EJPLT

European Journal of Privacy Law & Technologies • 2021/1 • ISSN 2704-8012



Cookies e consenso: le nuove prospettive.

Cookies and consent: the new perspectives.

MARIA ROBERTA PERUGINI
Lawyer

Abstract

Fin dagli esordi della disciplina del marketing comportamentale sono stati evidenziati gli effetti potenzialmente deleteri (in termini di alto rischio di violazioni dei dati personali e dei diritti degli utenti) derivanti dell'uso di identificativi univoci online, tanto più in quanto usati in sinergia con i più sofisticati strumenti di data mining.

L'articolo schematizza la storia e le problematiche collegate all'uso di marcatori online per farne emergere con chiarezza e concretezza il punto di arrivo sulle azioni oggi richieste per operare legittimamente i trattamenti a fini di marketing e profilazione che si basano sull'uso di queste tecnologie. Infine, l'articolo affronta brevemente le nuove frontiere del behavioural advertising nel contesto a tendere "cookieless".

Parole chiave: Cookies; GDPR; Direttiva e-Privacy; Proposta di Regolamento e-Privacy; Pubblicità comportamentale; Pubblicità programmatica; Monitoraggio online; Profilazione; Consenso; senza Cookies; EDPB; Corte di Giustizia.

Keywords: Cookies; GDPR; E-Privacy Directive; Proposal for an e-Privacy Regulation; Behavioural advertising; Programmatic advertising; Tracking online; Profiling; Consent; Cookieless; EDPB; Justice Court.

Summary: Introduzione. – 1. Gli esordi della disciplina di riferimento per il marketing comportamentale: i rischi. – 2. Gli esordi della disciplina di riferimento per il marketing comportamentale: le misure per mitigare il rischio. – 3. La normativa applicabile alle tecnologie di tracking online: le norme rilevanti. – 4. Le norme rilevanti per le tecnologie di tracking online: i rispettivi campi di applicazione… – 5. … e le regole di interazione. – 6. Tracking online e profilazione: quali basi giuridiche? – 7. La portata del consenso. – 8. La ricerca di una visione paneuropea. – 9. Il consenso per i marcatori online: quali caratteristiche operative? Aspetti che possono essere considerati risolti. – 10. Caratteristiche operative del consenso per i marcatori online: i problemi ancora aperti. – Conclusione: Verso un marketing digitale senza third party cookies.

Introduzione.

Parlare di cookies (e altri marcatori della navigazione web) significa parlare di behavioural advertising.

Fin dagli esordi della disciplina del marketing comportamentale sono stati evidenziati gli effetti potenzialmente deleteri (in termini di valutazione di alto rischio di violazioni dei dati personali e dei diritti degli utenti) derivanti dell'uso di identificativi univoci online, tanto più in quanto usati in sinergia con i più sofisticati strumenti di data mining.

Ciò che accade è che si sono affermate tecniche di "targetizzazione" delle inserzioni pubblicitarie via via sempre più precise, che cercano di indirizzare i contenuti agli utenti mediante la conoscenza sempre più esatta delle loro propensioni ed esigenze.

Il marketing comportamentale funziona sfruttando le tecnologie di tracciabilità (tracking) delle operazioni dei navigatori online: attraverso l'analisi di marcatori, soprattutto **cookies di prima e di terza parte** [1], è possibile risalire al numero di visite a determinati siti, alle ricerche effettuate sul web, agli acquisti conclusi su certi e-shop, al tempo globale passato su internet, ma anche all'attività sui social ...

Tutti questi dati vengono utilizzati per tracciare un profilo "pubblicitario" personalizzato di ogni singolo navigatore, il quale viene inserito in appositi filtri e dunque viene raggiunto da advert appositamente pensati per le sue caratteristiche. Dunque, è probabile che se, ad esempio, un utente ha acquistato un libro su Amazon, altre pubblicità su siti diversi gli proporranno libri simili o dello stesso autore.

Lo scopo di tale strategia comunicativa è quella di "contattare" o "ricontattare" gli utenti sulla base delle loro precedenti azioni su internet, al fine di portare quel determinato utente a concludere l'azione commerciale sperata (una cosiddetta "conversione": vale a dire, effettuare un acquisto o completare un acquisto "abbandonato", lasciare i propri contatti, iscriversi alla newsletter, etc).

[1] I cookie di "prima parte" sono quelli rilasciati nel terminale dell'utente direttamente dall'editore/gestore del sito che l'utente sta visitando; quelli di "terza parte" sono invece creati da dominî differenti da quello in cui si sta navigando, generalmente grandi piattaforme di advertising (la principale è Double Click di Google): i cookies permangono nel terminale dell'utente e tracciano la sua navigazione segnalando ai server dell'emittente le attività che l'utente svolge online. In questo modo, specialmente i cookie di terza parte diventano strumento essenziale, ed estremamente efficiente, per una profilazione dell'utente cross-site, che produce profili altamente dettagliati e precisi del consumatore e di conseguenza permette da un lato la personalizzazione del messaggio promozionale e dall'altro il suo inserimento in target group altamente definiti, da utilizzare nelle campagne di retargeting nell'ambito del programmatic advertising.

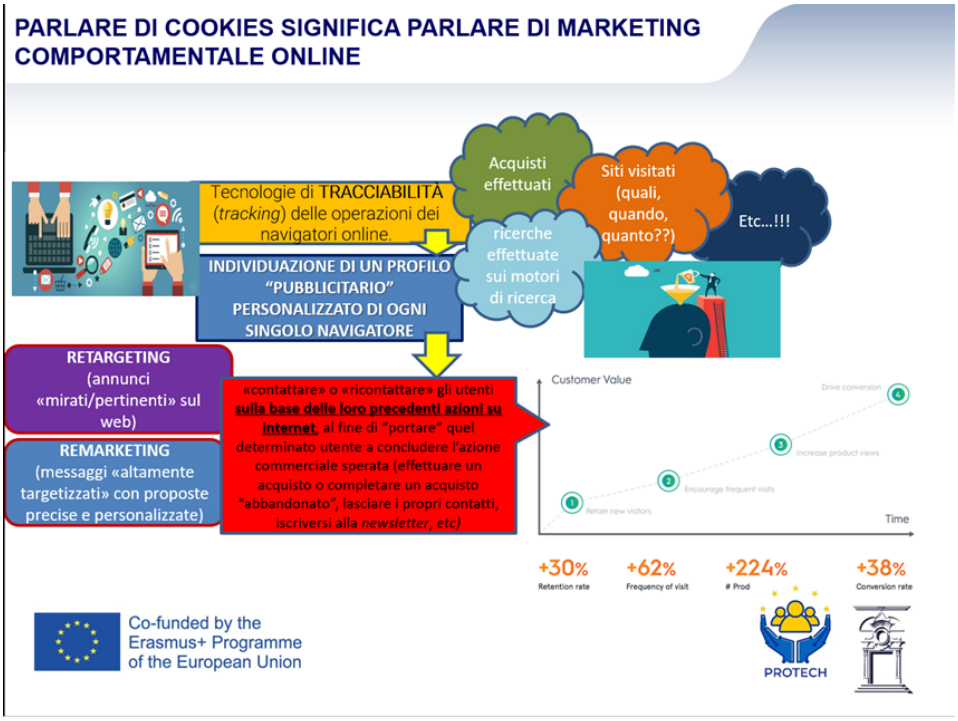


Figura 1

In particolare, si parla di **remarketing** o **retargeting** per indicare, nell'accezione più ampia dei termini, quella forma di marketing comportamentale basata sull'utilizzo dei cookies consistente nell'invio di messaggi/annunci pubblicitari agli utenti che sono transitati su uno specifico sito affinché ritornino sullo stesso sito per effettuare/completare un'azione significativa.

Più specificamente, il retargeting è lo strumento che permette di recuperare la comunicazione con l'utente (non convertito), mostrandogli annunci o inserzioni pertinenti mentre naviga sul web, mentre il remarketing (che si rivolge ai contatti, che hanno già eseguito la conversione e di cui si possiedono nome, cognome e/o altre informazioni di contatto) "riaggancia" l'utente tramite l'invio di messaggi diretti allo stesso (email) altamente "targettizzati" (con una proposta precisa e personalizzata) al fine di tentare di coinvolgerlo ancora una volta e convincerlo a trasformare le proprie intenzioni in azioni concrete.



Figura 2[2]

Ovviamente gli "over the top" (comunemente richiamati come OTT), come Google e Facebook, hanno elaborato propri strumenti di tecnologia pubblicitaria per attivare campagne di marketing comportamentale che mettono a disposizione di editori e inserzionisti: ad esempio Google AdWords o Facebook Ads, attraverso i quali gli **inserzionisti** possono pubblicare rispettivamente nelle pagine di ricerca di Google o all'interno di Facebook i loro annunci (di testo, banner, video) che verranno mostrati a persone potenzialmente interessate.

[2] Immagine estratta dal seguente sito: https://www.criteo.com/it/wp-content/uploads/sites/9/2017/07/Criteo-Retargeting101-eBook-IT.pdf

Enterprises' internet presence (use of internet ads by type, websites, social media), 2018

	Internet advertising	Contextual advertising	Behavioural targeting	Geo-targeting	Other method of targeted advertising	Having a website	Using social media*
	% of enterprises	% of enterprises using internet ads				% of enterprises	
EU-28	**26**	**80**	**32**	**37**	**38**	**77**	**47**
Belgium	30	71	33	38	43	84	58
Bulgaria	21	78	23	28	33	51	34
Czechia	31	89	32	36	41	83	36
Denmark	47	71	33	44	41	96	68
Germany	27	86	26	32	31	87	45
Estonia	28	74	54	40	58	78	40
Ireland	34	75	38	51	45	79	68
Greece	28	81	38	44	50	65	50
Spain	25	72	40	35	50	76	51
France	19	87	33	32	41	69	41
Croatia	27	68	30	22	24	73	45
Italy	21	75	25	38	42	71	44
Cyprus	33	83	48	55	9	71	67
Latvia	26	76	11	19	24	63	30
Lithuania	35	79	37	26	44	78	50
Luxembourg	36	63	25	33	35	83	54
Hungary	21	79	28	33	37	66	38
Malta	47	73	42	46	69	82	73
Netherlands	34	89	43	45	49	94	68
Austria	32	73	30	38	30	88	53
Poland	26	88	30	27	36	67	27
Portugal	16	75	42	45	55	63	46
Romania	15	90	41	32	38	44	35
Slovenia	22	93	30	31	5	84	47
Slovakia	25	75	32	23	42	76	39
Finland	37	83	49	44	31	96	63
Sweden	44	60	23	31	26	92	65
United Kingdom	32	78	37	47	40	82	63
Iceland	50	:	:	:	:	81	79
Norway	45	63	26	42	42	78	72
Montenegro	:	62	31	37	66	:	50
North Macedonia	:	:	:	:	:	:	:
Serbia	31	65	36	44	36	82	39
Turkey	15	82	53	63	32	66	46
Bosnia and Herzegovina	22	58	30	35	35	65	:

* Data on social media refer to 2017
(:) data not available

Source: Eurostat (online data codes: isoc_cismt, isoc_ciweb)

eurostat

Figura 3

È importante rilevare che questo mercato vede un fortissimo sviluppo anche grazie all'affermazione della navigazione e-commerce tramite le app piuttosto che tramite il tradizionale sito web: uno dei maggiori operatori mondiali nel retargeting, Criteo, ha stimato che già nel 2018 le vendite In-App rappresentavano fino al 65% delle transazioni online in Europa e che le app fanno registrare anche tassi di "conversione" (ossia di vendita) tre volte superiori rispetto a quelli del mobile web.

