CNIL: le sanzioni a Google e Facebook per il trattamento dei dati degli utenti tramite i cookie

Ersilia R.M. Lazzara
Senior Associate presso Chiomenti - Studio Legale Chiomenti

Vincenzo Colarocco
Avvocato presso lo Studio Previti-Associazione professionale, Responsabile del Dipartimento compliance, media e tecnologia, collabora con la cattedra di Informatica Giuridica e di Informatica Forense presso la Facoltà di Giurisprudenza dell'Università di Bologna, Data Protection Officer Università Bocconi, Presidente del Circolo dei Giuristi Telematici

1. Google e Facebook: cosa ha deciso l'Autorità garante per la protezione dei dati francese "CNIL"

Con la deliberazione del 31 dicembre 2021, la *Commission Nationale de l'Informatique et des Libertés* (rispettivamente "Decisione" e "CNIL") ha applicato la sanzione più severa mai comminata prima a Google, pari a 150 milioni di Euro. Tra il 2020 e il 2021, in realtà, Google è stata sanzionata – per l'utilizzo dei cookie sui terminali degli utenti francesi – per un importo complessivo di 250 milioni di euro (a fronte degli introiti pubblicitari indirettamente generati grazie agli strumenti di tracciamento e profilazione). Se si considera, poi, che nel gennaio 2019 era stata comminata una multa da 50 milioni di euro per mancata chiarezza sull'uso per fini pubblicitari dei dati degli utenti, ammontano a 300 i milioni richiesti in 3 anni. In quell'occasione, chiarisce la CNIL nella Decisione – anche per corroborare la tesi per la quale le nuove sanzioni non possono essere contestate per violazione del c.d. principio del *ne bis in idem* – le misure sanzionatorie erano state comminate in ragione (i) della mancata informativa e della mancata raccolta del consenso, prima dell'installazione dei cookie sui terminali degli utenti e (ii) di un meccanismo di opposizione all'installazione non del tutto funzionante e conforme alla normativa.

La Decisione, in commento riguarda, invece, le modalità con le quali gli utenti dei siti google.fr e youtube.com possono rifiutare i *cookie* precedentemente installati. A seguito di numerosi reclami, nel giugno 2021 è stata avviata un'indagine *online* ed è stato appurato che, pur offrendo un pulsante che permette l'accettazione immediata dei *cookie*, le piattaforme in questione non presentano una soluzione equivalente (pulsante o altro) che consenta all'utente di rifiutare – altrettanto facilmente – il rilascio. Sostanzialmente, con un solo "*click*" possono essere accettati, ma per rifiutarli il meccanismo non appare né immediato né agevole.
Secondo la CNIL, la soluzione adottata da Google sarebbe il frutto di una precisa strategia volta ad indurre gli utenti ad optare il pulsante "accetto" per una navigazione più semplice e veloce, scoraggiandoli – di fatto – nella scelta di rifiutare tutte le tipologie di cookie, non strettamente necessarie al funzionamento del sito stesso. In particolare, la posizione della CNIL troverebbe fondamento nel Considerando 42 del Regolamento UE n. 679/2016 ("GDPR") secondo il quale "*il consenso non dovrebbe essere considerato come dato liberamente se la persona interessata non dispone di un'effettiva libertà di scelta o non è in grado di negare o revocare il consenso senza pregiudizio*".
La CNIL ritiene che la condotta di Google incida sul principio di libera manifestazione del consenso, rappresentando una violazione dell'art. 82 della legge francese sulla protezione dei dati – la *Loi Informatique et Libertés* del 1978 opportunamente rivista, da ultimo, nel 2019 ("Legge Francese sul trattamento dei dati personali") – che non solo integra le disposizioni del GDPR, ma recepisce localmente le disposizioni della direttiva *ePrivacy* 2002/58/CE ("Direttiva ePrivacy") in materia di dati personali e telecomunicazioni.
Per tali motivi, la CNIL ha multato *Google LLC* per 90 milioni di Euro e *Google Ireland Limited* per 60 milioni di Euro. Gli importi sono stati determinati considerando i seguenti elementi:

- la gravità della violazione dell'art. 82 della Legge Francese sul trattamento dei dati personali;
- il numero di utenti coinvolti, quasi cinquanta milioni;
- i "notevoli profitti" che le società traggono dai ricavi pubblicitari generati dai *cookie* che permettono il tracciamento della navigazione effettuata degli utenti;
- la circostanza che, già a partire dal febbraio 2021, era stata segnalata dall'Autorità la necessità di semplificare la procedura per rifiutare i *cookie*.

