Andrea Folcio

Le nuove fondamenta del digital marketing

FrancoAngeli

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

La versione completa dell'e-book (a pagamento) è leggibile **con Adobe Digital Editions**.

Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta **cliccando qui** le nostre F.A.Q.

Am - La prima collana di management in Italia

Testi advanced, approfonditi e originali, sulle esperienze più innovative
in tutte le aree della consulenza manageriale,
organizzativa, strategica, di marketing, di comunicazione,
per la pubblica amministrazione, il non profit...

Andrea Folcio

Le nuove fondamenta del digital marketing

FrancoAngeli

Isbn: 9788835156192

Progetto grafico di copertina di Elena Pellegrini

Indice

Introduzione

Ho avuto la fortuna di nascere attorno alla metà degli anni '70, quando quella cosa strana che si chiamava internet ha cominciato a entrare di prepotenza nella nostra quotidianità diventando via via sempre più pervasiva, fino a modificare per sempre il nostro modo di accedere alle informazioni, di condividere esperienze, di interagire con gli amici e sicuramente di allargare i nostri orizzonti. Tutto è diventato più veloce, oggi siamo abituati a conoscere tutto di tutti in pochi secondi, a condividere le nostre esperienze in tutto il mondo e, ovviamente, a comprare prodotti e servizi senza doverci spostare dal luogo in cui siamo.

Ho scelto di trasformare la mia passione per le tecnologie in un lavoro – quello del digital marketer –, che da oscura professione pionieristica si è evoluto nel tempo, di pari passo con la nascita di nuove piattaforme che oggi ci abilitano all'interazione e alla pianificazione di campagne di comunicazione con obiettivi e caratteristiche anche molto differenziate.

Oggi diamo per scontata l'esistenza di Google e le sue piattaforme di marketing, Meta, Tiktok e i social media in generale, Amazon e l'ecommerce con la delivery di prodotti fisici a casa nostra in poche ore, Apple e i device che portiamo sempre in tasca; tuttavia, Google è nato nel 1998 ed è diventato un player rilevante solo a partire da metà degli anni 2000, l'origine di Facebook è del 2004, l'iPhone è stato presentato al mercato nel 2007. Osservando in retrospettiva gli sviluppi che hanno avuto le piattaforme di digital marketing, sembra incredibile come, nel giro di 15 anni, siamo passati dalla fase di Far West pionieristico a una serie di tool pervasivi, efficaci e con una scalabilità senza precedenti.

Il mercato pubblicitario digitale è cresciuto fino a superare gli investimenti in televisione anche nel nostro Paese, con un'espansione che non si è limitata a questi ambiti, ma si è estesa ad altri player come Salesforce. Tutto il mercato della marketing automation, dei big data analytics e delle piattaforme di loyalty che ci hanno fornito una conoscenza puntuale dei propri clienti,

permettendo di comunicare in maniera istantanea e personalizzata su larga scala, hanno realizzato la promessa del marketing *one-to-one* teorizzata già negli anni '90 del secolo scorso, ma solo ora realmente operativa e scalabile.

Tutte queste tecnologie hanno in comune un elemento fondante: per tracciare il comportamento degli utenti e trainare i propri algoritmi di AI e machine learning fanno affidamento su un piccolo strumento che è nato a metà degli anni '90, il cookie, che da allora si è evoluto molto poco, se paragonato a tutte le tecnologie che sono state costruite usandolo come elemento fondante.

Ecco che il momento della scomparsa dei cookie e della loro crescente incapacità di essere persistenti, cominciata negli scorsi anni e in rapida accelerazione, sta portando al nostro settore un cambiamento senza precedenti, tanto che per la prima volta, da anni, siamo costretti a porci il tema di come cambiare rapidamente il nostro approccio al marketing digitale per poter mantenere tutti i canali di interazione su cui abbiamo creato i nostri business plan, comprese le evoluzioni dei sistemi su cui stiamo lavorando per il futuro, come le televisioni connesse o il retail media.

Oggi una banale operazione come leggere le performance di un sito attraverso una piattaforma di web analytics, senza avere contezza di come sono raccolti i dati di navigazione degli utenti, vuol dire non conoscere la qualità del dato presentato e quindi avere una percezione distorta del proprio business digitale e dell'efficacia dei propri investimenti di marketing.

Questo tema è ancora più sentito per chi opera in ambiti di big data analytics o elabora informazioni per quanto riguarda le attività di acquisizione di clienti, profilazione e arricchimento degli stessi. Come dicono i tecnici, "g*arbage in – garbage out*": se non abbiamo contezza della qualità del dato in ingresso, non potremo fare affidamento sui risultati prodotti dalle analisi.

Benvenuti nell'era del digital marketing cookieless.

A chi è rivolto

Questo testo è pensato sia per tutti coloro che hanno a che fare con le tematiche del digital marketing in ambito lavorativo (professionisti che collaborano con agenzie di consulenza e servizi o con aziende), sia per gli studenti interessati a comprendere pienamente il perimetro su cui andranno ad operare quando entreranno nel mercato del lavoro.

L'intento è quello di presentare in maniera sistematica e organica le diverse tecnologie che compongono una moderna stack di digital e omnichannel marketing, per analizzare nel dettaglio gli impatti che la diminuzione di persistenza dei cookie attualmente in atto e il loro parziale deprecamento, previsto per il prossimo futuro, porteranno sui diversi casi d'uso.

Potremo ancora fare retargeting? Come potremo selezionare le audience per una campagna pubblicitaria? Come cambieranno le metodologie di analisi dei big data legati al digital marketing? Questi sono alcuni dei casi che saranno analizzati per capire come sono implementati in un contesto *cookie based* e come potranno essere gestiti nello scenario "*cookieless*".

Obiettivi e struttura del testo

Questo testo nasce con l'intento di fornire una visione approfondita su un tema che ha impatti su tutti gli aspetti della filiera del digital marketing e dell'omincanalità, per permettere di mettere a fuoco gli elementi sostanziali di questo cambiamento e infine proporre una serie di soluzioni organiche.

I primi tre capitoli, introduttivi, sono propedeutici al resto dell'opera: nel primo andremo a trattare come funzionano tecnicamente i cookie, nel secondo capitolo sarà presentata una panoramica sugli altri strumenti alla base del tracciamento degli utenti sui device mobili come smartphone o tablet.