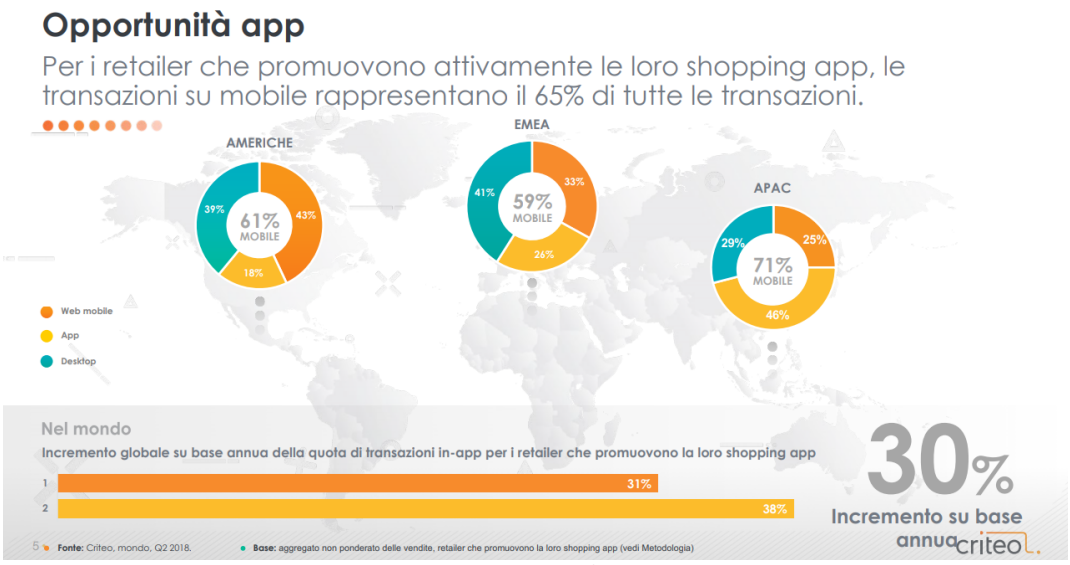


Figura 4[3]

Quindi Criteo ha sviluppato un sistema App Retargeting, che raggruppa le app di numerosi editori e consente di seguire l'utente nei suoi passaggi da un'app all'altra (ad esempio, da un'app di prenotazione viaggi ad una di gioco) in modo da tenerlo "agganciato" e ricondurlo con facilità alla transazione abbandonata.

Criteo ha dichiarato che tramite il proprio sistema "Criteo App Advertising" è in grado di acquisire dati da 1,2 miliardi di consumatori ogni mese, di avere una visione a 360 gradi e in tempo reale del comportamento di navigazione di un consumatore su dispositivi, browser e 550.000 app che il sistema utilizza per attirare ciascun utente con annunci ottimizzati in tempo reale in base all'intenzione di acquisto individuale e al contesto di navigazione, riportandolo all'app dove ha iniziato l'acquisto per completarlo.

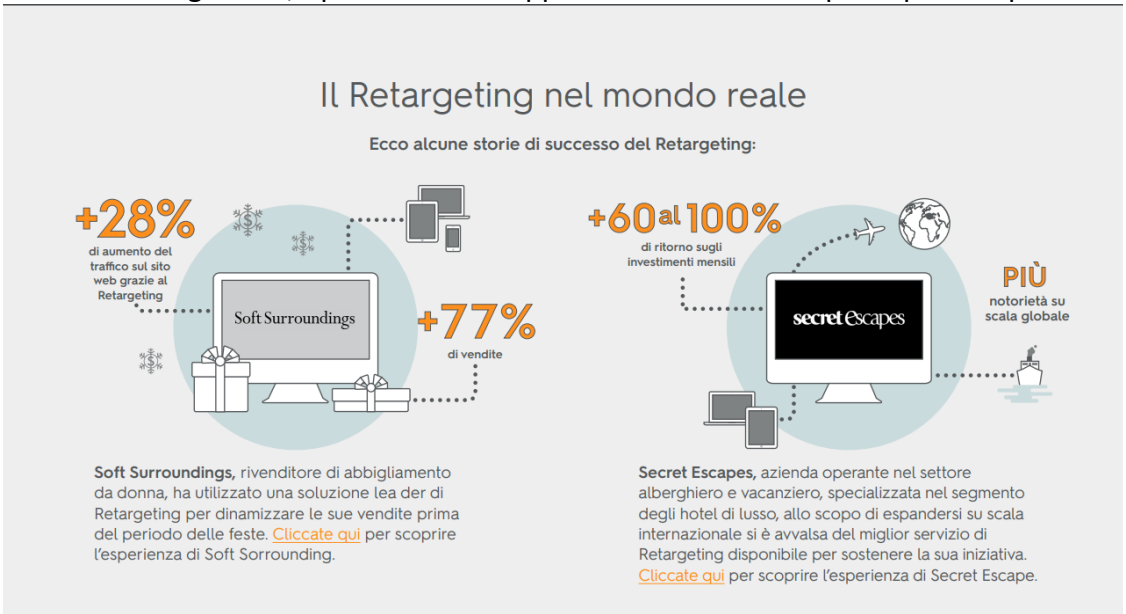


Figura 5

[3] Immagine estratta da: https://www.criteo.com/it/wp-content/uploads/sites/9/2018/09/18_GCR_Q2_Report_EMEA_IT.pdf

Criteo afferma altresì di essere il grado di identificare in modo univoco e anonimo su più di 2 dispositivi gli utenti da cui proviene oltre il 40% di tutte le vendite online.

Questo tipo di approccio comunicativo comporta naturalmente l'immagazzinamento di un numero molto elevato di informazioni sugli utenti del web.

Nel 2019 Apple ha introdotto sull'App store l'obbligo per gli sviluppatori di adottare "etichette" che indicano quali categorie di dati personali vengono raccolti dalle apps. Le categorie sono 14, tra cui la cronologia della navigazione, le ricerche fatte, gli acquisti, la geolocalizzazione, le informazioni di contatto, i dati finanziari… Il fornitore di servizi IT pCloud ha usato questa classificazione per censire il livello di dati raccolti per scopi commerciali da una serie di app tra le più popolari nel mondo.

Come mostrano le immagini, Facebook e Instagram sono quelle che usano più dati degli utenti (12 categorie su 14) per l'internal marketing (l'86%!), mentre sempre Instagram si distingue per la più massiva condivisione delle informazioni personali degli utenti con terze parti, sempre a fini di marketing, raccogliendo il 79% dei dati di 11 delle 14 categorie elencate.

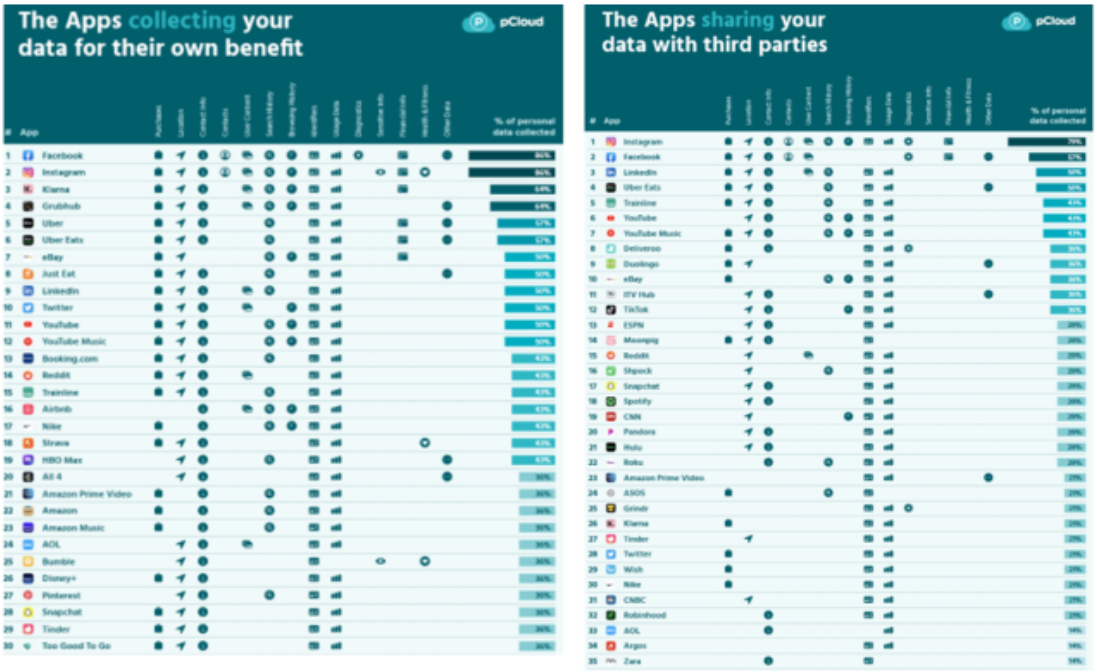


Figura 6[4]

Nella Figura 7 si possono vedere:

- uno stralcio della classifica delle 100 app più popolari nel mondo, stilata in ordine di invasività in termini di quantità di dati complessivamente raccolti e trattati per marketing interno e condivisione con terze parti: inaspettatamente, app come Amazon e Airbnb sono in fondo alla classifica (14%), mentre la parte del leone spetta a Instagram e Facebook;
- e anche la classifica delle app più virtuose.

[4] https://blog.pcloud.com/invasive-apps/



Figura 7[5]

1. Gli esordi della disciplina di riferimento per il marketing comportamentale: i rischi

Già alla fine degli anni '90 – nel vigore della Dir. 95/46/CE sulla protezione dei dati personali e della Dir 97/66/CE sulla tutela della vita privata nel settore delle telecomunicazioni – il WP29 mostrava con chiarezza quali fossero i punti focali della problematica: la **Racc. 1/99** evidenziava l'uso, già allora invalso, di tecniche di "clicktrails" – che si attuavano, all'insaputa dell'utente [6], mediante cookies di utenti internet identificati o identificabili – e ne deduceva la necessità di:

- stimolare una **configurazione dei software** che non consentisse il trattamento di default di informazioni persistenti dell'utente, lasciando invece all'utente stesso di **scegliere sempre** (i) "*se accettare o respingere la trasmissione o la memorizzazione di un cookie nel suo insieme*"; (ii) eliminare selettivamente informazioni "*in modo semplice e senza* (necessità della) *partecipazione del mittente*" del marcatore;
- **informare** l'utente in modo trasparente e comprensibile su "*quali informazioni s'intendono memorizzare nel cookie, ed a quale fine, nonché il periodo di validità del cookie stesso*". [7]

Nei primi anni 2000 poi il WP29 [8] sollevava specificamente anche altri aspetti più

[5] https://blog.pcloud.com/invasive-apps/

[6] Sulla mancanza di trasparenza della raccolta di dati effettuata in occasione della navigazione Internet, cfr. M. Viggiano, *«Navigazione» in internet e acquisizione occulta di dati personali*, Dir. Inf., 2007, II, 388; sul carattere occulto delle tecniche di profilazione online si veda anche A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa,* Milano, 2007, spec. 167 ss. e le opere ivi richiamate.

[7] WP17 – RACC. 1/1999 sul trattamento invisibile e automatico dei dati personali su Internet. In dottrina, sulla progressiva patrimonializzazione dell'informazione e l'evoluzione della normativa a protezione dei dati personali, cfr. A. Mantelero, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies,* in Dir. Inf, Vol. XXVIII, p. 781, 2012; Id. *Il costo della privacy tra valore della persona e ragione d'impresa,* cit. 171 ss.

[8] Cfr. doc. di lavoro WP37 sulla *"Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line",* adottato il 21 novembre 2000, in cui – nel contesto di una disamina di più di 100 pagine sugli aspetti tecnici di Internet e di specifici servizi (es. posta elettronica, chat, forum di discussione, pagamenti elettronici, browser, world wide web…), si analizzano sotto il profilo giuridico gli aspetti di rischio per la vita privata, anche in

specifici: prima il tema della rilevazione di dati personali effettuata tramite pseudonimi o numeri di identificazione non personalizzati e poi le caratteristiche di nuovi strumenti (il protocollo – allora nuovo – IPv6) [9] che, integrando un identificativo esclusivo nell'indirizzo IP del dispositivo, consentivano con sicurezza il collegamento tra loro di tutte le comunicazioni dell'utente che usa quel dispositivo.

Di conseguenza, già a quell'epoca il WP 29 identificava gli effetti di alto rischio per i dati personali e i diritti degli utenti che derivavano dell'uso di questi marcatori.

2. Gli esordi della disciplina di riferimento per il marketing comportamentale: le misure per mitigare il rischio.

Le conclusioni allora raggiunte quanto ai mezzi per mitigare questi rischi risultano tuttora estremamente attuali; quanto ai singoli siti, già allora il WP29 innanzitutto:

- chiedeva di adottare l'uso di meccanismi basati "perlomeno" sul diritto di opposizione al trattamento e comunque sul consenso informato e revocabile per la profilazione, prevedendo già la formula della finestra pop-up [10], e comunque capaci di garantire i diritti, oltre che di opposizione, anche di accesso, rettifica, cancellazione (anche selettiva) dei dati
- e dettava [11] gli elementi minimi dell'informativa, individuando obblighi informativi puntuali sia nell'oggetto (obbligo di fornire informazioni su tipo di dati raccolti, ambito di utilizzo e periodo di memorizzazione, nonché sulle finalità del trattamento, compresa la eventuale comunicazione a terzi) sia nella forma: anche questa raccomandazione già prevedeva l'uso del banner (casella prompt), da attivare a prescindere dalla capacità del browser di riconoscere e notificare all'utente il deposito del cookie.

