COOKIE E LIBERTA' DEL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI.

Di Antonio Paolo Seminara

ABSTRACT. *L'articolo indaga sulle condizioni giuridiche di legittimità dei cookie, strumenti mediante i quali i gestori dei siti internet richiedono e ottengono il consenso degli utenti al trattamento dei relativi dati personali. Partendo dalla disciplina in materia di privacy, recentemente riformata dal Reg. 679/2016/UE, si analizzano i requisiti del consenso dalla stessa previsti, per declinarli successivamente con riguardo al fenomeno dei cookie, le cui peculiarità operative sono oggetto di specifica considerazione. In tal senso, importanti spunti possono trarsi sia dalla prassi applicativa, nazionale ed europea, sia, più specificamente, dalle Linee Guida emanate nel 2020 dal Comitato Europeo per la protezione dei dati personali e, conseguentemente, dal Garante per la Privacy.*

The article investigates the legal conditions for the legitimacy of cookies, tools through which website operators request and obtain users' consent to the processing of their personal data. Starting from the privacy regulation, recently reformed by Reg. 679/2016/EU, the consent requirements are analyzed, and then declined with regard to the phenomenon of cookies, whose operational peculiarities are the subject of specific consideration. In this sense, important hints can be drawn both from the application practice, national and European, and, more specifically, from the Guidelines issued in 2020 by the European Data Protection Board and, consequently, by the national Privacy Guarantor.

1. Introduzione.

La progressiva instaurazione di una "società digitale", a partire dalla nascita del *World Wide Web* nel 1991 e di Google nel 1998, ha portato con sé, accanto ad innumerevoli, innegabili, benefici, anche una serie di questioni problematiche di estrema rilevanza. Per comprendere la portata del fenomeno, basti considerare che le persone connesse ad Internet sono circa 4,5 miliardi e che ognuna di esse è in grado di creare e fruire facilmente di materiali e di memoria in quantità prima impensabili.

Il fenomeno del digitale – che ha stimolato importanti lavori nei più svariati ambiti di studio[1] - non poteva non determinare una qualche riflessione tra gli operatori del diritto. Da un punto di vista giuridico, infatti, la rivoluzione digitale ha aperto la strada ad una ricostruzione, appunto in termini "digitali", delle esigenze di tutela della persona che si ritrova ad esistere ed agire nel mondo di Internet.

Vi è chi ha identificato il problema in termini di "frazionamento delle identità"[2] , chi in termini di sua "dispersione" [3]: in ogni caso, si è fatto riferimento al fenomeno, incentivato dai *social network* e dalla proliferazione dei *big data* degli utenti, della frammentazione dell'identità personale nel panorama digitale, per cui l'immagine del sé può mutarsi a seconda dei dati mostrati nelle varie piattaforme. In altre parole, le informazioni diffuse online permettono a chiunque di formarsi un'idea, più o meno autentica, di una persona, che potremmo definire "identità digitale".

Accanto ai dati inseriti volontariamente nel *cyberspazio*, si aggiungono quelli che l'utente lascia inconsapevolmente e, infine, quelli che, seppur riferiti a quest'ultimo, sono immessi da terzi. Se, ad una prima impressione, l'esigenza di tutela sembra manifestarsi con maggior rigore in quest'ultima ipotesi, una più attenta analisi induce a riflettere anche sulle prime.

Più in generale, l'evoluzione tecnologica ha reso possibile la raccolta e il successivo trattamento in massa dei dati personali, comportando una serie rischi dovuti da un lato al volume ed alla natura delle informazioni diffuse sul web, e dall'altro alla invasività delle modalità di trattamento tipicamente adottate dai siti[4]. Rischi che riguardano la persona non solo dal punto di vista meramente individuale, lesa nella propria riservatezza e autonomia decisionale, ma che dal punto di vista collettivo e democratico, considerando i pericoli di discriminazione derivanti dalla profilazione e dal possibile effetto di condizionamento che la medesima profilazione dei contenuti digitali è idonea a determinare.

Il patrimonio informativo del singolo utente di internet diventa un oggetto di cui si appropria il fornitore dei servizi digitali online, che ricava dal trattamento e dalla eventuale cessione dei dati enormi profitti commerciali: si pensi, nel caso dei *social networks*, alla quantità di informazioni che talune multinazionali sono in grado di amministrare e "monetizzare" attraverso accordi di *marketing*[5].

Appare chiaro come la tradizionale asserita indisponibilità dei diritti della personalità, in cui rientra il diritto alla privacy, debba scontrarsi con la concreta proliferazione delle cd. *non monetary transactions*, nelle quali, dietro al velo dell'apparente gratuità del servizio, si realizza una cessione di attributi immateriali della persona.

Proprio in questo segmento di realtà digitale si inseriscono i *cookie*, strumenti mediante i quali l'utente di internet acconsente alla cessione di informazioni a lui relative durante la navigazione online. I prevalenti (ma non gli unici) beneficiari, in queste ipotesi, sono le società commerciali, le quali utilizzano i dati ottenuti per la profilazione dell'utente-consumatore, così identificandone i gusti principali e la propensione all'acquisto.