Nel terzo capitolo saranno illustrate ad alto livello le tematiche legate alla privacy degli utenti e alla gestione dei dati, non tanto al fine di entrare nel dettaglio di ogni singola norma o delle interpretazioni di una materia che è in costante evoluzione e che necessita di un trattato dedicato e specifico da parte di legali e DPO, quanto di presentare i molteplici impatti che la tutela della privacy ha avuto nella gestione quotidiana delle aziende e di come essa sia uno degli elementi chiave della nascita del digital marketing cookieless. Per questo gli elementi maggiormente messi a fuoco saranno le intenzioni esplicite dei legislatori e i principali vincoli imposti alla gestione dei dati personali.

Nel quarto e nel quinto capitolo saranno introdotte le tipologie di dato e tutti gli elementi tecnologici che compongono la filiera del marketing digitale, perché la gestione di ogni singolo componente subirà impatti diversi nell'ecosistema cookieless; analizzando le diverse piattaforme, ci concentreremo sugli aspetti legati al digital marketing e ai big data analytics per il digital marketing, non andando ad approfondire invece tutti quegli aspetti, altrettanto interessanti ma non centrali per le finalità di questo testo, che coinvolgono i diversi aspetti della nostra esperienza da utenti.

Dal sesto capitolo si entrerà quindi nel dettaglio di come la perdita di efficacia nella raccolta e utilizzo delle informazioni stia deteriorando le performance delle attività di digital marketing, introducendo i temi della cookie apocalypse, per i diversi operatori del mercato: advertiser, publisher, strumenti di misurazione, tipologia di attività media.

Approfondiremo le soluzioni tecnologiche ad oggi disponibili per rispondere alle esigenze in ambiente cookieless e quelle che sono state proposte ma che non hanno ancora avuto modo di essere pienamente operative.

Infine, saranno proposte delle best practice trasversali e comuni a tutte le attività di chi opera in ambito digitale, per poi entrare nel dettaglio di alcune *use case*, per illustrare le soluzioni più idonee a rispondere alle singole esigenze.

1 Come funzionano i cookie

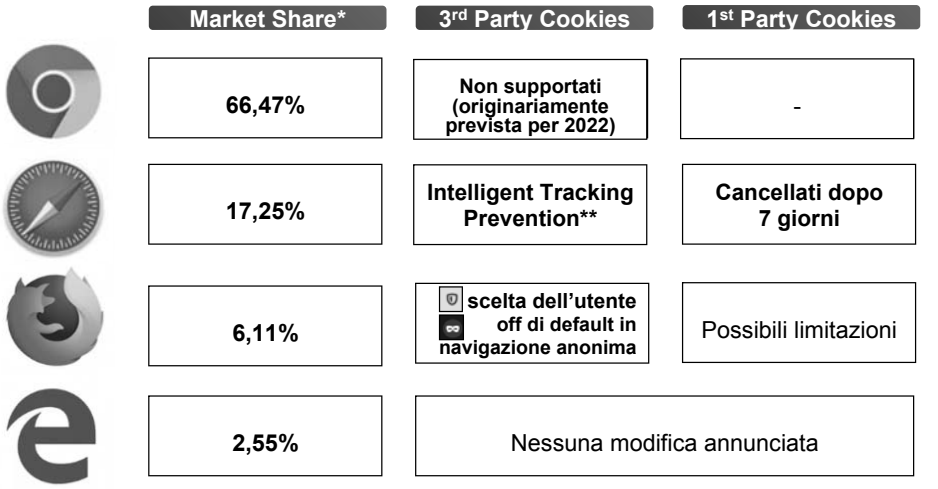
1. La nascita dei cookie

La prima volta che il termine "*cookie*" è comparso sulla scena digitale risale al lontano 1994, anno in cui Netscape (il più popolare browser dell'epoca) li implementò per permettere ai propri sistemi di riconoscere gli utenti che avevano già visitato le pagine del loro sito web.

A breve distanza di tempo anche Microsoft decise di adottare la stessa funzionalità all'interno del proprio browser Internet Explorer 2, dando definitivamente l'impulso all'uso di questa tecnologia per tutte le finalità di memorizzazione delle informazioni sugli utenti. La nascita dei cookie non è stata quindi decisa a tavolino da un consorzio (ad esempio il W3C che è oggi responsabile della definizione di diversi protocolli usati sul web) ma è stata **un'adozione spontanea da parte degli operatori di mercato** che ha definito le funzionalità direttamente sul campo, attraverso il loro utilizzo; ogni browser può arbitrariamente decidere di modificare la gestione dei cookie autonoma- mente, senza vincoli e senza dover sottostare a decisioni condivise con altri player. Un dettaglio, quest'ultimo, che sarà molto importante per capire l'at- tuale situazione legata alla cookie apocalypse.

I browser sono lo strumento che tutti noi usiamo per navigare all'interno del World Wide Web: i più diffusi oggi sono Chrome di Google, Firefox di Mozilla, Safari di Apple e Edge di Microsoft. Il loro compito è quello di gestire tutte le informazioni che servono per poter permettere agli utenti la fruizione dei contenuti sotto forma di testi, immagini, video. L'infrastruttura alla base di questo scambio di informazioni, come il protocollo HTTP (che si occupa di gestire la trasmissione delle informazioni sul web) o il linguaggio di markup HTML (che si occupa di formattare i contenuti delle pagine web), ha diverse eccezionali capacità, ma anche una grave lacuna: in termini in- formatici si definisce "stateless", ovvero privo di memoria rispetto a ciò che succede prima o dopo un determinato evento.

Fig. 1 – Diffusione dei browser



Fonte: Statcounter, settembre 2022, mercato Italia.

Mettiamoci nei panni di un comune cliente di una banca, che vuole accedere al proprio conto corrente online: arriva sul sito dell'istituto bancario, compila un semplice form, inserendo il proprio nome utente, password ed eventuali altri sistemi di sicurezza, clicca invio ed ecco che viene reindirizzato all'area privata in cui potrà visualizzare le proprie giacenze, operare sul conto o fare pagamenti. L'utente può muoversi liberamente all'interno dell'area privata, senza doversi preoccupare di essere riconosciuto dal sito della propria banca finché non chiuderà il browser o cliccherà sul pulsante di log out.

Senza cookie, tutto questo non potrebbe succedere: una volta arrivato sul sito e aver compilato il form, l'utente sarebbe poi costretto a reinserire le proprie informazioni ogni volta che intende passare da una pagina all'altra, rendendo un'operazione alquanto semplice una forma di moderna tortura.