Ma non solo: nella individuazione delle possibili azioni di mitigazione del rischio il WP29 assumeva anche un'ottica più generale, legata alle peculiarità di questo contesto in cui l'utente difficilmente percepisce ciò che accade e le conseguenze che possono verificarsi in termini di danno, e comunque raramente riesce ad agire di conseguenza in modo efficace, dovendo peraltro anche previamente identificare i responsabili.

Di conseguenza, il WP29 già all'epoca aveva:

a) sottolineato l'importanza dello sviluppo di tecnologie che "*migliorano, rispettano e sono conformi alla vita privata*", tra cui:
   - browser dotati di impostazioni predefinite in tale senso

---

tema di "cybermarketing": «*Queste informazioni devono essere fornite anche nei casi in cui i dati vengano rilevati usando pseudonimi o numeri di identificazione non personalizzati.*". Sul tema si veda anche WP28 – Op. 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali.

[9] Cfr. il parere WP37 2/2002 "*sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6*".

[10] Cfr. WP43 – RACC. 17/5/2001 relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione Europea, par. 2.2, par. 16, ma anche WP37, cit.

[11] Racc. 1/1999, cit.

- strumenti di navigazione anonima

b) e auspicato azioni di sensibilizzazione degli utenti su questi temi e l'adozione di una norma europea per le certificazioni sulla "vita privata".

Merita veramente rilevare come sin dall'inizio le analisi condotte sul trattamento occulto di dati personali e informazioni attinenti alla vita delle persone collegato alla navigazione online abbiano constatato l'insufficienza della sola applicazione di strumenti basati sul consenso informato e la necessità – perché la protezione sia effettivamente garantita – dell'integrazione con tecnologie che siano conformi alle norme by design [12].

3. La normativa applicabile alle tecnologie di tracking online: le norme rilevanti.

Tutte le analisi, pareri, raccomandazioni sul tema sono poi confluiti nella Direttiva 2002/58/CE, nella cui applicazione ricade l'uso di tecnologie di tracciamento online, cookies e altri [13].

Questa Direttiva assume un ruolo integrativo (anche in senso interpretativo ed esplicativo) rispetto a quella generale sulla protezione dei dati personali, come risulta chiaro sin dal suo esordio [14].

Oggi la Dir. 95/46/CE è stata sostituita dal GDPR, ma ciò non inficia la fattibilità dell'azione comune tra le due normative, che anzi le nuove norme generali sulla protezione dei dati prevedono esplicitamente (art. 95 e cons. 173) [15], così come prevedono infine un riesame – attualmente ancora in corso [16]– della Dir. e-Privacy al fine di garantirne omogeneità col GDPR[17].

---

[12] Sul ricorso a tecnologie conformate per consentire – in particolare nell'ambiente online - l'effettiva esplicazione del potere di controllo sui propri dati personali da parte dell'interessato, si veda A. Mantelero, *Digital privacy: tecnologie "conformate" e regole giuridiche*, in *Privacy digitale. Giuristi e informatici a confronto*, Torino, Giappichelli, 2005, 19 ss.

Non è questa la sede per approfondire l'argomento, ma merita rilevare che vi è da tempo ampia letteratura che osserva l'inidoneità di fatto del consenso a garantire tale controllo: *ex multis* cfr. S. Patti, *Il consenso dell'interessato al trattamento dei dati personali,* in *Riv. dir. civ.*, 1999, 467; L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2, 2017, 363 ss.; I. A. Caggiano, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in Annali 2016-2018 – Università degli Studi Suor Orsola Benincasa; A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa,* cit., 304.

[13] Questione poi ripetutamente affrontata da WP29, Opp. 1/2008, n. 148 e 2/2010, n. 171 e recentemente dettagliata nel parere dell'EDPB 5/2019 sulle interazioni tra GDPR e Dir. e-Privacy.

[14] Cfr. l'articolo 1, comma 2, che indica come: *"(…) le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE*".

[15] GDPR Art. 95: "*Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.*"; GDPR Cons. 173: "*È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche*.".

[16] Proposta di Regolamento e-privacy del 10 febbraio 2021: il testo è oggetto del mandato negoziale del Consiglio d'Europa al Parlamento Europeo per la revisione definitiva.

[17] GDPR Cons. 173: "*Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento*."

In quest'ottica è importante notare che, oltre all'aspetto programmatico, il GDPR risulta perfettamente coerente con una piena interazione delle due normative anche sotto il profilo dei contenuti specificamente relativi al contesto dell'uso di tecnologie di tracking online [18]: basta guardare il Cons. 30 del GDPR[19], che definisce gli identificativi online in modo perfettamente coerente con la Dir. e-privacy.



Figura 8

Come noto, il testo originario della Dir. e-Privacy ha poi subito modifiche nei punti d'interesse ad opera della Direttiva 136/2009, con previsioni infine recepite dall'Italia nel 2012 in legge (D. Lgs. del 28 maggio 2012, numeri 69 e 70), e che hanno anche aggiornato il Codice Privacy.

Allo stato, dunque, tra le norme rilevanti al fine della regolamentazione delle attività di trattamento effettuate tramite identificatori online in generale, e i cookies in particolare, si pone anche l'art. 122 del Codice Privacy.

4. Le norme rilevanti per le tecnologie di tracking online: i rispettivi campi di applicazione…

[18] EDPB – Op. 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities spec. par. 3.3.

[19] "*Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*".

Il WP29 nel tempo si è impegnato a specificare il campo di applicazione di ciascuna delle normative rilevanti nel contesto in esame e le caratteristiche della loro interazione, espressa dall'art. 1 co. 2 della Dir. e-privacy.

In questo senso,

a) nell'Op. 2/2010 (WP 171)[20], aveva sintetizzato come:

- il quadro normativo dell'UE relativo all'uso dei cookie fosse costituito in via principale dall'articolo 5.3 della Dir. e-privacy, che si applica in ogni caso di "informazioni" archiviate o recuperate dall'apparecchiatura terminale di un utente di Internet, quindi anche quando non si tratti di dati personali, perché "*ciò che determina l'obbligo di cui all'art. 5 par. 3 è la protezione di un aspetto che si ritiene appartenente alla sfera privata dell'interessato, non il fatto che le informazioni siano o meno dati personali*"[21]
- la normativa generale (all'epoca, Direttiva 95/46/CE) si applicasse "*nei casi non specificamente coperti dalla direttiva e-privacy ogniqualvolta si procede al trattamento dei dati personali*" [22];

b) nella precedente Op. 1/2008 (WP 148)[23] aveva dettagliato gli estremi essenziali dell'interazione delle norme applicabili:

- precisando che l'art. 5 comma 3 della Dir. e-Privacy è una disposizione generale che si applica trasversalmente a tutti i servizi che fanno uso di tali tecniche (anche servizi non strettamente "di comunicazione elettronica", come i motori di ricerca),
- ricordando che l'art. 5.3 e il Cons. 25, nel regolare la conservazione di cookie e analoghi dispositivi nel terminale di un utente, stabiliscono che ciò debba rispettare la normativa generale in tema di protezione dati personali
- e concludendo nel senso che dunque l'art. 5.3 chiarisce gli obblighi che in questo contesto (cioè, quanto alle tecnologie di tracking online) derivano dalla normativa generale.

---

[20] WP171 – Op. 2/2010 sulla pubblicità comportamentale online.

[21] Cfr. Op. 2/2010, cit., par. 3.2.1 e 6.1. Una piccola digressione: questa considerazione è particolarmente importante, e si ritrova costantemente rimarcata lungo tutta l'evoluzione del percorso di regolamentazione dei sistemi di tracciamento online, compresa l'attuale versione della proposta di Regolamento e-privacy, che precisa che "*Le apparecchiature terminali degli utenti finali di reti di comunicazione elettronica e tutte le informazioni relative all'uso di tali apparecchiature terminali, (…), fanno parte della sfera privata dell'utente finale* " e che "*Le informazioni raccolte dall'apparecchiatura terminale dell'utente finale possono spesso contenere dati personali*." (cons. 20: "*Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, in particular where such information is processed by, stored in, or collected from such equipment, or where information is collected from it or processed in order to enable it to connect to another device and or network equipment, are part of the end-user's private sphere, including the privacy of one's communications, and require protection in accordance with the Charter of Fundamental Rights of the European Union.*" e in fine: "*The information collected from end-user's terminal equipment can often contain personal data*.").
Come vedremo anche esaminando alcune pronunce della Corte di Giustizia e ulteriori pareri dell'EDPB, è fondamentale tenere sempre presente che la protezione offerta dalla Direttiva (e poi dal Regolamento) **opera oltre la categoria dei dati personali, andando a volte anche a derogare la normativa generale.**

[22] Cfr. Op. 2/2010, cit., par. 3.1 e 6.1.

[23] WP148 – Op. 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca

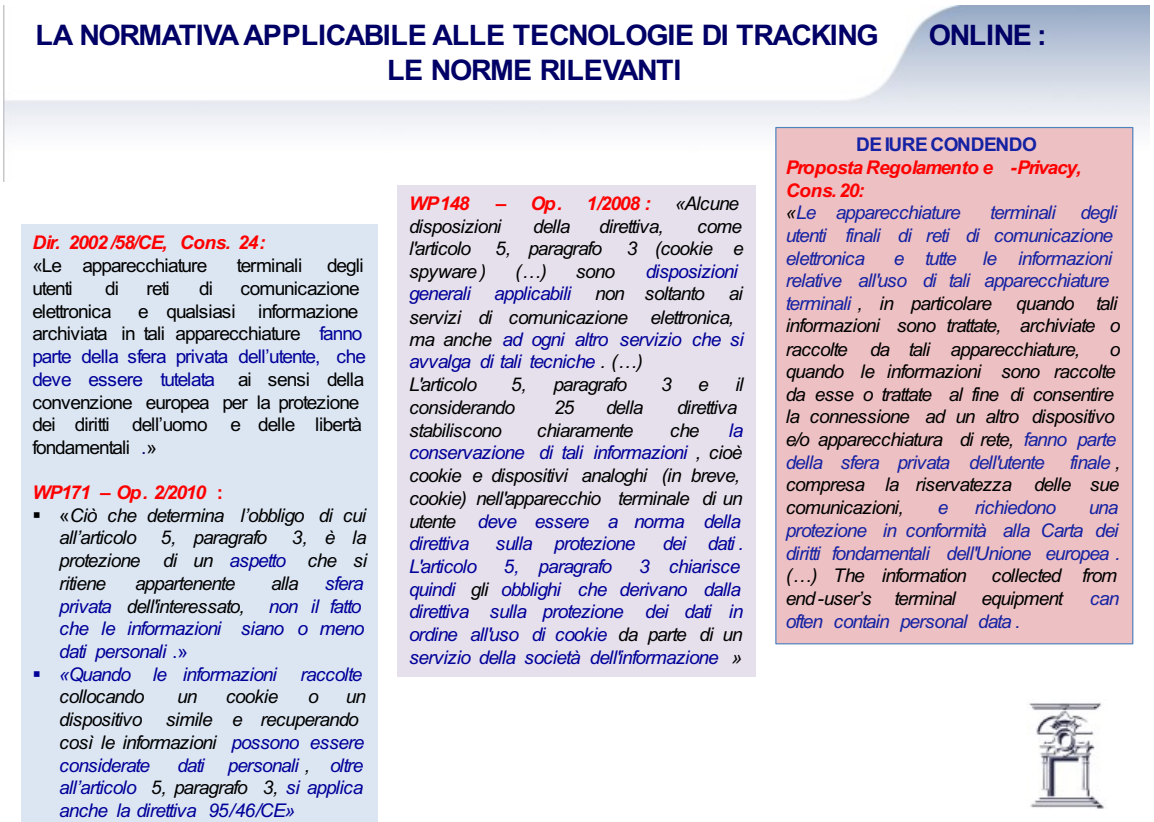


Figura 9

5. … e le regole di interazione.

Da ultimo, è intervenuto sul tema l'EDPB [24] con linee guida specificamente dedicate al tema della sovrapposizione e interazione della normativa generale sulla protezione dei dati con la Dir. e-privacy, in cui:

- ribadisce – a definitiva chiarezza – l'ambito di applicazione esteso dell'art. 5.3 della Dir. e-privacy, che si applica anche oltre il contesto dell'offerta di servizi di comunicazioni elettroniche, per cui anche agli editori di siti web o ad altre attività che fanno uso di cookies [25]
- ma soprattutto declina i meccanismi concreti della funzione integrativa che la Dir. e-Privacy è chiamata a svolgere nei confronti della normativa generale a tutela dei dati personali, chiarendo cosa intenda il comma 2 dell'art. 1 della Dir. e-privacy quando recita: "*le disposizioni della presente direttiva precisano e integrano [particularise and complement] la direttiva 95/46/CE*".

