμήμα περιγράφει λεπτομερώς τι καλύπτει η έννοια της «πληροφορίας». Η επιλογή του όρου «πληροφορίες», που αφορά μια ευρύτερη κατηγορία από ό,τι η απλή έννοια των δεδομένων προσωπικού χαρακτήρα, σχετίζεται με το πεδίο εφαρμογής της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

8. Στόχος του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες είναι η προστασία της ιδιωτικής ζωής των χρηστών, όπως αναφέρεται στην αιτιολογική σκέψη 24: «*Ο τερματικός εξοπλισμός των χρηστών δικτύων ηλεκτρονικών επικοινωνιών και κάθε πληροφορία που αποθηκεύεται στον εξοπλισμό αυτόν συνιστούν μέρος της ιδιωτικής ζωής των χρηστών η οποία χρήζει προστασίας δυνάμει της ευρωπαϊκής σύμβασης για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών*». Η ιδιωτική ζωή προστατεύεται επίσης από το άρθρο 7 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

9. Πράγματι, τα σενάρια που συνεπάγονται παραβίαση της ιδιωτικής ζωής ακόμη και χωρίς να αφορούν δεδομένα προσωπικού χαρακτήρα καλύπτονται ρητά από τη διατύπωση του άρθρου 5 παράγραφος 3 και της αιτιολογικής σκέψης 24 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, για παράδειγμα η αποθήκευση ιών στον τερματικό εξοπλισμό του χρήστη. Αυτό καταδεικνύει ότι ο ορισμός του όρου «πληροφορία» δεν θα πρέπει να περιορίζεται σε κάτι που αφορά ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

10. Το σημείο αυτό έχει επιβεβαιωθεί από το Δικαστήριο της ΕΕ: «*Η ως άνω προστασία αφορά κάθε πληροφορία που αποθηκεύεται στον τερματικό αυτό εξοπλισμό, ανεξαρτήτως του αν πρόκειται για δεδομένα προσωπικού χαρακτήρα ή όχι, και αποσκοπεί μεταξύ άλλων, όπως προκύπτει από την ίδια αυτή αιτιολογική σκέψη, στην προστασία των χρηστών από τον κίνδυνο να εισέλθουν κρυφά αναγνωριστικά στοιχεία ή άλλες παρόμοιες διατάξεις στον τερματικό εξοπλισμό των εν λόγω χρηστών εν αγνοία τους*»[6].

11. Το κατά πόσον η προέλευση των εν λόγω πληροφοριών και οι λόγοι για τους οποίους αποθηκεύονται στον τερματικό εξοπλισμό θα πρέπει να λαμβάνονται υπόψη κατά την αξιολόγηση της εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες έχει αποσαφηνιστεί προηγουμένως. Για παράδειγμα, στη γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29: «*Δεν είναι ορθή η ερμηνεία σύμφωνα με την οποία δεν απαιτείται*

[5] Γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29, σ. 10.
[6] Απόφαση του Δικαστηρίου της 1ης Οκτωβρίου 2019, Planet 49, υπόθεση C-673/17, ECLI:EU:C:2019:801, σκέψη 70.

εξασφάλιση συγκατάθεσης προκειμένου ο τρίτος να αποκτήσει πρόσβαση σε αυτές τις πληροφορίες απλώς και μόνον επειδή δεν προέβη σε αποθήκευσή τους. Η απαίτηση συγκατάθεσης ισχύει επίσης όταν πραγματοποιείται πρόσβαση σε τιμή μόνο για ανάγνωση (π.χ. όταν ζητείται η διεύθυνση MAC μιας διασύνδεσης δικτύου μέσω της API του λειτουργικού συστήματος)»[7].

12. Εν κατακλείδι, η έννοια των πληροφοριών περιλαμβάνει τόσο δεδομένα προσωπικού χαρακτήρα όσο και δεδομένα μη προσωπικού χαρακτήρα, ανεξάρτητα από τον τρόπο με τον οποίο αποθηκεύτηκαν τα δεδομένα αυτά και από ποιον, δηλαδή από μια εξωτερική οντότητα (συμπεριλαμβανομένων και άλλων οντοτήτων πέραν εκείνης που αποκτά πρόσβαση), από τον χρήστη, από έναν κατασκευαστή ή στο πλαίσιο οποιουδήποτε άλλου σεναρίου.

2.3 Έννοια του «τερματικού εξοπλισμού συνδρομητή ή χρήστη» – Κριτήριο Β.1

13. Η παρούσα ενότητα βασίζεται στον ορισμό που χρησιμοποιείται στην οδηγία 2008/63/ΕΚ και έτσι όπως αναφέρεται στο άρθρο 2 της οδηγίας (ΕΕ) 2018/1972, όπου ο «εξοπλισμός τερματικών» («τερματικός εξοπλισμός») ορίζεται ως εξής: «*κάθε εξοπλισμός που συνδέεται άμεσα ή έμμεσα με την ηλεκτρονική διασύνδεση ενός δημόσιου δικτύου τηλεπικοινωνιών για τη μεταβίβαση, επεξεργασία ή λήψη πληροφοριών· και στις δύο περιπτώσεις, δηλαδή είτε η σύνδεση είναι άμεση είτε είναι έμμεση, μπορεί να γίνει με καλώδιο, οπτικές ίνες ή ηλεκτρομαγνητικά κανάλια· η σύνδεση είναι έμμεση, αν μεταξύ του τερματικού και της ηλεκτρονικής διασύνδεσης του δημόσιου δικτύου παρεμβάλλεται άλλη συσκευή*»[8].

14. Η αιτιολογική σκέψη 24 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες επιτρέπει τη σαφή κατανόηση του ρόλου του τερματικού εξοπλισμού για την προστασία που παρέχεται δυνάμει του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες προστατεύει την ιδιωτική ζωή των χρηστών όχι μόνο σε σχέση με την εμπιστευτικότητα των πληροφοριών τους, αλλά διασφαλίζοντας επίσης την ακεραιότητα του τερματικού εξοπλισμού του χρήστη. Η ερμηνεία της έννοιας του τερματικού εξοπλισμού θα βασίζεται στην εν λόγω σημασία στο σύνολο του παρόντος εγγράφου.

15. Το άρθρο 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ορίζει ότι, προκειμένου να είναι δυνατή η εφαρμογή της εν λόγω οδηγίας, η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών. Αυτό συνεπάγεται ότι μια συσκευή θα πρέπει να μπορεί να χρησιμοποιηθεί σε σχέση με την εν λόγω υπηρεσία και ότι, προκειμένου να χαρακτηριστεί ως τερματικός εξοπλισμός, θα πρέπει να είναι συνδεδεμένη ή θα πρέπει να μπορεί να συνδεθεί[9] με τη διεπαφή ενός δημόσιου δικτύου επικοινωνιών. Το ΕΣΠΔ επισημαίνει ότι οι τροποποιήσεις που επήλθαν το 2009[10] στο κείμενο του άρθρου 5 παράγραφος 3

[7] Γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29, σ. 10.