Un secondo esempio può essere quello di un utente che vuole comprare un vestito sull'ecommerce del proprio stilista preferito: una volta scelto il prodotto e messo nel carrello, questo svanirebbe sia al semplice passaggio da una pagina all'altra del sito, sia qualora l'utente decidesse di completare l'acquisto, perché ad ogni cambio di pagina richiesto per l'inserimento delle informazioni di pagamento e spedizione, i dati inseriti non sarebbero più collegati alla stessa sessione di navigazione.

Ulteriori casi che ci capitano costantemente, senza che ce ne accorgiamo, sono legati alla personalizzazione della nostra esperienza di navigazione quando andiamo su un sito per scegliere dei biglietti aerei, un hotel o se vogliamo fare la spesa online; nei cookie sono salvate tutte le informazioni che consentono al dominio di riconoscere un browser e di personalizzare

di conseguenza l'esperienza di navigazione dell'utente che sta usando quel browser.

Questo è un primo concetto importante che molto spesso viene confuso: **un cookie non traccia un utente, un cookie traccia un browser**.

Se due utenti condividono lo stesso browser e non sono sotto login (dove viene esplicitata la loro diversità), verranno riconosciuti come un solo profilo collegato a quel determinato browser. Allo stesso modo, se su un device (ad esempio il mio computer portatile) ho più di un browser, in ciascuno di essi verrò riconosciuto per i miei comportamenti, ma in maniera separata. Esemplificando, nel momento in cui navigo sul mio sito di news preferito sia da Chrome che da Firefox, i due browser non potranno condividere tra loro alcuna informazione rispetto ai miei comportamenti e alle mie preferenze.

Il fatto che i cookie siano legati a doppio filo con il browser che li conserva è riconducibile all'epoca in cui sono stati tecnicamente definiti: nel 1994 il costo della memoria, sia RAM che quella basata su hard-disk, era estremamente alto e, per un gestore di siti web, mantenere una grande mole di informazioni sui propri server sarebbe stato molto oneroso; la scelta di salvare le informazioni di un determinato browser all'interno del browser stesso, memorizzando e archiviando piccole porzioni di informazioni direttamente sul computer dell'utente, permetteva di risparmiare risorse, di distribuire l'onere del mantenimento delle informazioni sui diversi computer e di lasciare all'utente la possibilità di gestire la cancellazione o il mantenimento di queste piccole stringhe di testo operando sulle impostazioni del proprio browser.

2. Tipologie di cookie

I cookie sono classificabili secondo diversi parametri. Per le nostre finalità, occorre approfondire due differenti metodologie di classificazione.

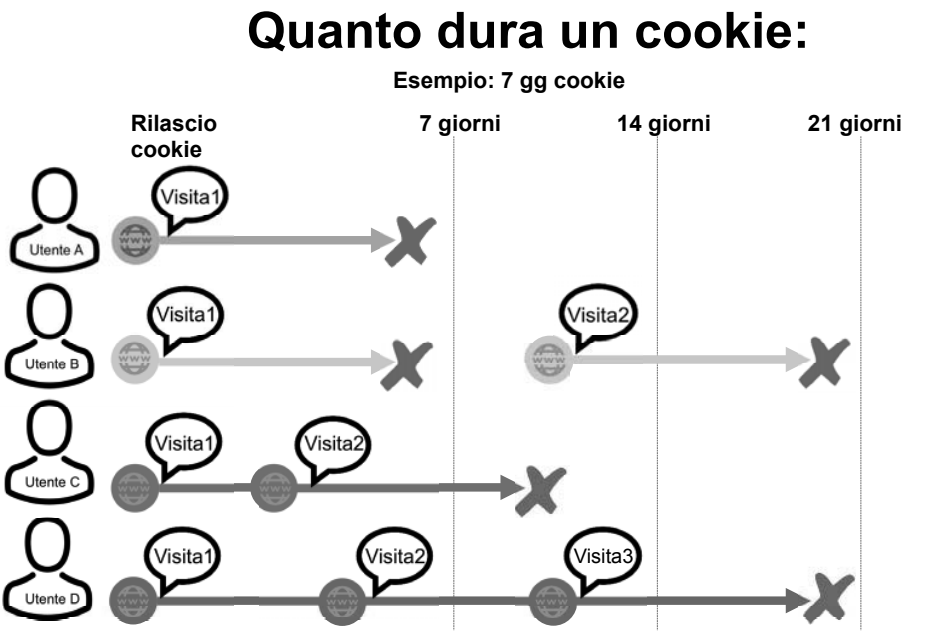
La prima suddivide i cookie in due grandi famiglie, i "*session cookie*" e "*persistent cookie*", mentre la seconda distingue tra cookie di prima e cookie di terza parte (o, anche, "*first party*" e "*third party*" cookies).

I *session cookie*, o cookie di sessione, hanno la caratteristica di non avere una data di scadenza perché restano in memoria solo fino a chiusura del browser; nel momento in cui il browser si chiude, i session cookies andranno persi per sempre. **Sono cookie utilizzati di solito per finalità tecniche**, per conservare le credenziali di accesso alla banca online o informazioni che devono servire solo per la durata della sessione di navigazione, come ad esempio l'accesso a informazioni sanitarie. Il motivo per cui le credenziali di accesso a un home banking sono tipiche di un cookie di sessione, a differenza dei login su siti informativi, ad esempio, è proprio legato alla necessità di avere la massima protezione possibile. Se così non fosse, un malintenzionato potrebbe accedere al nostro home banking semplicemente riaprendo un

browser su cui ci eravamo precedentemente loggati, accedendo a informazioni sensibili o svuotandoci il conto corrente.

Ai cookie persistenti viene invece assegnata una data di scadenza precisa nel momento in cui vengono creati; al raggiungimento di questa data il cookie verrà automaticamente cancellato dal sistema, senza alcuna necessità di intervento da parte dell'utente. Questi cookie sono utilizzati per conservare informazioni tipicamente legate alla profilazione e al comportamento degli utenti (come le sue preferenze o impostazioni per il sito e informazioni legate allo storico delle navigazioni) al fine di personalizzare le interfacce di navigazione, che traggono giovamento dal perdurare di queste informazioni nel tempo. Per i cookie persistenti è importante capire come funzioni l'impostazione della data di fine e come possa essere aggiornata automaticamente.

