ARTIKEL 29-ARBETSGRUPPEN FÖR SKYDD AV PERSONUPPGIFTER

14/SV
WP 224

Yttrande 9/2014 om tillämpningen av direktiv 2002/58/EG på digitala fingeravtryck

Antaget den 25 november 2014

ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ BEHANDLING AV PERSONUPPGIFTER HAR ANTAGIT DETTA YTTRANDE

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995, genom vilket arbetsgruppen inrättades,

med beaktande av artiklarna 29 och 30 i det direktivet, och

med beaktande av dess arbetsordning.

HÄRIGENOM FÖRESKRIVS FÖLJANDE:

1. Sammanfattning

Digitala fingeravtryck ger upphov till allvarliga farhågor rörande uppgiftsskyddet för enskilda personer. Ett antal online-tjänster har t.ex. föreslagit digitala fingeravtryck som ett alternativ till HTPP-kakor för att tillhandahålla analyser eller spårning utan samtycke enligt artikel 5.3.[1] Detta visar att riskerna i samband med digitala fingeravtryck inte är teoretiska, och forskning har också visat att digitala fingeravtryck redan används.[2]

I detta yttrande behandlar artikel 29-arbetsgruppen digitala fingeravtryck och tillämpligheten av artikel 5.3 i direktiv 2002/58/EG om integritet och elektronisk kommunikation i dess ändrade lydelse enligt direktiv 2009/136/EG, utan att det påverkar bestämmelserna i direktiv 95/46/EG om skydd av personuppgifter. Det viktigaste budskapet i detta yttrande är att artikel 5.3 i direktivet om elektronisk kommunikation är tillämplig på digitala fingeravtryck.

Yttrandet bygger vidare på arbetsgruppens tidigare yttrande 04/2012 om undantag från krav på samtycke till kakor (*cookies*)[3]. Syftet är att informera tredjeparter[4] som behandlar digitala fingeravtryck som skapas genom åtkomst till eller lagring av uppgifter på användarens terminalutrustning att de endast kan göra så med användarens giltiga samtycke (om inte undantag gäller).

2. Inledning

Artikel 5.3 i direktiv 2002/58/EG om integritet och elektronisk kommunikation i dess ändrade lydelse enligt direktiv 2009/136/EG[5] föreskriver att medlemsstaterna ska säkerställa att lagring av information eller tillgång till information ”som är lagrad i en abonnents eller användares terminalutrustning” endast är tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke och har tillgång till klar och fullständig information i enlighet med direktiv 95/46/EG[6] (direktivet om skydd av personuppgifter), bland annat om ändamålen med behandlingen.[7]

---

[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] Artikel 29-arbetsgruppen, 2012. Yttrande 04/2012 om undantag från krav på samtycke till kakor (*cookies*)
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_sv.pdf

[4] ”Tredjeparter” enligt definitionen i skäl 66 i direktiv 2009/136/EG.

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

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

[7] Detta ska inte förhindra eventuell teknisk lagring eller åtkomst endast för att överföra meddelanden via ett elektroniskt kommunikationsnät, eller lagring eller åtkomst som är absolut nödvändig för att en leverantör av samhällsomfattande tjänster ska kunna tillhandahålla en tjänst som uttryckligen efterfrågas av abonnenten eller användaren.

I sitt yttrande 04/2012 behandlade arbetsgruppen artikel 5.3 i direktivet om integritet och elektronisk kommunikation i förhållande till lagring av eller tillgång till information genom användning av kakor. I yttrandet anser arbetsgruppen att artikel 5.3 inte enbart gäller kakor, utan även är tillämplig på ”liknande tekniska lösningar”.

I detta yttrande behandlas de allt fler rapporterna om att tredjeparter aktivt utforskar alternativa tekniker till kakor för en rad olika ändamål i syfte att kringgå samtyckeskravet i artikel 5.3. Tekniken att kombinera en uppsättning informationselement för att unikt identifiera vissa enheter eller appar, s.k. digitala fingeravtryck, ägnas särskild uppmärksamhet.

Digitala fingeravtryck kan också utgöra personuppgifter. De berörda bestämmelserna i direktivet om skydd av personuppgifter analyseras inte i yttrandet, men arbetsgruppen hänvisar till uppgiftsskyddsfrågor som är särskilt relevanta i samband med digitala fingeravtryck. Ett exempel är när flera informationselement kombineras, särskilt unika identifierare som IP-adresser, och ändamålet för behandlingen är att identifiera användare över tiden via webbplatser, vilket är fallet med beteendestyrd annonsering. I sådana fall måste behandlingen även uppfylla bestämmelserna i direktivet om skydd av personuppgifter.