[8] Οδηγία 2008/63/ΕΚ της Επιτροπής, της 20ής Ιουνίου 2008, σχετικά με τον ανταγωνισμό στις αγορές εξοπλισμού τηλεπικοινωνιακών τερματικών (Κωδικοποιημένη έκδοση), άρθρο 1 παράγραφος 1.

[9] Δηλαδή, να υπάρχουν οι τεχνικές δυνατότητες για σύνδεση στο δίκτυο, ακόμη και αν αυτή η σύνδεση δεν υφίσταται επί του παρόντος.

[10] 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), ΕΕ L 337 της 18.12.2009 άρθρο 2 παράγραφος 5) και αιτιολογική σκέψη 65, σ. 11.

της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες διεύρυναν την προστασία του τερματικού εξοπλισμού διαγράφοντας την αναφορά στη «χρήση του δικτύου ηλεκτρονικών επικοινωνιών» ως μέσου αποθήκευσης πληροφοριών ή απόκτησης πρόσβασης σε πληροφορίες που είναι αποθηκευμένες στον τερματικό εξοπλισμό. Επομένως, εφόσον μια συσκευή διαθέτει διεπαφή δικτύου που την καθιστά επιλέξιμη για σύνδεση (ακόμη και αν δεν υπάρχει τέτοια σύνδεση), το άρθρο 5 παράγραφος 3 της ανωτέρω οδηγίας εφαρμόζεται σε κάθε οντότητα που θα μπορούσε να αποθηκεύσει και να αποκτήσει πρόσβαση σε πληροφορίες που είναι ήδη αποθηκευμένες στον τερματικό εξοπλισμό, ανεξάρτητα από το μέσο πρόσβασης στον τερματικό εξοπλισμό και από το αν είναι συνδεδεμένη σε δίκτυο ή αποσυνδεδεμένη από δίκτυο.

16. Ο εξοπλισμός που αποτελεί μέρος του ίδιου του δημόσιου δικτύου ηλεκτρονικών επικοινωνιών δεν θα θεωρείται τερματικός εξοπλισμός δυνάμει του άρθρου 5 παράγραφος 3 τηςοδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[11].

17. Ένας τερματικός εξοπλισμός μπορεί να αποτελείται από οποιονδήποτε αριθμό μεμονωμένων τμημάτων υλισμικού, τα οποία όλα μαζί αποτελούν τον τερματικό εξοπλισμό. Αυτό μπορεί να λάβει ή όχι τη μορφή μιας φυσικά κλειστής συσκευής, η οποία φιλοξενεί το σύνολο του υλισμικού απεικόνισης, επεξεργασίας, αποθήκευσης καθώς και του περιφερειακού εξοπλισμού (για παράδειγμα, έξυπνα τηλέφωνα, φορητοί υπολογιστές, συνδεδεμένη στο δίκτυο διάταξη αποθήκευσης, συνδεδεμένα αυτοκίνητα ή συνδεδεμένες τηλεοράσεις, έξυπνα γυαλιά).

18. Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες αναγνωρίζει ότι η προστασία της εμπιστευτικότητας των πληροφοριών που αποθηκεύονται στον τερματικό εξοπλισμό του χρήστη καθώς και της ακεραιότητας του τερματικού εξοπλισμού του χρήστη δεν περιορίζεται στην προστασία της ιδιωτικής ζωής των φυσικών προσώπων, αλλά αφορά επίσης το δικαίωμα σεβασμού της αλληλογραφίας τους ή των εννόμων συμφερόντων νομικών προσώπων[12]. Ως εκ τούτου, ένας τερματικός εξοπλισμός που επιτρέπει αυτή την αλληλογραφία και τον σεβασμό των έννομων συμφερόντων των νομικών προσώπων προστατεύεται βάσει του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

19. Ο χρήστης ή ο συνδρομητής μπορεί να είναι κάτοχος ή να μισθώνει ή να προμηθεύεται με άλλον τρόπο τον τερματικό εξοπλισμό. Πολλοί χρήστες ή συνδρομητές μπορούν να χρησιμοποιούν από κοινού τον ίδιο τερματικό εξοπλισμό.

20. Η προστασία αυτή η οποία διασφαλίζεται από την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ισχύει για τον τερματικό εξοπλισμό που συνδέεται με τον χρήστη ή τον συνδρομητή και δεν εξαρτάται από το αν ο χρήστης έχει θεσπίσει μέσα πρόσβασης (για παράδειγμα, εάν ξεκίνησε την ηλεκτρονική επικοινωνία) ή ακόμη και από το αν ο χρήστης είναι ενήμερος για τα εν λόγω μέσα πρόσβασης).

2.4 Έννοια του «δημόσιου δικτύου επικοινωνιών» – Κριτήριο Β.2

21. Δεδομένου ότι η κατάσταση που ρυθμίζεται από την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες σχετίζεται με «*την παροχή διαθέσιμων στο κοινό υπηρεσιών*

[11] Για τον προσδιορισμό των ορίων του δικτύου σε διαφορετικά πλαίσια, ανατρέξτε στις κατευθυντήριες γραμμές του BEREC σχετικά με τις κοινές προσεγγίσεις για τον προσδιορισμό του σημείου τερματισμού του δικτύου σε διάφορες τοπολογίες δικτύου (BoR (20) 46)

[12] Πράγματι, όπως υπενθυμίζεται στο άρθρο 2 παράγραφος 13 της οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών, ο χρήστης μπορεί να είναι φυσικό ή νομικό πρόσωπο.

ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα επικοινωνιών στην Κοινότητα»[13], και ο ορισμός του τερματικού εξοπλισμού αναφέρει ρητά την έννοια του «*δημόσιου δικτύου επικοινωνιών*», είναι εξαιρετικά σημαντικό να διευκρινιστεί η έννοια αυτή ώστε να προσδιοριστεί το πλαίσιο στο οποίο εφαρμόζεται το άρθρο 5 παράγραφος 3 της εν λόγω οδηγίας.

