RISPOSTA ALLA CONSULTAZIONE
LINEE GUIDA SULL'UTILIZZO DI COOKIE E DI ALTRI STRUMENTI DI TRACCIAMENTO

---

09 GENNAIO 2021

Alla cortese attenzione della

Autorità Garante per la protezione dei dati personali

Piazza Venezia n.11-00187 Roma

lineeguidacookie@gdpd.it

Il team dataTENET è un insieme di professionisti del diritto della protezione dei dati personali, di responsabili della protezione dei dati in ambiti sia pubblici che privati, di studiosi ed appassionati delle tematiche più spinose legate alla difesa dei diritti e delle libertà fondamentali, alla valorizzazione e libera circolazione dei dati personali e alla sicurezza dei relativi trattamenti, nella società globale in rapida trasformazione digitale.

Con il coordinamento di:

BARBARA CALDERINI, MARIA GRAZIA ROMANO E FLORIANA TAGLIAFERRO

Con i contributi, in ordine alfabetico, di:

FEDERICO ALESSANDRI Avvocato - Consulente Privacy

NATALIA ARTEMENKO Avvocato d'impresa - Consulente Privacy

BARBARA CALDERINI Giurista - Imprenditrice - Compliance Manager

PIETRO CALORIO Avvocato

GIANMARCO CENCI Responsabile Protezione Dati - Avvocato

SALVATORE COPPOLA Responsabile Protezione Dati - Avvocato - Formatore

ALESSANDRA ETZO Responsabile Protezione Dati - Avvocato - Consulente Privacy

MARIA GRASSETTO Responsabile Protezione Dati - Avvocato

MARIA ANTONIETTA IACOBELLI Avvocato

GIANLUCA LOMBARDI Responsabile Protezione Dati - Privacy Officer - Auditor 27001 - Ingegnere

EUGENIA LOPRESTI Avvocato - Consulente Privacy

ALESSANDRA LUCCHINI Avvocato - Consulente Privacy - Responsabile Protezione Dati

KARIN MALASPINA Data Protection Specialist - Avvocato

GERMANA MARAFFA Responsabile Protezione Dati

GLAUCO RAMPOGNA

MARIA GRAZIA ROMANO Responsabile Protezione Dati - Consulente Privacy

LEONARDO SCALERA Responsabile Protezione Dati - Formatore privacy & Digital transformation

FLORIANA TAGLIAFERRO Responsabile Protezione Dati - Avvocato

LUISA TUCCI Consulente Privacy - Commercialista

Nel rispondere all'invito dell'Autorità Garante a formulare osservazioni al documento di Consultazione in oggetto, il team di professionisti dataTENET [1] intende anzitutto ringraziare per l'opportunità offerta.

Il team dataTENET condivide, in particolare, la scelta dell'Autorità Garante della protezione dei dati personali di procedere nell'attività *ricognitiva in relazione al diritto applicabile alle operazioni di lettura e di scrittura all'interno del terminale di un utente, con specifico riferimento all'utilizzo di cookie e di altri strumenti di tracciamento*, *nonché l'obiettivo di specificare, al riguardo, le corrette modalità per la fornitura dell'informativa e per l'acquisizione del consenso online degli interessati, ove necessario, alla luce della piena applicazione del Regolamento (UE) 2016/679*, di seguito per brevità anche RGPD.

Ciò permetterà sia di operare un maggior allineamento con le attuali trasformazioni tecnologiche e sociali rispetto a quanto previsto nell'ambito della disciplina europea, sia di promuovere e favorire un'interpretazione uniforme e coordinata in tutti gli Stati membri.

[1] Il termine TeneT richiama il quadrato del Sator, ricorrente iscrizione latina, composta dalle cinque seguenti parole: SATOR, AREPO, TENET, OPERA, ROTAS. La loro giustapposizione, nell'ordine indicato, dà luogo a un palindromo. La stessa frase palindroma si ottiene leggendo le parole del quadrato dal basso verso l'alto purché ogni riga sia letta da destra verso sinistra. L'iscrizione è stata oggetto di frequenti ritrovamenti archeologici, sia in epigrafi lapidee sia in graffiti, ma il senso e il significato simbolico rimangono ancora oscuri, nonostante le numerose ipotesi formulate. Nella specie, tenet significa "tiene", "regge", "guida", ed è stato volontariamente indicato con la lettera iniziale e finale in maiuscolo ed abbinato all'espressione, eguale sia in latino che in inglese, Data.

SOMMARIO

INTRODUZIONE

Le trasformazioni della *sharing economy* e lo sviluppo delle applicazioni di intelligenza artificiale, dovute all'evoluzione tecnologica e al crescente impiego dei dati - visti quali input produttivi - hanno comportato un ampliamento delle condizioni in cui i trattamenti potrebbero considerarsi necessari e legittimi anziché abusati e deprecabili.

Da un lato, la prestazione agli utenti di servizi e contenuti senza l'applicazione di condizioni economiche e, dall'altro, la fornitura alle organizzazioni di spazi pubblicitari, la remunerazione dei protagonisti del *programmatic advertising* e copiosi set di dati per alimentare le capacità predittive degli algoritmi.

Cookie, *web beacon*, *pixel tag*, file di registro o altre tecnologie passive come il *fingerprinting* vengono impiegati, anche per il tramite di tecnologie *IoT*, per raccogliere determinate informazioni sui visitatori e sugli utenti del web. Esistono quasi due miliardi di siti web online in questo momento. Banner informativi, popup e schermate di caricamento *"splash screen*" presentano un design e un'esperienza utente non indicative di processi sottostanti uniformi, adeguati e rispettosi; le scelte appaiono fortemente influenzate dai requisiti e dagli obiettivi aziendali, se non addirittura dalla totale ignoranza dei vari titolari e responsabili del trattamento a scapito del rispetto dei principi della data protection.

Sempre di più e sempre con più "prepotenza" la vita dell' interessato si svolge, si snoda e alla fine, inevitabilmente, si scontra con la realtà tecnologica. Gli utenti, nonostante gli attuali quadri regolatori, si rivelano estremamente vulnerabili di fronte ad una persistente mancanza di trasparenza che inerisce (oltre ad esserne inevitabile conseguenza) alla vasta portata delle asimmetrie informative presenti nell'ecosistema *data driven*.

OSSERVAZIONI sulle modalità per promuovere la consapevolezza e la trasparenza.

Approccio Legal Design

[2]

Abstract: La prospettiva *legal* incontra il *design*, mossa dall'esigenza di rendere chiaro, semplice, immediato, accessibile e comprensibile sia il diritto in sé che le sue applicazioni pratiche, specialmente le più spinose. Promuovere e sviluppare l'impatto "estetico" del diritto rappresenta senza dubbio una delle sfide del futuro. Un approccio dunque multidisciplinare diretto dai canoni del *Legal Design* e della *Legal Compliance (well) designed*, che vorremmo fosse favorito e sostenuto dall'Autorità GPDP, poiché espressione di una metodologia progettuale che vuole rappresentare prima di ogni altra cosa un modo per essere socialmente responsabili e dare valore ai principi posti alla base della protezione dei dati personali.

Autori: Barbara Calderini, con il contributo di Natalia Artemenko, Maria Grassetto, Maria Grazia Romano, Alessandra Etzo, Karin Malaspina, Federico Alessandri, Floriana Tagliaferro

[2] Le icone utilizzate sono tratte dal progetto "DaPIS (Data Protection Icon Set)" created by CIRSFID, Università di Bologna and Accademia di Belle Arti di Bologna. DaPIS is released under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) (https://creativecommons.org/licenses/by-sa/4.0/).

LA PROPOSTA n.1

- chiediamo che Codesta Autorità Garante possa farsi promotrice in aderenza alla propria funzione - in seno al Comitato europeo per la protezione dei dati, al Garante europeo della protezione dei dati, e dunque sulla base delle rispettive competenze, alla Commissione UE - di una consapevole e proattiva richiesta di attivazione del meccanismo previsto dall'art. 12 par. 8) del RGPD.

Se da una parte condividiamo l'obiettivo delle Linee guida di specificare le corrette modalità per la fornitura dell'informativa e per l'acquisizione del consenso online degli interessati, ove necessario, alla luce della piena applicazione del Regolamento UE 2016/679, dall'altra vogliamo evidenziare l'esigenza (peraltro già colta in sede di approvazione del RGPD da Jan Philipp Albrecht, componente del Parlamento Europeo, con la sua proposta – non recepita - di standardizzazione di icone) che la nostra Autorità Garante possa farsi promotrice, in aderenza alla propria funzione - in seno al Comitato europeo per la protezione dei dati, al Garante europeo della protezione dei dati, e dunque sulla base delle rispettive competenze, alla Commissione UE - di una consapevole e sagace richiesta di attivazione del meccanismo previsto dall'art. 12 par. 8) del RGPD.

Ci riferiamo al potere conferito alla Commissione di adottare atti delegati ai sensi del successivo art. 92 (in combinato disposto con l'art. 290 T.F.U.E.) affinché possa stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

Riteniamo che proprio quest'ultimo strumento possa costituire una buona opportunità, anche in ottica di trattamento cookie e altri strumenti di tracciamento *"per rafforzare e rendere omogenea la protezione dei dati personali nell'Unione Europea"* (Considerando 166 RGPD).

Tale potere, consistente in atti non legislativi ma di dettaglio ed aventi comunque portata generale, potrebbe infatti contribuire efficacemente al processo di armonizzazione, diffusione della consapevolezza ed adeguamento di determinate caratteristiche del RGPD relative ai trattamenti di tracciamento e profilazione digitale degli individui, in linea con gli sviluppi del settore.

E, segnatamente, nei settori del *programmatic advertising* e dell'intelligenza artificiale (machine learning): ovvero un ecosistema dei poteri - spesso privati - legato alle logiche "*data business*",

dove la gestione nebulosa che segue l'accesso alle informazioni, affidata a big companies e terze parti, ha già dato prova ovunque di quanto ciò possa limitare l'autentica capacità di autodeterminazione (diritto principe tra i diritti umani) e le libertà fondamentali di ogni società democratica e dei suoi componenti.

Non a caso *"chi controlla le domande dà forma alle risposte e chi controlla le risposte dà forma alla realtà".*

Auspichiamo che la Commissione possa in tal modo continuare a svolgere il ruolo cruciale che le compete, forte della cooperazione delle Autorità e della comunità degli esperti, nella decisa e concreta valorizzazione del diritto all'intelligibilità, alla concisione, alla trasparenza e all'autodeterminazione informativa, al centro degli artt. 12, 25 e 5.1 del RGPD (e suoi Considerando, specie 58 e 60), dell'attuale art. 122 del Decreto Legislativo 196/03 e ancor prima dell'art 8 par. 2 Carta UE: dalla definizione delle modalità semplificate di informativa, alla predisposizione di icone standardizzate, fino alla chiara e corretta individuazione delle modalità di rilascio del consenso dell'utente per l'installazione dei cookie e dei corrispondenti casi di esenzione dalla suddetta necessità. Dal preciso inquadramento giuridico e semantico delle diverse tipologie di tracciamento digitale sia attivo che "silente e passivo" (o addirittura "predittivo") alla corretta considerazione della funzione identificativa legata alle inferenze (*inferred data*). Qui un interessante rapporto sull'incremento dell'incidenza in rete degli identificativi passivi intitolato *"Identity 2020 Changes to Cookies, Ad IDs, and Regulations Take Aim at Tracking"* reso da diciannove esperti del settore.

Questo anche sulla scia dell'iniziativa "Legiferare meglio", nel contesto dell'Accordo internazionale tra Parlamento europeo, Consiglio e Commissione nel 2016, e nella logica inclusiva e "multi-stakeholder" di cui la Commissione si sta facendo da tempo portavoce con il Programma di controllo dell'adeguatezza e dell'efficacia della regolamentazione **REFIT**.

E dunque avendo ben presente la complessità del quadro giuridico specifico di riferimento: dalla direttiva 2002/58/CE e successive modifiche (in attesa che prenda forma la preannunciata proposta di Regolamento e-Privacy), al RGPD, passando per le relative Linee guida del WP29, del Comitato europeo per la Protezione dei dati e la giurisprudenza delle Corti Europee (in particolare Corte di Giustizia - CGUE C-210/16 e C-40/17, Fashion ID). Non ultimi il provvedimento n. 229, del

8 maggio 2014 e le Linee Guida attualmente in consultazione, oltre a quelle pubblicate dalle altre Autorità Europee tra cui Gran Bretagna (ante Brexit), Francia e Belgio.

LA PROPOSTA n. 2

- L'approccio che suggeriamo, e che, se accolto dall'Autorità, potrà fungere da orientamento per la Commissione (ai fini di cui all'art. 12 par. 8) del RGPD) ma anche per auspicabili eventi ed iniziative promosse e dirette dell'Autorità (*regulatory sandbox*, proposte formative, *challenge*, *workshop*, *webinar*), è quello multidisciplinare del Legal Design e della Legal Compliance (*well*) designed, entrambi espressione di una metodologia progettuale che vuole rappresentare prima di ogni altra cosa un modo per essere socialmente responsabili.

"Il diritto è arte di tracciare limiti, e un limite non esiste se non in quanto sia chiaro. E poiché non vi è pensiero giuridico se non in quanto sia chiaro, tutto ciò che è oscuro può appartenere forse ad altre scienze, ma non al diritto!" Vittorio Scialoja

L'approccio che suggeriamo e che, se accolto dall'Autorità, potrà fungere da orientamento per la Commissione (ai fini di cui all'art. 12 par. 8) del RGPD) ma anche per auspicabili eventi ed iniziative promosse e dirette dell'Autorità (*regulatory sandbox*, proposte formative, *challenge*, *workshop*, *webinar*), è quello multidisciplinare del Legal Design e della Legal Compliance (*well*) designed, entrambi espressione di una metodologia progettuale che vuole rappresentare prima di ogni altra cosa un modo per essere socialmente responsabili.

Ciò non rappresenta una panacea per il diritto alla protezione dei trattamenti dei dati personali, ma siamo altrettanto convinti che possa apportare un significativo "avvicinamento" verso la trasparenza nel mondo della tecnologia e della diffusione della cultura della privacy.

Sul punto sosteniamo convintamente l'intenzione preannunciata dal Garante "*di avviare nelle sedi più opportune e tra tutti i soggetti interessati (accademia, industria, associazioni di categoria, decisori, stakeholder etc.) una riflessione circa la necessità dell'adozione di una codifica standardizzata relativa alla tipologia dei comandi, dei colori e delle funzioni da implementare all'interno dei siti web per conseguire la più ampia uniformità, a tutto vantaggio della trasparenza, della chiarezza e dunque anche della migliore conformità alle regole*".

Diverse organizzazioni di esperti e laboratori di studio del Legal Design si sono distinti in tale ambito e hanno reso evidenti le potenzialità legate ad una tale metodologia progettuale.

E' evidente, in tale contesto, l'importanza che riveste il binomio *user experience* (UX) – *user interface* (UI): una relazione da tradursi in una metodologia umano-centrica (utente-centrica) e pro-attiva, frutto di un lavoro in team multidisciplinari in grado di verificare il riscontro effettivo delle applicazioni teoriche con le fasi di successiva convalida derivanti dal relativo metodo scientifico.

In materia di cookie e altri identificatori, le soluzioni pratiche di acquisizione e manifestazione del consenso (informato, libero, specifico, inequivocabile, espresso), come la corretta esternazione del principio di autodeterminazione informativa, dovrebbero ispirarsi a relazioni di fiducia di lungo periodo, chiare e consapevoli, di tipo *win – win*, orientate al rispetto del principio del minimo intralcio (Cons. 32 e 39 e art 12 RGPD).

La condivisione di *framework* di progettazione consapevole e responsabile, di strumenti visuali, icone, illustrazioni, *chatbot*, diagrammi, *videotelling* e *storytelling*, veicolati attraverso iniziative promosse direttamente dalle Autorità, potrebbe favorire la creazione di valore e conformità normativa e contribuire a ridurre l'asimmetria informativa senza limitarsi alla sola gestione del rischio.

Gli operatori dei siti web e i titolari dei trattamenti, resi edotti dei *framework* in tal modo sviluppati, rimarrebbero comunque liberi di utilizzare, progettare o commissionare flussi di consenso adatti alle loro organizzazioni, purché tale consenso possa essere considerato valido ai sensi della legislazione UE e il processo di acquisizione rispondente ai principi di *privacy by design* (di cui all'art 25 del RGPD) e alle pertinenti disposizioni della direttiva e-Privacy 2002/58/CE, come modificata dalla direttiva 2009/136/CE.

L'obiettivo ambizioso sarebbe quello di favorire la creazione e la condivisione di interfacce ed esperienze ben progettate, caratterizzate dal design incentrato sull'uomo e sullo sviluppo tecnologico trasparente, agile ed inclusivo. Gli stessi strumenti andranno quindi orientati e predisposti al *semantic – web*, per applicazioni digitali o multicanale, *desktop* e *mobile*.

I progetti migliori dovrebbero essere quindi testati, verificati, convalidati, sistematizzati, diffusi e resi riutilizzabili attraverso degli standard condivisi in modo da veicolare applicazioni coerenti ed uniformi.

A tal riguardo, unitamente alla Commissione, il Garante potrebbe senza dubbio svolgere un ruolo fondamentale nella produzione di Linee guida di orientamento e nella promozione di iniziative dirette, mirate e lungimiranti (*regulatory sandbox* e specifiche *challenge* rivolte ai professionisti). Allo stesso modo il ruolo delle Autorità e delle Istituzioni sarà cruciale, potendo le stesse contribuire, in aderenza alle loro funzioni e agli obiettivi delle normative, ad individuare e dare risalto a *framework* progettuali specifici e *best practice* di progettazione "*data protection by design*" verificate e convalidate, uniformi ed efficaci.

Da qui rinnoviamo la richiesta di intervento da parte delle Commissione europea ai sensi dell'art. 12 par. 8) del RGPD e delle Autorità europee, ciascuna nell'alveo delle rispettive competenze e delle reciproche missioni in ottica di collaborazione e coerenza.

