Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Le regole dei Garanti privacy UE sulla raccolta a scopo di identificazione dei dati dei dispositivi ("*device fingerprinting*"): il Parere 25 Novembre 2014, n. 9.

di:
Prof. Avv. Alessandro del Ninno
Studio Legale Tonucci & Partners
adelninno@tonucci.com

Indice

---

§ 1. Introduzione: cenni sulle tecniche di "*device fingerprinting*" e i rischi per la privacy degli utenti.

Lo scorso 25 Novembre 2014 il cosiddetto "Gruppo ex art. 29" (che, proprio in base a quanto disposto dall'art. 29 della Direttiva UE sulla tutela dei dati personali n. 46/95, riunisce tutte le Autorità privacy nazionali degli Stati Membri) ha emanato un importante parere ("*Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*") relativo alle misure di tutela degli utenti avverso l'utilizzo di tecniche cosiddette di "*device fingerprinting*", atte ad identificare i dispositivi ed i loro utilizzatori mediante raccolta di dati tecnici e tracciatura del dispositivo connesso a Internet.

Il "*device fingerprint*" (letteralmente "*impronta digitale del dispositivo*") o *machine fingerprint* o *browser fingerprint* è una tecnica di raccolta di informazioni da e su un dispositivo connesso al web (PC, smartphone, tablet, etc) a scopo di identificazione (del dispositivo e dell'utente che lo utilizza).

Più in dettaglio, mediante il *device fingerprint* l'utente può essere monitorato attraverso la tracciatura e raccolta di dati tecnici e proprietà del suo dispositivo connesso a Internet (la raccolta dei dati tecnici – comunque identificativi ai sensi delle vigenti normative privacy UE – può spaziare dalla dimensione dello schermo, alle

versioni di *software* e *plug-in* installati, alla lista dei caratteri installati dall'utente - misurando l'altezza e la larghezza di stringhe stampate segretamente sulla pagina – alle configurazioni TCP/IP, alle informazioni tratte dall'orologio del dispositivo, al sistema operativo utilizzato, alle impostazioni delle connessioni *wireless*, fino all'indirizzo IP originale dell'utente).

Esistono due diverse modalità di operatività di tale tecnica: il *passive fingerprinting* (quello più rischioso per la privacy dell'utente inconsapevole) e *l'active fingerprinting*, che si basa sul fatto che l'utente si aspetta e tollera un certo grado di tracciamento, che avviene mediante istallazione direttamente sul dispositivo e da remoto di codice eseguibile che può accedere ad attributi come il *MAC address* (cioè lo speciale identificativo univoco che ciascun produttore hardware assegna ad ogni scheda di rete, sia ethernet che wireless, immessa sul mercato) o altri numeri seriali univoci dell'hardware del dispositivo.

La tecnica del *device fingerprinting* è stata in questi anni oggetto di approfonditi studi condotti da Università, gruppi di ricerca e associazioni a tutela della privacy. Ad esempio, in base ad un rapporto del 2013 dell'Università *Ku Leuven-iMinds,* si è scoperto che 145 tra i siti più importanti di Internet (oltre che 16 tra i più grandi *provider* del web) monitorano in tal modo gli utenti senza il loro consenso.

Un gruppo di ricerca presso lo *Stanford Security Laboratory* ha invece scoperto una serie di vulnerabilità nella struttura sensoriale dei più comuni *smartphone* sul mercato che permetterebbe l'archiviazione di identificativi unici attraverso strumenti interni come accelerometro, altoparlanti e microfono (il movimento del comune accelerometro può difatti rappresentare una impronta lasciata da un singolo dispositivo connesso al *web*, con un meccanismo di tracciamento molto simile a quello basato sui *cookies*).

Infine, già nel 2010, uno studio della *Electronic Frontier Foundation* (Eff) aveva evidenziato che il *device fingerprinting* non colpisce solo *Flash*, il diffusissimo *plug-in* utilizzato per la riproduzione di animazioni, video e audio (consentendo la raccolta dell'IP), ma anche *Java Script*, un linguaggio di programmazione molto comune tra le applicazioni web (e dunque anche i device della Apple, su cui notoriamente non "girà" *Flash*).