22. Η έννοια του δικτύου ηλεκτρονικών επικοινωνιών δεν ορίζεται στην ίδια την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Αναφορά στην εν λόγω έννοια έγινε αρχικά στην οδηγία 2002/21/ΕΚ (οδηγία-πλαίσιο) σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών[14], η οποία στη συνέχεια αντικαταστάθηκε από το άρθρο 2 παράγραφος 1 της οδηγίας 2018/1972 (Ευρωπαϊκός Κώδικας Ηλεκτρονικών Επικοινωνιών). Η νέα διατύπωση έχει ως εξής:

> *«δίκτυο ηλεκτρονικών επικοινωνιών»: τα συστήματα μετάδοσης και, κατά περίπτωση, ο εξοπλισμός μεταγωγής ή δρομολόγησης και οι λοιποί πόροι, περιλαμβανομένων μη ενεργών στοιχείων δικτύου, που επιτρέπουν τη μεταφορά σημάτων, με τη χρήση καλωδίου, ραδιοσημάτων, οπτικού ή άλλου ηλεκτρομαγνητικού μέσου, περιλαμβανομένων των δορυφορικών δικτύων, των σταθερών (μεταγωγής δεδομένων μέσω κυκλωμάτων και πακετομεταγωγής, περιλαμβανομένου του Διαδικτύου) και κινητών επίγειων δικτύων, των συστημάτων ηλεκτρικών καλωδίων, εφόσον χρησιμοποιούνται για τη μετάδοση σημάτων, των δικτύων που χρησιμοποιούνται για ραδιοτηλεοπτικές εκπομπές, καθώς και των δικτύων καλωδιακής τηλεόρασης, ανεξάρτητα από το είδος των μεταφερόμενων πληροφοριών.*[15]

23. Ο ορισμός αυτός είναι ουδέτερος όσον αφορά τις τεχνολογίες μετάδοσης. Σύμφωνα με τον ορισμό αυτό, ως δίκτυο ηλεκτρονικών επικοινωνιών νοείται κάθε σύστημα δικτύου που επιτρέπει τη μετάδοση ηλεκτρονικών σημάτων μεταξύ των κόμβων του, ανεξάρτητα από τον εξοπλισμό και τα πρωτόκολλα που χρησιμοποιούνται.

24. Η έννοια του δικτύου ηλεκτρονικών επικοινωνιών δυνάμει της οδηγίας 2018/1972 δεν εξαρτάται από τον δημόσιο ή ιδιωτικό χαρακτήρα της υποδομής, ούτε από τον τρόπο ανάπτυξης ή διαχείρισης του δικτύου («*είτε βασίζονται σε χωρητικότητα μόνιμων υποδομών ή κεντρικής διαχείρισης είτε όχι*»[16]). Ως εκ τούτου, ο ορισμός του δικτύου ηλεκτρονικών επικοινωνιών, σύμφωνα με το άρθρο 2 της οδηγίας 2018/1972, είναι αρκετά ευρύς ώστε να καλύπτει κάθε είδος υποδομής. Περιλαμβάνει δίκτυα τα οποία διαχειρίζεται ή δεν διαχειρίζεται ένας φορέας εκμετάλλευσης, δίκτυα τα οποία συνδιαχειρίζεται μια ομάδα φορέων εκμετάλλευσης, ή ακόμη και ad-hoc δίκτυα στα οποία ένας τερματικός εξοπλισμός μπορεί δυναμικά να ενταχθεί ή μπορεί να απομακρυνθεί από το πλέγμα άλλου τερματικού εξοπλισμού χρησιμοποιώντας πρωτόκολλα μετάδοσης μικρής εμβέλειας.

25. Ο εν λόγω ορισμός του δικτύου δεν θέτει κανέναν περιορισμό σε ό,τι αφορά τον αριθμό των τερματικών συσκευών που υπάρχουν στο δίκτυο ανά πάσα στιγμή. Ορισμένα συστήματα δικτύωσης βασίζονται σε κόμβους οι οποίοι παρέχουν πληροφορίες ad-hoc σε κόμβους οι που είναι επί του

[13] Άρθρο 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

[14] Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία-πλαίσιο)

[15] 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), άρθρο 2 παράγραφος 1).

[16] 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), άρθρο 2 παράγραφος 1).

παρόντος συνδεδεμένοι[17] και μπορούν σε κάποια χρονική στιγμή να επιτρέπουν τη διομότιμη επικοινωνία. Τέτοιες περιπτώσεις εμπίπτουν στο γενικό πεδίο εφαρμογής της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, υπό την προϋπόθεση ότι το πρωτόκολλο δικτύου επιτρέπει την περαιτέρω συμπερίληψη ομότιμων οντοτήτων.

26. Η δημόσια διαθεσιμότητα του δικτύου επικοινωνιών είναι απαραίτητη ώστε να θεωρηθεί η συσκευή ως τερματικός εξοπλισμός και, ως εκ τούτου, για την εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Αξίζει να σημειωθεί ότι το γεγονός ότι το δίκτυο καθίσταται διαθέσιμο σε ένα περιορισμένο υποσύνολο του κοινού (για παράδειγμα, συνδρομητές, είτε πληρώνουν είτε όχι, υπό προϋποθέσεις επιλεξιμότητας) δεν καθιστά ένα τέτοιο δίκτυο ιδιωτικό[18].

2.5 Έννοια της «απόκτησης πρόσβασης» — Κριτήριο Γ.1

27. Για την ορθή διατύπωση της έννοιας της «απόκτησης πρόσβασης», είναι σημαντικό να εξεταστεί το πεδίο εφαρμογής της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, όπως αναφέρεται στο άρθρο 1: «*προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, και ιδίως του δικαιώματος στην ιδιωτική ζωή και την εμπιστευτικότητα, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Κοινότητα*».

28. Εν ολίγοις, η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες είναι ένα νομικό μέσο που προστατεύει την ιδιωτική ζωή και αποσκοπεί στην προστασία του απορρήτου των επικοινωνιών και της ακεραιότητας των συσκευών. Στην αιτιολογική σκέψη 24 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες διευκρινίζεται ότι, στην περίπτωση φυσικών προσώπων, ο τερματικός εξοπλισμός του χρήστη συνιστά μέρος της ιδιωτικής ζωής του και ότι η πρόσβαση σε πληροφορίες αποθηκευμένες σε αυτόν εν αγνοία του συνιστά ενδεχόμενη σοβαρή παραβίαση της ιδιωτικής ζωής του χρήστη.

29. Τα νομικά πρόσωπα προστατεύονται επίσης από την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[19]. Κατά συνέπεια, η έννοια της «απόκτησης πρόσβασης» δυνάμει του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες πρέπει να ερμηνεύεται κατά τρόπο που να διασφαλίζει τα εν λόγω δικαιώματα έναντι παραβίασης από τρίτους.