Per fare questo:

assume come oggetto di analisi proprio l'uso di cookies, individuato quale

[24] EDPB – Op. 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, cit.

[25] Par. 28: "*The overarching aim of the ePrivacy Directive is to ensure the protection of fundamental rights and freedoms of the public when they make use of electronic communication networks. In light of this aim, "articles 5(3) and 13 of the ePrivacy Directive apply to providers of electronic communication services as well as website operators (e.g. for cookies) or other businesses (e.g. for direct marketing).*"

trattamento di dati personali che tipicamente coinvolge entrambe le normative[26] e indica come i concetti di "**precisare**" (*particularise*) e "**completare**" (*complement*) debbano essere letti nell'ottica dell'applicazione del principio *lex specialis derogat legi generali*, e dunque:

- quando la Dir. e-Privacy regola in modo specifico, nel contesto di sua pertinenza, un trattamento di dati personali, allora essa prevarrà sulle previsioni generali di cui al GDPR [27]. Rispondono a questo principio anche i casi in cui le previsioni della Dir. e-privacy ampliano di fatto il campo di applicazione della normativa (ad esempio, l'estensione della protezione ad "abbonati" – oggi "contraenti" – e "utenti" di servizi di comunicazione elettronica, che possono anche essere persone non fisiche)[28]
- in tutti i casi in cui il trattamento coinvolga dati personali e non ci sia una previsione specifica della Dir. e-privacy, si applicherà invece il GDPR [29].

[26] Par. 29: "*There are many examples of processing activities which trigger the material scope of both the ePrivacy Directive and the GDPR. A clear example is the use of cookies*.".
Il fatto che quando le informazioni raccolte tramite cookies sono dati personali si applica anche la relativa normativa generale emerge peraltro anche da quanto già a suo tempo rilevato da WP171 – par. 3.2.2, pag. 10: "*Quando le informazioni raccolte collocando un cookie o un dispositivo simile e recuperando così le informazioni possono essere considerate dati personali, oltre all'articolo 5, paragrafo 3, si applica anche la direttiva 95/46/CE.*", nonché dalla più recente giurisprudenza della Corte di Giustizia in casi riguardanti trattamenti di dati personali effettuati mediante cookies: cfr. CJEU, C-210/16, 5 June 2018, C 210/16, ECLI:EU:C:2018:388, spec. para. 33-34. Si veda anche l'Opinion of Advocate General Bobek in Fashion ID, C-40/17, 19 December 2018, ECLI:EU:C:2018:1039, spec. para. 111-115.

[27] Si veda, al proposito, il par. 40 di EDPB – Op. 5/2019, nonché al par. 41, con l'esempio riportato, che evidenzia un possibile caso in cui l'art. 5.3 Dir. e-privacy, che prevede la base giuridica esclusiva del consenso per i cookies, prevale sulla previsione dell'applicabilità generale di basi giuridiche alternative di cui all'art. 6 GDPR.

[28] Questo ampliamento è confermato anche nella proposta di Regolamento e-privacy, che prevede l'applicazione delle norme agli "*user*" e**,** quanto al consenso, che "*The provisions for consent provided for under Regulation (EU) 2016/679/EU shall apply to natural persons and, mutatis mutandis, to legal persons*".

[29] Come confermato dal Cons. 173 GDPR: "*È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche. Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento.*".



Figura 10

6. Tracking online e profilazione: quali basi giuridiche?

Come già detto, la Direttiva 2002/58/CE ha costituito il punto di arrivo sul tema di tutte le analisi, pareri e raccomandazioni degli anni che l'hanno preceduta.

Entrando nello specifico della base giuridica del trattamento di informazioni appartenenti alla sfera privata dell'utente (compresi i dati personali, ma non solo) effettuato tramite identificativi online, va ricordato che originariamente la Dir. e-privacy prevedeva la "*possibilità di rifiutare*" l'installazione del cookie: dunque, palesemente un consenso in forma passiva, di opt-out.

Soluzione che è stata modificata con la Dir. 136/2009, che ha introdotto la diversa richiesta di un consenso "*espresso preliminarmente*" (sempre con l'eccezione delle finalità tecniche).

Riferimento primario per queste indicazioni è stato il qui ripetutamente richiamato parere relativo alla pubblicità comportamentale on-line (WP 171), che nel 2010 aveva già tenuto conto (dichiarandolo esplicitamente) delle modifiche all'art. 5.3 Dir. e-privacy introdotte nel 2009, sebbene esse ancora non fossero state recepite dagli Stati membri (che avevano tempo per farlo fino al 2011).

In questo parere il WP29, in sede interpretativa dell'art. 5.3 della Dir., ha in particolare stabilito che il consenso:

a. deve essere ottenuto **prima** del collocamento del cookie o della raccolta delle informazioni archiviate nel terminale dell'utente ("*preliminarmente*");

b. deve essere espresso in modo conforme ai requisiti della normativa generale in materia di protezione dei dati personali.

Dunque, esaminando gli strumenti possibili:

B1. **il consenso espresso mediante le impostazioni del browser**

- ❖ non è conforme
- se consiste nell'inattività dell'utente, nel caso in cui questi usi un browser che di default consente il trasferimento delle informazioni,
- ma neppure "*se il browser è stato precedentemente impostato in modo tale da accettare tutti i cookie (…), in quanto, in generale, esso non può costituire una vera manifestazione di volontà dell'interessato*" perché "*non sarebbe né specifico né preliminare (al trattamento)"* [30] e neppure "informato", integrando così un consenso "di massa" a qualsiasi trattamento futuro, senza conoscenza delle relative circostanze.
- ❖ È invece conforme il consenso espresso mediante le impostazioni di browser che **di default respingono** i cookie di terzi **e** che **impongono** all'interessato di compiere un'azione positiva per accettare la collocazione e la continua trasmissione di informazioni contenute nei cookies.

Se i suddetti requisiti non sono soddisfatti, non basta certamente a integrare un consenso informato "*il fornire informazioni e, in una certa misura, il facilitare l'utente ad avvalersi della possibilità di respingere i cookie (spiegandogli il modo in cui procedere)*" [31].

B2. **Non è conforme l'opt-out**, che non presuppone alcuna partecipazione attiva perché in questa fattispecie l'intenzione dell'interessato è semplicemente presunta o implicita**.**

B3. È invece **conforme il meccanismo di consenso opt-in** [32] .

[30] WP 171, par. 4.1.1., lett. a), pag. 16

[31] WP 171, par. 4.1.1, pag. 17.

[32] WP 171, par. 4.1.3, pag. 18: "*Per permettere agli interessati di esprimersi chiaramente ex ante, prima cioè che avvenga il trattamento dei dati personali da parte di terzi, è necessario un consenso esplicito (quindi, un "opt-in") per tutte le operazioni di trattamento basate sul consenso"*.

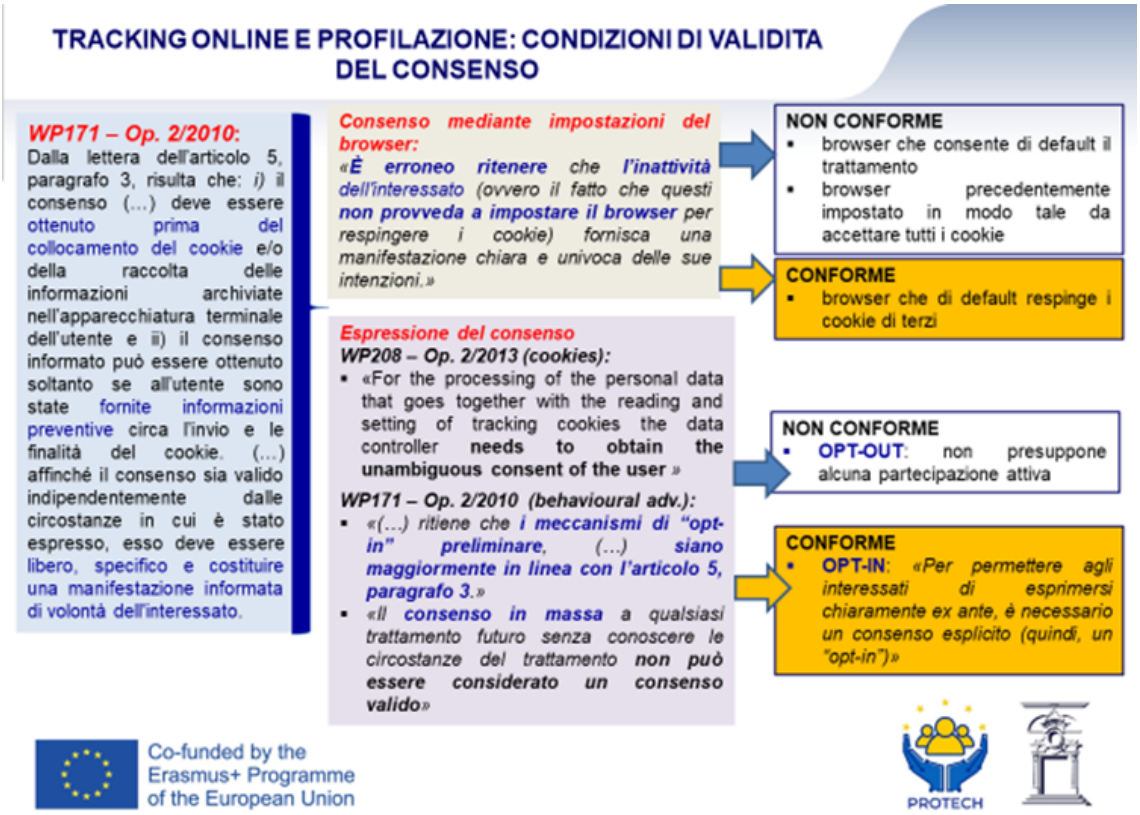


Figura 11

7. La portata del consenso.

Nell'ottica del processo tipico del marketing comportamentale, che coinvolge diversi attori / titolari del trattamento che operano per finalità proprie, la collocazione del cookie è prodromica a successivi trattamenti: dobbiamo dunque chiederci quale sia la portata del consenso ottenuto previamente all'installazione dei cookies.

L'Op. WP 171, anche tenendo esplicitamente in considerazione la difficoltà di ottenere in questo contesto consensi ripetuti, ha affrontato questo aspetto e, richiamando il tenore del Cons. 25 Dir. e-privacy[33], ha affermato che il consenso può essere ottenuto *in uno* per l'installazione del cookie e per la successiva raccolta di **dati anche da parte dei siti partner** di quello che ha installato il cookie [34], **purché**:

A. i cookie installati abbiano una **durata limitata;**

B. siano **fornite informazioni** in conformità alla normativa generale**, tra cui**:

B1. la spiegazione sull'uso dei cookies per pubblicità mirata [35], da inserire in una finestra pop-up **e non "affogata"** nelle condizioni generali o nell'informativa privacy

[33] "*25) L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni".*

[34] Cfr. par. 4.1.3, pag. 18.

[35] Non sono sufficienti indicazioni generiche tipo: "inserzionisti e parti terze possono inoltre utilizzare i propri cookie o action tag").

B2. una informazione periodica sul monitoraggio in corso [36] (perché le persone dopo un po' dimenticano i consensi che hanno dato): ad esempio, tramite la "*creazione di un simbolo e di messaggi associati che avvisino i consumatori del fatto che un fornitore di reti pubblicitarie sta monitorando il loro comportamento di navigazione al fine di trasmettere pubblicità mirata*" e che consenta la revoca del consenso;

C. il consenso sia **liberamente** e facilmente revocabile.

A questo proposito, il Garante, nelle recenti "Linee guida cookie e altri strumenti di tracciamento definitive, pubblicate il 9.7.2021,precisa che il gestore del sito web deve garantire la revoca del consenso "*in ogni momento e ciò in maniera semplice, immediata e intuitiva attraverso un'apposita area da rendere accessibile attraverso un link da posizionarsi nel footer del sito e che ne renda esplicita la funzionalità attraverso l'indicazione di "rivedi le tue scelte sui cookie" o analoga*": insomma, pur senza riproporre il banner la pagina iniziale del sito dovrà comunque rendere sempre disponibile il link alla privacy policy e all'area dedicata alle scelte granulari, tra cui i comandi per la revoca.

Naturalmente tutto ciò richiede un'attenta e aggiornata documentazione delle scelte dell'utente: a questo scopo, possono essere usati appositi cookie tecnici o comunque strumenti di tracciamento. Esistono ormai diverse piattaforme che offrono sistemi automatizzati di gestione dei cookies e alcune di queste consentono di tenere un "registro" aggiornato automaticamente in tempo reale dei consensi ricevuti e delle relative revoche.

