

UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI INGEGNERIA
Dipartimento di Ingegneria dell'Informazione
Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione



TESI DI LAUREA

**Progettazione e implementazione di un case study per l'analisi del
consent mode relativo ai cookie gestiti tramite Google**

**Design and implementation of a case study for the analysis of the
consent mode concerning cookies handled by Google**

Relatore

Prof. Domenico Ursino

Candidato

Mattia Vesperini

ANNO ACCADEMICO 2022-2023

Sommario

La gestione dei consensi di Google è un insieme di strumenti e funzionalità che permette agli utenti di controllare come vengono utilizzati i loro dati personali da parte di Google e dei suoi partner pubblicitari. Questo include la possibilità di scegliere quali informazioni condividere con Google, come la posizione, la cronologia delle ricerche e i dati di attività online, nonché di optare per la disattivazione dei cookie di terze parti.

Inoltre, la gestione dei consensi di Google fornisce anche opzioni di personalizzazione per gli annunci visualizzati agli utenti. Ciò permette a questi ultimi di scegliere gli interessi e le categorie di annunci che preferiscono visualizzare o evitare, migliorando, così, la loro esperienza online.

In linea con le leggi sulla privacy, Google ha implementato una serie di misure di sicurezza per garantire la protezione dei dati personali degli utenti. Ciò include l'adozione di standard di sicurezza elevati e l'uso di crittografia per proteggere i dati in transito e inattivi.

Keyword: Data Analytics, Customer Analytics, Consent mode, Digital Analytics, Marketing, Privacy.

Introduzione	1
1 Gestione dei dati per marketing e profilazione in Google	4
1.1 La Profilazione	4
1.2 Google Ads	6
1.3 Google Analytics	8
1.4 Google Tag Manager	10
1.5 Google Data Studio	11
1.6 Google Big Query	11
2 Introduzione ai Cookie	13
2.1 Cosa sono i cookie	13
2.2 Utilizzi e tipi di cookie	15
2.3 Struttura di un Cookie	17
2.4 Rispetto del GDPR e tutela della privacy (Cookie Law)	21
2.5 Come i cookie vengono regolamentati dallo stato Italiano	22
3 Il consent di Google per i cookie	24
3.1 Cosa si intende per Google Consent Mode	24
3.2 Funzionamento di Google Consent Mode (GCM)	25
3.3 Utilizzo dei cookie nella Google Consent Mode	26
3.4 Script e metodi di applicazione della Google Consent Mode.	30
3.4.1 Monitoraggio dello stato del consenso	30
3.4.2 Funzionalità di consenso avanzate	32
3.5 Esempio di applicazione e verifica	34
3.5.1 Verifica funzionamento Google Consent Mode	35
3.6 Benefici della Google Consent Mode	36
3.6.1 Benefici e creazione di modelli di comportamento in Google Analytics 4	38
3.7 Rispetto del GDPR e utilizzo dei dati da parte della GCS	39
4 Case study: analisi dei requisiti e progettazione	41
4.1 Analisi dei requisiti	41
4.2 Progettazione	44

5	Implementazione e risultati ottenuti	48
5.1	Implementazione degli strumenti di misurazione di Google	48
5.1.1	Installazione tramite codice di Google Ads e Analytics	49
5.1.2	Installazione tramite GTM di Google Ads e Analytics	50
5.1.3	Verifica del funzionamento degli strumenti di misurazione di Google .	51
5.2	Implementazione del banner Iubenda	52
5.3	Implementazione del Google Consent Mode	55
5.3.1	Implementazione del Google Consent Mode tramite codice	55
5.3.2	Implementazione tramite Google Tag Manager o implementazione mista	58
5.3.3	Debug e verifica funzionamento Google Consent Mode	61
5.3.4	Implementazione API per traffico sul sito	63
5.3.5	Risultati ottenuti	66
6	Conclusioni e uno sguardo al futuro	70
6.1	Conclusioni	70
6.2	Uno sguardo al futuro	71
	Bibliografia	73

Elenco delle figure

1.1	Funzionamento di Google Tag Manager	10
1.2	Funzionamento di Google Big Query	12
2.1	Funzionamento del cookie	14
2.2	Output della prima richiesta	20
2.3	Output della seconda richiesta	21
3.1	Sintesi del funzionamento di Google Consent Mode	25
3.2	Tipi di consenso gestiti da Google Consent Mode	26
3.3	Situazione ottimale, l'utente ha accettato tutti i cookie	27
3.4	Cookie relativi a Google Ads non accettati	27
3.5	Cookie relativi a Google Ads e al salvataggio non accettati	28
3.6	Cookie relativi a Google Analytics non accettati	28
3.7	Cookie relativi a Google Analytics non accettati	29
3.8	Piattaforme CMP supportate e integrate	31
3.9	Cookie relativi a Google Ads e al salvataggio non accettati.	36
3.10	Relazione tra tassi di consenso e conversioni modellate	37
4.1	Conversioni recuperate da Google con il Google Consent Mode	42
4.2	Differenza di funzionamento tra normale implementazione e Google Consent Mode	44
4.3	Risultati riassuntivi dopo l'implementazione del Google Consent Mode	45
4.4	Diagramma di flusso Google Consent Mode	46
4.5	Diagramma di flusso impatto Google Consent Mode su Google Analytics	46
5.1	Implementazione Google Ads con Google Tag Manager	50
5.2	Implementazione Google Analytics con parametro GCS impostato su "100" con Google Tag Manager	50
5.3	Implementazione Google Analytics con parametro GCS impostato su "111" con Google Tag Manager	51
5.4	Ping di verifica per la proprietà con GCS impostato su 100	51
5.5	Ping di verifica per la proprietà con GCS impostato su 111	52
5.6	Ping di verifica Google Ads	52
5.7	Schermata della home page del sito con estensione Google Tag legacy	53
5.8	Banner Iubenda all'arrivo sul sito	54
5.9	Opzioni di scelta dei cookie da parte del banner Iubenda	54

5.10	Struttura del cookie dopo l'implementazione del banner Iubenda	55
5.11	Variabile cookie proprietario con cookie policy ID	59
5.12	Tabella ReGex relativa a cookie a finalità di marketing	59
5.13	Tabella ReGex relativa a cookie analitici	60
5.14	Tabella ReGex relativa a cookie di performance e personalizzazione	60
5.15	Tag relativo allo stato di default"	61
5.16	Configurazione del tag relativo allo stato di "default"	61
5.17	Attivatore del tag per lo stato di "default"	62
5.18	Configurazione del tag per lo stato di update	62
5.19	Attivatore del tag per lo stato di "update"	63
5.20	Debug del parametro GCS tramite console	63
5.21	Debug mediante l'ispezione del datalayer	64
5.22	Entata in azione del modello di attribuzione del Google Consent Mode	67
5.23	Entata in azione del modello di attribuzione del Google Consent Mode	67
5.24	Sessioni nella proprietà con GCS 100	68
5.25	Sessioni nella proprietà con GCS 111	68
5.26	Conversioni di acquisto nella proprietà con GCS 100	69
5.27	Conversioni di acquisto nella proprietà con GCS 111	69

Ogni giorno, un individuo che si muove nella rete Internet rilascia numerose tracce, delle volte anche in modo incosciente, riguardo le proprie abitudini, preferenze, interessi, consumi e, di solito, non è del tutto a conoscenza del soggetto che avrà modo di trattare i suoi dati, nonchè delle modalità e degli scopi del trattamento. Le informazioni rilasciate vengono raccolte, selezionate ed analizzate al fine di creare profili rappresentativi dell'individuo o di un cluster di soggetti. In tal modo è possibile intraprendere azioni adeguate, come sviluppare offerte personalizzate e mirate, aumentare la user satisfaction e la fidelizzazione dell'utente con il fine di risultare più competitivi.

Concentrandosi sulle pratiche commerciali presenti nel mercato, si assiste ad una "negoiazione" di dati personali, in quanto l'utente, al fine di ricevere dei benefici, come, per esempio, campioni omaggio o sconti, fornisce agli operatori commerciali delle informazioni personali. Pertanto, avere a disposizione una massiccia quantità di dati, tramite l'attività di profilazione, consentirà a questi operatori di delineare profili dettagliati degli utenti. L'attività di profilazione non si limita ad essere usata nel settore commerciale ma viene adottata giornalmente nel web tramite l'utilizzo dei cookie.

L'importanza dei cookie nell'ambito digitale è cambiata in modo notevole nel corso degli anni. Questi sono piccoli file di testo che vengono salvati nel dispositivo di un utente quando egli visita un sito web; essi svolgono un ruolo fondamentale nel migliorare la user experience online. Nel corso degli anni l'importanza dei cookie è evoluta; all'inizio essi venivano principalmente utilizzati per ricordare le informazioni di base, come le credenziali di accesso e le preferenze di visualizzazione, con il fine di migliorare l'usabilità in modo che un utente non dovesse inserire i propri dati ad ogni visualizzazione della pagina web. Successivamente, i siti web hanno iniziato a utilizzare i cookie per tracciare il comportamento degli utenti e raccogliere dati sulle loro abitudini e sui loro comportamenti durante la navigazione. Tali dati sono, poi, utilizzati per creare una profilazione dell'utente in modo da offrire contenuti personalizzati, come, ad esempio, consigli sui prodotti o annunci mirati. Ciò ha portato ad un aumento dei modelli di business basati sulla pubblicità online e alla nascita di servizi di retargeting, dando inizio all'era del digital marketing.

L'utilizzo dei cookie ha ovviamente, sollevato preoccupazioni sulla privacy e sulla gestione delle informazioni personali dell'utente. Man mano che la tracciabilità e la raccolta di dati personali aumentavano, gli utenti si sono resi conto che i cookie potevano essere utilizzati per raccogliere informazioni sensibili senza il loro consenso. Ciò ha suscitato discussioni e la nascita di regolamentazioni sempre più rigorose sulla gestione dei cookie e sulla protezione dei dati personali.

Nel 2018 è entrato in vigore il regolamento generale dei dati (GDPR) nell'Unione Europea.

Esso ha introdotto requisiti più stringenti per il consenso degli utenti all'uso dei cookie per la profilazione, e ha reso obbligatoria la trasparenza nell'informare gli utenti sulle varie tecniche di raccolta dei dati.

Google ha definito un modo che riesce a tracciare comunque il cookie dell'utente anche quando c'è la negazione del tracciamento, anonimizzando l'utente. Tale approccio ha il nome di Google consent mode. Questo metodo si presenta come una soluzione avanzata e dinamica che consente alle organizzazioni di adattare il comportamento di Google Analytics 4 e Google Ads alle scelte degli utenti in termini di consenso all'uso dei cookie e degli identificatori. Attraverso l'interazione con la piattaforma di gestione del consenso (CMP), il consent mode ottimizza la raccolta di dati anonimi, garantendo, al contempo, la conformità alle normative sulla privacy.

Questo strumento, interagendo con i CMP o con banner custom, riceve le scelte degli utenti e adatta dinamicamente il comportamento relativo alla creazione e alla lettura dei cookie da parte dei tag Google Analytics 4 e Google Ads. Quando i visitatori accettano il consenso, i tag vengono attivati normalmente, creando o leggendo i dati di identificazione dai cookie di Google. Quando i visitatori negano il consenso, i tag inviano "ping" con informazioni anonime sugli utenti, senza leggere o creare cookie.

In un secondo momento Google Analytics 4 e Google Ads, attraverso degli algoritmi di modellazione che si basano sulla IA, integrano i dati raccolti direttamente, ovvero i dati degli utenti che hanno dato il consenso, con quelli stimati relativi agli utenti che non hanno rilasciato il loro consenso. In questo modo potremmo avere una visione di insieme più completa del traffico del sito.

La presente tesi si colloca in tale contesto ponendosi l'obiettivo di evidenziare come il Google Consent Mode riesca a recuperare conversioni e dati a livello statistico, nel caso in cui un utente abbia rifiutato i cookie di misurazione. Si è costruito un sito di test che simula un portale di e-commerce, nel quale sono stati implementati gli strumenti di tracking di Google, come Analytics e Google Ads. Inoltre è stato inserito un banner tramite il CMP Iubenda, installando all'interno del sito il codice necessario al suo funzionamento. Ad esso è stato integrato il Google Consent Mode con gli script necessari all'interno del sito, rispettando al contempo la cookie law attuale. Al banner è stata collegata un'API costruita ad hoc, che consente di generare 1000 utenti giornalieri, che randomicamente accettano o rifiutano i cookie di misurazione e che, contemporaneamente, simulano acquisti all'interno del sito e-commerce. Questa API consente di affrontare tutti i casi d'uso possibili, ovvero:

- un utente univoco che rifiuta tutti i cookie di misurazione e poi procede con un acquisto,
- un utente univoco che accetta i cookie analitici e non quelli di marketing e procede ad un acquisto;
- un utente univoco che non accetta i cookie analitici ma accetta quelli marketing e procede ad un acquisto;
- un utente univoco accetta tutti i cookie e procede ad un acquisto. (quest'ultimo rappresenta il caso ottimale).

Ai fini della misurazione l'acquisto è stato reso univoco cambiando randomicamente il prezzo di un oggetto e il suo ID di transazione. Poiché non era possibile a fini di policy interne aziendali condividere dati di altri siti web, si è scelto di simulare una situazione comune usando l'API precedentemente descritta in un sito di test, in modo da poter mostrare i vari report senza alcun tipo di problema di policy aziendale. Nelle dashboard saranno evidenziate le principali differenze statistiche che comporteranno l'utilizzo del Google Consent Mode,

concentrandosi su due scenari principali, ovvero quello ottimale, dove un utente dà l'autorizzazione completa a tutti i cookie, e quello sfavorevole dove un utente accetta soltanto i cookie necessari (tecnici). Infine, vengono mostrate le percentuali relative alle conversioni recuperate grazie a questo strumento e al suo modello di machine learning, facendo un paragone di quante conversioni andrebbero perse senza il suo prezioso uso.

La presente tesi è strutturata come di seguito specificato:

- Nel primo capitolo si porrà attenzione al concetto di profilazione e di come Google gestisce questa grande attività nel campo del digital marketing
- Nel secondo capitolo verrà dedicata particolare attenzione ai cookie, poiché il loro utilizzo può permettere di monitorare la navigazione dell'utente in modo da generare un accurato profilo di quest'ultimo.
- Nel terzo capitolo verrà presentato nel dettaglio il Google Consent Mode, metodo innovativo con il quale Google effettua la gestione delle preferenze dell'utente traendo dei benefici anche in caso di un rifiuto totale di esse.
- Nel quarto capitolo viene presentato il caso di studio reale, partendo dall'analisi dei requisiti dove vengono descritti i vari casi d'uso, per poi spostarsi sulla parte di progettazione, dove vengono mostrati nel dettaglio i casi d'uso mediante i diagrammi di sequenza e attività.
- Nel quinto capitolo si prosegue lo studio del caso reale, in cui ci si focalizza sulla parte pratica, partendo, quindi, dall'implementazione del Google Consent Mode effettuata all'interno del sito, dell'implementazione del banner effettuata tramite il CMP scelto. Successivamente vengono analizzati i dati e presentate le principali differenze e i maggiori benefici.
- Nel sesto capitolo, quello conclusivo, vengono tratte alcune conclusioni riguardanti il consent mode e i dati mostrati nell'elaborato, dando uno sguardo al futuro con la prossima mutazione dei cookie di terzi parti.

Gestione dei dati per marketing e profilazione in Google

In questo capitolo verrà introdotto il concetto di profilazione e si vedrà come Google gestisce questo importante processo attraverso i suoi tool, approfondendo gli scopi e gli usi e specificando i vari tipi di profilazione presenti nel mondo del digital marketing.

1.1 La Profilazione

La profilazione è una tecnologia ampiamente adottata dagli operatori commerciali, che utilizza algoritmi per elaborare automaticamente grandi quantità di dati personali degli utenti e ottenere informazioni dettagliate sulle loro preferenze, sugli stili di vita e le abitudini d'acquisto, creando, così, un profilo dell'utente e consentendone la personalizzazione. Permette, quindi, l'attuazione di strategie di marketing personalizzate e la costruzione di relazioni a lungo termine.

La profilazione è il processo necessario per identificare il pubblico target in base a parametri quali, ad esempio, le abitudini di acquisto, il comportamento di consumo, lo stile di vita, l'età, il sesso, il livello di reddito, il livello di istruzione e l'occupazione, etc., e per identificarlo come appartenente a un determinato gruppo. Più precisamente, la profilazione è definita come "la creazione di un profilo attraverso l'identificazione e la raccolta di dati personali caratteristici e di abitudini di una persona"¹. Attraverso la creazione di profili, le aziende possono ottenere una conoscenza più approfondita dei consumatori, prevedere e migliorare le loro offerte, condurre attività di marketing mirate, inviare messaggi pubblicitari personalizzati e attuare campagne promozionali o di digital marketing ad hoc.

La profilazione viene effettuata principalmente nel settore commerciale; nel corso degli anni abbiamo assistito all'evoluzione di questa attività. Si è passati, addirittura, da una profilazione su piccola scala, basata sui dati comunicati dai clienti dietro la distribuzione di fidelity card, a una profilazione a larga scala, effettuata nel mondo del web, utilizzando grandi database e cookie. Il motivo di ciò è che questo tipo di attività permette di definire gli obiettivi a cui indirizzare ogni campagna pubblicitaria e di modificarla sulla base dei diversi profili ottenuti in base agli obiettivi di mercato. Analizzando, invece, le informazioni ottenute dall'aggregazione automatica dei dati raccolti, è possibile sviluppare campagne specifiche che tengano conto dei comportamenti, delle abitudini e degli stili di vita del target, rendendo l'offerta più attraente. In realtà, questo fenomeno non è una scoperta nuova; è incominciato tra l'altro, quando i produttori e i distributori di beni e servizi di consumo hanno iniziato

¹Vocabolario Treccani https://www.treccani.it/vocabolario/profilazione_

a proporre promozioni, offerte speciali e sconti a condizione che i consumatori rivelassero le loro informazioni personali, compresi i dati anagrafici, al fine di aumentare la fedeltà dei clienti. Paragonandolo a quello che accade oggi quotidianamente visitando siti web, con registrazioni a newsletter ma soprattutto l'accettazione di i cookie o esprimendo preferenze di essi, l'utente è soggetto in ogni momento alla ricezione di offerte pubblicitarie personalizzate ad hoc in base ai siti precedentemente visualizzati che vengono memorizzati nei cookie.

Successivamente, le risorse umane ed economiche delle aziende hanno iniziato a concentrarsi sullo sviluppo di attività di profilazione e di campagne di direct marketing per raggiungere specifici target di consumatori. Lo sviluppo di Internet, il maggiore utilizzo delle tecnologie dell'informazione e della comunicazione, la scelta di preferenze tramite i cookie banner e l'iscrizione volontaria ai social network sono stati fattori che hanno ulteriormente sviluppato e semplificato le attività di profilazione, facilitate in particolare dall'uso di algoritmi. È stato sottolineato che la principale differenza tra le relazioni di mercato che esistevano ieri e quelle della società dell'informazione risiede nei diversi approcci adottati dalle aziende per raggiungere i potenziali clienti. Mentre in passato i clienti non erano visti come individui ma come oggetti appartenenti a un gruppo omogeneo e privo di diversità, oggi, con lo sviluppo di mezzi di comunicazione innovativi e interattivi, si stanno costruendo relazioni basate sulla personalizzazione dei messaggi pubblicitari, ponendo i consumatori al centro del sistema di comunicazione e utilizzando i loro bisogni e interessi per motivarli all'acquisto.

È importante ricordare che quando le aziende hanno accesso alle informazioni sui consumatori possono non solo utilizzarle direttamente, ma anche usarle come mezzo di scambio con terzi. Pertanto, con una grande quantità di dati a disposizione, un'azienda può acquisire una conoscenza approfondita dei propri clienti e avviare una strategia di Customer Relationship Management (CRM) per ottenere un maggiore vantaggio competitivo e una crescita aziendale. Il CRM è un approccio strategico valido per costruire e gestire le relazioni con i clienti, in questo modo le aziende diventano centrate sul cliente piuttosto che nel prodotto, mettendo il cliente verso al centro dell'attività.

In termini più specifici, potremmo quindi elencare i principali ambiti d'azione di una soluzione CRM e capire come i vari software sono in grado di soddisfare le nostre specifiche esigenze nei seguenti aspetti:

- Completezza della suite;
- Marketing automation;
- Customer service;
- Sales automation;
- Marketing cloud;
- Social monitoring;
- Community;
- Contact management;
- E-commerce;
- Analytics

Il CRM non è altro che un semplice confronto tabellare che ci consente di utilizzare un sistema di scoring per pesare il contributo dei vari elementi, a fronte dell'offerta dei vari

software CRM valutati. Alla proposta tecnica va, infine, associata la verifica di fattibilità economica, un aspetto molto importante. Dal momento che le soluzioni di pricing possono generare impatti piuttosto differenti sulle capacità di investimento previste dai business plan.

Nell'era digitale in cui viviamo, il vasto mondo di Internet ha portato alla creazione di numerosi strumenti e servizi che hanno rivoluzionato il modo in cui interagiamo con il mondo online. Il gigante tecnologico mondiale Google ha svolto un ruolo di primo piano in questo processo offrendo una serie di strumenti e servizi. Google ha creato una presenza onnipresente nella nostra vita quotidiana digitale. Tuttavia, la costante interazione con questa piattaforma solleva anche importanti questioni relative alla profilazione degli utenti.

La profilazione può essere definita come la raccolta, l'analisi e l'interpretazione dei dati personali per creare un profilo dettagliato di un individuo. Questa pratica sta diventando sempre più diffusa, soprattutto con la proliferazione della tecnologia digitale e il crescente utilizzo di Internet. Google, con i suoi numerosi servizi, svolge un ruolo fondamentale nella creazione di tali profili.

Tali strumenti, che consentono un approccio a 360° nel mondo della profilazione e analisi dei dati da parte di Google, sono:

- Google Ads;
- Google Analytics;
- Google Tag Manager;
- Google Data Studio;
- Google Big Query;

Questi sono i principali esempi di come la profilazione si intreccia con gli strumenti di Google. Sebbene l'obiettivo principale di Google sia quello di migliorare l'esperienza degli utenti, i dibattiti etici sulla profilazione e sulla protezione della privacy dei dati stanno diventando sempre più importanti. Trovare un equilibrio tra la personalizzazione dei servizi e la protezione dei dati personali rimane una sfida importante per Google e per l'industria tecnologica nel suo complesso.

1.2 Google Ads

Google Ads (ex Google AdWords) è la piattaforma pubblicitaria online di Google. I marketer e gli inserzionisti possono creare annunci mirati e promuovere i loro prodotti e servizi sui vari canali di Google, tra cui il motore di ricerca Google, YouTube e la Rete Display di Google.

Di seguito sono elencate alcune delle caratteristiche principali di Google Ads:

- *Campagne di ricerca*: rappresentano una delle caratteristiche principali di Google Ads. Gli inserzionisti possono visualizzare annunci di testo sponsorizzati nelle pagine dei risultati di ricerca di Google quando gli utenti cercano parole chiave specifiche relative alla loro attività.
- *Campagne display*: la Rete Display di Google (Google Display Network - GDN) consiste in una vasta rete di siti web, blog e applicazioni che possono visualizzare annunci grafici, responsive e video. La GDN raggiunge un vasto pubblico online e consente la pubblicità visiva promuovendo attraverso essa il marchio.

- *Campagne di shopping*: Google Shopping consente agli inserzionisti di promuovere i propri prodotti su Google e di visualizzare informazioni come immagini e prezzi direttamente nella pagina dei risultati di ricerca. Questa funzione è particolarmente utile per l'e-commerce.
- *Campagne video*: attraverso la pubblicità su YouTube, gli inserzionisti possono promuovere i video sulla piattaforma di condivisione video di Google. Gli annunci possono essere visualizzati prima, durante e dopo i video di YouTube o come annunci in-stream durante la visione di contenuti di terzi.
- *Campagne per le app*: gli sviluppatori di app possono promuovere le loro applicazioni nel Google Play Store e nella pubblicità in-app. Il targeting degli annunci può essere basato sul comportamento degli utenti e sulle interazioni con altre app.
- *Targeting e segmentazione*: Google Ads offre un'ampia gamma di opzioni per il targeting e la segmentazione degli annunci. Gli inserzionisti possono impostare criteri specifici come la geografia, la lingua, gli interessi, i dati demografici e il comportamento online per raggiungere il pubblico più adatto alle loro campagne.
- *CPC (Costo per clic) e metodi di pagamento*: Google Ads utilizza un modello pay-per-click in cui gli inserzionisti pagano solo quando un utente fa effettivamente clic sul loro annuncio. Inoltre, è possibile impostare un budget giornaliero per controllare le spese pubblicitarie.
- *Analisi delle prestazioni*: Google Ads offre strumenti avanzati per il monitoraggio delle prestazioni delle campagne. Gli inserzionisti possono analizzare i clic, le conversioni, i tassi di conversione, il costo per clic (CPC), il ritorno sulla spesa pubblicitaria (ROI) e altri elementi statistici creati con il fine di monitorare la campagna pubblicitaria.
- *Automazione delle offerte*: Google Ads offre opzioni di automazione delle offerte, come l'offerta automatica basata sul Costo per Acquisizione (CPA) e sul Ritorno sulla Spesa Pubblicitaria (ROAS), per ottimizzare in modo efficiente l'investimento fatto in partenza.

Queste sono solo alcune delle numerose funzionalità offerte da Google Ads. Gli inserzionisti possono utilizzare questa piattaforma in modo strategico per raggiungere il proprio pubblico di riferimento, aumentare la consapevolezza del marchio e ottenere risultati misurabili attraverso le campagne pubblicitarie online.

Il rapporto tra la pubblicità di Google e la profilazione è strettamente interconnesso, in quanto la piattaforma pubblicitaria di Google si basa sulla raccolta e sull'analisi dei dati degli utenti per fornire pubblicità altamente mirata. La profilazione è quindi usata per personalizzare le campagne pubblicitarie seguendo vari step:

1. *Raccolta di dati*: Google raccoglie grandi quantità di dati sui propri utenti attraverso i suoi vari servizi, tra cui il motore di ricerca, YouTube e Gmail. I dati raccolti comprendono le ricerche effettuate, le interazioni con gli annunci pubblicitari, le visite ai siti web e le preferenze di visualizzazione dei video. Questi dati forniscono a Google una panoramica dettagliata del comportamento, degli interessi e delle preferenze degli utenti.
2. *Profilazione del pubblico*: Google Ads utilizza i dati raccolti per profilare un pubblico specifico in base a vari criteri quali interessi, dati demografici e comportamento online. Questa profilazione consente agli inserzionisti di mostrare annunci solo agli utenti che

rientrano in segmenti di pubblico mirati, aumentando la rilevanza dell'annuncio per l'utente.

3. Targeting: Google Ads offre agli inserzionisti una serie di opzioni di targeting. Queste includono il targeting per parole chiave, il retargeting degli utenti che visitano un sito web specifico, il targeting geografico e il targeting per interessi. Tutte queste opzioni di targeting si basano sul profilo dell'utente e garantiscono che gli annunci corretti raggiungano gli utenti giusti.
4. Pubblicità personalizzata: la profilazione consente a Google Ads di fornire annunci altamente personalizzati. Gli annunci possono includere testi, immagini e video specifici, adattati agli interessi e alle preferenze del pubblico target, aumentando le probabilità di coinvolgimento degli utenti e le conversioni.
5. Misurazione delle prestazioni: la profilazione può anche consentire una misurazione più accurata delle prestazioni di una campagna pubblicitaria. Analizzando i dati demografici, il comportamento di coinvolgimento e le conversioni degli utenti, gli inserzionisti possono comprendere meglio e ottimizzare l'efficacia delle loro campagne.

È importante sottolineare che Google adotta misure di privacy per proteggere i dati personali degli utenti e per consentire a questi ultimi di utilizzare gli strumenti di controllo delle preferenze pubblicitarie. Questo perché la profilazione consente agli inserzionisti di trasmettere il messaggio ad un utente mirato, di migliorare l'efficacia delle campagne pubblicitarie e di offrire agli utenti un'esperienza più personalizzata.

In passato Google Ads ha avuto un rapporto significativo con i cookie, tuttavia nel corso del tempo ci sono stati cambiamenti significativi dovuti all'evoluzione delle politiche sulla privacy e delle tecnologie digitali. Google Ads ha utilizzato cookie di terze parti per tracciare gli utenti su siti web e piattaforme esterne. Questi cookie hanno permesso all'azienda di tracciare il comportamento degli utenti e di raccogliere dati per la profilazione degli interessi, il remarketing e l'analisi delle prestazioni delle campagne pubblicitarie. Tuttavia, diverse aziende e organizzazioni hanno sollevato dubbi sulla privacy dei dati degli utenti derivanti dal tracciamento anomalo e abusivo dei cookie.

