PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

14/CS
WP 224

Stanovisko č. 9/2014 k uplatňování směrnice 2002/58/ES na otisky zařízení

Přijaté dne 25. listopadu 2014

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na články 29 a 30 uvedené směrnice,

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO:

1. Shrnutí

Využívání otisků zařízení (*device fingerprinting*) vyvolává u jednotlivců vážné obavy s ohledem na ochranu údajů. Řada on-line služeb například navrhuje otisky zařízení jako alternativu cookies HTTP za účelem poskytování analytik nebo sledování, aniž by byl nutný souhlas podle čl. 5 odst. 3[1]. To ukazuje, že rizika spojená s využíváním otisků zařízení nejsou pouze teoretická, a výzkum prokazuje, že se již otisky zařízení využívají[2].

V tomto stanovisku se pracovní skupina podle článku 29 zabývá otázkou snímání otisků zařízení a použitelností čl. 5 odst. 3 směrnice 2002/58/ES o soukromí a elektronických komunikacích ve znění směrnice 2009/136/ES, aniž by tím byla dotčena ustanovení směrnice 95/46/ES o ochraně osobních údajů. Hlavním závěrem tohoto stanoviska je to, že se na otisky zařízení vztahuje čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

Toto stanovisko navazuje na dřívější stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies[3] a informuje třetí osoby[4], které zpracovávají otisky zařízení vytvořené získáním přístupu k informacím nebo uchováváním informací v koncovém zařízení uživatele, o tom, že tak mohou činit pouze s platným souhlasem uživatele (pokud se nepoužije výjimka).

2. Úvod

V čl. 5 odst. 3 směrnice 2002/58/ES ve znění směrnice 2009/136/ES[5] (dále jen „směrnice o soukromí a elektronických komunikacích“) je stanoveno, že členské státy zajistí, aby „*uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele*“ povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí 95/46/ES[6] (směrnice o ochraně osobních údajů), mimo jiné o účelu zpracování[7].

Ve stanovisku č. 4/2012 posoudila pracovní skupina podle článku 29 ustanovení čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích ve vztahu k uchovávání informací nebo přístupu

[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] Pracovní skupina podle článku 29, 2012. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf

[4] „Třetí osoba“ uvedená v 66. bodě odůvodnění směrnice 2009/136/ES.

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

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

[7] To nebrání technickému uchovávání informací nebo přístupu k informacím výhradně za účelem přenosu sdělení prostřednictvím sítě elektronických komunikací nebo v případě, kdy je nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal.

k informacím prostřednictvím používání cookies. Ve stanovisku bylo uvedeno, že se ustanovení čl. 5 odst. 3 nevztahuje výhradně na cookies, nýbrž je použitelné i na „podobné technologie“.

Toto stanovisko představuje reakci na rostoucí počet zpráv, že třetí osoby aktivně zkoumají technologie alternativní ke cookies k řadě účelů ve snaze vyhnout se požadavku na souhlas stanovenému v čl. 5 odst. 3. Stanovisko se zabývá zejména kombinováním souboru prvků informací za účelem jedinečné identifikace konkrétních zařízení nebo aplikací, tzv. „snímáním otisků zařízení“.

Také otisky zařízení mohou představovat osobní údaje. Toto stanovisko nepředkládá analýzu příslušných ustanovení směrnice o ochraně osobních údajů, nýbrž se zabývá otázkami ochrany údajů, které jsou obzvláště důležité v souvislosti se snímáním otisků zařízení. Příkladem je spojení několika prvků informací, zejména jedinečných identifikátorů, jako jsou IP adresy, přičemž účelem zpracování je identifikace uživatelů na webových stránkách v průběhu času, jak je tomu například u behaviorálně cílené reklamy. V těchto případech musí být zpracování rovněž v souladu s pravidly stanovenými ve směrnici o ochraně osobních údajů.

