GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

14/IT
WP 224

Parere 9/2014 sull'applicazione della direttiva 2002/58/CE al *device fingerprinting*

adottato il 25 novembre 2014

[NdT] Ai fini del presente parere, con “responsabile del trattamento” e con “incaricato del trattamento” si intendono rispettivamente il “titolare” e il “responsabile” di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della suddetta direttiva,

visto il proprio regolamento interno,

HA ADOTTATO IL PRESENTE PARERE:

Sintesi

Il *device fingerprinting* ("identificazione dei dispositivi") presenta gravi problemi connessi alla protezione dei dati per le persone. Ad esempio, vari servizi online hanno proposto il *device fingerprinting* in alternativa ai cookie HTTP allo scopo di fornire dati analitici o di effettuare un *tracking* senza dover richiedere il consenso ai sensi dell'articolo 5, paragrafo 3[1]. Ciò dimostra che i rischi connessi al *device fingerprinting* non sono solo teorici e dagli studi è emerso che esso viene già utilizzato[2].

Nel presente parere il Gruppo di lavoro "Articolo 29" (WP29) affronta gli argomenti del *device fingerprinting* e dell'applicabilità dell'articolo 5, paragrafo 3 della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, come modificata dalla direttiva 2009/136/CE, salvo quanto disposto dalla direttiva 95/46/CE sulla protezione dei dati. Il messaggio chiave del presente parere è che l'articolo 5, paragrafo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche è applicabile al *device fingerprinting*.

Il presente parere elabora ulteriormente il precedente parere 04/2012 relativo all'esenzione dal consenso per l'uso di cookie[3] e avverte i terzi[4] che elaborano *device fingerprint* generate attraverso l'accesso a informazioni o attraverso l'archiviazione di informazioni nelle apparecchiature terminali dell'utente che possono farlo solamente con il consenso valido dell'utente (salvo in caso di un'esenzione).

1. Introduzione

L'articolo 5, paragrafo 3 della direttiva 2002/58/CE come modificata dalla direttiva 2009/136/CE,[5] (direttiva relativa alla vita privata e alle comunicazioni elettroniche) stabilisce che gli Stati membri debbano assicurare che "*l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente*" siano consentiti unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso,

[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] Gruppo di lavoro "Articolo 29", 2012. Parere 04/2012 relativo all'esenzione dal consenso per l'uso di cookie.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_it.pdf

[4] "Terzo" come inteso al considerando 66 della direttiva 2009/136/CE.

[5] http://eur-lex.europa.eu/legal-content/EN-IT/TXT/?uri=CELEX:32009L0136&fromTab=ALL&from=it

dopo essere stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE[6] (direttiva sulla protezione dei dati), tra l'altro sugli scopi del trattamento[7].

Nel parere 04/2012, il WP29 ha esaminato l'articolo 5, paragrafo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche con riferimento all'archiviazione di informazioni oppure all'accesso a informazioni attraverso l'uso di cookie. Secondo il parere, l'articolo 5, paragrafo 3 non si applica esclusivamente ai cookie, bensì è applicabile anche a "*tecnologie simili*".

Il presente parere intende rispondere ad un numero crescente di segnalazioni secondo cui terzi stanno esplorando attivamente la possibilità di utilizzare tecnologie alternative ai cookie per vari scopi, per sottrarsi all'obbligo del consenso di cui all'articolo 5, paragrafo 3. In particolare, viene esaminata la combinazione di una serie di informazioni al fine di identificare in modo univoco particolari dispositivi o istanze applicative, il cosiddetto "*device fingerprinting*".

Le *device fingerprint* possono costituire anche dati personali. Il presente parere non fornisce un'analisi delle pertinenti disposizioni della direttiva sulla protezione dei dati, bensì tratta le questioni relative alla protezione dei dati che sono particolarmente importanti nel contesto del *device fingerprinting*. Quando vengono ad esempio combinate varie informazioni, in particolare identificativi unici quali gli indirizzi IP, e lo scopo del trattamento è di identificare gli utenti nel tempo, nei vari siti web, come con la pubblicità comportamentale, il trattamento deve rispettare anche le norme previste nella direttiva sulla protezione dei dati.