Oltre a Google, la CNIL ha sanzionato – per le medesime ragioni sopra esposte – *Facebook Ireland* comminando una sanzione di 60 milioni di

euro disposta in un'apposita deliberazione del 31 dicembre all'esito di una puntuale attività di indagine. Anche nella piattaforma social *facebook.com*, sono infatti necessari diversi *click* per rifiutare tutti i *cookie*, mentre ne basta uno solo per accettarli. Inoltre, è stato appurato che il pulsante con il quale l'utente potrebbe rifiutare i cookie è situato nella parte inferiore della seconda finestra e individuato dalla dicitura "Accetta i cookies": tale conformazione, quindi, determinerebbe nell'utente confusione al punto che potrebbe avere la sensazione di "non" poter scegliere se rifiutare o meno l'installazione di cookie, o che comunque potrebbe avere difficoltà nella gestione.

Nel giustificare la sanzione, la CNIL ha rimarcato "*la portata del social network Facebook e il posto essenziale che occupa in Francia, in quanto domina di gran lunga il mercato dei social network, […] Rileva inoltre gli "effetti di rete" generati da questa posizione dominante, evidenziati dall'autorità tedesca garante della concorrenza in una decisione del 6 febbraio 2019*" e "*sottolinea che tale inadempimento è tanto più dannoso per le persone interessate in quanto, parallelamente alla sua funzione tradizionale di mantenimento e sviluppo delle relazioni interpersonali, tale social network sta assumendo un posto sempre più importante anche in settori così diversi come l'accesso alle informazioni, il dibattito pubblico e persino la sicurezza civile attraverso la funzione «Facebook hazard check» (o «safety check») in caso di calamità naturale o di attacchi, che sono di una certa importanza in una società democratica*".

Oltre alle sanzioni amministrative, la CNIL ha emesso un'ingiunzione che impone a ciascuna delle società di fornire agli utenti situati in Francia – entro tre mesi dalla notifica della decisione – un mezzo per rifiutare i cookie altrettanto semplice rispetto a quello implementato per poterli accettare e ciò con lo scopo di garantire una libera manifestazione e revoca del consenso. In caso contrario, alle società verrà applicata una sanzione di 100.000 euro per ogni giorno di ritardo.

Le sanzioni, quindi, potrebbero essere giustificate non soltanto dalla condotta in violazione della normativa ma anche in ragione di quella *accountability* – da leggersi, in questa sede, come senso di responsabilità che esula dal contesto strettamente connesso al trattamento dei dati personali – che vorrebbe che ciascun titolare, ove determini un trattamento in ragione del consenso degli interessati, garantisca concretamente a questi ultimi la libertà di scelta, ma anche e soprattutto la libertà di "modificare" la propria volontà o, più semplicemente, di "cambiare idea" anche con un solo *click*.

Invero, dal 31 marzo 2021, data di scadenza del termine fissato per i siti e le applicazioni mobili per conformarsi alla nuova disciplina sui cookie, la CNIL ha adottato quasi 100 misure correttive (ordinanze e sanzioni) relative al mancato rispetto della normativa.

2. La competenza (per materia) della CNIL e la non applicazione del meccanismo di coerenza

Nell'ambito della Decisione, la competenza della CNIL a pronunciarsi legittimamente nei confronti della società vede due posizioni in netta contrapposizione.

La CNIL ritiene che la propria competenza derivi dall'art. 5 (3) della Direttiva ePrivacy. I trattamenti in esame – che rientrerebbero nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico attraverso una rete pubblica di comunicazione elettronica offerta nell'ambito dell'Unione Europea – sono coperti dall'art. 82 della Legge Francese sul trattamento dei dati personali che recepisce la Direttiva. Il legislatore francese ha, infatti, incaricato la CNIL di garantire il rispetto della Direttiva, anche prevedendo che l'Autorità possa comminare sanzioni.