A partire dal 2021, molti dei principali browser web, tra cui Google Chrome, hanno annunciato l'intenzione di eliminare o limitare l'uso dei cookie di terze parti. Questo cambiamento è stato determinato dalle crescenti preoccupazioni sulla privacy e sulla protezione dei dati degli utenti. Di conseguenza, Google Ads e altri servizi pubblicitari hanno dovuto adattarsi a nuovi modi di raccogliere dati e raggiungere il pubblico. In risposta alla riduzione dell'uso dei cookie di terze parti, Google ha sviluppato nuove soluzioni pubblicitarie basate sulla privacy, come il Federated Learning of Cohorts (FLoC), che raggruppa gli utenti in gruppi di interesse (cluster), anziché tracciarli singolarmente. Inoltre, sono state introdotte altre metodologie, come l'elaborazione dei dati all'interno del browser (elaborazione sul dispositivo) e la condivisione anonima delle informazioni sugli interessi degli utenti.

In sintesi, la relazione tra la pubblicità di Google e i cookie era parte integrante della profilazione degli utenti e dell'efficacia delle campagne pubblicitarie. Tuttavia, le preoccupazioni per la privacy e i cambiamenti nelle politiche digitali hanno spinto Google Ads e altri servizi pubblicitari ad adottare nuove soluzioni e strategie per proporre annunci pertinenti, proteggendo, al contempo, la privacy degli utenti.

1.3 Google Analytics

Google Analytics è una potente piattaforma di analisi web fornita da Google per tracciare e analizzare il traffico di siti web e applicazioni. Esso offre un'ampia gamma di funzionalità

tecniche per raccogliere, elaborare e visualizzare dati dettagliati sulle attività degli utenti sul sito web. La funzionalità di base di Google Analytics consiste nell'inserimento di un codice di tracciamento JavaScript all'interno del codice sorgente del sito web. Questo codice raccoglie i dati degli utenti, incluso il traffico, le pagine visitate, il comportamento di navigazione, e altro ancora.

```
1
2 <script async
3 src="https://www.googletagmanager.com/gtag/js?id=G-XXXXXX">
4 </script>
5 <script>
6   window.dataLayer = window.dataLayer || [];
7   function gtag(){dataLayer.push(arguments);}
8   gtag('js', new Date());
9
10  gtag('config', 'G-XXXXXX');
11 </script>
```

Source Code 1.1: Codice di tracciamento Analytics

Google Analytics tiene traccia del traffico del sito web e fornisce informazioni dettagliate sul numero di visitatori, sul tempo trascorso sul sito, sulle pagine visitate e sul tasso di rimbalzo (quando gli utenti abbandonano il sito immediatamente). Può anche identificare le fonti di traffico che portano gli utenti al sito web; queste includono i motori di ricerca, i siti di riferimento, le campagne pubblicitarie, i social media o qualsiasi mezzo per raggiungere la pagina internet. Una delle caratteristiche più importanti di Google Analytics è il monitoraggio delle conversioni; gli utenti possono impostare obiettivi e tracciare il numero di conversioni per qualsiasi azione che consenta loro di raggiungere i propri obiettivi, come la compilazione di moduli, l'acquisto e la registrazione all'interno della piattaforma. Esso fornisce inoltre, strumenti per analizzare il comportamento degli utenti sul sito web, come le mappe di calore, istogrammi e pie chart, creando dei report personalizzati in base alle esigenze dell'utente.

Lo strumento consente agli utenti di segmentare il proprio pubblico in base a criteri specifici, quali il comportamento di navigazione, le interazioni con il sito web e le fonti di traffico. Ciò consente agli inserzionisti di analizzare e raggruppare gli utenti in segmenti specifici, rendendo più facile indirizzare annunci e contenuti pertinenti a ciascun gruppo. È importante notare che la profilazione diretta degli utenti attraverso Google Analytics non è lo scopo principale. La piattaforma viene utilizzata principalmente per ottenere dati e informazioni aggregate sul traffico del sito e sul comportamento degli utenti al fine di migliorare l'esperienza del sito e l'efficacia delle campagne di marketing. Tuttavia, è fondamentale rispettare la normativa sulla privacy e fornire agli utenti informazioni chiare sull'uso dei cookie e sulla raccolta dei dati, ottenendo il consenso, ove necessario.

Google Analytics ha un rapporto importante con i cookie, poiché ne fa un uso estensivo per raccogliere dati sul comportamento degli utenti e per fornire un'analisi dettagliata del traffico di siti web e app. Per utilizzare Google Analytics, è necessario includere un codice di tracciamento JavaScript nel codice sorgente del sito web o dell'app. Tale codice è chiamato "cookie di prima parte" e viene utilizzato per identificare in modo univoco gli utenti e tracciarne il comportamento.

I cookie di prima parte sono cookie impostati dal dominio del sito web visitato dall'utente. Quando quest'ultima visita un sito web che utilizza Google Analytics, il codice di tracciamento crea un cookie di prima parte nel browser dell'utente. Questo cookie contiene un identificatore univoco (di solito un numero generato in modo casuale) che consente a Google Analytics di identificare l'utente e di tenere traccia della sua interazione con il sito. I cookie di prima parte vengono utilizzati per raccogliere dati sul traffico del sito web, come le pagine visitate, i tempi di sessione, le fonti di traffico e le conversioni. Questi dati vengono trasmessi ai server

di Google Analytics per essere elaborati e analizzati. Per proteggere la privacy dell'utente, Google Analytics può anonimizzare il suo indirizzo IP; questa funzione tronca una parte dell'indirizzo IP prima di memorizzarlo, in modo che l'indirizzo IP completo non venga memorizzato e l'utente rimanga anonimo per una parte dei dati raccolti. I cookie di prima parte utilizzati da Google Analytics possono avere tempi di scadenza diversi, ma in genere rimangono nel browser dell'utente per un certo periodo di tempo (due anni per impostazione predefinita). Ciò consente a Google Analytics di identificare l'utente nelle visite successive al sito web.

Google Analytics rispetta l'informativa sulla privacy di Google e le leggi vigenti in materia di protezione dei dati. Gli utenti di Google Analytics devono essere tenuti a informare adeguatamente le persone che visitando il sito fanno uso dei cookie sulle informazioni che verranno raccolte ottenendo il loro consenso.

1.4 Google Tag Manager

Google Tag Manager (GTM) è una piattaforma di gestione dei tag che consente agli utenti di implementare e gestire in modo efficiente i tag di tracciamento, le tracce su siti web e applicazioni senza modificare direttamente il codice sorgente. GTM offre un'interfaccia intuitiva che facilita l'implementazione dei tag di tracciamento senza dover modificare il codice del sito web o dell'applicazione. I tag possono essere aggiunti, modificati ed eliminati dal pannello di controllo di GTM. Tutti i tag, compresi quelli di Google Analytics e Google Ads possono essere gestiti da un'unica piattaforma centrale. GTM consente il tracciamento personalizzato come, ad esempio, il tracciamento dei clic su elementi specifici della pagina, l'invio di moduli, le interazioni con i video, ecc.

Questi eventi personalizzati possono essere utilizzati per analizzare ulteriormente il comportamento degli utenti. Inoltre, la piattaforma fornisce strumenti di test e debug per garantire il corretto funzionamento dei tag prima di attivarli su un sito o un'applicazione. Google Tag Manager (GTM) svolge un ruolo importante nel contesto della profilazione degli utenti, in quanto facilita l'implementazione e la gestione dei tag di tracciamento e consente la raccolta di dati che possono essere utilizzati per creare profili di utenti. Nella figura 1.1 viene riportato il funzionamento di Google Tag Manager.



Figura 1.1: Funzionamento di Google Tag Manager

Google Tag Manager non utilizza i cookie per impostazione predefinita; esso abilita i tag per gli script di terze parti che possono inserire cookie nel dispositivo dell'utente. GTM può leggere il valore dei cookie di prima parte impostati nella pagina web, ma non fa nulla con i

cookie di terze parti. Anche se lo strumento non imposta alcun cookie, c'è un caso in cui lo fa. Se si attiva la modalità Anteprima e Debug di GTM, vengono impostati alcuni cookie di prima parte sul sito in fase di anteprima. Questi cookie sono necessari per il funzionamento della modalità Anteprima, ossia per visualizzare ciò che accade sul sito e quali tag vengono attivati. Solo gli amministratori del sito o gli utenti che hanno abilitato la modalità di anteprima e debug riceveranno questi cookie; quando si esce dalla modalità di anteprima e debug, GTM cancella questi cookie dal dispositivo. A parte i log delle richieste HTTP che scadono in 14 giorni e altri dati diagnostici non personali, GTM non raccoglie, memorizza o condivide alcuna PII (Personally Identifiable Information) sui visitatori degli utenti che visualizzano il sito web

Tuttavia, supponiamo che si voglia utilizzare Google Analytics o altri strumenti sul proprio sito web tramite GTM è necessario aggiornare l'informativa sulla privacy e di conseguenza ottenere il consenso se questi strumenti raccolgono i dati personali dei visitatori.

1.5 Google Data Studio

Google Data Studio è uno strumento semplice e intuitivo che consente di creare rapporti interattivi e visualizzazioni dinamiche dei dati in modo chiaro. Esso può essere utilizzato con Google Analytics, Google Ads, Google Sheets, database SQL, file CSV, YouTube, e molte altre fonti di dati. Gli utenti possono importare i dati direttamente da queste fonti o caricarli manualmente nei report creando rapporti personalizzati da zero o utilizzare modelli predefiniti forniti da Google o da terzi. La piattaforma dispone di una serie di componenti grafici come grafici, tabelle, mappe, immagini e testo che possono essere trascinati nei report per creare visualizzazioni di dati. Queste ultime possono essere personalizzate in vari modi, tra cui la modifica dei colori, delle dimensioni, del tipo di grafico e delle etichette. In questo modo gli utenti possono personalizzare i report in base al proprio branding ed evidenziare determinati aspetti dei dati. I dati visualizzati nei report sono aggiornati in tempo reale, per cui gli utenti possono visualizzare i dati più recenti senza dover ricaricare manualmente il report. Gli utenti possono collaborare con altri utenti per creare e modificare i report; questi ultimi possono anche essere condivisi online o visualizzati da chiunque abbia un link di condivisione.

Google Data Studio non utilizza cookie e non è coinvolto nella loro creazione o nella loro gestione; in quanto piattaforma di visualizzazione dei dati, esso si basa esclusivamente sui dati forniti dagli utenti tramite link a fonti di dati selezionate. I cookie non sono quindi un elemento essenziale di Google Data Studio. Tuttavia, si noti che i dati utilizzati da Google Data Studio possono essere forniti da fonti di dati che utilizzano i cookie per tracciare e raccogliere informazioni sugli utenti. Ad esempio, se si collega Google Data Studio a fonti di dati come Google Analytics o Google Ads, i dati importati possono includere i cookie utilizzati da questi servizi per tracciare il comportamento degli utenti sui siti web e le campagne pubblicitarie.

1.6 Google Big Query

Google BigQuery è un data warehouse aziendale completamente gestito che gestisce e analizza i dati con machine learning integrato, analisi geospaziale, business intelligence e altro ancora, senza la necessità di gestire l'infrastruttura grazie alla sua architettura serverless. Le query SQL possono essere utilizzate per rispondere alle domande più importanti dell'azienda e il motore di analisi scalabile e distribuito di BigQuery consente di eseguire petabyte di query in pochi minuti. Lo strumento massimizza la flessibilità disaccoppiando il motore di elaborazione che analizza i dati dalle opzioni di archiviazione. I dati possono essere archiviati

in BigQuery per essere analizzati; in alternativa, BigQuery può essere utilizzato per valutare i dati in un unico luogo. Le query unificate consentono di caricare i dati da fonti esterne e i flussi supportano aggiornamenti continui dei dati. BigQuery ML e BI Engine e altri potenti strumenti consentono di analizzare e comprendere questi dati.

Le interfacce di BigQuery comprendono l'interfaccia della console di Google Cloud e lo strumento a riga di comando BigQuery. Gli sviluppatori e i data scientist possono trasformare e gestire i dati utilizzando le API REST e RPC di BigQuery, nonché le librerie client con programmi familiari come Python, Java, JavaScript e Go.

BigQuery è principalmente uno strumento di analisi dei dati, ma può anche essere indirettamente coinvolto nella profilazione degli utenti in base alle fonti di dati e alle query. Può essere popolato con dati provenienti da diverse fonti, tra cui piattaforme di tracciamento come Google Analytics, dati sul comportamento degli utenti e dati demografici. La piattaforma consente di eseguire query e analisi complesse su grandi quantità di dati. Tali query possono essere utilizzate per identificare modelli e comportamenti specifici degli utenti ed estrarre informazioni rilevanti per costruire profili dettagliati.

Le query personalizzate consentono di segmentare e raggruppare gli utenti in base a diversi criteri, ad esempio raggruppando gli utenti con comportamenti simili o appartenenti a determinate categorie. In questo modo, quindi è possibile creare segmenti di utenti per analisi e profili più approfonditi.

La relazione tecnica tra Google BigQuery e i cookie è indiretta: Google BigQuery è un servizio di archiviazione e analisi dei dati, i cookie sono piccoli file di testo. Esso viene utilizzato per l'elaborazione e l'analisi dei dati: se i dati dei cookie vengono raccolti e archiviati in un sistema di gestione dei dati come Google Cloud Storage o Google Cloud Datastore, possono essere trasferiti a BigQuery per l'analisi e la profilazione degli utenti. Una volta caricati i dati dei cookie in BigQuery, è possibile utilizzare potenti query SQL per eseguire analisi complesse e generare report basati su questi dati. Ciò include la segmentazione degli utenti in base ai dati dei cookie, l'analisi delle tendenze di navigazione e tutte le informazioni memorizzate nel cookie. Nella figura 1.2 viene mostrato il funzionamento di Google Big Query.

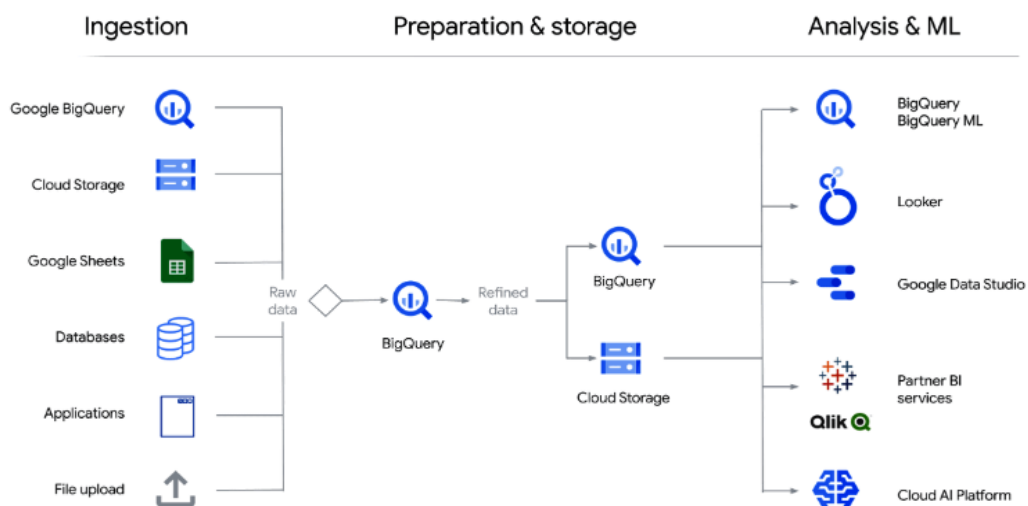


Figura 1.2: Funzionamento di Google Big Query

In questo capitolo si entrerà più nello specifico su che cosa sono i cookie, strumento al giorno d'oggi indispensabile ai fini del tracciamento e della profilazione, vedremo, anche, come esso è regolamentato dalla legge italiana. Inoltre, si approfondiranno le varie tipologie di cookie presenti sul mercato dando uno sguardo a come viene rispettato il GDPR (General Data Protection Regulation).

2.1 Cosa sono i cookie

Come già accennato, la profilazione è un'attività in cui specifici programmi elaborano grandi quantità di dati dei clienti con l'obiettivo di definire gruppi omogenei di utenti, i quali possono poi essere utilizzati per attività pubblicitarie e attività promozionali mirate sulla base di specifiche caratteristiche. La spinta a fornire servizi sempre più personalizzati in base alle preferenze dei singoli clienti ha, infatti, portato all'affinamento delle tecniche di marketing digitale grazie alla digitalizzazione e alla diffusione di internet. Per ottenere le informazioni necessarie, i fornitori di servizi possono osservare e monitorare il comportamento dei clienti, studiare le loro abitudini di acquisto, di consumo e valutare, ad esempio, quali prodotti e servizi scelgono più frequentemente utilizzando i cookie ed altri strumenti automatizzati di controllo.

I cookie sono dati relativi all'utente che vengono memorizzati sul computer e utilizzati per migliorare la navigazione. Essi sono noti anche come cookie HTTP, web cookie, internet cookie o browser cookie; questi vengono creati dal server e inviati al browser. Questo scambio di informazioni consente al sito di riconoscere il computer dell'utente e di inviargli informazioni personalizzate in base alla sua sessione. Il nome "cookie" deriva da una tecnica utilizzata in ambiente UNIX fin dagli anni '80 e nota come "magic cookie"; l'origine del suo nome è sconosciuta, ma i riferimenti alle fiabe sono innegabili.

Il primo utilizzo dei cookie in HTTP risale al 1994, quando furono usati per verificare se un lettore di un sito Netscape aveva già visitato quel sito in precedenza. Inizialmente l'introduzione dei cookie non è stata molto pubblicizzata; se ne è cominciato a parlare dopo un articolo del Financial Times del 12 febbraio 1996. Il successivo dibattito si è incentrato sull'impatto dei cookie sulla riservatezza; essi sono stati oggetto di due audizioni della Federal Trade Commission statunitense nel 1996 e nel 1997 e, a partire da queste date, l'uso dei cookie ha iniziato a essere regolamentato.

Al giorno d'oggi l'uso più comune è quello di memorizzare informazioni sulle abitudini degli utenti all'interno dei siti web visitati. Tali applicazioni hanno spesso suscitato il sospetto dei sostenitori della privacy dei navigatori, in quanto i cookie possono sia aiutare nella

navigazione che nello "spionaggio". Quest'ultimo caso riguarda molte catene pubblicitarie, le quali vendono ads a molti siti diversi, utilizzando i cookie allegati alle immagini pubblicitarie per associare le visite di uno stesso utente a diverse pagine web, costruendo una sorta di profilo dei suoi siti preferiti. Altri usi dei cookie, utili come servizio agli utenti, sono, ad esempio, la registrazione dei dati di sessione per evitare di dover ripetere l'autenticazione alla visita successiva, o nei siti di commercio elettronico dove vengono utilizzati utilizzati nel "carrello della spesa", ad esempio per conservarne il contenuto. Nella Figura 2.1 viene riportato il funzionamento dei cookie.

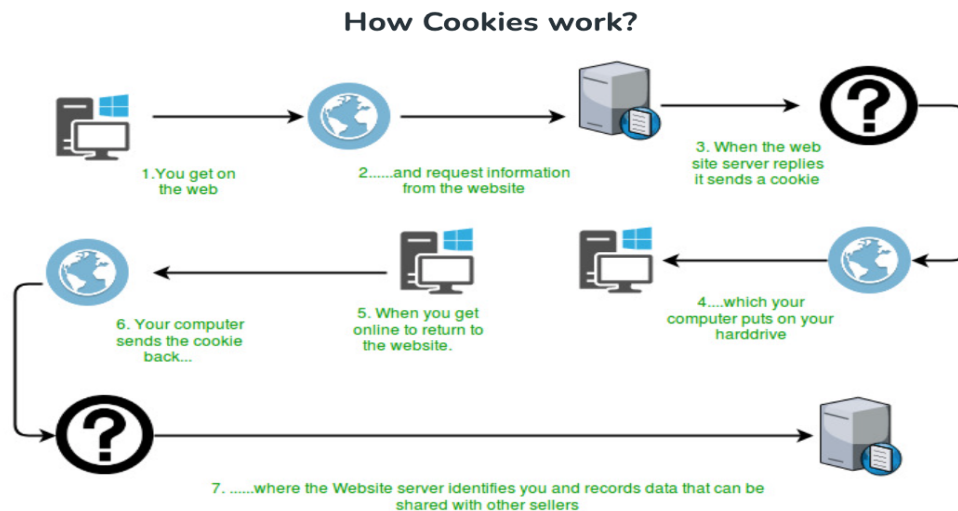


Figura 2.1: Funzionamento del cookie

Come si vede dal diagramma precedente, quando un utente richiede per la prima volta una pagina, il server, insieme alla risorsa, invia un oggetto cookie da memorizzare sul computer del client. Questo oggetto può contenere i dettagli della richiesta. In seguito, se l'utente richiede nuovamente la stessa risorsa, invia, insieme alla richiesta, il cookie memorizzato, che può essere utilizzato dai server per migliorare ulteriormente l'esperienza dell'utente.

Nello specifico, quindi, il server invia un cookie nella risposta HTTP al client, e il browser web deve memorizzare e inviare un cookie ad esso ogni volta che viene effettuata un'ulteriore richiesta al server web. Questo riconoscimento consente, ad esempio, l'implementazione di meccanismi di autenticazione utilizzati per il login, la memorizzazione di dati utili per la sessione di navigazione, come le preferenze per l'aspetto grafico e linguistico del sito, il tracciamento della navigazione dell'utente utile a fini statistici o pubblicitari. Ad esempio per gli acquisti su e-shop, il server può correlare i dati memorizzati in precedenza.

Considerando l'impatto sulla privacy dei navigatori, l'uso dei cookie è classificato e regolamentato dagli ordinamenti giuridici di molti Paesi, anche europei, come l'Italia. La sicurezza dei cookie di autenticazione dipende generalmente dalla sicurezza del sito che rilascia il cookie, dal browser web dell'utente e dal fatto che il cookie sia criptato. A causa delle vulnerabilità della sicurezza, gli hacker potrebbero essere in grado di leggere i dati del cookie e utilizzarli per accedere ai dati dell'utente o al sito web a cui appartiene il cookie utilizzando le credenziali dell'utente.

In base alla loro natura, i cookie scadono dopo un certo periodo di tempo e una nuova comunicazione ha luogo tra il server e il client. In tal modo si ha la possibilità di ottenere informazioni sempre aggiornate.

Infatti, in relazione alla loro durata, i cookie possono essere:

- *Cookie di sessione* in cui la rispettiva data di scadenza corrisponde alla fine della sessione di navigazione, cioè alla chiusura del browser. I cookie di sessione sono utilizzati per ottenere i dati di navigazione di una singola sessione e per analizzare le visite degli utenti alle pagine web. Non è necessario specificarli nelle informative.
- *Cookie persistenti* che vengono inviati dal server al browser dell'utente e rimangono anche dopo la fine della navigazione, finché non scadono o finché l'utente non li cancella. Devono essere specificati nelle informative.

Inoltre, i cookie si distinguono in base alla loro origine, cioè dando attenzione a chi invia il cookie al terminale dell'utente, questi possono essere distinti in:

- *Cookie di prima parte* inviati direttamente al browser dal gestore del sito web visitato.
- *Cookie di terze parti* inviati al browser da ulteriori siti diversi da quello visitato. Vengono quindi trasmessi da aziende terze attraverso alcuni codici aggiunti alla pagina visitata per aggiungere altre funzioni. Pertanto, i cookie installati sul dispositivo dell'utente contattano il fornitore della rete pubblicitaria, indipendentemente dal fatto che l'utente abbia visitato o meno il sito appartenente a quest'ultima.

In genere, i cookie che destano maggiore preoccupazione sono quelli di terze parti. Questo perché sono ampiamente utilizzati e spesso non sono sotto il diretto controllo del proprietario della pagina web, che potrebbe addirittura ignorarne l'esistenza e lo scopo. I cookie di terze parti sono spesso usati per ottenere dati utili a reperire informazioni sulle preferenze degli utenti nonché per condurre ricerche di mercato volte ad identificare gruppi e target specifici.

Sebbene tali cookie diano adito a incertezze in merito alla tutela della privacy, non dovrebbero esserci preoccupazioni di questo tipo in quanto le informazioni sulle abitudini di navigazione sono memorizzate nel cookie e i cookie non sono mai associati a dati personali o sensibili.

Pertanto, il termine "cookie di terze parti" è utilizzato per indicare i cookie impostati da un titolare del trattamento dei dati che non gestisce il sito web che l'utente sta visitando. Al contrario, il termine "cookie di prima parte" si riferisce ai cookie impostati dal titolare del trattamento dei dati che gestisce il sito web che l'utente sta visitando.

2.2 Utilizzi e tipi di cookie

I cookie sono piccoli file di testo che vengono memorizzati sul dispositivo quando viene visitato un sito web. Esistono diversi tipi di cookie, ciascuno con una funzione specifica.

È opportuno, quindi, ricordare che i cookie possono avere differenti finalità e pertanto possono distinguersi in tecnici e non tecnici. I cookie tecnici sono quei cookie che permettono all'utente di navigare su un sito web o di usufruire di un servizio; ad esempio fanno parte di tale categoria i cookie che semplificano le operazioni di acquisto online o quelli che individuano automaticamente la lingua usata dall'utente.

I principali tipi di cookie sono elencati di seguito:

- *Cookie tecnici funzionali*: necessari per il funzionamento del sito web. Comprendono i cookie di sessione, che vengono eliminati automaticamente alla chiusura del browser, e i cookie persistenti, che rimangono sul dispositivo fino a quando non vengono eliminati manualmente o scadono. Questi ci consentono di mantenere l'accesso dell'utente, di ricordare le sue preferenze e di fornire funzionalità di base.

- *Cookie HTTP*: vengono creati utilizzando il protocollo HTTP e sono inviati dal server del sito web al browser dell'utente come intestazione HTTP Set-Cookie. Il browser invia quindi il cookie al server ogni volta che viene richiesta una nuova pagina dal sito web, garantendo il mantenimento delle informazioni sullo stato tra le diverse richieste HTTP.
- *Cookie di profilazione*: utilizzati per creare profili al fine di tracciare il comportamento degli utenti e fornire pubblicità mirata. Questi cookie possono essere utilizzati da terze parti, come inserzionisti e reti pubblicitarie, per mostrare pubblicità pertinenti agli interessi dell'utente.
- *Cookie analitici*: raccolgono informazioni sull'utilizzo del sito web, come il numero di visitatori, le pagine visitate e le fonti di traffico. Le informazioni raccolte vengono utilizzate per analizzare e migliorare le prestazioni del sito.
- *Cookie di preferenza*: utilizzati per memorizzare le preferenze dell'utente relative al sito web, come la lingua preferita, la regione e altre personalizzazioni.
- *Cookie di sicurezza*: identificano e prevengono comportamenti dannosi o potenzialmente pericolosi su un sito web. Tuttavia, se un cookie ha la proprietà Secure, può essere trasmesso solo attraverso una connessione crittografata SSL/TLS (HTTPS). In tal modo si aumenta la sicurezza del cookie e si impedisce il furto di informazioni sensibili.
- *Cookie di terze parti*: impostati da un dominio diverso dal sito web che si sta visitando. Possono essere utilizzati per scopi pubblicitari, analitici e di tracciamento del comportamento.
- *Cookie HttpOnly*: se è contenuto l'attributo HttpOnly, è possibile accedervi solo dal server e il cookie non può essere manipolato da JavaScript. Questo aiuta a prevenire gli attacchi site-to-site scripting e protegge i cookie da accessi non autorizzati.
- *Cookie dei social media*: consentono agli utenti di condividere i contenuti del sito web sui social media e di interagire con i pulsanti di condivisione dei social media.
- *Evercookie, cookie zombie e supercookie*: nello specifico, non sono veri e propri cookie. Non sono salvataggi di dati, ma routine in grado di autoreplicarsi anche dopo che la cache del browser è stata svuotata. Quando ne viene eliminato uno, spesso essi sono in grado di installare copie del cookie originario in un'altra posizione. Questo è il caso di software video per i browser come Microsoft Silverlight o Adobe Flash, che consentono l'accesso agli stessi dati da più posizioni.

È opportuno precisare che un sito web può configurare un cookie sul browser dell'utente solamente nell'ipotesi in cui quest'ultimo abbia espresso il consenso per l'utilizzo. Inoltre, un browser può permettere ad un certo sito web di collegarsi soltanto ai cookie da esso impostati e non a quelli definiti da altri siti web, in virtù del fatto che il cookie è un mezzo di collegamento tra un certo sito web e un determinato utente. Per di più, i cookie sono uno strumento necessario affinché vi sia un'ottima e giusta funzionalità dei siti web. Inoltre, per via della presenza diffusa di tali strumenti, è bene adottare misure idonee all'esecuzione del trattamento dei dati.

2.3 Struttura di un Cookie

Un cookie è sempre composto da un nome, una scadenza, una modalità di accesso e un sistema di sicurezza crittografato. Il nome è la variabile che consente di riconoscere un cookie tra tanti. La scadenza del cookie, invece, indica la sua durata nel tempo, in termini di giorni. Una volta scaduto, il cookie cessa di essere attivo. Esistono, anche, cookie senza scadenza; in questo caso la loro durata non ha limiti e cessano di produrre effetti soltanto quando l'utente li cancella manualmente dal browser.