[36] A questo proposito, segnalo che quest'obbligo è ripreso nella proposta di Regolamento e-privacy, all'art. 4°, comma 3: "*Agli utenti finali che hanno acconsentito al trattamento dei dati di comunicazione elettronica conformemente al presente regolamento viene ricordata la possibilità di ritirare il loro consenso a intervalli periodici di [non più di 12 mesi], finché il trattamento continua, a meno che l'utente finale non chieda di non ricevere tali promemoria*".
In proposito anche il nostro Garante, nelle sue recenti Linee guida cookie e altri strumenti di tracciamento definitive, pubblicate il 9.7.2021, ha (par. 6.2) stigmatizzato la diffusa "*ridondante e invasiva riproposizione*" del banner da parte dei gestori dei siti web e precisato che quando l'utente abbia liberamente scelto di non prestare il consenso, esso non dovrà essere nuovamente richiesto a meno che (i) siano cambiate le condizioni del trattamento o (ii) quando il gestore del sito web non possa sapere se un cookie sia stato già in precedenza memorizzato sul dispositivo: ad esempio, se l'utente sceglie di cancellare i cookie legittimamente installati nel proprio dispositivo e il titolare non abbia adottato altro sistema per tenere traccia del consenso espresso; oppure siano trascorsi almeno sei mesi dalla presentazione del banner all'utente.



Figura 12

8. La ricerca di una visione paneuropea.

Negli anni successivi sono proliferate varie soluzioni pratiche individuate dagli operatori, variamente considerate dalle singole legislazioni e dalle DPA nazionali che a loro volta emettevano proprie linee guida (ad esempio, la legge svedese autorizzava addirittura l'obbligo di accettare i cookies per accedere al sito), finché nel 2013 il WP29 è nuovamente intervenuto in una visione di applicabilità pan-europea, **tramite il working document WP208**, a definire linee guida per ottenere un consenso valido ai fini specifici del trattamento effettuato tramite identificativi univoci online.

Lo fa richiamando in toto quanto già detto nel 2010 (WP 171) e ribadendo e ulteriormente specificando gli elementi fondanti un valido consenso:

- **un'informativa specifica contenente informazioni appropriate** (chiara, completa, visibile), posta in home page e visibile finché l'utente ha fatto la sua scelta, che indichi (anche con link):

- le tipologie di cookies utilizzati, per finalità,
- i terzi che possono avere accesso alle informazioni dell'utente,
- durata,
- dettagli su cookie di terze parti,
- chiara specificazione di quali azioni manifestano il consenso e delle modalità

per accettare o rifiutare l'installazione dei cookies, anche selettivamente, e revocare il consenso;

- **raccolta del consenso preventiva al trattamento**, ossia prima che i cookie siano installati o letti: dunque il sito deve utilizzare una forma di acquisizione del consenso priva di cookies;
- **consenso consistente in una manifestazione di volontà attiva e inequivocabile**: es click su un bottone o un link, su un'immagine o altri contenuti sulla home page, flag di un box, tramite impostazioni del browser solo alle condizioni indicate da WP171. Ciò che conta è che il contesto sia tale da rendere certa la volontà dell'utente. Non è valido a tale scopo il click su un link che offre ulteriori informazioni, così come l'inattività. Anche la pura permanenza sulla home page non è sufficiente;
- **libertà e specificità del consenso**: effettiva libertà di scegliere se accettare o meno i cookies, quali accettare o rifiutare e cambiare idea in futuro.

Un elemento integrante della libertà è la granularità del consenso, da definire sulla base delle finalità del trattamento: consentire di accettare o rifiutare selettivamente i cookies individuati per finalità garantisce la specificità del consenso.

Ciò è particolarmente importante anche per il rispetto dei principi di finalità, proporzionalità e non eccedenza: l'adozione di un meccanismo non granulare di accettazione dei cookies può indurre di fatto l'obbligo di accettare cookies non necessari per ottenere il servizio di interesse [37] (tanto più se tale servizio non può facilmente essere reperito altrove; ciò è stato rilevato accadere soprattutto nel settore pubblico).

[37] Cfr. EDPB, Guidelines 8/2020 v. 2.0, pag. 16: "*58. (…) Even if the processing of personal data is based on consent of the data subject, this would not legitimize targeting which is disproportionate or unfair*."



Figura 13

9. Il consenso per i marcatori online: quali caratteristiche operative? Aspetti che possono essere considerati risolti.

Questo parere del WP29, che presupponeva a richiamava il contenuto dettagliato e preciso del precedente parere WP171, **conteneva già le risposte definitive** sulla gran parte delle azioni da intraprendere per un uso legittimo degli identificativi univoci online.

Da allora non ci sono state novità sostanziali, ma **solo ripetuti chiarimenti, sempre più espliciti**, tanto da parte del WP29 e poi dell'EDPB quanto della giurisprudenza della Corte di Giustizia e delle DPA nazionali.

Di seguito una sintesi almeno dei temi principali aperti nel tempo e delle risposte fornite, in alcuni casi ormai certe e definitive e in altri ancora in discussione.

- ***Informazioni minime obbligatorie***: tipologia e finalità dei cookies, periodo di attività, accessibilità a terzi (le informative devono mettere l'utente in grado di identificare **tutti i soggetti** che possono trattare i suoi dati e le relative finalità in base al consenso che rilascia [38], dettagli su cookie di terze parti, modalità per esprimere il consenso, modalità di revoca del consenso.

A proposito dei contenuti dell'informativa, è importante sottolineare che la proposta di Regolamento e-privacy [39] chiarisce ripetutamente la necessità di offrire all'utente,

[38] In merito, si vedano *Corte Giust. C-673/17 Planet 49 Gmbh* e *Corte Giust. C-40/17 Fashion ID*, quest'ultima relativa al plugin Facebook. Si veda anche EDPB, Guidelines. 8/2020 v. 2.0, pag. 23 punto 75, che richiama EDPB Guidelines 05/2020 on consent under Regulation 2016/679, V.1.1, p. 16, punto 65.

[39] Cfr. art. 16, comma 6, lett. d).

contemporaneamente al diritto di revocare il consenso ma **in modo distinto**, la specifica informazione della **possibilità di opporsi al trattamento** a fini di marketing, gratuitamente e offrendo modalità semplici ed efficaci.

- ***Modalità per fornire l'informativa***: banner per le informazioni di base (tipologia di cookies e finalità) e link e pop-up (secondo livello) per le altre informazioni; il Garante suggerisce anche di sfruttare possibili modalità multichannel (canali video, interazioni vocali, assistenti virtuali, impiego del telefono, ricorso a chatbot…).

Il Garante inoltre **nelle sue linee guida** ha riscontrato l'esistenza di un problema generale di assenza di codifica semantica uniforme dei cookie e degli altri sistemi di tracciamento, per cui – allo stato – non esiste modo di distinguere in modo obiettivo i cookie tecnici dagli analitici o di profilazione, dovendosi affidare unicamente a quanto dichiarato dai singoli titolari**: ciò comporta la necessità che i titolari esplicitino nell'informativa o nella privacy policy i criteri di codifica adottati.**

- ***Forma del consenso*:**
  - ✓ "**soft opt-in" (preselezione**) e **opt-out**: **non sono ammessi**, è necessaria un'**azione positiva**, che per le Autorità di protezione dei dati di Francia, Gran Bretagna, Germania, Belgio e Olanda deve esplicarsi nel click di un bottone o di un link specificamente riferito al consenso ai cookies;
  - ✓ **lo scrolling** fino alla fine del 2019 sembrava ancora ammesso dall'Autorità di protezione dei dati spagnola [40], e anche dal nostro Garante fino alla fine del 2020*,* sebbene **già nel 2017 l'Art 29WP nelle sue linee guida sul consenso WP259 rev01** avesse chiarito che "*La semplice prosecuzione dell'uso normale di un sito web **non è un comportamento dal quale si può dedurre** una manifestazione di volontà dell'interessato a prestare il consenso a un trattamento proposto*".

A tagliare la testa al toro ha pensato **l'EDPB,** che nelle **Linee Guida 5/2020** sul consenso nel GDPR ha ribadito l'illegittimità di questo strumento ai fini del consenso, sulla base della considerazione del fatto che *"(…) azioni quali scorrere un sito o sfogliarne le pagine o azioni analoghe dell'utente non potranno in alcun caso soddisfare il requisito di un'azione positiva inequivocabile: azioni di questo tipo possono essere difficili da distinguere da altre azioni o interazioni dell'utente e quindi **non è possibile stabilire che è stato ottenuto un consenso inequivocabile**. Inoltre, in un caso del genere, sarà difficile dare all'utente la possibilità di revocare il consenso con la stessa facilità con cui lo ha espresso*." [41].

Anche il Garante, nelle sue nuove linee guida [42] (par. 6.1), ha finalmente dichiarato che lo *scroll down*, o *scrolling*, sia di per sé totalmente inadatto a fungere da consenso, ma ipotizza comunque che possa assumere tale funzione ove inserito in un processo che per le sue caratteristiche complessive manifesti un'azione positiva inequivoca dell'utente;

---

[40] Cfr. le Linee guida AEPD del novembre 2019 e la decisione AEPD (Vueling) del 10/10/2019, in cui è ammessa l'equivalenza tra l'accettazione espressa da parte dell'utente dell'utilizzo dei cookie tecnici e di profilazione e la mera continuazione della navigazione. Questa posizione è stata modificata con l'aggiornamento del maggio 2020, a seguito delle linee guida dell'EDPB di cui alla nota che segue.

[41] EDPB, Guidelines 5/2020 on consent under Regulation 2016/679, es. 16, par. 86.

[42] Cit. nota 35.

- ✓ **cookie walls e cookie barrier** (quest'ultima è la modalità per la quale il banner obbliga l'utente a scegliere se accettare o rifiutare i cookie, altrimenti non gli è consentito proseguire nella navigazione): anche su questo punto per lungo tempo non vi è stato accordo tra le Autorità di protezione dei dati, fino a quando con l'avvento delle linee guida EDPB 5/2020 è definitivamente emersa l'innegabile illiceità di questi strumenti di acquisizione del consenso [43]. Ciò, **salva l'ipotesi** (del tutto residuale, mi pare) che il gestore del sito sia in grado di offrire **anche un'alternativa** di navigazione/contenuto/servizio **equivalente che sia priva** di cookies.

In considerazione del fatto che questa ipotesi – a suo tempo già avanzata dall'**Art. 29WP** nelle sue linee guida sul consenso **WP259** del 2017 – è stata **ripresa integralmente dall'EDPB** e viene **riproposta anche dal Garante** nelle sue linee guida come **opzione da valutare caso per caso,** sembra necessario approfondire **quali sono le circostanze rilevanti.**

Questo il ragionamento proposto dall'EDPB:

"*37. Il titolare del trattamento **potrebbe sostenere** che la sua organizzazione offre all'interessato una scelta reale **mettendolo in grado di scegliere** tra un servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente che non implica un siffatto consenso, dall'altro.*

*Finché esiste la possibilità che il contratto venga eseguito, o che il servizio oggetto del contratto venga prestato, dal titolare del trattamento senza necessità di acconsentire ad usi ulteriori o supplementari dei dati in questione **non si è in presenza** di un servizio condizionato. Tuttavia, **i due servizi devono essere effettivamente equivalenti**.*

*38. Il Comitato ritiene che il **consenso non possa considerarsi prestato liberamente se** il titolare del trattamento sostiene che esiste la possibilità di **scegliere tra il suo servizio** che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, **e un servizio equivalente offerto da un altro titolare del trattamento**, dall'altro. In tal caso **la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti**. Ciò implicherebbe inoltre l'obbligo per i titolari del trattamento di **monitorare gli sviluppi** del mercato per garantire la continuità della validità del consenso per le rispettive attività di trattamento dei dati, in quanto un concorrente potrebbe successivamente modificare il servizio prestato.*

[43] EDPB Guidelines 5/2020, punto 39: "*Affinché il consenso sia prestato liberamente, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente alla memorizzazione di informazioni o all'ottenimento dell'accesso a informazioni già memorizzate nell'apparecchiatura terminale dell'utente (i cosiddetti "cookie wall")*". In generale sullo scambio tra consenso e servizio si veda C. Angiolini, *A proposito del caso Orange Romania deciso dalla Corte di Giustizia dell'UE: il rapporto tra contratto e consenso al trattamento dei dati personali*, in NLCC, n. 1/2021.