Tekniken för digitala fingeravtryck begränsas inte till konfigurationsparametrarna hos en traditionell webbläsare på en stationär persondator. Digitala fingeravtryck är inte heller knutna till ett visst protokoll, utan kan användas för att ta fingeravtryck av många olika internetanslutna enheter, konsumentelektronik och appar, bland annat appar för mobila enheter, smart-tv, spelkonsoler, e-böcker, webbradio, system i bilar eller smarta mätare.[8]

3. Definition

RFC6973[9] definierar fingeravtryck som ”en uppsättning informationselement som identifierar en enhet eller en app”. Denna term används i bred bemärkelse i detta yttrande, vilket innebär att den omfattar uppgiftsuppsättningar som kan användas för att särskilja[10], länka[11] eller identifiera[12] en användare, en användaragent (UA) eller en enhet över tiden. Detta omfattar, men är inte begränsat till, uppgifter från

(a) konfiguration av en användaragent/enhet, eller

(b) uppgifter som exponeras genom användning av nätverkskommunikationsprotokoll.

[8] Kallas ibland ”sakernas internet”.

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

[10] *Särskiljbarhet*, som motsvarar möjligheten att isolera en del eller alla poster som identifierar en enskild person i datasetet, yttrande 05/2014 om avidentifieringsmetoder, s. 11–12.

[11] *Länkbarhet*, som är förmågan att länka samman åtminstone två poster för samma registrerad eller en grupp av registrerade (antingen i samma databas eller i två olika databaser). Om en angripare kan fastställa (t.ex. genom korrelationsanalys) att två poster hänför sig till en och samma grupp av enskilda personer, men inte kan särskilja enskilda personer i denna grupp, ger metoden skydd mot särskiljbarhet men inte mot länkbarhet, yttrande 05/2014 om avidentifieringsmetoder, s. 11–12.

[12] *Inferens*, som är möjligheten att med signifikant sannolikhet sluta sig till värdet av ett attribut från värdet av en rad andra attribut, yttrande 05/2014 om avidentifieringsmetoder, s. 11–12.

Många olika typer av uppgifter kan bilda ett fingeravtryck, bland annat följande exempel:

(a) CSS-information.

(b) JavaScript-objekt (t.ex. dokument, fönster, skärm, webbläsare, datum och språk).

(c) HTTP-headerinformation (t.ex. mängden information (bits) i UA-strängen, HTTP-headerns order, HTTP-headerns variation per typ av begäran).

(d) Klockinformation (t.ex. ”clock skew” och klockfel).

(e) Variation i TCP-stacken.

(f) Installerade typsnitt.

(g) installerad insticksinformation (t.ex. konfigurations- och versionsinformation).[13]

(h) Detta sker antingen genom användning av interna programgränssnitt[14] (API) som exponeras av användaragenten/enheten, eller

(i) genom det externa programgränssnittets webbtjänster som användaragenten/enheten kommunicerar med.

4. Teknisk bakgrund

Internet och webben har utvecklats utifrån behovet av en motståndskraftig och öppen arkitektur i nätverksmiljön i fråga.[15] Styrda av designval för att tillgodose dessa behov sänder enheterna informationselement. Ett antal protokoll innehåller en uppsättning obligatoriska och frivilliga informationselement. HTTP/1.1[16]-protokollet anger exempelvis header-fält, där servern och klienten kan inbegripa kompletterande upplysningar om hypertexten. Vissa av dessa är särskilt avsedda för att servern ska känna igen klienttyper. Headerfältet UA-begäran innehåller t.ex. följande beskrivning: ”Detta är för statistiska ändamål, för spårning av protokollöverträdelser och automatisk igenkänning av användaragenter i syfte att anpassa svaren för att undvika begränsningar av användaragenter.”

Vanliga användningsområden för UA-strängar är att optimera innehållets layout för en viss typ av enhet, använda informationen för att rikta innehåll mot specifika användare[17], eller samla in uppgifter om enheten för säkerhets- eller analysändamål.

---

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

[14] Genom att programgränssnittet erbjuder en användarvänlig ram för åtkomst till funktioner eller rutiner inom en programvarukomponent.

[15] Kahn, 1972. *Communications Principles for Operating Systems*. Internal BBN memorandum.