Tra le informazioni analizzate, accanto a quelle espressamente richieste agli utenti, vi sono quelle ricavabili dalla sua navigazione online (ricerche effettuate, siti più visitati ecc.), dall'utilizzo di app o di particolari strumenti di pagamento.

Con riferimento al fenomeno dei *cookie*, la principale preoccupazione giuridica[6] – partendo dalla disciplina in materia di privacy, tanto nazionale quanto europea, soprattutto a seguito del nuovo *GDPR* (Reg. n. 679/2016/UE) – riguarda l'assenza, nell'utente accettante, di una vera consapevolezza e libertà in merito alla decisione di cessione. Considerate, infatti, le tecniche di indebita pressione adottate dai siti, in uno con una procedura estremamente semplificata (bastando un *click*) per il relativo con-

[1] Si consiglia, da un punto di vista meramente divulgativo ma estremamente interessante, l'analisi del mondo digitale in termini di "Game" svolta da A. Baricco, *The game*, Torino, 2018.
[2] Così S. Niger, *Diritto all'informazione, diritti della persona e archivi giornalistici online*, in *federalismi.it*, XI, 2013, 1 ss.
[3] S. Rodotà, *Il diritto di avere diritti*, Roma - Bari, 2012, 173.
[4] Evidenziano I rischi della evoluzione digitale del trattamento dei dati V. Zeno-Zencovich e G. Giannone Codiglione, *Ten legal perspectives on the "big data revolution"*, in *Conc. merc.*, 2016, vol. 23, 29 ss.
[5] Importanti spunti sulla natura contrattuale o meno degli accordi digitali implicanti la cessione dei dati nell'ambito dei *social network* possono trarsi dalla lettura di C. Perlingieri, *Profili civilistici del social network*, Napoli, 2014
[6] La dottrina ha anche analizzato la questione relativa all'inquadramento contrattuale della cessione dei dati sul web (e degli altri servizi telematici), ma ciò esula dal tema della presente trattazione. Ad ogni modo, uno scritto che vi ha dedicato interessanti osservazioni è G. Resta e V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. Trim. Dir. e Proc. Civ.*, fasc. 2, 2018, 411.

senso, non può escludersi che spesso il consumatore sia indotto a cedere i propri dati in modo tutt'altro che razionale, ponderato e quindi libero.

Anzi, non è per nulla chiaro se, quando un utente utilizza un sito internet o un'*app* sul proprio *smartphone* – che di per sé rappresentano certamente comportamenti positivi in un certo senso – lo stesso sia consapevole di fornire automaticamente i dati personali.

In altre parole, si vede, da più tardi, il rischio di una qualche aggressione, da parte dei *cookie*, alla sfera di riservatezza e di libertà nel consenso che viene posta al centro della tutela in materia di privacy.

In questo senso, appare interessante analizzare la posizione assunta da parte del Garante della privacy italiano, dal Comitato Europeo per la protezione dei dati personali e, infine, da parte della Corte di Giustizia dell'UE in relazione ai limiti di ammissibilità delle attuali forme di richiesta ed accettazione del trattamento dei dati utilizzate da parte dei gestori dei siti internet. Trattandosi di una pratica – quella dei *cookie* – di ampia diffusione, si evidenzia l'opportunità di fare chiarezza sulle condizioni della loro ammissibilità, per ragioni tanto di certezza quanto di intensità di tutela.

Lo scritto tenterà di mettere luce sugli orientamenti suddetti, ripercorrendo l'iter interpretativo seguito dal Garante e confrontandolo con la posizione assunta dalle competenti autorità europee sulle odierne modalità di ottenimento del consenso ai *cookie*.

Lo sfondo, che si analizzerà brevemente in apertura, è quello della disciplina della *privacy*, di cui occorre esaminare le disposizioni connesse al consenso al trattamento dei dati. Ci si concentrerà poi sullo strumento dei *cookie*, che ad oggi rappresenta la principale forma di trattamento dei dati personali sul *web*.

2. La privacy nel contesto digitale

Il *cyberspazio*, ormai da tempo luogo di espressione di molteplici attività umane, rappresenta probabilmente la dimensione più problematica per quanto attiene al "diritto alla privacy" [7]. Questo, come ormai noto, si riassume nel diritto al rispetto di una sfera di riservatezza e ad un adeguato trattamento dei propri dati personali[8]. Si tratta di uno degli attributi immateriali della persona, parte dei diritti della personalità, rispetto a cui in dottrina si è sviluppano un ampio dibattito in merito alla possibilità, ed ai relativi limiti, di una loro disposizione attraverso lo strumento negoziale[9].

Si è parlato, in tal senso, di una progressiva "giuridificazione" della persona[10], a cui si accompagna la possibile mercificazione (o "reificazione"[11]) dei suoi attributi, da molti avvertita come pericolo alla presupposta indisponibilità di tali valori[12]. Quest'ultima o deriva da un'espressa previsione di legge (come nel caso dell'art. 5 c.c.) o dalla stretta inerenza alla persona del valore giuridico considerato, a cui conseguirebbe l'impossibilità dell'oggetto del contratto che implichi il trasferimento del relativo diritto.

Per superare l'*impasse* tra l'intrinseca indisponibilità dei diritti della personalità e il loro concreto sfruttamento in talune circostanze, si è specificato come l'oggetto del trasferimento sia solo l'elemento patrimoniale dei diritti in questione[13], o comunque il singolo esercizio occasionale degli stessi[14], il che li renderebbe più oggetto di una obbligazione che di un atto di disposizione.