Technologie snímání otisků zařízení není omezena na konfigurační parametry tradičního internetového prohlížeče ve stolním počítači. Snímání otisků zařízení není spojeno ani s určitým protokolem, nýbrž je lze použít u široké škály zařízení připojených k internetu, spotřební elektroniky a aplikací, včetně aplikací běžících v mobilních zařízeních, inteligentních televizí, herních konzol, čteček elektronických knih, internetového rádia, systémů ve vozidlech nebo inteligentních měřičů[8].

3. Definice

V RFC6973[9] je otisk vymezen jako „soubor prvků informací, které identifikují zařízení nebo aplikaci“. V tomto stanovisku se tento pojem používá v širokém smyslu a znamená, že se jedná o soubor informací, které lze použít k vyčlenění[10], propojení[11] nebo dedukci[12] uživatele, uživatelského agenta (*user agent*) nebo zařízení v průběhu času. To zahrnuje mimo jiné údaje odvozené z:

a) konfigurace uživatelského agenta / zařízení nebo

b) dat získaných používáním síťových komunikačních protokolů.

Existuje mnoho druhů údajů, jež mohou tvořit otisk, včetně těchto příkladů:

[8] Někdy nazývané „internet věcí“.

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

[10] *Vyčlenění*: možnost izolovat některé nebo všechny záznamy, které v daném souboru dat identifikují fyzickou osobu, stanovisko č. 5/2014 k technikám anonymizace, s. 11–12.

[11] *Možnost propojení*: schopnost propojit nejméně dva záznamy týkající se téhož subjektu údajů nebo téže skupiny subjektů údajů (ve stejné databázi nebo ve dvou různých databázích). Může-li útočník zjistit (například pomocí srovnávací analýzy), že stejné skupině fyzických osob jsou přiděleny dva záznamy, ale nemůže z této skupiny vyčlenit jednotlivé osoby, je tato technika odolná proti „vyčlenění“, avšak nikoli proti možnosti propojení, stanovisko č. 5/2014 k technikám anonymizace, s. 11–12.

[12] *Dedukce*: možnost vyvodit se značnou pravděpodobností hodnotu jednoho atributu z hodnot souboru jiných atributů, stanovisko č. 5/2014 k technikám anonymizace, s. 11–12.

a) CSS informace (kaskádové styly);

b) JavaScriptové objekty (např. dokument, okno, obrazovka, navigátor, datum a jazyk);

c) informace z HTTP hlaviček (např. počet bitů informací v identifikačním řetězci prohlížeče (*user agent string*), seřazení HTTP hlaviček, rozdíly HTTP hlaviček dle použité HTTP metody);

d) informace o hodinovém signálu (např. skluz a chyby);

e) odchylka sady protokolů TCP;

f) nainstalované fonty;

g) informace o nainstalovaných rozšířeních (např. údaje o konfiguraci a číslu verze)[13];

h) používání interního rozhraní pro programování aplikací[14] (API) na základě uživatelského agenta / zařízení nebo

i) používání externího API webových služeb, se kterými uživatelský agent / zařízení komunikuje.

4. Technické souvislosti

Při vyvíjení internetu a webu se přihlíželo k nutnosti vytvořit prostředí sítě s odolnou a otevřenou architekturou[15]. Kvůli řešením zvoleným k uspokojení těchto potřeb přenášejí zařízení určité prvky informací. Řada protokolů zahrnuje celou škálu povinných a nepovinných prvků informací. Protokol HTTP/1.1[16] například specifikuje hlavičková pole, jež serveru a klientovi umožňují zahrnout dodatečné informace ohledně hypertextu. Některá z těchto polí byla výslovně navržena tak, aby mohl server rozpoznávat typy klientů. Pole v hlavičce žádosti uživatelského agenta obsahuje například popis: „*Určeno pro statistické účely, ke sledování porušování protokolu a automatickému rozpoznávání user agenta za účelem přizpůsobení odpovědi s cílem vyhnout se konkrétním omezením uživatelských agentů*“.