[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. Risker för uppgiftsskyddet

En individuell HTTP-header har vanligtvis ett icke-unikt värde, och användarna kan sällan identifieras individuellt bara med informationselementet.[18] De mediatyper som stöds av en webbläsare är t.ex. ofta desamma bland många andra användare som använder samma webbläsarversion. När de behandlas separat medför dessa icke-unika informationselement oftast inga risker för uppgiftsskyddet.

Ett antal informationselement kan dock kombineras för att ge en datauppsättning som är tillräckligt unik (särskilt när den kombineras med andra identifierare, t.ex. den ursprungliga IP-adressen) för att fungera som ett unikt digitalt fingeravtryck för enheten eller appen. Sådana fingertryck gör det möjligt att skilja en enhet från en annan och kan användas som ett dolt alternativ för kakor som spårar internetbeteende över tiden.[19] [20] [21]Som en följd av detta kan individen kopplas till och därför identifieras eller göras identifierbar av detta digitala fingeravtryck.

De risker för uppgiftsskyddet som uppstår i och med digitala fingeravtryck ökar med tanke på att den unika uppsättningen med uppgifter inte bara finns tillgänglig för webbplatsutgivaren, utan även för många andra tredjeparter. Detta strider mot policyn om *samma ursprung* för HTTP-kakor och förvärras dessutom till följd av webbens tekniska natur, där många tredjeparter bidrar till innehållet på webbsidan.

Det är vanligt att en webbplats skapas dynamiskt i realtid genom att begära innehåll från ett antal olika källor. Var och en av dessa resurser kommer att generera egna HTTP-begäran, och ladda ned bilder, JavaScript och CCS-filer. Många webbplatser innehåller dessutom insticksprogram och spårningsskript. De kan också utfärda en HTTP-begäran som registrerar när användaren skrollar eller klickar på en sida, en bild eller en annons. Tredjeparter har därför ofta möjlighet att samla in den information som behövs för att göra ett digitalt fingeravtryck av användarens enhet.

Riskerna för uppgiftsskyddet begränsas inte till spårning utförd av tredjeparter. Kombinationen av de uppgifter som fås genom programgränssnitt i programvaran i kundens enhet utgör också en risk för att enheten avger ett digitalt fingeravtryck. Olika programvaror, plattformar och programgränssnitt ger åtkomst till olika informationselement som lagras i enheten. Webbläsaren JavaScripts programgränssnitt kan t.ex. ge uppgifter om skärmstorlek, färgdjup och tillgängliga systemteckensnitt. Andra programgränssnitt kan begära åtkomst till informationselement som är lagrade i maskinvaran (t.ex. CPU-typ), operativsystem (t.ex. OS-typ) eller grafikkortsmodell.[22] Samtal till programgränssnittet kan också visa installerade programvaror (t.ex. webbanslutningar) eller till och

[18] Det finns fall där ett enda informationselement bär information som unikt kan identifiera en registrerad, t.ex. en OAuth-åtkomstmodul.

[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

med exakta versionsnummer. Tillgång till sådana informationsuppsättningar ökar antalet informationsdelar (entropi) och därmed risken för igenkänning av unika individer via deras enheter.[23]

I motsats till HTTP-kakor kan digitala fingeravtryck fungera i det dolda.[24] Det finns inga enkla sätt för användarna att förhindra denna aktivitet och möjligheterna att återställa eller ändra informationselement som används för att skapa fingeravtrycket är begränsade. Detta innebär att digitala fingeravtryck kan användas av tredjeparter för att i hemlighet identifiera eller särskilja användare med målet att rikta särskilt innehåll till dem eller behandla dem annorlunda på andra sätt.

I yttrande 16/2011[25]konstateras att reklamföretag har hävdat att användningen av unika koder eller andra värden inte medför behandling av personuppgifter. Detta strider mot ändamålet med behandling för att leverera personligt innehåll och personliga annonser, dvs. att kommunicera direkt med en viss person. Arbetsgruppen har ofta hävdat att sådana unika identifierare anses utgöra personuppgifter.[26]

6. Rättslig ram

När ett fingeravtryck skapas genom lagring av eller tillgång till information som finns lagrad i användarens terminalutrustning är direktivet om integritet elektronisk kommunikation tillämpligt.

Såsom anges i yttrande 04/2012 får behandling enligt artikel 5.3 undantas från samtyckeskravet om den uppfyller något av följande kriterier:

KRITERIUM A: teknisk lagring eller åtkomst ”endast […] för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät”.