La tecnica di *device fingerprinting*, che è stata icasticamente definita come il "*rastrellamento delle cosiddette impronte digitali lasciate dai singoli dispositivi per la navigazione online*" è altamente rischiosa per la privacy degli utenti/proprietari dei dispositivi tracciati per i seguenti motivi (tra gli altri):

1. il monitoraggio e la tracciatura del dispositivo (e dell'utilizzo che ne fa l'utente) avvengono – come detto - senza consenso e senza che l'utente ne sia consapevole;
2. il *device fingeprint* è una tecnica di tracciatura più insidiosa dei *cookies* poiché – a differenza di questi ultimi – è in grado di operare anche se i *cookies* sono totalmente disattivati (difatti tale tecnica rientra – dal punto di vista dell'Informatica – nella macro-categoria cosiddetta dei "*super-cookies*"); tanto è vero che in un interessante articolo pubblicato di recente sulla rivista *Forbes* e intitolato "*La morte dei cookies*" è stato evidenziato come le tecniche di *device fingerprinting* si stanno imponendo – in alternativa ai *cookies* e in modo sempre più sofisticato - come strumento utilizzato dalle Agenzie per la Sicurezza Nazionale di USA e di altri Paesi (ve detto, comunque, che tale tecnica è utilizzata anche per combattere i furti di identità digitale e le frodi su carte di credito);
3. il *device fingerprinting*, aspetto ancor più insidioso, può operare anche aggirando il *Do Not Track HTTP*, cioè lo strumento con cui gli utenti del *web* dichiarano esplicitamente di non voler essere monitorati attivando la relativa impostazione del *browser*.

§ 2. Il Parere 9/2014 del Gruppo dei Garanti privacy UE: le misure a tutela degli utenti contro le tecniche di *device fingerprinting*. L'obbligo del consenso preventivo.

Il Gruppo dei Garanti privacy UE parte dal presupposto che i citati studi e ricerche dimostrino come i rischi per la privacy degli utenti legati all'impiego del *fingerprinting* siano tutt'altro che teorici, visto l'ormai diffuso sfruttamento di tali tecniche nel modo ICT. In tale prospettiva, le Autorità privacy – ampliando l'ambito di applicabilità del precedente Parere 4/2012 sui *cookies* – ritengono applicabile al *fingerprinting* l'articolo 5, paragrafo 3, della direttiva 2002/58/CE, come modificato dalla direttiva 2009/136/CE (sulla tutela della privacy nelle reti di comunicazione elettronica), che ha rafforzato la tutela degli utenti di reti e servizi di comunicazione elettronica introducendo l'obbligo del consenso informato prima dell'archiviazione di informazioni o dell'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente (o dell'abbonato). E tale obbligo si applica a tutte le tipologie di informazioni sottoposte ad archiviazione o ad accesso nell'apparecchiatura terminale dell'utente e sebbene il dibattito (almeno all'epoca della redazione del Parere 4/2012 citato) si sia incentrato principalmente sull'impiego dei *cookies*, non si deve intendere tale termine in senso esclusivo rispetto a tecnologie simili.

Quindi sostanzialmente, il presupposto – e la conclusione – del Parere 9/2014 dei Garanti UE è che terze parti che raccolgono dati dell'utente mediante *device fingerprinting* sono soggette al medesimo obbligo di raccolta preventiva del consenso

degli interessati così come previsto per i titolari del trattamento di dati mediante monitoraggio e profilazione attuata mediante *cookies* (a meno che non ricorrano i casi di esenzione dall'obbligo del consenso, come nel caso dei cosiddetti *cookies tecnici*, cioè quelli utilizzati "*al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica*" o "*strettamente necessari al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio*").

Che la raccolta di informazioni tecniche attuata mediante *fingerprinting* rappresenti un vero e proprio trattamento di dati personali (e che le informazioni tecniche in quanto tali siano "dati personali") come definito dalle applicabili Direttive sulla protezione dei dati (la 96/45 e la 2002/58) è confermato dal Parere in esame: inoltre, l'incrocio di numerosi parametri tecnici (come identificatori univoci o indirizzi IP) e la finalità di identificare – anche in maniera permanente nel tempo – le connessioni dell'utente (per esempio anche a fini di pubblicità comportamentale) rappresentano per i Garanti UE un trattamento che pienamente ricade nelle tutele previste dalla legge. E ciò a maggior ragione considerando il fatto che altrettanto numerosi sono i dispositivi che possono essere soggetti al *fingerprinting*: non solo PC, *smartphone*, tablet e altri dispositivi mobili, ma anche smart TV, consolle di giochi connesse in rete, lettori di e-book, web radio o navigatori per le auto, solo per citare degli esempi.

I Garanti UE richiamano altresì un precedente – e interessante – Parere (*Opinion 2/2013 sulle impostazioni privacy delle app per smart devices*) in cui si specificava un principio che ritengono applicabile anche al *fingerprinting*: "*è importante notare 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, ciascuno in virtù di una diversa base giuridica, sono entrambi soggetti alla condizione che si tratti di una "manifestazione di volontà libera, specifica e informata" (ai sensi della definizione all'articolo 2, lettera h), della direttiva sulla protezione dei dati). Di conseguenza, i due tipi di consenso si possono fondere nella pratica, durante l'installazione o prima che l'applicazione cominci a raccogliere dati personali dal dispositivo, purché l'utente sia reso consapevole in modo inequivocabile di quello a cui acconsente*".