La struttura e l'impostazione corretta degli attributi di un cookie giocano un ruolo fondamentale per la sua vita. Questi attributi sono, nello specifico, i seguenti:

- *Coppia nome = valore*: rappresenta l'informazione effettiva memorizzata nel cookie. Nè il nome nè il valore devono contenere spazi bianchi o i seguenti caratteri: [] () = , " / ? @ : ;

Un esempio di coppia nome-valore di cookie valida è il seguente:

```
1 Set-Cookie:session-id = 187-4969589-3049309
2
```

- *Dominio*: per impostazione predefinita, un cookie si applica al server da cui proviene. Se un cookie è stato originariamente impostato da `www.test.example.com`, il browser lo rinvierà solo a `www.test.example.com`. Tuttavia, un sito può anche indicare che un cookie si applica a un intero sottodominio, non solo al server originale. Ad esempio, questa richiesta imposta un cookie utente per l'intero dominio `test.example.com`. In questo caso il browser restituirà il cookie non solo a `www.test.example.com`, ma anche a `prova.test.example.com`, `try.test.example.com`, `exam.test.example.com` e a qualsiasi altro host nel dominio `test.example.com`. Tuttavia, un server può impostare i cookie solo per i domini a cui appartiene immediatamente. `www.test.example.com` non può impostare un cookie per `www.testcookie.org`, `example.com` o `.com`, indipendentemente da come viene impostato il dominio.

```
1 Set-Cookie: user = test1; Domain =.test.example.com
2
```

- *Path*: quando si richiede un documento nel sottoalbero dallo stesso server, il client restituisce il cookie. Tuttavia, non utilizza il cookie in altre directory del sito.

```
1 Set-Cookie: user = test1; Path =/ restricted
2
```

- *Scadenza*: il browser dovrebbe rimuovere il cookie dalla sua cache dopo l'espiazione di questa data.

```
1 Set-Cookie: user = test1;
2 expires = Wed, 21-Feb-2025 15:23:00 IST
3
```

- *MaxAge*: tale attributo imposta la scadenza del cookie dopo un certo numero di secondi invece che in un momento specifico. Ad esempio, questo cookie scade un'ora (3.600 secondi) dopo che è stato impostato per la prima volta.

```
1 Set-Cookie: user = "test1"; Max-Age = 3600
2
```

- *HashKeys*: con questo attributo è possibile specificare se il cookie da noi creato è a chiave oppure no. Il formato di questo attributo è di tipo booleano (True o False) ed è di sola scrittura; quindi, non è possibile leggerlo in un secondo momento.
- *Secure*: questo attributo indica se il cookie inviato è sicuro o no.

```
1 Set-Cookie: user = "test1"; Secure=true
2
```

I vari metodi per la costruzione di un cookie sono i seguenti:

- *setDomain()*: imposta il dominio in cui questo cookie è visibile. I domini sono spiegati in dettaglio nella parte relativa agli attributi dei cookie.
- *getDomain()*: restituisce il dominio in cui questo cookie è visibile.
- *setComment()*: specifica lo scopo di questo cookie.
- *setMaxAge()*: specifica il tempo (in secondi) trascorso prima della scadenza del cookie.
- *getMaxAge()*: restituisce la componente di età massima di questo cookie.
- *setPath()*: specifica un percorso per il cookie a cui il client deve restituire il cookie.
- *getPath()*: restituisce il componente percorso di questo cookie.
- *setSecure()*: indica se il protocollo sicuro deve essere utilizzato durante l'invio di questo cookie. Il valore predefinito è false.
- *getSecure()*: restituisce true se questo cookie deve essere inviato tramite un protocollo sicuro, altrimenti false.
- *getName()*: restituisce il nome del cookie.
- *setValue()*: assegna un nuovo valore al cookie dopo l'inizializzazione.
- *getValue*: restituisce il valore del cookie.
- *getVersion()*: restituisce 0 se il cookie è conforme alle specifiche originali di Netscape; 1 se il cookie è conforme alle RFC 2965/2109.
- *setVersion()*: utilizzato per impostare la versione del protocollo del cookie utilizzato da questo cookie.
- *clone()*: restituisce una copia di questo cookie.

Presentiamo, ora, un esempio di come viene costruito un cookie in javascript. Il codice memorizza un cookie nel browser quando l'utente lo richiede per la prima volta e poi per le richieste successive visualizza quelli memorizzati.

```
1 import java.io.IOException;
2 import java.io.PrintWriter;
3 import java.util.List;
4 import javax.servlet.ServletException;
5 import javax.servlet.annotation.WebServlet;
6 import javax.servlet.http.Cookie;
7 import javax.servlet.http.HttpServlet;
```



```
8 import javax.servlet.http.HttpServletRequest;
9 import javax.servlet.http.HttpServletResponse;
10
11 /**
12 * Servlet implementation class cookieTest
13 */
14 @WebServlet("/cookieTest")
15 public class cookieTest extends HttpServlet
16 {
17     private static final long serialVersionUID = 1L;
18
19     /**
20     * @see HttpServlet#HttpServlet()
21     */
22     public cookieTest() {
23         super();
24         // TODO Auto-generated constructor stub
25     }
26
27     /**
28     * @see HttpServlet#doGet(HttpServletRequest request,
29     HttpServletResponse response)
30     */
31     protected void doGet(HttpServletRequest request,
32     HttpServletResponse response)
33     throws ServletException, IOException
34     {
35
36         response.setContentType("text/html");
37
38         // Create a new cookie with the name test cookie
39
40         // and value 123
41         Cookie cookie = new Cookie("test_cookie", "123");
42
43         // setComment() method
44         cookie.setComment("Just for testing");
45
46         // setDomain() method
47
48         // cookie.setDomain("domain");
49
50         // setMaxAge() method
51         cookie.setMaxAge(3600);
52
53         // setPath() method
54         cookie.setPath("/articles");
55
56         // setSecure() method
57         cookie.setSecure(false);
58
59         // setValue() method
60         cookie.setValue("321");
61
62         // setVersion() method
63         cookie.setVersion(0);
64         response.addCookie(cookie);
65         PrintWriter pw = response.getWriter();
66         pw.print("<html><head></head><body>");
67         Cookie ck[] = request.getCookies();
68         if (ck == null) {
69             pw.print("<p>This is first time the page is requested.</p>");
```

```
70     pw.print("<p>And therefore no cookies found</p>");
71         </body></html>");
72     } else {
73         pw.print("<p>Welcome Again...Cookies found</p>");
74         for (int i = 0; i < ck.length; i++) {
75
76             // getName() method
77             pw.print("<p>Name : " + ck[i].getName() + "</p>");
78
79             // getValue() method
80             pw.print("<p>Value : " + ck[i].getValue() + "</p>");
81
82             // getDomain() method
83             pw.print("<p>Domain : " + ck[i].getDomain() + "</p>");
84
85             // getPath() method
86             pw.print("<p>Name : " + ck[i].getPath() + "</p>");
87
88             // getMaxAge() method
89             pw.print("<p>Max Age : " + ck[i].getMaxAge() + "</p>");
90
91             // getComment() method
92             pw.print("<p>Comment : " + ck[i].getComment() + "</p>");
93
94             // getSecure() method
95             pw.print("<p>Name : " + ck[i].getSecure() + "</p>");
96
97             // getVersion() method
98             pw.print("<p>Version : " + ck[i].getVersion() + "</p>");
99         }
100     pw.print("<body></html>");
101
102     }
103     pw.close();
104 }
105
106
107 protected void doPost(HttpServletRequest request,
108                       HttpServletResponse response)
109     throws ServletException, IOException
110 {
111     doGet(request, response);}}
```

Source Code 2.1: Script costruzione cookie

Nella figura 2.2 è mostrato l'output per la prima richiesta mentre, la Figura 2.3 mostra l'output della seconda richiesta:

```
This is first time the page is requested.
And therefore no cookies found.
```

Figura 2.2: Output della prima richiesta

```
Welcome Again...Cookies found
Name :test_cookie
Value :321
Domain :null
Name :null
Max Age :-1
Comment :null
Name :false
Version :0
```

Figura 2.3: Output della seconda richiesta

2.4 Rispetto del GDPR e tutela della privacy (Cookie Law)

Il regolamento generale europeo sulla protezione dei dati (GDPR) è stato progettato per centralizzare la protezione dei dati per gli utenti europei ed è pienamente applicabile dal 25 maggio 2018. In poche parole, il GDPR chiarisce le modalità di trattamento dei dati personali, comprese le modalità di raccolta, utilizzo, protezione e condivisione.

Il GDPR si applica quando la base operativa dell'organizzazione si trova nell'UE (indipendentemente dal fatto che il trattamento avvenga o meno nell'Unione Europea); se l'organizzazione, senza sede nell'UE, fornisce beni o servizi (anche gratuitamente) a cittadini europei. Esempio sono le autorità pubbliche, aziende private, persone fisiche o organizzazioni senza scopo di lucro, organizzazioni che controllano il comportamento di persone residenti nell'UE, anche se non hanno sede nell'Unione Europea.

Questo ampio campo di applicazione copre praticamente tutte le attività, per cui si può concludere che il GDPR si applica indipendentemente dal fatto che l'organizzazione abbia o meno sede nell'UE.

Infatti, un'idea sbagliata comune è quella di pensare che solo gli utenti dell'UE siano coperti dal GDPR. In realtà, il regolamento si applica anche agli utenti extra-UE se il responsabile del trattamento dei dati ha sede nell'Unione Europea. Pertanto, se si è un responsabile del trattamento con sede nell'UE, si devono applicare gli standard del GDPR a tutti gli utenti.

La Direttiva e-Privacy (Cookie Law) è stata progettata ed è attualmente in fase di attuazione per implementare linee guida rigorose sulla protezione dei dati tramite mezzi elettronici, tra cui il marketing via e-mail e l'uso dei cookie.

La Cookie Law si applica non solo ai cookie, ma più in generale a tutte le tecnologie che memorizzano o accedono a informazioni sul dispositivo dell'utente (ad esempio, pixel tag, impronte digitali del dispositivo, identificatori unici). Per semplicità, tutte queste tecnologie, compresi i cookie, sono più comunemente definite strumenti di tracciamento (o tracker). Tuttavia, la direttiva ePrivacy è una normativa che opera in collaborazione con il GDPR.

Più precisamente, se si utilizzano i cookie, la Cookie Law deve essere rispettata prima del GDPR. Questo perchè essa, nota in termini giuridici come "lex specialis", ha la precedenza sul GDPR.

La direttiva stabilisce alcuni obiettivi e linee guida concordate che gli Stati membri implementano nelle loro leggi nazionali. I regolamenti, invece, sono giuridicamente vincolanti per tutti gli Stati membri dal momento in cui entrano in vigore e vengono attuati secondo le regole stabilite a livello europeo. In generale, si rientra nel campo di applicazione della cookie law se il proprietario del sito o gli utenti risiedono in Europa e se si fa uso di cookie o tecnologie simili per una pagina web o un'app. Tuttavia, la Direttiva e-Privacy sarà sostituita dal Regolamento e-Privacy, che dovrebbe essere finalizzato nel prossimo futuro e disciplinerà i requisiti per l'uso dei cookie e delle comunicazioni elettroniche in coordinamento con il GDPR.

Tuttavia, è molto probabile che il regolamento confermerà disposizioni simili a quelle della direttiva e implementerà molte delle stesse linee guida.

Secondo la Cookies Law, le organizzazioni che si rivolgono ai cittadini dell'UE devono informare gli utenti sulle attività di raccolta dei dati che verranno effettuate e fornire loro la possibilità di scegliere se acconsentire o meno. Ciò significa che se un sito o un'app (o qualsiasi servizio di terze parti utilizzato su di esso) utilizza cookie o tecnologie simili, si deve ottenere un consenso valido prima di installare i cookie, a meno che tali cookie non rientrino nella categoria dei cookie esenti come i cookie tecnici e statistici ma non a scopo di profilazione.

Le linee guida da tenere in considerazione sono le seguenti:

- Mostrare un cookie banner alla prima visita dell'utente.
- Predisporre una cookie policy che contenga tutte le informazioni richieste.
- Fornire agli utenti strumenti o informazioni per accettare, rifiutare o ritirare il proprio consenso. Ad eccezione dei cookie esenti, i cookie non possono essere installati se l'utente non ha dato un consenso informato ed esplicito.

2.5 Come i cookie vengono regolamentati dallo stato Italiano

Come descritto precedentemente, la Cookie Law italiana si allinea a quello che viene già espresso a livello europeo. Nello specifico verranno riportate le principali differenze in merito nazionale.

Per quanto riguarda l'utilizzo dei cookie e degli altri identificatori tecnici, il titolare del trattamento non è obbligato ad utilizzarli, anche se inseriti nell'informativa generale, in quanto il loro utilizzo costituisce un'ipotesi codificata che esonera l'interessato dall'obbligo di acquisire il suo consenso. Il titolare sarà soggetto solo all'obbligo di fornire un'informativa specifica. Se invece i cookie e gli altri strumenti di tracciamento sono utilizzati per finalità non tecniche, il consenso del contraente o dell'utente deve essere acquisito, in ogni caso, previa informazione. Il tutto in base alla norma dell'art. 122 del codice:

- *“1. L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad 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 dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente.*
- *2. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.*
- *2-bis. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente”¹.*

¹Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 - Normativa applicabile <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876>

Questa disposizione è stata introdotta nel diritto nazionale a seguito del recepimento della direttiva ePrivacy prima che il regolamento entrasse pienamente in vigore. La direttiva e le norme di diritto nazionale che la recepiscono si applicano attualmente in alcune aree relative al trattamento dei dati effettuato nel contesto delle comunicazioni elettroniche.

Si reputa, tuttavia, opportuno fornire taluni chiarimenti in relazione all'utilizzo del c.d. scrolling ai fini della raccolta del consenso all'installazione e all'utilizzo di cookie ed altri strumenti di tracciamento nonché all'utilizzo del c.d. cookie wall.

A riguardo viene riportato il punto 32 del regolamento *"Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe, pertanto, configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso"*²

L'EDPB (European Data Protection Board) ha, inoltre, chiarito che il semplice scrolling non è mai idoneo, di per sé, ad esprimere compiutamente la manifestazione di volontà dell'interessato volta ad accettare di ricevere il posizionamento, all'interno del proprio terminale, di cookie diversi da quelli tecnici e, dunque, non equivale, in sé considerato, al consenso "in nessuna circostanza"(4).

Il Garante condivide naturalmente l'opinione dell'EDPB: il semplice "scroll down" del cursore di pagina è inadatto in sé alla raccolta, da parte del titolare del trattamento, di un idoneo consenso all'installazione e all'utilizzo di cookie di profilazione ovvero di altri strumenti di tracciamento.

Inoltre, il Garante, stabilisce che l'attività di profilazione dei singoli individui, o gruppi di soggetti può svolgersi col solo impiego di dati anonimi o non identificativi (per esempio un codice numerico), senza alcuna relazione tra i dati che consentono di identificare gli interessati e le informazioni circa la loro sfera personale, quali preferenze, bisogni, gusti, abitudini, stili di vita. Non si ritiene lecito adoperare e conservare dati personali o identificativi per perseguire le finalità del trattamento, soprattutto nel caso di profilazione della clientela per categorie omogenee. Ciò in virtù del fatto che il Garante ha riscontrato nell'attività di profilazione dei clienti una possibile invasione nella sfera della riservatezza del soggetto interessato; perciò gli operatori commerciali nelle attività di analisi e valutazione commerciale devono attenersi a determinate regole e condotte che consentano di non risalire all'identità del singolo cliente.

²Linee guida cookie e altri strumenti di tracciamento - Le modalità per l'acquisizione del consenso online alla luce di alcuni opportuni chiarimenti e nuove raccomandazioni - Il c.d. "scrolling" e il cookie wall - 10 giugno 2021 <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876>

Il consent di Google per i cookie

In questo capitolo si parlerà a parlare nel dettaglio del Google Consent Mode, metodo con cui Google riesce a gestire i cookie di terze parti anche in caso di rifiuto dei cookie da parte dell'utente. Esso rappresenta uno strumento molto utile ai fini di non perdere conversioni da parte di utenti o per affinare le conversioni, con tale modo i cookie vengano inviati separatamente ai principali strumenti di Google per il marketing (Google Ads) e per analisi statistiche (Google Analytics).

3.1 Cosa si intende per Google Consent Mode

Google Consent Mode è una funzionalità introdotta da Google per affrontare le sfide legate al consenso dei cookie e al rispetto della privacy degli utenti in conformità con le normative come il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea.

In sostanza, Google Consent Mode è un framework che permette agli editori di siti web di adattare il funzionamento dei loro strumenti di misurazione e di pubblicità di Google in base al livello di consenso ottenuto dagli utenti per l'utilizzo dei cookie. Questa funzionalità è stata introdotta per rispondere alle nuove restrizioni imposte dalle normative sulla privacy, che richiedono agli editori di ottenere il consenso esplicito degli utenti prima di raccogliere determinati dati tramite i cookie.

Attraverso Google Consent Mode, gli editori possono configurare le impostazioni dei propri siti web in modo che le misurazioni e le attività di pubblicità di Google vengano adattate in base al consenso dell'utente. Ciò significa che se un utente non ha dato il proprio consenso all'uso dei cookie, le funzionalità di monitoraggio e di pubblicità di Google verranno limitate per rispettare la sua scelta.

Google Consent Mode utilizza tecnologie come l'API del consenso dell'Interactive Advertising Bureau (IAB) e le funzionalità di gestione dei tag di Google Tag Manager per implementare queste regole di consenso e adattare dinamicamente il comportamento dei cookie in base alle scelte degli utenti.

Infatti, questa funzionalità è un innovativo modo messo a disposizione di chi gestisce il sito web per rilevare le conversioni e acquisire dati analitici, mantenendo al contempo la piena conformità al GDPR nell'utilizzo di servizi come Google Analytics, Google Tag Manager (GTM) e Google Ads. Quindi, il Google Consent mode colma il divario tra la privacy dei dati e la pubblicità digitale, facendo in modo che i dati analitici e le attività di marketing di un sito web possano funzionare in modo fluido, sulla base della scelta di consenso di ciascun

utente specifico. Di conseguenza, Google Consent Mode consente di gestire senza problemi l'analisi dei siti web e le attività di marketing in base alle scelte di consenso di ciascun utente.

La modalità di consenso di Google è un passo importante verso la costruzione di un'economia di internet più sostenibile, abbandonando la raccolta su larga scala di dati personali per passare a un sistema dinamico e consensuale che bilanci meglio entrambi gli elementi. Nello stesso tempo si impegna a rispettare la privacy e la dignità dei singoli utenti senza sconvolgere i modelli di business che caratterizzano gran parte del mercato di Internet di oggi.

Nella Figura 3.1 viene sintetizzato il funzionamento del Google Consent Mode in entrambi gli scenari possibili.

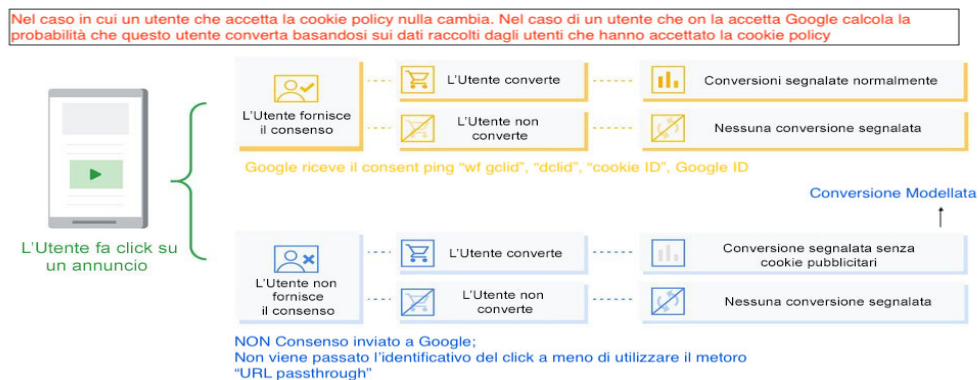


Figura 3.1: Sintesi del funzionamento di Google Consent Mode

3.2 Funzionamento di Google Consent Mode (GCM)

La modalità di consenso permette di comunicare a Google lo stato del consenso all'uso dei cookie o degli identificatori di app, concesso o meno dagli utenti. I tag modificano il loro comportamento e rispettano le scelte degli utenti. La GCM interagisce con la piattaforma di gestione del consenso (CMP) o con l'implementazione personalizzata per ottenere il consenso dei visitatori, ad esempio un banner del consenso all'uso dei cookie. La modalità di consenso riceve le scelte dell'utente relative al consenso dal banner o dal widget dei cookie e adatta in modo dinamico il comportamento di Analytics, Google Ads e tag di terze parti che creano o leggono i cookie.

Considerando in dettaglio, i tipi di consenso che vengono gestiti da Google Consent Mode, sono mostrati nella Figura 3.2.

Quando i visitatori negano il consenso, i tag inviano ping a Google anziché memorizzare i cookie. Se la GCM è attivata, i prodotti di misurazione di Google assicurano che lo stato di autorizzazione del visitatore sia mantenuto su tutte le pagine a cui il visitatore accede. Se il consenso viene rifiutato, il tag attivato non memorizza i cookie, ma trasmette informazioni minime sull'attività dell'utente. Lo stato di consenso e l'attività dell'utente vengono, quindi, trasmessi ai server di Google senza far utilizzo di cookie veri e propri, ma inviando i seguenti tipi di ping (indicatori):

- *Ping relativi allo stato del consenso per i tag Google Ads e Floodlight:* vengono utilizzati per comunicare lo stato predefinito del consenso configurato e l'aggiornamento dello stato quando i visitatori accordano o rifiutano il consenso per ciascun tipo di autorizzazione, come ad esempio "ad_storage" e "analytics_storage". Questi segnali, che riflettono lo

Tipo di consenso	Descrizione
ad_storage	Consente l'archiviazione di informazioni (ad esempio i cookie) correlate alla pubblicità.
analytics_storage	Consente l'archiviazione di informazioni (ad esempio i cookie) correlate all'analisi, come la durata della visita.
functionality_storage	Consente l'archiviazione di informazioni che supportano la funzionalità del sito web o dell'app, ad esempio le impostazioni relative alla lingua.
personalization_storage	Consente l'archiviazione di informazioni correlate alla personalizzazione, ad esempio i consigli sui video
security_storage	Consente l'archiviazione di informazioni relative alla sicurezza, ad esempio la funzionalità di autenticazione, la prevenzione delle frodi e altre protezioni per gli utenti

Figura 3.2: Tipi di consenso gestiti da Google Consent Mode

stato del consenso, vengono trasmessi da ogni pagina visitata dagli utenti in cui la modalità di consenso risulta attivata. Inoltre, vengono attivati anche per alcuni tag nel caso in cui lo stato cambi da "rifiutato" a "concesso", ad esempio quando un visitatore attiva l'opzione attraverso una finestra di dialogo per il consenso.

- *Ping di conversione*: utilizzati per indicare il verificarsi di una conversione.
- *Ping di Google Analytics*: trasmessi da ciascuna pagina di un sito web in cui è stato implementato Google Analytics durante il caricamento della pagina e al momento della registrazione degli eventi.

I ping descritti precedentemente possono includere:

- *Informazioni funzionali*: come le intestazioni aggiunte passivamente dal browser, il timestamp, lo user agent (solo per il web) o il referrer (parametro che esprime la provenienza da quale traffico arriva l'utente).
- *Informazioni aggregate/non identificative*: cioè un'indicazione che specifica se la pagina corrente, o una pagina precedente nella navigazione dell'utente sul sito, includeva o meno informazioni sui clic sugli annunci nell'URL. Fanno parte di questa categoria anche le informazioni booleane sullo stato del consenso, il numero casuale generato a ogni caricamento pagina nonché le informazioni sulla piattaforma per il consenso utilizzata dal proprietario del sito.

3.3 Utilizzo dei cookie nella Google Consent Mode

Google Consent Mode utilizza i cookie in modo specifico per gestire il consenso dell'utente e adattare il funzionamento dei servizi di Google in base alle preferenze di consenso espresse dagli utenti. A seconda delle scelte di consenso da parte del navigatore, Google Consent Mode adatta il comportamento dei cookie utilizzati dai servizi di Google. Ad esempio, se l'utente ha negato il consenso all'uso di cookie per la pubblicità mirata, i cookie legati alla pubblicità verranno limitati o non verranno impostati.

Nel dettaglio i ping di conversione e relativi al consenso possono includere i seguenti comportamenti a seconda dello stato delle impostazioni relative ad esso e della configurazione dei tag.

I comportamenti predefiniti funzionano come se venissero concesse tutte le opzioni di consenso, nella Figura 3.3 viene riassunto cosa accade in una situazione ottimale, quando l'utente accetta tutti i cookie.

<code>ad_storage='granted'</code> e <code>analytics_storage='granted'</code>	
Web	App mobile
<ul style="list-style-type: none"> • I cookie per la pubblicità possono essere letti e scritti. • Vengono raccolti gli indirizzi IP. • Viene raccolto l'URL della pagina web, incluse le informazioni relative ai clic sugli annunci nei parametri URL (ad esempio, GCLID/DCLID). • I cookie di terze parti precedentemente impostati su google.com e doubleclick.net e i cookie di conversione proprietari (ad esempio, _gcl_*) sono accessibili. 	<ul style="list-style-type: none"> • Gli identificatori di pubblicità (ad esempio, ID pubblicità/IDFA) possono essere raccolti. • Viene raccolto l'ID istanza dell'app generato dall'SDK di Google Analytics for Firebase.

Figura 3.3: Situazione ottimale, l'utente ha accettato tutti i cookie

Quando, invece, non vengono concessi tutti i cookie, ci sono molteplici scenari ai quali va incontro l'utente. Nelle Figure 3.4 , 3.5 e 3.6 vengono mostrati le varie situazioni possibili.

<code>ad_storage='denied'</code>	
Web	App mobile
<ul style="list-style-type: none"> • Nessun nuovo cookie relativo alla pubblicità può essere scritto. • Nessun cookie proprietario per la pubblicità esistente può essere letto. • Le richieste vengono inviate tramite un dominio diverso per evitare che i cookie di terze parti precedentemente impostati vengano inviati nelle intestazioni delle richieste. • Google Analytics non legge né scrive cookie di Google Ads e le funzionalità di Google Signals non accumuleranno dati relativi a questo traffico. • Viene raccolto l'URL completo della pagina. Potrebbero essere incluse le informazioni relative ai clic sugli annunci nei parametri URL (ad es. GCLID/DCLID), queste verranno utilizzate solo per effettuare una misurazione accurata del traffico. • Gli indirizzi IP vengono utilizzati per ricavare il paese IP, ma mai registrati dai nostri sistemi Google Ads e Floodlight. Inoltre, vengono immediatamente eliminati al momento della raccolta. Nota: Google Analytics raccoglie gli indirizzi IP nell'ambito delle normali comunicazioni internet. 	<ul style="list-style-type: none"> • Nessun ID pubblicità/IDFA può essere raccolto. • Le funzionalità di Google Signals non accumuleranno dati per questo traffico. • Gli indirizzi IP vengono utilizzati per ricavare il paese IP, ma mai registrati dai sistemi Google Ads e Floodlight. Inoltre, vengono immediatamente eliminati al momento della raccolta. Nota: Google Analytics raccoglie gli indirizzi IP nell'ambito delle normali comunicazioni internet.

Figura 3.4: Cookie relativi a Google Ads non accettati

Quando "`analytics_storage='denied'`", ping senza cookie vengono inviati a Google Analytics. Nessun cookie di Analytics viene impostato, raggiunto o letto dal dispositivo. Di conseguenza, i ping senza cookie vengono resi anonimi e non consentono di identificare gli eventi di Google Analytics.

I ping senza cookie, nell'ambito delle normali comunicazioni HTTP/browser, possono includere le seguenti informazioni: user agent, risoluzione dello schermo, indirizzo IP. Si noti che Google Analytics 4 non memorizza né registra gli indirizzi IP.

<code>ad_storage='denied' e ads_data_redaction='true'</code>	
Web	
<ul style="list-style-type: none"> • Nessun nuovo cookie relativo alla pubblicità può essere scritto. • Nessun cookie per la pubblicità esistente può essere letto. • Le richieste vengono inviate tramite un dominio diverso per evitare che i cookie di terze parti precedentemente impostati vengano inviati nelle intestazioni delle richieste. • Google Analytics non legge né scrive cookie di Google Ads e le funzionalità di Google Signals non accumuleranno dati relativi a questo traffico. • In Google Analytics viene raccolto l'URL completo della pagina. Nei parametri URL (ad esempio GCLID/DCLID) potrebbero essere incluse le informazioni relative ai clic sugli annunci (ad esempio GCLID/DCLID), queste verranno utilizzate solo per effettuare una misurazione accurata del traffico. In Google Ads, gli identificatori dei clic sugli annunci (ad esempio GCLID/DCLID) nei ping relativi a consenso e conversioni vengono oscurati. • Gli indirizzi IP vengono utilizzati per ricavare il paese IP, ma mai registrati dai sistemi Google Ads e Floodlight. Inoltre, vengono immediatamente eliminati al momento della raccolta. Nota: Google Analytics raccoglie gli indirizzi IP nell'ambito delle normali comunicazioni internet. 	