Pertanto, *il ricorso a tale argomentazione significa che* ***un consenso fondato sull'esistenza di un'opzione alternativa offerta da un terzo non è conforme al regolamento generale sulla protezione dei dati,*** *e pertanto un prestatore di servizi non può impedire all'interessato di accedere a un servizio per il fatto che questi non ha prestato il proprio consenso.*"

Insomma, è chiaro che condizione necessaria (ma non sufficiente) perché il servizio sia equivalente è che sia offerto dal medesimo titolare [44].

- ✓ **Consenso specifico**[45]: non è ammessa per ottenere un valido consenso l'estensione indebita delle funzionalità (ad esempio, tramite l'uso delle condizioni contrattuali: condizioni generali di acquisto, abbonamento…). Corollario della specificità del consenso è la sua **granularità** [46] : è ammesso un **consenso generale** per tutte le finalità di installazione e uso dei cookies, ma accompagnato da uno strumento (link, ulteriori layer…) che dia la possibilità alternativa di esprimerlo in modo granulare per singola finalità;
- ✓ **Consenso libero**: ciò implica che la revoca o il rifiuto del consenso non comporti **pregiudizi** [47] di alcun tipo all'interessato.

[44] Si vedano sul punto le riflessioni critiche di S. Thobani, in *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in MediaLaws 3/2019, 142. L'A., a supporto della rappresentazione del "consenso libero" quale consenso prestato a favore di un'alternativa, non rilevando se sia fornita da operatori terzi, richiama anche Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it.*, 3, 2019, 530 ss., che individua l'assenza di libertà nel consenso cui viene subordinata una prestazione "*ad un tempo infungibile e irrinunciabile per l'interessato*" (143).

[45] Cfr. EDPB 5/2020 par. 3.2, pag. 15, punto 56: *"(…) La necessità di un consenso specifico associata alla nozione di limitazione delle finalità di cui all'articolo 5, paragrafo 1, lettera b), funge da garanzia contro l'ampliamento progressivo, o la commistione, delle finalità di trattamento dei dati dopo che l'interessato ha acconsentito alla loro raccolta iniziale. Questo fenomeno, noto anche come "function creep", rappresenta un rischio per l'interessato, in quanto può comportare l'uso non previsto di dati personali da parte del titolare del trattamento o di terzi e la perdita del controllo da parte dell'interessato.*"

[46] Cfr. EDPB 5/2020 spec. par. 3.1.3.

[47] Cfr. EDPB 5/2020 spec. par. 3.1.4. Sulle possibili attribuzioni ed effetti del requisito di «libertà» del consenso, si veda – oltre alla dottrina e giurisprudenza citate in nota 44 – l'approfondita analisi di S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità,* in Europa e diritto privato - 2/2016, spec. 520 ss., e la ricca panoramica di dottrina ivi contenuta, che – benché si riferiscano alle norme del Codice Privacy ante GDPR – risultano, *mutatis mutandis*, ancora perfettamente attuali.

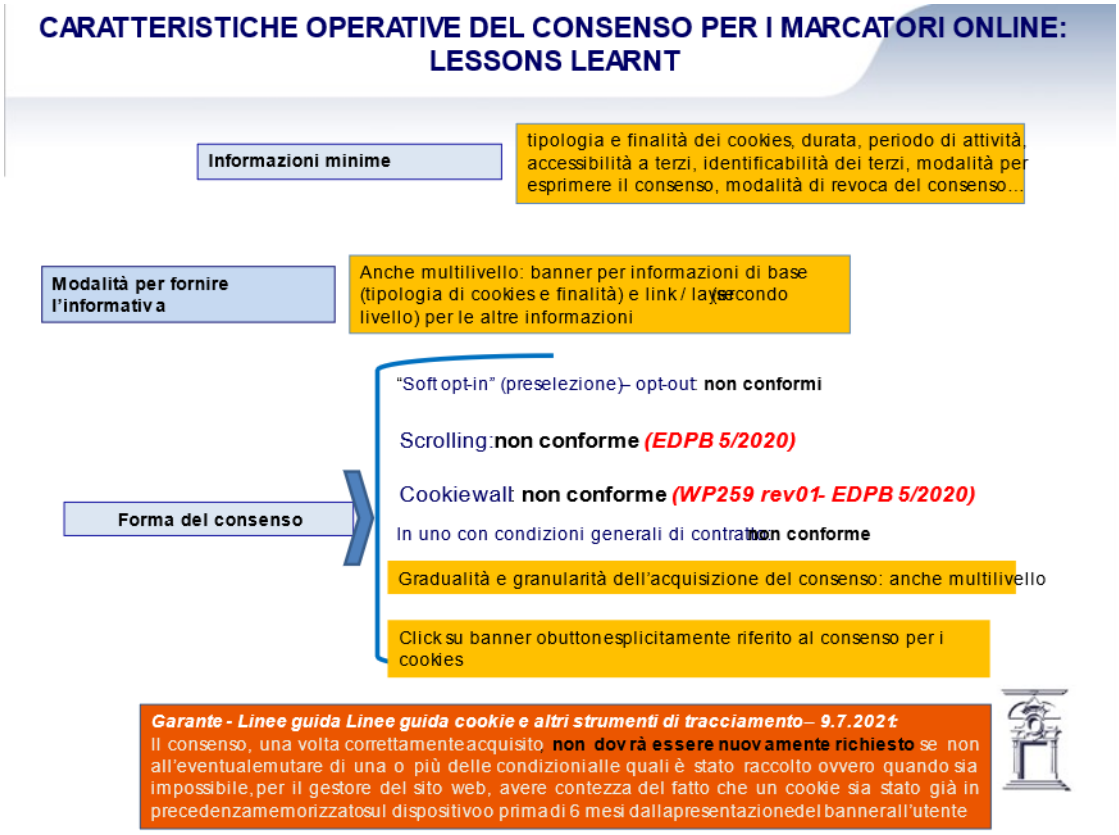


Fig. 14

- **Determinazione della base giuridica per l'inserimento del plug-in social in un sito:**

Il meccanismo del plugin è diverso dai cookies, sebbene operi mediante archiviazione di cookies nel terminale dell'utente; di base serve a consentire agli **utenti dei social network** di condividere contenuti a loro graditi con i loro "amici": in questo caso, rientra tra le esenzioni al consenso di cui alla seconda parte dell'art. 5.3 della Direttiva e-Privacy (che, si ricorda, fa riferimento all'archiviazione tecnica o accesso "*nella misura* ***strettamente necessaria al fornitore di*** *un servizio della società dell'informazione* ***esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio***").

Però in certi casi può anche essere utilizzato per altre finalità, ad esempio "*per monitorare gli individui, membri o meno* [del social network – n.d.r.]*, con cookie di terzi per finalità aggiuntive come, ad esempio, la pubblicità, l'analitica e le indagini di mercato a carattere comportamentale*" [48]: in tale caso, non opera l'esenzione e subentra l'obbligo di consenso.

Un recente precedente è costituito dalla **decisione della Corte di Giustizia Fashion ID, C-40/17**, del 29/7/2019, che ha spiegato [49] che nel caso dell'uso di plugin il Giudice deve previamente verificare **se si possa** ritenere che nel caso di specie il social network – fornitore del plugin – acceda, tramite l'uso di

[48] Cfr. Art. 29WP, Op. 4/2012 - WP 194, par. 4.1.

[49] Par. 90: «*Spetta al giudice (…) verificare se (…) il fornitore di un plug-in social (…) abbia accesso(…) a informazioni archiviate nell'apparecchiatura terminale, ai sensi dell'articolo 5, paragrafo 3, della direttiva 2002/58, di coloro che visitano il sito Internet del gestore di tale sito.*»

questo, a informazioni archiviate nel terminale dell'utente ai sensi della prima parte dell'art. 5.3 Dir. e-Privacy oppure se sia applicabile l'esenzione.

Nel caso di Fashion ID, peraltro, la Corte ha evidenziato (**par. 75 ss**.) come – fatti salvi gli accertamenti da effettuarsi da parte del Giudice del rinvio – "*dagli atti risulta che, avendo inserito sul suo sito Internet il pulsante «Mi piace» di Facebook, la Fashion ID sembra aver offerto la possibilità alla Facebook Ireland di ottenere dati personali dei visitatori del proprio sito Internet, possibilità concretizzatasi sin dal momento della consultazione di tale sito, e ciò* ***indipendentemente dal fatto che essi siano o meno iscritti al social network o che abbiano cliccato sul pulsante « Mi piace» di Facebook o, ancora, che siano a conoscenza di una tale operazione***."

Da ciò la Corte ha dedotto che la finalità dell'inserimento del plugin "Mi piace" da parte del sito fosse di tipo promozionale (rendere i suoi prodotti più visibili su FB) ed avesse un parallelo effetto economicamente favorevole per il social fornitore del plugin, che in questo modo beneficia dei dati del visitatore del sito ospitante, trasferitigli appunto mediante il plugin (e dunque accedendo a informazioni – cookies – archiviate nel terminale dell'utente). Ricorre pertanto in questo caso la necessità del consenso.

Peraltro la Corte svolge anche interessanti valutazioni in tema di titolarità del trattamento, specificando come (parr. 64 ss.) l'editore del sito che inserisce sul suo sito il plugin social sia titolare solo dei trattamenti di raccolta dei dati personali dei visitatori del suo sito Internet e conseguente comunicazione, mediante trasmissione, al social, mentre non ha possibilità di determinare i trattamenti che il social fa dei dati così ricevuti. PERÒ, attenzione: il social è contitolare del trattamento dell'editore del sito per queste stesse finalità.

Ciò malgrado, è **l'editore del sito il soggetto tenuto** a fornire l'informativa e chiedere il consenso per le finalità di raccolta e comunicazione mediante trasmissione al social dei dati personali dei visitatori del suo sito Internet, "*giacché è il fatto che un visitatore consulti tale sito Internet che attiva il processo di trattamento dei dati personali. (…) non sarebbe conforme a una tutela efficace e tempestiva dei diritti della persona interessata il fatto che il consenso sia prestato unicamente al corresponsabile del trattamento che interviene successivamente, ossia al fornitore di detto plug-in*".

Tutto questo è stato poi confermato **da EDPB Guidelines 8/2020 v. 2.0 sul targeting degli utenti di social media**, – che ha sottolineato che: "(…) *il consenso che dovrebbe essere raccolto dal gestore del sito web per la trasmissione di dati personali attivata dal suo sito web (incorporando un plug-in sociale) si riferisce solo all'operazione o all'insieme di operazioni che comportano il trattamento di dati personali di cui il gestore determina effettivamente le finalità e i mezzi. La raccolta del consenso da parte del gestore di un sito web, non esclude né diminuisce in alcun modo l'obbligo del fornitore di social media di assicurarsi che l'interessato abbia fornito un consenso valido per il trattamento di cui è responsabile in qualità di contitolare del trattamento, nonché per qualsiasi trattamento successivo o ulteriore che*

effettua e per il quale il gestore del sito web non determina congiuntamente le finalità e i mezzi (ad esempio, le operazioni di profilazione successive a fini di targeting)." [50]



Fig. 15

10. Caratteristiche operative del consenso per i marcatori online: i problemi ancora aperti.

Naturalmente permangono anche temi su cui dubbi e contrasti non sono ancora del tutto sopiti.

Di seguito ne ricordo i principali.

- ***Uso di cookies analytics: richiede il consenso?***

Le Autorità di protezione dei dati sono ormai tutte abbastanza allineate in senso positivo, seppure con qualche differenza: ad esempio, la Germania chiede il consenso per il caso in cui l'uso degli analytics sia preordinato ad un trasferimento dei dati a terzi.

In ogni caso, **il WP29 già nel 2012**[51] aveva specificato che gli analytics **non sono necessari** per erogare un servizio espressamente chiesto dall'utente, dunque **non sono**

[50] Par. 5.3.2, pag. 21, mia traduzione.

[51] Cfr. WP29 Op. 4/2012 - WP 194, sull'esenzione dal consenso per l'uso di cookies, par. 4.3.

esentati dal consenso ai sensi della seconda parte dell'art. 5.3 della Direttiva e-Privacy.

Aveva però anche osservato che gli analytics di prima parte che si limitino a formulare statistiche aggregate con completa anonimizzazione dell'indirizzo IP non sono pericolosi per la protezione dei dati personali, **a condizione che** siano attuate tutele ragionevoli, tra cui informazioni adeguate, la facile capacità di recesso e meccanismi di completa anonimizzazione di tutte le informazioni identificabili (tra cui l'indirizzo IP).

A tali condizioni, quindi, sebbene a rigore non rientrino nell'esenzione di cui alla seconda parte dell'art. 5.3 della Direttiva e-Privacy, è possibile utilizzarli senza il consenso.