K typickým příkladům použití identifikačního řetězce prohlížeče patří optimalizace uspořádání obsahu pro určitý typ zařízení; používání těchto informací k zacílení obsahu na konkrétní uživatele[17] nebo shromažďování informací o zařízení pro bezpečnostní či analytické účely.

---

[13] Viz a) http://www.w3.org/wiki/Fingerprinting, b) http://w3c.github.io/fingerprinting-guidance/#wsj-orbitz, c) https://wiki.mozilla.org/Fingerprinting a d) https://trac.webkit.org/wiki/Fingerprinting

[14] API poskytuje uživatelsky přívětivý rámec pro přístup k funkcím nebo rutinám v softwarovém komponentu.

[15] Kahn, 1972. Communications Principles for Operating Systems. Interní memorandum 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

5. Rizika z hlediska ochrany údajů

Jelikož individuální HTTP hlavička má obvykle neunikátní hodnotu, lze uživatele jen ojediněle identifikovat jednotlivě pouze z tohoto prvku informací[18]. Druhy médií podporované prohlížečem jsou například často stejné u mnoha ostatních uživatelů používajících stejnou verzi prohlížeče. Jsou-li tyto neunikátní prvky informací zpracovány izolovaně, nepředstavují z hlediska ochrany údajů obvykle rizika.

Řadu prvků informací však lze spojit s cílem vytvořit soubor, který je dostatečně unikátní (zejména v případě spojení s jinými identifikátory, jako je výchozí IP adresa), aby mohl fungovat jako unikátní otisk dotyčného zařízení nebo aplikace. Takovýto otisk umožňuje odlišit jedno zařízení od druhého a lze jej použít jako skrytou alternativu cookies k sledování chování na internetu v čase[19,20,21]. V důsledku toho může být s tímto otiskem zařízení spojena určitá fyzická osoba (a tudíž být identifikována či identifikovatelná).

Rizika snímání otisků zařízení z hlediska ochrany údajů zvyšuje skutečnost, že jedinečný soubor prvků informací není dostupný pouze provozovateli internetové stránky, nýbrž i mnoha třetím osobám. To je v rozporu se zásadou *stejného původu* cookies HTTP a navíc to je zhoršeno technickou povahou celosvětové sítě, kdy k obsahu určité internetové stránky přispívá mnoho třetích osob.

Je běžné, že je jedna internetová stránka vytvářena dynamicky v reálném čase vyžadováním obsahu z mnoha zdrojů. Každý z těchto zdrojů vytváří vlastní HTTP žádosti, stahuje obrázky a JavaScriptové a CSS soubory. Mnoho internetových stránek obsahuje rovněž webové štěnice (*web bugs*) a sledovací skripty. Navíc mohou vytvářet HTTP žádosti, které zaznamenávají, pokud uživatel roluje text nebo klikne na určitou stránku, obrázek či reklamu. Třetí osoby mají proto často možnost shromažďovat informace potřebné k snímání otisků zařízení uživatele.

Rizika z hlediska ochrany údajů nejsou omezena na sledování třetími osobami. Riziko snímání otisků zařízení představuje i kombinace údajů získaných prostřednictvím rozhraní pro programování aplikací (*Application Programming Interface*, API) v softwaru v klientských zařízeních. Různý software, platformy a API umožňují přístup k různým prvkům informacím uchovávaným v zařízení. JavaScriptové API ve webovém prohlížeči může například poskytovat informace týkající se velikosti obrazovky, barevné hloubky a dostupných systémových fontů. Jiná API mohou požadovat přístup k prvkům informací uloženým ve firmware (např. typ procesoru), operačním systému (např. typ operačního systému) nebo modelu grafické karty[22]. Volání API mohou zjistit také přítomnost nainstalovaného softwaru (např. modul plug-in prohlížeče) nebo dokonce přesná čísla verzí. Přístup k

[18] Existují případy, kdy jediný prvek informací nese informace, jež mohou jedinečně identifikovat subjekt údajů, jako je přístupový token OAuth.