30. Η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης μπορεί να αποτελούν ανεξάρτητες πράξεις και να εκτελούνται από ανεξάρτητες οντότητες. Η αποθήκευση πληροφοριών και η πρόσβαση σε ήδη αποθηκευμένες πληροφορίες δεν χρειάζεται να υφίστανται αμφότερες προκειμένου να εφαρμόζεται το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

31. Όπως επισημαίνεται στη γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29: «*Η χρήση των λέξεων "αποθήκευση ή πρόσβαση" υποδεικνύει ότι η αποθήκευση και η πρόσβαση δεν χρειάζεται να*

[17] Για παράδειγμα, στο πλαίσιο ενός συστήματος δικτύωσης με ανοχή στις καθυστερήσεις, το οποίο εφαρμόζει «τεχνικές αποθήκευσης και προώθησης», όπως το έργο ανοικτού κώδικα Briar.

[18] Για μια πιο εμπεριστατωμένη ανάλυση σχετικά με τον προσδιορισμό των δημόσιων δικτύων επικοινωνίας, ανατρέξτε στις κατευθυντήριες γραμμές του BEREC σχετικά με την εφαρμογή του κανονισμού για το ανοικτό διαδίκτυο (BoR (20) 112).

[19] Αιτιολογική σκέψη 26 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, βλ. σημείο 17 ανωτέρω.

πραγματοποιούνται στο πλαίσιο της ίδιας επικοινωνίας ούτε να διενεργούνται από το ίδιο ενδιαφερόμενο μέρος. Οι πληροφορίες που αποθηκεύονται από ένα μέρος (συμπεριλαμβανομένων των πληροφοριών που έχουν αποθηκευτεί από τον χρήστη ή τον κατασκευαστή της συσκευής) και στις οποίες στη συνέχεια έχει πρόσβαση άλλο μέρος εμπίπτουν, ως εκ τούτου, στο πεδίο εφαρμογής του άρθρου 5 παράγραφος 3.»[20]. Κατά συνέπεια, δεν τίθενται περιορισμοί στην προέλευση των πληροφοριών σχετικά με τον τερματικό εξοπλισμό για την εφαρμογή της έννοιας της πρόσβασης.

32. Κάθε φορά που μια οντότητα λαμβάνει μέτρα προκειμένου να αποκτήσει πρόσβαση σε πληροφορίες που είναι αποθηκευμένες στον τερματικό εξοπλισμό, θα εφαρμόζεται το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Συνήθως αυτό συνεπάγεται ότι η οντότητα πρόσβασης πρέπει να στέλνει προορατικά συγκεκριμένες οδηγίες στον τερματικό εξοπλισμό προκειμένου να λάβει πίσω τις στοχευμένες πληροφορίες. Για παράδειγμα, αυτό ισχύει για τα cookies, όπου η οντότητα πρόσβασης δίνει εντολή στον τερματικό εξοπλισμό να αποστέλλει προορατικά πληροφορίες για κάθε επόμενη κλήση πρωτοκόλλου μεταφοράς υπερκειμένου (Hypertext Transfer Protocol — «HTTP»).

33. Αυτό συμβαίνει επίσης όταν η οντότητα πρόσβασης διανέμει λογισμικό στον τερματικό εξοπλισμό του χρήστη το οποίο αποθηκεύεται και στη συνέχεια καλεί προορατικά ένα τελικό σημείο διεπαφής προγραμματισμού εφαρμογών («API») στο δίκτυο. Άλλα παραδείγματα είναι, μεταξύ άλλων, ο κώδικας JavaScript, όπου η οντότητα πρόσβασης δίνει εντολή στο πρόγραμμα περιήγησης του χρήστη να στέλνει ασύγχρονα αιτήματα με τις στοχευμένες πληροφορίες. Μια τέτοια πρόσβαση εμπίπτει σαφώς στο πεδίο εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, καθώς η οντότητα πρόσβασης δίνει ρητή εντολή στον τερματικό εξοπλισμό να αποστείλει τις πληροφορίες.

34. Σε ορισμένες περιπτώσεις, η οντότητα που δίνει εντολή στον τερματικό εξοπλισμό να στείλει πίσω τα στοχευμένα δεδομένα και η οντότητα που λαμβάνει τις πληροφορίες μπορεί να μην είναι οι ίδιες. Αυτό μπορεί να προκύψει από την παροχή ή/και τη χρήση ενός κοινού μηχανισμού μεταξύ των δύο οντοτήτων. Η εντολή στη συσκευή να στείλει ήδη αποθηκευμένες πληροφορίες (για παράδειγμα, μέσω της χρήσης ενός πρωτοκόλλου ή ενός SDK[21], γεγονός που συνεπάγεται την προορατική αποστολή πληροφοριών από τον τερματικό εξοπλισμό) καθιστά δυνατή την εισβολή στον τερματικό εξοπλισμό και, επομένως, μια τέτοια πρόσβαση ενεργοποιεί την εφαρμογή του άρθρου 5 παράγραφος 3.) της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Όπως επισημαίνεται στη γνωμοδότηση 09/2014 της ομάδας εργασίας του άρθρου 29, αυτό μπορεί να συμβαίνει όταν ένας ιστότοπος δίνει εντολή στον τερματικό εξοπλισμό να αποστέλλει πληροφορίες σε τρίτους που παρέχουν τις υπηρεσίες διαφήμισης μέσω της συμπερίληψης ενός εικονοστοιχείου ιχνηλάτησης[22]. Αυτή η περίπτωση χρήσης αναπτύσσεται περαιτέρω στην ενότητα 3.1.

2.6 «Αποθήκευση πληροφοριών» και «αποθηκευμένες πληροφορίες» — Κριτήριο Γ.2

35. Η αποθήκευση πληροφοριών κατά την έννοια του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες αφορά την τοποθέτηση πληροφοριών

[20] Γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29, σ. 10.

[21] Ένα SDK («κιτ ανάπτυξης λογισμικού») είναι μια δέσμη εργαλείων ανάπτυξης λογισμικού που διατίθενται για να διευκολύνουν τη δημιουργία λογισμικού εφαρμογών.

[22] Γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29, σ. 11.

σε φυσικό ηλεκτρονικό μέσο αποθήκευσης που αποτελεί μέρος του τερματικού εξοπλισμού του χρήστη ή του συνδρομητή[23].

36. Κατά κανόνα, οι πληροφορίες δεν αποθηκεύονται στον τερματικό εξοπλισμό ενός χρήστη ή συνδρομητή μέσω άμεσης πρόσβασης στη μνήμη της συσκευής από ένα άλλο ενδιαφερόμενο μέρος, αλλά δίνοντας εντολή στο λογισμικό του τερματικού εξοπλισμού να παράγει συγκεκριμένες πληροφορίες. Η αποθήκευση που πραγματοποιείται μέσω τέτοιων εντολών θεωρείται ότι πραγματοποιείται απευθείας από το άλλο ενδιαφερόμενο μέρος. Αυτό περιλαμβάνει τη χρήση καθιερωμένων πρωτοκόλλων, όπως η αποθήκευση cookies στον φυλλομετρητή, καθώς και προσαρμοσμένου λογισμικού, ανεξάρτητα από το ποιος δημιούργησε ή εγκατέστησε τα πρωτόκολλα ή το λογισμικό στον τερματικό εξοπλισμό.

37. Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες δεν θέτει κανένα ανώτατο ή κατώτατο όριο ως προς το χρονικό διάστημα κατά το οποίο οι πληροφορίες πρέπει να παραμένουν σε ένα αποθηκευτικό μέσο ώστε να θεωρηθούν αποθηκευμένες, ούτε προβλέπει ανώτατο ή κατώτατο όριο για την ποσότητα των πληροφοριών που πρέπει να αποθηκεύονται.

38. Ομοίως, η έννοια της αποθήκευσης δεν εξαρτάται από το είδος του μέσου στο οποίο αποθηκεύονται οι πληροφορίες. Τυπικά παραδείγματα είναι, μεταξύ άλλων, οι σκληροί δίσκοι («HDD»), οι δίσκοι στερεάς κατάστασης («SSD»), η ηλεκτρικά απαλείψιμη προγραμματίσιμη μνήμη μόνο για ανάγνωση («EEPROM») και η μνήμη τυχαίας προσπέλασης («RAM»), αλλά δεν αποκλείονται από το πεδίο εφαρμογής και λιγότερο τυπικά σενάρια που περιλαμβάνουν ένα μέσο όπως η μαγνητική ταινία ή η κρυφή μνήμη κεντρικής μονάδας επεξεργασίας («CPU»). Το μέσο αποθήκευσης μπορεί να συνδέεται εσωτερικά (π.χ. μέσω σύνδεσης SATA), εξωτερικά (π.χ. μέσω σύνδεσης USB).

39. Ως «αποθηκευμένες πληροφορίες» νοούνται οι πληροφορίες που ήδη υπάρχουν στον τερματικό εξοπλισμό, ανεξάρτητα από την πηγή ή τη φύση των εν λόγω πληροφοριών. Περιλαμβάνεται κάθε αποτέλεσμα της αποθήκευσης πληροφοριών κατά την έννοια του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, όπως περιγράφεται ανωτέρω (είτε από το ίδιο ενδιαφερόμενο μέρος που θα αποκτήσει αργότερα πρόσβαση είτε από άλλο τρίτο μέρος). Επιπλέον, περιλαμβάνονται αποτελέσματα διαδικασιών αποθήκευσης πληροφοριών πέραν του πεδίου εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, όπως: η αποθήκευση στον τερματικό εξοπλισμό από τον ίδιο τον χρήστη ή τον συνδρομητή ή από κατασκευαστή του υλικού (όπως οι διευθύνσεις MAC των ελεγκτήρων διεπαφής δικτύου), οι αισθητήρες που είναι ενσωματωμένοι στον τερματικό εξοπλισμό ή οι διαδικασίες και τα προγράμματα που εκτελούνται στον τερματικό εξοπλισμό, που ενδέχεται να παράγουν ή να μην παράγουν πληροφορίες οι οποίες εξαρτώνται ή προέρχονται από αποθηκευμένες πληροφορίες.

3 ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ

40. Όπως επισημαίνεται στην εισαγωγή των παρουσών κατευθυντήριων γραμμών[24], δεν αναλύεται η εφαρμογή των εξαιρέσεων από την υποχρέωση λήψης συγκατάθεσης όπως προβλέπεται στο άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Το ΕΣΠΔ υπενθυμίζει ότι σε όλες τις περιπτώσεις όπου υπάρχει αποθήκευση πληροφοριών ή απόκτηση πρόσβασης σε πληροφορίες που έχουν ήδη αποθηκευτεί, θα πρέπει να αξιολογηθεί εάν απαιτείται

[23] Όπως ορίζεται στο τμήμα 2.3 των παρουσών κατευθυντήριων γραμμών.
[24] Βλ. σημείο 4 ανωτέρω.

συγκατάθεση ή εάν θα μπορούσε να εφαρμοστεί εξαίρεση βάσει του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Συνεπώς, ο αναγνώστης θα πρέπει να εξετάσει τις εξαιρέσεις στην αντίστοιχη περίπτωση χρήσης, σε συνδυασμό με την παρούσα τεχνική ανάλυση.

41. Με την επιφύλαξη του ειδικού πλαισίου στο οποίο μπορούν να χρησιμοποιηθούν οι τεχνικές κατηγορίες που είναι απαραίτητες προκειμένου να διαπιστωθεί κατά πόσον εφαρμόζεται το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, είναι δυνατόν να προσδιοριστούν, κατά τρόπο μη εξαντλητικό, ευρείες κατηγορίες αναγνωριστικών και πληροφοριών που χρησιμοποιούνται ευρέως και μπορούν να εξαρτώνται από την εφαρμογή του άρθρου 5 παράγραφος 3 της εν λόγω οδηγίας.

42. Η επικοινωνία δικτύου βασίζεται συνήθως σε ένα πολυεπίπεδο μοντέλο το οποίο απαιτεί τη χρήση αναγνωριστικών ώστε να είναι δυνατή η ορθή θέσπιση και εκτέλεση της επικοινωνίας. Η κοινοποίηση των εν λόγω αναγνωριστικών σε απομακρυσμένους φορείς παρέχεται μέσω λογισμικού κατόπιν συμφωνίας στο πλαίσιο πρωτοκόλλων επικοινωνίας. Όπως περιγράφεται ανωτέρω, το γεγονός ότι η οντότητα που παραλαμβάνει τις πληροφορίες μπορεί να μην είναι η οντότητα που δίνει την εντολή για την αποστολή των πληροφοριών δεν αποκλείει την εφαρμογή του άρθρου 5 παράγραφος 3 της ανωτέρω οδηγίας. Μπορεί να πρόκειται για αναγνωριστικά δρομολόγησης, όπως η διεύθυνση MAC ή η διεύθυνση IP του τερματικού εξοπλισμού, αλλά και για αναγνωριστικά συνεδρίας (SSRC, αναγνωριστικό Websocket) ή αδειοπλαίσια επαλήθευσης.