Questa conclusione oggi è condivisa dal nostro Garante, che ha dato le seguenti indicazioni:

- ha confermato la validità in questo senso del "mascheramento" di parte dell'indirizzo IP: "*La struttura del cookie analytics dovrà allora prevedere la possibilità che lo stesso cookie sia riferibile non soltanto ad uno, bensì a più dispositivi, in modo da creare una ragionevole incertezza sull'identità informatica del soggetto che lo riceve.* ***Di regola questo effetto si ottiene mascherando opportune porzioni dell'indirizzo IP all'interno del cookie***";
- ha escluso la liceità di qualsiasi combinazione con altre informazioni e trasferimenti a terzi: "*Resta inteso pertanto che i soggetti terzi, che forniscono al publisher il servizio di web measurement, non dovranno comunque combinare i dati, anche così minimizzati, con altre elaborazioni (file dei clienti o statistiche di visite ad altri siti, ad esempio) né trasmetterli a loro volta ad ulteriori terzi, pena l'inaccettabile incremento dei rischi di identificazione dell'utente; tranne il caso in cui la produzione di statistiche da loro effettuata con i dati minimizzati interessi più domini, siti web o app riconducibili al medesimo publisher o gruppo imprenditoriale.*"



Fig. 16

Da ultimo, mi sembra utile affrontare brevemente l'interrogativo – che da qualche parte viene ancora posto – relativamente alla possibilità che ricorrano basi giuridiche diverse dal consenso in casi di trattamenti successivi all'installazione dei cookies (per esempio, la profilazione).

In particolare, **sono sempre più numerosi i siti web che ricorrono all'interesse legittimo** come base per questi trattamenti. Ad esempio:

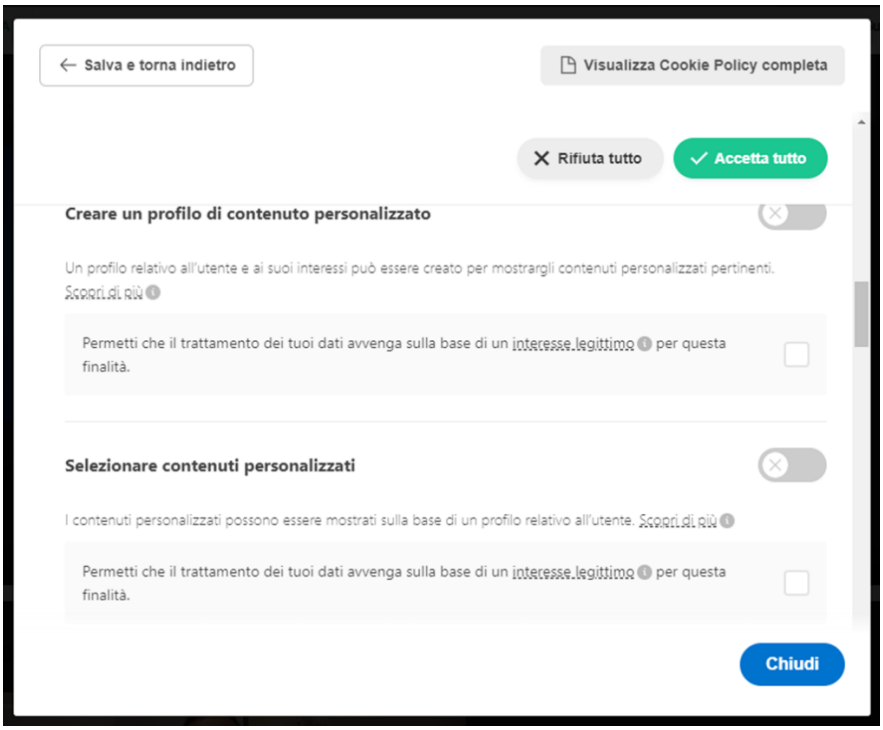


Fig. 17

Questa pratica deve ritenersi illegittima: vediamo perché.

- ***Per i trattamenti successivi all'installazione dei cookies è lecito utilizzare basi giuridiche diverse dal consenso?***

Il **WP29 nell'Op. 2/2010** (par. 3.2.1)
identificando il campo di applicazione materiale dell'art. 5.3 Direttiva e-Privacy nell'ottica proprio di individuare gli adempimenti per chi fa pubblicità comportamentale,

- ✓ **ha ricordato** che l'art. 5.3 della Direttiva e-Privacy prevede il consenso per "***l'archiviazione di informazioni*** *oppure* ***l'accesso a informazioni già archiviate*** *nell'apparecchiatura terminale di un abbonato o di un utente*";
- ✓ **e ha quindi precisato** che: "*Considerato che (i) i tracking cookie sono "informazioni" archiviate nell'apparecchiatura terminale dell'interessato, e che (ii) i fornitori di reti pubblicitarie accedono a tali cookie quando l'interessato visita un sito web partner, l'articolo 5, paragrafo 3, trova piena applicazione.*

Pertanto, (…) ***qualsiasi successivo utilizzo*** *di cookie precedentemente archiviati per accedere alle informazioni dell'interessato* ***dovrà essere conforme all'articolo 5, paragrafo 3****."*

Successivamente l'EDPB con l'Op. 5/2019

- ✓ **ha affermato** (par. 75) che i (diversi) trattamenti **successivi**

all'archiviazione o all'accesso alle informazioni ("*all other processing operations that follow the storing of or access to information in the terminal device of the end-user*") restano regolati dalla legge generale (e dunque, **teoricamente potrebbero** applicarsi basi giuridiche diverse dal consenso, ai sensi dell'art. 6 GDPR)

- ✓ **ma ha anche ricordato** che i precedenti pareri WP sulla limitazione delle finalità (WP3/2013) e sul legittimo interesse (WP 6/2014) hanno richiamato il **consenso attivo (opt-in)** come unica legittima base giuridica per tutti i trattamenti **a fini di marketing diretto o comportamentale e di profilazione** basati su sistemi di tracking online (**il WP 6/2014 richiamando peraltro direttamente l'applicabilità dell'art. 5.3 Dir**.).

Infine **l'EDPB ancora più recentemente, nell'Op. 8/2020** (par. 5.3.2)

- ✓ **ha riaffermato** l'operatività dell'art. 5.3 della Direttiva e-Privacy in materia di requisiti per l'uso dei cookies, compreso ogni trattamento successivo dei dati personali ottenuti accedendo alle informazioni nel terminale **e che** "*For what concerns the legal basis of the processing in Examples 4, 5, and 6, the EDPB considers that **legitimate interest cannot act as an appropriate legal basis** as the targeting relies on the monitoring of individuals' behavior across websites and locations **using tracking technologies.***

*78. Therefore, in such circumstances, the appropriate legal basis **for any subsequent processing** under Article 6 GDPR **is also likely to be the consent** of the data subject."* (par. 5.3.2, parr. 77-78, pag. 23 s.).

È evidente da tempo pertanto la esclusione – secondo l'interpretazione del WP29 e quella conforme e complementare dell'EDPB –**della ricorrenza di basi giuridiche differenti dal consenso per trattamenti basati sull'uso di identificatori univoci online, anche successivi all'installazione dei marcatori**.

Da ultimo, anche il nostro Garante Privacy, con le **Linee guida cookie e altri strumenti di tracciamento** pubblicate a luglio 2021

- ✓ ha precisato che *"(...) la disciplina di carattere speciale applicabile alla specie **non contempla ulteriori basi giuridiche** che rendano legittimo il trattamento se non in presenza del consenso dell'interessato ovvero al ricorrere di una delle ipotesi di deroga rispetto all'obbligo della sua raccolta previste proprio da tale disciplina speciale. **In nessun caso sarà pertanto possibile invocare ad esempio, come è stato invece osservato nel corso delle verifiche effettuate su diversi siti web, la scriminante del legittimo interesse del titolare per giustificare il ricorso a cookie o altri strumenti di tracciamento**."* (par. 5, ult. paragrafo, pag. 7).



Fig. 18

Credo poi che si debba **anche considerare il fatto che** la tutela apprestata dall'art. 5.3 **non si applica solo ai dati personali, ma a tutte le "informazioni" dell'utente archiviate nell'apparecchiatura terminale**, che sono considerate **comunque** afferenti tutte alla sua sfera privata, come da ultimo sottolineato anche dalla proposta di Regolamento e-Privacy (cons. 20)[52], che dichiara fermamente che proprio a causa della **tipologia** di informazioni **archiviate o trattate dagli apparati**, potenzialmente rivelatrici dei **dettagli più intimi** della vita e della personalità dell'utilizzatore, **tutte queste informazioni meritano una protezione rafforzata**.

E – aggiunge – tra queste informazioni possono essere presenti anche dati personali.

Mi sembra dunque che non avrebbe senso logico, né giuridico, creare due differenti percorsi di protezione quando la ***ratio*** della normativa è quella di difendere l'utente da tutte le attività di marketing comportamentale (profilazione compresa) che coinvolgono informazioni che lo riguardano raccolte e trattate nel contesto dell'uso di "*tutte le tecnologie basate sul principio dell'archiviazione e dell'accesso a informazioni*

[52] Cons. 20 della proposta Regolamento e-Privacy (v. nota 36): "*Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. (…) Therefore, the use of processing and storage capabilities and the collection of information from end-user's terminal equipment should be allowed only with the end-user's consent and or for other specific and transparent purposes as laid down in this Regulation. The information collected from end-user's terminal equipment can often contain personal data*".

sull'apparecchiatura terminale dell'utente" [53].

Da ultimo, neppure mi pare che possa essere invocata in senso contrario la decisione della Corte di Giustizia C-40/17 Fashion ID, che si è preoccupata di valutare l'applicabilità del legittimo interesse[54].

L'**approfondimento** sull'applicabilità del legittimo interesse infatti in quella sede è stato condotto doverosamente **sul presupposto del fatto** (indicato dalla decisione come rilevato dal Giudice del rinvio) che **in quella specifica circostanza** il trattamento **non** aveva coinvolto **solo** informazioni **archiviate nell'apparecchiatura terminale** degli utenti, **ma anche altri dati personali.** È dunque **al trattamento di questi dati** che eventualmente potrebbe essere applicato il legittimo interesse: **solo per questo, e in relazione solo a questo,** la Corte ha ritenuto rilevante analizzare la questione.



Fig. 19

11. Verso un marketing digitale senza third party cookies.

Negli ultimi anni, reagendo all'attenzione sempre maggiore manifestata dagli utenti rispetto all'uso dei propri dati personali, sempre più operatori hanno deciso di eliminare dai propri browser i cookie di terza parte. Già oggi i browser che impediscono l'uso di

[53] WP29, Op. 2/2010, par. 2.2.
[54] Cfr. par. 87 ss.

cookie di terza parte detengono circa il 29% di market share in Italia[55].

Firefox, Safari e anche Edge di Microsoft hanno nel tempo avviato azioni in questo senso:

- Firefox ha stabilito come modalità predefinita il blocco di tutti i cookie di terze parti e di tutte le eventuali attività di cryptomining con l'attivazione di default della funzione "enhanced tracking protection", praticamente invisibile all'utente, il quale si accorge del suo funzionamento solo quando visita un sito e vede l'icona di uno scudo nella barra degli indirizzi accanto all'URL, insieme a una piccola icona 'i' a dimostrazione che Firefox "*sta bloccando l'accesso di migliaia di società alle sue attività online*".
- Safari ha limitato il monitoraggio dei cookie dal 2017, utilizzando algoritmi di apprendimento automatico per identificare i comportamenti di tracciamento, come i cookie persistenti provenienti da reti pubblicitarie di terze parti.
- Edge prevede nella sua nuova versione tre profili preimpostati in base ai permessi concessi: "Di base", "Bilanciato" e "Rigido", che è possibile personalizzare: le autorizzazioni concesse ai siti, così come le notifiche ma anche i cookie di terze parti, comprendono anche il controllo del microfono e della fotocamera e la possibilità di essere avvisati se un sito desidera accedere al testo e alle immagini copiati negli appunti.

L'ultimo è Google, che già dal 2019 ha annunciato l'intenzione di bloccare i third-party cookie su Chrome a partire dal 2022, nel contesto di un progetto che ha chiamato "privacy Sandbox"[56]: in pratica viene creata una sandbox (un ambiente isolato) del browser, non accessibile agli inserzionisti, e qui i segnali registrati dai cookies, come clic o conversioni, vengono archiviati e misurati con metodi di machine learning che applicano misure di limitazione, offuscamento e anonimizzazione prima che i dati vengano restituiti.

L'algoritmo dunque segue la navigazione dell'utente e sulla base delle preferenze di navigazione lo inserisce in un grande gruppo di utenti aventi interessi simili, conservato nel sandbox e a cui poi mostra gli annunci dei terzi ritenuti appropriati.