Figura 3.5: Cookie relativi a Google Ads e al salvataggio non accettati

<code>analytics_storage='denied'</code>	
Web	App mobile
<ul style="list-style-type: none"> • I cookie di Analytics proprietari non vengono letti né scritti. • I ping senza cookie verranno inviati a Google Analytics per scopi di misurazione futuri. Google Analytics 4 utilizzerà ping senza cookie per la definizione di modelli. • Questa impostazione non influisce su Google Optimize. 	<ul style="list-style-type: none"> • Nessun IDFV può essere raccolto. • Gli eventi senza identificatori utente o dispositivo verranno inviati a Google Analytics per scopi di misurazione futuri. Google Analytics 4 utilizzerà questi eventi per la definizione di modelli.

Figura 3.6: Cookie relativi a Google Analytics non accettati

Se un inserzionista imposta altri campi, ad esempio "user_id" e dimensioni personalizzate, queste informazioni vengono inviate normalmente grazie al cookie. I dati raccolti nel ping senza cookie vengono utilizzati per la definizione di modelli comportamentali e di conversione per colmare le lacune nei dati.

Ai fini di una perfetta implementazione ci sono delle best practice direttamente consigliate da Google, queste sono le seguenti:

- Impostazione di uno stato iniziale con i valori predefiniti stabiliti dall'organizzazione. Lo stato del consenso predefinito viene applicato la prima volta che un visitatore visualizza una pagina del sito web.
- Implementazione del caricamento dei tag di pagina prima dell'apertura della finestra di dialogo per il consenso.
- Caricamento dei tag Google in tutti i casi, non solo se l'utente dà il consenso. Se il consenso viene negato, Google riceve ping senza cookie. Nelle proprietà Google

Analytics 4, i ping senza cookie consentono di definire modelli comportamentali e di conversione per colmare le lacune nei dati.

- Le opzioni di consenso dovrebbero essere mostrate al visitatore appena possibile. Oppurtuno aggiornare lo stato del consenso quando il visitatore indica la propria scelta.
- È opportuno offrire agli utenti la possibilità di negare o concedere il consenso per ogni tipo di spazio di archiviazione utilizzato dai tag su un sito web. Ad esempio, un utente potrebbe concedere il consenso per i cookie di Analytics e negarlo per quelli per la pubblicità.
- A cause delle leggi sulla privacy correnti, che sono specifiche per regione, si deve configurare uno stato predefinito da applicare a determinate regioni anziché a tutti i visitatori. Soprattutto se l'organizzazione richiede che lo stato predefinito sia "negato", l'applicazione di "negato" solo ai visitatori della regione appropriata evita la perdita di misurazioni precise per tutte le altre regioni.

In conclusione, viene mostrata una panoramica sulle due possibilità di implementazione della Google Consent Mode, la modalità avanzata e quella di base.

Se si sceglie di implementare la modalità di consenso bloccando i tag Google finché la finestra di dialogo per il consenso non viene visualizzata e gli utenti non acconsentono, non si usufruirà di tutti i vantaggi della modalità di consenso. Ad esempio, nella proprietà GA4 non si riceveranno dati modellati per colmare le lacune per i dati osservati mancanti quando gli utenti negano il consenso. Che si scelga di bloccare i tag (implementazione di base) o di sbloccare i tag (implementazione avanzata), i tag Google modificano il loro comportamento in base allo stato del consenso degli utenti.

Nella Figura 3.7 vengono sintetizzate questi due tipi di implementazione:

	Implementazione avanzata	Implementazione di base
Comportamento dei tag	<ul style="list-style-type: none"> • I tag Google vengono caricati prima della finestra di dialogo per il consenso • I tag inviano ping senza cookie quando il consenso all'uso dei cookie viene rifiutato 	<ul style="list-style-type: none"> • I tag Google vengono bloccati finché non viene concesso il consenso
Creazione di modelli di comportamento in GA4	✓	
Definizione del modello di conversione in GA4	✓	
Definizione del modello di conversione in Google Ads	✓	✓*

Figura 3.7: Cookie relativi a Google Analytics non accettati

Per quanto riguarda la definizione del modello di conversione i Google Ads nell'implementazione di base, quando si bloccano i tag, la definizione del modello di conversione in Google Ads si basa su un modello generale, con i valori di conversione modellati solo sugli utenti che danno il consenso. Questa pratica è meno precisa della definizione del modello che si ottiene dall'implementazione avanzata, in quanto il modello viene addestrato sia sui dati osservati dagli utenti che concedono il consenso sia sui ping senza cookie provenienti dagli utenti che negano il consenso.

3.4 Script e metodi di applicazione della Google Consent Mode.

L'attivazione della modalità di consenso cambia in base alla struttura dei siti web e delle app. Ciò dipende dall'implementazione per ottenere il consenso e dalla piattaforma di tagging che si utilizza.

Ci sono vari metodi per l'attivazione della modalità di consenso; se si vuole utilizzare una programmazione minima, la scelta ricadrà sull'uso di Google Tag Manager utilizzando i modelli della community. I partner CMP (Cookie Management Platform) forniscono modelli di GTM e le istruzioni per attivare la modalità di consenso tramite la loro integrazione.

Nella figura 3.8 sono mostrate le piattaforme CMP supportate e le integrazioni disponibili per ognuno di esse.

L'attivazione e l'utilizzo della modalità di consenso dipendono dall'implementazione per ottenere il consenso e dalla piattaforma di tagging (Google Tag Manager (GTM) o tag Google) che si utilizzano. In particolare

- Le piattaforme di gestione del consenso (CMP) che supportano la modalità di consenso di Google forniscono: modelli di Tag Manager nella Galleria modelli della community da utilizzare per creare tag per la gestione del consenso; codici JavaScript per i siti che utilizzano `gtag.js` per gestire il consenso.
- Per le implementazioni e le CMP personalizzate che non supportano la modalità di consenso, se si adotta GTM, si consiglia di creare un modello utilizzando le API di consenso di Tag Manager. Se si utilizza invece, il `gtag.js`, si dovrà aggiungere manualmente il codice di consenso a ogni pagina del sito come comandi diretti o in uno snippet HTML personalizzato.

Quando si scrivono i modelli o tag HTML personalizzati, non è garantito che i comandi eseguiti nei callback o nei comandi che utilizzano `gtag()` siano disponibili prima dell'attivazione del trigger successivo. Per assicurarsi che le informazioni sul consenso siano disponibili il più rapidamente possibile, si utilizzino modelli di tag che usino le API Tag Manager per il consenso per impostare gli stati del consenso.

3.4.1 Monitoraggio dello stato del consenso

Lo stato del consenso predefinito deve essere immediatamente impostato al caricamento della pagina in base alle impostazioni predefinite richieste dalla propria organizzazione. La CMP o la soluzione di gestione del consenso personalizzata devono, quindi, chiedere al visitatore di concedere o negare il permesso per i tipi di consenso applicabili. Poiché la modalità di consenso non memorizza le scelte relative al consenso, è fondamentale che la soluzione di gestione del consenso emetta un comando di aggiornamento della modalità di consenso in base alle scelte dell'utente il prima possibile su ogni pagina dopo l'espressione della preferenza.

Il primo passo, quindi, è quello di configurare le impostazioni predefinite con lo stato di "granted", se ciò non è impostato esplicitamente. È consigliato impostare un valore predefinito per ogni tipo di archiviazione utilizzato. La responsabilità di assicurarsi che, per ciascuno dei prodotti di misurazione, la modalità di consenso sia impostata in modo da rispettare i criteri dell'organizzazione appartiene al proprietario del sito o dell'app. Un punto fondamentale è che il comando "consent" sia richiamato in ogni pagina del sito.

Per modificare le funzionalità di misurazione predefinite, è necessario utilizzare il comando `gtag('consent', 'default', ...)` in ogni pagina del sito prima di qualsiasi

Strumento per il consenso	Tipi di consenso supportati	Modello della community di Tag Manager disponibile	Integrazione con le chiamate di aggiornamento del consenso	Integrazione con le chiamate predefinite per il consenso
Commanders Act	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (modello GTM integrato + modello TrustCommander)
ConsentManager	ad_storage analytics_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)
Cookie Information A/S	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)
Cookiebot (Cybot)	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)
CookieYes	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)
Crownpeak	ad_storage analytics_storage		✓	✓ (fornita solo come esempio di codice in-page)
Didomi	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (integrazione completa di GTM + soluzioni non GTM)
iubenda	ad_storage analytics_storage functionality_storage personalization_storage security_storage		✓	✓ (fornita solo come esempio di codice in-page)
LiveRamp	ad_storage analytics_storage		✓	✓ (fornita solo come esempio di codice in-page)
OneTrust	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)
Osano	ad_storage analytics_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)
Sourcepoint	ad_storage analytics_storage functionality_storage personalization_storage security_storage		✓	✓ (fornita solo come esempio di codice in-page)
Termly	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)
Usercentrics	ad_storage analytics_storage functionality_storage personalization_storage security_storage	✓	✓	✓ (modello GTM integrato + esempio di codice per gtag.js)

Figura 3.8: Piattaforme CMP supportate e integrate

comando che invia dati di misurazione (come config o event). Ad esempio, per rifiutare "ad_storage" e "analytics_storage" per impostazione predefinita, si devono specificare le impostazioni nei parametri "consent", come si osserva nel listato sottostante.

```
1 gtag('consent', 'default', {
2   'ad\textunderscorestorage': 'denied',
3   'analytics\textunderscorestorage': 'denied'
4 });
```

Il passo successivo, è quello dell'aggiornamento dello stato del consenso, cioè quando gli utenti specificano il consenso o modificano la propria scelta su di esso, aggiornando, così, il comportamento di misurazione. Lo stato del consenso verrà modificato solo per i campi forniti alla chiamata "update". Nell'esempio riportato di seguito, è stato modificato solo il valore "ad_storage". Se il criterio "analytics_storage" è stato impostato su "denied", sarà comunque negato dopo questa chiamata.

```
1 gtag('consent', 'update', {
2   'ad\textunderscorestorage': 'granted'
3   'analytics\textunderscorestorage' : 'denied'
4 });
```

Si trasmetteranno, quindi, aggiornamenti il prima possibile su ogni pagina. Dopo che un utente ha concesso il consenso, si mantiene la sua scelta e si chiama il comando "update"; poi, di conseguenza, la stessa azione avverrà nelle pagine successive. Poiché la modalità di consenso non memorizza le scelte relative ad esso, è fondamentale che la soluzione di gestione del consenso fornisca un comando di aggiornamento della modalità di consenso in base alle scelte dell'utente il più presto possibile, in ogni pagina dopo le scelte dell'utente.

È importante tenere conto delle possibili integrazioni con le varie CMP che possono essere presenti. Infatti, se la piattaforma CMP viene caricata in modo asincrono, potrebbe non essere sempre eseguita prima dei tag Google. Per gestire situazioni di questo tipo, si specifica il comando "wait_for_update" insieme a un valore di millisecondi, per controllare quanto tempo attendere prima di inviare i dati.

Ad esempio, per negare "ad_storage" in una determinata pagina per impostazione predefinita, ma per consentire alla CMP di aggiornare lo stato del consenso, si utilizza "wait_for_update". Nel codice seguente, "ad_storage" è impostato su "denied" per impostazione predefinita, e allo strumento di consenso sono assegnati 500 millisecondi per chiamare "gtag('consent', 'update', ...)" prima che i tag vengano attivati.

```
1 gtag('consent', 'default', {
2   'ad_storage': 'denied',
3   'wait_for_update': 500
4 });
```

3.4.2 Funzionalità di consenso avanzate

Le funzionalità avanzate del consenso includono la possibilità di:

- Impostare il comportamento per una regione geografica.
- Trasmettere informazioni su clic sugli annunci, ID cliente e ID sessione negli URL quando gli utenti non hanno concesso il consenso per i cookie.
- Oscurare completamente le informazioni sugli annunci quando gli utenti negano il consenso per i cookie degli annunci.

Nel dettaglio, per modificare il comportamento predefinito dei tag per gli utenti di determinate regioni, si specifica un'area geografica nel comando di consenso. Se si specifica

un valore di regione, è possibile perfezionare le impostazioni predefinite in base alla posizione geografica degli utenti.

L'esempio seguente imposta "analytics_storage" su "denied" per gli utenti provenienti da Spagna e Alaska e imposta "ad_storage" su "denied" per tutti gli utenti.

```
1 gtag('consent', 'default', {
2   'analytics_storage': 'denied',
3   'region': ['ES', 'US-AK']
4 });
5
6 gtag('consent', 'default', {
7   'ad_storage': 'denied'
8 });
```

Se, nella stessa pagina, si verificano due comandi per il consenso predefiniti con valori relativi a un'area geografica e a una sottoregione, verrà applicato quello con un'area geografica più specifica. Ad esempio, se si è impostato "ad_storage" su "granted" per la regione US e "denied" per la regione US-CA, per un gruppo di visitatori proveniente dalla California l'impostazione utilizzata sarà quella più specifica per US-CA.

Per quanto riguarda trasmettere informazioni sul clic sull'annuncio, ID cliente e ID sessione negli URL, invece, si intende che quando un utente arriva sul sito web dopo aver fatto clic su un annuncio, le informazioni su quest'ultimo possono essere aggiunte agli URL della pagina di destinazione come parametro di ricerca, al fine di migliorare l'accuratezza delle conversioni. Queste informazioni di solito vengono memorizzate nei cookie proprietari del dominio.

Tuttavia, se il criterio "ad_storage" è impostato su "denied", queste informazioni non verranno archiviate localmente. Per migliorare la qualità della misurazione dei clic sugli annunci quando "ad_storage" è denied, è possibile facoltativamente scegliere di passare informazioni sui clic degli annunci tramite i parametri URL tra le pagine utilizzando il passthrough URL.

Analogamente, se "analytics_storage" è impostato su denied, il passthrough URL può essere utilizzato per inviare dati e analisi basati sugli eventi e sulle sessioni (incluse le conversioni) senza cookie tra le pagine.

Per utilizzare il passthrough URL, è necessario soddisfare le seguenti condizioni:

- Il tag Google deve essere sensibile al consenso e presente nella pagina.
- La modalità di consenso deve essere implementata nella pagina.
- L'inserzionista deve aver attivato l'utilizzo della funzionalità passthrough URL.
- Il link in uscita si riferisce allo stesso dominio del dominio della pagina corrente.
- Deve essere presente un gclid/dclid nell'URL.

Per l'abilitazione di questa funzionalità, va impostato il parametro "url_passthroug" su true, come nel seguente script:

```
1 gtag('set', 'url_passthrough', true);
```

Questo comando viene solitamente aggiunto allo snippet predefinito prima di qualsiasi comando config.

Infine, oscurando completamente le informazioni sugli annunci quando gli utenti negano il consenso per i cookie degli annunci, cioè quando "ad_storage" è "denied", i nuovi cookie non verranno impostati per scopi pubblicitari. Inoltre, i cookie di terze parti precedentemente impostati su www.google.com e www.doubleclick.net non verranno utilizzati, tranne

che per scopi di spam e di attività fraudolenta. I dati inviati a Google continueranno a includere l'URL completo della pagina, comprese eventuali informazioni sui clic sull'annuncio nei parametri URL.

Per oscurare ulteriormente i dati degli annunci quando "ad_storage" è "denied", si deve impostare "ads_data_redaction" su "true" come si può osservare nel seguente script.

```
1 gtag('set', 'ads_data_redaction', true);
```

Quando "ads_data_redaction" è true e "ad_storage" è denied, gli identificatori dei clic sugli annunci inviati nelle richieste di rete dai tag Google Ads verranno oscurati. Le richieste di rete verranno inviate anche tramite un dominio senza cookie. Il parametro "ads_data_redaction" non avrà effetto quando "ad_storage" è "granted" o se il comando "gtag('consent')" non viene utilizzato.

3.5 Esempio di applicazione e verifica

Il seguente esempio pone "ad_storage" su "denied" per impostazione predefinita. Quando l'utente indica che acconsente alle funzionalità alla base di "ad_storage", viene aggiornato in granted.

L'ordine del codice è di fondamentale importanza. Infatti, se il codice di consenso è stato chiamato fuori ordine, le impostazioni predefinite per il consenso non funzioneranno. A seconda dei requisiti aziendali, le specifiche possono variare, ma in generale il codice deve essere eseguito nel seguente ordine:

1. *Caricamento del tag Google.* Questo è il codice snippet predefinito. Lo snippet predefinito deve essere aggiornato per includere una chiamata al numero "gtag('consent', 'default', ...)". Se non sono impostati valori predefiniti, verranno abilitate tutte le funzionalità di tagging.
2. *Caricamento della soluzione per il consenso.* Se la soluzione per il consenso viene caricata in modo asincrono, bisogna tener conto dei criteri precedentemente descritti relativi a questo tipo di implementazione.
3. Se la scelta non viene gestita dalla soluzione scelta per il consenso, si chiami lo script "gtag('consent', 'update', ...)" dopo che l'utente indica la preferenza.

Nel codice seguente è stato creato un esempio di un'implementazione del Google Consent mode:

```
1 <script>
2 // Define dataLayer and the gtag function.
3 window.dataLayer = window.dataLayer || [];
4 function gtag(){dataLayer.push(arguments);}
5
6 // Default ad_storage to 'denied' as a placeholder
7 // Determine actual values based on your own requirements
8 gtag('consent', 'default', {
9   'ad_storage': 'denied'
10 });
11 </script>
12 <!-- Google tag (gtag.js) -->
13 <script async src="https://www.googletagmanager.com/gtag/js?id=TAG_ID">
14 </script>
15 <script>
16   window.dataLayer = window.dataLayer || [];
17   function gtag(){dataLayer.push(arguments);}
```



```
18
19   gtag('js', new Date());
20   gtag('config', 'TAG_ID');
21 </script>
22
23 <!-- Update this section based on your business requirements. -->
24 <script>
25   function consentGranted() {
26     gtag('consent', 'update', {
27       'ad_storage': 'granted'
28     });
29   }
30 </script>
31
32 <body>
33   ...
34   <button onclick="consentGranted">Yes</button>
35   ...
36 </body>
```

Source Code 3.1: Esempio di implementazione standard del Google Consent Mode

Quello mostrato in precedenza è il metodo standard con il quale implementare la modalità di consenso di Google. Ad esempio, se il sito web o l'app usa un CMP specifico, si dovranno consultare i metodi di implementazione specifici poichè i codici potrebbero differire in base all'implementazione del cookie banner.

Inoltre, come alternativa, per non operare direttamente nel codice è possibile personalizzare in Google Tag Manager i tag per la modalità di consenso analizzando come il cookie viene salvato dal browser. Se il cookie rispetta i canoni descritti in precedenza, sarà possibile procedere con l'implementazione tramite GTM.

3.5.1 Verifica funzionamento Google Consent Mode

Per verificare ed eseguire il debug della configurazione della modalità di consenso, è consigliato utilizzare lo strumento Google Tag Assistant. Un'alternativa più specifica e tecnica, invece, è quella di utilizzare gli strumenti per sviluppatori che sono all'interno di ogni browser. Per accedere a quest'ultimi, basta fare un click con il tasto destro su qualunque parte della pagina web e successivamente su "Ispeziona" (Comando in Google Chrome).

Da qui, per analizzare le impostazioni del consenso dobbiamo procedere effettuando i seguenti passi:

1. Nella scheda Elementi, si deve digitare "dataLayer" nella barra di ricerca. Dopodichè si dovrà verificare che:
 - Il comando default viene prima di tutti gli altri eventi Google.
 - Gli stati del consenso vengono impostati in base all'interazione dell'utente e con il comando update.
 - I tag si attivano solo quando vengono soddisfatte le impostazioni di consenso richieste.
 - "ads_data_redaction" e "url_passthrough" sono configurati in base alle impostazioni fornite dall'utente.
2. Nella scheda Rete, invece, si dovrà verificare che:
 - Il parametro "gcs=" negli URL per conoscere lo stato del consenso abbia il seguente formato: gcs=G1"ad_storage"] ["analytics_storage"].

- I valori del parametro "gcs=" siano corretti in base al consenso fornito. Il valore di "ad_storage" e "analytics_storage" sarà uno di quelli che è possibile vedere nella Figura 3.9.

Valore	Significato
G100	Il consenso sia per ad_storage che per analytics_storage è stato negato.
G110	Il consenso è stato concesso per ad_storage e negato per analytics_storage.
G101	Il consenso è stato negato per ad_storage e concesso per analytics_storage.
G111	Il consenso sia per ad_storage che per analytics_storage è stato concesso.
G1--	Il sito non ha richiesto il consenso per ad_storage o analytics_storage.

Figura 3.9: Cookie relativi a Google Ads e al salvataggio non accettati.

- I domini senza cookie (ad esempio googlesyndication.com) vengano utilizzati quando "ads_data_redaction" è impostato su "true".
- Il criterio gclid/dclid viene aggiunto agli URL in uscita quando "url_passthrough" è impostato su true ed è il parametro linker _gl (ad esempio https://www.example.com/?_gl=1abcde5).

I metodi di verifica precedentemente descritti sono quelli che consentono di verificare con precisione che la modalità di consenso è implementata correttamente all'interno del sito o applicazione.

3.6 Benefici della Google Consent Mode

Dopo l'implementazione della modalità di consenso si devono rispettare le rigorose soglie di confidenza di Google, superando i seguenti controlli:

- Essere in possesso di una presenza pubblicitaria nello Spazio Economico Europeo (SEE) o nel Regno Unito.
- Aver implementato correttamente la Google Consent Mode avendo seguito i passaggi obbligatori precedentemente descritti.
- Aver raggiunto una soglia sugli annunci di 700 clic al giorno in un periodo di 7 giorni, per ogni paese e raggruppamento per dominio.

Una volta soddisfatti i criteri riportati sopra, i modelli di Google entrano nei periodi di addestramento. È probabile che le conversioni modellate appaiano gradualmente nei report sulle conversioni e che si verifichino miglioramenti gradualmente del rendimento registrato.

Per definizione di modello, si intende che quando un utente non acconsente ai cookie di Google Ads o di Analytics, la modalità di consenso utilizza l'IA di Google per regolare il comportamento dei tag pertinenti. In questo modo si fa sì che i cookie non vengano letti o scritti a fini pubblicitari o di analisi. Senza i cookie, gli inserzionisti riscontrano una lacuna nella misurazione e perdono visibilità sui percorsi degli utenti sul loro sito. Infatti, non sono più in grado di collegare direttamente le interazioni degli utenti con gli annunci alle conversioni.

La definizione del modello di conversione può aiutare a colmare le lacune nella misurazione dei media nei casi in cui non sia possibile osservare il percorso tra le interazioni con gli annunci e le conversioni. La definizione di questo modello utilizza l'IA di Google

per analizzare i dati osservabili e le tendenze storiche, quantificando la relazione tra utenti che hanno fornito il consenso e utenti che lo hanno negato. In seguito, utilizzando i percorsi osservabili degli utenti nei quali questi hanno acconsentito all'uso dei cookie, i modelli di Google valuteranno i percorsi di attribuzione per i percorsi degli utenti che non hanno fornito il consenso. Ciò permette di avere una visione più completa e accurata della spesa pubblicitaria e dei risultati, rispettando, allo stesso tempo, le scelte degli utenti relative al consenso.

Le conversioni modellate tramite la modalità di consenso saranno integrate direttamente nei report delle campagne Google Ads con lo stesso livello di granularità delle conversioni osservate. Questi dati verranno quindi utilizzati dagli strumenti di offerta di Google per garantire che le campagne pubblicitarie saranno ottimizzate in base a una visione completa dei risultati.

I tassi di conversione degli utenti che non hanno fornito il consenso dovrebbero essere sensibilmente inferiori rispetto a quelli degli utenti che lo hanno fornito. Da un'analisi approfondita si è riscontrato che i tassi di conversione degli utenti variano in base al loro stato di consenso. Gli utenti che hanno dato il consenso hanno in genere una probabilità di conversione da 2 a 5 volte più elevata rispetto a quelli che non lo hanno fornito. Tuttavia, questo comportamento varia notevolmente in base a fattori quali tassi di consenso, settore e tipo di conversione.

Nella Figura 3.10 viene riassunto il risultato di quest'analisi mettendo in evidenza il rapporto tra il tasso di consenso e le conversioni modellate:

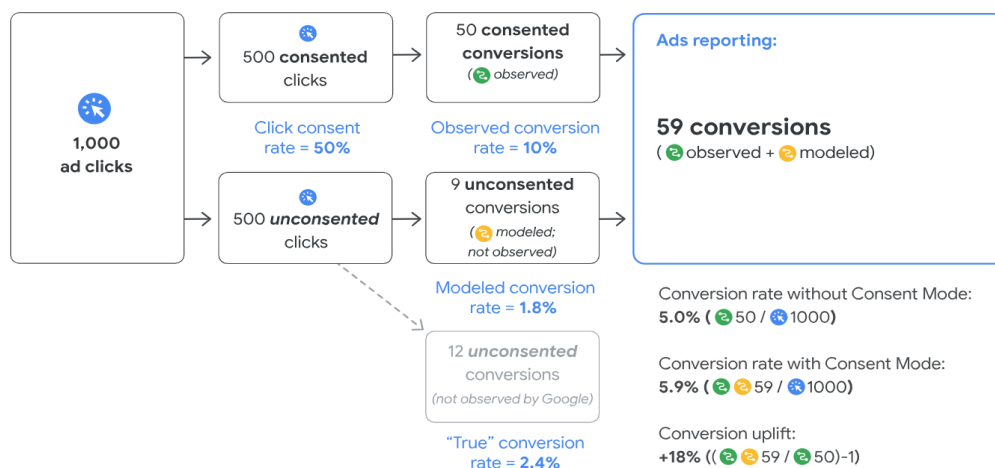


Figura 3.10: Relazione tra tassi di consenso e conversioni modellate

L'esempio riportato sopra mostra come i tassi di consenso e la diminuzione/l'aumento dei tassi di conversione non corrispondano, in quanto gli utenti che non hanno fornito il consenso tendono a effettuare conversioni meno di frequente. In questo caso, l'inserzionista registra un tasso di consenso del 50%, ma una diminuzione delle conversioni solo del 19% (12 conversioni su 62) e un aumento del tasso di conversione del 18% grazie alla definizione del modello di conversione.

Importante notare che Google non è in grado di verificare se la conversione di un utente che non ha fornito il consenso ha avuto origine da un'interazione precedente con l'annuncio. I suoi modelli aiutano a colmare il percorso tra interazioni con gli annunci ed eventi di conversione allo scopo di ridurre al minimo il rischio di sovrastime. Infatti, alcune conversioni che si sono realmente verificate potrebbero non essere prese in considerazione, in quanto non attribuibili ai clic sugli annunci senza cookie.

3.6.1 Benefici e creazione di modelli di comportamento in Google Analytics 4

Dopo aver implementato il banner del consenso per un sito web o una app, Analytics non avrà dati disponibili per gli utenti che negano il consenso. La creazione di modelli di comportamento per la modalità di consenso utilizza il Machine Learning per modellare il comportamento degli utenti che rifiutano i cookie di Analytics in base al comportamento di utenti simili che accettano questi cookie. I dati modellati consentono di ottenere informazioni utili dai report di Analytics rispettando la privacy degli utenti.

Ad esempio, la creazione di modelli di comportamento stima i dati in base a metriche relative a utenti e sessioni, come gli utenti attivi giornalieri e il tasso di conversione. Questi potrebbero non essere osservabili quando identificatori come cookie o ID utente non sono completamente disponibili.

Per capire nel dettaglio cosa accade all'interno di Analytics c'è bisogno di confrontare dati modellati e dati osservati.

Quando gli utenti visitano il sito e concedono il consenso ai cookie di Analytics o non disattivano la personalizzazione utilizzando l'ID pubblicità, Analytics associa il comportamento degli utenti a vari identificatori per fornire continuità nella misurazione. I dati di questo tipo sono definiti "osservabili" perchè si riferiscono a utenti che hanno concesso la loro autorizzazione ad osservare il loro comportamento.

Tuttavia, quando gli utenti non concedono il consenso, gli eventi vengono associati a un identificatore utente permanente. Ad esempio, se Google Analytics raccoglie 10 eventi di visualizzazione di pagina, non può nè osservare nè indicare se sono riconducibili a 10 utenti solo ad 1.

Analytics, però, applica il Machine Learning per stimare il comportamento di questi utenti in base al comportamento di utenti simili che hanno accettato i cookie analitici. In conclusione, i dati di addestramento utilizzati per la creazione di modelli si basano sui dati degli utenti osservati nella proprietà in cui la creazione dei modelli è attivata.

L'approccio di Google alla creazione di modelli di comportamento si basa sulle seguenti best practice per il Machine Learning:

- *Verificare l'accuratezza e comunicare le modifiche.* La convalida di holdback garantisce l'accuratezza costante dei modelli di Google. I dati utente stimati vengono confrontati con una parte dei dati utente osservati esclusi dall'addestramento del modello e le informazioni vengono utilizzate per perfezionare i modelli. Google comunicherà le modifiche che potrebbero avere un impatto rilevante sui dati in questione.
- *Adottare un approccio rigoroso per la generazione di report.* La creazione di modelli di comportamento viene inclusa solo quando si è certi della loro qualità. Ad esempio, se non c'è abbastanza traffico con consenso per fornire dati al modello, gli eventi attivati dagli utenti che negano il consenso non vengono registrati. Ciò garantisce l'accuratezza dei dati.
- *Eseguire la personalizzazione per la tua attività.* L'algoritmo di definizione dei modelli più generale di Google viene applicato separatamente per riflettere l'unicità dell'attività e del comportamento degli utenti.