[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

těmto souborům informací zvyšuje počet bitů informací (entropii), a tudíž riziko rozpoznání konkrétních fyzických osob prostřednictvím jejich zařízení[23].

Na rozdíl od cookies HTTP může snímání otisků zařízení fungovat skrytě[24]. Uživatelé nemají k dispozici jednoduché prostředky, aby této aktivitě zabránili, a existují pouze omezené možnosti výmazu nebo změny prvků informací používaných k vytvoření otisku. Otisky zařízení mohou proto třetí osoby používat tajně k identifikaci nebo vyčlenění uživatelů s možností zaměřit obsah na uživatele nebo s nimi zacházet odlišně.

Ve stanovisku č. 16/2011[25] bylo uvedeno, že reklamní společností tvrdí, že používání unikátních kódů nebo jiných hodnot nezahrnuje zpracovávání osobních údajů. To je v rozporu s účelem zpracování pro poskytování cíleného obsahu a cílené reklamy na uživatele, tj. k přímé komunikaci s konkrétní fyzickou osobou. Pracovní skupina mnohokrát tvrdila, že se tyto unikátní identifikátory považují za osobní údaje[26].

6. Právní rámec

Je-li otisk vytvořen uchováváním informací nebo získáním přístupu k informacím uchovávaným v koncovém zařízení uživatele, použije se směrnice o soukromí a elektronických komunikacích.

Jak je popsáno ve stanovisku č. 4/2012, ustanovení čl. 5 odst. 3 povoluje výjimku z požadavku na souhlas, pakliže je splněno jedno z těchto kritérií:

KRITÉRIUM A: technické uchovávání nebo přístup za „*jediným účelem spočívajícím v provedení přenosu sdělení prostřednictvím sítě elektronických komunikací*“.

KRITÉRIUM B: technické uchovávání nebo přístup, které jsou „*nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal*“.

Provozovatel internetových stránek musí mimoto respektovat stanovený význam jakéhokoli jiného signálu, který udává preference uživatele v tomto ohledu, jako je hlavička[27] Do-Not-Track (Nesledovat)[28].

---

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

[24] Protokol vyžaduje signál uživateli pouze v určitých případech, jako je specifikace HTML5 API pro geolokaci. Viz: http://www.w3.org/TR/geolocation-API/#privacy_for_uas

[25] Pracovní skupina podle článku 29, 2014. Stanovisko č. 16/2011 k doporučení organizací EASA/IAB o osvědčených postupech při on-line behaviorálně cílené reklamě. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_cs.pdf

[26] Pracovní skupina podle článku 29, 2014. Stanovisko č. 5/2014 k technikám anonymizace, s. 11–12. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf

[27] Protokol Do Not Track se může za určitých okolností stát mechanismem k udělování strukturovaného souhlasu, který je v souladu s 66. bodem odůvodnění směrnice 2009/136/ES. Tento bod odůvodnění umožňuje uživatelům vyslovit souhlas nastavením prohlížeče, avšak pouze v případě, je-li souhlas v souladu s výše

Ačkoliv se toto stanovisko netýká uplatňování směrnice o ochraně osobních údajů, v případě, že snímání otisků zařízení představuje zpracovávání osobních údajů, je důležité, aby se provádělo v souladu se všemi příslušnými ustanoveními této směrnice.

Ustanovení čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích ukládá požadavek na souhlas uživatele vztahující se na každou osobu, která zamýšlí uchovávat informace nebo získat přístup k informacím uchovávaným v koncovém zařízení uživatele, a to i v případě, že se tyto informace nepovažují za osobní údaje. Pracovní skupina podle článku 29 se souhlasem zabývala v řadě stanovisek, a to obecně[29] i v souvislosti s on-line behaviorálně cílenou reklamou[30]. Pracovní skupina se zabývala požadavkem na souhlas rovněž v souvislosti s ustanoveními čl. 5 odst. 3 a cookies[31].