Vogliamo sottolineare gli apprezzabili risultati, di cui si potrà senz'altro tenere conto, ottenuti nell'ambito della recente iniziativa promossa dal GPDP e dal gruppo dei Legal Hackers di Roma: l'hackathon "HACKtheDOC".

Il primo hackathon in Italia in materia di Legal Design contenente la sfida "Policy – challenge del Garante INFOPRIVACY", avente come obiettivo il fatto di dover ridurre di almeno il 50% i caratteri delle informative privacy delle principali piattaforme web e social, utilizzando icone e altri elementi grafici e visivi.

Tra gli otto finalisti è presente anche il progetto che vede tra gli autori e ideatori alcuni dei sottoscritti.

Le realizzazioni rilasciate nel corso dell'evento hanno reso evidente come sia possibile coniugare etica e rule of law.

Ovvero cultura della materia, conoscenza condivisa, etica e rigore creativo, come peraltro ci insegna Enzo Mari, uno tra i più autorevoli esponenti del design italiano, recentemente scomparso.

Design Thinking e Legal Design, insieme ad una sapiente declinazione dell'incrocio tra semantica e semiotica potranno contribuire efficacemente ad abbattere non solo le manifestazioni più "ardite" della pratica nota come cookie wall, bene evidenziata nelle considerazioni che seguiranno, ma altresì quella del "*wall of text*" rappresentato dai tecnicismi e dalla complessità lessicale giuridica, per di più amplificati in caso di visualizzazioni da dispositivo mobile.

La sfida importante che il Legal Design può vincere, consisterà nel trovare il modo giusto per "dare gusto" alla lettura attraverso la diffusione di interfacce *visual* idonee a definire velocemente lo scopo dello strumento legale, apportando evidenza e intelligibilità senza perdere il rigore e la gestione dei rischi normativi.

Più le policy, i banner informativi e le piattaforme di gestione del consenso per cookie saranno comprensibili e resi attrattivi e a misura dell'utente, più sarà facile ottenere la consapevole interazione di quest'ultimo anche nella conseguente manifestazione del consenso.

I SUGGERIMENTI DI APPROFONDIMENTO

Utili si riveleranno in tal senso gli studi e le prime applicazioni strutturate del Legal Design curate da esperti tra i quali Helena Haapio e Stefania Passera, oltre ovviamente alla prof.ssa Margaret Hagan, Direttrice del Legal Design Lab.

E tra questi, a livello internazionale, anche il network denominato "The Legal Design Alliance". Una rete di esperti in cui convergono competenze trasversali, giuristi, designers, tecnici, accademici, da cui è scaturito l'interessante programma ad accesso libero The Legal Design Manifesto, finalizzato a far conoscere e promuovere lo sviluppo del Legal Design, migliorandone la comprensione e favorendone le concrete applicazioni.

Ancora, l'associazione internazionale IACCM International Association for Contract & Commercial Management, dove Stefania Passera e Helena Haapio hanno partecipato alla creazione della Contract Design Pattern Library, una raccolta di linee guida, spiegazioni ed esempi finalizzata a fornire supporto e ad ampliare, attraverso il libero contributo dei partecipanti alla relativa piattaforma, nuovi metodi di approccio alla realizzazione di documenti legali.

Interessante anche il progetto **GDPR BYDESIGN** del CIRSFID (Centro interdipartimentale di ricerca in storia del diritto, filosofia e sociologia del diritto e di informatica giuridica dell'Università di Bologna), che ha proposto una serie di icone intuitive e a rapida velocità di riconoscimento, utilizzabili per le informative Data protection (progetto **DaPIS**)[3].

I CAMPI D'AZIONE SPECIFICI SUI QUALI AGIRE

Abstract: Il campo d'azione specifico, al quale intendiamo riferirci suggerendo l'approccio Legal *Design*, riguarda tanto l'informativa breve contenuta nel pop up o *banner* iniziale - insieme informativo e di controllo dei *cookie consent* - CMP(*consent management platform*), quanto l'informativa estesa. Sono ovviamente inclusi i *devices* dell'IoT che spesso non disponendo di interfacce analoghe a quelle dei *pc* o degli *smartphone* dovrebbero prevedere la progettazione di metodologie adeguate per informare gli utenti, ad esempio, nella fase di registrazione del prodotto sul *web* o tramite un'apposita *app* mobile, in modo che anche necessari consensi possano essere adeguatamente raccolti (a tal proposito, si evidenziano le raccomandazioni fornite da parte dell'ICO - cfr. paragrafo "What about other devices like mobiles, smartTVs, wearables, and the 'Internet of Things'?" in Guidance on the use of cookie and similar technologies).

Richiamandoci all'osservazione di Codesta Autorità sulla "*necessità di un quadro rafforzato di tutele maggiormente orientate a favorire e a rendere effettivo il controllo sulle informazioni personali oggetto di trattamento e, in definitiva, la capacità di autodeterminazione del singolo*" a maggior ragione "*in considerazione dell'evoluzione comportamentale degli stessi utenti della rete, sempre più orientati alla proliferazione delle proprie identità digitali come risultanti dall'accesso a molteplici servizi e funzioni disponibili e, in primo luogo, ai social network*" e al "*rischio che le informazioni personali oggetto di trattamento siano raccolte proprio incrociando i dati anche relativi all'utilizzo di funzionalità e servizi diversi (cd. enrichment), con l'effetto della creazione di profili sempre più specifici e dettagliati*" – vogliamo sottolineare che:

il campo d'azione specifico, al quale intendiamo riferirci suggerendo l'approccio Legal Design, riguarda tanto l'informativa breve contenuta nel pop up o banner iniziale - insieme informativo e

[3] Le icone sono scaricabili gratuitamente e possono essere utilizzate con licenza "Creative Commons Attribution-ShareAlike 4.0 International License".

di controllo del cookie consent - CMP (*consent management platform*), quanto l'informativa estesa. Sono ovviamente inclusi i devices dell'IoT che spesso, non disponendo di interfacce analoghe a quelle dei pc o degli smartphone, dovrebbero prevedere la progettazione metodologie adeguate per informare gli utenti, ad esempio, nella fase di registrazione del prodotto sul web o tramite un'apposita app mobile, in modo che anche necessari consensi possano essere raccolti (a tal proposito, si evidenziano le raccomandazioni fornite da parte dell'ICO - cfr. paragrafo "*What about other devices like mobiles, smartTVs, wearables, and the 'Internet of Things'?"* in Guidance on the use of cookie and similar technologies).

Policy e banner, ad oggi, veicolo tanto di modelli oscuri - dark patterns - ovvero interfacce utente che avvantaggiano un servizio online (una sorta di progettazione circumvention by design) inducendo gli utenti a prendere decisioni che altrimenti non potrebbero prendere, quanto di "patterns luminosi" che veicolano erronee e irriflessive percezioni di controllo, ambedue pesantemente e pericolosamente fuorvianti e a diretto pregiudizio della compliance normativa e della corretta valorizzazione dei diritti degli interessati.

Qui una rassegna dei modelli di progettazione relativi alla richiesta di consenso sui cookie, notifiche push intrusive, richieste di autorizzazione, tracciamento di terze parti ed esperienza di offboarding, in uso tra le maggiori piattaforme social e le società di media.

Strumenti, questi, che, in piena difformità normativa:

- non permettono o rendono eccessivamente arduo optare per scelte granulari e non condizionanti sulle tipologie di cookie, quando addirittura contengono caselle preflaggate;
- non consentono di rifiutare in blocco tutti i cookie, anche dopo averli – eventualmente – accettati in blocco;
- introducono surrettiziamente basi giuridiche per l'installazione dei cookie diverse dal consenso, come l'interesse legittimo, subordinandone la presa d'atto ad estenuanti e deplorevoli visualizzazioni. Sul punto si rimanda a quanto evidenziato nello specifico paragrafo relativo alla corretta individuazione delle basi di legittimità ;

- non ultimo, non permettono di ricordare, aggiornare e revocare le scelte operate dall'utente.

Parliamo di un ampio scacchiere di cookie banner, prompt , overlay o finestre popup che si aprono o scorrono in primo piano sui siti web progettati ed implementati in maniera del tutto distante dal rispetto dei più basilari canoni normativi. Quelli più semplici in uso affermano semplicemente che il sito web utilizza i cookie senza alcuna opzione, mentre quelli più complessi consentono agli utenti di (de!)-selezionare individualmente ciascun servizio di terza parte utilizzato dal sito web, spesso con artifici giuridici e grafici davvero poco decorosi.

LA PROPOSTA n. 3

- Undici osservazioni relative alla redazione dell'Informativa riepilogati nell'Allegato 2 all'Avviso relativo alla Consultazione sulle "Linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento"

Quanto ai consigli di miglioramento che *"i titolari potranno adottare al fine di rendere agli utenti una informativa conforme ai rinnovati requisiti di trasparenza imposti dagli articoli 12 e 13 del RGPD, compresa l'indicazione circa gli eventuali altri soggetti destinatari dei dati personali ed i tempi di conservazione delle informazioni acquisite",* ribadendo le precedenti osservazioni circa la necessità di un approccio di Legal Design, di cui la stessa Commissione e l'Autorità Garante potranno farsi primi promotori, osserviamo quanto segue:

1. Fermo il fatto per cui le responsabilità dei singoli titolari del trattamento resteranno elemento centrale dell'*accountability*, posta alla base del quadro regolatorio in tema di protezione dei dati, va comunque preso atto che, stanti le difformità interpretative delle diverse Autorità europee, al fine di avere un grado di tutela dei diritti degli utenti uniforme, riteniamo possa essere vantaggioso prevedere approcci quanto più possibilmente compartecipati e *framework* tecnologici, condivisi e ispirati a criteri di comprensibilità, correttezza e trasparenza by design.
2. Riteniamo condivisibile l'indicazione del Garante relativa alla sola presenza di cookie tecnici per i quali potrà essere data informazione nella home page, o ad altra pagina di accesso del sito web, o nell'informativa generale senza l'esigenza di apporre specifici

banner da rimuovere a cura dell'utente. Muovendo da un'altra prospettiva, la relativa informazione potrebbe comunque essere ben inserita all'interno della sola informativa sul trattamento dei dati personali per garantire la giusta attenzione e preservarne il nesso col trattamento dei dati personali.

3. Quanto all'indicazione contenuta al punto c) dell'Allegato 2 Informativa e Consenso per cui *"la prosecuzione della navigazione mediante la selezione di un esplicito comando o di un elemento contenuto nella pagina sottostante il banner comporta la prestazione del consenso alla profilazione",* siamo del parere che la selezione di un esplicito comando o di un elemento contenuto nella pagina sottostante il banner possa integrare i requisiti previsti per una valida manifestazione del consenso (come previsti dalle normative vigenti), solo se lo stesso sia progettato e reso comprensibile in modo tale da non favorire *bias* cognitivi dell'utente inducendolo a cliccare nella pagina sottostante soltanto per eliminare il banner.
4. Relativamente al punto d) dell'Allegato 2 Informativa e Consenso, circa la presenza di "*un comando per accettare tutti i cookie o altre tecniche di tracciamento*" riteniamo che lo stesso rappresenti una scelta progettuale ottimale solo laddove riesca allo stesso tempo ad attenersi ai parametri del Legal Design volti a rendere efficacemente edotto l'utente dell'effettiva portata della profilazione sia attiva che, a maggior ragione, passiva. In aggiunta, riteniamo utile prevedere all'interno del banner anche un comando "rifiuta tutti i cookie non necessari".
5. Analoghe considerazioni valgono per il punto e) dell'Allegato 2 Informativa e Consenso relativamente alla previsione di un *"link ad un'altra area nella quale poter scegliere in modo analitico le funzionalità, le terze parti e i cookie che si vogliono installare e, tramite due ulteriori comandi, poter prestare il consenso all'impiego di tutti i cookie se non dato in precedenza o revocarlo, anche in unica soluzione, se già espresso*". In particolare, tramite l'individuazione degli specifici *framework* progettuali di cui si è detto e le apposite icone, i cookie potrebbero essere suddivisi per gruppi in base alla funzionalità, servendosi di apposite visualizzazioni stilistiche che riducono l'asimmetria informativa e i *bias* cognitivi a cui è esposto l'utente. Per ogni gruppo di cookie potrebbero essere previsti due comandi, per accettarli tutti o rifiutarli tutti. Un utente potrebbe essere ben disposto ad accettare, ad esempio, solo cookie analitici/statistici, a prescindere dalla loro titolarità, mentre

potrebbe non essere disposto ad acconsentire a cookie di marketing o a cookie di profilazione. Prevedere un unico comando che consenta di accettare tutti i cookie del gruppo analitici/statistici evita all'utente l'onere di doverli selezionare uno ad uno.

6. Il Garante suggerisce la necessità di valutare *"l'adozione di una codifica standardizzata relativa alla tipologia dei comandi, dei colori e delle funzioni da implementare all'interno dei siti web per conseguire la più ampia uniformità, a tutto vantaggio della trasparenza, della chiarezza e dunque anche della migliore conformità alle regole".* Siamo favorevoli a tale impostazione per tutte le motivazioni già espresse. Tale orientamento è peraltro in linea anche con le raccomandazioni espresse dalla CNIL nella Délibération n° 2020-092 la quale, tuttavia, attraverso il rimando ad esempi concreti, si limita a raccomandare ai titolari del trattamento di non ricorrere alle pratiche di design potenzialmente ingannevoli per gli utenti, senza adottare una vera e propria codifica standardizzata. Ciononostante, dovranno essere prese in considerazione le problematiche relative a particolari limitazioni visive e disturbi specifici della lettura che si manifestano con una difficoltà nella decodifica del testo; e dunque previste modalità alternative ai colori e alla sola grafica (*chatbot*, video).
7. Condividiamo con Il Garante l'adesione all'interpretazione contenuta nell'opinione dell'EDPB (che si pone, peraltro, in una coerente linea di continuità rispetto alla posizione già rappresentata con il provvedimento del 2014 e i "Chiarimenti in merito all'attuazione della normativa in materia di cookie" del 5 giugno 2015) e che il semplice "scroll down" del cursore di pagina sia assolutamente inadatto in sé alla raccolta, da parte del titolare del trattamento, di un idoneo consenso all'installazione e all'utilizzo di cookie di profilazione.
8. A maggior ragione ribadiamo l'importanza dell'approccio Legal Design laddove dovesse essere invece confermata la posizione del GPDP in fatto di scrolling nello specifico contesto in cui questo fosse una "*componente di un più articolato processo che consenta comunque all'utente di segnalare al titolare del sito, con la generazione di un preciso pattern, una scelta inequivoca nel senso di prestare il proprio consenso all'uso dei cookie*." In tal caso preme comunque evidenziare che un tale ragionamento, sebbene tecnicamente sostenibile, si presenti sempre particolarmente insidioso specie se riferito a contesti di dispositivi mobile e di scarsa percezione dell'utente. Lo scroll infatti può essere spesso

involontario (tipicamente si scende nella pagina verso la parte che ci interessa scrollando verso il basso) rivelandosi chiaramente inidoneo a soddisfare il requisito di chiara azione.

Come ha affermato Geoffrey Keating nel suo articolo, " The cookie Law and UX ", riferendosi specificamente alla legislazione in Irlanda, secondo l'Ufficio del Commissario per la protezione dei dati, "*the minimum requirement is that clear communication to the user as to what he/she is being asked to consent to in terms of cookie usage and a means of giving or refusing consent is required".*

9. Altrettanto vale in ottica di ridondanza e reiterazione della richiesta di consenso: sebbene il Garante osservi che *"il consenso, una volta correttamente acquisito, non debba essere nuovamente richiesto se non all'eventuale mutare di una o più delle condizioni alle quali è stato raccolto ovvero quando sia impossibile, per il gestore del sito web, avere contezza del fatto che un cookie sia stato già in precedenza memorizzato sul dispositivo per essere nuovamente trasmesso, in occasione di una successiva visita del medesimo utente, al sito che lo ha generato",* va evidenziato come l'accesso ai device fissi o mobile si presti ad usi promiscui da parte di più soggetti (specie in contesti familiari) generando diverse aspettative di protezione che non sarebbero soddisfatte dagli specifici criteri enunciati nelle Linee guida in consultazione. In tali circostanze il Legal Design potrebbe quindi intervenire fornendo soluzioni di interfaccia grafica risolutive e ad alta velocità di percezione, che prevedono formulazioni visive o di altro genere (interattive ad esempio) idonee a rendere edotta, senza appesantirla, l'esperienza di navigazione del singolo utente e, allo stesso tempo si rivelano adeguate ai dettami normativi. Ad esempio, nelle medesime circostanze indicate dal Garante, potrebbe essere previsto l'utilizzo di un micro banner con icona che, posizionato a regola d'arte, evidenzi lo stato attuale del consenso per categorie di cookie consentendone l'aggiornamento tramite meccanismi di opt-out e opt-in diretti, o che rimandano al secondo livello - informativa estesa- anch'essa elaborata secondo criteri di Legal Design, per l'eventuale esigenza di approfondimento.
10. Il Garante suggerisce, inoltre, la collocazione nell'area home page, o ad altra pagina di accesso del sito web, di due comandi "*idonei a garantire il cd. "diritto di ripensamento" e di revoca del consenso agli utenti che, avendo già effettuato una specifica scelta al momento del primo accesso al sito web, intendano successivamente optare per una scelta*

diversa". Sul punto osserviamo come il termine "diritto di ripensamento", frequentemente usato come sinonimo del diritto di recesso nell'ambito della materia di diritto dei consumatori (disciplinata dalla Direttiva 2011/83/UE U.E. recepita in Italia dal D.lgs. n. 21/2014 e dal Codice del consumo emanato con il D.lgs. n. 206/2005 e s.m.i.), sia sostanzialmente ben distinto dall'istituto di "revoca del consenso prestato" ai sensi del Regolamento UE 2016/679. Il consenso costituisce infatti una base giuridica a sé stante, differente da quella contrattuale (art. 6, par. 1, lett. b) del Regolamento), da cui invece può scaturire il diritto di ripensamento. Pertanto, al fine di scongiurare rischi di ambiguità e confusione negli utenti, in alternativa all'inserimento di "due ulteriori comandi idonei a garantire il c.d. "diritto di ripensamento" e di revoca del consenso agli utenti" riteniamo conveniente che nell'area in questione, oltre al link sulla privacy policy, sia previsto soltanto un comando, relativo alla revoca del consenso azionabile in qualsiasi momento e agevolmente da parte dell'utente.