Il diritto alla privacy, la cui indisponibilità deve ricavarsi dalla natura strettamente personale, rientra certamente tra i diritti coinvolti dal processo di "progressiva negoziabilità", come reso evidente dal-

[7] Tra gli spunti dottrinali sul tema, cfr.: V. Cuffaro, V. Ricciuto, R. D'Orazio (a cura di), *I dati personali nel diritto europeo*, , Torino, 2019; A. S. Esposito, *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in *Dir. dell'informazione e dell'informatica* (II), fasc. 4, 2019, 1071 ss.; A. Iuliani, *Note minime in tema di trattamento dei dati personali*, in *Europa e dir. privato*, fasc. 1, 2018, 293 ss.; S. Martinelli, *Diritto all'oblio e motori di ricerca. Memoria e privacy nell'era digitale*, Milano, 2017; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; V. Zeno Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Riv. dir. media*, 2018, 2, 5 ss.

[8] L'esigenza di una protezione della sfera privata è stata avvertita già molto tempo addietro. In questo senso, la prima configurazione di un diritto alla privacy è tradizionalmente ricondotta all'articolo scritto da Samuel D. Warren e Louis D. Brandeis nel 1890 (cfr. *The right to privacy*, in *Harvard Law Review*, Vol. 4, 1890, 193 ss.).

[9] Cfr., sul tema, S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, in *Memorie del Dipartimento di Giurisprudenza dell'Università di Torino*, Milano, 2018.

[10] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 179 ss

[11] V. Cuffaro, *A proposito del ruolo del consenso*, in *Trattamento dei dati e tutela della persona,* a cura di V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich, Milano, 1999, 121.

[12] Si evidenzia come il dogma dell'indisponibilità, oltre ad essere messo in crisi dalla prassi, è stato oggetto di una revisione critica in dottrina. Sul punto, cfr. S. Thobani, *op. cit.*, 51 ss.

[13] Così, P. Manes, *Il consenso al trattamento dei dati personali*, Padova, 2001, 44, nonché C. Scognamiglio, *Il diritto all'utilizzazione del nome e dell'immagine delle persone celebri*, in *Dir. inf.*, 1988, 38 ss.

[14] Vedi, in tal senso, Cass., 17 febbraio 2004, n. 3014, in *Resp. Civile*, 2004, 112 ss. In dottrina, cfr. V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, in *Dir. inf.*, 1993, 545 ss.

la prassi sempre più frequente di cessione dei dati da parte di ciascun individuo: si è sottolineato come le informazioni diventino "estrinsecazioni immateriali della persona in grado di circolare autonomamente", e come lo sviluppo tecnologico determini "un salto non solo quantitativo ma anche qualitativo di tale circolazione"[15].

Pertanto, è di fondamentale importanza che il diritto alla privacy sia in qualche modo protetto da utilizzi che, privi di limitazione giuridica, ne compromettano il nucleo essenziale, del quale occorre salvaguardare una certa intangibilità.

In un contesto "fluido", privo di barriere, come quello digitale evidente appare il rischio di un'invasione della riservatezza individuale e della libertà di trattamento per gli utenti che vi navigano.

In questo senso, i passi compiuti sul *web* verso il superamento dei tradizionali ostacoli alla libertà di movimento, fisica e ideale, sembrano accompagnarsi ad una progressiva compressione delle esigenze di mantenimento di una qualche sfera personale, unica ed invalicabile.

L'attuale disciplina della *privacy* va rintracciata nel recente "Regolamento in materia di protezione dei dati personali" dell'Unione Europea (cd. *GDPR*, Reg. UE n. 679/2016)[16] che, direttamente applicabile ed efficace in Italia, ha introdotto importanti novità nel settore (con particolare riguardo al digitale). Lo stesso ha integrato e riformato il "Codice della privacy" (d. lgs. n. 196/03), *corpus* normativo nazionale di riferimento in materia prima dell'avvento della normativa europea[17].

Il quadro giuridico va integrato con la Direttiva n. 2002/58/CE (cd. Direttiva "ePrivacy", modificata dalla Dir. n. 2009/136/CE), con cui deve coordinarsi il suddetto Regolamento, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[18]. Dal momento che molte forme di trattamento sono riconducibili tanto alla Direttiva quanto al Regolamento, nei casi di sovrapposizione potenziale – considerato che la Direttiva rappresenta, secondo l'art 1, par. 2 della stessa, *lex specialis* rispetto al Regolamento – prevarrà la prima; le disposizioni del Regolamento, invece, resteranno applicabili per le fattispecie non specificamente previste dalla Direttiva, oltre che per offrire a quest'ultima la cornice regolatoria di carattere generale.

Un rapporto inverso sussiste, invece, tra il Regolamento e la recente Direttiva 2019/770/UE "relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali"[19], la quale fa espressamente salvi sia il GDPR sia la Direttiva 2002/58 (considerando 37).