La conclusione è dunque quella di imporre ad ogni soggetto (incluse terze parti) che mediante *fingerprinting* archivia e/o accede a informazioni tecniche del dispositivo dell'utente di richiedere il consenso dell'interessato. I termini "archiviazione" e "accesso" – poi – vanno interpretati secondo i Garanti nel senso che non occorre che tali attività avvengano nell'ambito della medesima connessione o siano poste in essere dallo stesso soggetto: l'informazione archiviata da un certo soggetto (incluse le informazioni immagazzinate dall'utente o dal produttore del dispositivo) che sia successivamente oggetto di accesso ad opera di un altro (es: provider, gestore del sito

web, etc), ricadono ugualmente nell'obbligo di richiesta di consenso preventivo al trattamento.

§ 3. La regolamentazione dei diversi scenari: casi pratici.

Il Parere dei Garanti – fissato il principio legislativo generale del consenso preventivo dell'utente (salvi i casi di esenzione) alla operatività delle tecniche di *device fingerprinting* (incluso il divieto di rispettare l'eventuale impostazione del *Do Not Track http*) - si occupa di fornire una serie di scenari pratici atti e chiarire i casi di applicabilità al *fingerprinting* delle prescrizioni (ed esenzioni) già dettate per la operatività dei *cookies* nel Parere 4/2012 (a cui ha fatto seguito, per quel che riguarda il Garante privacy italiano, il Provvedimento generale *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014* che i titolari del trattamento dovranno implementare al massimo entro la data del 3 Giugno 2015).

Il primo caso esemplificativo è quello di utilizzo della tecnica di *device fingerprinting* come alternativa ai cookies per l'operatività dei servizi cosiddetti di *analytics* da parte del gestore di un sito web (c.d. "*prima parte*"). Come è noto l'analitica consiste in rilevazioni statistiche sulle visite ai siti web effettuate mediante strumenti che spesso si fondano su cookie (si pensi a *Google Analytics*, il servizio di statistiche più usato nel web, attualmente in uso presso circa il 57% dei 10.000 siti web più popolari e presso circa il 49,95% del primo milione di siti web). Tali strumenti sono utilizzati soprattutto dai proprietari di siti web per stimare il numero di visitatori unici, al fine di individuare le principali parole chiave per i motori di ricerca che portano a una pagina web oppure per individuare le problematiche di navigazione di un sito web. Gli strumenti analitici disponibili oggi utilizzano svariati modelli di raccolta e analisi dei dati, ciascuno dei quali presenta rischi differenti per la protezione dei dati.

Nel Parere 4/2012 sui cookies i Garanti europei avevano evidenziato che un sistema analitico utilizzato direttamente dal gestore di un sito web basato su cookie di tale "prima parte" presenta chiaramente rischi diversi rispetto al sistema analitico di terzi (basato su cookie di una "terza parte"). Inoltre, continuano i Garanti, "*i cookie analitici di prima parte non generano un rischio per la privacy quando sono strettamente limitati alle finalità statistiche aggregate del gestore del sito web 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, la conclusione dei Garanti è di segno opposto: non essendo è previsto un caso di esenzione dall'obbligo di richiedere il consenso dell'interessato anche se i cookies del gestore del sito web sono strettamente limitati a finalità statistiche

aggregate e anonime, è necessario ugualmente richiedere il consenso e dunque l'utilizzo in alternativa ai cookies della tecnica di *device fingerprinting* per le medesime finalità del trattamento ricade ugualmente nel medesimo obbligo di acquisizione del consenso preventivo dell'utente.

Il secondo caso preso in esame dai Garanti UE è quello dell'utilizzo delle tecniche di *device fingerprinting* per tracciare le abitudini comportamentali e di acquisto *on line* dell'utente al fine di tarare messaggi pubblicitari e di marketing (anche da parte di terzi che offrono i relativi servizi) nell'ottica della cosiddetta pubblicità comportamentale. Come già enfatizzato nel Parere 4/2012 sui cookies, l'utilizzo della tecnica di *device fingerprinting* per le medesime finalità di marketing e promozione pubblicitaria ricade ugualmente nel medesimo obbligo di acquisizione del consenso preventivo dell'utente.

