ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

14/EL
WP 224

Γνώμη 9/2014 σχετικά με την εφαρμογή της οδηγίας 2002/58/ΕΚ στην αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος

Εκδόθηκε στις 25 Νοεμβρίου 2014

Η παρούσα ομάδα εργασίας συστάθηκε βάσει του άρθρου 29 της οδηγίας 95/46/ΕΚ. Συνιστά ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για την προστασία των δεδομένων και της ιδιωτικής ζωής. Τα καθήκοντα της ομάδας ορίζονται στο άρθρο 30 της οδηγίας 95/46/ΕΚ και στο άρθρο 15 της οδηγίας 2002/58/ΕΚ.

Γραμματειακή υποστήριξη παρέχεται από τη Διεύθυνση Γ (Θεμελιώδη δικαιώματα και ιθαγένεια της Ένωσης) της Ευρωπαϊκής Επιτροπής, Γενική Διεύθυνση Δικαιοσύνης, B-1049 Brussels, Belgium, Γραφείο αριθ. MO-59 02/013.

Διεύθυνση δικτυακού τόπου: http://ec.europa.eu/justice/data-protection/index_el.htm

Η ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

η οποία συστάθηκε με την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995,

έχοντας υπόψη τα άρθρα 29 και 30 της εν λόγω οδηγίας,

έχοντας υπόψη τον εσωτερικό κανονισμό της,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΓΝΩΜΗ:

1. Σύνοψη

Η αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος εγείρει σοβαρές ανησυχίες όσον αφορά την προστασία των δεδομένων των πολιτών. Για παράδειγμα, ορισμένες επιγραμμικές υπηρεσίες έχουν προτείνει την αναγνώριση συσκευών βάσει του ψηφιακού τους αποτυπώματος ως εναλλακτική επιλογή έναντι των cookies HTTP, με σκοπό την παροχή εργαλείων ανάλυσης ή την παρακολούθηση χωρίς την ανάγκη εξασφάλισης συγκατάθεσης βάσει του άρθρου 5 παράγραφος 3.[1] Το γεγονός αυτό καταδεικνύει ότι οι κίνδυνοι τους οποίους θέτει η αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος δεν είναι θεωρητικού χαρακτήρα και από έρευνες έχει προκύψει ότι το ψηφιακό αποτύπωμα αξιοποιείται ήδη.[2]

Στην παρούσα γνώμη, η ομάδα εργασίας του άρθρου 29 εξετάζει το θέμα της αναγνώρισης συσκευών βάσει ψηφιακού αποτυπώματος και τη δυνατότητα εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ, με την επιφύλαξη των διατάξεων της οδηγίας 95/46/ΕΚ για την προστασία των δεδομένων. Βασικό μήνυμα της παρούσας γνώμης είναι ότι το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες εφαρμόζεται στην αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος .

Η παρούσα γνώμη αναπτύσσει περαιτέρω τα όσα αναφέρονται στην προηγούμενη γνώμη 04/2012 σχετικά με την απαλλαγή που ισχύει σε σχέση με τη συναίνεση για τα cookies[3] και επισημαίνει σε τρίτους[4] οι οποίοι επεξεργάζονται ψηφιακά αποτυπώματα συσκευών που έχουν δημιουργηθεί μέσω της εξασφάλισης πρόσβασης σε πληροφορίες ή της αποθήκευσης πληροφοριών στην τερματική συσκευή του χρήστη ότι κάτι τέτοιο μπορεί να επιτραπεί μόνο με την έγκυρη συγκατάθεση του χρήστη (εκτός αν ισχύει απαλλαγή).

2. Εισαγωγή

Το άρθρο 5 παράγραφος 3 της οδηγίας 2002/58/ΕΚ, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ,[5] (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) ορίζει ότι τα κράτη μέλη μεριμνούν ώστε «*η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη*» να επιτρέπεται μόνον εάν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεσή του με βάση σαφείς και

[1] Wall Street Journal, 2013. Web Giants Threaten End to Cookie Tracking. http://online.wsj.com/news/articles/SB10001424052702304682504579157780178992984

[2] Nikiforakis, 2013. Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. https://lirias.kuleuven.be/bitstream/123456789/393661/1/

[3] Ομάδα εργασίας του άρθρου 29, 2012. Γνώμη 04/2012 σχετικά με την απαλλαγή που ισχύει σε σχέση με τη συναίνεση για τα cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_el.pdf

[4] «Τρίτος» όπως αναφέρεται στην αιτιολογική σκέψη 66 της οδηγίας 2009/136/ΕΚ.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:el:NOT

εκτεταμένες πληροφορίες σύμφωνα με την οδηγία 95/46/ΕΚ[6] (οδηγία για την προστασία των δεδομένων), μεταξύ άλλων για τον σκοπό της επεξεργασίας.[7]

Η ομάδα εργασίας του άρθρου 29, στη γνώμη 04/2012 που εξέδωσε, εξέτασε το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες σε σχέση με την αποθήκευση πληροφοριών ή την πρόσβαση σε αυτές μέσω της χρήσης cookies. Στην εν λόγω γνώμη αναφερόταν ότι το άρθρο 5 παράγραφος 3 δεν ισχύει αποκλειστικά για τα cookies, αλλά εφαρμόζεται και σε «παρεμφερείς τεχνολογίες».

Η παρούσα γνώμη εξετάζει τον αυξανόμενο αριθμό αναφορών βάσει των οποίων τρίτα μέρη δραστηριοποιούνται στη διερεύνηση εναλλακτικών τεχνολογιών έναντι των cookies για την εξυπηρέτηση διαφόρων σκοπών, σε μια προσπάθεια να αποφύγουν την απαίτηση της συγκατάθεσης που προβλέπεται στο άρθρο 5 παράγραφος 3. Ειδικότερα, εξετάζεται ο συνδυασμός μιας σειράς στοιχείων πληροφοριών για τη μοναδική αναγνώριση συγκεκριμένων συσκευών ή της παρουσίας εφαρμογών, το επονομαζόμενο «ψηφιακό αποτύπωμα των συσκευών».