43. Κατά τον ίδιο τρόπο, το πρωτόκολλο εφαρμογής μπορεί να περιλαμβάνει διάφορους μηχανισμούς για την παροχή δεδομένων πλαισίου (όπως η επικεφαλίδα HTTP που περιλαμβάνει το πεδίο «accept» ή τον πράκτορα χρήστη), μηχανισμό προσωρινής αποθήκευσης (όπως το ETag[25]) ή άλλες λειτουργίες (όπως τα cookies ή το HSTS[26]). Και πάλι, η χρήση των εν λόγω μηχανισμών για τη συλλογή πληροφοριών (για παράδειγμα στο πλαίσιο του ψηφιακού αποτυπώματος[27] ή της ιχνηλάτησης των αναγνωριστικών πόρων) μπορεί να έχει ως αποτέλεσμα την εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

44. Εξάλλου, υπάρχουν ορισμένα πλαίσια στα οποία οι τοπικές εφαρμογές που είναι εγκατεστημένες στον τερματικό εξοπλισμό χρησιμοποιούν ορισμένες πληροφορίες αυστηρά εντός του τερματικού, όπως ενδέχεται να συμβαίνει στην περίπτωση των API των συστημάτων έξυπνων τηλεφώνων (πρόσβαση σε κάμερα, μικρόφωνο, αισθητήρα GPS, τσιπ επιταχυντή, ραδιοτσιπ, πρόσβαση σε τοπικό αρχείο, κατάλογος επαφών, πρόσβαση σε αναγνωριστικά κ.λπ.). Αυτό μπορεί επίσης να ισχύει για φυλλομετρητές ιστού που επεξεργάζονται πληροφορίες αποθηκευμένες ή παραχθείσες στο εσωτερικό της συσκευής (όπως cookies, τοπική αποθήκευση, WebSQL ή ακόμη και πληροφορίες που παρέχονται από τους ίδιους τους χρήστες). Η χρήση αυτών των πληροφοριών από μια εφαρμογή δεν θα συνιστά «απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες» κατά την έννοια του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, εφόσον οι πληροφορίες δεν εξέρχονται από τη συσκευή, αλλά όταν αποκτάται

[25] Το HTTP ETag είναι ένα αναγνωριστικό που επιτρέπει την υποβολή αίτησης υπό όρους με βάση την εγκυρότητα των αποθηκευμένων δεδομένων του πελάτη.

[26] Το HTTP Strict Transport Security (HSTS) επιτρέπει στους διακομιστές να καθορίζουν για ποιους πόρους θα πρέπει να υποβάλλονται τα αιτήματα πάντα μέσω συνδέσεων HTTPS.

[27] Όπως επισημαίνεται στην εισαγωγή, βλ. γνώμη 9/2014 της ομάδας εργασίας του άρθρου 29 σχετικά με την εφαρμογή της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες στην αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος

πρόσβαση στις πληροφορίες αυτές ή σε οποιαδήποτε άλλη πληροφορία παράγεται από αυτές, θα εφαρμόζεται το άρθρο 5 παράγραφος 3 της ανωτέρω οδηγίας.

45. Τέλος, σε ορισμένες περιπτώσεις, οι φορείς διανέμουν κακόβουλα στοιχεία λογισμικού, για παράδειγμα λογισμικό εξόρυξης κρυπτονομισμάτων ή γενικότερα κακόβουλο λογισμικό, εκμεταλλευόμενοι τις ικανότητες επεξεργασίας του τερματικού εξοπλισμού προς όφελος του φορέα διανομής. Η διανομή του εν λόγω κακόβουλου λογισμικού στον τερματικό εξοπλισμό του χρήστη θα αποτελεί «αποθήκευση» κατά την έννοια του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Επιπλέον, εάν το λογισμικό δημιουργήσει σύνδεση δικτύου για την αποστολή πληροφοριών σε μεταγενέστερο στάδιο, αυτό θα συνιστά «απόκτηση πρόσβασης» κατά την έννοια του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

46. Για ένα υποσύνολο αυτών των κατηγοριών που παρουσιάζουν ειδικό ενδιαφέρον, είτε λόγω της ευρέως διαδεδομένης χρήσης τους είτε επειδή δικαιολογείται ειδική μελέτη όσον αφορά τις περιστάσεις της χρήσης τους, παρέχεται ειδική ανάλυση κατωτέρω.

3.1 Διεύθυνση URL και παρακολούθηση εικονοστοιχείων

47. Ένα εικονοστοιχείο παρακολούθησης είναι ένας υπερσύνδεσμος προς έναν πόρο, συνήθως ένα αρχείο εικόνας, που είναι ενσωματωμένο σε περιεχόμενο, όπως ένας ιστότοπος ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Αυτό το εικονοστοιχείο δεν εκπληρώνει συνήθως κανένα σκοπό που να σχετίζεται με το ίδιο το αιτηθέν περιεχόμενο. Μοναδικός του σκοπός είναι να εγκαταστήσει αυτομάτως την επικοινωνία του πελάτη με τον υποδοχέα (host) του εικονοστοιχείου, η οποία διαφορετικά δεν θα είχε πραγματοποιηθεί. Ωστόσο, αυτό δεν είναι συστηματικό και τα εικονοστοιχεία παρακολούθησης μπορούν επίσης να δημιουργηθούν με την προσθήκη επιπλέον πληροφοριών σε εικόνες φόρτωσης υπερσυνδέσμων οι οποίες σχετίζονται με το περιεχόμενο που εμφανίζεται στον χρήστη. Με την εγκατάσταση της επικοινωνίας διαβιβάζονται διάφορες πληροφορίες στο υποδοχέα (host) του εικονοστοιχείου, ανάλογα με τη συγκεκριμένη περίπτωση χρήσης.

48. Στην περίπτωση ενός μηνύματος ηλεκτρονικού ταχυδρομείου, ο αποστολέας μπορεί να συμπεριλάβει ένα εικονοστοιχείο παρακολούθησης για να ανιχνεύσει πότε ο παραλήπτης διαβάζει το μήνυμα ηλεκτρονικού ταχυδρομείου. Τα εικονοστοιχεία παρακολούθησης σε δικτυακούς τόπους μπορούν να συνδέονται με μια οντότητα που συλλέγει πολλά τέτοια αιτήματα και, ως εκ τούτου, είναι σε θέση να παρακολουθεί τη συμπεριφορά των χρηστών. Τα εν λόγω εικονοστοιχεία παρακολούθησης μπορούν επίσης να περιέχουν πρόσθετα αναγνωριστικά, μεταδεδομένα ή περιεχόμενο ως μέρος του συνδέσμου. Αυτά τα σημεία δεδομένων μπορούν να προστεθούν από τον ιδιοκτήτη του δικτυακού τόπου, ενδεχομένως σε σχέση με τη δραστηριότητα του χρήστη στον εν λόγω δικτυακό τόπο, ώστε να είναι δυνατή η δημιουργία αναλυτικών εκθέσεων χρήσης. Μπορούν επίσης να δημιουργηθούν δυναμικά μέσω της λογικής εφαρμογών από την πλευρά του πελάτη που παρέχεται από την οντότητα.