La CNIL, in particolare, osserva che gli accertamenti effettuati si sono incentrati solo sulla iniziale fase di trattamento rientrante nell'ambito della Direttiva ePrivacy (ossia la fase di lettura e installazione dei cookie sui terminali degli utenti) non già sulla fase ulteriore (ossia l'esame dei trattamenti effettuati per il perseguimento di diverse finalità, c.d. "trattamenti successivi") per le quali una valutazione ai sensi del GDPR sarebbe certamente necessaria.

La CNIL rispetto al rapporto tra Direttiva ePrivacy e GDPR – norma che le società, come di seguito illustrato, riterrebbero applicabile – rammenta come sia il testo della Direttiva ePrivacy sia quello del GDPR chiariscano i rapporti tra le due normative. Da una parte la Direttiva ePrivacy stabilisce che le disposizioni in essa contenute specificano e integrano quelle del GDPR (prima della Direttiva 95/46/Ce) e dall'altra parte il Considerando 173 del GDPR chiarisce che quest'ultimo non dovrebbe trovare applicazione "*fatto salvo specifici obblighi aventi lo stesso obiettivo* [di tutela dei diritti e delle libertà fondamentali] *previsti dalla Direttiva*". A conferma vi sarebbe analogo ragionamento avallato sia dalla Corte di Giustizia, nel noto **procedimento C-673/17 avverso la società tedesca Planet49**, sia dall'*European Data Protection Board* ("EDPB") nel suo **parere 5/2019** sulle interazioni tra Direttiva ePrivacy e GDPR[1].

[1] L'*European Data Protection Board* nel suo Parere n. 5/2019 del 12 marzo 2019 sulle interazioni tra la direttiva "privacy e comunicazioni elettroniche" e il GDPR, ha esplicitamente escluso l'applicazione del meccanismo dello "sportello unico" per le materie rientranti materialmente nell'ambito della Direttiva: "*ai sensi del Capo VII del GDPR, i meccanismi di cooperazione e coerenza a disposizione delle autorità per la protezione dei dati ai sensi del GDPR riguardano il monitoraggio dell'applicazione delle disposizioni del GDPR*". I meccanismi del GDPR, quindi,

Secondo la CNIL la Direttiva ePrivacy sarebbe norma speciale che, in deroga al GDPR, rappresenta il perimetro normativo rilevante e applicabile al caso in esame. La fonte dell'obbligo giuridico starebbe, quindi, nella normativa a tutela delle comunicazioni elettroniche, competenza inclusa (in particolare, l'art. 5.3 della Direttiva).

La CNIL rileva, inoltre, che anche altre autorità nazionali per la protezione dei dati personali hanno già imposto sanzioni relative alle operazioni di lettura e/o scrittura di informazioni nel terminale dell'utente. L'autorità spagnola, ad esempio, ha adottato diverse decisioni di natura sanzionatoria nei confronti di vari titolari del trattamento applicando esclusivamente la normativa nazionale di recepimento della Direttiva, nella fattispecie l'articolo 22, comma 2 della *Ley 34/2002* dell'11 luglio dei *Servicios de la Sociedad de la Información y de Comercio Electrónico*, senza attuare la procedura di cooperazione prevista dal GDPR.

Facebook e Google hanno entrambe opposto alla CNIL una questione relativa al c.d. ***one-stop-shop***: cioè il meccanismo di sportello unico *ex* art. 56 GDPR, per cui sarebbe competente solo l'autorità capofila dello stabilimento principale del titolare. In pratica, la sede europea di Facebook sarebbe solo quella irlandese, a Dublino, per cui la CNIL non avrebbe avuto competenza per giudicare le condotte della società.