Τα ψηφιακά αποτυπώματα συσκευών μπορούν επίσης να αποτελούν δεδομένα προσωπικού χαρακτήρα. Η παρούσα γνώμη δεν προχωρά σε ανάλυση των σχετικών διατάξεων της οδηγίας για την προστασία των δεδομένων, όμως αναφέρεται σε θέματα προστασίας δεδομένων τα οποία παρουσιάζουν ιδιαίτερη συνάφεια στο πλαίσιο της αναγνώρισης συσκευών βάσει ψηφιακού αποτυπώματος. Παράδειγμα αποτελεί η διαδικασία κατά την οποία συνδυάζονται διάφορα στοιχεία πληροφοριών, ιδίως μοναδικά αναγνωριστικά όπως διευθύνσεις IP, και ο σκοπός της επεξεργασίας είναι η αναγνώριση χρηστών διαχρονικά, σε διάφορους δικτυακούς τόπους, όπως συμβαίνει στην περίπτωση της συμπεριφορικής διαφήμισης. Σε τέτοιες περιπτώσεις, η επεξεργασία πρέπει επίσης να συμμορφώνεται με τους κανόνες που προβλέπονται στην οδηγία για την προστασία των δεδομένων.

Η τεχνολογία του ψηφιακού αποτυπώματος συσκευών δεν περιορίζεται στις παραμέτρους ρύθμισης ενός παραδοσιακού φυλλομετρητή ιστού σε επιτραπέζιο υπολογιστή. Το ψηφιακό αποτύπωμα συσκευών δεν συνδέεται ούτε με συγκεκριμένο πρωτόκολλο, αλλά μπορεί να χρησιμοποιηθεί για να αποτυπώσει ένα ευρύ φάσμα συσκευών συνδεδεμένων με το διαδίκτυο, καταναλωτικών ηλεκτρονικών ειδών και εφαρμογών, συμπεριλαμβανομένων όσων εκτελούνται σε κινητές συσκευές, έξυπνες τηλεοράσεις, κονσόλες παιχνιδιών, συσκευές ανάγνωσης ηλεκτρονικών βιβλίων, διαδικτυακό ραδιόφωνο, συστήματα επί οχημάτων ή έξυπνους μετρητές.[8]

3. Ορισμός

Στην αίτηση υποβολής παρατηρήσεων RFC6973[9] το ψηφιακό αποτύπωμα ορίζεται ως «ένα σύνολο στοιχείων πληροφοριών το οποίο προσδιορίζει την ταυτότητα μιας συσκευής ή την παρουσία μιας

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EL:NOT

[7] 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.

[8] Ενίοτε αποκαλείται «διαδίκτυο των πραγμάτων».

[9] Cooper, 2013. Privacy Considerations for Internet Protocols. http://tools.ietf.org/html/rfc6973

εφαρμογής». Στην παρούσα γνώμη, ο όρος χρησιμοποιείται με ευρεία έννοια, που σημαίνει ότι περιλαμβάνει ένα σύνολο πληροφοριών που μπορούν να χρησιμοποιηθούν για τον εντοπισμό[10], τη σύνδεση[11] ή τη διαχρονική εξαγωγή συμπερασμάτων[12] όσον αφορά την ταυτότητα ενός χρήστη, ενός παράγοντα χρήστη ή μιας συσκευής. Το ψηφιακό αποτύπωμα περιλαμβάνει, αλλά δεν περιορίζεται, σε δεδομένα που προέρχονται από τα ακόλουθα:

α) ρυθμίσεις παράγοντα χρήστη/συσκευής· ή

β) δεδομένα που εκτίθενται λόγω της χρήσης πρωτοκόλλων επικοινωνίας δικτύου.

Υπάρχουν πολλά είδη δεδομένων τα οποία μπορούν να διαμορφώσουν ένα αποτύπωμα, συμπεριλαμβανομένων των ακόλουθων παραδειγμάτων:

α) πληροφορίες CSS·

β) αντικείμενα JavaScript (π.χ. έγγραφο, παράθυρο, οθόνη, πρόγραμμα πλοήγησης, ημερομηνία και γλώσσα)·

γ) πληροφορίες κεφαλίδας HTTP (π.χ. ο αριθμός των bit πληροφοριών στη συμβολοσειρά παράγοντα χρήστη, η διάταξη κεφαλίδας HTTP, η παραλλαγή κεφαλίδας HTTP ανάλογα με το είδος του αιτήματος)·

δ) πληροφορίες ώρας (π.χ. διαφορά ώρας και σφάλμα ρολογιού)·

ε) διαφοροποίηση στοίβας TCP·

στ) εγκατεστημένες γραμματοσειρές·

ζ) πληροφορίες εγκατεστημένης συνδεόμενης υπομονάδας (π.χ. πληροφορίες ρυθμίσεων και έκδοσης)·[13]

η) η χρήση εσωτερικών διασυνδέσεων προγραμματισμού εφαρμογών[14] (API) που εκτίθενται από τον παράγοντα χρήστη/τη συσκευή· ή

---

[10] *Εντοπισμός φυσικού προσώπου*: η δυνατότητα απομόνωσης ορισμένων ή όλων των καταχωρίσεων βάσει των οποίων εξακριβώνεται η ταυτότητα ενός φυσικού προσώπου στο σύνολο δεδομένων, Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης, σ. 11-12.