11. Reputiamo condivisibile il richiamo del Garante al fatto per cui *"l'informativa, oltre che multilayer, e cioè dislocata su più livelli, possa ad oggi essere resa, eventualmente in relazione a specifiche necessità, anche per il tramite di più canali e modalità (cd. multichannel), in modo da sfruttare al massimo più dinamici e meno tradizionali ulteriori punti di contatto tra il titolare e gli interessati"*. E certamente il modo in cui potrebbero essere fornite le informazioni oltre che testuale e visivo, potrebbe essere uditivo o leggibile dalla macchina e addirittura interattivo (es. con il chatbot), navigabile tramite tag, ricerca a testo libero o riferimento legale. Anche in tal senso il Legal Design potrebbe assolvere allo scopo di trovare una soluzione ai problemi di trasparenza e comprensibilità degli specifici testi a contenuto normativo, a partire proprio dalla loro ideazione e progettazione. E dunque proprio la definizione dei criteri base dell'informativa da presentare sotto forma di icone standardizzate costituisce l'oggetto della nostra richiesta di attivazione ai sensi dell'art 12 par.8 del RGPD, favorita dall'iniziativa diretta delle Autorità. Un auspicio che si pone in linea anche con la speranza espressa dal Garante affinché "*si addivenga in tempi rapidi ad una codifica di carattere generale, tanto più importante specie nell'attuale mondo connesso online, nel quale le distanze geografiche perdono rilevanza a fronte delle sempre più accentuate potenzialità della rete*" e alla necessità che i titolari debbano "*rendere manifesti, mediante apposita, opportuna*

integrazione dell'informativa, almeno i criteri di codifica degli identificatori adottati da ciascuno." Criteri che certamente "*potranno, inoltre, a richiesta, costituire oggetto di comunicazione all'Autorità, quale strumento di ausilio alle attività di carattere istruttorio che saranno intraprese con riguardo al fenomeno in considerazione*."

Sotto questo profilo si potrebbe pensare anche ad una doppia codifica per adulti e per minori, proponendo forme/icone e linguaggi diversi, che catturino l'attenzione dell'utente e raggiungano per quanto possibile l'obiettivo di renderlo consapevole dell'esistenza e del significato del cookie o degli altri sistemi di tracciamento (l'utente medio non sa cosa sono), delle finalità della raccolta e dei possibili usi che ne vengono fatti sia dal titolare del sito che dalle terze parti.

DARK PATTERNS: GLI STUDI PIU' AUTOREVOLI

- A seguire, una rassegna dei migliori studi sui modelli oscuri. Le analisi e i consigli degli esperti per il miglioramento della progettazione dei banner informativi e di controllo dei cookie consent

---

"I principi di privacy by design e privacy by default sono componenti fondamentali del RGPD. I modelli oscuri sono un modo per le aziende di aggirare questi principi spingendo spietatamente i consumatori a ignorare la loro privacy e a fornire più dati personali del necessario. Questo è un problema che dobbiamo affrontare."
Così Giovanni Buttarelli, Garante europeo della protezione dei dati, all'apertura della Tavola rotonda sui modelli oscuri tenutasi il 27 aprile 2019 a Bruxelles.

Siamo convinti che uno dei problemi che limitano l'efficacia delle norme sia la mancanza di una metodologia condivisa per identificare i dark patterns.

Nudge marketing, Circumvention by design, Dark Patterns: questi i nuovi paradigmi veicolati attraverso l'uso distorto del growth hacking.

Di seguito abbiamo selezionato CINQUE tra gli studi più autorevoli redatti dai maggiori esperti, grazie ai quali si è iniziato a far luce su molte delle tecniche scorrette che vengono usate online a partire proprio dalle interfacce cookie. Ogni approfondimento riporta una preziosa panoramica

dei casi pratici di studio e una serie di consigli che potrebbero fungere da stimolo e opportunità di ulteriore sviluppo anche da parte del Garante.

1. Qui l'interessante approfondimento del maggio 2020 intitolato "Dark Patterns: Past, Present, and Future - The evolution of tricky user interfaces" di cui sono autrici Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar, che cataloga dozzine di schemi problematici che prendono di mira l'utente (comprese le maggiori piattaforme online), ostacolano il regolare flusso della propria attività cognitiva e prevedono impostazioni predefinite intrusive per la privacy. Basandosi sulle risultanze ottenute da Harry Brignull, esperto di UX design, tra i primi a proporre una tassonomia dei *pattern* oscuri e fondatore del noto sito darkpatterns.org (ricco di esempi), i ricercatori hanno inteso spiegare il funzionamento dei modelli oscuri riportando prove preliminari a dimostrazione di quanto siano in grado di sfruttare efficacemente i pregiudizi cognitivi degli individui attraverso la manipolazione del comportamento. L'analisi si conclude con alcuni consigli per i designer attenti all'etica e alla correttezza.
2. Lo studio, pregevole, Dark Patterns after the RGPD: Scraping Consent Pop-ups and Demonstrating their Influence di cui è autore Michael Veale, insieme a Midas Nouwens, Ilaria Liccardi, D. Karger e Lalana Kagal, del Massachusetts Institute of Technology, dell'University College London e della Aarhus University, evidenzia come i progetti dei cinque CMP (Cookiebot, Crownpeak, OneTrust, Quantcast e TrustArc) più popolari, sui primi 10.000 siti Web web nel Regno Unito adottino in gran parte modelli oscuri e di consenso implicito; solo l'11,8% si è rivelato adeguato ai requisiti minimi in base alla legge europea. Secondo gli autori "schemi oscuri" e consenso implicito sono onnipresenti. L'analisi arriva a suggerire in particolare la possibilità di concentrarsi sui servizi CMP centralizzati di terze parti. Per questo studio è stata progettata anche un'estensione del browser, che consente risposte pop-up automatiche in base alle preferenze personalizzabili dell'utente, che hanno chiamato "Consent-o-Matic", disponibile sia su Firefox che su Chrome.
3. Altrettanto stimolante lo studio, ricco di esempi reali presi dal web, intitolato Circumvention by design - dark patterns in cookie consents for online news outlets a cura di Than Htut, Oda Elise, Frode Guriby e Marija Slavkovik del Department of Information

Science and Media Studies, University of Bergen, Norvegia. I ricercatori hanno presentato un'analisi di 300 banner di richiesta del consenso presi da una selezione di agenzie di stampa online. L'analisi ha rilevato come la maggior parte di loro (297) utilizzi schemi oscuri fuorvianti. La ricerca ha consentito di individuare otto pattern specifici, potenzialmente utili per l'individuazione di esempi deprecabili.

4. La ricerca accademica "**Are cookie banners indeed compliant with the law"**? condotta da Cristiana Santos, Nataliia Bielova, e Célestin Matte Inria, le stesse autrici della Contribution to the public consultation on the CNIL's draft recommendation on "cookie and other trackers", arriva ad identificare 22 requisiti tecnico-legali (che oltre alle normative da fonti primarie tengono conto anche della giurisprudenza della Corte di Giustizia – Planet49 - e delle indicazioni delle Autorità degli Stati membri) utilizzabili per verificare e rilevare, in sede di audit, o ex post in fase di controllo, la conformità della progettazione di un processo atto a gestire la manifestazione di un valido consenso all'installazione dei cookie. Per misurare la conformità dei banner hanno sviluppato due strumenti. Il primo, "Cookinspect" (per Google Chrome) visita automaticamente i siti web con le preferenze di consenso salvate e intercetta la trasmissione del consenso a terzi. Il secondo, "cookie glasses" (per Google Chrome e Firefox) consente agli utenti di verificare se la loro scelta di consenso in un determinato banner viene trasmessa correttamente agli inserzionisti dalle CMP. Una tale metodologia tuttavia risulta fortemente condizionata dalla mancanza di approcci uniformi tra le diverse Autorità. Sfumature interpretative, a volte sostanzialmente divergenti, che sono ben rappresentate ed inquadrate nello sviluppo dello studio, ricco di grafici, esempi e schemi riepilogativi.
5. Di sicuro interesse anche lo studio dei ricercatori dell'Università del Michigan e dell'Università tedesca della Ruhr di Bochum, denominato **(Un)informed Consent: Studying RGPD Consent Notices in the Field** indaga sull'influenza della posizione dell'avviso, della presentazione del tipo di scelta, e dell'inquadratura dei contenuti, sul consenso. L'analisi si riferisce a circa 1000 siti web in Europa. I risultati evidenziano che gli utenti (un campione di 80.000 in Germania) siano più propensi ad interagire con un avviso mostrato nella parte inferiore (sinistra) dello schermo, tanto per applicazioni mobile, quanto desktop, ma conferma anche che il livello di scarsa consapevolezza riconducibile all'effettiva portata della scelta. I risultati sono piuttosto netti: se i siti web applicassero le impostazioni di

privacy by design e by default previste dalla normativa vigente, il consenso attivo all'invio di dati a terze parti sarebbe dato da meno dello 0,1 per cento degli utenti.

Gli utenti, o almeno la maggior parte di loro, oggi, è al corrente (diverso essere consapevole) che i siti web tengono traccia dei loro dati, e tuttavia lo vedono come un male necessario in cambio dell'agevole accesso ai contenuti spesso mascherati come "gratuiti".

La stessa revoca del consenso viene vista come un'alternativa non vantaggiosa e non praticabile. Per molti, l'unica opzione ragionevole è, pertanto, fornire il consenso optando per l'estensione in blocco a qualsiasi forma di tracciamento nel browser.

Tuttavia, secondo una bella ricerca del febbraio 2019 condotta nel Regno Unito dall'Information Commissioner's Office (ICO), dall'Office of Communications (Ofcom) e dalla società di ricerche di mercato Harris Interactive, il supporto dei consumatori per la visualizzazione di pubblicità digitale in cambio di contenuti gratuiti è sceso da circa due terzi (63%) a circa un terzo (36%) quando ai partecipanti al sondaggio sono state fornite alcune chiare informazioni di base su come i dati personali possono essere utilizzati nell'ambito della pubblicità digitale.

LE CONCLUSIONI SUL LEGAL DESIGN

- Non riteniamo che, requisiti normativi a parte, sia ulteriormente tollerabile l'attuale pressione "sostanziale" esercitata sull'utente finale, considerato, suo malgrado, elemento centrale delle decisioni invasive "dei vari titolari del trattamento", così come dei rispettivi processi decisionali. E' questo un terreno minato dove proprio il Legal Design, inteso come modalità per dimostrarsi socialmente oltre che legalmente responsabili, potrebbe contribuire non poco. Ma anche il tal caso la sostanza dovrebbe prendersi la rivincita sulla forma. La semantica sulla sintassi.

A conclusione delle presenti osservazioni vorremmo richiamare l'attenzione dell'Autorità sul framework Privacy by Design - adottato dall'Assemblea internazionale dei commissari per la privacy e delle Autorità per la protezione dei dati nel 2010 e inizialmente sviluppato da Ann Cavoukian. Esso (sebbene piuttosto risalente - gennaio 2011 - e poco noto al grande pubblico degli sviluppatori, stante la sua veste internazionale) potrebbe affiancarsi ai framework normativi e costituire una valida base di partenza a cui dare il giusto risalto per sollecitare aggiornamenti,

adeguamenti e best practice, specie in ambito tracciamento digitale, da parte dei team (anche Legal Design) di progettazione di software ed interfacce web o - ancora - per progetti di più ampio respiro con portata europea o anche globale. Attori di questo processo potrebbero essere il Garante e le altre Autorità ed Istituzioni europee coinvolte nella protezione dei dati e nella difesa dei diritti umani.

Allo stesso fine evidenziamo la bontà dell'iniziativa "**Data Protection as a Corporate Social Responsibility Research Group**" dell'Università di Maastricht nell'ambito dello sviluppo di un prossimo *framework* di cui è promotore il prof. avv. Paolo Balboni. E sempre sulla stessa scia l'idea dell'Istituto italiano per la privacy, con la Scuola Fumetto Cassino, che ha portato alla creazione di un generatore automatico di informative sulla privacy scandita a vignette: un modo accattivante e una buona opportunità di cui tener conto per sviluppare una lettura trasparente e intelligibile anche per i minori (tenaci naviganti del web), da applicare in tema profilazioni e cookie, sfruttando l'arte dello *storytelling*.

Non riteniamo, infatti, che requisiti normativi a parte, sia ulteriormente tollerabile l'attuale pressione "sostanziale" esercitata sull'utente finale, considerato suo malgrado elemento centrale esclusivo delle decisioni invasive "dei vari titolari del trattamento", così come dei rispettivi processi decisionali.

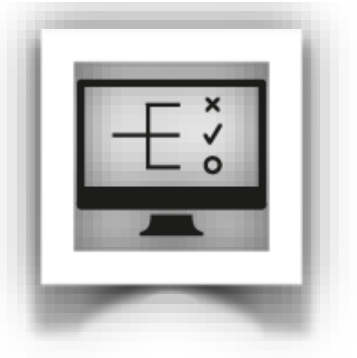
Il design dell'interfaccia di consenso che un utente deve affrontare durante la navigazione - su base quotidiana e con ramificazioni a lungo termine - non è mai pienamente conoscibile e, troppo spesso, neppure attendibile.

Lo sforzo cognitivo dell'utente "presta il fianco" alle opportunità privilegiate legate alle profilazioni, molto spesso vittima tanto dei modelli "oscuri" che incoraggiano certe scelte per scoraggiarne altre, quanto di quelli "luminosi" che veicolano erronee e irriflessive percezioni di controllo.

E' questo un terreno minato dove proprio il Legal Design, inteso come modalità per dimostrarsi socialmente oltre che legalmente responsabili, potrebbe contribuire non poco.

Ma anche il tal caso la sostanza dovrebbe prendersi la rivincita sulla forma. La semantica sulla sintassi.

Fingerprinting e altri strumenti di tracciamento. Il problema delle asimmetrie informative



Abstract: **La consapevolezza degli individui sugli strumenti di tracciamento alternativi ai *cookie*, utilizzati da siti *web* e dalle applicazioni (di cui, peraltro, si prevede un ulteriore incremento di utilizzo nel prossimo futuro) è ancora fortemente limitata e tutt'al più riservata ad un pubblico esperto. Se, inoltre, da una parte la trasparenza e il pregiudizio (discriminazione algoritmica -asimmetrie informative sia in termini di volume che di mezzi di raccolta dei dati) legati a queste forme di tracciamento sono intrinsecamente collegati, dall'altro siamo certi, alla luce dei quadri regolatori attuali, che la trasparenza di per sé non sarà un rimedio adeguato per il pregiudizio e la diffusione della consapevolezza. Sulla base di questa premessa riteniamo tuttavia utile che le Linee guida possano contribuire almeno ad una maggiore comprensione del fenomeno, prevedendo forme di trasparenza che, al fine di ridurre le asimmetrie informative, impongano agli sviluppatori maggiore attenzione verso i dati di addestramento problematici e dunque a mettere a punto programmi di tracciamento che rimuovano le inferenze dannose. Suggeriamo, in particolare, di valutare il mercato ancora "non adeguatamente regolamentato" degli annunci online alla stregua di una "borsa merci" e dunque da sottoporre agli stessi meccanismi regolatori e principi di trasparenza dei mercati finanziari.**

Autori: Leonardo Scalera, Glauco Rampogna, Barbara Calderini, con il contributo di Maria Grassetto e Gianluca Lombardi

LA PROPOSTA n.4

- Si propone di integrare le Linee guida con l'esplicito riferimento alle forme di tracciamento alternative ai cookie, prevedendo che in tali casi il titolare debba dichiararne correttamente l'uso e le finalità, dando modo agli interessati di

sottrarsi al trattamento quando questo sia per finalità di marketing e profilazione. Laddove lo scopo del rilevamento delle "impronte digitali" è infatti il tracciamento delle persone, ciò costituirà un "trattamento dei dati personali" e sarà coperto dalle normative vigenti in materia.

La preannunciata inibizione progressiva dei cookie di terze parti ha costretto il mercato ad utilizzare altri strumenti per garantire la tracciabilità degli eventi. Una tecnica consiste nell'utilizzare il sito web del titolare quale punto erogante del cookie di terzi, "ingannando" il browser, che li vede di prima parte. Un altro stratagemma consiste, invece, nell'utilizzo di funzioni di hashing di dati propri del dispositivo, del browser o delle caratteristiche di alcuni elementi HTML5 (Canvas, Audio, Image, Font, WebRTC).

La funzione di generazione delle impronte informatiche avviene nel pc dell'interessato e viene inviata ed utilizzata lato server.

Come noto, inizialmente queste tecniche venivano utilizzate per finalità di sicurezza, in modo da porre un'alternativa ai CAPTCHA e ai Proof of Work e per permettere l'individuazione di dispositivi e software da inserire in una sorta di *whitelist* del Titolare, ma ora se ne constata un uso sempre maggiore nel campo del marketing e del *programmatic advertising*. Società e reti impegnate in un complicato groviglio di contratti, subappalti e reti di partnership dove l'utente difficilmente può supervisionare realisticamente o prendere decisioni su quali aziende hanno raccolto che tipo di informazioni su di lui, quanto e cosa hanno imparato dai processi di data analisi a cui saranno sottoposte.

Anche in questo caso alcuni browser sarebbero in grado individuare e bloccare il codice che tenta la generazione delle impronte; tuttavia questa opzione dovrebbe essere abilitata esplicitamente e non è dato sapere, nella stragrande maggioranza dei siti web, quali di questi utilizzino tali tecniche, data l'assenza di richiami a ciò sia nelle informative privacy sia nelle informative cookie. Esiste inoltre un rischio nell'abilitazione di questa funzione lato browser, per la quale si potrebbe compromettere la corretta funzionalità del codice legittimo, posto per ragioni di sicurezza dal Titolare del sito web o della *web application*. L'interessato che intenda pertanto sottrarsi al trattamento potrebbe incorrere in problemi di accesso e fruibilità.