La recente Direttiva risulta certamente rilevante nella materia in esame, dal momento che il suo ambito di applicazione si estende ai contratti in cui un operatore commerciale fornisce, o si impegna a fornire, contenuto digitale al consumatore, a fronte di una "controprestazione non pecuniaria", sotto forma anche di cessione "di dati personali o di qualsiasi dato" (art. 3, par. 1). In caso di conflitto tra la Direttiva 2019/770 e il diritto dell'Unione in materia di protezione dei dati personali, quest'ultimo dovrebbe prevalere (come confermato dal successivo considerando n. 38), con la conseguenza che si applicheranno, ai contratti di fornitura di servizi digitali, tutte le condizioni normative per il consenso al trattamento, ivi compresa la sua revocabilità (considerando 39).

Prima di procedere con l'analisi dei *cookie*, dunque, appare opportuna una sia pur breve illustrazione dei principali criteri normativi che vigono in materia di *privacy* e che rendono ogni "trattamento" dei dati legittimo. Ciò ci permetterà, nel prosieguo, di verificare se il trattamento ordinariamente effettuato mediante i *cookie* da buona parte dei siti risulti conforme alle maglie legislative e alla loro interpretazione datane tanto in ambito nazionale quanto europeo.

Un primo sguardo al GDPR suggerisce con evidenza come l'intero sistema normativo ruoti attorno all'elemento, appunto, del "consenso" del soggetto dei cui dati si tratta[20]. Ciò era previsto, d'altronde, già nella disciplina previgente di cui al Codice della Privacy, il cui articolo 23 ammetteva il trattamento dei dati "solo con il consenso espresso dell'interessato".

[15] Così S. THOBANI, *op. cit.*, 15.

[16] Il Regolamento ha abrogato la Direttiva n. 95/46/CE in materia di "*tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*". Per l'adeguamento della normativa nazionale al GDPR è stato emanato il d. lgs. n. 101 del 10 agosto 2018.

[17] E' pur vero che, già prima del Codice, sia la giurisprudenza che la dottrina avevano ampiamente contribuito alla teorizzazione di un diritto alla riservatezza. In giurisprudenza, vedi Cass. 22 dicembre 1956 n. 4487, in *Giur. it*., 1957, I, 366 ; Cass., 20 aprile 1963, n. 990, in *Foro it*. 1963, 2, 877; Cass., 27 maggio 1975, n. 2129, in *Foro it*. 1976, I, 2895.

[18] In ambito europeo, inoltre, fanno riferimento alla sfera di riservatezza l'art. 8 della Convenzione Europea per la salvaguardia dei diritti dell'uomo del 1950 e l'art. 8 della Carta dei diritti fondamentali dell'Unione Europea del 2000; invece, in ambito internazionale, si può far riferimento all'art. 12 della Dichiarazione Universale dei Diritti Umani del 1948.

[19] Per approfondimenti sulla Direttiva, cfr. C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. Civ*., fasc. 3, 2019, 499 ss.

[20] Dalla libertà del consenso derivano diversi diritti per l'interessato: il diritto di accesso ai dati, alla loro rettificazione, all'oblio (o alla cancellazione dei dati personali), alla limitazione del trattamento e, infine, alla portabilità dei dati.

Oltre che sul consenso, è bene precisare, il trattamento dei dati personali può fondarsi anche su altre basi legittimanti, come l'esecuzione del contratto o di un obbligo legale, o ancora la necessità di salvaguardare interessi vitali dell'interessato o di un'altra persona fisica, o di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6 GDPR). Rimane indiscussa, in ogni caso, la centralità del consenso quale fonte di legittimazione di ogni trattamento, come suggerito sia dall'ordine di indicazione seguito dall'art. 6 del GDPR sia dall'attenzione allo stesso specificamente dedicata nella disposizione immediatamente successiva. Consenso rilevante non solo al momento dell'inizio del trattamento dei dati, ma che trova manifestazione anche nell'esercizio, da parte dell'interessato, di particolari facoltà durante il trattamento stesso, sintetizzate normativamente nei diritti all'accesso ai dati (art. 15 GDPR), alla loro rettificazione (art. 16) o cancellazione (cd. "all'oblio" *ex art.* 17), alla limitazione del trattamento (art. 18) e, infine, alla portabilità dei dati stessi (art. 20).

Come giustamente rilevato dalla Corte di Cassazione[21], il consenso al trattamento è un consenso "rafforzato" rispetto a quello ordinariamente richiesto a fini negoziali, reso necessario in considerazione della intrinseca debolezza del destinatario del trattamento, tanto dal punto di vista dell'asimmetria informativa quanto da quello della potenziale aggressività e suggestione delle pratiche comunicative del digitale. In questo senso, la giurisprudenza pare aver preso le distanze dalla posizione che vede nel consenso al trattamento un atto meramente dispositivo[22]. Il consenso nella *privacy* pare, dunque, possedere un *quid pluris* in qualche modo giustificato dalla intrinseca connessione tra la materia considerata – la protezione dei dati personali, appunto – e la personalità dell'individuo, insuscettibile di una valorizzazione meramente economica[23].