La tecnologia del *device fingerprinting* non si limita ai parametri di configurazione di un browser tradizionale su un PC da tavolo. Il *device fingerprinting* non è neanche vincolato ad un protocollo particolare, ma può essere utilizzato per raccogliere la *fingerprint* di una vasta gamma di dispositivi connessi ad Internet, apparecchi elettronici e applicazioni di consumo, comprese quelle utilizzate su dispositivi mobili, televisioni connesse, console per videogiochi, lettori di libri elettronici, Web radio, sistemi per auto o contatori intelligenti[8].

2. Definizione

La RFC6973[9] definisce una *fingerprint* come "*una serie di informazioni che identificano un dispositivo o un'istanza applicativa*". Nel presente parere il termine viene utilizzato in un senso ampio, ovvero includendo un insieme di informazioni che possono essere usate per individuare[10], correlare[11] o

[6] http://eur-lex.europa.eu/legal-content/EN-IT/TXT/?uri=CELEX:31995L0046&fromTab=ALL&from=IT

[7] Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio.

[8] Talvolta denominati "Internet degli oggetti" (*Internet of Things*).

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

[10] *Individuazione*: la possibilità di isolare alcuni o tutti i dati che identificano una persona all'interno dell'insieme di dati, parere 05/2014 sulle tecniche di anonimizzazione, pagg. 11-12.

dedurre[12] un utente, un programma utente (*user agent*) o un dispositivo nel tempo. Ciò include, senza limitarsi a questi, i dati provenienti da:

(a) configurazione di un programma utente/dispositivo; o

(b) dati esposti tramite l'uso di protocolli di comunicazione di rete.

Esistono molte tipologie di dati che possono formare una *fingerprint*, inclusi gli esempi seguenti:

(a) informazioni relative ai CSS (*Cascading Style Sheets*, fogli di stile a cascata);

(b) oggetti JavaScript (ad esempio documento, finestra, schermo, navigatore, data e lingua);

(c) informazioni relative all'intestazione HTTP (ad esempio, il numero di bit di informazioni nella stringa del programma utente, l'ordine delle intestazioni HTTP, variazione dell'intestazione HTTP a seconda del tipo di richiesta);

(d) informazioni relative al *clock* (ad esempio, sfasamento del *clock* (*clock skew*) e errore del *clock*);

(e) variazione dello *stack TCP*;

(f) caratteri installati;

(g) informazioni relative al *plugin* installato (ad esempio, informazioni sulla configurazione e sulla versione);[13]

(h) l'utilizzo di interfacce per programmi applicativi[14] (*Application Programming Interfaces*, API) interne esposte dal programma utente/dispositivo; o

(i) l'utilizzo di API esterne dei servizi web con cui sta comunicando il programma utente/dispositivo.

---

[11] *Correlabilità*: la possibilità di correlare almeno due dati concernenti la medesima persona interessata o un gruppo di persone interessate (nella medesima banca dati o in due diverse banche dati). Se un intruso riesce a determinare (ad esempio mediante un'analisi della correlazione) che due dati sono assegnati allo stesso gruppo di persone, ma non è in grado di identificare alcuna persona del gruppo, la tecnica fornisce una protezione contro l'individuazione, ma non contro la correlabilità, parere 05/2014 sulle tecniche di anonimizzazione, pagg. 11-12.

[12] *Deduzione*: la possibilità di desumere, con un alto grado di probabilità, il valore di un attributo dai valori di un insieme di altri attributi, parere 05/2014 sulle tecniche di anonimizzazione, pagg. 11-12.

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

[14] L'API offre un quadro di facile utilizzazione per accedere a funzioni o routine all'interno di un componente software.