Je třeba připomenout stanovisko č. 2/2013 k aplikacím v inteligentních zařízeních[32], v němž se uvádělo:

„Je důležité uvědomit si rozdíl mezi souhlasem potřebným k ukládání informací v zařízení a čtení informací ze zařízení a souhlasem nutným k získání právního důvodu pro zpracování různých druhů osobních údajů. Ačkoli jsou oba požadavky týkající se souhlasu použitelné současně […], v praxi mohou být oba druhy souhlasu spojeny, za předpokladu, že uživatel byl jasně informován o tom, s čím souhlasí.“

V 66. bodě odůvodnění směrnice o soukromí a elektronických komunikacích se odkazuje na „*neodůvodněné narušení soukromé sféry*“ a článek 5 se zabývá požadavkem na důvěrnost sdělení. Lze mít za to, že ustanovení čl. 5 odst. 3 rozšiřuje požadavek na zachování důvěrnosti informací na informace, které jsou uchovávány nebo k nimž je získán přístup v koncovém zařízení uživatele. Zpracování, které provádí třetí osoba a které ovlivňuje chování tohoto zařízení či jinak zajišťuje, aby zařízení uchovávalo informace nebo umožňovalo přístup k informacím uchovávaným v tomto zařízení nebo aby je vystavilo, proto spadá do oblasti působnosti čl. 5 odst. 3.

Použití slov „*které jsou uchovávány nebo k nimž je získán přístup*“ naznačuje, že k uchovávání a přístupu nemusí dojít v rámci stejné komunikace a nemusí je provést tatáž strana. Informace, které uchovává jedna strana (včetně informací uchovávaných uživatelem nebo výrobcem zařízení) a k nimž

---

uvedenými požadavky na platný souhlas. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

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

[29] Pracovní skupina podle článku 29, 2011. Stanovisko č. 15/2011 k definici souhlasu. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[30] Pracovní skupina podle článku 29, 2010. Stanovisko č. 2/2010 k on-line behaviorálně cílené reklamě. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf

[31] Pracovní skupina podle článku 29, 2013. Pracovní dokument č. 2/2013 o pokynech k vyžadování souhlasu s cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[32] Pracovní skupina podle článku 29, 2013. Stanovisko č. 2/2013 k aplikacím v inteligentních zařízeních. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_cs.pdf

později získá přístup jiná strana, proto spadají do oblasti působnosti čl. 5 odst. 3. Příkladem je aplikace v mobilním telefonu, která zpracovává seznam kontaktů uživatele, do něhož kontaktní údaje ukládá samotný uživatel, přístup k nim však má třetí osoba. To nelze vykládat v tom smyslu, že třetí osoba nepotřebuje souhlas s přístupem k těmto informacím pouze z toho důvodu, že je neuložila. Požadavek na souhlas platí rovněž v případě přístupu k hodnotě určené pouze ke čtení (např. žádost o MAC adresu síťového rozhraní prostřednictvím API operačního systému).

Je tudíž důležité, aby měly třetí osoby na paměti, že pokud snímání otisků zařízení vyžaduje uchovávání (souboru) informací v zařízení uživatele nebo přístup k těmto informacím, je nezbytný souhlas (pokud se nepoužije platná výjimka). Tak je tomu i v případě, nevyžadují-li některé z těchto prvků informací uchovávání informací nebo přístup k informacím.