Poiché il modello è addestrato sui dati osservati per la proprietà Google Analytics 4, quest'ultima deve disporre di dati sufficienti per addestrare il modello. Per essere idonea alla creazione di modelli di comportamento, la proprietà deve soddisfare i seguenti criteri:

1. La modalità di consenso deve essere attivata su tutte le pagine dei siti o in tutte le schermate dell'app.

2. La modalità di consenso per le pagine web deve essere implementata in modo da caricare i tag prima che venga visualizzata la finestra di dialogo per il consenso e i tag Google vengano caricati in tutti i casi, non solo se l'utente dà il consenso (implementazione avanzata).
3. La proprietà raccoglie almeno 1000 eventi al giorno con `"analytics_storage='denied'"` per almeno 7 giorni.
4. La proprietà ha almeno 1000 utenti giornalieri che inviano eventi con `"analytics_storage='granted'"` per almeno 7 dei 28 giorni precedenti.

Per il corretto addestramento del modello potrebbe essere necessario che la soglia dei dati venga raggiunta per più di 7 dei 28 giorni. Tuttavia, è possibile che anche i dati aggiuntivi non siano sufficienti per consentire ad Analytics di addestrare il modello. La creazione di modelli di comportamento inizia dalla data in cui una determinata proprietà diventa idonea.

Nei rari casi in cui una proprietà non soddisfi più i prerequisiti per la creazione di modelli di comportamento dopo averli soddisfatti in precedenza, i dati stimati non saranno più disponibili. Se, invece, in un secondo momento la proprietà soddisfa nuovamente i prerequisiti, i dati stimati saranno di nuovo disponibili. Questi dati saranno reperibili, di nuovo, solo a partire dalla data in cui la proprietà sarà idonea.

3.7 Rispetto del GDPR e utilizzo dei dati da parte della GCS

La modalità di consenso permette di modificare il comportamento dei tag Google in base allo stato del consenso degli utenti. È possibile indicare se è stato concesso il consenso per i cookie di Analytics e Google Ads. I tag di Google si adattano in modo dinamico e utilizzano i cookie solo per gli scopi specificati quando l'utente ha dato il consenso.

La Google Consent Mode è disponibile in Google Tag Manager, Google Analytics, Google Marketing Platform e Google Ads. Poiché la modalità di consenso è una funzionalità del prodotto Google in cui viene implementata, è soggetta ai termini e condizioni dei prodotti precedentemente citati, compresi i Termini per il trattamento dei dati. La modalità di consenso non influisce sui termini del GDPR relativi al responsabile o al titolare del trattamento dei dati del prodotto sottostante.

Come per qualsiasi altro dato proveniente dai tag, Google garantisce la riservatezza e la sicurezza dei dati grazie agli stessi standard leader del settore adottati per proteggere i dati dei propri utenti.

Ecco come Google gestisce i dati:

- *Accesso limitato ai dati.* Google utilizza la crittografia e i controlli di accesso dei dipendenti per proteggere i dati da accessi non autorizzati, sia interni che esterni.
- *Condivisione limitata dei dati.* Nel caso in cui non venga fornita l'autorizzazione dall'inserzionista, Google non condivide con altri inserzionisti i dati degli eventi di conversione che lo riguardano. Se necessario, è possibile condividere questi dati per ottemperare a eventuali leggi o norme vigenti, procedimenti giudiziari o richieste del governo con forza esecutiva.
- *Sicurezza dei dati.* Google si impegna a garantire che i sistemi utilizzati per archiviare i dati siano sicuri e affidabili. È presente un team di tecnici della sicurezza dedicati alla protezione contro minacce esterne ai sistemi Google e tutti i dati vengono archiviati in formato criptato per evitare accessi non autorizzati.

Google ha ottenuto la certificazione ISO 27001 per sistemi, applicazioni, personale, tecnologie, processi e data center relativi a una serie di prodotti Google, tra cui la modalità di consenso.

ISO/IEC 27001:2013 (ISO 27001) è lo standard internazionale che descrive le best practice per un ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI, in italiano). Ottenere una certificazione accreditata ISO 27001 permette di dimostrare che la un'azienda sta seguendo le best practice sulla sicurezza delle informazioni e fornisce un controllo indipendente e qualificato sul fatto che la sicurezza delle informazioni è gestita in linea con le best practice internazionali e gli obiettivi aziendali.

Case study: analisi dei requisiti e progettazione

In questo capitolo verrà messa in pratica la teoria precedentemente descritta. Si presenterà il caso di studio reale, partendo dall'analisi dei requisiti dove vengono descritti i vari casi d'uso, per poi spostarsi sulla parte di progettazione, dove vengono mostrati nel dettaglio i casi d'uso mediante l'utilizzo di diagrammi di sequenza, attività e flusso.

4.1 Analisi dei requisiti

L'analisi dei requisiti è una fase fondamentale nella pianificazione e nello sviluppo di qualsiasi progetto, specialmente nel contesto dello sviluppo software o dell'ingegneria dei sistemi. Essa consiste nel processo di identificazione, raccolta, documentazione e comprensione approfondita delle esigenze, delle funzionalità e dei vincoli associati a un progetto.

Nel contesto informatico, l'analisi dei requisiti è il processo di comprensione delle esigenze degli utenti, degli stakeholder e degli utilizzatori finali e traduce tali esigenze in requisiti tecnici dettagliati che guideranno il processo di progettazione e sviluppo del software. Questi requisiti possono essere di natura funzionale (e, quindi, indicare ciò che il software deve fare) o non funzionale (come prestazioni, sicurezza, usabilità, scalabilità, etc.)

Il Consent Mode di Google è una soluzione orientata alla privacy che mira a bilanciare i diritti degli utenti e le esigenze delle aziende in un contesto di raccolta e utilizzo dei dati.

Per quanto riguarda il GDPR, il Google Consent Mode affronta la questione dei dati personali evitando la raccolta di identificatori associati al dispositivo quando le opzioni più ampie di esso sono disabilitate. Di conseguenza, nessuna delle informazioni raccolte rientrerebbe nella definizione di "dati personali" e, pertanto, non rientra nell'ambito del GDPR. Il GDPR richiede una base giuridica legittima per il trattamento dei dati personali, che può essere basata sul "consenso" o sull' "interesse legittimo".

Nel caso del Google Consent Mode, i dati anonimi raccolti senza consenso presentano un ostacolo inferiore per dimostrare un interesse legittimo. Questo almeno è la logica che Google cela dietro questa funzionalità, che si propone di recuperare, almeno in parte, i dati sugli utenti che non acconsentono al tracciamento.

Google Consent Mode, combinato con il modello di dati basato sugli eventi di Google Analytics 4 e Google Ads, offre alle aziende la possibilità di lavorare con un set di dati più ricco, migliorando le potenzialità delle analisi dei dati in un mercato attento alla privacy.

I requisiti fondamentali all'attivazione del Google Consent Mode sono molteplici.

Quelli dal lato del proprietario del sito sono:

- Avere una presenza pubblicitaria nello Spazio Economico Europeo (SEE) o nel Regno Unito. Nel case study citato, è stato costruito un sito ecommerce di test (www.coldman95.github.io/ecommerce-template-pcc) localizzato in Polonia, dove sono stati creati degli account Google Ads, Google Tag Manager e Google Analytics al fine della misurazione.
- Avere implementato correttamente la modalità di consenso o lo IAB Transparency & Consent Framework (TCF v2.0). Nel case study presentato, è stato implementato un banner usando il CMP "Iubenda", che dà la possibilità all'utente di esprimere le preferenze del consenso. Un banner per essere considerato conforme alle norme sul consenso e privacy di Google deve dare la possibilità di scegliere se accettare o rifiutare i cookie relativi a finalità di marketing (Google Ads, ads_storage) e quelli relativi a finalità analitiche (Google Analytics, analytics_storage). Nel banner cookie devono essere espresse le leggi sulla privacy relative all'uso che si andrà a fare dei cookie salvati in base alle preferenze. Inoltre, nel banner cookie deve essere obbligatoria la possibilità di rifiutare completamente tutti i cookie di terze parti, altrimenti il Google Consent Mode non verrà attivato.
- La presenza dello script relativo al consent mode deve essere in ogni pagina del sito e deve partire di default prima di ogni altro comando che invia dati di misurazione. Una volta inserito lo script nelle pagine del sito, i tag di Google si adatteranno automaticamente alle scelte di consenso degli utenti, utilizzando un update per aggiornare i consensi ogni volta che l'utente cambia le proprie scelte di consenso.

Quelli espressi precedentemente sono i requisiti che un sito web deve avere ai fini dell'attivazione del Google Consent Mode. Una volta effettuata l'implementazione, il modello Machine Learning è pronto per iniziare a recuperare le conversioni; come citato da Google (figura 3.1) "In media, il Consent Mode recupera più del 70% delle conversioni provenienti dagli annunci Google Ads che andrebbero perse a causa delle scelte di consenso degli utenti"¹.

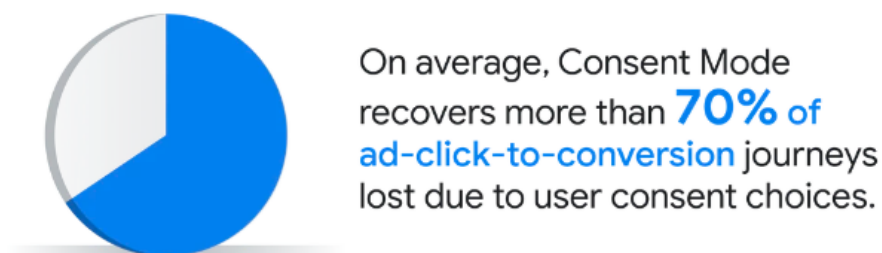


Figura 4.1: Conversioni recuperate da Google con il Google Consent Mode

I requisiti precedenti rendono pronto il modello di Machine Learning per la collezione dei dati. Tuttavia devono verificarsi altri 3 requisiti di traffico che il sito web deve raggiungere

¹Conversion modeling through Consent Mode in Google Ads - <https://blog.google/products/marketingplatform/360/conversion-modeling-through-consent-mode-google-ads/>

per far partire in modo effettivo il modello di attribuzione del Google Consent Mode. Essi sono:

- avere una soglia giornaliera di click dell'annuncio di 100 click al giorno, per paese e raggruppamento di dominio;
- la proprietà di Google Analytics deve raccogliere almeno 1000 eventi al giorno con "analytics_storage='denied'" per almeno 7 giorni;
- la proprietà di Google Analytics deve avere almeno 1000 utenti giornalieri che inviano eventi con analytics_storage='granted' per almeno 7 dei 28 giorni precedenti.

Per addestrare correttamente il modello potrebbe essere necessario che la soglia dei dati venga raggiunta per più di 7 dei 28 giorni. Tuttavia, è possibile che anche i dati aggiuntivi non siano sufficienti per consentire ad Analytics di farlo. Infine, è importante sottolineare che la creazione di modelli comportamentali inizia dalla data in cui una determinata proprietà diventa idonea.

Al fine di raggiungere le soglie di traffico richieste da Google, è stata creata un'API che manda a Google Analytics 1000 utenti giornalieri che randomicamente accettano tutti i consensi, rifiutano parte di essi o li rifiutano completamente. Inoltre l'API è stata progettata in modo tale da creare eventi di conversione, come un acquisto e una visualizzazione di pagina. In questo modo è stato possibile addestrare il modello e mettere in luce le differenze di prestazione rispetto a quando la modalità di consenso è attiva o meno. I report che si sono generati ci fanno capire, a fini statistici, come le conversioni vengano recuperate da Google.

È importante sottolineare che è stato possibile far vedere gli effetti solo su Google Analytics poichè risulta impossibile avviare una campagna pubblicitaria di test in modo da vedere gli effetti su Google Ads. I dataset e i risultati aziendali interni non sono stati resi disponibili dall'azienda per la condivisione.

Una volta che il Google Consent Mode ha iniziato a procedere con il suo modello per l'acquisizione di traffico all'interno del sito, i casi d'uso che possono riscontrarsi sono molteplici. Tuttavia, quelli fondamentali sui quali si concentrerà lo studio sono i seguenti:

- L'utente, tramite il banner Iubenda installato nel sito, rifiuta tutti i tipi di cookie eccetto quelli tecnici. Grazie al Google Consent Mode installato nel sito, gli strumenti di misurazione di Google riveleranno un ping di dati contenente le informazioni di navigazione. Questo cookie, utile alla modellazione, arriverà in forma aggregata e non identificativa. Infatti, è composto dal timestamp della visita dell'utente sul sito web, dallo user agent, che indica se gli utenti sono effettivamente arrivati sul sito web, dal refererrer, che esprime in che modo l'utente è arrivato sul sito web e se la pagina precedente alla visualizzazione dell'utente contiene informazioni utili nell'URL ai fini della profilazione.

In questo modo il Google Consent Mode farà sì che il nostro sito riesca a mostrare la pubblicità contestuale basata su dati anonimi, al posto della pubblicità mirata basata sul tracciamento di dati personali, nonchè riesce a misurare le conversioni relative a una specifica campagna a livello aggregato, anzichè a livello di singolo utente.

Questo scenario è molto importante, poichè ci consente di addestrare il modello basandosi sulle informazioni precedentemente descritte che verranno collezionate in base al traffico di tutti gli utenti che non hanno accettato i cookie di misurazione.

- L'utente, tramite il banner Iubenda installato nel sito, accetta tutti i cookie disponibili, i quali sono i cookie relativi alle funzionalità di marketing (Google Ads) e quelli relativi alle funzionalità analitiche (Google Analytics). In questo modo il Google Consent

Mode assicura che i due cookie siano inviati in modo specifico ai due strumenti di misurazione evitando perdite di attribuzione e ottimizzando il remarketing dinamico. Quest'ultimo è uno strumento molto utilizzato al giorno d'oggi che consente di mostrare all'utente informazioni personalizzate, tramite una campagna pubblicitaria, mostrando i contenuti pertinenti ai prodotti o ai servizi per i quali egli ha manifestato interesse prima della visita al sito. Il tutto avviene con uno scambio di cookie che risulta essere più efficiente a fini analitici con il Google Consent Mode attivato.

Questi due casi d'uso, lavorando in parallelo, riescono ad addestrare un modello di AI che stima, e quindi recupera, le conversioni che venivano perse. Ciò avviene prevedendo il comportamento degli utenti che non hanno accettato i cookie basandosi sul comportamento medio degli utenti profilati in modo dettagliato.

4.2 Progettazione

In questa sezione verrà descritta nel dettaglio la progettazione dei casi d'uso precedentemente citati mediante l'uso di diagrammi di flusso.

Il primo passo fondamentale, prima di concentrarsi sulla progettazione dei casi d'uso, è capire quale è la differenza principale nell'aver installato il Google Consent Mode all'interno di un sito web rispetto al non averlo fatto. La Figura 4.2 ci mostra i principali vantaggi.

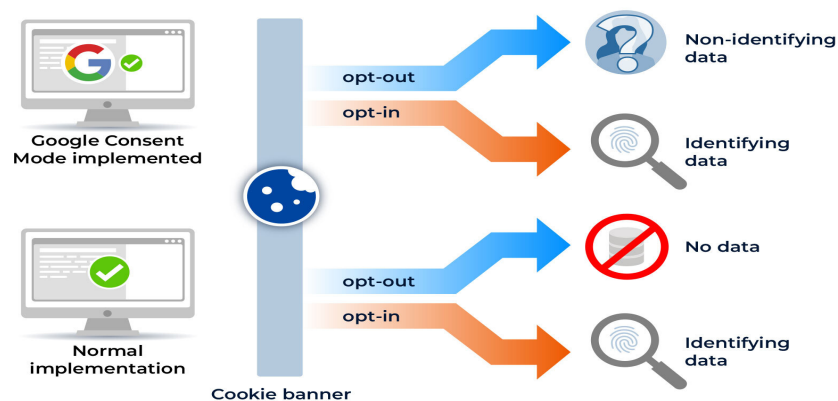


Figura 4.2: Differenza di funzionamento tra normale implementazione e Google Consent Mode

Per interpretare al meglio la Figura 4.2 si premette che, secondo il GDPR, non è consentito raccogliere dati personali degli utenti senza il loro consenso. Tuttavia, se i visitatori forniscono il consenso tramite il cookie banner, è possibile impostare i cookie di tracciamento. Per "opt-out" si intende quando un utente indica un particolare tipo di comunicazione nell'ambito della quale non è richiesto il consenso o la manifestazione di volontà di un soggetto affinché succedano determinati effetti, in questo caso quando un utente non accetta i cookie. Per "opt-in" si intende l'azione attraverso la quale un utente decide di esprimere il proprio consenso in maniera positiva, in questo caso quando un utente accetta i cookie. Come si evince nella Figura 4.2, la differenza principale è che senza il Google Consent Mode, in caso di "opt-out", non si ha nessun tipo di dato rispetto a quelli anonimizzati ottenuti con il Google Consent Mode.

Una volta chiarito il concetto sostanziale dell'installazione del Google Consent Mode, il passo successivo descritto nella Figura 4.3 sono i vantaggi esistenti dopo la sua implementazione che può avvenire mediante due metodi, ovvero utilizzando l'implementazione tramite

codice e modificando gli script del banner forniti dal CMP utilizzato, oppure tramite Google Tag Manager. Entrambi i metodi portano alla stessa conclusione, come è rappresentato dalla Figura 4.3.

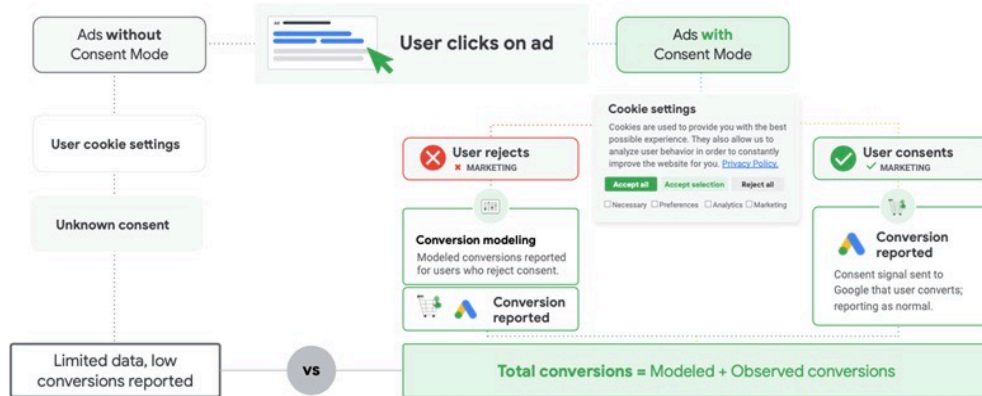


Figura 4.3: Risultati riassuntivi dopo l'implementazione del Google Consent Mode

La Figura 4.3 ci descrive che l'attore principale (utente), quando clicca su un annuncio pubblicitario o semplicemente arriva sul sito web, ha la possibilità di fornire i consensi tramite il banner cookie che è collegato al Google Consent Mode. Se accetta, l'utente fornisce a Google il "gclid", il "dclid", il "cookieID" e il "GoogleID". In caso di conversione dell'utente, la stessa viene registrata memorizzando tali dati aggiuntivi.

Nello scenario opposto, quando un utente non accetta i cookie e converte, il cookie viene fornito senza dati identificativi, ma comunque i dati sulla conversione vengono recuperati dal modello di Machine Learning.

Dopo aver descritto i casi d'uso più generali nella figura 4.4 viene descritto nello specifico come funziona l'algoritmo che è all'interno del Google Consent Mode. Il primo momento è quello in cui l'utente arriva sul sito, causa il caricamento dello script o del container Google Tag manager con cui è installato il Google Consent mode, che va ad attivare i tag necessari (quelli per i cookie tecnici), e controlla se il cookie attribuito sia già esistente. In caso affermativo, si aggiorna il timestamp del cookie per poi arrivare alla sua validazione. Tuttavia, in caso in cui il cookie non sia presente, si salva il cookie all'interno del sito e lo si comunica al Google Consent Mode inviando il timestamp e i dati di profilazione contenuti nel cookie. Arrivati al momento della scelta del consenso, se positivo, il Google Cosent Mode attiva i tag opzionali di misurazione (quelli di Google Analytics e Google Ads) e aggiorna il cookie. Nello scenario opposto, il Google Consent Mode blocca i tag opzionali ma comunica e salva nei cookie i dati anonimizzati.

Possiamo, quindi, riassumere il diagramma descritto nella Figura 4.4 in quattro step:

1. Al caricamento della prima pagina, il Google Consent Mode attiva solo i tag "necessari" e chiede all'utente il consenso per attivare quelli facoltativi.
2. Una volta che l'utente dà il consenso, il Google Consent Mode rilascia un cookie che memorizza il suo consenso e attiva i tag opzionali.
3. Se il cookie di consenso esiste già, il Google Consent Mode controlla se esso è ancora valido. Nel caso affermativo, rispetta il consenso precedente e non mostra più il pop-up.
4. Il Google Consent Mode reimposta il consenso se la scelta precedente non è più valida e visualizza nuovamente il pop-up.

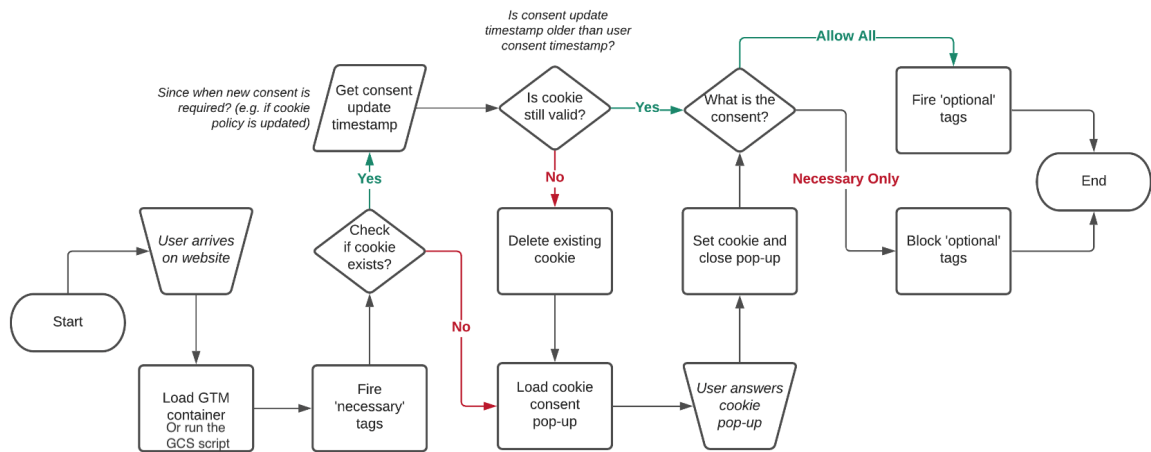


Figura 4.4: Diagramma di flusso Google Consent Mode

Dopo aver descritto il caso d’uso a livello generale, cioè senza specificare su quale strumento il Google Consent Mode incide, ma descrivendo solo il funzionamento del suo algoritmo, in Figura 4.5 viene rappresentato il diagramma di flusso relativo agli effetti su Google Analytics.

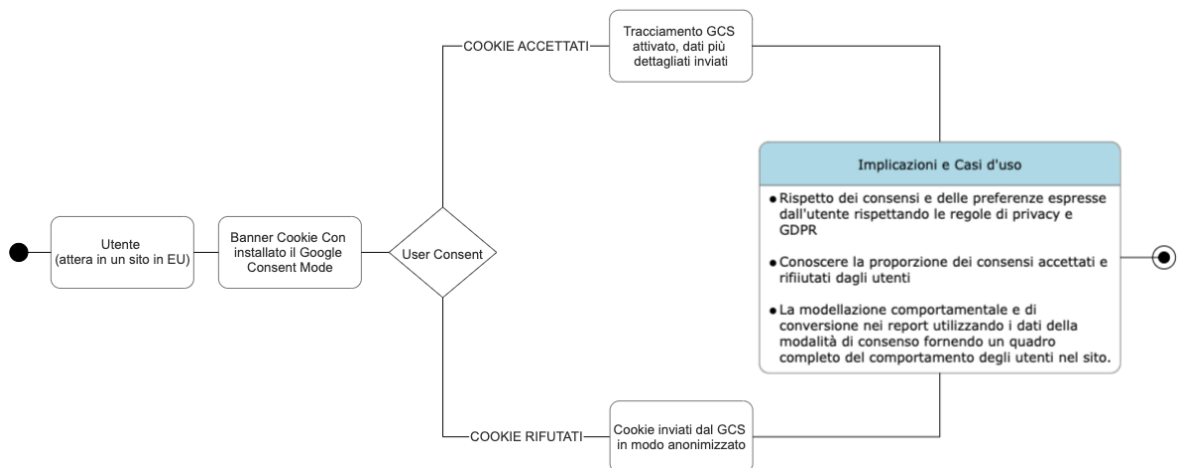


Figura 4.5: Diagramma di flusso impatto Google Consent Mode su Google Analytics

Nella Figura 4.5 si evince che un utente naviga nel web e arriva su un sito che si trova nell’Unione Europea. A questo punto parte l’algoritmo del Google Consent Mode (come illustrato nella Figura 4.4) e fa i vari controlli sulla validazione dei cookie e sulla veridicità dell’utente. Successivamente, l’utente interagisce con il banner cookie (nel case study, un banner del CMP Iubenda) e sceglie quale azione effettuare. Se accetta tutte le preferenze, i cookie verranno inviati in modo dettagliato allo strumento includendo i parametri di identificazione specifici. Se, al contrario, rifiuta i cookie, i dati verranno anonimizzati, ma comunque inviati a Google Analytics. Come si nota dalla Figura 4.5, entrambe le scelte portano alla realizzazione di un modello e al raggiungimento dei medesimi casi d’uso.

In entrambi i casi ci sarà un rispetto dei consensi e delle preferenze espresse dall’utente nonchè delle regole di privacy e del GDPR; inoltre si conoscerà la proporzione dei consensi accettati e rifiutati dagli utenti; infine, queste azioni portano alla modellazione comportamentale e di conversione nei report, grazie all’uso del Machine Learning. Quest’ultimo utilizza

i dati della modalità di consenso fornendo un punto della situazione completo relativo al comportamento degli utenti nel sito indipendentemente dall'accettazione dei cookie.

Implementazione e risultati ottenuti

In questo capitolo è stata impiegata particolare attenzione sulla descrizione dell'implementazione del cookie banner Iubenda, degli strumenti di misurazione di Google (Google Analytics, Google Ads, Google Tag Manager) e sull'implementazione dei codici del Google Consent Mode. Inoltre è mostrata anche l'API che è stata creata per la simulazione di traffico all'interno del sito web. La parte finale del capitolo è concentrata sull'esposizione e sulla discussione dei report ottenuti dopo il periodo di misurazione.

5.1 Implementazione degli strumenti di misurazione di Google

Prima di procedere con l'implementazione del Google Consent Mode, si devono installare all'interno del sito i vari strumenti di misurazione di Google e il banner cookie di Iubenda. Ci sono più soluzioni su come inserire nel sito web questi strumenti; tuttavia verrà mostrata l'implementazione tramite codice e l'implementazione tramite Google Tag Manager. Utile sottolineare che non c'è differenza in termini di efficienza; sono due soluzioni ugualmente performanti. Gli strumenti di misurazione che verranno installati sono: Google Tag Manager, Google Analytics e Google Ads.

L'unico strumento che può essere installato nel nostro caso tramite codice è Google Tag Manager. Dopo aver creato un account in Google Tag Manager, si devono inserire gli script mostrati in seguito nella sezione "head" del sito web e nella sezione "body".

Il seguente script è da inserire nella sezione "head":

```

1 <!-- Google Tag Manager -->
2 <script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
3 new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
4 j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
5 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,
6   f);
7 }) (window,document,'script','dataLayer','GTM-NH7VZRPW');</script>
8 <!-- End Google Tag Manager -->

```

Il seguente script è da inserire nella sezione "body":

```

1 <!-- Google Tag Manager (noscript) -->
2 <noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-NH7VZRPW
3   "
4   height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
5 <!-- End Google Tag Manager (noscript) -->

```

Dopo aver inserito i precedenti script, Google Tag Manager è pronto all'uso. Google tag manager sarà utile per l'installazione di Google Ads, Analytics e per la configurazione del Google Consent Mode senza utilizzare nessun tipo di codice.

5.1.1 Installazione tramite codice di Google Ads e Analytics

Per procedere all'installazione di Google Ads tramite codice, dopo aver creato un account, deve essere installato in tutte le pagine del sito il seguente script di misurazione:

```
1 <!-- Google tag (gtag.js) -->
2 <script async src="https://www.googletagmanager.com/gtag/js?id=AW-821269769"></
  script>
3 <script>
4   window.dataLayer = window.dataLayer || [];
5   function gtag(){dataLayer.push(arguments);}
6   gtag('js', new Date());
7
8   gtag('config', 'AW-821269769');
9 </script>
```

Questo script consente l'inizializzazione in tutte le pagine di Google Ads, strumento fondamentale per il tracciamento degli utenti che provengono dagli annunci pubblicitari.