49. Οι σύνδεσμοι παρακολούθησης μπορούν να λειτουργούν με τον ίδιο τρόπο, αλλά το αναγνωριστικό προστίθεται στη διεύθυνση του ιστότοπου. Όταν ο χρήστης επισκεφτεί τον ομοιόμορφο εντοπιστή πόρων («URL»), ο ιστότοπος-στόχος φορτώνει τον ζητούμενο πόρο, αλλά συλλέγει επίσης ένα αναγνωριστικό το οποίο δεν είναι συναφές όσον αφορά την ταυτοποίηση του πόρου. Χρησιμοποιούνται πολύ συχνά από ιστότοπους ηλεκτρονικού εμπορίου για να προσδιορίσουν την προέλευση της εισερχόμενης πηγής κυκλοφορίας τους. Για παράδειγμα, οι εν λόγω ιστότοποι μπορούν να παρέχουν συνδέσμους που παρακολουθούνται σε συνεργάτες, οι οποίοι τους χρησιμοποιούν στον τομέα τους, ώστε ο ιστότοπος ηλεκτρονικού εμπορίου να γνωρίζει ποιος από

τους συνεργάτες είναι υπεύθυνος για μια πώληση και να καταβάλλει προμήθεια, μια πρακτική γνωστή ως μάρκετινγκ συνεργατών (affiliate marketing).

50. Τόσο οι σύνδεσμοι παρακολούθησης όσο και τα εικονοστοιχεία παρακολούθησης μπορούν να διανέμονται μέσω διαφόρων διαύλων, για παράδειγμα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, ιστοτόπων ή ακόμη, στην περίπτωση συνδέσμων παρακολούθησης, μέσω οποιουδήποτε είδους συστημάτων ανταλλαγής γραπτών μηνυμάτων. Αυτή η διανομή στον τερματικό εξοπλισμό του χρήστη συνιστά αποθήκευση, τουλάχιστον μέσω του μηχανισμού αποθήκευσης σε κρυφή μνήμη του λογισμικού από την πλευρά του πελάτη. Ως εκ τούτου, εφαρμόζεται το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ακόμη και αν η αποθήκευση αυτή δεν είναι μόνιμη.

51. Η προσθήκη πληροφοριών ιχνηλάτησης σε διευθύνσεις URL ή εικόνες (εικονοστοιχεία) που αποστέλλονται στον χρήστη συνιστά εντολή προς τον τερματικό εξοπλισμό να στείλει πίσω τις στοχευμένες πληροφορίες (το καθορισμένο αναγνωριστικό). Στην περίπτωση των δυναμικά κατασκευασμένων εικονοστοιχείων ιχνηλάτησης, η διανομή της λογικής εφαρμογών (συνήθως ένας κώδικας JavaScript) αποτελεί την εντολή. Ως εκ τούτου, μπορεί να θεωρηθεί ότι η συλλογή αναγνωριστικών που παρέχονται μέσω τέτοιων μηχανισμών ιχνηλάτησης συνιστά «απόκτηση πρόσβασης» κατά την έννοια του άρθρου 5 παράγραφος 3 οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, επομένως εφαρμόζεται και σε αυτό το στάδιο.

3.2 Τοπική επεξεργασία

52. Ορισμένες τεχνολογίες βασίζονται στην τοπική επεξεργασία η οποία πραγματοποιείται μέσω λογισμικού που διανέμεται στον τερματικό εξοπλισμό των χρηστών, όπου οι πληροφορίες που παράγονται από την τοπική επεξεργασία καθίστανται στη συνέχεια διαθέσιμες σε επιλεγμένους φορείς μέσω API από την πλευρά του πελάτη. Αυτό μπορεί, για παράδειγμα, να ισχύει για μια API που παρέχεται από τον φυλλομετρητή Ιστού, όπου τα τοπικά παραγόμενα αποτελέσματα μπορούν να είναι προσβάσιμα εξ αποστάσεως.

53. Εάν σε οποιοδήποτε σημείο και για παράδειγμα στον κώδικα από την πλευρά του πελάτη, οι υπό επεξεργασία πληροφορίες καθίστανται διαθέσιμες σε τρίτο μέρος, για παράδειγμα αποστέλλονται πίσω σε διακομιστή, μια τέτοια πράξη (η οποία ανατίθεται από την οντότητα που παράγει τον κώδικα από την πλευρά του πελάτη και διανέμεται στον τερματικό εξοπλισμό του χρήστη) θα συνιστά «απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες». Το γεγονός ότι οι πληροφορίες αυτές παράγονται σε τοπικό επίπεδο δεν αποκλείει την εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

3.3 Παρακολούθηση με βάση μόνο τη διεύθυνση IP

54. Ορισμένοι πάροχοι αναπτύσσουν λύσεις που βασίζονται μόνο στη συλλογή ενός στοιχείου, δηλαδή της διεύθυνσης IP, για την παρακολούθηση της πλοήγησης[28] του χρήστη, σε ορισμένες περιπτώσεις σε πολλαπλούς τομείς. Στο πλαίσιο αυτό, θα μπορούσε να εφαρμοστεί το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ακόμη και αν η εντολή

[28] Αυτή είναι μια πρόσθετη πράξη, η οποία είναι ανεξάρτητη από τη χρήση και τη λειτουργία μιας διεύθυνσης IP για τη δημιουργία και τη μεταφορά ή τη διαβίβαση υποκείμενων τεχνικών επικοινωνιών, ή από το γεγονός ότι μπορεί να πρόκειται ή να μην πρόκειται για δεδομένα προσωπικού χαρακτήρα (σε ό,τι αφορά την ανάλυση της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, πρόκειται για «πληροφορίες»).

να καταστεί διαθέσιμη η διεύθυνση IP έχει δοθεί από διαφορετική οντότητα από εκείνη που λαμβάνει τις πληροφορίες.