Il ricorso al *fingerprinting* sta, inoltre, aumentando anche per la relativa semplicità di generazione e salvataggio dell'impronta rispetto alla scrittura di dati nel pc, siano essi presenti in un cookie oppure in un insieme di dati maggiormente strutturato negli spazi detti Storage di sessione o Storage locale. Si prevede anche un ulteriore incremento a seguito sia della variazione nei settaggi di default dei *device* Apple, a partire da marzo 2020, sia delle dichiarazioni da parte di Google circa l'eliminazione del supporto ai cookie di terze parti a partire dal 2022. Ad ogni modo, leggendo le caratteristiche dei servizi dei fornitori di advertising e di soggetti intermediari, si nota come il *fingerprinting* sia una scelta alternativa ai cookie, valida ed ormai ben collaudata. Non da ultimo le novità relative alle Progressive Web Application (PWA), introdotte da Google per dotare gli sviluppatori di un sistema unificato di sviluppo web, fruibile da browser e da app smartphone, portano con sé nativamente funzionalità di *fingerprinting*, secondo una logica diversa da quelle presentate finora, ovvero mediante la personalizzazione dello start_url con un ID univoco per utente associato.

Come noto, il problema principale non consiste tanto nell'utilizzo di queste tecniche, quanto nella trasparenza che i soggetti non applicano nelle loro policy e dei loro sistemi di data analysis.

Richiamandoci a quanto espresso anche dal WP art. 29 nell'Opinion 9/2014 proponiamo, pertanto, di integrare le Linee guida con l'esplicito riferimento a questo tipo di tracciamento, prevedendo che il titolare debba dichiararne l'uso e le finalità, dando modo agli interessati di sottrarsi al trattamento quando questo sia per finalità di marketing e profilazione. Laddove, infatti, lo scopo del rilevamento delle "impronte digitali" sia il tracciamento delle persone, ciò costituirà un "trattamento dei dati personali" e sarà coperto dalle normative vigenti in materia. Suggeriamo, in particolare, di valutare il mercato ancora "non adeguatamente regolamentato" degli annunci online alla stregua di una "borsa merci" e dunque da interpretare in base agli stessi meccanismi regolatori e principi di trasparenza dei mercati finanziari.

Sosteniamo l'indicazione dell'Autorità per la *quale "analogamente ai cookie, gli altri strumenti di tracciamento possono essere catalogati secondo una serie di criteri diversi, dei quali il principale resta, tuttavia, la finalità con la quale vengono utilizzati: tecnica o di natura commerciale".*

Si suggerisce, pertanto, che il contenuto minimo delle informazioni da rendere all'interessato, da declinare in ottica Legal Design come sopra argomentato, debba riguardare un nucleo minimo composto da:

- indicazione di tutte le informazioni che sono in grado di raccogliere;
- lo scopo e la base giuridica delle operazioni di lettura delle informazioni;
- informazioni significative sulla logica coinvolta nel processo di profilazione (sul punto siamo consapevoli che c'è un'enorme differenza tra fornire al consumatore gli algoritmi completi che svolgono le attività di profilazione, o all'estremo opposto semplicemente dire al consumatore che tali algoritmi esistono). A tal riguardo ci riportiamo anche al contributo del Gruppo di lavoro articolo 29, "Linee guida sul processo decisionale automatizzato delle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679 dove viene chiarito che, sebbene "non vi sia alcun obbligo per i titolari e/o responsabili del trattamento di fornire "una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo", tuttavia la complessità non è di per sé una scusa per non fornire informazioni significative;
- le specifiche modalità previste per accettare o rifiutare i traccianti;
- le conseguenze del conseguente rifiuto o dell'accettazione;
- le procedure per esercitare i diritti di cui agli artt. 15 e seguenti del RGPD.

Si ritiene, altresì, opportuno che vengano riportati nelle Linee guida degli esempi di utilizzo e funzionamento del *fingerprinting* che, sfruttando le tecniche del Legal Design e dello *storytelling*, permettano agli operatori di orientarsi sull'individuazione della specifica base di legittimità.

LA PROPOSTA n.5

- Con riferimento all'esercizio dei diritti il Garante segnala che *"mentre nel caso dei cookie se l'utente non intende essere profilato, oltre ovviamente a poter rifiutare il proprio consenso, o a ricorrere alle tutele di carattere giuridico connesse all'esercizio dei diritti di cui al Regolamento, ha anche la possibilità pratica di rimuovere direttamente i cookie, in quanto archiviati all'interno del proprio dispositivo, nel caso del fingerprinting questo non è possibile. L'utente*

non dispone di strumenti autonomamente azionabili, dovendo necessariamente far ricorso all'azione del titolare. Ciò in quanto quest'ultimo fa uso di una tecnica di accesso che non presuppone l'archiviazione di informazioni all'interno del dispositivo dell'utente, bensì la mera lettura delle configurazioni che lo contraddistinguono rendendolo identificabile. L'esito si sostanzia in un "profilo" che resta nella sola disponibilità del titolare, cui l'interessato non ha, ovviamente, alcun accesso libero e diretto." Per tali ragioni, proponiamo che la versione definitiva delle Linee guida contribuisca attraverso esempi e precise definizioni a far luce e ad agevolare l'utente nella comprensione dell'esercizio dei propri diritti: dall'accesso ai suoi dati, alla portabilità fino ad ottenerne - per quanto possibile - la cancellazione. Ovvero i "nuovi diritti" legati alle sfide che, la rapidità dell'evoluzione tecnologica e lo sviluppo della globalizzazione, comportano per la protezione dei dati personali (Considerando 6).

Ci permettiamo di far osservare a Codesta Autorità quanto difficoltoso sia per l'interessato comprendere le reali dinamiche del trattamento dei dati, per via della mancanza di informazioni che agevolino il corretto esercizio dei diritti; spesso è addirittura difficilmente decifrabile quale sia il corretto titolare del trattamento a cui inviare la richiesta. Pertanto è da parte nostra forte l'auspicio che le Linee guida contribuiscano, con esempi concreti (magari ispirati alle piattaforme di uso più comune), a rendere maggiormente comprensibile la terminologia talora poco amichevole o eccessivamente astratta presente nel GDPR e nelle altre normative coinvolte (e-privacy).

E' illuminante in tal senso la ricerca **Automated Experiments on Ad Privacy Settings** di cui sono autrici Amit Datta, Michael Carl Tschant e Anupam Datta che ha dimostrato come i profili comportamentali siano molto più ampi e dettagliati di quanto mostrato all'utente quando esercita il suo diritto di accesso. Tali risultati unitamente ad altri autorevoli studi potranno senz'altro costituire il punto di partenza per indagini più approfondite da parte delle società stesse o degli organismi di regolamentazione e delle Autorità.

LA PROPOSTA n.6

- Vorremmo richiamare l'attenzione del Garante Privacy su un tema inerente le forme di tracciamento che risulta ancora non completamente chiaro agli operatori e per il quale si auspica un intervento esplicativo del Garante stesso: facciamo riferimento al tema dei metadati che possono essere generati dalle agenzie pubblicitarie che installano i propri cookie e si servono di altri traccianti di profilazione su più siti internet, appartenenti ad editori diversi, quindi a titolari diversi. Suggeriamo di interpretare il mercato ancora "non adeguatamente regolamentato" degli annunci online alla stregua di una "borsa merci" e dunque di compierne una prima ricognizione giuridica alla luce degli stessi principi regolatori dei mercati finanziari: fiducia, correttezza e trasparenza nell'interesse degli utenti e per l'integrità dei trattamenti.

Con riferimento al tema dei metadati che possono essere generati dalle agenzie pubblicitarie nel contesto del settore del *programmatic advertising*, vi sono alcuni punti da analizzare che potranno fungere da spunti di riflessione ed orientamento per la redazione finale delle Linee Guida:

il mercato ad oggi "non regolamentato" degli annunci online si comporta come una "borsa merci", un mercato dei commercio elettronico brillantemente descritto da Dina Srinivasan, Fellow del Thurman Arnold Project a Yale, già autrice di " The Antitrust Case Against Facebook ", in cui si rincorrono sotto la supervisione e direzione degli intermediari digitali, miliardi di transazioni, quotazioni in tempo reale, scambi di annunci, analisi, andamenti e dati aggiornati. Editori che vendono spazio pubblicitario e inserzionisti che lo acquistano. Tutto in un processo automatizzato chiamato "offerta in tempo reale" al momento però privo di adeguata regolamentazione.

Un meccanismo, dunque, per certi aspetti paragonabile alle dinamiche dei mercati finanziari, in cui in particolare Google, attraverso la propria "Rete Display" e il programma basato su connessioni da server a server, denominato Open Bidding (precedentemente noto come Exchange Bidding), riveste un ruolo cruciale, consentendo di invitare piattaforme di scambio di terze parti a competere in tempo reale per poi sfruttare la tecnologia di DoubleClick for Publishers e Ad Exchange (AdX) nell'allocazione dinamica dei contenuti e nelle offerte di intestazione (asta

di annunci in tempo reale). Gli inserzionisti in tal modo sono messi in condizione di raggiungere gli utenti su centinaia di migliaia di siti web e app in tutte le categorie di publisher: dai siti più grandi e famosi a siti e segmenti di nicchia.

Ne consegue una sorta di clusterizzazione in cui un vasto pubblico "chirurgicamente profilato" viene orientato e interessato in corrispondenza di contenuti correlati su migliaia di siti.

Ora, come noto all'Autorità, le agenzie pubblicitarie riescono a generare nuove informazioni (metadati) da un'attività esclusiva di interpolazione delle informazioni provenienti dai vari siti. Queste informazioni "di nuova generazione" sono nella loro disponibilità ma non vengono condivise con i titolari dei siti su cui sono ospitati i cookies dell'agenzia pubblicitaria. L'interessato, tanto meno, ha percezione di questo processo.

Questa questione, evidentemente molto delicata, rappresenta solo la punta dell'iceberg, in quanto le attività di microtargeting svolte dalle agenzie di pubblicità entrano nel profondo della profilazione dei gusti di coloro che navigano i vari siti internet e, spesso, i dati raccolti alimentano potenti sistemi di CRM.

Si ritiene, pertanto, che sia fondamentale dare un chiarimento da parte dell'Autorità Garante su questo tema e si propongono alcuni spunti di riflessione e/o soluzioni praticabili:

- favorire la granularità del consenso per le attività di profilazione da parte del titolare (es. editore) e per la profilazione da parte di terzi (es. l'agenzia pubblicitaria).
- ove pertinente, favorire la comprensione chiara ed esauriente dei meccanismi di data analysis e inferenza a cui saranno sottoposte le informazioni
- sulla scia delle recenti Linee guida n. 7 del 2020 dell'EDPB, promuovere la corretta individuazione dell'"organigramma dei responsabili coinvolti nei trattamenti" da cui deriveranno i metadati creati dall'interpolazione delle informazioni; questo anche per favorire il corretto esercizio dei diritti dell'interessato.

LE CONCLUSIONI SUL FINGERPRINTING

- Sebbene il RGPD sostenga e promuova la valorizzazione del principio di trasparenza e correttezza anche informativa, una parte sostanziale della suddetta

responsabilità si riversa ancora una volta sugli stessi interessati ponendo a carico di questi ultimi l'onere di agire in tal senso. Allo stato attuale non si ha motivo di credere che relativamente a certe forme di tracciamento possa essere garantita una trasparenza che, de facto, risulta ancora impossibile per l'utente. Siamo, tuttavia, certi che l'Autorità possa efficacemente contribuire, con tali Linee Guida, prevedendo indicazioni e risposte chiare in grado di limitare le ambiguità sulle questioni più spinose, tra cui sicuramente quella della profilazione ad opera di forme di tracciamento silenti e passive.

Sebbene il RGPD sostenga e promuova la valorizzazione del principio di trasparenza e correttezza anche informativa, una parte sostanziale della suddetta responsabilità si riversa ancora una volta sugli stessi interessati ponendo a carico di questi ultimi l'onere di agire in tal senso.

Un tale livello di investimento, oltre a non essere giuridicamente sostenibile, non appare neppure realisticamente credibile, stanti le evidenti, quanto al momento ineludibili, asimmetrie informative che inficiano la corretta realizzazione della relazione tra utenti e operatori digitali.

Allo stato attuale, dunque, non si ha motivo di credere che relativamente a certe forme di tracciamento possa essere garantita una trasparenza che, de facto, risulta impossibile per l'utente.

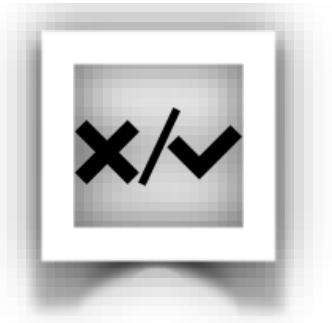
A tal fine EDPB, EDPS (cha ha recentemente pubblicato il TechDispatch 3/2020 sui Sistemi di gestione delle informazioni personali- PIMS) e le altre Autorità di controllo potranno comunque sin d'ora adottare tutti gli ulteriori orientamenti pratici che possano fornire risposte chiare in grado di limitare le ambiguità sulle questioni più spinose relative all'applicazione del Regolamento generale sulla protezione dei dati, tra cui sicuramente quella della profilazione ad opera di forme di tracciamento silenti e passive. Allo stesso modo saranno utili gli orientamenti della giurisprudenza della Corte di giustizia, e le consultazioni, compresa la presente , tese a sviluppare strumenti pratici e a dare risalto alle *best practice*.

Confidiamo, cionondimeno, in una prossima tempestiva opera di aggiornamento delle normative in essere a cominciare dall'adeguamento del RGPD (malgrado al riesame di maggio, dopo due anni di cambiamenti globali, la Commissione ha deciso che fino al 2024 il Regolamento non sarà rivisto) e delle regole alla base delle comunicazioni elettroniche così come delle normative a guida

dei modelli tipici dei mercati noti come *"Two sided market"*, dominio dei grandi intermediari digitali. Su tanto avremo modo di testare anche le previsioni contenute nel pacchetto *"Digital Services Act"* presentato dalla Commissione nel mese di dicembre 2020.

OSSERVAZIONI sulle modalità per la corretta individuazione delle basi di legittimità e l acquisizione del consenso

Scrolling e cookie wall



Abstract*:* Dall'adozione del Regolamento generale sulla protezione dei dati (RGPD) nel maggio 2018, la maggior parte dei siti *web* in Europa visualizza avvisi di consenso sui *cookie*. La sfida che oggi siamo chiamati a risolvere è quella di riuscire a cogliere sapientemente le difficoltà riscontrate dall'utente quando si approccia e utilizza un sito *internet* (al quale può accedere attraverso strumenti diversi, dal *pc* al *tablet*, al cellulare, etc.) bilanciandole con gli interessi dell'operatore digitale. Un bilanciamento delicato che tiene conto del fatto per cui come ogni utente ha una propria identità in quanto "persona fisica": minore, anziano, con problemi di salute, con un buon livello di istruzione o con pochissima istruzione e cultura digitale, ma soprattutto nella maggior parte dei casi un utente anche "consumatore". In tutto ciò i cookie wall e le interfacce delle richieste di consenso mediante azioni di "scroll down", rappresentano una vera e propria insidia poiché tendono ad eludere la libertà di scelta dell'utente e di fatto svuotano di significato l'intero impianto normativo del consenso.

Autori: Luisa Tucci, Germana Maraffa, Karin Malaspina, Maria Antonietta Iacobelli, Eugenia Lopresti, Alessandra Lucchini, con il contributo di Barbara Calderini e Pietro Calorio

LA PROPOSTA n.7

- "*Lo scrolling può essere una componente di un più articolato processo che consenta comunque all'utente di segnalare al titolare del sito, con la generazione di un preciso pattern, una scelta inequivoca nel senso di prestare il proprio consenso all'uso dei cookie*". Suggeriamo un ripensamento dell'Autorità su tale punto, sulla base del fatto per cui, alla luce delle prassi in essere, lo "scroll", in alcun modo può essere ritenuto aprioristicamente un "atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento". La vasta gamma di banner attualmente presenti nei siti online presta evidentemente il fianco ad inopportune attività di scroll al solo fine di procedere agevolmente nella navigazione. Altrettanto riteniamo fuorviante e scorretta la pratica rappresentata dai cosiddetti cookie wall, il noto meccanismo di "take it or leave it". Sosteniamo, quindi, convintamente la posizione dell'Autorità conforme anche alle Linee guida 5/2020 dei Garanti europei relativamente al riconoscimento dell'incompatibilità con il RGPD dei cd. "cookie wall" e parimenti dell'invalidità di consensi "privacy" espressi per mero scroll o *swipe*. Proponiamo, inoltre, che i titolari del trattamento debbano rendere trasparenti i criteri utilizzati in caso di raccolta consenso con tecniche di web dinamico, così da conoscere i criteri di valutazione ed interpretazione dei consensi validamente prestati ed evitare che il colore possa rappresentare un discrimine per illegittimità o meno del consenso in quanto potenzialmente pregiudizievole per alcune categorie di utenti.

I cookie wall rappresentano una vera e propria insidia poiché tendono, non solo ad eludere la libertà di scelta dell'utente, ma anche a svilire e svuotare di valore oltre che di significato l'intero impianto normativo del consenso.

Se, inoltre, fino ad oggi, il consenso per l'accettazione dei cookie sui siti internet è avvenuto spesso, sulla base del semplice scrolling della pagina che l'utente sta visualizzando, ciò non significa che possa costituire la manifestazione di un valido consenso, espressione del diritto di autodeterminazione informativa. E, in modo particolare, manifestazione del potere di controllo dell'interessato, riconosciuto in modo espresso anche dall'art 8, par.2 della Carta dell'UE.