Successivamente, in questo caso di studio, sono stati create due proprietà differenti di Google Analytics, una proprietà che tramite API riceverà il parametro GCS con valore "111" (caso ottimale con tutti i cookie accettati) e un'altra con il parametro GCS impostato a "100" (caso peggiore in cui l'utente rifiuta tutti i cookie). Gli script che devono essere inseriti sono mostrati qui di seguito.

Il seguente script è quello relativo alla proprietà di misurazione che riceve il GCS impostato su "111":

```
1 <!-- Google tag (gtag.js) -->
2 <script async src="https://www.googletagmanager.com/gtag/js?id=G-03HQFL22KX"></
  script>
3 <script>
4   window.dataLayer = window.dataLayer || [];
5   function gtag(){dataLayer.push(arguments);}
6   gtag('js', new Date());
7
8   gtag('config', 'G-03HQFL22KX');
9 </script>
```

Il seguente script, invece, è quello relativo alla proprietà di misurazione che riceve il GCS impostato su "100":

```
1   <!-- Google tag (gtag.js) -->
2 <script async src="https://www.googletagmanager.com/gtag/js?id=G-8E4SH08FZL"></
  script>
3 <script>
4   window.dataLayer = window.dataLayer || [];
5   function gtag(){dataLayer.push(arguments);}
6   gtag('js', new Date());
7
8   gtag('config', 'G-8E4SH08FZL');
9 </script>
```

Utile sottolineare che, in un caso normale, è sufficiente installare una sola proprietà Google Analytics all'interno del sito. Nel caso di studio si è scelto di installare due proprietà differenti per evidenziare le differenze statistiche che si creano nei report in base all'accettazione o al rifiuto dei cookie, comportamento che è gestito dalla API creata.

5.1.2 Installazione tramite GTM di Google Ads e Analytics

L'implementazione tramite Google Tag Manager ci consente di installare all'interno del sito gli strumenti di misurazione di Google senza utilizzare alcun tipo di codice ma semplicemente creando dei tag indicando l'ID di misurazione.

Nella Figura 5.1 è mostrato come Google Ads è implementato nel sito tramite Google Tag Manager.

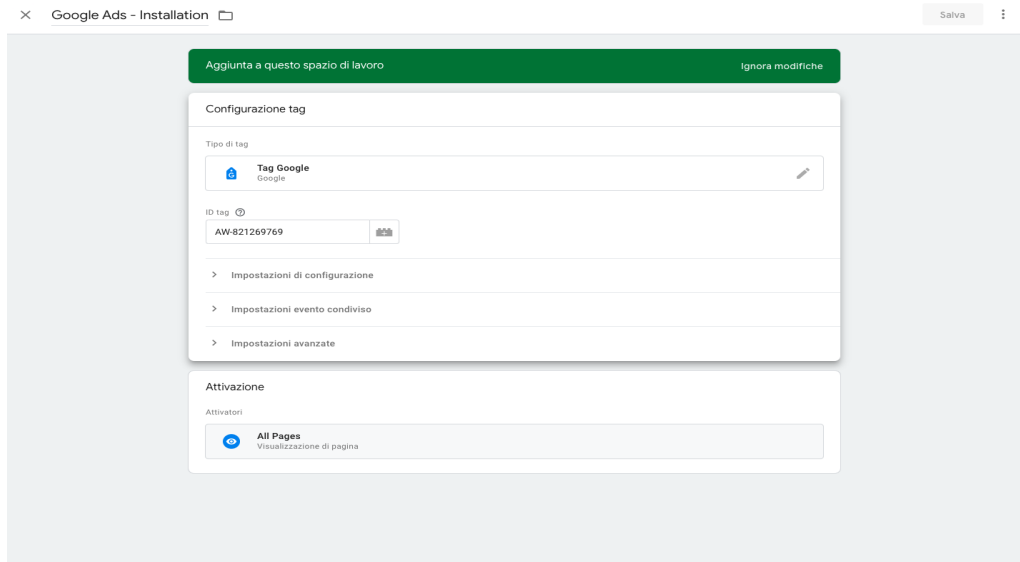


Figura 5.1: Implementazione Google Ads con Google Tag Manager

Nella Figura 5.2 è mostrato come Google Analytics con parametro GCS impostato su "100" è implementato nel sito tramite Google Tag Manager.

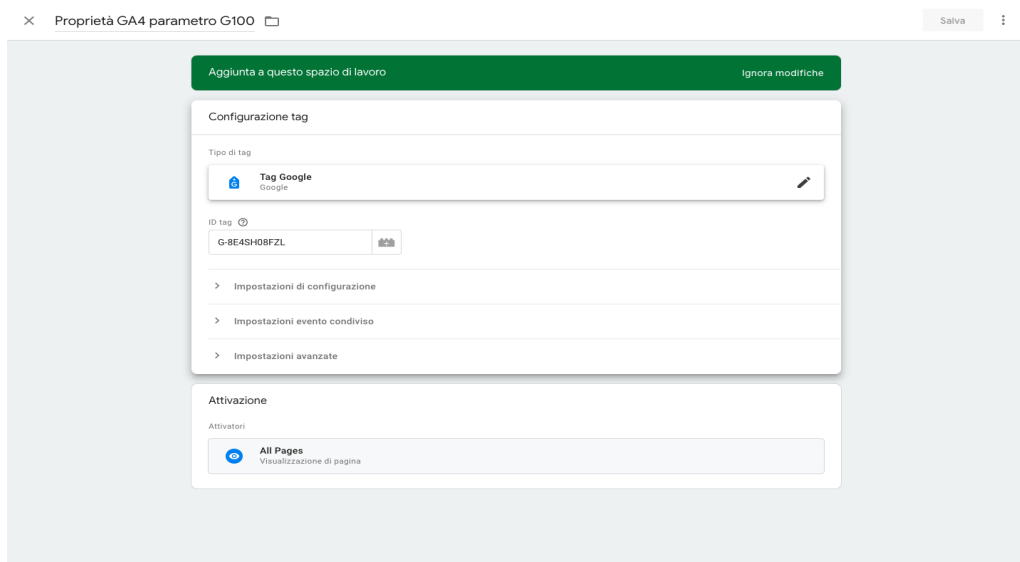


Figura 5.2: Implementazione Google Analytics con parametro GCS impostato su "100" con Google Tag Manager

Nella Figura 5.3 è mostrato come Google Analytics con parametro GCS impostato su "111" è implementato nel sito tramite Google Tag Manager.

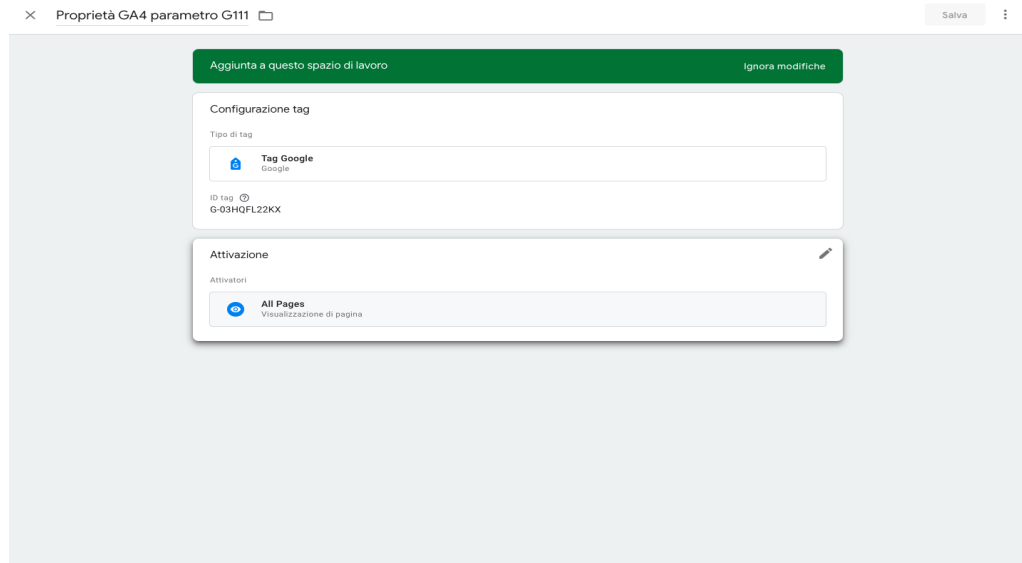


Figura 5.3: Implementazione Google Analytics con parametro GCS impostato su "111" con Google Tag Manager

È facilmente intuibile che la configurazione tramite Google Tag Manager è molto più rapida e semplice. Tutti e 3 i tag sono di tipo "Tag Google" che è un'opzione che ci consente di configurare ogni strumento di Google semplicemente inserendo l'ID di misurazione. Inoltre, avendo l'esigenza di installare gli strumenti di misurazione in tutte le pagine, è stato scelto un attivatore "all pages".

5.1.3 Verifica del funzionamento degli strumenti di misurazione di Google

Per verificare se gli strumenti di misurazione di Google risultano installati correttamente ci sono diversi metodi. Sicuramente, i principali sono quelli che prevedono di controllare i ping che il sito manda ai server di Google; per farlo si andrà nella sezione "network" del browser mediante la modalità da sviluppatore. L'altro metodo consiste nell'utilizzo di un'estensione ufficiale di Google dal nome "Google Tag Legacy" che va a controllare in tempo reale i tag che si attivano all'interno della pagina su cui ci si trova.

Le Figure 5.4 e 5.5 ci mostrano i ping di Google Analytics che partono dal sito web e arrivano ai server Google. Si noti che il parametro relativo a consent mode viene inviato alle due proprietà come precedentemente descritto.

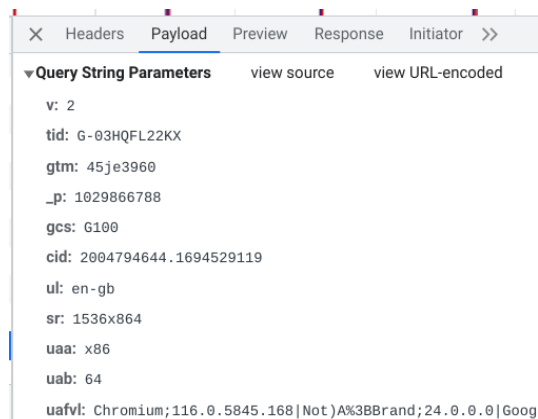


Figura 5.4: Ping di verifica per la proprietà con GCS impostato su 100

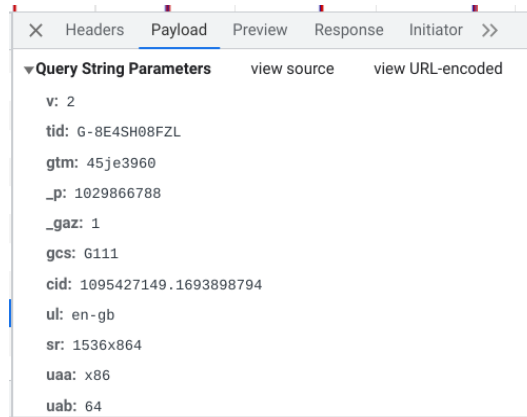


Figura 5.5: Ping di verifica per la proprietà con GCS impostato su 111

Nella Figura 5.6 è mostrato come lo script di Google Ads si attiva ed è pronto ad inviare un ping nel caso in cui un utente arrivi sul sito tramite un annuncio pubblicitario.

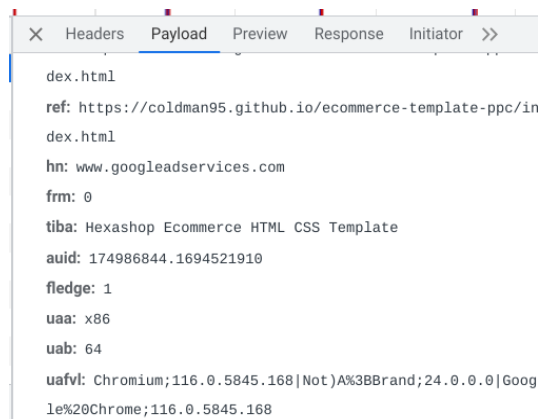


Figura 5.6: Ping di verifica Google Ads

Il secondo metodo, come precedentemente accennato, è quello basato sull'uso dell'estensione ufficiale Google Tag Legacy. Una volta configurata e attivata, l'estensione mostrerà in tempo reale tutti i tag che si attivano sulla pagina. Rispetto al metodo tramite la console del browser, questa soluzione risulta più rapida e intuitiva consentendo di effettuare un debug in tempo reale.

Nella Figura 5.7 viene mostrato come l'estensione rileva i tag di misurazione nella home page del sito di test.

Quelli descritti precedentemente sono due metodi equivalenti che assicurano che gli strumenti di misurazione di Google siano attivati in modo corretto e che i tag partono nella giusta pagina.

5.2 Implementazione del banner Iubenda

Iubenda è un CMP (Consent Management Platform) che offre un servizio assolutamente importante per tutti coloro che possiedono un portale web e devono adeguarsi ai regolamenti della privacy. È una soluzione online che permette di creare una Privacy Policy perfettamente integrata con qualsiasi sito web o app. Questo è uno dei tanti CMP presenti sul mercato, ma lo si è scelto per la sua perfetta integrazione con il Google Consent Mode e per le sue

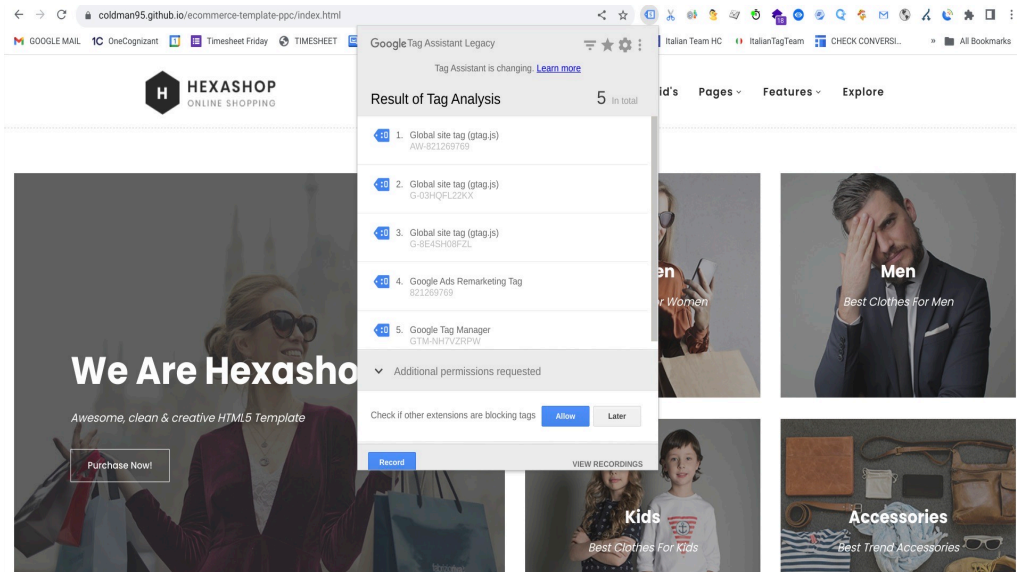


Figura 5.7: Schermata della home page del sito con estensione Google Tag legacy

ottime performance che hanno consentito lo svolgimento del caso di studio in maniera del tutto gratuita.

L'implementazione tramite codice del banner Iubenda è effettuata mediante l'inserimento di uno script all'interno della sezione "head" del sito. Prima di procedere con l'installazione è necessario registrarsi nella piattaforma, rivendicare il sito web rispettando i canoni di policy legislativa e dare la disponibilità a Iubenda sulla gestione della cookie law.

Nella script seguente è mostrato il codice del banner cookie Iubenda:

```

1 <script type="text/javascript">
2 var _iub = _iub || [];
3 _iub.csConfiguration = {
4   "askConsentAtCookiePolicyUpdate":true,
5   "floatingPreferencesButtonDisplay":"bottomright",
6   "perPurposeConsent":true,
7   "purposes": 1,3,4,5,
8   "siteId":3298795, \
9   "whitelabel":false,
10  "cookiePolicyId":17424772, \
11  "lang":"it",
12  "banner":{
13    "acceptButtonDisplay":true,
14    "closeButtonDisplay":false,
15    "customizeButtonDisplay":true,
16    "position":"float-top-center",
17    "rejectButtonDisplay":true }};
18 </script>
19 <script type="text/javascript"
20 src="https://cs.iubenda.com/autoblocking/3298795.js"></script>
21 <script type="text/javascript" src="//cdn.iubenda.com/cs/iubenda_cs.js" charset
    ="UTF-8" async></script>

```

Il banner che verrà installato sarà conforme alle norme GDPR, con le opzioni di rifiuto dei cookie e la possibilità di specificare le preferenze. Nello script sono specificati il "cookiePolicyId", che è un codice univoco che fa riferimento alla regolamentazione della policy per il sito preso in questione, e il "siteId", che è un codice univoco che serve ad identificare il nostro sito. Questi due parametri saranno molto utili per la configurazione del Google

Consent Mode. Nelle Figure 5.8 e 5.9 viene mostrato come è il banner realizzato tramite lo script precedentemente descritto.

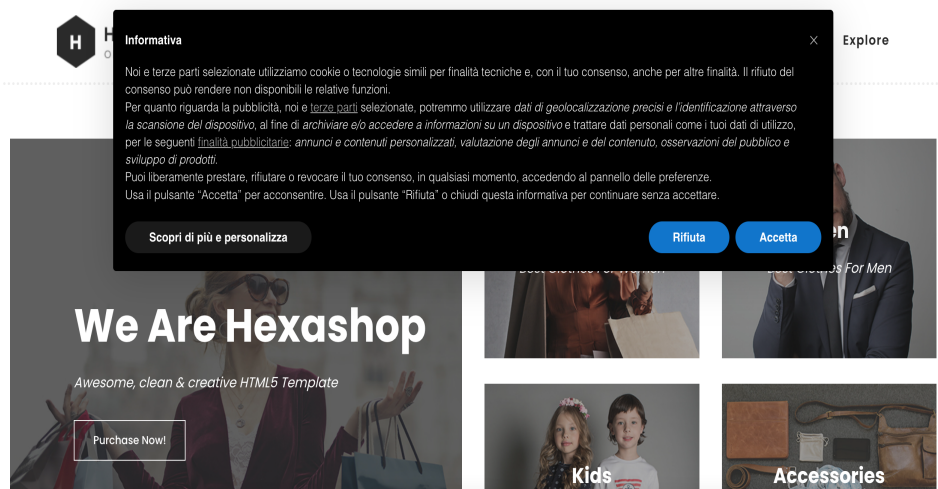


Figura 5.8: Banner Iubenda all'arrivo sul sito

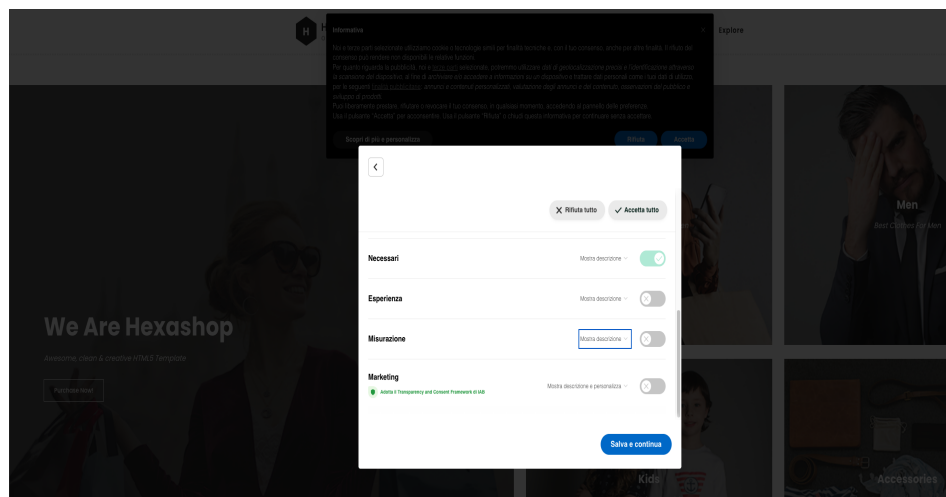


Figura 5.9: Opzioni di scelta dei cookie da parte del banner iubenda

Dopo la configurazione precedentemente descritta, il cookie che viene generato ha il nome di "_iub_cs - userID" e la sua struttura è quella mostrata in Figura 5.10.

Quella mostrata in questa figura è la struttura del cookie nel caso ottimale in cui l'utente ha accettato tutti i consensi. La struttura del cookie è composta da un timestamp, che indica il momento in cui il nostro cookie è salvato per la prima volta all'interno del sito; è presente un userID che verrà poi condiviso con gli strumenti analitici di Google e nella sezione "purposes" sono specificati quali cookie sono stati accettati. La stringa contiene degli ID che vanno da 1 a 5 e ognuno di essi si riferisce a specifici cookie che possono avere il valore "true" in caso vengano accettati e "false" in caso contrario. Nel dettaglio gli ID descrivono i seguenti cookie:

- L'ID 1 si riferisce ai cookie tecnici (necessari) come il salvataggio e gestione del backup, servizi di piattaforma e hosting, protezione dagli SPAM, monitoraggio dell'infrastruttura,
- l'ID 2 si riferisce al cookie di interazione e funzionalità semplici, come la gestione dei tag, la gestione di database dell'utente, la registrazione ed autenticazione,

Cookie Name	Cookie Value	Domain	Path	Expires	Size	Secure	HttpOnly	SameSite	Medi...
_jub_cs-88644770	%7B%22timestamp%22%3A%222023-06-23T15:45:36.995Z%22%2C%22version%22%3A%221.48.0%22%2C%22purposes%22%3A%5B%221%22%3Atrue%2C%222%22%3Atrue%2C%223%22%3Atrue%2C%224%22%3Atrue%2C%225%22%3Atrue%22%7D	.jub...	/	/ 2024...	282		✓	None	Medi...
_jub_cs-10320411	%7B%22timestamp%22%3A%222023-06-23T15:45:36.995Z%22%2C%22version%22%3A%221.48.0%22%2C%22purposes%22%3A%5B%221%22%3Atrue%2C%222%22%3Atrue%2C%223%22%3Atrue%2C%224%22%3Atrue%2C%225%22%3Atrue%22%7D	.jub...	/	/ 2024...	218		✓	None	Medi...

Cookie Value Show URL-decoded
 {"timestamp":"2023-06-23T15:45:36.995Z","version":"1.48.0","purposes":{"1":true,"2":true,"3":true,"4":true,"5":true},"id":"88644770","cons":{"rand":"5d38f3"}}

Figura 5.10: Struttura del cookie dopo l'implementazione del banner Iubenda

- l'ID 3 si riferisce al cookie per il miglioramento dell'esperienza, come, ad esempio, la gestione dei feed RSS, l'interazione con i social network e le piattaforme esterne e l'interazione con piattaforme di raccolta dati e altre terze parti,
- l'ID 4 si riferisce al cookie di misurazione, quindi quello che gestisce la parte relativa a Google Analytics occupandosi di tutta la parte statistica che viene comunicata esternamente,
- l'ID 5 si riferisce al cookie di targeting e pubblicità. Le sue finalità sono quelle di gestire Google Ads e quindi tutta la parte riguardante la pubblicità, il remarketing e il behavioral targeting, la gestione dei contatti e le agevolazioni commerciali.

Questa è la situazione in cui in un sito non è implementato il Google Consent Mode; sarà, quindi, il punto di partenza su cui andare ad applicare questo strumento modificando lo script del banner a seconda del tipo di implementazione che verrà scelta, quella tramite codice o quella tramite Google Tag Manager.

5.3 Implementazione del Google Consent Mode

Per quanto riguarda l'implementazione del Google Consent Mode ci sono svariate opzioni. Quelle che verranno presentate sono le due soluzioni principali e le più adottate nel mondo del digital marketing. La prima soluzione è quella basata soltanto sul codice, questa soluzione prevede di interfacciarsi esclusivamente con la parte backend del sito web inserendo gli script del Google Consent Mode e modificando lo script del banner (in questo caso Iubenda) in modo opportuno al fine di aggiornare i consensi e comunicarli al Google Consent Mode; in sintesi, quindi, tutta la gestione dei tag avverrà tramite codice. La seconda soluzione, invece, è quella relativa all'implementazione tramite Google Tag Manager, o "implementazione mista". Il termine "mista" è utilizzato perchè, comunque, lo script di Google Tag Manager dovrà essere installato tramite codice e anche lo script originale per il banner cookie dovrà essere installato via script (come mostrato precedentemente). In realtà, è possibile anche installare il banner cookie adattato al Google Consent Mode tramite Google Tag Manager; tuttavia questa opzione in termini di efficienza risulta peggiore.

5.3.1 Implementazione del Google Consent Mode tramite codice

Come precedentemente citato, l'implementazione tramite codice del Google Consent Mode ci consentirà di gestire tutti i tag e gli strumenti di misurazione di Google senza il bisogno di usare Google Tag Manager. Il primo passo è installare i vari script del Google

Consent Mode che andranno inseriti tutti prima del codice del banner dei cookie, premessa molto importante è che si deve rispettare l'ordine mostrato in modo da dare la precedenza agli script nell'ordine in cui vengono inseriti.

Il primo script da inserire è il seguente:

```
1 window.dataLayer = window.dataLayer || [];
2   function gtag() {
3     dataLayer.push(arguments);
4   }
```

Il precedente script serve ad inizializzare il Google Consent Mode creando una struttura dati chiamata datalayer. Un datalayer è un oggetto Javascript (più nel dettaglio un array Javascript) creato da Google che è utilizzabile per gestire le informazioni dei tag inseriti nel sito e far comunicare tra di loro i vari strumenti di misurazione di Google.

Il secondo script da inserire è il seguente:

```
1   gtag("consent", "default", {
2     ad_storage: "denied",
3     analytics_storage: "denied",
4     wait_for_update: 2000 // milliseconds
5   });
```

Il precedente script serve ad impostare la modalità tramite cui deve partire la modalità di consenso. Dallo script possiamo intuire che, di default, il Google Consent Mode partirà prima dell'accettazione dei cookie da parte dell'utente in modalità "denied" sia per quanto riguarda i cookie relativi a Google Ads (ad_storage) e sia per quelli relativi a Google Analytics (analytics_storage). La riga "wait_for_update" sta a significare quanto tempo deve passare tra lo stato iniziale di "default" allo stato iniziale di "update".

Il terzo script da installare è il seguente:

```
1   gtag('set', 'url_passthrough', true);
2   gtag("set", "ads_data_redaction", false);
```

Lo script precedente è relativo alla qualità del tracciamento degli annunci di Google Ads mediante il metodo "url_passthrough", che consente di controllare l'URL della pagina che un utente visita salvando i parametri identificativi contenuti per poi aggiungerli a tutti i collegamenti interni che un utente potrebbe fare. La seconda riga dello script è relativa ai dati degli annunci di Google Ads che saranno rimossi in caso di rifiuto dei cookie da parte dell'utente.

Il terzo script da installare è il seguente:

```
1   async src="https://www.googletagmanager.com/gtag/js?id=ID_ANALYTICS"
2   async src="https://www.googletagmanager.com/gtag/js?id=ID_ADS"
3   gtag('js', new Date());
4   gtag('config', 'G-8E4SH08FZL'); // GCS su 100
5   gtag('config', 'G-03HQFL22KX'); //GCS su 111
6   gtag('config', 'AW-821269769');
```

Lo script precedente è quello standard per l'installazione di Google Ads e Analytics con l'unica differenza che deve trovarsi all'interno dello script del Google Consent Mode per essere gestito da esso.

Dopo l'installazione dello script del Google Consent Mode è da inserire lo script del banner Cookie (in questo caso Iubenda), modificato secondo le indicazioni fornitoci dal CMP. Per il caso di Iubenda l'attivazione della modalità di consenso di Google va "flaggata" anche all'interno della pagina admin del CMP.

Lo script del banner aggiornato per il consent mode è il seguente:

```
1   var _iub = _iub || [];
2   _iub.csConfiguration = {
3     "siteId":3298795, // ID di Iubenda
```

```

4   "cookiePolicyId":17424772,      // ID policy di Iubenda
5   "gdprAppliesGlobally":false,    //add from default
6   "countryDetection":true,        //add from default
7   "reloadOnConsent":true,         //add from default
8   "perPurposeConsent":true,
9   "purposes":"1,3,4,5",
10  "enableTcf":true,                //add from default
11  "googleAdditionalConsentMode":true, //attivazione Google Consent Mode
12  "askConsentIfCMPNotFound":false, //add from default
13  "lang":"it",
14  "floatingPreferencesButtonDisplay":false,
15  "banner":{
16    "acceptButtonDisplay":true,
17    "closeButtonDisplay":false,
18    "customizeButtonDisplay":true,
19    "position":"float-top-center",
20    "rejectButtonDisplay":true });
21    "listPurposes":true
22  }
23  };
24
25  src="//cdn.iubenda.com/cs/tcf/stub-v2.js"
26  src="//cdn.iubenda.com/cs/iubenda_cs.js" charset="UTF-8" async

```

Rispetto all'implementazione standard sono stati aggiunti diversi comandi; i quali sono:

- "gdprApplies (boolean, default true)": parametro impostato su "false" e "countryDetection" su "true" per chiedere il consenso solo agli utenti UE. Da ricordarsi che se si ha sede nell'UE, si deve applicare il GDPR anche agli utenti residenti al di fuori dell'UE.
- "reloadOnConsent (boolean, default false)": parametro che consente di ricaricare la pagine dopo che il consenso è stato salvato dal Google Consent Mode.
- "enableTcf (boolean, default false)": impostata su "true", quest'opzione consente agli utenti di gestire le proprie preferenze di tracciamento della pubblicità sulla base dello IAB Transparency and Consent Framework, requisito fondamentale per l'attivazione del Google Consent Mode.
- "googleAdditionalConsentMode (boolean, default false)": se parte a "true", permette di raccogliere il consenso per i partner pubblicitari di Google che non hanno ancora aderito al TCF, ma che sono presenti nella lista dei fornitori di tecnologia pubblicitaria di Google.
- "askConsentIfCMPNotFound (boolean, default true)":
se l'opzione "enableTcf" è impostata su "true" e la preferenza del Framework IAB non viene trovata, gli utenti saranno invitati a fornire nuovamente il consenso, anche se quest'ultimo è stato dato prima dell'attivazione del Framework. Se, invece, l'opzione è impostata su "false", il comportamento descritto verrà impedito.