In sostanza Google, tramite Chrome, non identificherà più l'utente con l'identificatore univoco personale salvato nei cookie e richiamato dai siti web terzi (anzi, l'ID verrebbe dissimulato), ma ne salverà le preferenze: dunque, la profilazione avviene lo stesso, ma senza più possibilità di individuare lo specifico utente.

[55] Dati del Politecnico di Milano – Osservatorio Internet Media – presentati il 9/3/2021 nel contesto della ricerca "Internet advertising: no cookie, no party" (accesso limitato agli abbonati). La presentazione La ricerca ha anche evidenziato come, con la realizzazione della "privacy sandbox" di Google Chrome la quota di mercato detenuta dai browser con limitazioni all'uso dei cookies salirà al 96% (Chrome da solo detiene il 67%).

[56] https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/ .

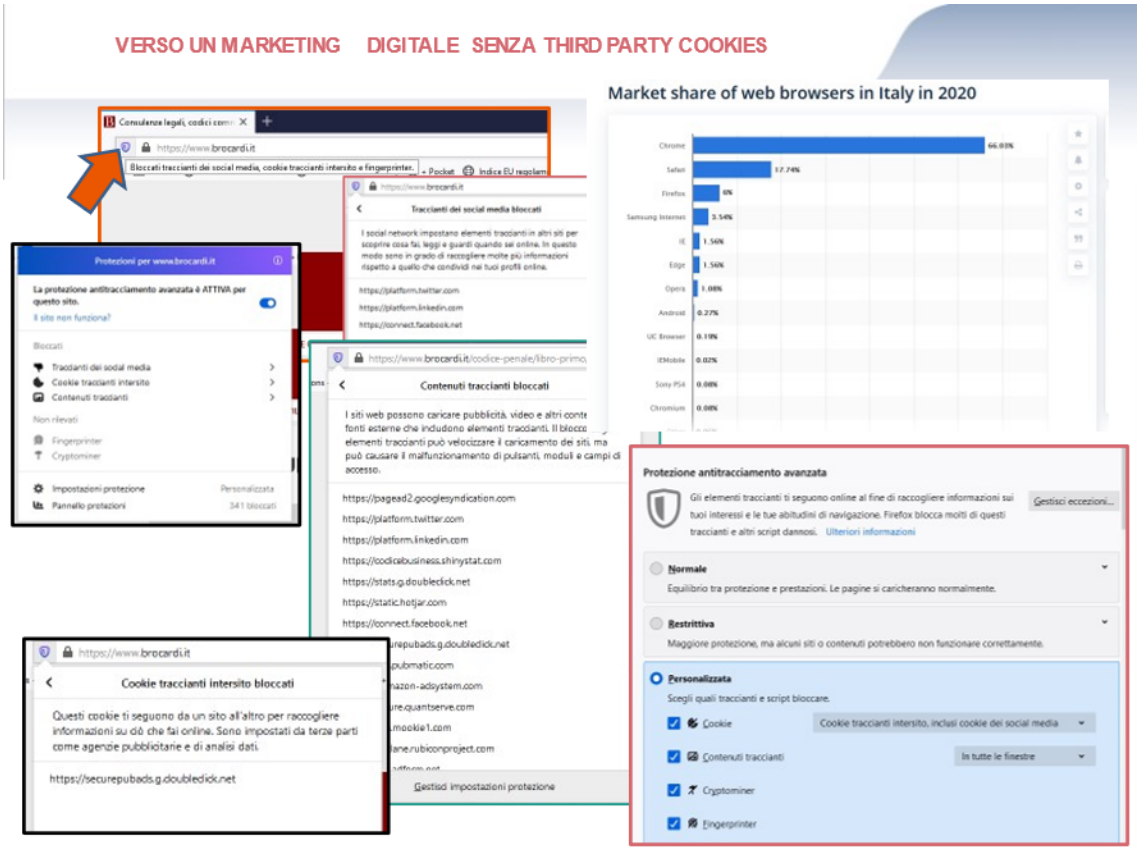


Fig. 20

È importante sottolineare ancora che quando si parla di un futuro senza cookie si fa riferimento al blocco da parte dei browser dei third party cookie (cioè creati da domini differenti da quello in cui si sta navigando), utilizzati per il tracciamento cross-site, il retargeting, la profilazione dell'utente e il matching degli ID degli utenti tra diverse piattaforme.

Per valutare gli impatti sul mercato di questo mutamento radicale va tenuto presente che Google controlla i due terzi del mercato e gestisce la più grande rete pubblicitaria su internet: DoubleClick (piattaforma di advertising che quando l'utente visita un dato sito rilascia i cookies che permettono di ricordare che quell'utente ha visitato quel dato sito) è il più grande fornitore di tecnologia pubblicitaria per editori e inserzionisti. E Google Analytics raccoglie informazioni da milioni di siti Web…

Quello che è chiamato Programmatic Advertising (il marketing basato sulla sincronizzazione dei cookies che consente di tracciare cross-site l'utente, profilarlo e veicolargli al momento giusto l'annuncio adatto) negli anni ha aumentato il suo peso all'interno dell'industry pubblicitaria proprio grazie alle sue alte potenzialità di targetizzazione: secondo l'Osservatorio Internet Media del Politecnico di Milano, ha raggiunto nel 2020 il valore di 588 milioni di euro in Italia, in crescita del 6% rispetto al 2019.

Per questo la decisione di Google di abbandonare i cookie di terza parte potrà generare conseguenze veramente importanti per tutto l'ecosistema di marketing e comunicazione, che negli ultimi anni ne ha fatto larghissimo utilizzo.

È importante considerare che il blocco dei cookie di terza parte non avrà impatti solo sulla delivery degli annunci e la targetizzazione degli utenti, ma ci saranno conseguenze anche per quanto riguarda l'ambito della misurazione delle campagne online: ad esempio, sarà molto difficile ricostruire il percorso di navigazione dell'utente per l'impossibilità di individuare gli accessi precedenti effettuati con browser e device diversi, e quindi impossibile sapere cosa ha portato ad un determinato click e come interpretare il significato di una determinata conversione (vendita). Si presume che interverranno sempre più logiche di machine learning, che sostituiranno i modelli probabilistici al tracciamento diretto dell'utente.

Nel report dell'Osservatorio Internet Media del Politecnico di Milano (pag. 3) si legge: "*Solo gli Over The Top, almeno in questa fase, verranno toccati marginalmente, tanto che probabilmente rafforzeranno ancora il loro ruolo e peso all'interno del panorama pubblicitario. Grazie ai loro ecosistemi walled garden* [ossia caratterizzati da un parco di utenti registrati, loggati, con cui hanno un rapporto diretto e da cui traggono informazioni di prima mano, anche usando di cookie di prima parte – n.d.r.] *potranno utilizzare all'interno di questi ambienti (chiusi) l'ampia quantità di dati in loro possesso, ovviamente anche per fini pubblicitari. Il rapporto di forza degli OTT rispetto agli editori online potrà forse ridursi se i publisher, in un futuro prossimo, saranno in grado di organizzarsi con una "soluzione unica di sistema" in grado di rafforzare il proprio peso sul mercato e proporsi quindi come reale alternativa.*".

Si prevede quindi un impatto veramente importante se gli operatori, specie le aziende brand e anche gli editori online, non si attrezzeranno per trovare soluzioni alternative.

In quest'ottica, ciò che emerge dalla ricerca dell'Osservatorio Internet Media del Politecnico di Milano è la previsione del fatto che *"(…) oltre all'accelerazione verso il digitale indotta dalla pandemia, l'avvento dello "scenario cookieless" stimolerà ulteriormente in tutte le aziende (della domanda e dell'offerta) un forte senso di urgenza verso una cultura più matura del dato e della sua gestione.*", con l'assunzione di una rilevanza sempre maggiore:

- dei cookie di prima parte – che non sono impattati da queste evoluzioni dei browser –
- e dei dati acquisiti direttamente, con o senza meccanismi di tracciamento, magari ampliando il novero delle richieste di registrazione ai siti, alle newsletter, in modo da arricchire sempre più i sistemi CRM aziendali. In questo contesto, un ruolo particolare potrebbe essere assunto dall'indirizzo e-mail, che viene già raccolto con il consenso e cui vi è la possibilità tecnica di agganciare meccanismi che costituiscono veicolo di informazioni su azioni compiute dall'utente (es. apertura, cancellazione, attivazione di immagini all'interno mediante click…).

Ciò presumibilmente spingerà gli operatori verso l'introduzione di strategie e strumenti di marketing capaci di creare con gli utenti/interessati rapporti diretti e leali, destinati a durare e rafforzarsi nel tempo; ma, al di là della capacità di ridefinizione delle strategie di comunicazione che sapranno mostrare gli operatori, per il momento l'effetto più evidente e concreto resta quello che tramite la realizzazione della Privacy Sandbox Google si avvii ad un prossimo ulteriore e repentino rafforzamento della propria

posizione di mercato, idonea a distorcere pericolosamente la concorrenza[57].

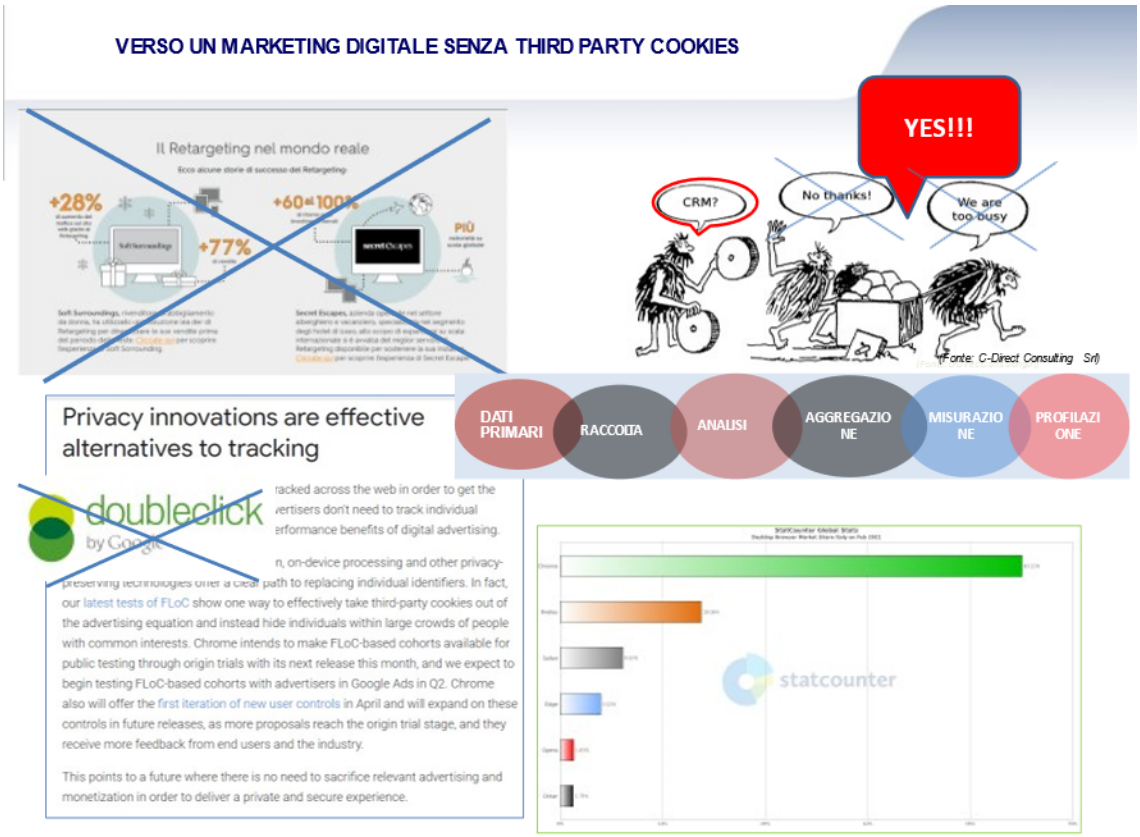


Fig. 21

[57] L'8 gennaio 2021 la Competition and Markets Authority (CMA), sollecitata da operatori del mercato, ha aperto un procedimento nei confronti di Google proprio con riferimento alla rimozione dei cookie di terze parti e altre funzionalità da Chrome. Attualmente Google ha proposto impegni, che includono tra l'altro limiti specifici su come Google può utilizzare e combinare i dati dei clienti per la pubblicità digitale, la cui idoneità a tutelare la concorrenza sul mercato della pubblicità digitale e contestualmente salvaguardare i dati personali degli utenti e stata oggetto di consultazione da parte di CMA e ICO e delle terze parti interessate; la consultazione si è chiusa l'8 luglio 2021 e allo stato l'Autorità sta valutando possibili modifiche agli impegni proposti da Google.