Le Società fondano le loro argomentazioni sul nesso tra GDPR e Direttiva ePrivacy, ritenendo che l'applicazione del GDPR non possa essere esclusa laddove trovi spazio l'art. 82 della Legge francese sul trattamento dei dati personali. In particolare, ritengono che la mancanza di regole specifiche sulla determinazione della competenza dell'autorità di controllo in caso di trattamenti transfrontalieri che rientrano nel campo di applicazione della Direttiva ePrivacy dovrebbe essere sostituita dall'applicazione del quadro procedurale previsto dal GDPR. Sostengono che l'applicazione del meccanismo dello "sportello unico" non solo è in linea con l'intenzione del legislatore europeo, ma anche con l'interpretazione sia dell'*European Data Protection Board* sia delle diverse autorità europee. A questo proposito, riconoscono che il potere in capo agli Stati membri di scegliere l'autorità nazionale competente per le questioni afferenti la Direttiva ePrivacy non impedisce l'applicazione del meccanismo dello "sportello unico" previsto dal GDPR, nella misura in cui sono stati conclusi accordi di cooperazione tra queste autorità in diversi Stati membri in modo che le autorità di protezione dei dati e le autorità nazionali competenti per le questioni afferenti la Direttiva

non si applicano al monitoraggio dell'applicazione delle disposizioni della Direttiva. (GEPD, parere 5/2019, 12 marzo 2019, pt. 80).

ePrivacy – se sono autorità diverse – possano esercitare congiuntamente i poteri di controllo su una questione che rientra nell'ambito di applicazione del GDPR e della Direttiva ePrivacy e, conseguentemente, partecipare al meccanismo dello sportello unico.

3. La competenza (per territorio) della CNIL

Fermo restando i criteri di cui all'art. 3 del GDPR in tema di applicazione territoriale della norma, l'art. 3, comma I, della Legge Francese sul trattamento dei dati personali prevede che, per quanto concerne le attività operate da un titolare del trattamento stabilito sul territorio francese, – e indipendentemente dal fatto che il trattamento avvenga o meno in Francia – si applichino le disposizioni della medesima Legge.

La CNIL ritiene di avere, quindi, non solo competenza per materia ma anche per territorio quando il trattamento (i) è svolto nell'ambito del "quadro delle attività" della società *Google France*, che costituisce lo "stabilimento" sul territorio francese del gruppo Google e (ii) consiste in operazioni di accesso o registrazione di informazioni sul terminale di utenti residenti in Francia durante l'utilizzo del motore di ricerca *Google Search e YouTube*, in particolare a fini pubblicitari.

Le società – dal loro punto di vista – ribadiscono quanto affermato in tema di competenza per materia e che, quindi, riconoscendo la rilevanza del GDPR, dovrebbe essere applicato l'art. 3 dello stesso in forza del quale la competenza spetterebbe all'Autorità Irlandese, luogo in cui è localizzata la sede effettiva di Google in Europa.

La CNIL, invece:

1. rileva che la società Google France – con locali su territorio francese – costituisce la controllata francese della società GOOGLE LLC, e ha – quale oggetto sociale – "*la prestazione di servizi e/o consulenza relativi al software, alla rete Internet, alle reti telematiche o on line, compresa l'intermediazione nella vendita della pubblicità online, la promozione in tutte le sue forme di pubblicità online, la promozione diretta di prodotti e servizi e l'implementazione di centri di elaborazione dati*";
2. osserva, dalle informazioni pubblicate sul sito di Google France, che la società si occupa di sostenere le PMI in Francia "*attraverso lo sviluppo di strumenti di collaborazione, soluzioni pubblicitarie o per fornire loro le chiavi per comprendere i loro mercati e i loro consumatori*"; e
3. rileva che sul sito "ads.google.com" viene specificato che "*Google Ads consente alle aziende francesi di promuovere i propri prodotti o servizi sul motore di ricerca e su una grande rete pubblicitaria*".

Pertanto, sulla base dei predetti elementi e assodata la competenza *ratione materiae*, la CNIL riconosce l'applicabilità dell'art. 3 della Legge Francese per la protezione dei dati personali – poc'anzi menzionato – in quanto il trattamento si identifica con l'"*accesso alle informazioni" o* con le registrazioni "*nel terminale degli utenti del motore di ricerca Google Search e di YouTube residenti in Francia, in particolare a fini pubblicitari*" ed è effettuato nell'ambito delle attività della società Google France "*sul territorio francese, che si occupa della promozione e commercializzazione dei prodotti Google e delle loro soluzioni pubblicitarie in Francia*".