Ciò d'altronde risulta confermato dalla Dir. 2019/770/UE, che al considerando n. 24, pur ammettendo la potenziale azionabilità dei rimedi contrattuali nel caso in cui la cessione delle informazioni personali diventi oggetto di una prestazione negoziale[24], riconosce "*appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce*". Come già visto sopra, inoltre, la Direttiva mantiene ferma l'applicazione ai contratti di fornitura di servizi digitali delle regole del GDPR sul consenso dell'interessato, ivi compresa la revocabilità: in questo modo, continua ad essere salvaguardata una sfera minima di intangibilità e indisponibilità del diritto alla privacy.

Tra l'altro, si è giustamente rilevato[25] che la necessità che vi sia un consenso, e che il consenso presenti determinati requisiti, si giustifica anche in un'ottica collettiva, connessa al regime di circolazione delle informazioni, volta a limitare la raccolta di dati personali in modo da mantenerla entro una corretta e trasparente dinamica di mercato, e pur sempre nel rispetto dei principi di una società democratica[26].

3. I requisiti del consenso al trattamento dei dati personali.

Se nella direttiva *ePrivacy* si rinviene l'obbligo di acquisizione del consenso per l'installazione dei *cookie*, è nel GDPR che devono rintracciarsi i requisiti specifici che il consenso deve possedere perché sia valido. Si evidenzia solo di passaggio che il consenso, lungi dall'essere concetto dal carattere univoco e scontato, è fattore ricco di implicazioni psicologiche ed emotive, che qui non si analizzeranno ma che devono ritenersi presupposte nella scelta normativa dei caratteri che il consenso stesso deve possedere.

Dalla definizione contenuta nell'art. 4 del GDPR si desume che il consenso deve consistere in una manifestazione di volontà "*libera, specifica, informata e inequivocabile*"[27], effettuata mediante di-

[21] Cass., 2 luglio 2018, n. 17278, in *Guida al diritto*, 2018, 20.

[22] Aderiscono a tale impostazione: F. Bilotta, *Consenso e condizioni generali di contratto*, in *Il trattamento dei dati personali,* V. Cuffaro e V. Ricciuto (a cura di), Torino, 1993, vol. II, 91 ss.; P. Manes, *op. cit.*, 62 ss.; G. Oppo, *Sul consenso dell'interessato*, in *Trattamento dei dati e tutela della persona*, cit., 124 ss.; V. Zeno-Zencovich, *Una lettura comparatistica della L. 675/96 sul trattamento dei dati personali*, in *op. ult. cit.*, 169.

[23] Partendo da tale presupposto, vi è chi ha considerato il consenso al trattamento dei dati come atto di tipo autorizzativo, assimilabile al consenso dell'avente diritto, il quale escluderebbe semplicemente l'antigiuridicità di una condotta altrui, senza con ciò tradursi in un atto di disposizione vero e proprio. Cfr., in tal senso: A. Di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in *op. ult. cit.*, 230 ss.; G. Mirabelli, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.,* 1993, 324; S. Patti, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, 456 ss.

[24] In ogni caso, la direttiva lascia agli Stati membri la facoltà di decidere in merito al soddisfacimento dei requisiti in materia di formazione, esistenza e validità di un contratto a norma del diritto nazionale.

[25] Così S. Thobani, *op. cit.,* 115.

[26] Come affermato anche dall'Autorità Antitrust nei provv. nn. 10276, 10277, 10278 e 10279 del 20 dicembre 2001, in *Boll. sett. AGCM* n. 51-52 del 7 gennaio 2002, 148-165.

[27] Il precedente art. 23 del Codice della privacy prevedeva, al terzo comma, che il consenso dovesse ritenersi "validamente prestato" solo se fosse stato espresso liberamente e specifica-

chiarazione o azione positiva dell'interessato[28]. Quest'ultimo ha il diritto di revocarlo in qualsiasi momento "*con la stessa facilità con cui è accordato*" (art. 7, par. 3, Reg.).

Il diritto di revoca *ad nutum* previsto in materia di privacy è giustificato dalla necessità da un lato di garantire all'interessato un controllo sui propri dati, e dall'altro di controbilanciare il potere di chi li tratta, non senza ragioni di protezione collettiva da possibili abusi[29]. Pertanto, che si voglia attribuire

natura contrattuale o meno al consenso al trattamento, questo è sicuramente sempre revocabile[30].

Ai requisiti del consenso corrispondono importanti doveri in capo a coloro che si occupano del trattamento dei dati. Secondo il principio della "responsabilizzazione" (cd. *accountability*), reso centrale dalla recente normativa europea, si impone sia al titolare che al responsabile del trattamento l'adozione di comportamenti attivi, idonei a dimostrare il rispetto di ogni disposizione a tutela dell'interessato, ferma restando la discrezionalità sulla scelta delle precauzioni. In altre parole, il legislatore europeo enfatizza il ruolo della valutazione *ex ante* dei pericoli che possono emergere dall'uso di informazioni personali ed accentua le responsabilità degli autori del trattamento rispetto all'adozione delle soluzioni tecniche, logiche e organizzative necessarie ad evitare eventuali situazioni di rischio[31].

L'articolo 7, paragrafo 1, pone chiaramente in capo al titolare del trattamento l'onere di dimostrare di aver ottenuto preventivamente il consenso dell'interessato, nel rispetto dei requisiti stabiliti dal GDPR[32]. Ciò significa che, in assenza di specifiche previsioni legislative (come quella di cui all'art. 130, co. 3-*bis*, d. lgs. 196/03 per la ricezione di *newsletters* pubblicitarie), non pare invece compatibile con la disposizione la configurazione di un obbligo dell'interessato di opporsi al trattamento, in base ai generali obblighi di buona fede e correttezza o in considerazione degli usi invalsi tra le parti.