Così anche Enrico Pelino[4], esperto in diritto delle nuove tecnologie e protezione dei dati personali, "*bisogna astenersi da frasi del tipo: Continuando la navigazione o scorrendo la pagina accetti i cookie e similari. La ragione? Il consenso deve essere inequivocabile, ossia non ambiguo. Anche qui la principale disposizione di riferimento è l'art. 4.11) RGPD e, in collegamento ad essa, l'art. 7".*

Se da una parte condividiamo la posizione del Garante (aderente anche con il provvedimento del 2014 e i "*Chiarimenti in merito all'attuazione della normativa in materia di cookie*" del 5 giugno 2015) che, conformemente all'EDPB ritiene che "*il semplice scrolling non sarebbe mai idoneo, 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 equivarrebbe consenso "in nessuna circostanza""*; dall'altra non siamo concordi con la posizione espressa nelle Linee guida per cui: "*Lo scrolling, tuttavia, può essere una componente di un più articolato processo che consenta comunque all'utente di segnalare al titolare del sito, con la generazione di un preciso pattern, una scelta inequivoca nel senso di prestare il proprio consenso all'uso dei cookie."* Ciò in quanto il mero scroll, o uno *swipe*, possono essere gesti del tutto casuali, oppure essere volti a percorrere la "via più breve" (continuare la navigazione) e non anche necessariamente l'intenzione di acconsentire positivamente ai trattamenti di dati permessi dall'utilizzo dei cookie.

[4] Enrico Pelino nel suo articolo "Cookie wall e consenso per scroll/swipe: il chiarimento dei Garanti europei - Riskmanagement (riskmanagement360.it)"

Lo scrolling è, infatti, un'azione che l'utente compie innumerevoli volte per diverse finalità durante la navigazione e in alcun modo può essere ritenuta aprioristicamente un "atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento". Seppure le soluzioni tecniche per tracciare il comportamento dell'utente (scrolling) esistano, l'utente non può automaticamente avere la corretta percezione del fatto che sta compiendo un'azione di accettazione. Lo scroll può essere involontario (tipicamente si scende nella pagina verso la parte che ci interessa scrollando verso il basso). A tal riguardo, l'EDPB è stato chiaro nell'indicare inidoneo lo scrolling o *swiping* a soddisfare il requisito di chiara azione positiva "*under any circumstances*":

- *Punto 40 -Esempio 6 bis: "Un fornitore di un sito web predispone uno script che blocca la visualizzazione del contenuto e fa apparire solo la richiesta di accettare i cookie, le informazioni sui cookie che verranno installati e le finalità per le quali i dati saranno trattati. Non è possibile accedere al contenuto senza cliccare sul pulsante "Accetto i cookie". Poiché all'interessato non è offerta una scelta effettiva, il suo consenso non è espresso liberamente".*
- *Punto 86 -Esempio 16: "In base al Considerando 32, 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".*

Sarebbe inoltre altamente improbabile (se non impossibile) pensare di impostare ed indicare una modalità analoga allo scrolling o *swiping* per revocare la medesima manifestazione di consenso. E' evidente come la vasta gamma di banner attualmente presenti nei siti *on line* presti il fianco ad inopportune attività di scroll al solo fine di procedere agevolmente nella navigazione.

Come garantire, dunque, che i cookie banner prevedano tutti i requisiti di validità della pertinente base giuridica? In questo caso, il consenso, inteso quale atto unilaterale recettizio informato, libero, specifico, inequivocabile ed espresso? Premessa l'autonomia dei titolari del trattamento

nel valutare le migliori misure da adottare per assicurare la conformità alle disposizioni di legge, crediamo che possa costituire un valido supporto in tal senso proprio la predisposizione di framework normativi e progettuali condivisi, sviluppati e testati in chiave di Legal Design, sulla scorta delle precedenti considerazioni alle quali si rimanda.

Con riferimento alla proposta enunciata dal Garante, ovverosia segnalare azioni positive ed inequivocabili dell'utente attraverso cambiamenti di stato di specifiche aree, quali cambiamenti di colore, si ritiene che tale procedura possa trarre in inganno la maggior parte degli utenti qualora i suddetti cambiamenti di colore siano minimi e/o comunque impercettibili ingenerando confusione nel pubblico degli utenti. Probabilmente il rischio più alto sarebbe proprio quello di creare confusione nell'utente, o addirittura delle forme di discriminazione, ad esempio in utenti minorenni, meno abituati a soffermarsi su tali aspetti durante la loro navigazione. Ancora, nel caso in cui si decida di avvalersi di cambiamenti di colore, si potrebbero avere problemi non trascurabili negli utenti affetti da daltonismo o affetti da gravi patologie visive. In queste situazioni dovrebbero essere individuate soluzioni ad hoc di facile comprensione per l'interessato, altrimenti tali soggetti non sarebbero neppure potenzialmente in grado di percepire il cambiamento di colore della pagina o comunque di interpretarlo correttamente.

Posto che per quanto concerne i cookie di profilazione e i cookie analitici di terze parti non anonimizzati (e quindi potenzialmente profilanti) e non indispensabili alla navigazione del sito, il titolare debba necessariamente prevedere un sistema che sia in grado di "bloccare" questi cookie ai fini all'espressione attiva e consapevole di consenso, allora le soluzioni da privilegiare saranno quelle in grado di mettere in risalto la funzione svolta dal banner cookie che è sia informativa che di controllo del "*cookie consent*": ovvero un momento di discontinuità nella navigazione in grado di dare origine ad un'azione positiva che il titolare dovrà tracciare e documentare. Ovviamente a seconda che l'utente sia autenticato o meno e, dunque, non provvisto di account, la manifestazione del consenso o del dissenso dovrà essere strutturata affinché sia riconducibile al solo dispositivo di riferimento o piuttosto ad una serie di ulteriori *device* di pertinenza.

La conformità ed il rispetto dei principi espressi dalla normativa di protezione dei dati personali richiede che il proprietario del sito non debba scaricare alcun cookie potenzialmente profilante,

come anche impedire la medesima azione a oggetti e codici di terze parti (es. *widget social*) fino alla necessaria manifestazione di consenso.

Ci preme evidenziare come con la pratica del cookie wall vengano infranti non solo i tre principi cardine (liceità, correttezza e trasparenza) della normativa vigente, ma innanzitutto viene ad essere compromessa la condizione di libertà del consenso (art. 7.4 del RGPD).

Proprio con riferimento alla manifestazione del consenso, la Corte di Giustizia nella causa nota come Planet49[5] ha ribadito che è necessario un comportamento attivo da parte dell'utente affinché il consenso venga considerato validamente prestato e ha statuito, altresì, che informazioni archiviate nel dispositivo dell'utente fanno parte della sfera privata di quest'ultimo e che in quanto tale deve essere tutelata in virtù del diritto fondamentale al rispetto della vita privata di ciascuno. La Corte prosegue, inoltre, affermando che è del tutto irrilevante il fatto che le informazioni archiviate o consultate costituiscano o meno dati personali. Ciò in quanto, il diritto dell'Unione Europea tutela l'individuo da qualsiasi ingerenza nella sua vita privata, in particolare "*dal rischio che identificatori occulti o altri dispositivi analoghi si introducano nel dispositivo terminale dell'utente a sua insaputa*".
Ribadiamo, quindi, la necessità che ogni banner debba prevedere un'interfaccia "*Cookie Consent Management*" in grado di offrire agli utenti la possibilità di scegliere quali cookie (ulteriori) si intenda installare e soprattutto permetta agli utenti di modificare le proprie scelte in qualsiasi momento, revocando in modo facile il consenso prestato anche successivamente.
Del resto, appare evidente come lo stesso concetto di *accountability* richieda che il soggetto da tutelare sia l'utente e/o fruitore di servizi elettronici. Ogni onere e/o adempimento probatorio sull'adozione o meno delle misure atte a consentire una libera manifestazione di consenso ricade in capo all'attore principale, ovvero il titolare del trattamento. E` innegabile che una reale libertà di esprimere consenso deve potersi tradurre anche nella libertà di negarlo.
Un'efficace manifestazione del consenso, espressa e mai dedotta né deducibile *per facta concludentia*, non può esimersi da una preventiva rappresentazione esauriente dei sistemi di tracciamento dell'accesso ad un sito web.

[5] Corte di Giustizia dell'Unione Europea, Sentenza nella causa C-673/17 sul caso Planet49, punto 70.

Poiché se può prevedersi che l'attività di monitorare e tracciare a fini di marketing e/o promozionali le preferenze e le attitudini di consumo dell'utente possano essere astrattamente lecite, non si può negare come nelle fattispecie concrete, le attività cui viene indotto l'utente / consumatore per poter svolgere navigazione/lettura/consultazione del sito siano pesantemente compromesse attraverso ingerenze continue e ricorrenti, quali i cookie e altre forme di tracciamento.

A tal riguardo vogliamo sottolineare come anche in merito all'attività di *data enrichment* (raccolta di informazioni personali oggetto di trattamento tramite incrocio con i dati relativi all'utilizzo di funzionalità e servizi diversi), menzionata nelle Linee Guida in commento, una certa attenzione debba essere dedicata da parte dell'Autorità alla valutazione della necessità di un consenso aggiuntivo (Considerando 42), ulteriore e specifico per la relativa finalità, peraltro particolarmente invasiva.

Si ritiene inoltre opportuno formulare due ulteriori osservazioni:

- in numerosi casi si è notato che l'esperienza dell'utente su alcuni banner presenta significative differenze a seconda che si navighi su browser per pc e laptop da un lato, e per tablet e smartphone dall'altro: nel secondo caso (specie con i dispositivi meno aggiornati a livello di sistema operativo) si riscontrano sovente dei rallentamenti, che rendono ancor più difficoltoso per l'utente gestire le proprie preferenze. Per questo ci sembra necessario che nelle Linee Guida siano presenti indicazioni per i titolari del trattamento, nel senso di suggerire di verificare in concreto che l'esperienza dell'utente sui banner non presenti apprezzabili differenze a seconda del dispositivo utilizzato dall'utente;

- notevole importanza hanno in questo contesto i fornitori di CMP (le già menzionate *Consent Management Platform*), che debbono considerarsi come responsabili del trattamento[6]. Come tali, peraltro, essi sono soggetti ai principi normativi: in particolare, in

[6] Si elencano qui i principali:
https://cookie-script.com https://www.cookiebot.com/it https://rethinkingprivacy.com https://www.trustarc.com/products/cookie-consent-manager/ https://www.quantcast.com/gdpr/consent-management-solution/ https://www.iubenda.com/it/cookie-solution https://www.cookiepro.com/products/cookie-consent/ https://blog.getadmiral.com/interested-in-admirals-gdpr-consent-management-module https://gdpr.clickio.com https://www.aboutcookies.org https://www.civicuk.com/cookie-control https://cookieinformation.com/: https://www.uniconsent.com/ https://cmp.sirdata.com/

ossequio al principio di "*data protection by design*" sancito dall'art. 25 del RGPD, tali soluzioni dovrebbero implementare sin dalla progettazione meccanismi per integrare nel trattamento le garanzie per gli interessati. Ciò significa che il fornitore della CMP dovrebbe fornire degli avvertimenti al proprio cliente (il gestore del sito, titolare del trattamento) se una configurazione adottata non fosse rispettosa dei principi o, addirittura, impedire radicalmente al cliente ogni impostazione che non rispetti i principi. Ad esempio, qualora il sistema della CMP rilevasse che il titolare del trattamento ha inserito cookie per finalità di marketing pre-marcando il consenso, dovrebbe comparire un "*warning*" che avvisa l'amministratore dell'utenza lato cliente in ordine al fatto che tale impostazione non è permessa dalle norme, e chiede quindi un superamento (*override*) consapevole da parte del titolare del trattamento. L'Autorità potrebbe anche valutare di prescrivere che titolare e responsabile del trattamento, in questo genere di servizi, siano tenuti ad inserire una clausola secondo la quale le parti si impegnano reciprocamente a verificare l'esistenza di meccanismi tecnici idonei alla verifica in ogni tempo del rispetto delle norme in materia, e in particolare di quello di trasparenza, di protezione dei dati fin dalla progettazione e di responsabilizzazione.

Si ritiene molto importante che indicazioni di questo tipo siano presenti all'interno delle Linee Guida, in quanto contribuirebbero all'effettività della tutela dei diritti dell'interessato e ad una maggiore trasparenza nel tracciamento degli utenti online.

Vogliamo evidenziare a corredo delle nostre osservazioni l'interessante studio "*Do cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*" [7] che partendo dall'esame dei banner implementati da *Consent Management Providers* (CMP), che rispettano il *Transparency and Consent Framework* (TCF) di IAB Europe (attualmente nel mirino dell'Autorità di controllo del Belgio che ha avviato una istruttoria in merito a presunte violazioni), hanno analizzato la validità del consenso memorizzato dietro l'interfaccia alla luce sia del RGPD che della Direttiva e-Privacy. I risultati indicano che su

[7] C. Matte, N. Bielova and C. Santos, "Do cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework," 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 791-809, doi: 10.1109/SP40000.2020.00076.

560 siti web, in almeno una sospetta 54% di essi è presente una potenziale violazione di conformità legale.

LA PROPOSTA n.8

- Affinché le Linee guida non abbiano esclusivamente un valore descrittivo e ricognitivo ma anche un peso chiarificatore e facilitatore, si suggerisce che il riferimento a "*l'ipotesi -da verificare caso per caso- nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di cookie*" possa essere ulteriormente precisato a tutela della parte debole. Un elenco esemplificativo e descrittivo del "contenuto" o del "servizio" equivalenti potrebbe rappresentare un primo valido orientamento per gli operatori del mercato.

Condividiamo quanto sostenuto dal Garante in merito ai "servizi equivalenti" e, sulla scia di quanto sostenuto dal Comitato Europeo, nel suo Provvedimento 255/2020 (che ha opportunamente esaminato la prassi scorretta che porta a pensare che l'utente non sia costretto ad accedere ai contenuti di uno specifico sito web, potendo in alternativa scegliere di "cambiare strada" su siti che offrono servizi equipollenti nel libero mercato), siamo d'accordo sul fatto che la disponibilità di un servizio "equivalente" (fungibile) - senza richiesta di consenso - possa costituire la "condizione di equilibrio" che può legittimare un provider di internet a subordinare la prestazione del proprio servizio al consenso; ma che una tale condizione debba tuttavia essere verificata nei singoli casi.

Come abbiamo avuto modo di discutere con il **Prof. Giovanni Crea**, Direttore della Rivista DETEP dell'Istituto Italiano per la Privacy, tenuto conto anche della divergente prospettiva tra la sentenza della Cass. 17278/2018 (per la quale la fungibilità può valere a livello di mercato) e l'EDPB, sulla fungibilità del servizio (che per l'EDPB deve essere lo stesso provider a garantirla), proprio tale condizione di equilibrio si può misurare dal modo in cui l'interessato è messo in condizione di poter liberamente rilasciare il proprio consenso a trattamenti attraverso cookie "non tecnici". Ciò non dovrebbe limitare la libertà del provider di negare il proprio servizio a chi il consenso non voglia prestarlo.

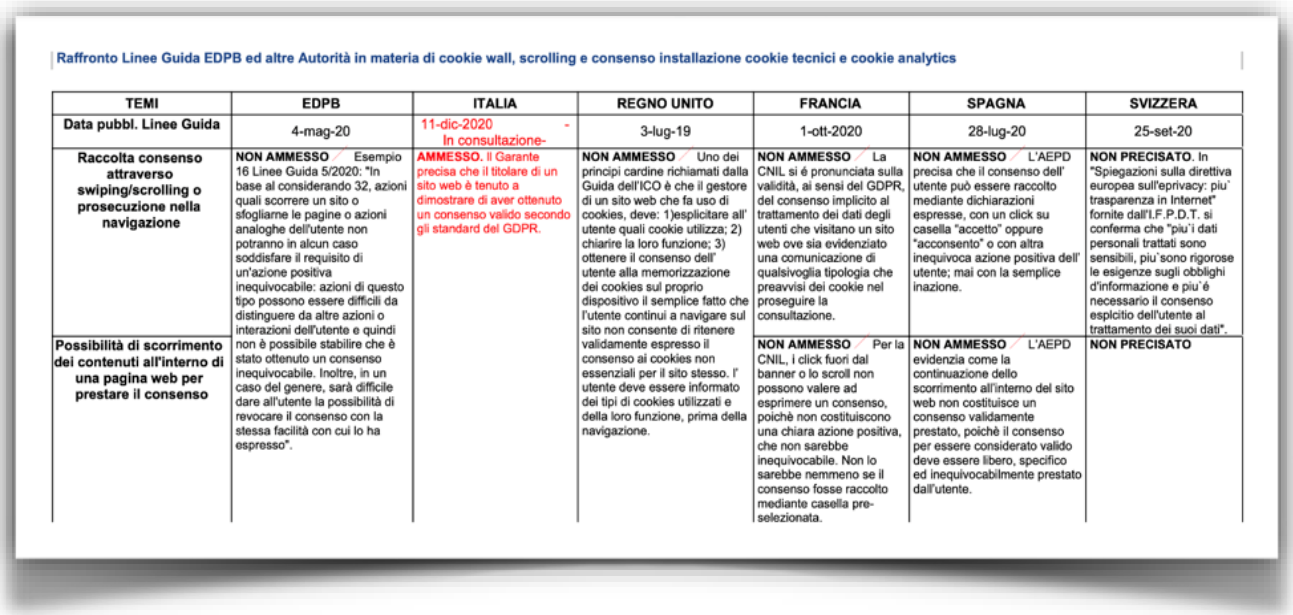
La verifica della fungibilità di un servizio garantisce sia la libertà del consenso sia la libertà di iniziativa economica del provider.

LE POSIZIONI DELLE AUTORITA'

Le Linee guida costituiranno un'ottima opportunità per fare chiarezza e disciplinare in maniera maggiormente uniforme prassi attualmente adottate in materia, anche alla luce del lavoro già svolto da Autorità estere come quella inglese ICO, la spagnola AEPD e la francese CNIL, che hanno già fornito utili indicazioni.

Insieme alla tedesca DSK, anche l'inglese ICO e la francese CNIL ritengono che l'azione degli utenti consistente nel continuare la navigazione di un dato sito non possa essere considerata espressione inequivocabile del consenso per l'installazione dei cookie, che necessitano invece proprio del consenso come loro legittima base giuridica.