4. La posizione dell'Autorità (Nazionale) Garante per la protezione dei dati personali

Come noto, l'Autorità Garante per la protezione dei dati personali ("Garante") ha adottato nuove linee guida in tema di utilizzo di cookie e altri strumenti di tracciamento ("Linee Guida"). Al punto 7.1 si prevede quanto segue: "Il rispetto di tali regole impone dunque che, **per impostazione predefinita**, al momento del primo accesso dell'utente a un sito web, **nessun cookie o altro strumento diverso da quelli tecnici venga posizionato all'interno del suo dispositivo**, né che venga utilizzata alcuna altra tecnica attiva o passiva di tracciamento […]. Qualora l'utente **scegliesse**, com'è nella sua piena disponibilità, di **mantenere quelle impostazioni di default e dunque di non prestare il proprio consenso al posizionamento dei cookie o all'impiego di altre tecniche di tracciamento**, dovrebbe dunque **limitarsi a chiudere il banner mediante selezione dell'apposito comando usualmente utilizzato a tale scopo**, cioè quello contraddistinto **da una X** posizionata di regola, e secondo prassi consolidata, **in alto a destra e all'interno del banner medesimo**, senza essere costretto ad accedere ad altre aree o pagine a ciò appositamente dedicate".

La posizione del Garante appare, pertanto, chiara e volta a garantire all'utente la possibilità di rifiutare con un semplice *click* i cookie non necessari. I titolari del trattamento dovranno quindi selezionare e avvalersi solo di fornitori **di *banner* e *cookie solution* che siano conformi** alle prescrizioni delle Linee Guida, ad es. tramite apposite configurazioni lato back-end. Come noto, sul titolare – in forza del principio di *accountability* – grava l'onere di selezionare fornitori che siano in grado di erogare soluzioni in linea con la normativa applicabile.

Adesso, con la piena applicabilità delle Linee Guida a partire dallo scorso mese di gennaio, è naturale chiedersi se anche il Garante interverrà verso Facebook e Google in Italia, sulla base degli stessi ragionamenti della CNIL.

5. CNIL, Garante e quadro europeo: manca ancora una visione d'insieme?

Le Linee Guida non affrontano il nodo più problematico della disciplina relativa a *cookie* e tecnologie simili e, cioè, il rapporto tra le diverse implementazioni e interpretazioni della Direttiva ePrivacy nei singoli Stati Membri. Un quadro normativo frammentato nei diversi Stati Membri, infatti, comporta una notevole incertezza sulle modalità di adeguamento laddove gli operatori, titolari del trattamento, operano in diverse giurisdizioni. Sovrapposizioni e contraddizioni tra i diversi orientamenti delle autorità, infatti da un lato, rendono più difficoltosa la *compliance* e, dall'altro, rischiano di far prevalere le posizioni più restrittive, svuotando di significato le altre interpretazioni. Infatti – come sopra descritto – la Direttiva ePrivacy non prevede un meccanismo di cooperazione e consultazione tra le autorità di controllo, come quello disciplinato dal GDPR, ma un mero obbligo di collaborazione nell'applicazione delle norme nazionali adottate. Tuttavia, lo stesso *European Data Protection Board*[2] ("EDPB") ha sottolineato come il rapporto di legge generale – speciale che intercorre tra GDPR e Direttiva ePrivacy comporta che, nel caso di materie rientranti nell'ambito di applicazione del GDPR, le autorità hanno l'obbligo di applicare il meccanismo di cooperazione e coerenza previsto dallo stesso.

Pertanto, poiché ingenti aspetti relativi ai *cookie* (e, *in primis*, le caratteristiche del consenso) rimangono disciplinati dal GDPR, è lecito ritenere che il meccanismo di cooperazione possa applicarsi anche in tale contesto, attraverso l'opportuna individuazione dell'autorità capofila.