[11] *Συνδεσιμότητα*: η δυνατότητα σύνδεσης δύο, τουλάχιστον, καταχωρίσεων που αφορούν το ίδιο πρόσωπο στο οποίο αναφέρονται τα δεδομένα ή ομάδα προσώπων στα οποία αναφέρονται τα δεδομένα (είτε στην ίδια βάση δεδομένων είτε σε δύο διαφορετικές βάσεις δεδομένων). Εάν ένας εισβολέας μπορεί να εξακριβώσει (π.χ. μέσω ανάλυσης συσχετισμών) ότι δύο καταχωρίσεις αποδίδονται σε μία ομάδα φυσικών προσώπων, χωρίς ωστόσο να είναι σε θέση να εντοπίσει μεμονωμένα φυσικά πρόσωπα εντός της εν λόγω ομάδας, η τεχνική είναι μεν ανθεκτική έναντι του «εντοπισμού φυσικού προσώπου», αλλά όχι και έναντι της συνδεσιμότητας, Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης, σ. 11-12.

[12] *Εξαγωγή συμπερασμάτων*: η δυνατότητα υπολογισμού, με σημαντικό βαθμό βεβαιότητας, της τιμής ενός ιδιοχαρακτηριστικού από τις τιμές ενός συνόλου άλλων ιδιοχαρακτηριστικών, Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης, σ. 11-12.

[13] *Πρβλ.* α) http://www.w3.org/wiki/Fingerprinting, β) http://w3c.github.io/fingerprinting-guidance/#wsj-orbitz γ) https://wiki.mozilla.org/Fingerprinting και δ) https://trac.webkit.org/wiki/Fingerprinting για τους μηχανισμούς.

θ) η χρήση εξωτερικής API υπηρεσιών ιστού με τις οποίες επικοινωνεί ο παράγοντας χρήστη/η συσκευή.

4. Τεχνικό πλαίσιο

Το διαδίκτυο και ο ιστός έχουν αναπτυχθεί με βάση τις ανάγκες για ένα ευέλικτο και ανοικτό περιβάλλον αρχιτεκτονικής δικτύου[15]. Λόγω των επιλογών που έγιναν στον σχεδιασμό προκειμένου να ικανοποιούνται οι εν λόγω ανάγκες, οι συσκευές μεταδίδουν στοιχεία πληροφοριών. Ορισμένα πρωτόκολλα περιλαμβάνουν σειρά υποχρεωτικών και προαιρετικών στοιχείων πληροφοριών. Για παράδειγμα, το πρωτόκολλο HTTP/1.1[16] προσδιορίζει τα πεδία κεφαλίδας που επιτρέπουν στον διακομιστή και τον πελάτη να συμπεριλάβουν πρόσθετες πληροφορίες σχετικά με το υπερκείμενο. Ορισμένα από τα εν λόγω πεδία είναι ειδικά σχεδιασμένα ώστε ο διακομιστής να αναγνωρίζει τύπους προγράμματος-πελάτη. Για παράδειγμα, η κεφαλίδα αίτησης παράγοντα χρήστη περιλαμβάνει την περιγραφή: «*Εξυπηρετεί στατιστικούς σκοπούς, τον εντοπισμό παραβιάσεων πρωτοκόλλων και την αυτόματη αναγνώριση παραγόντων χρηστών για λόγους προσαρμογής απαντήσεων ώστε να αποφεύγονται ειδικοί περιορισμοί παραγόντων χρηστών*».

Μεταξύ των χαρακτηριστικών χρήσεων της συμβολοσειράς παράγοντα χρήστη περιλαμβάνεται η βελτιστοποίηση της διάταξης του περιεχομένου για έναν συγκεκριμένο τύπο συσκευής· η χρήση των εν λόγω πληροφοριών για στόχευση του περιεχομένου σε συγκεκριμένους χρήστες·[17] ή η συλλογή πληροφοριών σχετικά με τη συσκευή για σκοπούς ασφάλειας ή ανάλυσης.

5. Κίνδυνοι από την άποψη της προστασίας δεδομένων

Λόγω του ότι μια μεμονωμένη κεφαλίδα HTTP συνήθως έχει μη μοναδική τιμή, σπανίως μπορεί να προσδιοριστεί η ταυτότητα ενός επιμέρους χρήστη βάσει του στοιχείου πληροφοριών και μόνο.[18] Για παράδειγμα, οι τύποι των μέσων που υποστηρίζονται από έναν φυλλομετρητή συχνά είναι ίδιοι για πολλούς άλλους χρήστες που χρησιμοποιούν την ίδια έκδοση φυλλομετρητή. Συνεπώς, κατά τη μεμονωμένη επεξεργασία, αυτά τα μη μοναδικά στοιχεία πληροφοριών δεν ενέχουν, εν γένει, κάποιον κίνδυνο για την προστασία των δεδομένων.

Ωστόσο, μπορεί να γίνει συνδυασμός ορισμένων στοιχείων πληροφοριών ώστε να δημιουργηθεί ένα επαρκώς μοναδικό σύνολο (ιδίως όταν συνδυάζονται με άλλα αναγνωριστικά όπως η αρχική

---

[14] Η εσωτερική διασύνδεση προγραμματισμού (API) παρέχει στον χρήστη ένα φιλικό περιβάλλον για πρόσβαση σε λειτουργίες ή ρουτίνες στοιχείων του λογισμικού.

[15] Kahn, 1972. Communications Principles for Operating Systems. Εσωτερικό υπόμνημα της BBN.

[16] Fielding, Reschke, 2014. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. http://www.ietf.org/rfc/rfc7231.txt

[17] Wall Street Journal, 2012. On Orbitz, Mac Users Steered to Pricier Hotels, http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html.

[18] Υπάρχουν περιπτώσεις στις οποίες ένα μεμονωμένο στοιχείο πληροφοριών φέρει πληροφορίες που μπορούν να οδηγήσουν σε πλήρη ταυτοποίηση του προσώπου στο οποίο αναφέρονται τα δεδομένα, όπως το διακριτικό πρόσβασης OAuth.