In un contesto *online*, il titolare del trattamento potrebbe, in attuazione dell'art. 7, par. 1, conservare le informazioni sulla sessione in cui è stato espresso il consenso, unitamente alla documentazione della procedura di consenso al momento della sessione, oltre a una copia delle informazioni presentate all'interessato in quel momento.

Tra i doveri dei titolari rientrano specifiche formalità che devono essere rispettate per ottenere la decisione sul consenso dell'interessato. Occorre, infatti, che la richiesta di consenso sia comprensibile, semplice e chiara, oltre che chiaramente distinguibile dalle eventuali altre dichiarazioni rivolte all'interessato (art. 7, par. 2, Reg.).

Ciò significa che deve esistere, quanto meno nelle aspettative normative, una piena consapevolezza da parte dell'interessato della equivalenza del proprio comportamento ad un consenso al trattamento dei dati.

Ove il consenso manchi, o comunque il trattamento non rispetti le condizioni normative, quest'ultimo sarà illegittimo, salvo che si versi in una delle ipotesi – tassativamente indicate dall'art. 6 e, per i dati sensibili, dall'art. 9 del GDPR – in cui, data la prevalenza di un altro interesse pubblico o privato, il consenso non risulti necessario. Nel caso di trattamento illegittimo, si prevede la possibilità di attivare una serie di rimedi, sia di natura privatistica (inibitori e risarcitori[33]), sia di tipo amministrativo (in particolare, con sanzioni pecuniarie).

3.1. L'informatezza del consenso

Secondo le indicazioni di cui all'art. 4, dunque, innanzi tutto il consenso deve essere (preventivamente) "informato" su tutte le condizioni riguardanti il trattamento (finalità, tipo di dati, titolare del trattamento, responsabile del trattamento, limiti di esso). Ciò è in linea con quanto era previsto dall'art. 23 del Codice della Privacy, che stabiliva che il consenso fosse validamente prestato ove fossero

mente in riferimento ad un trattamento chiaramente individuato, documentato per iscritto, e fossero state rese all'interessato le informazioni di cui all'art. 13.

[28] Per un approfondimento dei requisiti del consenso al trattamento dei dati si consiglia S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Sarcangelo di Romagna, 2016.

[29] Tali particolari esigenze di protezione giuridica, assenti nei casi più tradizionali di sfruttamento dei diritti della personalità, giustificano una facoltà di revoca così ampia. Sul confronto tra le peculiarità del diritto alla privacy e le condizioni di disponibilità degli altri diritti della personalità, vedi S. THOBANI, *Diritti della personalità e contratto*, cit. 149 ss.

[30] Sulle conseguenze della revoca del consenso sul contratto cui tale consenso accede, vedi S. THOBANI, *Diritti della personalità e contratto,* cit., 187 ss.

[31] Cfr. in questo senso, A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove Leggi Civ. Comm.*, 2017, I, 144 ss.

[32] Ciò è confermato dal considerando 42 del Regolamento, che afferma che "*per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento*".

[33] Quanto al risarcimento del danno, è del tutto pacifico che occorre, per il risarcimento, un danno-conseguenza, e non un mero danno-evento. Aderiscono a tale principio: Cass. civ. sez. III, 20 maggio 2015, n. 10280, reperibile sul sito www.iusexplorer.it; Cass. civ., sez. III, 15 luglio 2014, n. 16133, in *Foro it.*, 2015, I, 120, 162 ss. In ambito europeo, si è stabilito che il danno debba essere "reale e certo", imminente e prevedibile con sufficiente sicurezza, e non "puramente ipotetico e indeterminato" (Trib. UE, 3 dicembre 2015, CN v. Parlamento europeo).

state rese le informazioni di cui all'art. 13 del medesimo codice, analoghe a quelle previste dall'art. 13 del nuovo GDPR[34].

Possono distinguersi, nell'art. 13 del Regolamento, due categorie di informazioni: quelle che riguardano il contenuto e l'estensione del consenso sotto un profilo sia oggettivo che soggettivo (tra cui quelle sulle finalità e modalità di trattamento, l'indicazione del titolare e del responsabile, i destinatari dei dati, il periodo di conservazione degli stessi e l'esistenza di un processo decisionale automatizzato); quelle volte a richiamare l'attenzione dell'interessato sui suoi diritti e a garantire che il suo consenso sia adeguatamente informato in merito all'obbligatorietà o meno del conferimento dei dati.

Si evidenzia come, nell'ambiente digitale, difficilmente l'interessato è in grado di valutare l'estensione e la portata del trattamento dei suoi dati durante la navigazione, realizzato attraverso tecniche spesso altamente specializzate che lo rendono immediato ed impercettibile.

L'informazione, nell'ottica della normativa europea, diventa quindi strumentale alla consapevolezza della decisione, e deve essere concisa, facilmente accessibile e di facile comprensione (considerando n. 58 GDPR). Come vedremo nel prosieguo, proprio nell'ambiente digitale si ammette anche la possibilità che l'informativa sia fornita attraverso due livelli, uno più sintetico ed uno più analitico.