Questi sono i parametri aggiunti, rispetto all'implementazione standard, che consentono di far funzionare il Google Consent Mode. L'implementazione tramite codice è così terminata; tuttavia, è importante sottolineare che il comando "consent, update" verrà inviato automaticamente allo script di "consent, default" aggiornando i parametri in base alle preferenze dell'utente. Lo svantaggio di questa soluzione è che non è possibile gestire i tag nello specifico come avviene in Google Tag Manager.

5.3.2 Implementazione tramite Google Tag Manager o implementazione mista

L'implementazione che verrà descritta è quella detta mista poichè il banner dei cookie Iubenda e lo script di Google Tag Manager devono essere installati comunque tramite codice, ma tutta la gestione dei tag e la loro attivazione in base ai consensi avviene in Google Tag Manager. Importante sottolineare che si sarebbe potuto installare il banner Iubenda tramite Google Tag Manager, ma questa opzione rimane sconsigliata in termini di efficienza di prestazioni del sito web.

Gli script da installare sono quello di Google Tag Manager e quello del banner Iubenda. Lo script di Google Tag Manager è il seguente:

```

1      <!-- Google Tag Manager -->
2  <script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
3  new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
4  j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
5  'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,
6  f);
7  })(window,document,'script','dataLayer','GTM-NH7VZRPW');</script>
8  <!-- End Google Tag Manager -->

```

Lo script per il banner iubenda dovrà essere il seguente:

```

1      var _iub = _iub || [];
2      _iub.csConfiguration = {
3          "siteId":3298795,           // ID di Iubenda
4          "cookiePolicyId":17424772, // ID policy di Iubenda
5          "gdprAppliesGlobally":false, //add from default
6          "countryDetection":true,    //add from default
7          "reloadOnConsent":true,     //add from default
8          "perPurposeConsent":true,
9          "purposes":"1,3,4,5",
10         "enableTcf":true,           //add from default
11         "googleAdditionalConsentMode":true, //attivazione Google Consent Mode
12         "askConsentIfCMPNotFound":false, //add from default
13         "lang":"it",
14         "floatingPreferencesButtonDisplay":false,
15         "banner":{
16             "acceptButtonDisplay":true,
17             "closeButtonDisplay":false,
18             "customizeButtonDisplay":true,
19             "position":"float-top-center",
20             "rejectButtonDisplay":true ;
21             "listPurposes":true}} ;
22
23     src="//cdn.iubenda.com/cs/tcf/stub-v2.js"
24     src="//cdn.iubenda.com/cs/iubenda_cs.js" charset="UTF-8" async

```

Entrambi gli script erano stati già presentati precedentemente; è necessario mantenere questo ordine all'interno del codice del sito, cioè avere subito dopo l'"head" di apertura lo script del Google Tag Manager immediatamente seguito dallo script del banner di Iubenda. L'infrazione di questa sequenza, creerà problemi nell'utilizzo del Google Consent Mode che non riuscirà attivarsi in Google Tag Manager in modo corretto.

A questo punto, verrà presentato come l'implementazione deve avvenire all'interno di Google Tag Manager.

Il primo passo in Google Tag Manager è quello di creare una variabile "cookie proprietario" in cui dovremmo inserire il nome della variabile cookie seguita dal "cookiePolicyId" specificato nel banner. In tal modo Google Tag Manager riesce ad associare e leggere il cookie che viene salvato nel banner di riferimento. Nella Figura 5.11 viene mostrata la configurazione di questa variabile, con la spunta sulla casella "decodifica in formato URI il cookie". Questa

funzione consente di trasformare il codice in una stringa decifrabile, in questo caso caso, da Google Tag Manager.

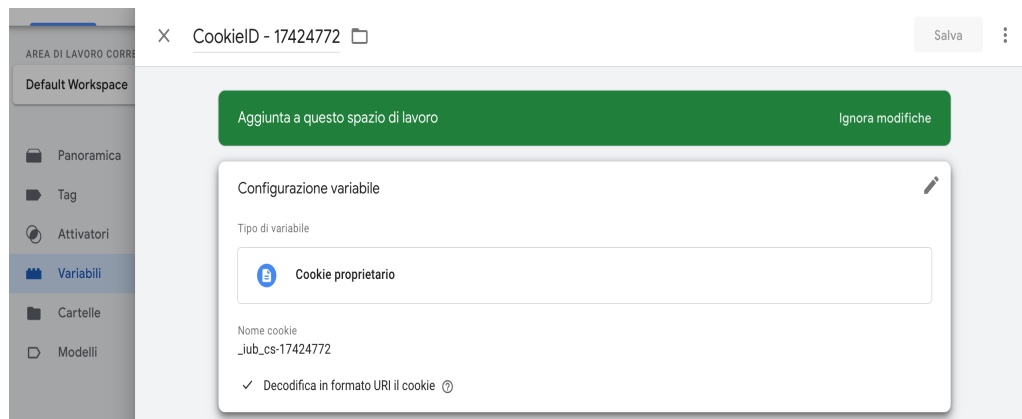


Figura 5.11: Variabile cookie proprietario con cookie policy ID

Lo step successivo è quello di usare il concetto delle tabelle ad espressioni regolari (tabella ReGex). Si creeranno quindi 3 differenti tabelle Regex aventi in input la variabile cookie mostrata in Figura 5.11 per ogni categoria che si vorrà "mappare". Tutte le tabelle Regex avranno come valore predefinito "denied", poichè è lo stato di partenza che il Google Consent Mode impone a queste categorie di cookie; infine, nelle impostazioni avanzate, è selezionata l'opzione "ignorare maiuscole e minuscole" al fine di leggere il cookie senza questo criterio.

Nella Figura 5.12 è mostrata la tabella Regex relativa alla categoria di cookie a finalità di marketing. Nel pattern è stata inserita la categoria con ID 5 (ID relativo ad ad_storage) con i due possibili stati che possono essere scritti nel cookie, "true" e "false". Nella colonna "output" sono stati inseriti il valore che il Google Consent Mode associa a true (granted) e false (denied).

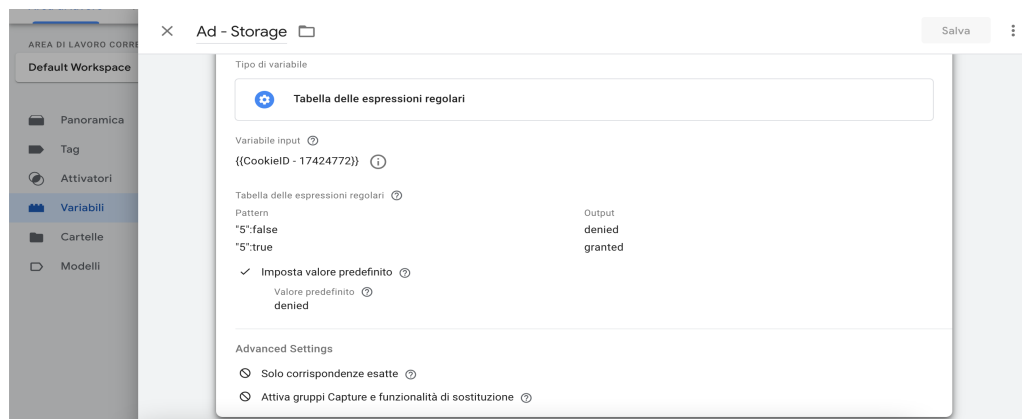


Figura 5.12: Tabella ReGex relativa a cookie a finalità di marketing

Nella Figura 5.13 è mostrata la tabella Regex relativa alla categoria dei cookie a fini analitici. Nel pattern è stata inserita la categoria con ID 4 (ID relativo ad analytics_storage) con i due possibili stati che possono essere scritti nel cookie, ovvero "true" e "false". Nella colonna "output" sono stati inseriti il valori che il Google Consent Mode associa a true (granted) e false (denied).

Nella Figura 5.14 è mostrata la tabella Regex relativa alla categoria di cookie relativi alla personalizzazione e performance. Nel pattern è stata inserita la categoria con ID 3 (ID relativo ad personalization_storage) con i due stati che possono essere scritti nel cookie, ovvero "true"

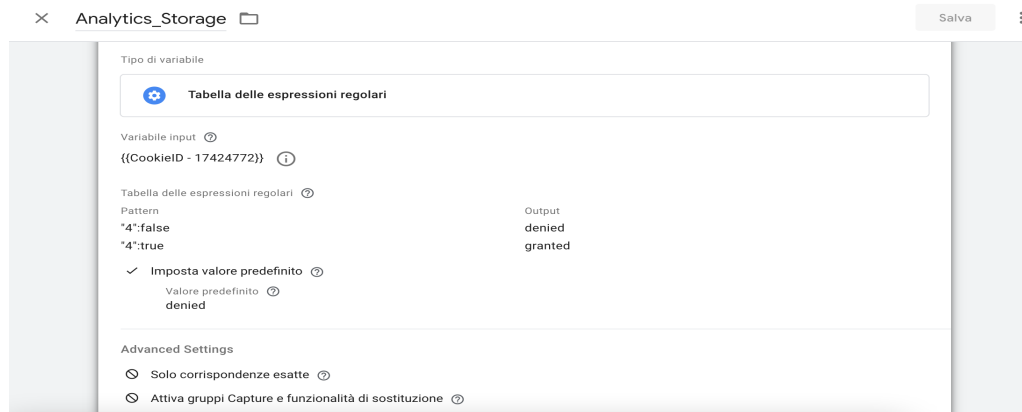


Figura 5.13: Tabella ReGex relativa a cookie analitici

e "false". Nella colonna "output" sono stati inseriti i valori che il Google Consent Mode associa a true (granted) e false (denied).

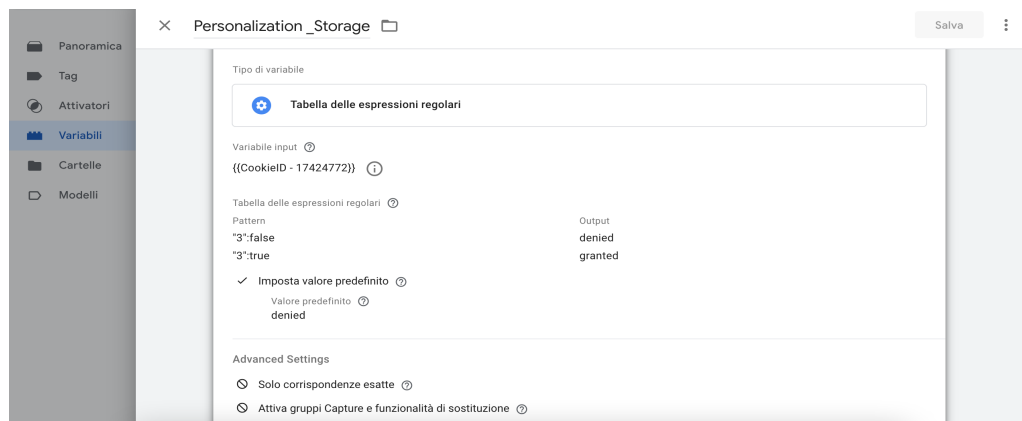


Figura 5.14: Tabella ReGex relativa a cookie di performance e personalizzazione

Lo step successivo è quello di creare i tag per la gestione del cookie per il Google Consent Mode per lo stato di "default" e per quello di "update". Per avere un risultato ottimale è stato adattato il template per il Google Consent Mode creato da Simo Hava. Nelle Figure 5.15 e 5.16 è mostrata la configurazione del tag per lo stato di "default". Nella sezione "consent command" è stato selezionato "Default", e nelle categorie "Advertising", "Analytics" e "Personalization" sono state inserite le tabelle Regex precedentemente create relative a queste categorie. Le sezioni "functionality" e "security" sono state configurate già con lo stato di "granted", poichè esse riguardano i cookie tecnici e di sicurezza; quindi, non c'è bisogno che vengano bloccati dal Google Consent Mode.

L'attivatore di questo tag è mostrato in Figura 5.17 dove si vede che esso viene attivato nel caso in cui la variabile relativa al cookie rimane nello stato di "undefined". In tal modo il tag per lo stato di "default" si attiverà soltanto se l'utente non ha espresso alcuna preferenza, quindi appena arriva sul sito web.

La parte conclusiva è la creazione del tag per la gestione dei cookie del Google Consent Mode per la fase di update. Nella Figura 5.18 è mostrata la configurazione del tag per lo stato di "update".

Nella sezione "consent command" è stato selezionato "Update" e nelle categorie "Advertising", "Analytics" e "Personalization" non sono state inserite le tabelle ReGex relative alle categorie dei cookie, ma direttamente lo stato di "granted". Questo perchè il tag andrà ad

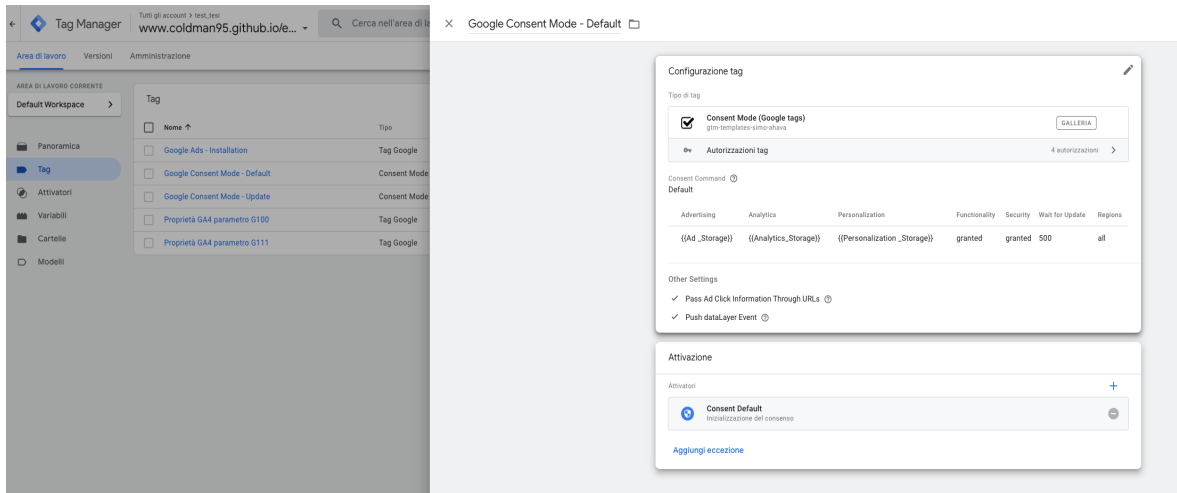


Figura 5.15: Tag relativo allo stato di default"

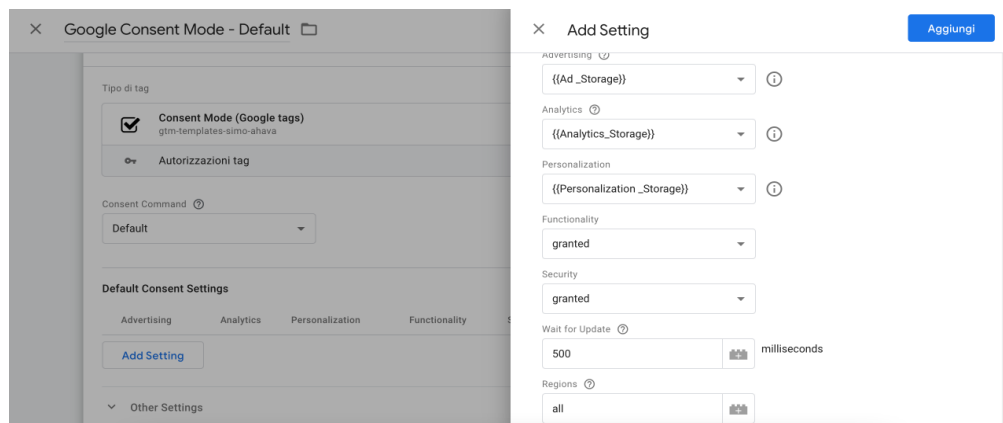


Figura 5.16: Configurazione del tag relativo allo stato di "default"

aggiornare solamente lo stato del cookie nelle tabelle ReGex precedentemente inserite nel tag per lo stato di "default". Tuttavia, anche qui, le sezioni "functionality" e "security" sono configurate con lo stato di "granted" per gli stessi motivi precedentemente descritti.

L'attivazione di questo tag avviene mediante un trigger mostrato in Figura 5.19 che si attiva nel caso in cui la variabile relativa al cookie non contiene lo stato di "undefined". In questo modo il tag per lo stato di "update" si attiverà soltanto se l'utente ha espresso una preferenza.

In entrambi i tag ("default" e "update") è stata attivata l'impostazione relativa all'inclusione delle informazioni del clic sull'annuncio in caso di rifiuto dei cookie pubblicitari (`url_passthrough`) e l'impostazione per salvare la preferenza dell'utente in un `dataLayer`.

Dopo aver eseguito questi passaggi, la configurazione del Google Consent Mode tramite Google Tag Manager può rivelarsi completata.

5.3.3 Debug e verifica funzionamento Google Consent Mode

Per la verifica del corretto funzionamento del Google Consent Mode ci sono diversi metodi, ovvero è possibile vedere nel network del sito se viene inviato un ping con il parametro GCS correttamente popolato oppure vedere se viene popolato il `dataLayer`.

Il primo metodo, mostrato in Figura 5.20, è quello di andare nella parte per sviluppatori del browser, recarsi nella parte "network" ed inserire nei filtri il parametro GCS. Si vedrà che

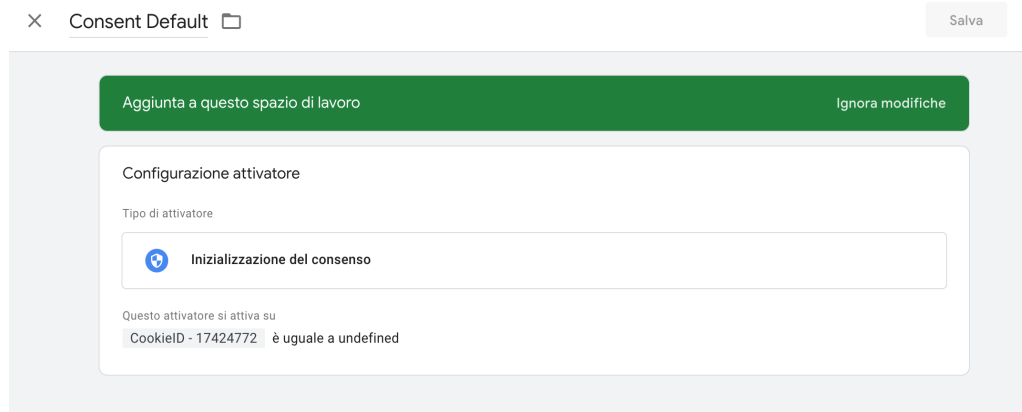


Figura 5.17: Attivatore del tag per lo stato di "default"

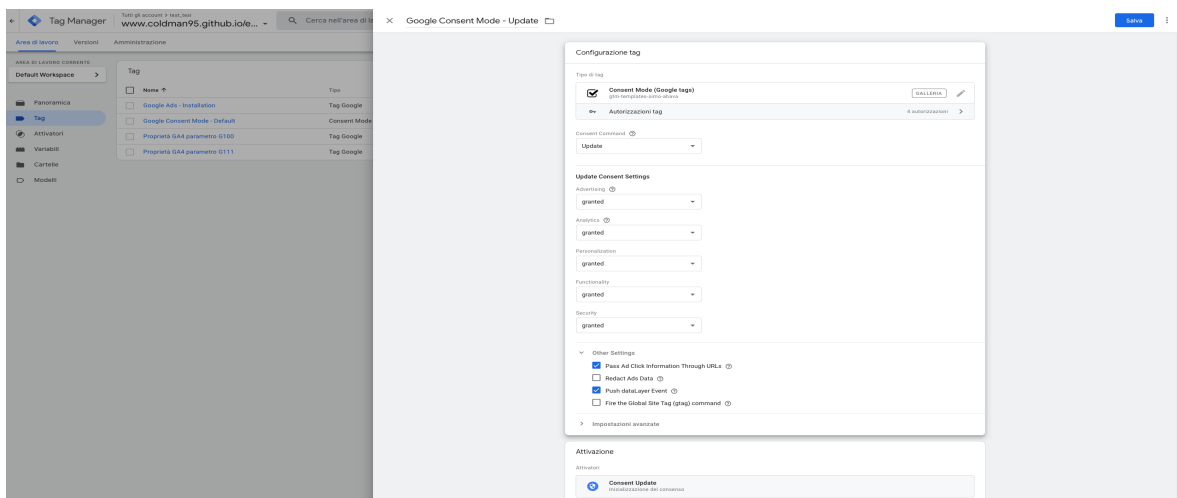


Figura 5.18: Configurazione del tag per lo stato di update

nei collect il parametro GCS è popolato con 101, poichè , in questo caso, l'utente ha accettato i cookie analitici e non quelli a finalità di marketing. Di fatto, il Google Consent Mode si è attivato sulle categorie dei cookie riferite a finalità analitiche e a quelle tecniche.

Come precedentemente menzionato il parametro GCS può assumere diversi valori in base alle preferenze dell'utente:

- G100: La modalità di consenso è stata impostata e Ads e Analytics storage sono impostati su denied. Stesso stato si avrà se l'utente dopo essere arrivato sul sito rifiuta tutti i cookie.
- G110: Sono stati accettati i cookie di marketing e non di analisi.
- G101: Sono stati accettati i cookie di analisi e non di marketing.
- G111: Sono stati accettati i cookie di marketing e di analisi.

Il secondo metodo per la verifica del funzionamento del Google Consent Mode è quello mediante l'ispezione del datalayer che viene salvato. Per procedere con questa opzione, si va nella console Javascript del browser e si digita "dataLayer" premendo invio. Si aprirà così una schermata come quella in Figura 5.21.

È possibile notare che il datalayer è correttamente popolato, poichè la situazione di default quando un utente arriva nel sito web è impostata su "denied" per le categorie dei cookie

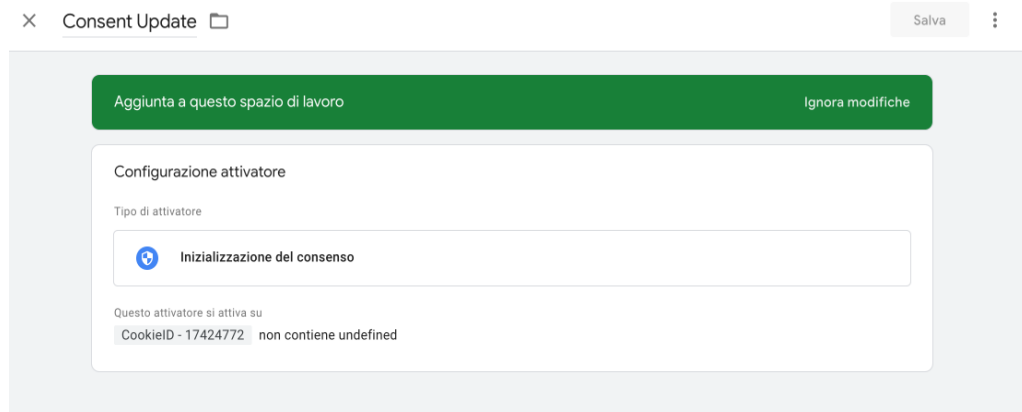


Figura 5.19: Attivatore del tag per lo stato di "update"

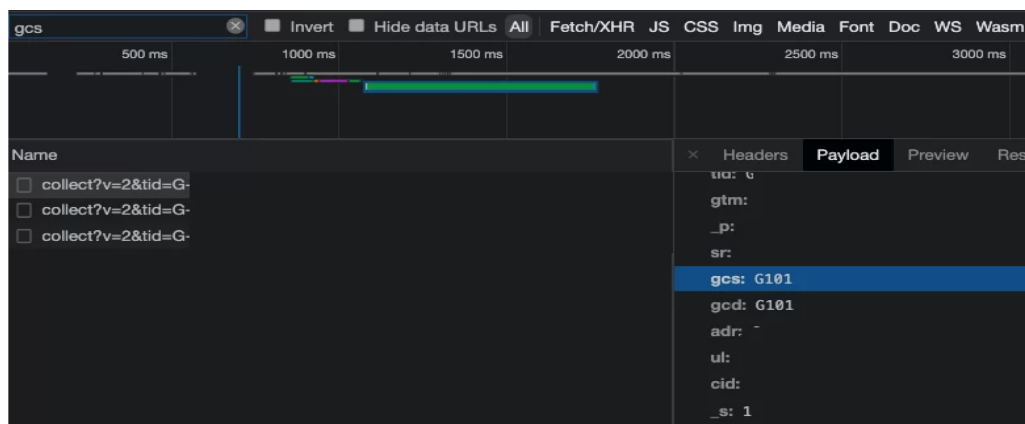


Figura 5.20: Debug del parametro GCS tramite console

analitici e di marketing. Nel caso in cui questi due test diano esito negativo, è opportuno ricontrollare l'implementazione, altrimenti ci saranno dei problemi con il Google Consent Mode.

5.3.4 Implementazione API per traffico sul sito

Precedentemente è stato menzionato che, per attivare il Google Consent Mode ed iniziare ad addestrare il suo modello, è necessario raggiungere delle soglie di traffico. In particolare, è necessario:

- avere una soglia giornaliera di click dell'annuncio di 100 click al giorno, per paese e raggruppamento di dominio per il modello di attribuzione di Google Ads;
- la proprietà di Google Analytics deve raccogliere almeno 1000 eventi al giorno con "analytics_storage='denied'" per almeno 7 giorni;
- la proprietà di Google Analytics deve avere almeno 1000 utenti giornalieri che inviano eventi con analytics_storage='granted' per almeno 7 dei 28 giorni precedenti.

Nel caso di studio non è stata possibile raggiungere la prima soglia di traffico poichè doveva esserci una vera e propria campagna di marketing in azione, con dei costi giornalieri e con degli utenti che realmente andavano ad effettuare conversione.

Per quanto riguarda la seconda e la terza soglia si è pensato di costruire un'API ad hoc per raggiungere i requisiti richiesti. Si è scelta questa soluzione al fine di generare traffico sul sito

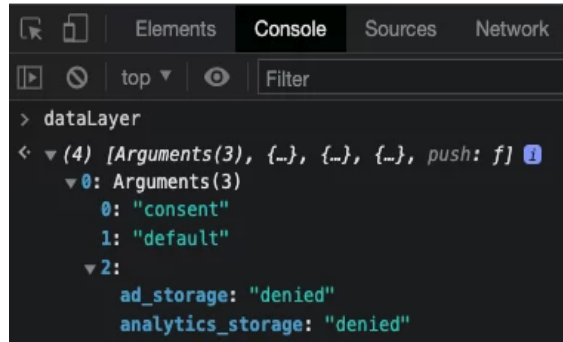


Figura 5.21: Debug mediante l'ispezione del datalayer

creando degli userID randomici, simulando i due principali casi d'uso descritti, quello del completo rifiuto dei consensi e quello della completa accettazione di essi.

L'API è stata costruita in Python e la sua progettazione è stata configurata in modo tale da inviare a Google Analytics 1000 utenti giornalieri simulando contemporaneamente due scenari; essi sono:

- utenti che non accettano cookie ed effettuano le conversioni di purchase e "page_view" (con parametro GCS impostato a 100),
- utenti che accettano tutti i cookie ed effettuano le conversioni di purchase e "page_view" (con parametro GCS impostato a 111).

L'API è stata fatta partire per più del tempo di richiesto con l'obiettivo di assicurarsi l'attivazione del modello del Google Consent Mode.