Fig. 2 – Esempio di durata di un cookie



Prendiamo l'esempio di un sito che utilizzi un cookie persistente che ha una durata di sette giorni, come rappresentato in figura 2.

L'utente A arriva sul sito, conclude la sua navigazione e nell'arco dei successivi sette giorni non accede nuovamente. Il cookie verrà automaticamente cancellato alla fine del periodo.

L'utente B arriva sul sito, come l'utente A conclude il suo percorso di navigazione e poi, per sette giorni, non effettua altre visite al sito, ma ci torna

solo dopo dieci giorni; in questo caso i nostri sistemi di tracciamento non potranno riconoscerlo, perché nel frattempo il cookie che tracciava il suo comportamento è stato cancellato. Risulterà quindi a tutti gli effetti come un nuovo utente, un nuovo cookie verrà impostato con durata di sette giorni e alla scadenza, se non ci saranno nel frattempo altre visite, verrà cancellato automaticamente dal sistema.

Nel caso dell'utente C, abbiamo invece una prima visita seguita da una seconda dopo quattro giorni, quindi entro la finestra dei sette giorni. In questo caso l'utente sarà riconosciuto, sapremo quindi che lo stesso utente è alla sua seconda visita ed eventuali informazioni immagazzinate nel cookie potranno essere utilizzate per personalizzare la sua navigazione. Questo caso ci consente di capire quello che succede alla data di scadenza del cookie: **la data di scadenza non sarà più quella originaria, cioè a sette giorni dalla prima creazione del cookie, ma sarà aggiornata a sette giorni dalla data della sua ultima visita**. Il periodo di vita di questo cookie sarà quindi pari alla somma dei sette giorni originariamente impostati, più i quattro giorni intercorsi fra le due visite.

Compreso lo schema, possiamo ipotizzare il comportamento del cookie per l'utente D, che è un visitatore abituale; passando dal nostro sito frequentemente, di volta in volta a una distanza inferiore ai sette giorni, il nostro utente continuerà per sempre ad essere tracciato con lo stesso cookie e continueremo a leggerlo sugli analytics come un singolo utente con una serie di visite cumulate nel tempo.

Alcuni cookie, quindi, hanno la capacità di durare molto più della loro data di scadenza originaria. Per diversi anni, dalla loro comparsa, i cookie hanno mediamente avuto vite molto lunghe, potendo così rappresentare una base per la lettura dei comportamenti degli utenti molto precisa ed efficace. Nel momento in cui i cookie cominciano ad avere durate brevi e cancellazioni frequenti, ecco che questa solidità viene meno e le osservazioni sul comportamento degli utenti risultano parziali.

3. Cookie di prima e terza parte

Un secondo modo di classificare i cookie prende in considerazione altre caratteristiche che sono importanti soprattutto per la gestione di alcuni casi d'uso, ad esempio tutti quelli legati al mondo della profilazione per campagne di advertising. Sia i cookie di prima che di terza parte utilizzati per queste finalità sono parte della famiglia dei persistent cookie e servono entrambi per la raccolta dei dati degli utenti; le modalità tecniche di raccolta e mantenimento sono molto simili, cambiano invece scopi e finalità.

I cookie di prima parte sono salvati direttamente dal sito (o meglio, dal dominio) che si sta visitando in quel preciso momento. Questi cookie permettono al titolare del sito di collezionare informazioni rispetto al comportamento dell'utente, potendo quindi abilitare diverse *use case*:

- leggere il comportamento degli utenti con strumenti di web analytics;
- gestire il funzionamento degli strumenti di ottimizzazione delle performance del sito;
- personalizzare l'esperienza dell'utente, modificando l'interfaccia in base alle caratteristiche di navigazione pregresse dell'utente (ad esempio, un cliente torna su un ecommerce e in home page trova un elenco dei prodotti che solitamente acquista).

I *third party cookie* sono invece creati da domini che non sono il sito su cui l'utente sta navigando.

Come può succedere questo? Semplicemente grazie a piccoli codici (tendenzialmente javascript o image pixel) è possibile per un dominio esterno richiamare attraverso uno script la scrittura di un proprio cookie.

I cookie di terza parte sono molto potenti perché consentono alle piattaforme digitali di riconoscere quel determinato utente anche quando naviga su diversi siti, non solo quando è presente sul proprio dominio.

Questa caratteristica è il motivo per cui i cookie di terza parte sono il pilastro su cui si è fondata l'industry del digital advertising; in questo specifico caso è importante poter riconoscere un utente non tanto quando è sul proprio sito, ma durante la sua navigazione sul web.

4. Chi può leggere un cookie

I cookie non sono universalmente accessibili perché **solo il dominio che ha scritto quello specifico cookie può accedere alle informazioni in esso contenute e andare a modificarle** a suo uso.

Questo dettaglio è particolarmente importante perché spesso si crede che con un solo cookie sia possibile leggere tutte le informazioni raccolte sulla propria navigazione, in relazione ad ogni sito visitato e per ogni interazione svolta: non è assolutamente così.

Per esemplificare, ipotizziamo che io apra un browser e vada sul sito A, che è un ecommerce di cibo per animali; navigo diverse pagine per guardare alcuni prodotti di mio interesse e poi clicco su un link che mi porta sul sito B, che tratta di sport. Anche in questo caso navigo diverse pagine

a tema calcio, prima di chiudere il browser e interrompere la mia sessione di navigazione.

In questo scenario gli strumenti di web analytics del sito A vedranno un utente che arriva da digitazione diretta del dominio, leggeranno la sessione di navigazione nelle sue diverse pagine e permetteranno di conseguenza la creazione di un profilo legato a quell'utente solo ed esclusivamente in base al contenuto delle pagine che sono state visitate su quello specifico sito. In questo caso possiamo quindi ipotizzare che l'utente verrà inserito in un cluster che lo classificherà come appassionato di animali domestici, specialmente gatti.

Leggendo i web analytics del secondo sito, lo stesso utente verrà riconosciuto invece come un appassionato di sport, nella fattispecie di calcio.

La vista di un agente esterno che collega entrambi i siti identificherebbe quell'utente come appartenente a 2 macro-cluster, quello degli appassionati di animali domestici (gatti) e di sport (calcio).

Nel caso di tracciamento con un cookie di prima parte, per il sito A le informazioni che sono state raccolte dalla navigazione del sito B non sono visibili; nessuna delle informazioni legate allo sport potrà essere utilizzata. Parimenti, per il sito B non saranno disponibili le informazioni raccolte dalla navigazione del sito A; in pratica ogni dominio potrà accedere solo alle informazioni che lui stesso ha scritto e non avrà accesso alle informazioni conservate nei cookie di prima parte scritti da altri domini.