διεύθυνση IP), το οποίο επέχει θέση μοναδικού ψηφιακού αποτυπώματος για τη συσκευή ή την παρουσία εφαρμογής. Το εν λόγω ψηφιακό αποτύπωμα παρέχει τη δυνατότητα να διακρίνουμε τη μία συσκευή από την άλλη και μπορεί να χρησιμοποιηθεί ως συγκεκαλυμμένη εναλλακτική επιλογή αντί των cookies για τη διαχρονική ιχνηλάτηση διαδικτυακών συμπεριφορών.[19,20,21] Ως εκ τούτου, μέσω αυτού του ψηφιακού αποτυπώματος της συσκευής καθίσταται εφικτός ο συσχετισμός και, συνεπώς, η αναγνώριση ή η αναγνωρισιμότητα ενός φυσικού προσώπου.

Οι κίνδυνοι που ενέχει το ψηφιακό αποτύπωμα των συσκευών για την προστασία των δεδομένων αυξάνονται λόγω του ότι το μοναδικό σύνολο στοιχείων πληροφοριών διατίθεται όχι μόνο στον εκδότη του δικτυακού τόπου αλλά και σε πολλούς άλλους τρίτους. Το γεγονός αυτό έρχεται σε αντίθεση με την πολιτική *ίδιας προέλευσης* των HTTP cookies και επιδεινώνεται λόγω του τεχνικού χαρακτήρα που έχει ο παγκόσμιος ιστός, στο πλαίσιο του οποίου πολλοί τρίτοι συνεισφέρουν στο περιεχόμενο μιας ιστοσελίδας.

Αποτελεί συνήθη πρακτική η δυναμική δημιουργία μιας ιστοσελίδας σε πραγματικό χρόνο, με αιτήματα για περιεχόμενο από πολλαπλές πηγές. Καθεμία από αυτές τις πηγές δημιουργεί δικές της αιτήσεις HTTP, πραγματοποιώντας λήψη εικόνων, αρχείων JavaScript και CSS. Επίσης, πολλές ιστοσελίδες περιέχουν δικτυακούς «κοριούς» (web-bugs) και δέσμες ενεργειών παρακολούθησης. Ενδέχεται επίσης να εκδίδουν αιτήσεις HTTP που καταγράφουν πότε ένας χρήστης χρησιμοποιεί τη δυνατότητα κύλισης ή κάνει κλικ πάνω σε μια σελίδα, εικόνα ή διαφήμιση. Συνεπώς, δίδεται συχνά σε τρίτους η δυνατότητα να συλλέγουν τις πληροφορίες που απαιτούνται για τη δημιουργία ψηφιακού αποτυπώματος της συσκευής του χρήστη.

Οι κίνδυνοι από την άποψη της προστασίας δεδομένων δεν περιορίζονται στην ιχνηλάτηση εκ μέρους τρίτων. Ο συνδυασμός δεδομένων που προέρχονται από διασυνδέσεις προγραμματισμού εφαρμογών (API) που υπάρχουν στο λογισμικό συσκευών πελατών ενέχει επίσης τον κίνδυνο αναγνώρισης των συσκευών βάσει του ψηφιακού τους αποτυπώματος. Τα διάφορα λογισμικά, πλατφόρμες και API παρέχουν πρόσβαση σε διαφορετικά στοιχεία πληροφοριών που είναι αποθηκευμένα στη συσκευή. Για παράδειγμα, η JavaScript API του φυλλομετρητή ιστού μπορεί να παρέχει πληροφορίες σχετικά με το μέγεθος οθόνης, το βάθος χρώματος και τις διαθέσιμες γραμματοσειρές συστήματος. Κάποιες άλλες API μπορούν να ζητήσουν πρόσβαση σε στοιχεία πληροφοριών που είναι αποθηκευμένα στο υλικολογισμικό (π.χ. ο τύπος της κεντρικής μονάδας επεξεργασίας), στο λειτουργικό σύστημα (π.χ. ο τύπος του λειτουργικού συστήματος) ή στο μοντέλο της κάρτας γραφικών.[22] Οι κλήσεις API μπορούν επίσης να αποκαλύψουν την παρουσία εγκατεστημένου λογισμικού (π.χ. συνδεόμενες υπομονάδες για φυλλομετρητή) ή ακόμα και τους ακριβείς αριθμούς έκδοσης. Η πρόσβαση σε τέτοιου είδους σύνολα πληροφοριών αυξάνει τον αριθμό των bit πληροφοριών (εντροπία) και, κατά συνέπεια, τον κίνδυνο μοναδικής αναγνώρισης φυσικών προσώπων μέσω της συσκευής τους.[23]

---

[19] Panopticlick, Electronic Frontier Foundation, 2010. https://panopticlick.eff.org/

[20] Yen, 2012. Host Fingerprinting and Tracking on the Web: Privacy and Security Implications. http://research.microsoft.com/pubs/156901/ndss2012.pdf

[21] Eckersley, 2010. A Primer on Information Theory and Privacy.https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

[22] Mowery, 2012. Pixel Perfect: Fingerprinting Canvas in HTML5. http://cseweb.ucsd.edu/~hovav/dist/canvas.pdf

[23] Mozilla, 2014. https://wiki.mozilla.org/Fingerprinting

Σε αντίθεση με τα cookies HTTP, η διαδικασία αναγνώρισης συσκευών βάσει ψηφιακού αποτυπώματος μπορεί να λειτουργεί συγκαλυμμένα.[24] Δεν υπάρχουν απλά μέσα για να αποτρέψουν οι χρήστες την εν λόγω δραστηριότητα, ενώ είναι ελάχιστες οι διαθέσιμες δυνατότητες επαναφοράς ή τροποποίησης των στοιχείων πληροφοριών που χρησιμοποιούνται για τη δημιουργία του αποτυπώματος. Συνεπώς, τα ψηφιακά αποτυπώματα συσκευών μπορούν να χρησιμοποιηθούν από τρίτους με σκοπό την κρυφή αναγνώριση ή τον εντοπισμό χρηστών, με τη δυνατότητα να τους απευθύνουν στοχευμένο περιεχόμενο ή με άλλο τρόπο να τους επιφυλάσσουν διαφορετική αντιμετώπιση.