3. Contesto tecnico

Internet e il web sono stati sviluppati tenendo conto delle esigenze di una rete con un'architettura resiliente e aperta[15]. A causa di scelte legate alla progettazione, prese per soddisfare tali esigenze, i dispositivi trasmettono informazioni. Molti protocolli includono una serie di informazioni obbligatorie e facoltative. Ad esempio, il protocollo HTTP/1.1[16] specifica i campi di intestazione che consentono al server e al client di includere informazioni aggiuntive riguardo all'ipertesto. Alcuni di questi sono stati specificamente destinati ai server per riconoscere i tipi di client. Ad esempio, il campo di intestazione User-Agent delle richieste include la descrizione: "*Ciò è a fini statistici, per la localizzazione di violazioni di protocollo e per il riconoscimento automatico di programmi utente, al fine di approntare risposte su misura per evitare particolari limitazioni del programma utente*".

Gli usi tipici della stringa User Agent includono l'ottimizzazione del layout del contenuto per un tipo particolare di dispositivo, l'uso di queste informazioni per adattare il contenuto a utenti specifici,[17] o la raccolta di informazioni sul dispositivo per finalità quali la sicurezza o l'analitica.

4. Rischi per la protezione dei dati

Dal momento che una singola intestazione HTTP normalmente ha un valore non univoco, raramente gli utenti possono essere identificati solo dalla singola informazione[18]. Ad esempio, le tipologie di media supportate da un browser sono spesso le stesse per molti altri utenti che utilizzano la stessa versione del browser. Pertanto, se trattate isolatamente, queste informazioni non univoche non presentano generalmente rischi per la protezione dei dati.

Tuttavia, varie informazioni possono essere combinate per fornire un insieme di informazioni che sia sufficientemente univoco (in particolare quando vengono combinate con altri identificativi quali gli indirizzi IP di origine) per fungere da *fingerprint* univoca del dispositivo e dell'istanza applicativa. Tale *fingerprint* offre la possibilità di distinguere un dispositivo da un altro e può essere utilizzata come alternativa "nascosta" per monitorare il comportamento su Internet nel tempo[19,20,21]. Di

---

[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

[18] Ci sono casi in cui una singola informazione fornisce ciò che serve per identificare in modo univoco un interessato, come un *token* di accesso 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

conseguenza, una persona può essere associata, e quindi identificata, o resa identificabile, da tale *fingerprint* del dispositivo.

I rischi per la protezione dei dati connessi al *device fingerprinting* sono aumentati dal fatto che l'insieme univoco di informazioni non è a disposizione solo del gestore del sito web, ma anche di molti altri terzi. Ciò è in contrasto con la *same origin policy* (regola della stessa origine) dei cookie HTTP e viene aggravato dalla natura tecnica del *world wide web*, in cui molti terzi contribuiscono al contenuto di una pagina web.

È una pratica comune che una singola pagina web venga generata dinamicamente in tempo reale, chiedendo contenuti a molteplici fonti. Ognuna di queste risorse creerà autonomamente richieste HTTP, scaricando immagini, file JavaScript e CSS. Molte pagine web contengono anche bachi invisibili (*web bugs*) e script di monitoraggio. Esse possono anche inviare richieste HTTP che registrano quando un utente scorre sulla pagina o clicca su di essa, su un'immagine o su una pubblicità. Pertanto, accade di frequente che terzi abbiano l'opportunità di raccogliere le informazioni necessarie per effettuare il *fingerprinting* del dispositivo dell'utente.

I rischi per la protezione dei dati non si limitano al monitoraggio da parte di terzi. Anche la combinazione di dati ottenuti attraverso interfacce per programmi applicativi (*Application Programming Interfaces*, API) presenti nel software dei dispositivi client comporta il rischio di *device fingerprinting*. Software, piattaforme e API differenti offrono accesso a informazioni diverse archiviate nel dispositivo. Il software di navigazione JavaScript API, ad esempio, può fornire informazioni relative alle dimensioni dello schermo, alla profondità del colore e ai font di sistema disponibili. Altre API possono richiedere l'accesso a informazioni archiviate nel firmware (ad esempio, il tipo di CPU), il sistema operativo (ad esempio, il tipo di SO) o il modello della scheda grafica[22]. Le chiamate API possono anche rivelare la presenza di software installati (ad esempio i plug-in del browser), o addirittura i numeri precisi di versione. L'accesso a tali serie di informazioni aumenta il numero di bit di informazioni (entropia) e quindi il rischio di riconoscimento dei singoli individui attraverso i loro dispositivi[23].