KRITERIUM B: teknisk lagring eller åtkomst som är ”absolut nödvändig för att en leverantör av samhällsomfattande tjänster ska kunna tillhandahålla en tjänst som uttryckligen efterfrågas av abonnenten eller användaren”.

Dessutom måste webbleverantören respektera det definierade ändamålet med eventuella andra signaler som anger användarens preferenser i detta avseende, t.ex. ”spåra inte”[27]-listrubriken.[28]

---

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

[24]Endast i begränsade fall kräver protokollet en signal till användaren, som lokaliseringsuppgifter via HTML5:s programgränssnitt. Se: http://www.w3.org/TR/geolocation-API/#privacy_for_uas.

[25] Artikel 29-arbetsgruppen, 2014. Yttrande 16/2011 om EASA/IAB:s rekommendationer om bästa metoder vid beteendestyrd annonsering på internet. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_sv.pdf

[26] Artikel 29-arbetsgruppen, 2014. [26] Yttrande 05/2014 om avidentifieringsmetoder, s. 11–12, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_sv.pdf

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

[28] Protokollet med önskemål om att inte spåras (*Do Not Track protocol*) kan, under vissa omständigheter, utgöra en mekanism för detaljerat samtycke i linje med skäl 66 i direktiv 2009/136/EG, där det anges att användare kan ge sitt samtycke via sina webbläsarinställningar, men endast om samtycket uppfyller ovannämnda krav för giltigt samtycke. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

Tillämpningen av direktivet om skydd av personuppgifter omfattas inte av detta yttrande, men det bör noteras att när digitala fingeravtryck utgör behandling av personuppgifter är det viktigt att detta görs enligt varje relevant bestämmelse i direktivet.

Enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation måste alla parter som har för avsikt att lagra eller få åtkomst till information som är lagrad i användarens terminalutrustning inhämta användarens samtycke, även om informationen i det skedet inte anses utgöra personuppgifter. Artikel 29-arbetsgruppen har diskuterat samtycke i ett antal yttranden, både i allmänna termer[29] och med särskild hänsyn till beteendebaserad reklam.[30] Arbetsgruppen har också diskuterat kravet på samtycke inom ramen för artikel 5.3 och kakor.[31]

I detta sammanhang hänvisar arbetsgruppen till yttrande 02/2013 om appar på smarta enheter[32], där den konstaterade följande:

”Det är viktigt att notera skillnaden mellan det samtycke som krävs för att lägga in och läsa information från enheten och det samtycke som krävs för att ha en rättslig grund för behandling av olika typer av personuppgifter. Även om båda samtyckeskraven kan vara tillämpliga samtidigt […]. De två olika typerna av samtycke kan därför i praktiken förenas[…], förutsatt att användaren otvetydigt informeras om vad han eller hon samtycker till.”

I skäl 66 i direktivet om integritet och elektronisk kommunikation hänvisas till ”oberättigat intrång i privatlivet” och i artikel 5 behandlas kravet på konfidentialitet vid kommunikation. Genom artikel 5.3 kan informationssekretessen anses utvidgas till att omfatta de uppgifter som lagras på användarens enhet eller som enheten ger åtkomst till. All behandling från en tredje parts sida som påverkar enhetens beteende eller på annat sätt leder till att den lagrar eller ger åtkomst till uppgifter från enheten eller uppgifter som exponeras av enheten omfattas därför av artikel 5.3.

Orden ”uppgifter som lagras eller ges åtkomst till” anger att lagring och åtkomst inte behöver ske inom samma kommunikation och inte behöver utföras av samma part. Uppgifter som lagras av en part (inklusive uppgifter som lagras av användaren eller produkttillverkaren) och som en annan part senare får åtkomst till omfattas därför av artikel 5.3. Ett exempel är mobiltelefonappar som behandlar användarens kontaktlista. Användaren lagrar själv kontaktuppgifterna, men en tredje part får åtkomst till dem. Detta ska dock inte tolkas som att den tredje parten inte behöver samtycke för att få åtkomst till informationen bara för att den inte har lagrat uppgifterna. Samtyckeskravet gäller även när åtkomst ges till ett ”read-only”-värde (t.ex. en begäran om MAC-adressen för ett nätverksgränssnitt via OS API).