Se nello stesso scenario la piattaforma avesse utilizzato un cookie di terza parte, avrebbe potuto comportarsi come l'agente esterno, andando quindi a leggere entrambi i patrimoni informativi e avere una visione più allargata delle caratteristiche dell'utente.

È comprensibile quindi come **i cookie di terza parte siano più potenti di quelli di prima parte, proprio per la loro capacità di rendere interoperabili informazioni da contesti diversi**; ciò non toglie che nella realtà dei fatti anche **un cookie di terza parte non potrà mai avere una vista globale di tutti i comportamenti di navigazione che un singolo utente opera**, perché resta il vincolo secondo cui, per tracciare un utente su una pagina, deve essere presente un codice di tracciamento che consenta di rilasciare il cookie: questo fa sì che non ci siano attualmente sul mercato network che abbiano un'estensione **globale totalitaria**.

Nel mercato pubblicitario online sono ovviamente premiati quegli operatori che hanno un'ampia e capillare diffusione, perché possono avere un punto di osservazione più esteso sugli utenti.

Diventa naturale osservare come su una singola pagina web possono essere rilasciati diversi cookie, sia di prima che di terza parte, proprio perché può essere conveniente consentire a diversi operatori di intercettare il sin-

golo utente, ed ogni operatore dovrà rilasciare un proprio cookie per poter tracciarlo.

Fig. 3 – Esempio del numero di cookie scaricati da una singola pagina, come riportato dalla console sviluppatori di Chrome

5. Anatomia di un cookie

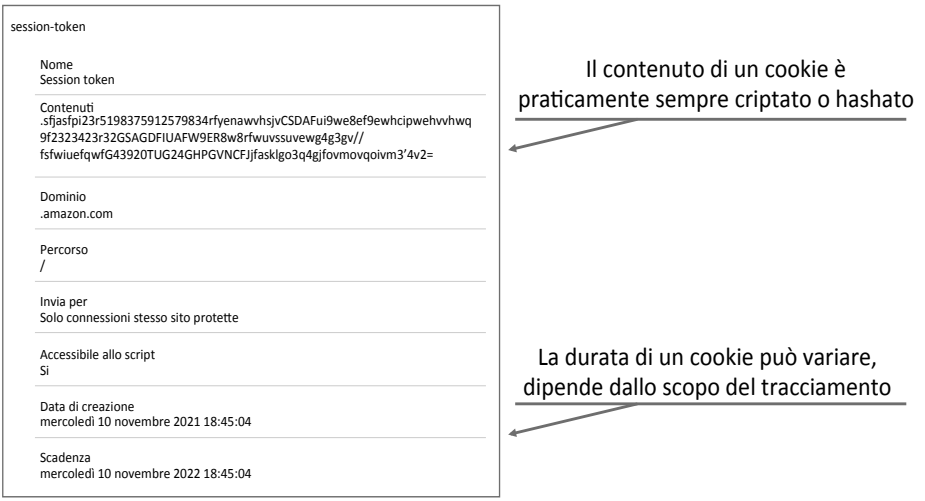
Prima di entrare nel merito della loro struttura, occorre premettere un concetto piuttosto essenziale: **i cookie non sono informazioni compiute, ma solo uno degli strumenti tecnici che ci consentono di raccogliere dati che dovranno poi essere elaborati e messi a disposizione delle piattaforme di target-ing e segmentazione, per poter essere azionati**.

Ognuno di noi può accedere ai cookie presenti sui nostri device esattamente come se fossimo l'operatore che li ha generati (su Chrome ad esempio chrome://settings/cookies).

Questo ci consente di analizzare come è fatto un cookie e che contenuti possono essere immagazzinati al loro interno.

Nell'immagine 4 è possibile identificare come amazon.com sia il dominio a cui appartiene questo cookie specifico, che è nominato come "*session-token*". Nonostante il nome, questo cookie è persistente, perché ha sia una data di creazione che una data di scadenza, in questo caso impostata a 12 mesi.

Fig. 4 – Scheda di un cookie all'interno della console di Chrome



Il motivo per cui Amazon utilizza un cookie di sessione di questa durata è molto probabilmente da imputarsi al fatto che vuole evitare che un normale utente si debba loggare nuovamente ogni volta che esplora il sito, per poter avere un'interfaccia personalizzata sulla base della propria esperienza di navigazione pregressa.

L'ultima parte che ci interessa analizzare è alla voce Contenuti, dove sono presenti le informazioni conservate dal cookie; in questo caso solo Amazon può accedere al dettaglio leggibile perché la stringa è stata opportunamente offuscata per impedire a terzi di leggere le informazioni conservate in questo cookie.

È diventata nel tempo buona prassi di programmazione fare in modo che le informazioni scambiate sul web vengano offuscate, per minimizzare il rischio di divulgazione di dati sensibili (*data leak*).

Un singolo dominio può decidere di utilizzare più di un cookie per salvare diverse tipologie di informazioni, ad esempio in figura 5 possiamo vedere come amazon.com utilizzi 9 cookie, diversi sia per durata che per finalità, con lo scopo di separare singoli elementi e rendere più facile la gestione delle informazioni conservate nel singolo cookie.

Un ultimo elemento da sottolineare è quello di come amazon.com e amazon.it siano da considerarsi in questo caso due domini completamente separati, con un proprio set di cookie completamente indipendenti gli uni dagli altri.

Questo non vuol dire che Amazon non possa collegare le informazioni raccolte dai due domini una volta che i dataset siano stati fatti confluire in un *data lake*, ad esempio, ma per quanto riguarda la gestione a livello di cookie restano completamente disgiunti.