Όπως επισημαίνεται στη γνώμη 16/2011[25], οι διαφημιστικές εταιρείες υποστηρίζουν ότι η χρήση μοναδικών κωδικών ή άλλων τιμών δεν συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Αυτό έρχεται σε αντίθεση με τον σκοπό της επεξεργασίας που γίνεται για την παροχή εξατομικευμένου περιεχομένου και διαφημίσεων, δηλαδή την άμεση επικοινωνία με συγκεκριμένο φυσικό πρόσωπο. Η ομάδα εργασίας έχει επανειλημμένα υποστηρίξει ότι τα εν λόγω μοναδικά αναγνωριστικά χαρακτηρίζονται ως δεδομένα προσωπικού χαρακτήρα.[26]

6. Νομικό πλαίσιο

Σε περιπτώσεις δημιουργίας αποτυπώματος μέσω της αποθήκευσης πληροφοριών ή της πρόσβασης σε πληροφορίες που βρίσκονται αποθηκευμένες στην τερματική συσκευή του χρήστη, ισχύει η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Όπως περιγράφεται στη γνώμη 04/2012, το άρθρο 5 παράγραφος 3 επιτρέπει την απαλλαγή από την απαίτηση της συναίνεσης εφόσον πληρούται ένα από τα ακόλουθα κριτήρια:

ΚΡΙΤΗΡΙΟ Α: τεχνικής φύσεως αποθήκευση ή πρόσβαση « αποκλειστικός σκοπός της οποίας είναι η διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών».

ΚΡΙΤΗΡΙΟ Β: τεχνικής φύσεως αποθήκευση ή πρόσβαση η οποία «*είναι αναγκαία μόνο για την παροχή υπηρεσίας στην κοινωνία των πληροφοριών την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής* ».

Επιπλέον, ο χειριστής δικτυακού τόπου πρέπει να σέβεται την προσδιορισθείσα έννοια κάθε άλλου σήματος το οποίο υποδεικνύει την προτίμηση του χρήστη εν προκειμένω - όπως η κεφαλίδα «Do Not Track» (απαγόρευση της ιχνηλάτησης)[27].[28]

---

[24] Το πρωτόκολλο προϋποθέτει την αποστολή ειδοποίησης στον χρήστη μόνο σε ειδικές περιπτώσεις, όπως η προδιαγραφή γεωεντοπισμού HTML5 API. Βλέπε: http://www.w3.org/TR/geolocation-API/#privacy_for_uas.

[25] Ομάδα εργασίας του άρθρου 29, 2014. Γνώμη 16/2011 σχετικά με τη σύσταση βέλτιστων πρακτικών EASA/IAB για την επιγραμμική συμπεριφορική διαφήμιση. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_el.pdf

[26] Ομάδα εργασίας του άρθρου 29, 2014. Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης, σ. 11-12. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf

[27] W3C, Tracking Preference Expression (DNT). http://www.w3.org/TR/tracking-dnt/

[28] Το πρωτόκολλο «Do Not Track» (απαγόρευση της ιχνηλάτησης) έχει, υπό ορισμένες προϋποθέσεις, τη δυνατότητα να μετατραπεί σε μηχανισμό συγκεκριμένης συγκατάθεσης που συνάδει με την αιτιολογική

Μολονότι η εφαρμογή της οδηγίας για την προστασία των δεδομένων δεν εμπίπτει στο πεδίο εφαρμογής της παρούσας γνώμης, σε κάθε περίπτωση κατά την οποία η δημιουργία ψηφιακού αποτυπώματος συσκευών συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα, είναι σημαντικό να πραγματοποιείται σύμφωνα με κάθε σχετική διάταξη της εν λόγω οδηγίας.

Στο άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες θεσπίζεται η απαίτηση εξασφάλισης της συγκατάθεσης του χρήστη για κάθε τρίτο που προτίθεται να αποθηκεύσει ή να αποκτήσει πρόσβαση σε πληροφορίες που είναι αποθηκευμένες στην τερματική συσκευή του χρήστη, ακόμα και αν οι εν λόγω πληροφορίες δεν θεωρούνται ακόμα δεδομένα προσωπικού χαρακτήρα. Η ομάδα εργασίας του άρθρου 29 έχει εξετάσει το ζήτημα της συγκατάθεσης σε σειρά από γνώμες που έχει εκδώσει, αναφερόμενη τόσο γενικά[29] όσο και ειδικότερα στην επιγραμμική συμπεριφορική διαφήμιση.[30] Η ομάδα εργασίας έχει επίσης εξετάσει την απαίτηση συγκατάθεσης στο πλαίσιο του άρθρου 5 παράγραφος 3, καθώς και τα cookies.[31]

Αξίζει να υπενθυμιστεί η γνώμη 02/2013 για τις εφαρμογές των έξυπνων συσκευών[32], στην οποία επισημαίνεται ότι:

«η διάκριση μεταξύ της συγκατάθεσης που απαιτείται για την τοποθέτηση και την ανάγνωση πληροφοριών από τη συσκευή και της συγκατάθεσης που απαιτείται προκειμένου να υπάρχει νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Μολονότι και οι δύο απαιτήσεις συγκατάθεσης είναι εφαρμοστέες ταυτόχρονα [...] τα δύο είδη συγκατάθεσης είναι δυνατόν στην πράξη να συμπίπτουν, υπό την προϋπόθεση ότι ο τελικός χρήστης γνωρίζει σαφώς σε τι συγκατατίθεται.»