L'informativa non è dovuta se e nella misura in cui l'interessato dispone già delle informazioni (art. 13, par. 4, del Regolamento).

Deve pur evidenziarsi che vi è il rischio che gli interessati, anche se informati, non si rendano realmente conto delle potenzialità lesive dell'impiego dei dati[35]: in tal senso, ad una formale informazione potrebbe non combaciare una reale presa di consapevolezza.

Non a caso, il legislatore prevede, accanto al requisito dell'informazione, anche quello della libertà del consenso, che vedremo più avanti. In questo senso, appare opportuno, per consentire una minima ponderazione dell'interessato, che tra l'informazione e il consenso vi sia un periodo temporale ragionevole, la cui mancanza, in uno con eventuali forme di pressione, potrebbe pregiudicare l'effettiva informatezza e libertà della decisione[36].

3.2. La specificità

Quanto alla *specificità* del consenso, occorre far riferimento al "principio di minimizzazione dei dati" di cui all'art. 5 del GDPR: secondo quest'ultimo, il consenso deve essere "*adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati*". Analogamente l'art. 23, co. 3, del Codice della privacy prevedeva che il consenso, per essere valido, dovesse essere prestato "*specificamente in riferimento ad un trattamento chiaramente individuato*".

Una lettura severa di tale requisito suggerisce che, se un servizio viene utilizzato per una certa finalità, non dovrebbe essere *preteso* un utilizzo dei dati dei suoi utenti a fini diversi da quelli connessi al servizio stesso (relativi al suo funzionamento, ad esempio). Alla specificità è connessa la "granularità" del trattamento, per cui si impone al titolare di prevedere, già alla richiesta del consenso, una differenziazione in ragione delle singole modalità con cui saranno trattati i dati, consentendo all'utente di esprimere le proprie preferenze; occorre evitare, dunque, una richiesta onnicomprensiva del consenso per ogni tipologia di trattamento.

Il Garante ha stabilito, in attuazione del principio della specificità del consenso, che debbano essere indicate separatamente le finalità di fidelizzazione, profilazione e marketing diretto[37], e che debba essere ottenuto un consenso separato per ciascuna di esse[38].

Come correttamente osservato, una manifestazione di volontà generica non permetterebbe "un reale apprezzamento delle concrete conseguenze dell'atto dispositivo", a differenza di un consenso espresso "in maniera distinta e in relazione a ciascuna delle finalità rilevanti", il quale costituisce maggiore garanzia di consapevolezza della decisione presa[39]. Appare evidente che la specificità del consenso è strettamente legata all'informatezza, considerato che una parte degli obblighi di informa-

[34] La disposizione del Regolamento sostituisce solamente l'indicazione delle modalità del trattamento con quelle, più specifiche, relative al periodo di conservazione dei dati oppure ai criteri utilizzati per determinare tale periodo, nonché all'eventuale esistenza di un processo decisionale automatizzato (compresa la profilazione) e alle relative caratteristiche.

[35] Come già rilevato da S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 82.

[36] Come evidenziato, per le carte di fidelizzazione, dal Garante per la protezione dei dati personali, nel provvedimento "'*Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione*" del 24 febbraio 2005, doc. web n. 1103045, in *www.garanteprivacy.it*.

[37] Garante per la protezione dei dati personali, provv. del 24 febbraio 2005, cit.

[38] Garante per la protezione dei dati personali provv. n. 6 del 10 gennaio 2013, doc. web n. 2438949.

[39] G. RESTA e V. ZENO-ZENCOVICH, *Volontà e consenso*, cit., 414.

zione riguarda proprio i limiti oggettivi e soggettivi del trattamento consentito.

3.3. L'inequivocabilità

Il consenso, inoltre, deve essere "inequivocabile", con ciò implicandosi la necessità che esso si concretizzi in un atto chiaro e univoco, non diversamente interpretabile, di manifestazione di volontà affermativa da parte dell'utente. Che un'azione positiva fosse necessaria ai fini del consenso era già stato, d'altronde, precisato anche dall'*Art.29 Data Protection Working Party*, che aveva evidenziato come un atto di rifiuto non si conciliasse bene con il termine "consenso"[40].

Più precisamente, il considerando n. 32 del GDPR dispone che "*il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale".* Si ammette, quindi, la possibilità di esprimere il consenso al trattamento dei dati anche in forma orale, purché in modo percepibile da terzi e con atto inequivocabile[41], diversamente dal Codice della Privacy, che prevedeva la necessità di una forma scritta *ad probationem* o, per i dati sensibili, *ad substantiam*.

Tale previsione va letta in combinazione con l'onere probatorio posto dall'art. 7, par. 1, del GDPR in capo al titolare del trattamento, che dunque non implica la necessaria produzione di documentazione scritta, ma la semplice dimostrazione di un atto inequivocabile di assenso.

Il considerando prosegue precisando che l'atto positivo del consenso "*potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle*". Si tratta, come vedremo fra poco, di una previsione normativa cruciale rispetto alla valutazione della legittimità dei *cookie*.