Fig. 5 – Elenco di cookie presenti all'interno di un browser

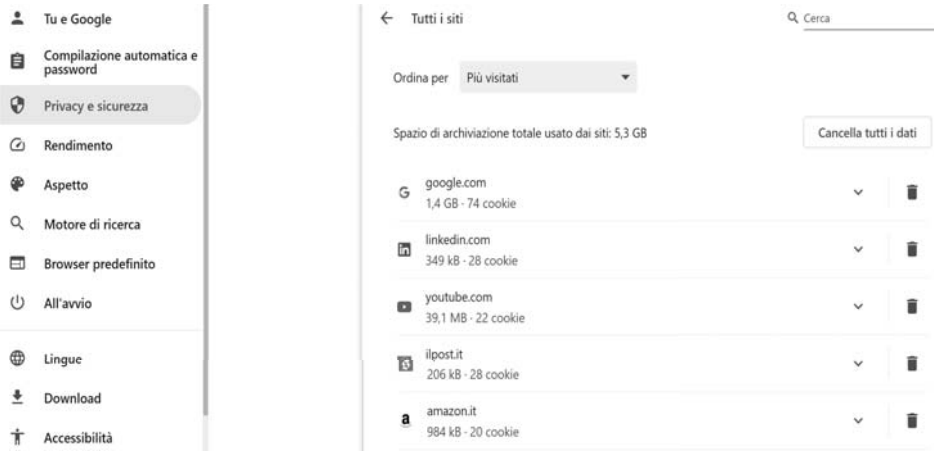
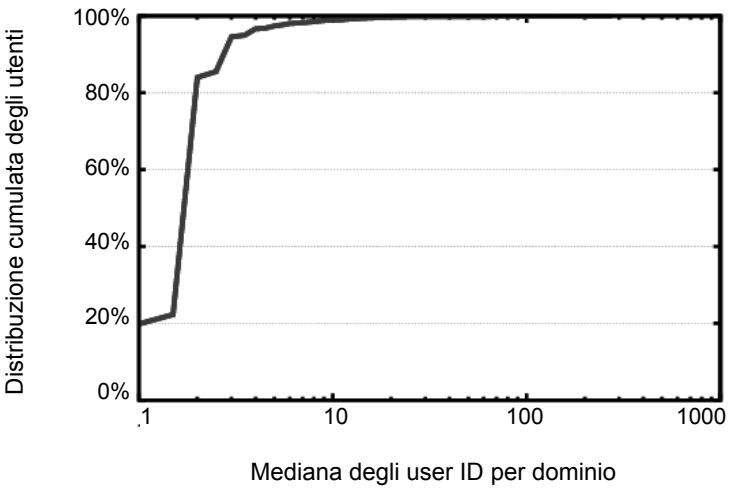


Fig. 6 – Numero di cookie per dominio per singolo utente



Fonte: Researchgate (https://www.researchgate.net/figure/Number-of-first-and-thirdparty-cookies-per-domain-per-user-We-see-that-the-median_fig2_325414165).

Si stima che il numero di cookie rilasciati da ogni singolo dominio per ciascun utente si attesti intorno ai 10 (sommando sia quelli di prima che di terza parte).

6. Gestione dei cookie in modalità navigazione anonima

Tutti i browser moderni presentano una modalità di navigazione definita "anonima": in pratica è possibile aprire una sessione di navigazione in una modalità separata da quella tradizionale, che differisce dal fatto che quello che avviene all'interno di questo ambiente di navigazione non viene condiviso con il resto delle informazioni raccolte e gestite dal browser in uso.

Questa tipologia di navigazione è molto utile in diverse operazioni, perché ci permette di operare in maniera semplice da uno stesso browser come se fossimo due utenti separati; per esempio, possiamo navigare uno stesso sito sia in versione riconosciuta, con tutte le personalizzazioni del caso, sia senza essere riconosciuti.

Per chi si occupa di web design, sviluppo siti o digital advertising, è uno dei modi semplici per testare il comportamento di un sito o di una campagna pubblicitaria sia quando l'utente è riconosciuto che quando è anonimo.

È importante specificare che questa modalità, per quanto definita "anonima", in realtà abbia ben poco di anonimo:

- durante la navigazione vengono rilasciati cookie esattamente come sulla navigazione principale;
- fintanto che la sessione è attiva, la cronologia dei siti visitati viene conservata;
- i siti possono tracciare gli utenti esattamente come sulla navigazione principale, anche se conservati in un ambiente separato, e non sono condivisi con i dati conservati sui cookie della navigazione principale.

La vera differenza della navigazione anonima sta nel fatto che, alla chiusura della sessione di navigazione, tutti i cookie (sia di prima che di terza parte) e tutti i dati relativi alla cronologia vengono cancellati e non sono più conservati sul proprio device.

È bene precisare che anche in questo caso non vuol dire che tutto quello che abbiamo fatto in modalità anonima è dimenticato una volta che il browser è stato chiuso, perché gli operatori telefonici che gestiscono il nostro traffico dati hanno avuto la possibilità di sapere cosa abbiamo visualizzato nel nostro percorso di navigazione, esattamente come nella modalità tradizionale.

Questo tipo di modalità è più una "soluzione di servizio" che una reale anonimizzazione della navigazione, e presenta delle limitazioni per alcuni utilizzi (come ad esempio il tracciamento degli utenti a scopo pubblicitario o la personalizzazione della loro esperienza di navigazione), dovute alla breve durata dei tracciamenti, che per un cookie in navigazione anonima è mediamente di pochi minuti.

7. Estensione nell'uso dei cookie

I cookie sono nati dalla necessità di conservare diversi tipi di informazione rispetto alla navigazione degli utenti e il fatto che sono ancora alla base del funzionamento di una moltitudine di strumenti digitali ci dimostra come, **in ambito informatico, uno strumento malleabile, per quanto vetusto, non venga quasi mai soppiantato a meno che non se ne presenti la necessità**. Le Smart TV, ultimo elemento connesso che è entrato nelle nostre case, utilizzano molto spesso un sistema operativo derivato dai più comuni browser (es.: Chromium), il cui sistema di tracciamento, sia tecnico che di profilazione, si basa anch'esso su cookie.

SUM-UP: come funzionano i cookie

Alla luce di quanto descritto in questo capitolo ci è chiaro, ora, che i cookie siano nati per degli scopi ben precisi e come il loro utilizzo sia stato di volta in volta piegato a casi d'uso per cui non erano stati pensati originariamente. Appare evidente come siano diventati uno strumento obsoleto per sostenere le attività di tracciamento e profilazione degli utenti alla luce delle necessità del digital marketing moderno.
Innanzitutto non sono uno strumento trasparente, perché il singolo utente può avere un minimo controllo su chi scarica un cookie sul proprio device, ma non ha consapevolezza di che tipo di informazioni vengano conservate e per quanto tempo.
I cookie di profilazione, inoltre, non tracciano persone, ma tracciano browser, e questo aspetto crea un disallineamento fra le prospettive di analisi dei dati e quanto invece viene effettivamente raccolto. Dal momento che non esiste un processo automatico di interscambio tra diverse tecnologie o domini, per poter condividere informazioni fra operatori di mercato è quindi necessario ricorrere a matching table.
Infine, i cookie hanno una durata variabile, sia perché gli operatori hanno la libertà di impostare autonomamente questo parametro, sia perché la durata può essere estesa in caso di nuovo riconoscimento nell'arco della finestra temporale attiva.
È evidente quindi che, con l'aumentata sensibilità sui temi di privacy e compliance alle norme GDPR, i cookie siano stati fra i primi "osservati speciali", soprattutto per quanto riguarda i cookie di terza parte; ma il contagio si sta già diffondendo anche ai cookie di prima parte, come vedremo nei prossimi capitoli.