Στην αιτιολογική σκέψη 66 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες γίνεται αναφορά στην «*αυθαίρετη εισβολή στην ιδιωτική σφαίρα*», ενώ το άρθρο 5 καλύπτει την απαίτηση απορρήτου των επικοινωνιών. Το άρθρο 5 παράγραφος 3 μπορεί να θεωρηθεί ως επέκταση του απορρήτου των πληροφοριών στις πληροφορίες που βρίσκονται αποθηκευμένες ή είναι προσβάσιμες στη συσκευή του χρήστη. Συνεπώς, κάθε επεξεργασία εκ μέρους τρίτων η οποία επηρεάζει τη συμπεριφορά της εν λόγω συσκευής ή οδηγεί καθ' οιονδήποτε άλλο τρόπο στην αποθήκευση πληροφοριών ή στη χορήγηση πρόσβασης σε πληροφορίες στη συγκεκριμένη συσκευή, ή

σκέψη 66 της οδηγίας 2009/136/ΕΚ. Η αιτιολογική σκέψη επιτρέπει στους χρήστες να εκφράζουν τη συγκατάθεσή τους μέσω των ρυθμίσεων του φυλλομετρητή τους, μόνον όμως εφόσον η συγκατάθεση συμμορφώνεται με τις προαναφερόμενες απαιτήσεις έγκυρης συγκατάθεσης. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

[29] Ομάδα εργασίας του άρθρου 29, 2011. Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_el.pdf

[30] Ομάδα εργασίας του άρθρου 29, 2010. Γνώμη 2/2010 σχετικά με την επιγραμμική συμπεριφορική διαφήμιση. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_el.pdf

[31] Ομάδα εργασίας του άρθρου 29, 2013. Working Document 02/2013 providing guidance on obtaining consent for cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[32] Ομάδα εργασίας του άρθρου 29, 2013. Γνώμη 02/2013 για τις εφαρμογές των έξυπνων συσκευών. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_el.pdf

οδηγεί σε έκθεση δεδομένων από την εν λόγω συσκευή εμπίπτει στο πεδίο εφαρμογής του άρθρου 5 παράγραφος 3.

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. 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. Παράδειγμα αποτελεί μια εφαρμογή κινητού τηλεφώνου η οποία επεξεργάζεται τον κατάλογο επαφών του χρήστη, όπου ο ίδιος ο χρήστης έχει αποθηκεύσει τα στοιχεία των επαφών, όμως η πρόσβαση σε αυτήν πραγματοποιείται από τρίτο. Δεν είναι ορθή η ερμηνεία σύμφωνα με την οποία δεν απαιτείται 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).

Επομένως, είναι σημαντικό οι τρίτοι να έχουν κατά νου ότι στις περιπτώσεις κατά τις οποίες η δημιουργία ψηφιακού αποτυπώματος συσκευής απαιτεί την αποθήκευση (ενός συνόλου) πληροφοριών ή την πρόσβαση σε πληροφορίες στη συσκευή του χρήστη, τότε απαιτείται συγκατάθεση (εκτός εάν ισχύει έγκυρη απαλλαγή). Αυτό ισχύει ακόμα και αν ορισμένα από τα εν λόγω στοιχεία πληροφοριών δεν απαιτούν την αποθήκευση πληροφοριών ή την πρόσβαση σε πληροφορίες.

7. Σενάρια περιπτώσεων χρήσης

7.1. Περίπτωση χρήσης: Εργαλεία ανάλυσης δικτυακών τόπων πρώτου μέρους

Ορισμένες επιγραμμικές υπηρεσίες προτείνουν την αναγνώριση συσκευών βάσει ψηφιακού αποτυπώματος συσκευών ως εναλλακτική επιλογή έναντι των cookies HTTP, με σκοπό την παροχή εργαλείων ανάλυσης χωρίς την ανάγκη εξασφάλισης συγκατάθεσης βάσει του άρθρου 5 παράγραφος 3. Στη γνώμη 04/2012 η ομάδα εργασίας αναγνωρίζει την ανάγκη ύπαρξης τρίτου κριτηρίου απαλλαγής για την απαίτηση συγκατάθεσης για εργαλεία ανάλυσης πρώτου μέρους:

«*υπό την προϋπόθεση ότι περιορίζονται αυστηρά σε σκοπούς συλλογής συγκεντρωτικών στατιστικών δεδομένων από πρώτο μέρος και ότι χρησιμοποιούνται από δικτυακούς τόπους οι οποίοι ήδη παρέχουν σαφή πληροφόρηση σχετικά με τα συγκεκριμένα cookies στους όρους τους περί προστασίας της ιδιωτικότητας, καθώς και επαρκή εχέγγυα ως προς το εν λόγω ζήτημα. Τα εχέγγυα αυτά περιλαμβάνουν, κανονικά, έναν εύχρηστο μηχανισμό με τον οποίον ο χρήστης μπορεί να δηλώσει την προτίμησή του για τη μη συλλογή δεδομένων, καθώς και ολοκληρωμένους μηχανισμούς ανωνυμοποίησης οι οποίοι εφαρμόζονται σε άλλες συλλεγόμενες αναγνωρίσιμες πληροφορίες, όπως είναι οι διευθύνσεις IP.*»

Ωστόσο, στη γνώμη επισημαίνεται επίσης ότι επί του παρόντος δεν υφίσταται κανενός είδους απαλλαγή για τα cookies που περιορίζονται αυστηρά σε σκοπούς συλλογής συγκεντρωτικών και ανωνυμοποιημένων στατιστικών δεδομένων από πρώτο μέρος.[33] Συνεπώς, τα εργαλεία ανάλυσης

[33] Ομάδα εργασίας του άρθρου 29, 2012. Γνώμη 04/2012 σχετικά με την απαλλαγή που ισχύει σε σχέση με τη συναίνεση για τα cookies, σ. 10-11.

δικτυακών τόπων πρώτου μέρους μέσω της δημιουργίας ψηφιακού αποτυπώματος συσκευών δεν εμπίπτουν στην απαλλαγή βάσει του ΚΡΙΤΗΡΙΟΥ Α ή Β, και απαιτείται η συγκατάθεση του χρήστη.