L'esigenza di un approccio uniforme tra le diverse autorità è stato ribadito da ultimo dall'EDPB nello *Statement* sul Regolamento E-Privacy del 9 marzo 2021; da un lato, è stato rammentato come le norme del futuro Regolamento E-Privacy dovranno essere applicate non già isolatamente, ma in combinato disposto con il GDPR; dall'altro lato, è stato evidenziato come solo un perfetto allineamento con il meccanismo di cooperazione del GDPR possa garantire la corretta applicazione del Regolamento E-Privacy e ciò nell'ottica di evitare frammentazioni nell'applicazione della disciplina rilevante e ridurre gli oneri dei fornitori che rischierebbero di doversi confrontare con più di 27 autorità di controllo.

[2] Si veda il "*Parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati",* disponibile al seguente link https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_it.pdf.

L'auspicio è che il futuro Regolamento E-Privacy segua la direzione indicata dall'EDPB, facendo chiarezza sulla competenza in materia di applicazione ed *enforcement* per i cookie, tenendo quanto più possibile in considerazione le difficoltà operative da parte dei *player* e la necessità di stabilire indicazioni quanto più possibile armonizzate a livello europeo.

6. Conclusioni

All'alba del sesto anno in cui è entrato in vigore il GDPR, ad avviso degli scriventi, si rende necessario un intervento deciso da parte dell'EDPB in merito all'applicazione del principio dell'one-stop-shop, al fine di poter garantire, in tempi rapidi, un'uniforme interpretazione del GDPR volta ad avere (per quanto possibile) una maggiore certezza del diritto in tutta Europa.
Ed infatti nell'attuale scenario le Supervisory Authorities ricorrono ad interpretazioni giuridiche per "eludere" il summenzionato principio al fine di attrarre innanzi a sé la competenza in modo da poter garantire più velocemente la tutela dei "propri" interessati.
Ciò, ancorché possa considerarsi lodevole sul piano della tutela effettiva della data protection non può dirsi lo stesso sul piano della certezza del diritto, in quanto le decisioni decentralizzate e non coordinate portano con sé rischi interpretativi e applicativi delle misure sanzionatorie, che potrebbero determinare una disomogeneità nell'impianto regolatorio nonché avere un impatto anche sul mercato. Si pensi ad esempio ai recenti casi, aventi ad oggetto il trasferimento dei dati personali in America attraverso Google analytics, giudicati – anche a seguito dei 101 ricorsi presentati dal Noyb» (European Center for digital rights) in giro per l'Europa[3] – dalla autorità austriaca[4], francese[5] e dall'European Data Protection Supervisor[6]. Ebbene, pur essendo *de facto* la medesima violazione realizzata attraverso lo stesso servizio erogato da Google, le pronunce e le sanzioni sono state differenti, essendo stati instaurati differenti procedimenti. Ad avviso degli scriventi, l'adozione di un unico provvedimento sanzionatorio avrebbe

[3] Si veda, sul punto, il comunicato stampa diffuso da *Noyb*, disponibile al seguente url: https://noyb.eu/en/101-complaints-eu-us-transfers-filed.
[4] Il provvedimento ufficiale, in lingua originale, è disponibile al seguente url: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf, mentre la traduzione automatica dall'inglese è disponibile al seguente url: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf.
[5] Il provvedimento è disponibile, in lingua francese al seguente url: https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf.
[6] Il provvedimento è disponibile al seguente url: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf.

anche una maggior forza applicativa nei confronti del mercato, in quanto il principio ivi affermato potrebbe essere letto – in termini di efficacia – in chiave nomofilattica consentendo alle aziende (e non solo) di concorrere concretamente con le medesime regole in ogni stato europeo ed aiutando a contrastare il fenomeno della migrazione delle aziende verso le nazioni che hanno interpretazioni maggiormente favorevoli.

Dunque, l'EDPB – quale fulcro imprescindibile del nuovo sistema di rapporti tra le autorità nazionali, nell'esercizio del suo potere di regolamentare il meccanismo dello sportello unico, indirizzando e rafforzando la cooperazione delle autorità di controllo competenti per il trattamento dei dati all'interno del territorio dell'Unione – dovrebbe orientare maggiormente i suoi sforzi proprio nell'applicazione dello strumento dell'"one-stop-shop".

Oggi più che mai c'è bisogno di unità da parte dell'Europa, anche in questo campo di battaglia.