La tabella che segue fornisce un confronto delle posizioni assunte dalle varie Autorità europee in ordine ad aspetti fondamentali relativi agli strumenti di tracciamento.



Raffronto Linee Guida EDPB ed altre Autorità in materia di cookie wall, scrolling e consenso installazione cookie tecnici e cookie analytics

TEMI	EDPB	ITALIA	REGNO UNITO	FRANCIA	SPAGNA	SVIZZERA
Data pubbl. Linee Guida	4-mag-20	11-dic-2020 - In consultazione-	3-lug-19	1-ott-2020	28-lug-20	25-set-20
Raccolta consenso attraverso swiping/scrolling o prosecuzione nella navigazione	**NON AMMESSO** Esempio 16 Linee Guida 5/2020: "In base al considerando 32, 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".	**AMMESSO.** Il Garante precisa che il titolare di un sito web è tenuto a dimostrare di aver ottenuto un consenso valido secondo gli standard del GDPR.	**NON AMMESSO** Uno dei principi cardine richiamati dalla Guida dell'ICO è che il gestore di un sito web che fa uso di cookies, deve: 1)esplicitare all' utente quali cookie utilizza; 2) chiarire la loro funzione; 3) ottenere il consenso dell' utente alla memorizzazione dei cookies sul proprio dispositivo il semplice fatto che l'utente continui a navigare sul sito non consente di ritenere validamente espresso il consenso ai cookies non essenziali per il sito stesso. l' utente deve essere informato dei tipi di cookies utilizzati e della loro funzione, prima della navigazione.	**NON AMMESSO** La CNIL si é pronunciata sulla validità, ai sensi del GDPR, del consenso implicito al trattamento dei dati degli utenti che visitano un sito web ove sia evidenziato una comunicazione di qualsivoglia tipologia che preavvisi dei cookie nel proseguire la consultazione.	**NON AMMESSO** L'AEPD precisa che il consenso dell' utente può essere raccolto mediante dichiarazioni espresse, con un click su casella "accetto" oppure "acconsento" o con altra inequivoca azione positiva dell' utente; mai con la semplice inazione.	**NON PRECISATO**. In "Spiegazioni sulla direttiva europea sull'eprivacy: piu` trasparenza in Internet" fornite dall'I.F.P.D.T. si conferma che "piu`i dati personali trattati sono sensibili, piu`sono rigorose le esigenze sugli obblighi d'informazione e piu`é necessario il consenso esplcitio dell'utente al trattamento dei suoi dati".
Possibilità di scorrimento dei contenuti all'interno di una pagina web per prestare il consenso				**NON AMMESSO** Per la CNIL, i click fuori dal banner o lo scroll non possono valere ad esprimere un consenso, poichè non costituiscono una chiara azione positiva, che non sarebbe inequivocabile. Non lo sarebbe nemmeno se il consenso fosse raccolto mediante casella pre-selezionata.	**NON AMMESSO** L'AEPD evidenzia come la continuazione dello scorrimento all'interno del sito web non costituisce un consenso validamente prestato, poichè il consenso per essere considerato valido deve essere libero, specifico ed inequivocabilmente prestato dall'utente.	**NON PRECISATO**

Possibilità di utilizzo cookie wall	**NON AMMESSO** / 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").	**AMMESSO**, ma nelle nuove regole proposte sull'uso dei cookie, il Garante considera illeciti i cookie wall, salvo che il sito web offra all'utente la possibilità di accedere a un contenuto o a un servizio equivalenti senza dover prestare il proprio consenso (da valutare caso per caso).	**NON PRECISATO.** Nessuna chiara dichiarazione esplicita. L'approccio di ICO è più flessibile poichè non esclude categoricamente che il cookie wall possa essere utilizzato, considerando che il GDPR prevede il bilanciamento con altri diritti tra cui la libertà di espressione e la libertà di iniziativa economica.	**NON AMMESSO** / Secondo la CNIL il cosiddetto cookie wall non è compliant al regolamento.	**NON AMMESSSO** / L' AEPD ha sanzionato la compagnia aerea "Vueling Airlines" perché l'utilizzo dei cookie sul sito web di quest' ultima è stato ritenuto contrario ai principi del GDPR. Dall' esame del provvedimento, in particolare, si apprende come l'AEDP abbia considerato illegittima la pratica di non prevedere la possibilità di opporsi all'installazione dei cookie sui vari dispositivi, ritenendo insufficiente prevedere la sola possibilità di negare il consenso all' installazione dei cookie attraverso le opzioni del browser.	**NON PRECISATO**
Possibilità uso checkbox pre-selezionate	**NON AMMESSO** / Punto 79 delle Linee Guida 5/2020 EDPB: "L'uso di caselle di adesione preselezionate non è valido ai sensi del regolamento".	**NON AMMESSO** / Secondo il considerando 32 del Regolamento: "Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle".	**NON AMMESSO** / Secondo l'ICO ogni adesione preselezionata deve ritenersi inefficace ai fini della validità del consenso.	**NON AMMESSO** / Vietato l'utilizzo dei cosiddetti "box pre-spuntati", dato che il silenzio o l'inattività dell' interessato non costituiscono una valida manifestazione del consenso.	**NON PRECISATO.** L' AEPD non ha specificato nulla in merito all'uso di checkbox con pre-flag.	**NON AMMESSO** / Si veda art. 21 Nuova LPD (ut supra).

Necessità del consenso per l'installazione dei Cookies Tecnici	**NON NECESSARIO** Consenso non richiesto per cookie tecnici e analitici se di prima parte. NECESSARIO consenso per i cookie di terza parti e non anonimizzati.	**NON NECESSARIO** Cookie tecnici e i cookie statistici di prima e terza parte (possono essere considerati "cookie tecnici" se rispettano una serie di condizioni: 1) hanno come unico scopo la produzione di statistiche aggregate e il loro uso è limitato a un singolo sito/app 2) se cookie statistici di terza parte, non sono condivisi o comunicati a terzi 3)se cookie statistici di terza parte, non sono combinati con altri dati) non necessitano di un preventivo consenso per essere installati.	**NON NECESSARIO** Qualsiasi cookie sia necessario per l'esecuzione del contratto richiesto dall' utente non necessita di consenso, esattamente come non necessita di consenso il trattamento dei dati personali se ciò avviene, appunto, in esecuzione di un contratto. **NECESSARIO** per qualunque cookie "non essenziale" compresi quelli analitici (assimilabili a cookie tecnici) va fornito un consenso esplicito (no a qualsiasi pre-flag) Gli utenti devono poter avere il controllo sui cookie che vengono serviti al momento della loro visita sulla pagina web.	**NON NECESSARIO** se si tratta di cookie legati strettamente al funzionamento del sito/servizio - **NECESSARIO** se i cookie raccolgono dati anche in concomitanza di altri "tracciatori" consentendo quindi un livello di dettaglio elevato dell'utente.	**NON NECESSARIO** in caso di cookie necessari alla comunicazioni/trasferimento tra device e rete e nel casao forniscano servizi espressamente richiesti dall'utente o che forniscano esclusivamente dati aggregati per scopi statistici purchè vengano fornite informazioni tali sul loro utilizzo da consentire il rifiuto all'installazione	**NON NECESSARIO** se trattasi di cookies esclusivamente legati all' uso di un sito web, l' accesso, la qualità del servizio di un negozio online o i cookies utilizzati per l'analisi del sito web. **NECESSARIO** nel caso si verifichi uno sbilanciamento di interessi sull'uso dei cookies a favore dell'utente (e non del gestore del "sito"), i cookies in questione dovrebbero essere utilizzati solo previo consenso dell' interessato.
Necessità di consenso per i Cookie analytics di prima parte	**NON NECESSARIO**	**NON NECESSARIO** per quelli che rispettano le misure indicate dal Garante. Per quelli che, al contrario, tali misure non le rispettano si pone la questione: non potranno essere in alcun modo utilizzati o, ragionevolmente, fornita l' informativa con le finalità e la specifica tipologia di cookie che si intende utilizzare, potranno essere utilizzati previo consenso?	**NECESSARIO**	**NON NECESSARIO**	**NECESSARIO**	**NON NECESSARIO** se collegati all'uso di un sito web, l'accesso, la qualità del servizio di un negozio online o i cookies utilizzati per l'analisi del sito web. **NECESSARIO** nel caso si verifichi uno sbilanciamento di interessi sull'uso dei cookies a favore dell'utente (e non del gestore del "sito"), i cookies in questione dovrebbero essere utilizzati solo previo consenso dell' interessato (non chiara distinzione fra prima parte e altre).
Necessità di consenso per i Cookie analytics di seconda parte	**NECESSARIO**		**NECESSARIO**	**NECESSARIO** (non è indicato esplicitamente ma si desume).	**NECESSARIO**	

Se da una parte è ormai pacifico - in Italia e in Europa - che **il consenso espresso attraverso il mero** scroll **o** *swipe* **di una pagina** web **o il consenso raccolto con l'utilizzo di un** cookie wall **non siano**

validi, dall'altra riteniamo di fondamentale importanza che tali posizioni non siano soggette a interpretazioni differenti da parte degli operatori del mercato e delle stesse Autorità e si possa in tal modo bilanciare l'interesse "imprenditoriale" con l'interesse del "consumatore".

E' bene ricordare, infatti, che non ogni attività di pubblicità e/o promozione deve ritenersi lesiva per l'utente/consumatore e, di conseguenza, un invito al consumo non può ritenersi di per sé stesso nocivo per l'utente.

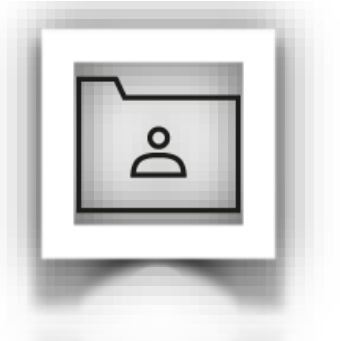
LE CONCLUSIONI SU SCROLLING E COOKIE WALL

- I cookie wall e il consenso tramite scrolling violano le normative vigenti in materia di protezione dei dati. A tale riguardo i poteri e la vigilanza del Garante saranno cruciali.

In conclusione, proprio in ragione del "*far west*" al quale si assiste, giorno dopo giorno, e alla luce di quanto finora esposto, si auspica una sempre più attenta valutazione da parte delle Autorità degli interessi in gioco o, in alternativa, "coinvolti" nel caso di utilizzo della base giuridica del consenso - laddove la stessa sia correttamente individuata (cookie e altre forme di tracciamento di marketing e profilazione) - poiché sussiste il concreto rischio che la tutela della sicurezza dei trattamenti di dati personali possa essere rimessa alle mere scelte del singolo quando non addirittura dettate dal mercato. I poteri e la vigilanza del Garante saranno cruciali, per garantire il rispetto del principio di finalità e correttezza e per garantire il corretto esercizio dei diritti degli interessati.

E affinché le Linee guida non risultino "subito superate", avendo ad oggetto un argomento che necessariamente deve "andare al passo con la tecnologia", si suggerisce alla Autorità di prevedere delle sessioni di aggiornamento delle stesse, soprattutto in termini di esemplificazioni ivi contenute, a distanza ragionevole le une dalle altre.

Anonimizzazione e pseudonimizzazione. I cookie analytics



Abstract: La presente sezione del documento ha l'obiettivo di illustrare la funzionalità dei *cookie analytics* di prima o terza parte, nonché la natura di "necessarietà", o meno, che questi rivestono nell'interazione dell'Utente/Interessato con il sito *web* oggetto di accesso. Tali sistemi di tracciamento condizionano in maniera significativa i presupposti di efficacia della manifestazione di consenso che precorre/precede, o così` dovrebbe, l'attività di indicizzazione dei dati.

Autori: Gianmarco Cenci, Salvatore Coppola, Karin Malaspina, Leonardo Scalera con il contributo di Maria Grazia Romano e Floriana Tagliaferro

LA PROPOSTA n.9

- In un'ottica di certezza del diritto e trasparenza, si formulano alcune istanze all'Autorità Garante:
  - ✓ porre in disamina l'esenzione dei cookie analytics dalla richiesta di consenso prodromico alla loro installazione, alla luce della loro non inclusione ai sensi del WP29 - Opinion 4/2012, tra i tracciatori che non necessitano di previo assenso all'indicizzazione dei dati trattati;
  - ✓ qualora, alla luce dell'attuale indirizzo del Garante e della proposta di Regolamento e-Privacy (Considerando 21 ed art 8), si ritenga di consolidare l'orientamento secondo cui è legittima l'installazione di cookies analytics senza il consenso degli interessati, siano adottate misure tecniche ed organizzative che garantiscano un utilizzo dei dati degli interessati unicamente per le finalità

statistiche ritenute legittime, escludendo la legittimità di elaborazioni ed arricchimento dei dati che possano tracciare gli interessati;

- ✓ fornire indicazioni puntuali sulle modalità di impiego dei cookie analytics che non rispettino i parametri cristallizzati dall'Autorità Garante, chiarendo se tali cookie non possano essere utilizzati affatto o se, fornita adeguata informativa, possano essere subordinati al previo consenso dell'Interessato.

I cookie analytics sono quei particolari cookie necessari ad esempio a generare report inerenti l'efficacia di un sito e/o il traffico generato.

Tali tracciatori informatici possono essere di prima parte se installati direttamente dal titolare del trattamento e gestore del sito visitato, oppure di terze parti qualora facciano riferimento ad altri siti diversi da quello visitato.

Il Garante sin dal 2014 ha ritenuto di assimilare, a determinate condizioni, questa tipologia di cookie ai cosiddetti cookie tecnici che possono legittimamente essere installati senza consenso dell'interessato[8], secondo le prescrizioni fornite dall'Autorità.

Possiamo individuare i cookie tecnici secondo il Parere 04/2012 del WP29[9], in base a due criteri fondamentali inerenti la funzionalità dei medesimi: a) il tracciatore è installato "al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica" oppure b) il cookie è "strettamente necessario al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio".
In tale ambito il WP29 aveva ritenuto che i cookie analytics non rispondessero a tali criteri e non li aveva indicati espressamente tra quelli che non richiedessero il consenso dell'interessato per la loro installazione.
In ogni caso, si osservava che "Il Gruppo di lavoro non ritiene probabile tuttavia che i cookie analitici di prima parte generino un rischio per la privacy quando sono strettamente limitati alle

---

[8] Individuazione delle modalità semplificate per l´informativa e l´acquisizione del consenso per l´uso dei cookie - 8 maggio 2014 *(Pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014)* /https://www.garante-Privacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884

[9] Opinion 04/2012 on Cookie Consent Exemption Adopted on 7 June 2012 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pd f pag. 11

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

A tale riguardo, qualora l'articolo 5, paragrafo 3, della direttiva 2002/58/CE fosse rivisitato in futuro, il legislatore europeo potrebbe aggiungere a ragion veduta un terzo criterio di esenzione dal consenso per i cookie strettamente limitati a finalità statistiche aggregate e anonime di prima parte.

L'analitica di prima parte dovrebbe essere nettamente distinta da quella di terzi, che utilizza un cookie di terzi comune per raccogliere informazioni sulla navigazione connesse agli utenti su siti web distinti e che pongono un rischio decisamente superiore per la riservatezza.".

Dunque, da un lato si indicava che i cookie analytics non erano in grado di soddisfare i criteri inerenti la loro necessaria installazione similmente ai cookie tecnici, dall'altro sembrava "profilarsi" uno spiraglio alla loro utilizzazione considerando che il loro utilizzo per finalità statistiche non comportasse un particolare rischio per la privacy degli interessati.

Pur non essendo espressamente indicato né dal WP29 né dal Garante, la liceità dell'installazione dei cookie tecnici avrebbe dovuto trovare base giuridica nell'art. 7 lett. b) della Dir. 95/46/UE e nell'art. 24, lett. b) dell'ora emendato Codice Privacy, mentre l'art. 7 lett. f) della Dir. 95/46/UE e l'art. 24, lett. g) dell'ora emendato Codice Privacy avrebbero potuto costituire la base giuridica per l'installazione dei cosiddetti Analytics.

Infatti, non rientrando questi ultimi nei criteri indicati dal WP29, che richiamano quale base giuridica l'esecuzione di un contratto, l'unica base giuridica che potrebbe escludere la raccolta del consenso per un lecito trattamento dei dati è proprio il legittimo interesse del Titolare.

In tale contesto si sono seguite nel panorama europeo diverse strade.

Il Garante inglese (ICO), nella sua "*Guidance on the use of cookie and similar technologies*", adottata nel 2019 (ante Brexit), ha osservato che: "*Certamente, i cookie analitici non rientrano*

all'interno dell'eccezione dello strettamente necessario"[10]. Dunque, sempre secondo l'Autorità inglese, ciò significa che bisogna informare gli utenti dell'esistenza di questi cookie e ottenere il relativo consenso al loro utilizzo.

Il Garante inglese, peraltro, ne compie una descrizione puntuale: i cookie di analisi vengono utilizzati per consentire ai servizi web di raccogliere informazioni relative l'accesso degli utenti, ad esempio, il numero di visitatori su un sito web, la durata della loro permanenza sul sito e quali parti del sito visitano (attività anche conosciuta come "*web audience measurement*").

L'osservazione più ficcante evidenziata dall'ICO risiede nella circostanza secondo la quale *"sebbene i cookie analytics siano in grado di fornire informazioni utili al gestore del sito"* non rientrano tra le funzionalità richieste dagli utenti nell'utilizzo di un servizio web, tanto che, anche se tali cookie non sono installati, l'utente è comunque in grado di accedere al servizio web. In altre parole, a parere di scrive, viene affermato il concetto secondo il quale lo "strettamente necessario" dovrebbe essere rapportato al punto di vista dell'utente o del contraente, non del gestore del servizio[11].

Muovendo da un'altra angolazione[12], invece, lo "strettamente necessario" andrebbe rapportato alla necessità di utilizzare gli Analytics per l'esecuzione del contratto secondo quanto indicato nelle Linee guida 2/2019 tenendo presente una serie di fattori tra cui i reciproci punti di vista di titolare e interessati.

Ma vi è di più.