7.2. Περίπτωση χρήσης: Ιχνηλάτηση για την επιγραμμική συμπεριφορική διαφήμιση

Πολλοί δικτυακοί τόποι περιέχουν δικτυακούς «κοριούς», ετικέτες εικονοστοιχείων και κώδικα JavaScript ώστε να είναι δυνατή η παροχή υπηρεσιών διαφήμισης. Αυτό έχει ως αποτέλεσμα την υποβολή σειράς αιτήσεων για στοιχεία πληροφοριών από τη συσκευή του χρήστη. Οι αιτήσεις διαβιβάζονται στους τρίτους που παρέχουν τις υπηρεσίες διαφήμισης, δίνοντάς τους τη δυνατότητα να δημιουργήσουν ένα ψηφιακό αποτύπωμα συσκευής για να ακολουθούν τους χρήστες διαχρονικά και μεταξύ διαφορετικών δικτυακών τόπων και να δημιουργήσουν ένα προφίλ ενδιαφερόντων για στοχευμένη διαφήμιση, ακόμα και αν ο χρήστης δεν συγκατατεθεί στη χρήση cookies. Η εν λόγω επεξεργασία μπορεί από τεχνική άποψη να διενεργείται με συγκεκαλυμμένο τρόπο εν αγνοία του χρήστη.

Στη γνώμη 04/2012 επισημαίνεται ότι η διαφήμιση εκ μέρους τρίτων δεν εμπίπτει στην απαλλαγή που ορίζεται στο ΚΡΙΤΗΡΙΟ Α ή Β. Ως εκ τούτου, η δημιουργία ψηφιακού αποτυπώματος συσκευών με σκοπό τη στοχευμένη διαφήμιση απαιτεί τη συγκατάθεση του χρήστη.

7.3. Περίπτωση χρήσης: Παροχή δικτύου

Η ορθή διαχείριση ενός δικτύου απαιτεί τη διαβίβαση ορισμένων στοιχείων πληροφοριών σχετικών με κάθε συσκευή του δικτύου. Για παράδειγμα, ένα σημείο ασύρματης πρόσβασης το οποίο διαχειρίζεται τη σύνδεση μεταξύ ασύρματων συσκευών και ενσύρματου δικτύου επεξεργάζεται μοναδικά και μη μοναδικά στοιχεία πληροφοριών, όπως η διεύθυνση[34] και το κανάλι MAC, με σκοπό την ορθή συντήρηση των συνδέσεων και την ορθή δρομολόγηση πακέτων δεδομένων.

Όταν η παροχή δικτύου απαιτεί στοιχεία πληροφοριών τα οποία αποθηκεύουν πληροφορίες ή αποκτούν πρόσβαση σε πληροφορίες στη συσκευή του χρήστη, τότε εμπίπτει στο πεδίο εφαρμογής του άρθρου 5 παράγραφος 3. Όταν η εν λόγω επεξεργασία είναι απαραίτητη για την ομαλή λειτουργία του δικτύου, τότε ισχύει η απαλλαγή βάσει του ΚΡΙΤΗΡΙΟΥ Α.

Η δευτερεύουσα χρήση ενός στοιχείου πληροφοριών ή ενός ψηφιακού αποτυπώματος με σκοπό την ιχνηλάτηση δεν θεωρείται ότι γίνεται «*με αποκλειστικό σκοπό τη διενέργεια της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών*» ούτε «*είναι αναγκαία μόνο για την παροχή υπηρεσίας της στην κοινωνία των πληροφοριών την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής*». Κατά την εξέταση των cookies πολλαπλού σκοπού στη γνώμη 04/2012, η ομάδα εργασίας του άρθρου 29 επεσήμανε ότι «*η ιχνηλάτηση είναι λίαν απίθανο να πληροί τους όρους του ΚΡΙΤΗΡΙΟΥ Α ή Β*», άρα αν κάποιος τρίτος επιθυμεί να χρησιμοποιήσει ψηφιακό αποτύπωμα συσκευής για πολλαπλούς σκοπούς, τότε «*απαλλάσσεται από την απαίτηση συναίνεσης μόνον εφόσον όλοι οι διακριτοί σκοποί [...] απαλλάσσονται ατομικώς από την εν λόγω απαίτηση*».

[34] Η διεύθυνση MAC πιθανόν να είναι μοναδική για κάθε συσκευή του δικτύου. Το πρόθεμα διεύθυνσης MAC αναφέρεται επίσης στον κατασκευαστή τσιπ.

7.4. Περίπτωση χρήσης: Πρόσβαση και έλεγχος χρήστη

Μια επιγραμμική υπηρεσία ενδεχομένως προτίθεται να χρησιμοποιήσει ψηφιακό αποτύπωμα συσκευών για να υποστηρίξει την πρόσβαση και τον έλεγχο του χρήστη (δηλαδή σε συνδυασμό με το όνομα χρήστη και τον κωδικό πρόσβασης). Το ψηφιακό αποτύπωμα συσκευής μπορεί να χρησιμοποιηθεί για να διασφαλίσει ότι ένας λογαριασμός είναι συνδεδεμένος με μια συγκεκριμένη συσκευή ούτως ώστε η συσκευή να ενεργεί ως δεύτερος παράγοντας επαλήθευσης ταυτότητας.

Για παράδειγμα, μια συνδρομητική υπηρεσία μουσικής επιτρέπει στον χρήστη την πρόσβαση στην υπηρεσία μόνο από περιορισμένο αριθμό συγκεκριμένων συσκευών. Αν ο χρήστης έχει χρησιμοποιήσει στο παρελθόν τη συγκεκριμένη συσκευή, τότε ο χειριστής του δικτυακού τόπου μπορεί να επιλέξει τη διενέργεια λιγότερων ελέγχων επαλήθευσης πριν από την παροχή πρόσβασης.

Αν το ψηφιακό αποτύπωμα συσκευής αποτελείται από στοιχεία πληροφοριών τα οποία αποθηκεύουν πληροφορίες ή αποκτούν πρόσβαση σε πληροφορίες στη συσκευή του χρήστη, τότε η εν λόγω περίπτωση εμπίπτει στο πεδίο εφαρμογής του άρθρου 5 παράγραφος 3. Ωστόσο, οι εν λόγω σκοποί δεν θεωρούνται «*αναγκαίοι μόνο*» για την παροχή της λειτουργικής δυνατότητας την οποία έχει ζητήσει ρητά ο χρήστης και, συνεπώς, απαιτείται έγκυρη συγκατάθεση του χρήστη.