55. Ωστόσο, η απόκτηση πρόσβασης σε διευθύνσεις IP θα ενεργοποιεί την εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες μόνο στις περιπτώσεις που οι πληροφορίες αυτές προέρχονται από τον τερματικό εξοπλισμό συνδρομητή ή χρήστη. Μολονότι αυτό δεν συμβαίνει συστηματικά (για παράδειγμα, όταν ενεργοποιείται η μετατροπή διευθύνσεων μέσω μεταφορέα βαθμίδας - CGNAT[29]), οι στατικές εξερχόμενες IPv4 που προέρχονται από τον δρομολογητή ενός χρήστη εμπίπτουν στην περίπτωση αυτή, καθώς και οι διευθύνσεις IPV6, δεδομένου ότι ορίζονται εν μέρει από τον υποδοχέα (host). Εάν η οντότητα δεν μπορεί να διασφαλίσει ότι η διεύθυνση IP δεν προέρχεται από τον τερματικό εξοπλισμό ενός χρήστη ή συνδρομητή, πρέπει να λάβει όλα τα μέτρα σύμφωνα με το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

56. Παρόλο που οι παρούσες κατευθυντήριες γραμμές δεν αναλύουν την εφαρμογή των εξαιρέσεων από την υποχρέωση της λήψης συγκατάθεσης που προβλέπεται στο άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, κρίνεται σκόπιμο να υπενθυμιστεί για άλλη μια φορά ότι η εφαρμογή του εν λόγω άρθρου δεν σημαίνει συστηματικά ότι πρέπει να δίνεται συγκατάθεση. Το ΕΣΠΔ υπενθυμίζει, συνεπώς, ότι σε κάθε περίπτωση θα πρέπει να αξιολογείται εάν απαιτείται συγκατάθεση ή εάν θα μπορούσε να εφαρμοστεί εξαίρεση βάσει του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[30].

3.4 Διακοπτόμενες και διαμεσολαβούμενες αναφορές στο διαδίκτυο των πραγμάτων (IoT)

57. Οι συσκευές του διαδικτύου των πραγμάτων (IoT) παράγουν πληροφορίες κατά τρόπο συνεχή, για παράδειγμα μέσω αισθητήρων ενσωματωμένων στη συσκευή, οι οποίες μπορεί να είναι ή να μην είναι προεπεξεργασμένες τοπικά. Σε πολλές περιπτώσεις, οι πληροφορίες είναι διαθέσιμες σε έναν απομακρυσμένο διακομιστή, αλλά οι ρυθμίσεις που αφορούν αυτή τη συλλογή μπορεί να διαφέρουν.

58. Ορισμένες συσκευές IoT είναι άμεσα συνδεδεμένες σε δημόσιο δίκτυο επικοινωνίας μέσω κάρτας SIM κινητής τηλεφωνίας. Άλλες μπορεί να είναι έμμεσα συνδεδεμένες σε δημόσιο δίκτυο επικοινωνιών, για παράδειγμα μέσω της χρήσης WIFI ή της μετάδοσης πληροφοριών σε άλλη συσκευή μέσω διασημειακής σύνδεσης (για παράδειγμα, μέσω Bluetooth). Η άλλη συσκευή μπορεί, για παράδειγμα, να είναι ένα έξυπνο κινητό τηλέφωνο ή μια ειδική πύλη η οποία μπορεί ή δεν μπορεί να προβεί σε προεπεξεργασία των πληροφοριών πριν να τις αποστείλει στον εξυπηρετητή.

59. Οι συσκευές IoT μπορεί να έχουν εντολή από τον κατασκευαστή να μεταδίδουν πάντα σε συνεχή ροή τις συλλεχθείσες πληροφορίες, αφού αποθηκεύσουν πρώτα προσωρινά τις πληροφορίες, για παράδειγμα έως ότου είναι διαθέσιμη μια σύνδεση.

60. Σε κάθε περίπτωση, η συσκευή IoT, όταν συνδέεται (άμεσα ή έμμεσα) σε δημόσιο δίκτυο επικοινωνιών, θα θεωρείται και η ίδια τερματικός εξοπλισμός. Το γεγονός ότι οι πληροφορίες μεταδίδονται σε συνεχή ροή ή αποθηκεύονται προσωρινά για την υποβολή διακοπτόμενων

[29] Το Carrier-grade NAT ή CGNAT χρησιμοποιείται από τους παρόχους υπηρεσιών Διαδικτύου για τη μεγιστοποίηση της χρήσης του περιορισμένου χώρου μιας διεύθυνσης IP. Ομαδοποιεί έναν αριθμό συνδρομητών στην ίδια δημόσια διεύθυνση IP.

[30] Η γνωμοδότηση 9/2014 της ομάδας εργασίας του άρθρου 29 παρέχει ορισμένα παραδείγματα περιπτώσεων στις οποίες ενδέχεται να μην απαιτείται συγκατάθεση.

αναφορών δεν μεταβάλλει τη φύση των εν λόγω πληροφοριών. Και στις δύο περιπτώσεις θα εφαρμόζεται το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, καθώς υφίσταται «απόκτηση πρόσβασης», μέσω της εντολής που είναι γραμμένη στον κώδικα της συσκευής IoT για αποστολή των δυναμικά αποθηκευμένων δεδομένων στον απομακρυσμένο διακομιστή.

3.5 Μοναδικό αναγνωριστικό

61. Ένα κοινό εργαλείο που χρησιμοποιούν οι εταιρείες είναι η έννοια των «μοναδικών αναγνωριστικών» ή των «μόνιμων αναγνωριστικών». Τα εν λόγω αναγνωριστικά μπορούν να προέρχονται από τα μόνιμα δεδομένα προσωπικού χαρακτήρα (όνομα και επώνυμο, ηλεκτρονικό ταχυδρομείο, αριθμός τηλεφώνου κ.λπ.), τα οποία κλειδώνονται στη συσκευή του χρήστη, συλλέγονται και κοινοποιούνται σε διάφορους υπεύθυνους επεξεργασίας για την αποκλειστική ταυτοποίηση ενός προσώπου μέσω διαφορετικών συνόλων δεδομένων (χρήση δεδομένων που συλλέγονται μέσω της χρήσης ιστοτόπου ή εφαρμογής, δεδομένα διαχείρισης πελατειακών σχέσεων (CRM) που σχετίζονται με την αγορά ή τη συνδρομή εντός ή εκτός διαδικτύου, κ.λπ.). Στους ιστοτόπους, τα μόνιμα δεδομένα προσωπικού χαρακτήρα λαμβάνονται γενικά στο πλαίσιο της ηλεκτρονικής επαλήθευσης ταυτότητας ή της συνδρομής σε ενημερωτικά δελτία.

62. Όπως αναφέρθηκε προηγουμένως, το γεγονός ότι οι πληροφορίες εισάγονται από τον χρήστη δεν αποκλείει την εφαρμογή του άρθρου 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, καθώς οι πληροφορίες αυτές αποθηκεύονται προσωρινά στον τερματικό εξοπλισμό πριν από τη συλλογή τους.

63. Στο πλαίσιο της συλλογής «μοναδικού αναγνωριστικού» σε ιστοτόπους ή εφαρμογές για φορητές συσκευές, η οντότητα που συλλέγει τις πληροφορίες δίνει εντολή στον φυλλομετρητή (μέσω της διανομής κωδικού για την πλευρά του πελάτη) για την αποστολή των εν λόγω πληροφοριών. Ως εκ τούτου, πραγματοποιείται «απόκτηση πρόσβασης» και εφαρμόζεται το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.