Nel distinguere i cookie analytics in due tipi, di prima parte e di terze parti, l'ICO giunge finanche a puntualizzare che il consenso è necessario anche per i cookie analytics di prima parte, nonostante quest'ultimi possano sembrare meno invadenti di altri in grado di tracciare l'utente tra più siti o dispositivi.

Dunque, a parere dell'ICO, è necessario fornire agli utenti informazioni chiare sui cookie analytics e adottare le opportune misure per acquisire il consenso, senza tralasciare di prospettare agli

---

[10] Si tratta di una traduzione non ufficiale di Information Commissioner's Office (ICO), *Guidance on the use of cookies and similar technologies, 2019, pag. 36*

Inoltre v. ICO, *Guide to Privacy and Electronic Communications Regulations,* (v. FAQ) *Are analytics cookies exempt?,* in *https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply15* (consultato il 31/12/2020).

[11] Salvatore Coppola

[12] Gianmarco Cenci

utenti le ragioni per le quali tali cookie sono utili e assicurandosi, allo tempo stesso, di non influenzarli nella scelta delle opzioni.

Nello stesso senso, nel luglio del 2020, anche l'Agencia Española Protection Datos (AEPD) con la sua Guía sobre el uso de las cookie ha stabilito che: *"Respecto al tratamiento de datos recabados a través de las cookie de análisis, el GT29 manifestó que, a pesar de que no están exentas del deber de obtener un consentimiento informado para su uso, es poco probable que representen un riesgo para la privacidad de los usuarios siempre que se trate de cookie de primera parte, que traten datos agregados con una finalidad estrictamente estadística, que se facilite información sobre sus usos y se incluya la posibilidad de que los usuarios manifiesten su negativa sobre su utilización."*[13]

Peraltro sui cookie analytics di prima parte, già nel 2012 il Gruppo di lavoro ex art. 29 (cd. WP29) nel Parere n. 4 aveva stabilito che: "*Benché spesso considerati come uno strumento 'strettamente necessario' per i gestori dei siti web, essi non sono strettamente necessari per offrire la funzionalità esplicitamente richiesta dall'utente (o abbonato). In realtà, l'utente può accedere a tutte le funzionalità offerte dal sito web se tali cookie sono disabilitati. Di conseguenza, tali cookie non ricadono nell'esenzione definita nel CRITERIO A o B."*[14]

Alla luce di tali considerazioni sembrerebbe opportuno che per ritenere legittima l'installazione anche dei cookie analytics si richiedesse il consenso degli interessati visto il tenore letterale dell'art. 122 del Codice Privacy, quantomeno sino all'adozione di una normativa che preveda un ulteriore criterio di esenzione dal consenso per i cookie analytics di prima parte, come auspicato dal WP29 e secondo le attuali proposte in discussione, del Regolamento e-Privacy.

In ordine ai cookie analytics, anche di terze parti, la posizione del Garante italiano è differente come si illustrerà meglio infra e si ritiene sarebbe opportuno intraprendere tutte le iniziative dirette a comporre le opinioni contrastanti anche per il tramite del Comitato europeo per la protezione dei dati.

---

[13] Così Agencia EspañolaProtection Datos, *Guía sobre el uso de las cookies*, Julio 2020, pag. 12. La traduzione italiana (non ufficiale) è*: "Per quanto riguarda il trattamento dei dati raccolti attraverso i cookie di analisi, il WP29 ha dichiarato che, sebbene non siano esenti del dovere di ottenere il consenso segnalato per l'uso, è improbabile che rappresentano un rischio per la privacy di utenti purché siano cookie prima parte, che trattano dati aggregati con uno scopo strettamente statistico, per fornire informazioni sui suoi usi e la possibilità che l'utente esprima il suo rifiuto sul suo utilizzo."*

[14] Parere 04/2012 WP 194: *CRITERIO A: il cookie è utilizzato "al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica". CRITERIO B: il cookie è "strettamente necessari[o] al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio".*

Il Garante Italiano, perseguendo la strada suggerita dallo spiraglio lasciato aperto dalle Linee guida 4/2012, adottava il sopra citato provvedimento del 08.05.2014 ed i successivi Chiarimenti del 05.06.2015[15], che sembrano invece ritenere legittima a determinate condizioni l'installazione degli Analytics.

E' opportuno osservare che prima dell'entrata in vigore del RGPD, l'articolo 24, lettera g), del Codice Privacy prevedeva la liceità di trattamenti di dati per perseguire un legittimo interesse di un titolare o di un terzo solamente nei casi individuati dal Garante, qualora non prevalessero i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.

Dunque, i provvedimenti del Garante sopra citati paiono doversi ritenere un giudizio di bilanciamento tra i legittimi interessi dei titolari ed i diritti e le libertà fondamentali degli interessati, secondo il quale l'installazione dei tracciatori informatici era da ritenersi legittima a determinate condizioni e solamente per alcune finalità.

Nel nuovo contesto normativo e considerato il richiamo operato nelle Linee guida in esame ai precedenti provvedimenti, si ritiene che il Garante abbia sostanzialmente delineato i criteri secondo i quali: i titolari dovranno procedere ad effettuare il cosiddetto *balancing test* tra il loro legittimo interesse ed i diritti degli interessati, prospettando il punto di incontro.

Infatti, viene sostanzialmente indicato dal Garante a quali condizioni il trattamento dei dati degli interessati inerente e conseguente l'installazione dei cookie analytics possa ritenersi legittimamente effettuato in base all'art 6.1 f) del RGPD.

Quest'ultimo, come rilevato nella bozza di nuove Linee guida del Garante, ha comunque introdotto più stringenti criteri per determinare la liceità dell'installazione di tali cookie.

Anche la CNIL (art. 5 Linee Guida) indica i cookie analytics tra i tracciatori che possono essere installati a prescindere dal consenso dell'interessato, effettuando anch'essa, de facto, un test di bilanciamento tra gli interessi di titolari ed i diritti degli interessati[16].

Per la verità, la CNIL sembra quasi effettuare una fuga in avanti ritenendo necessaria l'installazione dei cookie analytics per misurare il traffico su un sito web richiamando la proposta del Regolamento e-Privacy, in particolare il Considerando 21 e l'art 8.1. d) secondo i quali: *"le*

---

[15] Chiarimenti in merito all´attuazione della normativa in materia di *cookie* https://www.garante-Privacy.it/web/guest/home/docweb/-/docweb-display/docweb/4006878

[16] Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) art 5 https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000038783350

eccezioni all'obbligo di ottenere il consenso per avvalersi delle capacità di trattamento e conservazione dell'apparecchiatura terminale o per accedere alle informazioni in essa conservate dovrebbero essere limitate alle situazioni che comportano un'intrusione nella vita privata scarsa o nulla. Nella fattispecie, il consenso non dovrebbe essere richiesto per autorizzare la conservazione tecnica o l'accesso strettamente necessario e proporzionato per l'uso legittimo di consentire l'uso di un servizio specifico espressamente richiesto dall'utente finale. Vi si può includere la conservazione dei marcatori per la durata di un'unica sessione stabilita su un sito web per tenere traccia di quanto inserito dall'utente finale in moduli in linea su diverse pagine. ***I marcatori possono anche costituire uno strumento legittimo e utile, per esempio per misurare il traffico in un sito****. […]"* e *"L'uso delle capacità di trattamento e conservazione dell'apparecchiatura terminale e la raccolta di informazioni dall'apparecchiatura terminale degli utenti finali, comprese informazioni relative ai programmi e i componenti, da parte di una parte diversa dall'utente finale, è proibita, eccetto per i seguenti motivi:* […] *(d) se necessario per misurare il pubblico del web,* ***purché tale misurazione sia effettuata dal fornitore del servizio della società dell'informazione richiesto dall'utente finale****."*

Ad esaustività dell'intervento interpretativo svolto, si osserva che la CNIL prevede alcune cautele da applicare per legittimare il trattamento dei dati.

Ed infatti, tanto la bozza di Linee guida del Garante, quanto le Linee guida della CNIL indicano che in seguito all'entrata in vigore del RGPD si debbano approntare misure di salvaguardia per gli interessati in ottica di privacy by design ex art 25 RGPD.

Inoltre, affinché i cookie possano essere ritenuti esenti da un preventivo consenso per la loro legittima installazione, è evidente che tali misure debbano essere sicuramente maggiori laddove i cookie analytics siano di "terze parti".

Infatti, tali tracciatori implicano in particolar modo rischi maggiori per gli interessati come evidenziato anche dal WP29 nel Parere 4/2012, ut supra.

Il WP29 indicava, tuttavia, quale misura idonea a salvaguardare gli interessati la completa anonimizzazione degli IP per gli analytics di prima parte[17].

[17] *Fra tali tutele dovrebbero rientrare …. meccanismi di completa anonimizzazione applicati alla raccolta di altre informazioni identificabili, come gli indirizzi IP.* Opinion 04/2012 on cookie Consent Exemption Adopted on 7 June 2012 pag. 11.

Diversamente, sia le precedenti indicazioni del Garante che le Linee guida in consultazione indicavano ed indicano, a tutela degli interessati, solo alcune misure di minimizzazione dei dati raccolti.

Infatti si richiede solo il mascheramento di alcuni elementi degli IP, ed esclusivamente allorquando ci si avvalga di terze parti per l'installazione ed elaborazione degli analytics.

Tale misura di salvaguardia è sostanzialmente equivalente a quelle già adottate dalle maggiori società fornitrici di strumenti per la misurazione del traffico[18] di visitatori sui vari siti internet.

L'efficacia di tali misure rimane dubbia. Invero, il semplice mascheramento (la cifratura o la pseudonimizzazione) degli indirizzi IPv4 non sembra idoneo a scongiurare che l'indirizzo IP dell'interessato possa, comunque, essere facilmente reidentificato come evidenziato anche da ENISA[19] .

Ed infatti, nel documento del garante del 05.06.2015 citato, veniva chiaramente prescritto che i titolari adottassero ulteriori cautele di natura contrattuale puntualmente individuate.

Le Linee guida in consultazione, al contrario, non recano un'espressa indicazione inerente la necessità di prevedere clausole contrattuali che vincolino le terze parti a seguire le indicazioni inerenti le ulteriori salvaguardie da aggiungere al mascheramento degli indirizzi IP già indicate nel provvedimento del 2015 quali l'impegno della terza parte o a utilizzarli esclusivamente per la fornitura del servizio, a conservarli separatamente e a non "arricchirli" o a non "incrociarli" con altre informazioni di cui esse dispongano.

Sotto questo aspetto sarebbe auspicabile che laddove vi siano terze parti che gestiscono per conto del Titolare o forniscono servizi inerenti l'elaborazione di statistiche relative, ad esempio, alla frequentazione del sito, venga espressamente previsto che le indicazioni fornite dal Garante divengano vincoli contrattuali da inserire negli accordi ex art. 28 da stipulare tra Titolare e terze parti coinvolte a vario titolo nella gestione del sito del Titolare medesimo.

In tal senso sembra si sia chiaramente espresso il Consiglio d'Europa nell'ultima bozza di proposta di Regolamento e-Privacy e, in maniera meno esplicita nelle indicazioni pubblicate il 1.10.2020, la CNIL[20].

---

[18] https://support.google.com/analytics/answer/2763052?hl=it

[19] Enisa, Pseudonymisation Techniques And Best Practices, November 2019 https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

[20] Cookies et traceurs : comment mettre mon site web en conformité ? https://www.cnil.fr/fr/cookies-et-traceurs-comment-mettre-mon-site-web-en-conformite

In pratica, un'ulteriore misura di salvaguardia degli interessati, potrebbe essere la previsione di un accordo ex art. 28 che estenda espressamente alle terze parti gli obblighi del Titolare imponendo ai Responsabili di usare gli Analytics con le modalità definite dal Garante.

Potrebbero, inoltre, indicarsi i tempi di conservazione dei dati utilizzati per le finalità ritenute legittime dal Garante, similmente a quanto indicato dalla CNIL[21].

Rispetto a tale tema, sarebbe anche auspicabile che venissero individuati dei tempi di conservazione o dei criteri per declinarli in maniera uniforme tra le varie Autorità europee.

A tali misure, il WP29 suggeriva di aggiungere un meccanismo di facile utilizzo che consentisse agli interessati di essere esclusi da qualsiasi raccolta di dati[22].

Allo stato le soluzioni tecniche approntate dai maggiori fornitori di tali servizi [23] non sembrano essere facilmente fruibili dall'utilizzatore medio di internet ed ancor meno da categorie fragili di interessati quali minori e/o anziani.

Si auspica quindi che il Garante voglia tenere conto di tali indicazioni implementando le tutele che consentono di installare i cookie analytics senza il consenso degli interessati, soprattutto ad opera di terze parti.

LE CONCLUSIONI SU ANONIMIZZAZIONE E PSEUDONIMIZZAZIONE PER COOKIE ANALYTICS

- Valutare l'esenzione dei cookie analytics dalla richiesta di consenso per la loro installazione
- Adottare misure tecniche ed organizzative che garantiscano un utilizzo dei dati per le finalità statistiche ritenute legittime
- Fornire indicazioni puntuali circa i cookie analytics che non rispettano le misure indicate dal Garante

Alla stregua delle precedenti considerazioni:

[21] si veda la nota precedente

[22] *Fra tali tutele dovrebbero rientrare un meccanismo di facile utilizzo per scegliere di essere esclusi da qualsiasi raccolta di dati…* . Opinion 04/2012 on cookie Consent Exemption Adopted on 7 June 2012 pag. 11

[23] https://tools.google.com/dlpage/gaoptout?hl=en

a) si ritiene che dovrebbe essere attentamente valutata l'esenzione dei cookie analytics dalla richiesta di consenso per la loro installazione, considerato che il WP29 nella Opinion 4/2012 non include espressamente tale tipologia di tracciatori tra quelli che non richiedono il consenso degli interessati in applicazione dei criteri ivi menzionati e, considerata altresì la posizione di ICO e dell'Autorità spagnola che pure escludono i cookie in questione tra quelli esentati dalla richiesta di consenso;

b) qualora, alla luce dello spiraglio aperto dallo stesso WP29 nella citata Opinion 4/2012, della posizione della CNIL e della proposta di Regolamento e-Privacy (Considerando 21 ed art. 8), si continui a ritenere legittima l'installazione di cookie analytics senza il consenso degli interessati, per l'effetto siano adottate misure tecniche ed organizzative che garantiscano un utilizzo dei dati degli interessati unicamente per le finalità statistiche ritenute legittime;

c) qualora tali tracciatori siano installati tramite "terze parti" si ritiene auspicabile un'implementazione delle ulteriori misure di salvaguardia per gli interessati, sulla scorta di quelle già indicate dal WP29 e dalla CNIL, volte ad impedire che tramite elaborazioni ed incrocio dei dati si possano tracciare gli interessati;

d) sarebbe auspicabile che venissero fornite indicazioni puntuali circa i cookie analytics che non rispettano le misure indicate dal Garante, chiarendo se tali cookie non possano essere in alcun modo utilizzati o se, fornita adeguata informativa agli interessati, possano essere utilizzati previo consenso, come sembrerebbe in linea con le indicazioni delle Linee guida stesse.

Consenso e legittimo interesse

Abstract: A partire dall'estate del 2020, si è diffusa una prassi che consiste nell'utilizzo, da parte di numerosi siti *web*, del legittimo interesse come base giuridica per l'installazione dei *cookie* sul terminale dell'utente e nel suo sviluppo ulteriore, con la richiesta all'utente di "prestare il consenso" al "legittimo interesse" del titolare del trattamento.

Autori: Maria Grazia Romano, Floriana Tagliaferro, con il contributo di Barbara Calderini, Federico Alessandri, Alessandra Etzo

LA PROPOSTA n.10

- Si intende sottoporre all'attenzione dell'Autorità Garante la prassi evidenziata del "consenso dell'interessato al legittimo interesse del titolare", diffusa a partire dall'estate 2020 e per la quale si auspica un intervento di Codesta Autorità al fine di dichiarare "illegittima" tale pratica.

La possibilità di acconsentire o negare l'interesse legittimo da parte dell'interessato, come richiesto nelle opzioni riportate nelle cookie policy di alcuni siti, sembra essere del tutto artificiosa.

Seguendo tale ragionamento è come se si sovrapponessero (!) le basi giuridiche per il medesimo trattamento e per le medesime finalità, avvalorando con il consenso il legittimo interesse del Titolare.

Tale pratica risulta essere ingannevole, creando anche confusione tra le basi giuridiche sulle quali si fondano i relativi trattamenti.

Le basi giuridiche del legittimo interesse e del consenso agiscono distintamente, individuando situazioni giuridiche diverse.

Se il legittimo interesse può essere utilizzato dal titolare per giustificare il trattamento dei dati attraverso lo svolgimento di attività che non siano eccessivamente invasive per l'interessato ed in ragione di esigenze specifiche del titolare, **il consenso rimane la base giuridica legittima rispetto al trattamento per il perseguimento delle finalità di marketing**.

Nella cookie law la base giuridica del "legittimo interesse" non ricorre; il riferimento ad essa – mutuato dal RGPD – viene utilizzato per descrivere le situazioni che beneficiano della predetta deroga (ad esempio, quando è necessario installare cookie tecnici per motivi di protezione del sito web).

A partire dall'estate dello scorso anno, si è diffusa una prassi che consiste nell'utilizzo, da parte di numerosi siti web, del legittimo interesse come base giuridica per l'installazione dei cookie sul terminale dell'utente e nel suo sviluppo ulteriore, con la richiesta all'utente di "prestare il consenso" al "legittimo interesse" del titolare del trattamento.

Il RGPD ha introdotto il concetto di "legittimo interesse" del titolare quale base giuridica su cui valutare la liceità delle operazioni di trattamento di dati personali.

Le basi giuridiche del legittimo interesse e del consenso agiscono distintamente, individuando situazioni giuridiche diverse; l'una (il legittimo interesse) ricorre in presenza di una finalità legittima – per la quale il trattamento è necessario – normalmente non riconducibile ai casi (diversi dal consenso) tratteggiati all'art. 6, par. 1 del RGPD (contratto, obbligo legale, interessi vitali dell'interessato o di un'altra persona fisica, compito di interesse pubblico); l'altra (il consenso) si applica in via residuale rispetto ai casi di 'necessità' di cui al medesimo art. 6, par. 1, compreso il legittimo interesse.