---

2 Identificativi in ambito mobile

Nel precedente capitolo abbiamo visto come i cookie non siano uno strumento universale per il tracciamento degli utenti, ma abbiano invece un territorio ben circoscritto in cui operare: i browser.

A partire dall'introduzione di iPhone e degli app store, si è sviluppato un ecosistema parallelo per l'interazione fra utenti e device, che avviene all'interno di un'app e non all'interno di un browser: in questo caso la gestione del tracciamento degli utenti può basarsi su strumenti diversi dai cookie, che vanno sotto il nome di MAID.

MAID è l'acronimo di *Mobile Advertising IDentifier*, ed è lo strumento pensato e implementato nell'ecosistema dei dispositivi mobile che prevedono l'utilizzo di app, per permettere il riconoscimento degli utenti e abilitare tutte quelle casistiche che in ambito browser si basano sui cookie.

1. Browser e web view

Prima di addentrarci nella disamina degli identificativi specifici del mondo mobile, osserviamo come anche gli smartphone e i tablet siano provvisti di alcune app specifiche per la navigazione in ambito web, che altro non sono che una versione appositamente sviluppata dei browser che conosciamo per desktop e laptop.

Tutti i device con sistema operativo IOS hanno Safari come browser predefinito, così come Chrome è quello preinstallato in tutti i device con sistema operativo Android. In entrambi i casi, tuttavia, è possibile scaricare e utilizzare app per Firefox o qualsiasi altro browser alternativo.

Il tracciamento degli utenti all'interno di queste app-browser è del tutto simile a quello che abbiamo illustrato per i browser.

Più in generale, lo sviluppo di un'app può essere fatto utilizzando sia framework e linguaggi di programmazione nativi, sia una tecnologia ibrida

che consiste nell'avere l'equivalente di un sito web aperto all'interno dell'app stessa. Questa seconda soluzione, in gergo tecnico definita una "web view", non è nient'altro che l'apertura di una sessione browser all'interno dell'app, che riconduce tutta l'esperienza di interazione con l'app stessa all'equivalente della navigazione di un sito.

Anche in questo caso, gli elementi base del tracciamento degli utenti saranno i cookie, che però avranno vita solo all'interno dell'app stessa, con una durata più esigua e una capacità di interscambio con l'ecosistema esterno ancor più limitato.

2. Cos'è MAID

MAID è un identificativo univoco del device, che viene rilasciato direttamente dal sistema operativo ed è condiviso da tutte le app presenti sul device dell'utente. I dati che possono essere raccolti sono molto estesi, come ad esempio **informazioni sull'esatta posizione GPS** quando l'app è aperta (e in alcuni casi anche in background) o sulle altre app presenti sul dispositivo dell'utente.

MAID non ha data di scadenza ma può essere rinnovato, vale a dire che chiunque può sostituire il proprio MAID attuale con uno nuovo, attraverso una procedura semplice ma pressoché sconosciuta, dalle impostazioni di sistema del proprio smartphone.

Data la natura dei device su cui opera (principalmente smartphone e tablet), **MAID è molto più assimilabile a uno strumento di tracciamento di un singolo individuo rispetto a un cookie che invece, come abbiamo detto, traccia un browser e non l'intera navigazione effettuata da un dispositivo**.

Essendo generato dal sistema operativo, non sorprende che non esista un solo MAID, ma IOS e Android abbiano sviluppato due sistemi di tracciamento che, per quanto molto simili, sono al contempo specifici del proprio ambiente; in ambito Apple IOS l'identificativo si chiama IDFA (*Identifier For Advertising*) mentre in ambito Android AAID (*Android Advertising ID*) o GAID (*Google Advertising ID*).

Quando si fa genericamente riferimento a MAID, si dà per scontato che si parli di due sistemi di tracciamento diversi, separati in base al sistema operativo, che non vanno a condividere alcuna informazione fra i diversi ecosistemi.

Ad esempio, se si sta utilizzando un Google account per collegare il proprio smartphone ai servizi dell'ecosistema Google su un dispositivo Android, quel device sarà riconoscibile come AAID, ma non associabile ad alcun IDFA.

Già da questa descrizione, sintetica ma sufficientemente esaustiva ai fini della comprensione dei contenuti di questo testo, possiamo comprendere come MAID sia molto più pervasivo, persistente e "personale" di un cookie.

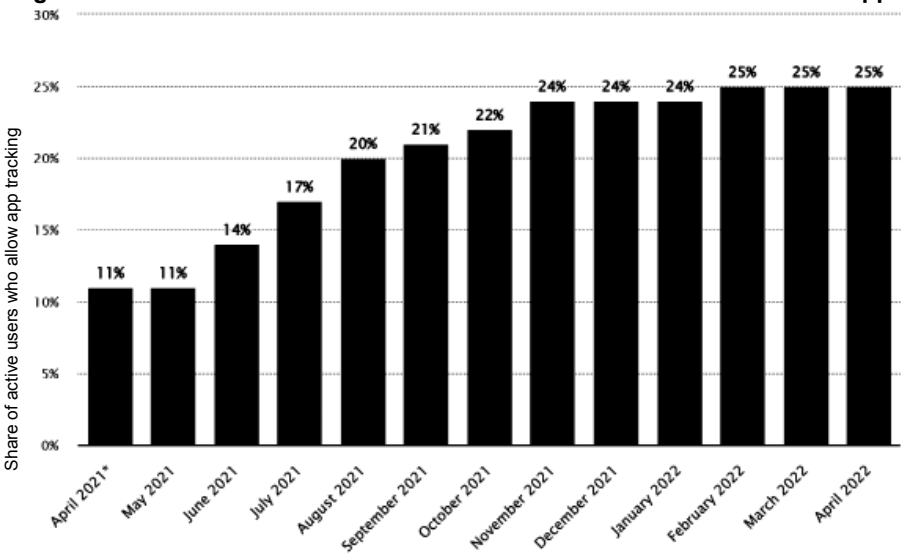
3. Apple App Tracking Transparency

Con il rilascio del sistema operativo IOS 14.5 nell'aprile 2021 Apple ha introdotto un'innovativa funzionalità chiamata App Tracking Transparency; ogni app presente sui device Apple, che permetta in qualche modo il tracciamento dati dei propri utenti, deve chiedere preventivamente il consenso all'utente stesso prima di procedere al tracciamento.