---

[29] Artikel 29-arbetsgruppen, 2011. Yttrande 15/2011 om definitionen av begreppet ”samtycke”. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_sv.pdf

[30] Artikel 29-arbetsgruppen, 2010. Yttrande 2/2010 om beteendebaserad reklam på Internet. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_sv.pdf

[31] Artikel 29-arbetsgruppen, 2013. Arbetsdokument 02/2013 om vägledning för inhämtande av samtycke för kakor (*cookies*). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[32] Artikel 29-arbetsgruppen, 2013. Yttrande 02/2013 om appar på smarta enheter, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_sv.pdf

Det är därför viktigt att tredjeparter är medvetna om att det krävs samtycke när digitala fingeravtryck kräver lagring av eller åtkomst till (en uppsättning) uppgifter på användarens enhet (om inte ett giltigt undantag är tillämpligt). Så är fortfarande fallet om vissa av dessa informationselement inte kräver lagring av eller åtkomst till information.

7. Användningsscenarier

7.1. Scenario: Webbanalyser utförda av förstaparter

Ett antal online-tjänster har föreslagit digitala fingeravtryck som ett alternativ till HTPP-kakor för att tillhandahålla analyser utan samtycke enligt artikel 5.3. I yttrande 04/2012 bekräftade arbetsgruppen behovet av ett tredje undantag från kravet på samtycke för webbanalyser av förstaparter:

”Om de är strikt begränsade till användning för aggregerad statistik för ”förstapartens” räkning och om de används av webbplatser som redan tillhandahåller dels tydlig information om dessa kakor i sina integritetsriktlinjer, dels lämpligt skydd för privatlivet. Sådant skydd förväntas omfatta dels en användarvänlig mekanism som gör det möjligt att välja bort all datainsamling, dels heltäckande anonymiseringsmekanismer som tillämpas på annan insamlad identifierbar information såsom IP-adresser.

I yttrandet påpekade arbetsgruppen dock att det för närvarande inte finns något undantag till samtycke för kakor som är strikt begränsade till anonymiserade och aggregerade statistiska ändamål för förstapartens räkning.[33] Webbanalyser för förstaparten via digitala fingeravtryck omfattas således inte av undantaget i kriterium A eller B och användarens samtycke krävs.

7.2. Scenario: Spårning för beteendestyrd annonsering på internet

Många webbplatser innehåller webbsignaler, pixeltaggar och JavaScript-kod från tredjeparter för att möjliggöra annonseringstjänster. Detta ger upphov till en rad förfrågningar om informationselement från användarens enhet. Förfrågningarna överförs till de tredjeparter som tillhandahåller annonseringstjänsterna och ger dem möjlighet att skapa ett digitalt fingeravtryck för att följa användaren runt webbplatser och över tiden. På så sätt kan de skapa en intresseprofil för riktad annonsering, även om användaren avböjer kakor. Sådan behandling kan tekniskt sett utföras i det dolda utan användarens vetskap.

I yttrande 04/2012 betonar arbetsgruppen att tredjepartsannonsering inte omfattas av undantaget i kriterium A eller B. Digitala fingeravtryck för riktad annonsering kräver därför användarens samtycke.

7.3. Scenario: Tillhandahållande av nätverk

För en korrekt hantering av nätverk krävs överföring av vissa informationselement till varje enhet i nätet. En wi-fi-åtkomstpunkt som styr anslutningen mellan trådlösa enheter och ett nätverk behandlar

[33] Artikel 29-arbetsgruppen, 2012. Yttrande 04/2012 om undantag från krav på samtycke till kakor (*cookies*), s. 10–11.

unika och icke-unika informationselement, t.ex. MAC-adress[34] och kanal, så att anslutningarna och datapaketens rutter fungerar korrekt.

Om det krävs informationselement som lagrar eller får åtkomst till information på användarens enhet för att tillhandahålla nätverket omfattas detta av artikel 5.3. Denna behandling är nödvändig för att nätverket ska fungera normalt, och undantas därför enligt kriterium A.

Sekundär användning av ett informationselement eller ett digitalt fingeravtryck för spårningsändamål omfattas inte av kravet ”endast för att överföra meddelanden via ett elektroniskt kommunikationsnät”, eller ”lagring eller åtkomst som är absolut nödvändig för att en leverantör av samhällsomfattande tjänster ska kunna tillhandahålla en tjänst som uttryckligen efterfrågas av abonnenten eller användaren”. När det gäller kakor med flera syften (*multipurpose cookies*) konstaterade arbetsgruppen i yttrande 04/2012 att ”det är mycket osannolikt att spårning skulle uppfylla kriterium A eller B”. En tredjepart som vill använda digitala fingeravtryck med flera syften bör således ”bara undantas från samtyckeskravet om alla olika syften […] är undantagna från samtyckeskravet”.