A differenza dei cookie HTTP, il *device fingerprinting* può agire di nascosto[24]. Non vi è alcuno strumento semplice che consenta agli utenti di prevenire tale attività e vi sono limitate possibilità di reimpostare o modificare eventuali informazioni utilizzate per generare la *fingerprint*. Di conseguenza, le *device fingerprint* possono essere utilizzate da terzi per identificare o individuare di nascosto gli utenti per offrire contenuti mirati oppure per trattarli in modo diverso.

Nel parere 16/2011[25] è stato rilevato che, secondo quanto affermato dalle agenzie pubblicitarie, l'uso di codici o di altri valori univoci non comporta il trattamento di dati personali. Ciò è in contraddizione

[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

[24] Solo in casi specifici, il protocollo richiede che venga dato un segnale all'utente, ad esempio la specifica delle API HTML5 di geolocalizzazione. Si veda: http://www.w3.org/TR/geolocation-API/#privacy_for_uas.

[25] Gruppo di lavoro "Articolo 29", 2014. Parere 16/2011 relativo alla raccomandazione dell'EASA/IAB sulle buone prassi in materia di pubblicità comportamentale online. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_it.pdf

con la finalità del trattamento che è la fornitura di contenuti e pubblicità personalizzati, ossia la comunicazione diretta con una persona specifica. Il Gruppo di lavoro ha sostenuto in diverse occasioni che tali identificativi unici sono qualificabili come dati personali[26].

5. Contesto giuridico

Quando una *fingerprint* viene generata attraverso l'archiviazione di informazioni o l'accesso a informazioni archiviate nelle apparecchiature terminali dell'utente, si applica la direttiva relativa alla vita privata e alle comunicazioni elettroniche.

Come illustrato nel parere 04/2012, l'articolo 5, paragrafo 3, prevede l'esenzione del trattamento dall'obbligo del consenso se viene soddisfatto uno dei criteri seguenti:

CRITERIO A: archiviazione tecnica o accesso "*al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica*".

CRITERIO B: archiviazione tecnica o accesso che è "*strettamente necessaria[/o] al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio*".

Inoltre, il gestore del sito web deve rispettare il significato stabilito di ogni altro segnale che indichi la preferenza dell'utente in merito, quale l'intestazione Do Not Track[27,28].

Sebbene l'applicazione della direttiva sulla protezione dei dati esuli dal presente parere, qualora il *device fingerprinting* costituisca un trattamento di dati personali, è importante che esso sia effettuato conformemente alle disposizioni pertinenti di tale direttiva.

L'articolo 5, paragrafo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche stabilisce l'obbligo del consenso dell'utente per qualsiasi soggetto che intenda archiviare o accedere a informazioni archiviate nelle apparecchiature terminali dell'utente, anche se tali informazioni non vengono ancora considerate come dati personali. Il WP29 ha trattato il consenso in vari pareri, sia a livello generale[29] che nello specifico, per quanto riguarda la pubblicità comportamentale online[30]. Il

---

[26] Gruppo di lavoro "Articolo 29", 2014. Parere 05/2014 sulle tecniche di anonimizzazione, pagg. 11-12. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf

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

[28] Il protocollo Do Not Track può potenzialmente diventare, in determinate circostanze, un meccanismo di consenso granulare in linea con il considerando 66 della direttiva 2009/136/CE. Tale considerando prevede che gli utenti possano esprimere il consenso mediante l'uso delle impostazioni del motore di ricerca (browser), ma solo se il consenso è conforme ai requisiti di validità summenzionati. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

[29] Gruppo di lavoro "Articolo 29", 2011. Parere 15/2011 sulla definizione di consenso. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_it.pdf

Gruppo di lavoro ha anche trattato l'obbligo del consenso nel contesto dell'articolo 5, paragrafo 3 e dei cookie[31].