7. Scénáře případů použití

7.1 Případ použití: webová analytika první strany *(First party analytics)*

Řada on-line služeb navrhuje otisky zařízení jako alternativu cookies HTTP za účelem poskytování analytiky, aniž by bylo nutné vyžádat si souhlas podle čl. 5 odst. 3. Ve stanovisku č. 4/2012 uznala pracovní skupina potřebu třetí výjimky z požadavku na souhlas s analytikou první strany:

„omezují-li se striktně na účely souhrnných statistik první strany a jsou-li používány internetovými stránkami, které již o těchto cookies poskytují přehledné informace v rámci své politiky v oblasti ochrany údajů, jakož i odpovídající záruky týkající se ochrany údajů. Takové záruky by měly zahrnovat uživatelsky nenáročný mechanismus, s jehož pomocí se lze jakémukoliv sběru údajů vyhnout, a srozumitelné mechanismy anonymizace, které se použijí pro další shromažďované identifikovatelné informace, jako jsou IP adresy.“

Ve stanovisku se však rovněž uvádělo, že v současnosti neexistuje výjimka z požadavku na souhlas s cookies, které se striktně omezují na anonymizované účely souhrnných statistik první strany[33]. Webová analytika první strany prostřednictvím otisků zařízení tudíž nespadá do výjimky stanovené v KRITÉRIU A nebo B a je nutný souhlas uživatele.

7.2 Případ použití: sledování za účelem behaviorálně cílené reklamy

Mnoho internetových stránek obsahuje webové štěnice třetí strany, pixelové tagy a JavaScriptový kód s cílem umožnit reklamní služby. To má za následek řadu žádostí o prvky informací ze zařízení uživatele. Žádosti jsou předávány třetím osobám poskytujícím reklamní služby a umožňují jim vytvářet otisky zařízení s cílem sledovat uživatele na internetových stránkách v čase a vytvářet zájmový profil pro cílenou reklamu, a to i v případě, odmítne-li uživatel cookies. Takovéto zpracovávání lze z technického hlediska provádět skrytě bez vědomí uživatele.

Ve stanovisku č. 4/2012 bylo zdůrazněno, že reklama třetích stran nespadá do výjimky stanovené v KRITÉRIU A nebo B. Snímání otisků zařízení pro účely cílené reklamy proto vyžaduje souhlas uživatele.

[33] Pracovní skupina podle článku 29, 2012. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies, s. 10–11.

7.3 Případ použití: poskytování sítě

Náležitá správa sítě vyžaduje předávání určitých prvků informací týkajících se každého zařízení v síti. Přístupový bod WiFi, který spravuje spojení mezi bezdrátovými zařízeními a drátovou sítí, bude například zpracovávat unikátní i neunikátní prvky informací, jako je MAC adresa[34] a kanál, za účelem řádného udržování spojení a správného směrování datových paketů.

Pokud poskytování sítě vyžaduje prvky informací, které uchovávají informace nebo získávají přístup k informacím uchovávaným v zařízení uživatele, spadá toto do oblasti působnosti čl. 5 odst. 3. Je-li takové zpracování nezbytné pro běžné fungování sítě, bylo by vyňato podle KRITÉRIA A.

Druhotné použití prvku informací nebo otisku zařízení pro účely sledování se nepovažuje za použití, „*jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací*“, ani za „*nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal*“. Při posuzování víceúčelových cookies ve stanovisku č. 4/2012 pracovní skupina podle článku 29 poznamenala, že „*je velice nepravděpodobné, že by sledování splnilo KRITÉRIUM A nebo B*“, chce-li tudíž třetí osoba používat otisky zařízení k více účelům, lze je „*vyjmout z požadavku na souhlas, pouze pokud jsou všechny rozličné účely […] jednotlivě vyňaty z požadavku na souhlas*“.

7.4 Případ použití: uživatelský přístup a kontrola

On-line služba může chtít využívat otisky zařízení na podporu uživatelského přístupu a kontroly (tj. ve spojení s uživatelským jménem a heslem). Otisk zařízení lze použít k zajištění toho, aby byl účet spojen s určitým zařízením, takže zařízení představuje druhý faktor ověření.

Předplatitelská hudební služba například umožňuje uživateli přístup ke službě pouze z omezeného počtu konkrétních zařízení. Jestliže uživatel použil toto zařízení již dříve, může se provozovatel internetových stránek rozhodnout, že před poskytnutím přístupu bude provádět méně kontrol pro ověření.