Il terzo caso riguarda la gestione delle infrastrutture di rete. Partendo dal presupposto che la corretta gestione di una rete richiede la raccolta di determinate informazioni (univoche e non univoche) relative a ciascun dispositivo (es: il trattamento dell'indirizzo MAC da parte di un *access point wi-fi* per consentire e mantenere la connessione), il Parere in esame specifica che se tale trattamento (anche mediante *device fingerprinting*) è unicamente finalizzato a rendere possibile il normale funzionamento della rete, allora pur ricadendo in astratto nell'obbligo di richiesta del consenso dell'utente per l'accesso e l'archiviazione delle informazioni, troverà comunque applicazione – come per i cookies – la stessa ipotesi di esenzione dell'obbligo.

Se però le medesime informazioni raccolte "*al solo scopo di consentire la trasmissione di una comunicazione su una rete*" sono altresì utilizzate per fini di tracciatura "*secondari*" o "*multi-scopo*" (anche da terze parti) è conseguente che sarà necessario acquisire il consenso dell'interessato.

Il quarto caso pratico riguarda i servizi di controllo e identificazione preventiva di un utente che utilizza un servizio *on line*. Spesso i servizi *on line* utilizzano la tecnica del *fingerprinting* per controllare e identificare l'utente che quel servizio richiede (e spesso la tecnica opera in associazione con la richiesta di inserire le credenziali di autenticazione, come una *userd id* e una *password*). La tecnica di *device fingerprinting* può essere utilizzata per assicurare che un *account* sia legato a quel particolare dispositivo, determinandosi che lo stesso dispositivo diventa esso stesso un fattore di autenticazione. Ad esempio, l'abbonamento ad un servizio di download di contenuti consente di accedere al servizio solo da un limitato numero di specifici dispositivi registrati (si pensi al caso del servizio SKY Go, accessibile ad un massimo di due dispositivi). In casi del genere i Garanti europei ritengono che l'identificazione

dell'utente mediante *device fingerprinting* non sia "*strettamente necessaria*" per poter fornire il servizio, potendosi utilizzare metodi alternativi di identificazione dell'utente basati su una metodologia meno invasiva, come ad esempio l'utilizzo di una *one time password* o l'invio di una e-mail di conferma. Conseguentemente, la tecnica di *device fingerprinting* impiegata a tali scopi non può che basarsi sulla acquisizione obbligatoria di un valido consenso da parte dell'utente.

Il quinto caso pratico analizzato dai Garanti UE riguarda le finalità di potenziamento della sicurezza di un servizio richiesto esplicitamente dall'utente. Nel Parere 4/2012 sui cookies i Garanti avevano chiarito che l'esenzione dall'obbligo di richiedere il consenso può essere estesa ai cookies predisposti allo scopo specifico di accrescere la sicurezza di un servizio esplicitamente richiesto dall'utente, come nel caso di cookie utilizzati per individuare ripetuti tentativi falliti di login a un sito web, oppure di altri meccanismi analoghi studiati per proteggere il sistema di login dagli abusi.

Tale esenzione – nel Parere in esame - si applica anche alle tecniche di *device fingerprinting* che perseguono il medesimo scopo, anche se – come per i cookies – tornerà ad applicarsi l'obbligo del consenso se il loro impiego è relativo alla sicurezza di siti web o di servizi di terzi che non sono stati richiesti esplicitamente dall'utente. Inoltre, l'obbligo del consenso troverà applicazione se i dati raccolti mediante *fingerprinting* sono utilizzati per scopi secondari: sul punto il Parere richiede ai titolari del trattamento di predisporre idonee cautele tecniche ed organizzative atte a prevenire qualsiasi utilizzo secondario dei dati di *fingerprinting* (raccolti per i fini di sicurezza appena sopra spiegati), come ad esempio la loro conservazione sui server mediante log di sicurezza.

L'ultimo caso pratico preso in esame dai Garanti europei riguarda le finalità di adattamento dell'interfaccia utente al dispositivo. Accedere alle informazioni del dispositivo (come ad esempio al formato o alla dimensione dello schermo) può essere utile per ottimizzare il *layout* dei contenuti visualizzati. Per esempio, un sito web che offre contenuti media può cambiare l'impostazione di visualizzazione, utilizzando una risoluzione grafica più bassa o un *layou*t a colonna singola per i telefoni cellulari. In altri casi, un sito web può richiedere che il dispositivo sia dotato di determinate capacità tecniche per supportare – ad esempio – certi formati video. In questi e similari casi, l'accesso alle informazioni del dispositivo mediante *fingerprinting* per adattare il contento web richiesto alle caratteristiche del dispositivo è consentito senza obbligo di richiedere il consenso preventivo dell'utente. Ovviamente, l'obbligo del consenso troverà applicazione se i dati così raccolti mediante *fingerprinting* sono utilizzati per scopi secondari.