7.4. Scenario: Användarens åtkomst och kontroll

En online-tjänst kan vilja använda digitala fingeravtryck för att stödja användarnas åtkomst och kontroll (dvs. i kombination med ett användarnamn och ett lösenord). Digitala fingeravtryck kan användas för att säkerställa att ett konto är kopplat till en viss enhet så att enheten agerar som en andra autentiseringsfaktor.

Ett musikabonnemang tillåter t.ex. endast användaren att få åtkomst till tjänsten från ett begränsat antal specifika enheter. Om en användare har använt enheten tidigare, kan webbleverantören välja att utföra färre verifieringskontrollen innan åtkomst beviljas.

Om ett digitalt fingeravtryck består av informationselement som lagrar eller får åtkomst till information på användarens enhet för att tillhandahålla nätverket omfattas detta av artikel 5.3. Sådana ändamål skulle emellertid inte anses vara ”strikt nödvändiga” för att tillhandahålla de funktioner som uttryckligen efterfrågas av användaren, vilket i sin tur kräver giltigt samtycke från användarens sida.

Webbleverantörer kan behöva överväga en rad olika lämpliga och proportionella kontroller eller en annan autentiseringsmetod (t.ex. engångslösenord, sekundär e-post-bekräftelse).

7.5. Scenario: Användarcentrerad säkerhet

I yttrande 04/2012 konstaterade artikel 29-arbetsgruppen att ”kakor som utplacerats med det särskilda syftet att öka säkerheten hos den tjänst som uttryckligen begärts av användaren” (t.ex. att upptäcka upprepade misslyckade inloggningsförsök) kan omfattas av undantaget enligt kriterium B.

Detta undantag bör även omfatta digitala fingeravtryck, men precis som kakor, bör de ”inte omfatta användningen av kakor som har att göra med webbplatsers säkerhet eller tredjepartstjänster som inte uttryckligen begärts av användaren”.

Om uppgifter som samlas in via digitala fingeravtryck för ett användarcentrerat säkerhetssyfte får de inte användas för sekundära syften för att kunna omfattas av undantaget från samtycke. Tekniska och

[34] MAC-adressen är sannolikt unik för enheterna i nätverket. MAC-adressens prefix hänvisar också till chiptillverkaren.

organisatoriska säkerhetsåtgärder måste vidtas för att förebygga eventuell sekundär användning av uppgifter från digitala fingeravtryck, som vanligen finns i serverns säkerhetsloggar.

7.6. Scenario: Anpassa användargränssnittet till enheten

Tillgång till information om enheten, t.ex. skärmstorlek, kan vara användbar för att optimera innehållets utformning.[35] En mediawebbplats kan t.ex. gå över till en låg grafikinställning eller en layout med enda kolumn för mobila enheter. Alternativt kan en webbplats, eller de tredjeparter som levererar innehåll via den webbplatsen, skicka förfrågningar till enheten för att få information om teknisk kapacitet, t.ex. vilka videoformat som stöds.

Om en tredjepart begär åtkomst till information som lagras på användarens enhet endast för att anpassa innehållet till enhetens egenskaper, gäller kriterium B. Detta innebär att kortvarigt samtycke för UI-anpassning inte krävs.

Undantaget gäller emellertid inte om informationen även används för sekundära syften.

8. Slutsats

I detta yttrande behandlas digitala fingeravtryck och tillämpligheten av artikel 5.3 i direktiv 2002/58/EG om integritet och elektronisk kommunikation i dess ändrade lydelse enligt direktiv 2009/136/EG, utan att det påverkar bestämmelserna i direktiv 95/46/EG om skydd av personuppgifter. Yttrandet bygger vidare på arbetsgruppens tidigare yttrande 04/2012 om undantag från krav på samtycke till kakor (*cookies*) och bekräftar att tekniken, under ett antal omständigheter, leder till åtkomst till eller lagring av uppgifter på användarens terminalutrustning. Artikel 5.3 i direktivet om integritet och elektronisk kommunikation är således även tillämplig på vissa former av digitala fingeravtryck.

Parter som vill behandla digitala fingeravtryck som skapas genom åtkomst till eller lagring av uppgifter på användarens terminalutrustning måste därför först inhämta användarens giltiga samtycke (om inte undantag gäller).

[35] Observera att det kan finnas andra mindre integritetsinkräktande metoder för att uppnå samma mål, t.ex. UA-strängar.