Il quadro normativo europeo che disciplina i trattamenti effettuati attraverso le tecnologie cookie – rappresentato dall'art. 5, par. 3 della direttiva 2002/58/CE, come modificata dalla direttiva 2009/136/CE (c.d. cookie law) – opera alla stregua di una lex specialis rispetto al RGPD, contemplando la base giuridica del consenso all'utilizzo dei cookie ed una deroga a tale base giuridica nel caso di "archiviazione tecnica o accesso, al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente

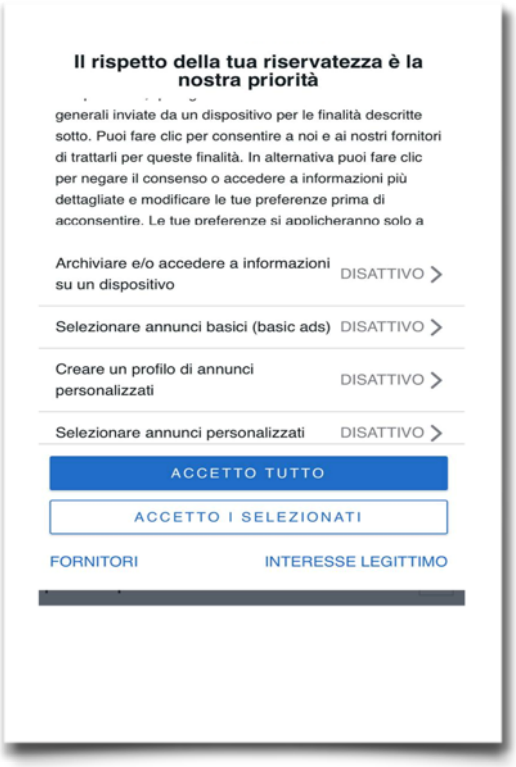
necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio".

Nella cookie law pertanto la base giuridica del "legittimo interesse" non ricorre; il riferimento ad essa – mutuato dal RGPD – viene utilizzato per descrivere le situazioni che beneficiano della predetta deroga (ad esempio, quando è necessario installare cookie tecnici per motivi di protezione del sito web).

Eppure, a partire dall'estate 2020, per accedere a numerosi siti web, sempre più di frequente si assiste ad un nuovo modo di informare dell'esistenza dei cookie.

Accanto al banner con il pulsante "accetta i cookie" vi è spesso un link o un bottone contenente un'espressione che richiama all'interesse legittimo.

Di seguito un esempio, che come è possibile notare, si concretizza nell'"erigere" un cookie wall dopo qualche istante dall'accesso ad un sito web.

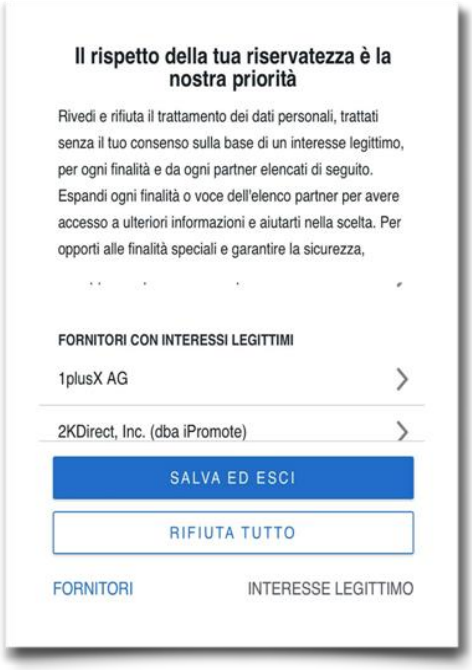


Il cookie wall ormai eretto prevede numerose scelte relative a cookie di profilazione, anche di terze parti. L'utente potrà agevolmente accettare tutto ed accedere immediatamente al sito web, ovvero selezionare (nei casi più virtuosi come nell'esempio sopra riportato) ovvero deselezionare (nei casi meno virtuosi) i cookie, anche di terze parti, che accetta di installare sul proprio terminale.

Si segnala che non sempre, nella ricerca effettuata al fine di ricavare immagini pertinenti per la presente Consultazione, è stato rinvenuto il pulsante "rifiuta tutto", così come nell'esempio riportato di seguito.

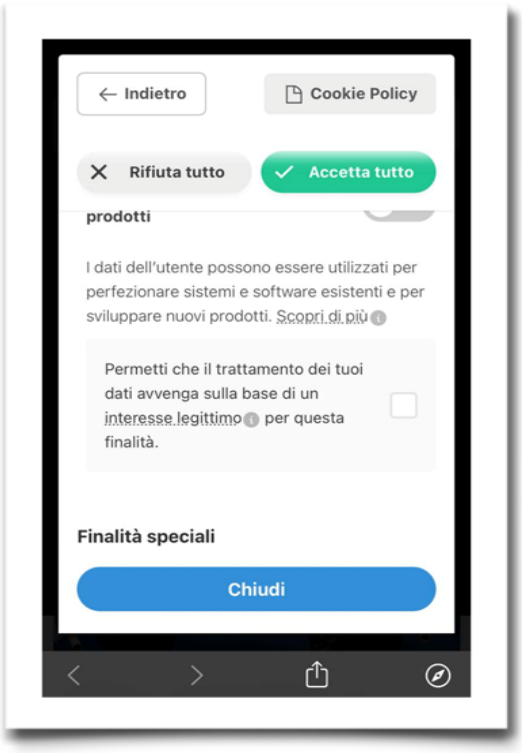
In ogni caso, la pratica che si vuole portare all'attenzione del Garante, è il richiamo e l'utilizzo dell'interesse legittimo, come base giuridica per l'installazione di cookie di profilazione, senza che vi siano informazioni chiare alla base e chiedendo, inoltre, all'interessato di esprimere il proprio "consenso", quasi un'autorizzazione, per l'utilizzo di tale base giuridica.

La pratica descritta risulta essere ingannevole, creando anche confusione tra le basi giuridiche sulle quali si fondano i relativi trattamenti.



Altra pratica riscontrata, forse meno invasiva, ma comunque, a parere di chi scrive, **non corretta**, è una casella da spuntare con l'indicazione "permetti che il trattamento dei tuoi dati avvenga sulla base di un interesse legittimo per questa finalità".

Di seguito un esempio.



La possibilità di acconsentire o negare l'interesse legittimo da parte dell'interessato, come richiesto nelle opzioni riportate nelle cookie policy di alcuni siti, sembra essere del tutto artificiosa per le seguenti motivazioni:

- se la base giuridica del trattamento è l'interesse legittimo, per il quale il Titolare ha ragionevolmente operato un bilanciamento di interessi, risulta difficile comprendere come l'interessato possa apporre ovvero negare il suo consenso rispetto all'interesse legittimo dichiarato dal titolare del trattamento;
- seguendo tale ragionamento è come se si sovrapponessero (!) le basi giuridiche per il medesimo trattamento e per le medesime finalità, avvalorando con il consenso dell'interessato il legittimo interesse del Titolare;
- nella prospettiva del RGPD, l'interessato può opporsi a tale trattamento esercitando il proprio diritto ai sensi dell'art. 21 par. 1 del Regolamento; incombe sul titolare del trattamento la responsabilità di dimostrare (*accountability*) che il suo legittimo interesse prevale sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato;

- difficilmente un utente con una conoscenza media potrà comprendere quanto gli viene richiesto con tale pratica, in violazione del principio di "lealtà" e "trasparenza" nei confronti dell'interessato, due dei principi fondamentali che permeano tutto il RGPD;
- tale pratica non è legittima, anche perché un utente medio difficilmente andrà ad approfondire il legittimo interesse del titolare e tenderà ad accettare tutti i cookie pur di accedere al sito web che gli interessa. Non tutti gli utenti, inoltre, sono disponibili a trascorrere del tempo a selezionare da quali aziende o per quali scopi potrà essere profilato; pertanto tale pratica si pone in palese contrasto con i principi del RGPD e le indicazioni dell'EDPB in ordine al consenso;
- il modello di LIA (per la valutazione del legittimo interesse) elaborato dall'ICO, ad esempio, nella valutazione del bilanciamento, considera l'ipotesi in cui venga consentito o meno un opt-out agli interessati. Ora, pur volendo usare tale modello, l'azione da parte dell'interessato, relativa all'apposizione di un flag rispetto ad una richiesta del titolare circa il proprio legittimo interesse, non pare ricadere in tale ipotesi di opt-out. Ciò che manca è una chiara indicazione circa il bilanciamento degli interessi in gioco: in sostanza tali pratiche peccano di mancanza chiarezza e di lealtà nei confronti dell'utente del sito web.
- fondare poi un trattamento di dati per il quale la giusta base giuridica sarebbe il consenso, sul legittimo interesse, e peraltro artatamente e senza una valutazione concreta dell'interesse sottostante e contrapposto rappresenta una pratica che, a parere di chi scrive, rende illecito lo stesso trattamento. L'art. 6, par. 1, lett. f) del RGPD, che qualifica l'interesse legittimo come una delle basi giuridiche che rende lecito un trattamento, fa riferimento ai Considerando 47 e 50.

  Il Cons. 47 così recita: *"Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto"* e contestualmente esige che si tengano in debito *"conto le ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento*".

  Il Cons. 50 riguarda le finalità diverse rispetto a quelle per le quali i dati sono stati inizialmente raccolti. Le finalità diverse sono consentite solo se compatibili con le finalità iniziali, con riferimento anche alle ragionevoli aspettative degli interessati, in base alla relazione con il titolare con riguardo all'ulteriore utilizzo, della natura dei dati

personali, delle conseguenze dell'ulteriore trattamento previsto per gli interessati, e dell'esistenza di garanzie adeguate sia nel trattamento originale, sia nell'ulteriore trattamento previsto.

Laddove si tratti di cookie di profilazione, anche di terze parti, non appare corretto considerare come base giuridica l'interesse legittimo, alla luce di tale Considerando 50 e ancor di più alla luce dell'art. 22 RGPD: il diritto dell'interessato non deve essere sottoposto a decisioni basate su trattamenti automatizzati, compresa la profilazione, al fine di valutarne le preferenze personali.

Il legittimo interesse può essere utilizzato dal titolare per giustificare il trattamento dei dati attraverso lo svolgimento di attività che non siano eccessivamente invasive per l'interessato ed in ragione di esigenze specifiche del titolare.

Il Legittimo interesse può costituire la base giuridica per l'installazione di cookie tecnici, ma il consenso, a parere di chi scrive, rimane la base giuridica legittima rispetto al trattamento per il perseguimento delle finalità di marketing e quindi per l'installazione di cookie di profilazione.

Alla luce della particolare invasività che Internet e le connesse tecnologie di registrazione dei comportamenti di navigazione possono avere nella sfera privata degli utenti, le normative europea e nazionale prevedono che l'utente debba essere adeguatamente informato sull'uso degli stessi ed esprimere il proprio valido consenso.

Tale consenso, secondo il Considerando 32 del RGPD, "dovrebbe essere espresso mediante un atto positivo inequivocabile" e dovrebbe essere anche un consenso "attivo", come sancito dalla Corte di Giustizia dell'Unione Europea nella sentenza Planet49: *"il consenso che l'Utente di un sito internet deve prestare ai fini dell'installazione e della consultazione di cookie sulla sua apparecchiatura terminale non è validamente espresso mediante una casella di spunta preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso".*[24]

Tra l'altro il tema del consenso è stato affrontato in una sentenza della Cassazione[25] in quanto *la previsione del consenso sia dettata dall'esigenza di rimediare alla intrinseca situazione di*

[24] Corte di Giustizia dell'Unione Europea, Sentenza nella causa C-673/17 sul caso Planet49.
[25] Corte di Cassazione, Sentenza 02.07.2018 n. 17278 nella Causa tra l'Autorità Garante contro AD Spray, con riferimento alle newsletter promozionali.

debolezza dell'interessato, sia sotto il profilo della evidente "asimmetria informativa", sia dal versante della tutela contro possibili tecniche commerciali aggressive o suggestive.

L'evoluzione dell'attività di marketing nella direzione del monitoraggio individuale pone una questione di equilibrio tra il diritto dell'impresa alla libertà di iniziativa economica e il diritto dei consumatori alla riservatezza delle informazioni che descrivono le loro abitudini e preferenze.
In ogni caso, qualora tale trattamento sia effettuato per perseguire uno scopo legittimo del titolare, la condizione che deve essere rispettata è che non siano prevalenti su tale scopo gli interessi o i diritti e le libertà fondamentali dell'interessato (art. 6, 1° comma, lett. f).
L'onere di verificare l'adeguatezza e legittimità di un determinato trattamento - e quindi di identificarne la pertinente base giuridica - ricade sul titolare del trattamento in accordo con il principio di *accountability* (artt. 5 par. 2 e 24 RGPD).
Il RGPD affida proprio al titolare del trattamento il compito di effettuare il bilanciamento di interessi alla base del riconoscimento del legittimo interesse (con la precedente normativa in Italia tale compito era demandato al Garante) a propria discrezionalità; lo stesso dovrà, in ogni caso, anche raccogliere e documentare elementi sufficienti per essere in grado di "dare conto" (cfr. art. 5 par. 2 e art. 24 RGPD) delle proprie scelte. L'applicazione del legittimo interesse presuppone, quindi, la prevalenza in concreto di quest'ultimo sui diritti, libertà e meri interessi degli interessati, cioè dei destinatari delle comunicazioni promozionali non assistite dal consenso. Il giudizio di prevalenza deve risultare da un bilanciamento svolto dal titolare, ma sempre valutabile dall'Autorità di controllo.[26]
Il titolare del trattamento non può usare in maniera retroattiva l'interesse legittimo in caso di problemi di validità del consenso in quanto ha l'obbligo di comunicare, nell'informativa rilasciata all'interessato, la base legittima al momento della raccolta dei dati personali. Il titolare del trattamento deve aver deciso la base legittima prima della raccolta dei dati.
Se il Titolare decide di fondare il trattamento sull'interesse legittimo, prima di iniziare tale trattamento, deve valutare se ha correttamente considerato tutti i rischi in gioco, e quindi tutte le possibili conseguenze sugli interessati (eventualmente svolgendo una DPIA).

[26] Antonio Ciccia Messina, Il legittimo interesse non è il passepartout per le attività di Marketing. La check list per fare il bilanciamento, Federprivacy, 21 febbraio 2020.

LE CONCLUSIONI SULLA CORRETTA FORMULAZIONE DELLA BASE GIURIDICA

Si auspica un intervento dell'Autorità al fine di:

- esprimere una indicazione chiara circa la base giuridica o le basi giuridiche di cui all'art. 5, par. 3, secondo periodo, della direttiva 2002/58/CE come modificata dalla direttiva 2009/136/CE
- esprimere una indicazione chiara del nesso o dell'assenza di un nesso della base giuridica o delle basi giuridiche di cui al predetto art. 5, par. 3, secondo periodo con la base giuridica di cui all'art. 6, par. 1, lett. f), RGPD (legittimo interesse)
- dichiarare ingannevole – e dunque illegittima – la pratica che richiede all'interessato di esprimere il "consenso" al "legittimo interesse" del Titolare all'installazione dei cookie sul terminale dell'interessato stesso.

CONCLUSIONE DEI LAVORI

di Barbara Calderini

Lo sviluppo esponenziale che sta caratterizzando i processi tecnologici determina profonde modificazioni nei rapporti sociali e, con essi, in senso adattivo o in funzione di limite, al diritto.

Nell'era della data economy, le informazioni, i dati personali e le "impronte digitali", vengono raccolte con notevole impiego di tecniche, memorizzate, trasmesse, analizzate e inferite in uno spazio digitale senza confini.

Gli individui, prima scomposti in frammenti di dati personali, vengono rimessi insieme secondo i precetti delle profilazioni del microtargeting computazionale e delle impenetrabili logiche algoritmiche, spesso predittive. Ne risultano influenzati i comportamenti e quindi le libertà e i diritti ad essi riferibili.

Il nostro obiettivo ultimo mira a far sì che il Garante per la protezione dei dati personali possa farsi interprete, attraverso l'esercizio delle sue funzioni, della particolare natura della base giuridica del

consenso, quale condizione di legittimità delle forme attive e passive di tracciamento individuale, evidenziando e promuovendo, attraverso approcci ispirati al Legal Design, l'importanza del principio di trasparenza e dell'obbligo di informare. Valori che, sebbene fortemente limitati dalle persistenti asimmetrie informative, non costituiscono meri corollari dei relativi trattamenti, bensì parte integrante del processo di gestione e raccolta dei dati, determinandone direttamente e severamente la validità.

Un percorso, dunque, in linea con le **Linee guida sui** Big Data **e** con la successiva **Indagine conoscitiva congiunta di Agcom, Agcm e Garante privacy del febbraio 2020.** Due documenti che, in previsione della richiesta istituzione di un "**coordinamento permanente**" tra Autorità (anche europee), raccolgono diverse raccomandazioni in cui spicca tra tutte la volontà di addivenire "*alla riduzione delle asimmetrie informative tra utenti e operatori digitali, nella fase di raccolta dei dati, nonché tra le grandi piattaforme digitali e gli altri operatori che di tali piattaforme si avvalgono.*"

In tal modo, ciascuna Autorità, in sinergia e nel rispetto delle proprie competenze, stante il particolare impatto derivante dalla profilazione algoritmica e dall'attività di *microtargeting* comportamentale abilitato dalle piattaforme on-line, dovrebbe rivelarsi "garante" di scelte consapevoli dell'utente e del consumatore. Favorire trasparenza e consapevolezza. Presidiare la tutela dei minori in relazione al consenso circa l'uso delle proprie informazioni personali.

Grazie per l'attenzione

dataTENET [27]

[27] I nominativi dei membri del gruppo di professionisti e studiosi che hanno partecipato alla risposta alla Consultazione sono indicati all'inizio del presente documento e, come autori, all'inizio di ciascun paragrafo.