Vale la pena di richiamare il parere 02/2013 sulle applicazioni per dispositivi intelligenti[32] che ha evidenziato:

"la distinzione tra il consenso richiesto per inserire o consultare informazioni nel dispositivo e il consenso necessario per legittimare il trattamento di diversi tipi di dati personali. Benché i due requisiti siano applicabili simultaneamente […] i due tipi di consenso si possono fondere nella pratica, […], purché l'utente sia reso consapevole in modo inequivocabile di quello a cui acconsente."

Il considerando 66 della direttiva relativa alla vita privata e alle comunicazioni elettroniche fa riferimento a "*un'intrusione ingiustificata nella sfera privata*" e l'articolo 5 riguarda il requisito per la riservatezza nelle comunicazioni. L'articolo 5, paragrafo 3 può essere visto come un'estensione della riservatezza delle informazioni a quelle sottoposte ad archiviazione o ad accesso nel dispositivo dell'utente. Pertanto, qualsiasi trattamento effettuato da terzi che influenzi il comportamento di tale dispositivo o che altrimenti faccia in modo che esso archivi informazioni o consenta l'accesso alle informazioni su tale dispositivo, o esposto da tale dispositivo, rientra nell'ambito di applicazione dell'articolo 5, paragrafo 3.

L'uso delle parole "*sottoposte ad archiviazione o ad accesso*" indica che non è necessario che l'archiviazione e l'accesso avvengano nell'ambito della stessa comunicazione o che siano effettuate dallo stesso soggetto. Le informazioni che vengono archiviate da un soggetto (comprese le informazioni archiviate dall'utente o dal fabbricante del dispositivo) alle quali successivamente accede un altro soggetto rientrano quindi nel campo d'applicazione dell'articolo 5, paragrafo 3. Un esempio è costituito da un'applicazione per telefono cellulare che sottopone a trattamento l'elenco dei contatti in cui le coordinate dei contatti sono state archiviate dall'utente stesso ma l'accesso viene effettuato dal terzo. Non è corretto interpretare ciò nel senso che il terzo non necessiti del consenso per accedere a tali informazioni semplicemente perché non le ha archiviate. L'obbligo del consenso si applica anche quando si accede a un valore di sola lettura (ad esempio, richiedendo l'indirizzo MAC di un'interfaccia di rete attraverso l'API del sistema operativo).

Pertanto per un terzo è importante tenere a mente che quando il *device fingerprinting* richiede l'archiviazione o l'accesso a (una serie di) informazioni sul dispositivo dell'utente, allora sarà necessario il consenso (a meno che non sia applicabile una valida esenzione). La situazione rimane tale anche se alcune di quelle informazioni non richiedono l'archiviazione di informazioni oppure l'accesso a informazioni.

---

[30] Gruppo di lavoro "Articolo 29", 2010. Parere 2/2010 sulla pubblicità comportamentale online. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_it.pdf

[31] Gruppo di lavoro "Articolo 29", 2013. Working Document 02/2013 providing guidance on obtaining consent for cookies (Documento di lavoro 02/2013 che fornisce orientamenti sull'ottenimento del consenso per i cookie). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[32] Gruppo di lavoro "Articolo 29", 2013. Parere 02/2013 sulle applicazioni per dispositivi intelligenti. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_it.pdf

6. Scenari relativi all'impiego

6.1. Caso di impiego: analitica di prima parte di siti web

Vari servizi online propongono il *device fingerprinting* in alternativa ai cookie HTTP allo scopo di fornire dati analitici senza dover richiedere il consenso ai sensi dell'articolo 5, paragrafo 3. Nel parere 04/2012 il Gruppo di lavoro ha riconosciuto la necessità di una terza esenzione dall'obbligo del consenso per l'analitica di prima parte:

"*[purché siano] strettamente limitati alle finalità statistiche aggregate di prima parte e se sono utilizzati da siti web che già forniscono chiare informazioni circa questi cookie nella propria politica in materia di riservatezza nonché tutele adeguate al riguardo. Fra tali tutele dovrebbero rientrare un meccanismo di facile utilizzo per scegliere di essere esclusi da qualsiasi raccolta di dati nonché meccanismi di completa anonimizzazione applicati alla raccolta di altre informazioni identificabili, come gli indirizzi IP.*"

Tuttavia, il parere affermava altresì che attualmente non vi è alcuna esenzione dal consenso per i cookie strettamente limitati a finalità statistiche aggregate e anonime di prima parte[33]. Pertanto, l'analitica di prima parte di siti web attraverso il *device fingerprinting* non è contemplata nell'esenzione definita nel CRITERIO A o B ed è richiesto il consenso dell'utente.

6.2. Caso di impiego: monitoraggio per la pubblicità comportamentale online

Molti siti web includono bachi invisibili, *pixel tag* e codici JavaScript di terzi per permettere la pubblicità. Ne deriva un numero elevato di richieste di informazioni dal dispositivo dell'utente. Le richieste vengono trasmesse ai terzi che effettuano i servizi pubblicitari e permettono loro di generare una *device fingerprint* per seguire gli utenti nei vari siti web e nel tempo e creare un profilo di interessi per la pubblicità mirata, anche se l'utente rifiuta i cookie. Tale trattamento, sotto il profilo tecnico, può essere effettuato di nascosto, all'insaputa dell'utente.

Nel parere 04/2012 è stato sottolineato che la pubblicità di terzi non è contemplata nell'esenzione definita nel CRITERIO A o B. Pertanto, il *device fingerprinting* ai fini della pubblicità mirata è soggetto al consenso dell'utente.

6.3. Caso di impiego: fornitura della rete

La corretta gestione di una rete richiede il trasferimento di certe informazioni relative ad ogni dispositivo presente nella rete. Ad esempio, un punto di accesso Wi-Fi che gestisce la connessione tra dispositivi senza fili e una rete cablata elaborerà informazioni univoche e non univoche, quali l'indirizzo MAC[34] e il canale, al fine di mantenere le connessioni e indirizzare i pacchetti di dati in modo corretto.

[33] Gruppo di lavoro "Articolo 29", 2012. Parere 04/2012 relativo all'esenzione dal consenso per l'uso di cookie, pagg. 10-11.

[34] È probabile che l'indirizzo MAC sia unico tra tutti i dispositivi sulla rete. Il prefisso dell'indirizzo MAC farà anche riferimento al fabbricante del chip.

Qualora la fornitura della rete richieda informazioni che archiviano o accedono a informazioni sul dispositivo dell'utente, allora essa rientra nel campo di applicazione dell'articolo 5, paragrafo 3. Qualora tale trattamento sia necessario per il normale funzionamento della rete, allora esso sarà esente ai sensi del CRITERIO A.

L'uso secondario di un'informazione o di una *device fingerprint* ai fini del monitoraggio non è considerato come "*al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica*" o "*strettamente necessari[o] al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio*". Con riferimento ai cookie multiscopo, nel parere 04/2012, il WP29 ha sottolineato che "*è molto improbabile che la seconda funzionalità [ovvero il monitoraggio] soddisfi il CRITERIO A o B"*, quindi se un terzo intende utilizzare una *device fingerprint* per finalità multiple, esso sarà "*esente dal consenso solo qualora tutte le distinte finalità […], prese singolarmente, siano esenti dal consenso*".

6.4. Caso di impiego: accesso e controllo dell'utente

Un servizio online può voler utilizzare il *device fingerprinting* per gestire l'accesso ed effettuare il controllo dell'utente (ossia in combinazione con un nome utente e una password). La *device fingerprint* può essere utilizzata per assicurarsi che un account sia collegato a un particolare dispositivo, in modo tale che il dispositivo agisca come un secondo fattore di identificazione.