Skládá-li se otisk zařízení z prvků informací, které uchovávají informace nebo získávají přístup k informacím uchovávaným v zařízení uživatele, spadá do oblasti působnosti čl. 5 odst. 3. Tyto účely se však nepokládají za „*nezbytně nutné*“ k poskytnutí funkce výslovně požadované uživatelem, a je proto nezbytný platný souhlas uživatele.

Provozovatelé internetových stránek musí případně uvážit řadu vhodných a přiměřených kontrol nebo jiný způsob ověření (např. jednorázové heslo, druhé potvrzení e-mailem).

7.5 Případ použití: zvyšování bezpečnosti uživatele

Ve stanovisku č. 4/2012 pracovní skupina podle článku 29 uvedla, že pro „*cookies nastavené pro konkrétní úkol zvyšování bezpečnosti služby, kterou si uživatel výslovně vyžádal*“ (např. k detekci opakovaných neúspěšných pokusů o nalogování se), by platila výjimka podle KRITÉRIA B.

[34] MAC adresa bude pravděpodobně u všech zařízení v síti jedinečná. Prefix MAC adresy bude odkazovat rovněž na výrobce čipu.

Tato výjimka by se vztahovala i na otisky zařízení, avšak stejně jako v případě cookies by se „*netýkala […] použití techniky, která souvisí s bezpečností internetových stránek nebo službami třetích osob, jež si uživatel výslovně nevyžádal*“.

Jsou-li prostřednictvím snímání otisků zařízení shromažďovány data za účelem zvýšení bezpečnosti uživatele, nesmí být používány k druhotným účelům, aby se na ně vztahovala výjimka z požadavku na souhlas. Je nutno přijmout technická a organizační ochranná opatření, která zamezí druhotnému použití údajů z otisků zařízení, jež jsou obvykle uchovávány v bezpečnostních záznamech na serveru.

7.6 Případ použití: přizpůsobení uživatelského rozhraní zařízení

Informace o přistupujícím zařízení, jako je například velikost obrazovky, mohou být užitečné k optimalizaci uspořádání obsahu[35]. Stránky médií mohou například v případě mobilních zařízení přepínat na nízký grafický mód nebo jeden sloupec. Internetová stránka nebo správa obsahu třetích stran prostřednictvím internetové stránky se může alternativně zařízení dotazovat za účelem zjištění technických schopností, například toho, které formáty videa jsou podporovány.

Pokud třetí osoba požaduje přístup k informacím uchovávaným v zařízení uživatele výhradně za účelem přizpůsobení obsahu vlastnostem zařízení, platí KRITÉRIUM B. To znamená, že se v případě krátkodobého přizpůsobení uživatelského rozhraní nevyžaduje souhlas.

Pokud se však tyto informace používají rovněž k druhotným účelům, tato výjimka se nepoužije.

8. Závěr

Toto stanovisko se zabývá otázkou snímání otisků zařízení a použitelností čl. 5 odst. 3 směrnice 2002/58/ES o soukromí a elektronických komunikacích ve znění směrnice 2009/136/ES, aniž by byla dotčena ustanovení směrnice 95/46/ES o ochraně osobních údajů. Toto stanovisko navazuje na dřívější stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies a potvrzuje, že v řadě případů vede technologie k získání přístupu k informacím nebo k uchovávání informací v koncovém zařízení uživatele. Na případy snímání otisků zařízení se tudíž vztahuje čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

Strany, které chtějí zpracovávat otisky zařízení vytvořené získáním přístupu k informacím nebo uchováváním informací v koncovém zařízení uživatele, si proto musí nejprve vyžádat platný souhlas uživatele (pokud se nepoužije výjimka).

[35] Upozorňuje se, že k dosažení stejného cíle mohou existovat jiné metody méně narušující soukromí, jako je používání identifikačního řetězce prohlížeče.