Οι χειριστές δικτυακών τόπων μπορεί να χρειαστεί να εξετάσουν μια σειρά κατάλληλων και αναλογικών ελέγχων ή οποιαδήποτε άλλη μέθοδο επαλήθευσης ταυτότητας (π.χ. κωδικό πρόσβασης μίας χρήσης, δευτερεύουσα επιβεβαίωση διεύθυνσης ηλεκτρονικού ταχυδρομείου).

7.5. Περίπτωση χρήσης: Ασφάλεια με επίκεντρο τον χρήστη

Στη γνώμη 04/2012, η ομάδα εργασίας του άρθρου 29 επεσήμανε ότι «*cookies τα οποία εγκαθίστανται με ειδικό σκοπό την αύξηση της ασφάλειας της υπηρεσίας την οποία έχει ζητήσει ρητά ο χρήστης*» (π.χ. για την ανίχνευση επανειλημμένων αποτυχημένων προσπαθειών σύνδεσης) τυγχάνουν απαλλαγής βάσει του ΚΡΙΤΗΡΙΟΥ Β.

Η εν λόγω απαλλαγή ισχύει επίσης για τη δημιουργία ψηφιακού αποτυπώματος συσκευών, όμως, όπως και στην περίπτωση των cookies, «*δεν καλύπτει τη χρήση της τεχνικής η οποία σχετίζεται με την ασφάλεια δικτυακών τόπων ή υπηρεσιών τρίτων μερών που δεν έχουν ζητηθεί ρητά από τον χρήστη*».

Τα δεδομένα που συλλέγονται μέσω ψηφιακού αποτυπώματος για την εξυπηρέτηση σκοπού που αφορά την ασφάλεια με επίκεντρο τον χρήστη τυγχάνουν απαλλαγής σε σχέση με τη συγκατάθεση υπό την προϋπόθεση ότι δεν χρησιμοποιούνται για δευτερογενείς σκοπούς. Πρέπει να παρέχονται τεχνικά και οργανωτικά εχέγγυα για την αποτροπή οιασδήποτε δευτερογενούς χρήσης δεδομένων αποτυπώματος, τα οποία συνήθως διατηρούνται σε αρχεία καταγραφής ασφαλείας του διακομιστή.

7.6. Περίπτωση χρήσης: Προσαρμογή της διεπαφής χρήστη στη συσκευή

Η πρόσβαση σε πληροφορίες της συσκευής όπως το μέγεθος της οθόνης μπορεί να αποβεί χρήσιμη για τη βελτιστοποίηση της διάταξης του περιεχομένου.[35] Για παράδειγμα, ένας δικτυακός τόπος ενημέρωσης θα μπορούσε να μεταβεί σε λειτουργία χαμηλών γραφικών ή σε διάταξη μονής στήλης για τις κινητές συσκευές. Εναλλακτικά, ένας δικτυακός τόπος ή τα τρίτα μέρη που παρέχουν

[35] Πρέπει να σημειωθεί ότι για την επίτευξη του ίδιου στόχου ενδέχεται να υπάρχουν και άλλες μέθοδοι που να παρέχουν λιγότερες πληροφορίες σχετικά με την ιδιωτική ζωή, όπως η συμβολοσειρά παράγοντα χρήστη.

περιεχόμενο μέσω αυτού μπορούν να υποβάλουν ερώτημα στη συσκευή προκειμένου να εξακριβώσουν τεχνικές δυνατότητες όπως π.χ. ποιες μορφές βίντεο υποστηρίζει.

Όταν κάποιος τρίτος ζητεί πρόσβαση σε πληροφορίες που βρίσκονται αποθηκευμένες στη συσκευή του χρήστη, με αποκλειστικό σκοπό την προσαρμογή του περιεχομένου στα χαρακτηριστικά της συσκευής, τότε ισχύει το ΚΡΙΤΗΡΙΟ Β. Συνεπώς, αυτό σημαίνει ότι δεν απαιτείται συγκατάθεση για βραχυπρόθεσμη προσαρμογή της διεπαφής χρήστη.

Ωστόσο, αν οι εν λόγω πληροφορίες χρησιμοποιούνται και για δευτερεύοντες σκοπούς, παύει πλέον να ισχύει η συγκεκριμένη απαλλαγή.

8. Συμπέρασμα

Στην παρούσα γνώμη εξετάζεται το θέμα της αναγνώρισης συσκευών βάσει ψηφιακού αποτυπώματος και η δυνατότητα εφαρμογής του άρθρου 5 παράγραφος 3 της οδηγίας 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ, με την επιφύλαξη των διατάξεων της οδηγίας 95/46/ΕΚ για την προστασία των δεδομένων. Η παρούσα γνώμη αναπτύσσει περαιτέρω τα όσα αναφέρονται στην προηγούμενη γνώμη 04/2012 σχετικά με την απαλλαγή που ισχύει σε σχέση με τη συναίνεση για τα cookies και επιβεβαιώνει ότι, σε ορισμένες περιπτώσεις, η τεχνολογία οδηγεί στην εξασφάλιση πρόσβασης ή την αποθήκευση πληροφοριών στην τερματική συσκευή του χρήστη. Επομένως, το άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ισχύει και για τις περιπτώσεις αναγνώρισης συσκευών βάσει ψηφιακού αποτυπώματος.

Συνεπώς, τα μέρη που επιθυμούν να επεξεργάζονται ψηφιακά αποτυπώματα συσκευών που έχουν δημιουργηθεί μέσω της εξασφάλισης πρόσβασης σε πληροφορίες ή της αποθήκευσης πληροφοριών στην τερματική συσκευή του χρήστη πρέπει πρώτα να εξασφαλίζουν την έγκυρη συγκατάθεση του χρήστη (εκτός αν ισχύει απαλλαγή).