Ad esempio, un servizio di abbonamento musicale permette all'utente di accedere al servizio solo da un numero limitato di dispositivi specifici. Se un utente ha usato tale dispositivo in precedenza, il gestore del sito web può decidere di effettuare un numero inferiore di verifiche prima di fornire l'accesso.

Qualora una *device fingerprint* sia costituita da informazioni che archiviano o accedono a informazioni sul dispositivo dell'utente, allora essa rientra nel campo di applicazione dell'articolo 5, paragrafo 3. Tali finalità, tuttavia, non sarebbero considerate come "*strettamente necessarie"* per offrire una funzionalità esplicitamente richiesta dall'utente e pertanto è richiesto il consenso valido dell'utente.

I gestori dei siti web possono aver bisogno di prendere in considerazione una serie di misure di controllo adeguate e proporzionate o eventuali altri metodi di autenticazione (ad esempio, una password monouso, la conferma dell'indirizzo e-mail secondario).

6.5. Caso di impiego: sicurezza incentrata sugli utenti

Nel parere 04/2012, il WP29 ha affermato che i "*cookie predisposti allo scopo specifico di accrescere la sicurezza del servizio esplicitamente richiesto dall'utente"* (ad esempio, per individuare ripetuti tentativi falliti di login) sarebbero esenti ai sensi del CRITERIO B.

Tale esenzione si applicherebbe anche al *device fingerprinting* ma, come per i cookie, "*non […] riguarderebbe però l'impiego [della tecnica] relativ[a] alla sicurezza di siti web o di servizi di terzi che non sono stati richiesti esplicitamente dall'utente.*"

Se vengono raccolti dati attraverso il *device fingerprinting* per uno scopo legato alla sicurezza incentrata sugli utenti, per beneficiare dell'esenzione essi non possono essere utilizzati per alcun fine secondario. Devono essere adottate misure tecniche e organizzative di salvaguardia per impedire eventuali usi secondari di dati da *fingerprinting*, solitamente conservati nei *log* di sicurezza dei server.

6.6. Caso di impiego: adattamento dell'interfaccia utente al dispositivo

L'accesso a informazioni del dispositivo quali le dimensioni dello schermo può essere utile per ottimizzare il layout del contenuto[35]. Ad esempio, un sito web di media potrebbe passare alla modalità a grafica ridotta o al layout a singola colonna per i dispositivi mobili. In alternativa, un sito web, o i terzi che forniscono contenuti attraverso tale sito web, potrebbero interrogare il dispositivo per verificarne le capacità tecniche, quali i formati video supportati.

Qualora terzi richiedano l'accesso a informazioni archiviate nel dispositivo dell'utente al solo scopo di adattare il contenuto alle caratteristiche del dispositivo, allora il CRITERIO B è valido. Ciò significa che per la personalizzazione dell'interfaccia utente a breve termine non è richiesto il consenso.

Se tuttavia tali informazioni vengono utilizzate per fini secondari, questa esenzione cessa di essere applicabile.

7. Conclusione

Il presente parere tratta gli argomenti del *device fingerprinting* e dell'applicabilità dell'articolo 5, paragrafo 3 della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, come modificata dalla direttiva 2009/136/CE, salvo quanto disposto dalla direttiva 95/46/CE sulla protezione dei dati. Il presente parere elabora ulteriormente il precedente parere 04/2012 relativo all'esenzione dal consenso per l'uso di cookie e conferma che, in diverse circostanze, la tecnologia comporta l'accesso a informazioni oppure l'archiviazione di informazioni nelle apparecchiature terminali dell'utente. Pertanto, l'articolo 5, paragrafo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche si applica ai casi di *device fingerprinting*.

Dunque, le parti che intendono elaborare i dati contenuti nelle *device fingerprint* generate attraverso l'accesso a informazioni o attraverso l'archiviazione di informazioni nelle apparecchiature terminali dell'utente devono ottenere preventivamente il consenso valido dell'utente (salvo in caso di un'esenzione).

[35] Si precisa che ci possono essere altri metodi meno invasivi della vita privata per raggiungere lo stesso obiettivo, ad esempio utilizzare la stringa User Agent.