Quando si apre un'app per la prima volta, compare un pop-up contenente una richiesta di autorizzazione all'utilizzo dei dati al fine di raccogliere informazioni sulle attività dell'utente e condividerle con terzi per finalità pubblicitarie, ad esempio.

È comunque consentito alle app sollecitare un cambiamento delle preferenze da parte dell'utente, e il percorso per poterlo fare è tutto sommato semplice (attraverso le Impostazioni, nella sezione Privacy). Come vedremo anche in seguito, Apple è spesso stata l'azienda first mover nel mettere a disposizione degli utenti gli strumenti necessari ad esercitare un maggiore controllo sulla propria privacy, anche se questo ha più volte generato contestazioni da parte di altri operatori del mercato.

Fig. 7 – Percentuale di utenti che hanno acconsentito al tracciamento via app



Fonte: Statista (https://www.statista.com/statistics/1234634/app-tracking-transparency-opt-in-rate-worldwide/).

Non ci sono fonti ufficiali sul numero di utenti che abbiano effettivamente fornito il consenso al tracciamento: i dati più precisi di cui disponiamo sono riportati in figura 7 e indicano nel 25% la soglia di coloro che

hanno dato consenso al tracciamento: **l'impatto per quegli operatori il cui business si basa sui volumi di utenti tracciati sarà stato, quindi, tutt'altro che marginale**.

Nel caso di App Tracking Transparency (ATP) molte aziende che fondano il loro business sulla pubblicità, come Meta (proprietaria di Facebook, Instagram e WhatsApp), hanno visto in questo blocco un potenziale pericolo alla raccolta dei dati di profilazione degli utenti, elemento fondamentale nel digital marketing moderno per poter garantire performance elevate agli investitori pubblicitari.

Alcune analisi[1] hanno dato ragione alla posizione di Meta e degli altri operatori che hanno una grande mole di utenti via app, perché le stime dicono che, nel semestre successivo all'adozione di ATP, la perdita di revenue per questi player è stata di 10 miliardi di dollari.

Un secondo tema molto dibattuto consiste nel fatto che queste regole valgono per tutti gli operatori esclusa Apple stessa, poiché le app di sistema possono avere accesso ai dati senza previo consenso da parte degli utenti. Questa impostazione non è chiara, come invece è quella fra cookie di sessione e cookie di tracciamento, perché è labile il confine fra le informazioni essenziali al corretto funzionamento del sistema operativo e delle relative app, e le informazioni tracciate a fini comportamentali, che possono rappresentare un importante vantaggio competitivo nei confronti degli altri operatori. Queste differenze saranno centrali per comprendere appieno i regolamenti che i legislatori hanno predisposto e stanno innovando per il futuro.

4. Android Privacy Sandbox

Nel febbraio del 2022 Google ha annunciato come intende muoversi sul versante della privacy degli utenti e della gestione di AAID.

Come ben descritto nella sezione per sviluppatori del sito Android[2], la scelta di Google è stata diversa da quella di Apple: non ha ricondotto il consenso alla decisione dei singoli utenti, ma ha cominciato un percorso di sviluppo di alcune tecnologie che dovrebbero mandare in dismissione gli attuali strumenti di tracciamento e porteranno al redesign dell'attuale architettura basata su AAID, con lo scopo di anonimizzare il tracciamento degli utenti, mantenendo però la possibilità, per i publisher e i diversi operatori del mercato, di erogare pubblicità rilevanti per i propri utenti.

1. https://www.ilpost.it/2021/11/01/apple-privacy-pubblicita-facebook-snapchat/.
2. https://developer.android.com/design-for-safety/privacy-sandbox.

5. Tracciamenti *Phygital*

Phygital è una definizione interessante perché **descrive il comportamento di un utente a cavallo fra l'esperienza nel mondo fisico e quella nel mondo digitale**.

L'utilizzo di ecommerce integrati con gli store fisici, gli strumenti di analisi dei comportamenti degli utenti sul territorio (ad esempio la gestione delle informazioni sul traffico nelle app di navigazione) sono esempi di come il mondo fisico e quello digitale vanno fondendosi nell'esperienza comune degli utenti.

Grazie alla semplicità con cui è possibile connettere dispositivi, si sono sviluppate diverse applicazioni sui device mobili e svariati oggetti IoT che si occupano di tracciare oggetti e persone nel mondo fisico.

Un esempio sono gli AirTag di Apple, grazie ai quali è possibile collegare un piccolo oggetto (un tag) che ha la funzione di rintracciare ovunque l'oggetto cui è collegato (trova il mio mazzo di chiavi, stessa funzione di trova il mio telefono o il mio tablet).

In questo contesto si stanno muovendo alcune operazioni per limitare la possibilità che informazioni indesiderate possano essere trasmesse a terzi, la più rilevante delle quali vede Google e Apple[3] promuovere congiuntamente una proposta di specifica per il settore, atta a contrastare l'uso improprio dei sistemi di localizzazione Bluetooth.

SUM-UP: tracciamenti mobile

In questo momento è evidente come non ci sia, nel mercato, una cabina di regia congiunta, impegnata nel tentativo di trovare una soluzione univoca alle problematiche di tracciamento su mobile, ma che la questione dell'implementazione tecnica dei regolamenti sulla privacy sia, piuttosto, lasciata all'arbitraria gestione dei singoli player. Ci troviamo, così, di fronte a scelte tecnologiche diverse, che rendono sempre più complicato gestire le informazioni connesse con il profilo degli utenti, anche in presenza di esplicito consenso al tracciamento dei propri dati, da parte dell'utente.

---

3. https://www.apple.com/it/newsroom/2023/05/apple-google-partner-on-an-industry-specification-to-address-unwanted-tracking/.