L'API è presentata nel seguente listato:

```

1
2 import requests
3 import json
4 import time
5 import random
6 import calendar
7 import string
8
9
10
11 # Dati delle proprietà GA4
12 webStreams = [
13     {'name': 'GA4_test-GCS=100',
14      'measurementId': 'G-8E4SH08FZL',
15      'gcs': '100',
16      'secret': 'DTtG5jKmSt2mvoDw-yj8Yg'},
17     {'name': 'GA4_test-GCS=111',
18      'measurementId': 'G-03HQFL22KX',
19      'gcs': '111',
20      'secret': 'MjvaNvtwSuKRH_9hAC8HCQ'}
21 ]
22
23
24 def generate_random_string(length):
25     characters = string.ascii_letters + string.digits
26     random_string = ''.join(random.choice(characters) for _ in range(length))
27     return random_string
28
29 i = 0

```

```
30 while i < 1000:
31     for stream in webStreams:
32         # Queste variabili crea l'ID utente, cid e un timestamp casuale per il
33         session ID
34         current_GMT = time.gmtime()
35         cid_id = random.randint(10000000, 999999999)
36         cid_ts = calendar.timegm(current_GMT)
37
38         #random valore e transaction ID
39         random_value = generate_random_string(10)
40         random_price = random.randint(1, 500)
41
42         url = f"https://www.google-analytics.com/mp/collect?api_secret={stream
43         ['secret']}&measurement_id={stream['measurementId']}&gcs={stream['gcs']}&v
44         =2&dl=http%3A%2F%2Ffoo.com%2Fhome%3Fa%3Db&ul=en-us&de=UTF-8&sr=800x600&geoid
45         =IT"
46
47         headers = {
48             "Content-Type": "application/json"
49         }
50         cid = str(cid_id) + "." + str(cid_ts)
51         print(cid)
52
53         # Create payload for each event
54         payload = {
55             "client_id": cid,
56             "non_personalized_ads": False,
57             "events": [
58                 {
59                     "name": "page_view",
60                     "params": {
61                         "page_location": "https://www.coldman95.github.io/
62                         ecommerce-template-ppc/products.html",
63                     }},
64                 {
65                     "name": "purchase", # "page_view", # nome dell'evento
66                     "params": {
67                         "items": [
68                             {
69                                 "item_id": "SKU_12345",
70                                 "item_name": "pc gaming",
71                                 "quantity": 1,
72                                 "affiliation": "Google Store",
73                                 "coupon": "SUMMER_FUN",
74                                 "discount": 2.33,
75                                 "item_brand": "Gucci",
76                                 "item_category": "PC",
77                                 "tax": 1.22,
78                                 "price": random_price ,
79                                 "currency": "EUR"
80                             }
81                         ],
82                     "affiliation": "Google Store",
83                     "coupon": "SUMMER_FUN",
84                     "currency": "EUR",
85                     "transaction_id": random_value,
86                     "shipping": 0.99,
87                     "tax": 12,
88                     "value": 500,
89                     'currency': "EUR",
90                     "client_id": cid,
91                     "ga_session_id": cid_ts,
```

```
87         "ga_session_number": 1
88     }
89 }
90 ]
91 }
92
93 # Convert payload to JSON
94 payload_json = json.dumps(payload)
95
96 # Send the POST request
97 response = requests.post(url, data=payload_json, headers=headers)
98
99
100
101
102 # Print the response
103 print(i)
104 print(f"URL: {url}, Stream: {stream['name']}")
105 print(response.status_code)
106 print(response.text)
107 print(random_value)
108 print(random_price)
109 i += 1
```

Source Code 5.1: API per traffico su sito web

Nel dettaglio, il Listato 5.1; inizia dichiarando le varie librerie utili al suo funzionamento per poi creare dei webstreams per collegare le due proprietà Google Analytics nelle quali si è andato ad applicare il Google Consent Mode. Ad una proprietà, indicata con "measurement-id" è stato mandato il parametro GCS impostato a "100", per simulare il traffico di utenti che abbiano rifiutato i cookie. Nell'altra proprietà, è mandato lo scenario opposto, cioè quello in cui l'utente ha accettato tutti i cookie. Si è pensato di ricorrere a questa soluzione per cercare di mostrare le dashboard da due punti di vista differenti, uno in cui il modello di attribuzione del Google Consent Mode è completamente disattivato e un altro dove è sempre attivato, in modo da mostrare le differenze statistiche che ci sono tra le due proprietà di Google Analytics.

Si è proceduto, poi, a mandare 1000 utenti giornalieri ad entrambe le proprietà creando uno userID randomico e un timestamp differente per ogni utente, in modo che Google Analytics lo avrebbe riconosciuto come un utente univoco.

Successivamente sono stati creati due eventi di conversione usando una struttura data-layer, uno per simulare un acquisto all'interno del sito web e l'altro la visualizzazione di una specifica pagina. La parte riguardante l'evento "page_view" è, semplicemente, creata dando il nome corretto all'evento per il conteggio da parte di analytics e indicando un URL specifico della pagina. Per quanto riguarda l'evento di acquisto, invece, è stato dato il nome dell'evento "purchase" e sono stati passati ad esso dei parametri che si riferiscono sempre allo stesso oggetto, ma che ogni volta cambia di prezzo e di ID transazione. In questo modo si avranno dei dati diversificati.

In conclusione, la scelta di creare un API si è rivelata vincente, poichè ha rappresentato un metodo per simulare traffico all'interno del sito facilitando la riuscita del caso studio per il raggiungimento delle rigide metriche richieste da Google al fine di attivare il modello di attribuzione del Google Consent Mode.

5.3.5 Risultati ottenuti

Dopo l'attivazione del modello di Machine Learning, Google Analytics e Google Ads, attraverso degli algoritmi di modellazione, integrano i dati raccolti direttamente, ovvero i

dati degli utenti che hanno dato il consenso, con i dati stimati relativi agli utenti che non hanno lasciato il loro consenso. In questo modo si potrà avere una visione più completa del traffico del sito. Inoltre, il sito è stato fatto aprire ogni giorno a dei colleghi lavorativi che lo hanno messo in background durante l'orario di lavoro per cercare di attirare anche utenti veritieri al fine di mostrare risultati vicini a quelli che potrebbero essere di un caso reale.

I benefici del Google Consent Mode dipendono da molti fattori, come, ad esempio, la richiesta di consenso che deve essere ottimizzata, cioè cercare di avere quante più accettazioni possibili di cookie, ma comunque ci sono numerose variabili.

Le prime due dashboard che vengono messe a confronto riguardano quando il modello di Machine Learning è passato da una fase di apprendimento alla fase in cui entra in azione.

Nelle Figure 5.22 e 5.23 vengono mostrate le principali differenze.



Figura 5.22: Entata in azione del modello di attribuzione del Google Consent Mode

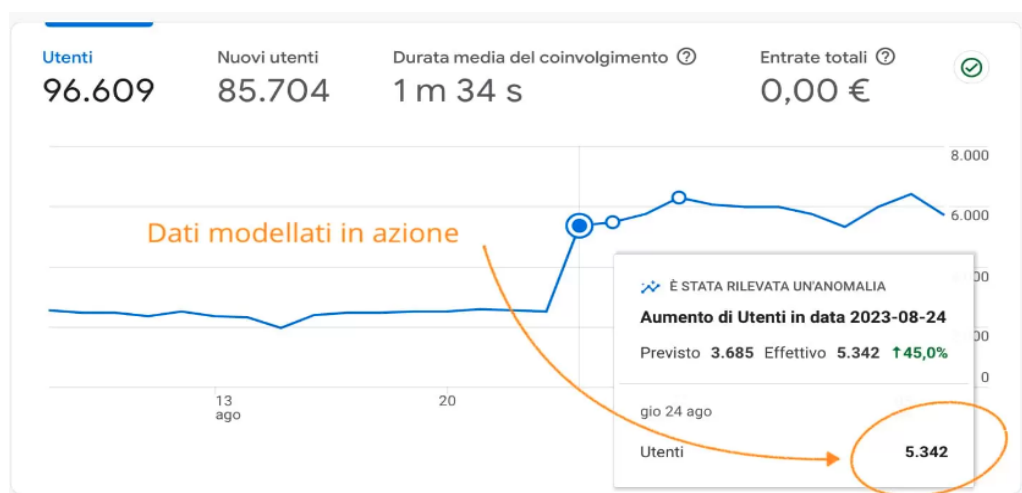


Figura 5.23: Entata in azione del modello di attribuzione del Google Consent Mode

La Figura 5.22 ci mostra che c'è stato un totale di 96.609 utenti raccolti nel mese di agosto, ma il dato più importante riguarda il fatto che fino al 23 agosto il modello rimaneva sempre su un livello costante di identificazione degli utenti che al giorno 23 agosto, si aggirava su una media di 2400 utenti tracciati. Nella Figura 5.23, invece, è mostrato che il modello è entrato in azione avendo un tracciamento che, grazie al Machine Learning, era previsto di

3685 utenti ma che poi è diventato effettivamente di 5342 utenti. Si nota, quindi, che, grazie al Google Consent Mode sono stati tracciati e profilati il 45% in più degli utenti visitanti il sito.

Altre due dashboard che vengono messe confronto sono quelle che descrivono gli utenti che sono stati catturati nello specifico in Polonia, in questo caso persone vere che hanno tenuto il sito aperto negli ultimi 7 giorni di Agosto, quindi non utenti generati da API. Si nota che ci sono differenze nello stesso arco di tempo tra le due proprietà.

Le dashboard sono mostrate nelle Figure 5.24 e 5.25.

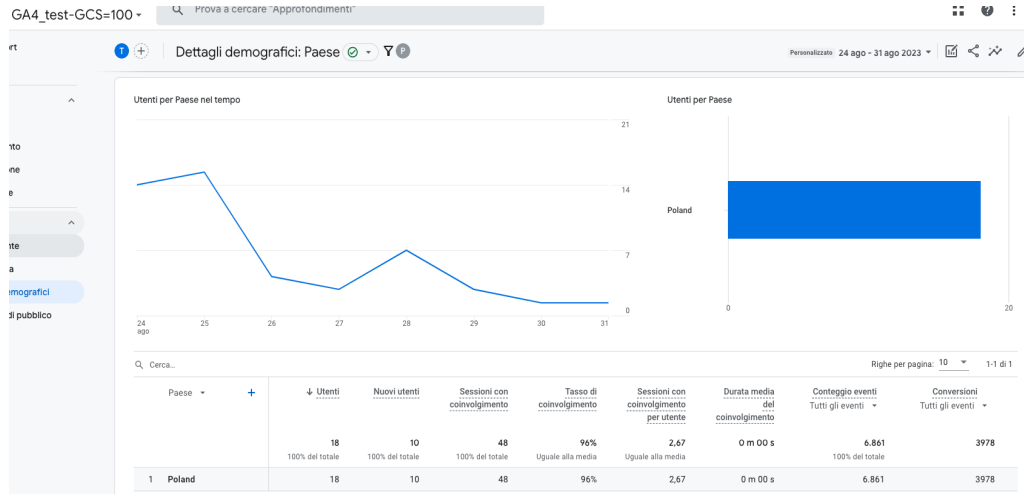


Figura 5.24: Sessioni nella proprietà con GCS 100

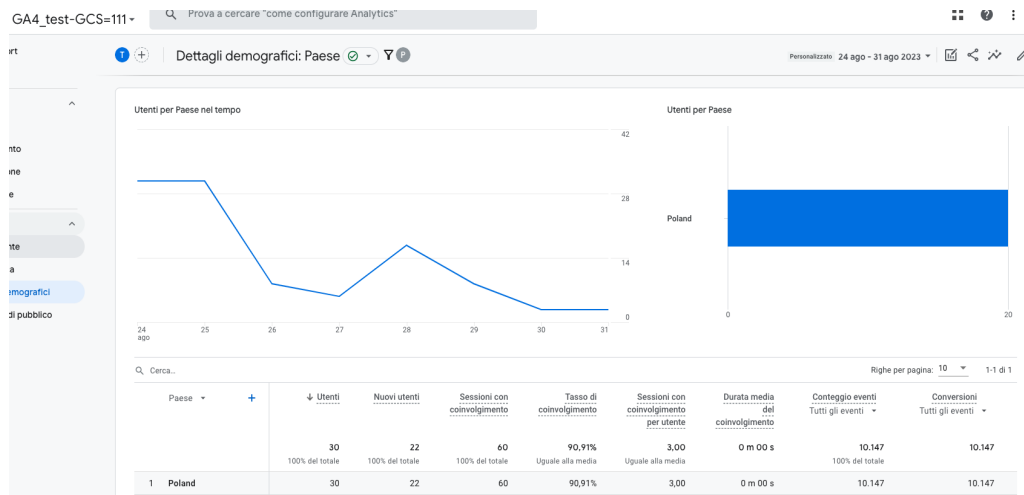


Figura 5.25: Sessioni nella proprietà con GCS 111

Nella figura 5.24 è mostrato che la proprietà in cui il Google Consent Mode non è attivo. È stato preso come arco temporale il periodo che va dal 24 agosto al 31 agosto 2023, in cui gli utenti sono stati 18 con un totale di 6,861 eventi mandati dall'API ma solo parte di essi sono stati riconosciuti come conversioni (3978). Nella Figura 5.25, invece, gli utenti nello stesso periodo in cui il Google Consent Mode era attivato ammontano a 30 con un conteggio di eventi pari a 10.147. Da notare, però, che il 100% di essi è stato riconosciuto come conversione, si è quindi colmata questa differenza rispetto allo scenario senza Google Consent Mode.

In conclusione, come nel risultato precedente, anche qui è presente un aumento di circa il 40% di utenti recuperati ma soprattutto il riconoscimento di tutti gli eventi come eventi di conversione.

A questo punto, vengono presentate altre due dashboard che analizzano gli acquisti e le sessioni riguardante gli acquisti che sono arrivate tramite lo stream API chiamato "Test", mettendo sempre a confronto le due proprietà precedentemente menzionate. Anche qui si prende come riferimento il periodo in cui il modello del Google Consent Mode è entrato in azione. Nelle figure 5.26 e 5.27 è mostrato quanto precedentemente descritto

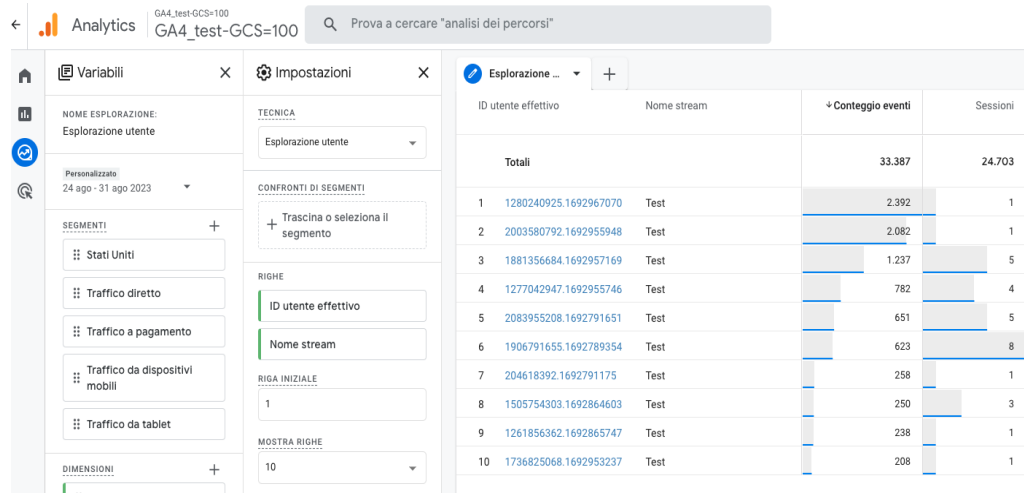


Figura 5.26: Conversioni di acquisto nella proprietà con GCS 100

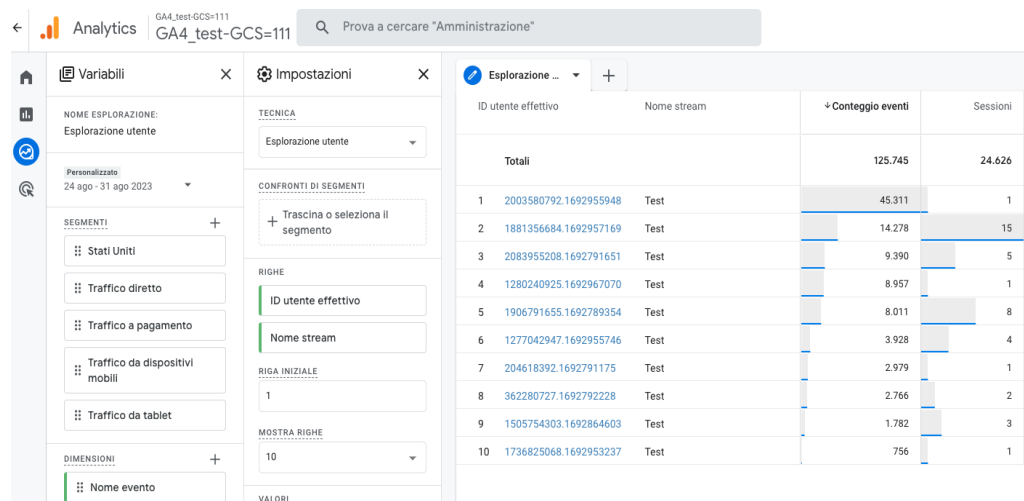


Figura 5.27: Conversioni di acquisto nella proprietà con GCS 111

Nel report mostrato in Figura 5.26 il conteggio degli acquisti ammonta a 33.387 acquisti per un totale di 24.703 conversioni. Nella dashboard in Figura 5.27, invece, gli eventi di conversione di acquisto ammontano a 124.743 con un numero di sessioni addirittura inferiore rispetto al precedente. Questo risultato risulta un pò sorprendente, poichè dovrebbero registrarsi anche aumenti di sessione collegati all'aumento degli acquisti. In conclusione, è possibile che il modello di machine learning nella proprietà in cui è attivo va a recuperare tutte le conversioni di acquisto anche in caso di rifiuto del cookie. A testimonianza di questo, le sessioni risultano essere più o meno le stesse ma mancano eventi di conversione associati ad esse. Qui il recupero di conversioni di acquisto è stato notevole, poichè si è registrato un aumento di circa 4 volte.

Conclusioni e uno sguardo al futuro

In questo capitolo finale, si andranno a riassumere le conclusioni e le opinioni dell'elaborato presentato, basandosi sui risultati proposti nel case study. Inoltre, si presenteranno l'alternativa sulla quale Google sta lavorando per non utilizzare i cookie di terze parti e i possibili benefici che potranno esserci da questa eventuale soluzione

6.1 Conclusioni

La società in cui viviamo oggi è in continuo cambiamento, caratterizzata da numerose e ricorrenti innovazioni tecnologiche, sempre più ricorrenti in diversi settori della vita quotidiana. Appare evidente come le società maggiormente sviluppate dal punto di vista tecnologico si identifichino come società dell'informazione poichè, appunto, in esse le informazioni sono considerate risorse strategiche e di valore, in cui gli individui non sono soltanto circondati da un flusso incessante di dati, ma sono diventati essi stessi dei dati. La rilevazione e il monitoraggio, da parte di tecnologie e dispositivi, stanno diventando giorno dopo giorno sempre più frequenti e la targetizzazione dell'utente in base alle sue caratteristiche comportamentali sta diventando un business piuttosto remunerativo.

Tale sistema presenta comunque una natura piuttosto pervasiva ed invasiva; pertanto, risulta necessario porre attenzione alla protezione della privacy in relazione all'attività di profilazione e di trattamento automatizzato di dati, specie se da tale trattamento scaturiscono effetti sulla sfera giuridica dell'individuo. Nell'elaborato, infatti, è stato presentato lo strumento con cui Google cerca di offrire agli utenti il rispetto della privacy ma, allo stesso tempo, un maggior tracciamento di essi.

Il Google Consent Mode è stato lanciato nel settembre 2020 come un modo per far mantenere a Google la sua solida attività di pubblicità digitale, e allo stesso tempo, di rispondere alla crescente esigenza di privacy dei consumatori sulla scia di un numero sempre maggiore di violazioni dei dati. Questo strumento consente di controllare la memorizzazione dei tag cookie in base alle scelte di consenso degli utenti e di mantenere un equilibrio tra gli interessi aziendali e la privacy degli utenti.

Rispondere alla domanda "perchè si dovrebbe utilizzare il Google Consent Mode" è molto semplice; esso, infatti, garantisce la conformità al GDPR, che è molto importante, ma è un requisito, piuttosto che un vantaggio. Ad oggi, la maggior parte della copertura mediatica sulla privacy dei dati si concentra ancora su ciò che le aziende e la pubblicità perdono, piuttosto che su ciò che guadagnano.

Con il Google Consent Mode il marketing basato sui dati non solo è possibile, ma è a prova di futuro. E fa balzare le aziende in avanti rispetto ai concorrenti, che sono ancora bloccati nel tentativo di capire come continuare a raccogliere i dati senza l'utilizzo di questa piattaforma. Le aziende devono rispettare le leggi sulla privacy e hanno bisogno dei dati degli utenti per prendere decisioni di marketing e assicurarsi le entrate pubblicitarie. Questi requisiti funzionano bene insieme e la modalità di consenso di Google consente agli operatori dei siti web di recuperare oltre il 70% dei dati per gli inserzionisti. Di fatto, è possibile ottimizzare i tassi di opt-in e ottenere informazioni sulla conversione per coloro che non forniscono il consenso grazie al suo modello di Machine Learning che si addestra ricevendo sempre più dati basandosi su tutti gli scenari possibili relativi alla scelta del consenso dei cookie. Google Consent Mode rende, inoltre, sicuramente più facile l'implementazione dei tag Google, ci mette nelle condizioni di non dover bloccare manualmente i tag rischiando di commettere errori sui parametri e, soprattutto, errori di distrazione che, magari, ci fanno pubblicare dei tag senza rispettare le regole del GDPR.

Costruire e mantenere la fiducia degli utenti è sempre più fondamentale per il successo delle aziende, e la trasparenza è una parte importante di questo processo. Essere trasparenti sui requisiti della legge sulla privacy e sui motivi per cui si richiedono i dati degli utenti è una parte fondamentale di questo processo.

Infatti, il Google Consent Mode aiuta i gestori di siti web ad abbandonare la raccolta di massa dei dati personali degli utenti per passare a un sistema dinamico basato sul consenso. Il modello commerciale pubblicitario rimane intatto, pur rispettando la privacy degli utenti. Gli operatori di marketing continuano a ottenere i dati di cui hanno bisogno avendo, inoltre, un guadagno sulle conversioni e sulla profilazione dell'utente.

Concludendo è possibile dire che il Google Consent Mode, combinato con il modello di dati basato sugli eventi di Google Analytics 4 e Google Ads, offre alle aziende la possibilità di lavorare con set di dati più ricco, migliorando le potenzialità delle analisi dei dati in un mercato attento alla privacy.

6.2 Uno sguardo al futuro

A partire dalla seconda metà del 2024, Google smetterà di utilizzare i cosiddetti cookie di terze parti sul browser Chrome. Una scelta che, per gli esperti di marketing, i gestori di siti web e gli utenti Internet, comporterà alcuni cambiamenti.

Questo tipo di cookie viene inserito nei siti web o nei domini da fornitori terzi. Questi cookie, noti anche come tracking code, consentono di analizzare il comportamento degli utenti su diversi siti web e per un periodo di tempo più lungo. Talvolta vengono creati interi profili utente, dai quali trae vantaggio soprattutto l'industria pubblicitaria. I dati tracciati consentono di mostrare agli utenti pubblicità mirate. È anche possibile che un cookie sia stato creato come cookie di prima parte e venga registrato come cookie di terze parti (o viceversa).

Nel corso degli ultimi anni i cookie di terze parti sono stati sempre più oggetto di critiche sul piano della protezione dei dati. Questo ha aumentato la pressione sui fornitori di browser, come Google, affinché sospendano questa forma di tracking.

Google ora ha intenzione di disabilitare o vietare questi cookie di terze parti nel browser Chrome a partire dalla seconda metà del 2024. Una misura già adottata da altri browser: Microsoft Edge, Firefox e la versione di Apple Safari bloccano ormai da tempo l'uso dei cookie di terze parti. Ma dal momento che Google Chrome è il leader indiscusso tra i browser a livello mondiale (con oltre il 65%), la decisione di Google è considerata estremamente significativa nel settore.

Il motivo di questa misura è, indubbiamente, la protezione dei dati: nel quadro dell'iniziativa "Privacy Sandbox", Google intende elaborare alternative ai cookie di terze parti più

rispettose della privacy. Originariamente, Google voleva offrire nuove opzioni di tracking già nel corso del 2023 e, quindi, mettere fine ai cookie di terze parti. Tuttavia questi piani sono stati progressivamente rimandati, principalmente per mancanza di tempo e risorse, ma anche perché Google, a differenza di altri fornitori di browser, deve affrontare alcune questioni legali in quanto operatore a integrazione verticale.

I piccoli fornitori di tecnologie pubblicitarie che competono con Google, invece, hanno il problema di avere un modello di business fortemente incentrato sui cookie di terze parti. Nel medio termine, volenti o nolenti, dovranno, quindi, trovare nuove soluzioni. Tutte le parti coinvolte, in particolare gli operatori pubblicitari che, con l'eliminazione dei cookie di terze parti, all'improvviso potranno raggiungere solo il 20-30% del gruppo target originale, si trovano ora a dover elaborare nuove soluzioni che siano conformi alle leggi sulla protezione dei dati. Alcune soluzioni esistono già: Google sta attualmente testando quelle di FLEDGE e Topics nel quadro della cosiddetta "Privacy Sandbox". La prima permette di contrassegnare e raggruppare in gruppi target gli utenti di un sito web, mentre Topics attribuisce gli utenti a determinati segmenti di gruppi target in base alle loro ultime visite, in modo da poterli approcciare almeno come gruppo aggregato.

Esiste anche un approccio improntato sulla trasparenza che si concentra interamente sui cookie di prima parte; esso punta a ottenere il massimo dalle informazioni e dai mezzi esistenti ad oggi, purché nel rispetto delle leggi sulla protezione dei dati. Anche in questo settore si stanno creando nuovi incentivi per gli utenti promuovendo nuove possibilità di tracking proporzionato grazie alle tecnologie avanzate.

Tuttavia, Google potrebbe trarre vantaggio dall'intero processo di trasformazione e consolidare ulteriormente la propria posizione di leader. Infatti, come Facebook (Meta) o Amazon, Google è già in possesso di una grande quantità di dati degli utenti. Questo significa che, a differenza di molti operatori pubblicitari, Google non deve fare affidamento sui cookie di terze parti.

Il consenso non solo rimane cruciale nella maggior parte delle normative sulla privacy dei dati, ma sta anche assumendo sempre maggiore rilevanza per l'industria pubblicitaria stessa. Tale tendenza è consolidata dal lancio del Google Consent Mode nel settembre 2020, il quale permette ai siti web di eseguire tutti i servizi Google sulla base del consenso degli utenti finali, trovando, in tal modo, un equilibrio tra la conformità e il tracciamento consensuale.

Google Consent Mode rappresenta un chiaro segnale del fatto che Google, una delle più importanti aziende tecnologiche a livello mondiale, intende orientare l'industria ad-tech verso la direzione del consenso e introdurre un più giusto equilibrio tra la pubblicità digitale e la privacy dei dati personali.

Quindi, mentre è vero che i cookie di terze parti potrebbero scomparire nei prossimi anni, il consenso è destinato a prendersi sempre più la scena, con un ruolo da protagonista su Google e non solo, integrandosi ancora più a fondo e in maniera sistematica con le tecnologie di tracciamento del futuro e con l'industria ad-tech stessa.

- ANTONACCI, F. (2023), «E-commerce e digital marketing. Strategie SEO, Google Ads, Web Analytics per vendere online», *Franco Angeli*.
- BARBAROSSA, F. (2010), «Google marketing. Guida al più grande mercato del mondo», *Franco Angeli*.
- BIASOTTI, A. (2016), «Il nuovo regolamento europeo sulla protezione dei dati», *EPC editore*.
- FETTMAN, E. (2016), «Google Analytics Breakthrough», *Wiley*.
- GOLDMAN, A. (2010), «Everything I Know about Marketing I Learned From Google», *McGraw Hill LLC*.
- HARTMAN, K. (2023), «Digital Marketing Analytics: In Theory And In Practice», *Ostmen Bennettsbridge Publishing Services*.
- LOCSEA (2016), «Digital Marketing using Google Services», *Balu*.
- MCGRUER, D. (2020), «Dynamic Digital Marketing», *Wiley*.
- STEFANI, F. D. (2010), «Cil GDPR per il marketing e il business online. Gestire correttamente siti, blog e social network», *Hoepli*.
- TRAFICANTE, F. (2015), «Cookie, Profilazione On-Line e Web Marketing: Privacy e Digital Marketing: binomio possibile!», *CreateSpace Independent Publishing Platform*.

Websites consulted

- Vocabolario Treccani – www.treccani.it
- UniverseIT - blog per manager e professionisti del settore – www.universeit.blog
- CookieYes Cookie Consent Solution – www.cookieyes.com
- Google Cloud Solutions – www.cloud.google.com
- Panda Security | Official Website – www.pandasecurity.com

-
- GeeksforGeeks | A computer science portal for geeks – www.geeksforgeeks.org
 - Iubenda | Cookie consent management platform – www.iubenda.com
 - Cookieboot CMP – www.cookiebot.com
 - Google Help – www.support.google.com
 - Google for Developers - Software Development Guides www.developers.google.com
 - IT Governance - Governance and Risk Management – www.itgovernance.eu
 - Peak Metrics – www.peakmetrics.net
 - Hostpoint | Domini, web hosting, managed server e molto di più! – www.hostpoint.ch/it
 - Simo Ahava's blog: Google Tag Manager and Google Analytics – www.simoahava.com/