Per quanto riguarda i dati sensibili[42] di cui all'art. 9 del GDPR, comprensivi dei dati genetici e biometrici, si richiede che il consenso sia "esplicito"[43] – e lo stesso vale per i trattamenti automatizzati, compresa la profilazione *ex art.* 22 – dunque preferibilmente (anche se non necessariamente) per iscritto. Come recentemente precisato dalla Corte di Giustizia dell'UE, il divieto del trattamento di tali dati, in assenza del consenso esplicito, vale anche per i gestori dei motori di ricerca[44].

Considerato che uno dei requisiti del consenso di cui al GDPR è quello della "dichiarazione o azione positiva inequivocabile", e che lo stesso è già di per sé più elevato rispetto a quanto previsto dalla precedente Direttiva 95/46/CE, il carattere "esplicito" del medesimo deve inevitabilmente arricchirsi di ulteriori presupposti. Lo stesso implica certamente una dichiarazione espressa di consenso, ad esempio mediante scritto cartaceo firmato dall'interessato[45].

Nel contesto digitale, l'interessato potrebbe emettere la dichiarazione richiesta compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato con la propria firma oppure utilizzando una firma elettronica, o ancora, più agevolmente cliccando su un tasto digitale come "accetto" o "si", a condizione che vi sia una chiara informativa sul tipo di trattamento accettato e siano rispettate le altre condizioni per la validità del consenso[46].

3.4. La libertà

[40] Article 29 Data Protection Working Party, Opinion 2/2010 sulla pubblicità digitale comportamentale, WP 171 (2010), P. 13.

[41] L'art. 23, co. 1, del Codice della privacy prevedeva, analogamente, che il consenso al trattamento dei dati dovesse essere "espresso", dunque o conferito mediante esplicita dichiarazione, o quantomeno deducibile come certo da circostanze univoche e chiare. Sull'applicazione della disposizione codicistica la giurisprudenza nazionale si è mostrata tutt'altro che pacifica. Cfr. S. THOBANI, *I requisiti del consenso*, cit., 31 ss.

[42] Si tratta di quei dati "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati personali biometrici intesi a identificare in modo univoco una persona fisica, e quelli relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*" (art. 9 GDPR).

[43] L'art. 9, par. 2, del GDPR prevede una serie di altre ipotesi in cui il trattamento di tale categoria di dati risulta legittimo, anche in assenza di un consenso esplicito.

[44] Corte Giust. UE, 24 settembre 2019, C-136/2017 (*GC, AF, BH, ED* contro *Commission nationale de l'informatique et des libertés*).

[45] La contrapposizione europea consenso univoco/consenso esplicito può in qualche modo confrontarsi, anche se non vi corrisponde del tutto, alla precedente contrapposizione nazionale consenso espresso/consenso scritto prevista, rispettivamente, per i dati personali ordinari e per i dati sensibili.

[46] Come precisato dal Comitato Europeo per la protezione dei dati nelle *Linee Guida sul consenso ai sensi del Regolamento (UE) 2016/679*, punti 94 e 96.

Quanto, infine, al requisito della *libertà* del consenso[47], una sua decifrazione attenta alle esigenze valorizzate dalla normativa impone di darvi un significato non troppo "leggero": la medesima non può, come lo stesso tenore della disposizione suggerisce[48], combaciare con la semplice informazione sul trattamento, ma deve arricchirsi di ulteriori caratteri, riassumibili nella mancanza di coartazione e nella piena consapevolezza.

Tra l'altro, come giustamente rilevato[49], a prescindere dalla posizione adottata in merito alla natura del consenso al trattamento dei dati personali, si registra in dottrina una sostanziale uniformità di vedute nel considerare che il richiamo alla libertà del consenso in materia di privacy non sia riducibile all'applicazione delle normali regole del contratto, ma muova dall'esigenza di tenere conto di una più generale posizione di debolezza dell'interessato, oltre che di delicatezza della situazione soggettiva protetta. Così, è stato ad esempio considerato non libero il consenso che "pur non essendo viziato da errore, violenza e dolo ai sensi degli artt. 1427 s. cod. civ., è indotto da pressioni, situazioni di debolezza contrattuale o da altre circostanze che non lo rendono frutto di una determinazione spontanea o consapevole o che lo piegano al raggiungimento di obiettivi che esulano dalla causa del negozio concluso"[50].

Ma ancora, come vedremo nel prosieguo, anche il Garante della Privacy sembra aver consolidato un'interpretazione severa ed articolata della libertà del consenso, la quale deve rimanere al riparo da indebite pressioni.

Pertanto, libero è un consenso non coartato e consapevole. Sebbene si tratti di un concetto dai contorni sfuggenti, pare potersi attribuire un contenuto minimo alla *consapevolezza* in termini di "coscienza" e, *ex adverso*, di "assenza di ogni costrizione fisica o psichica": in ogni caso, elemento imprescindibile della consapevolezza è il fattore razionale, quindi la realizzazione interna, volontaria e cosciente, di una decisione.

Che ciò implichi una minima maturità mentale, soprattutto in certi ambiti più insidiosi come il digitale, è confermato dal fatto che l'art. 2 *quinquies* del Codice della privacy stabilisce che il consenso al trattamento dei dati nell'ambito dei servizi digitali è valido a partire dai 14 anni, mentre prima può essere dato dai genitori o da chi ne fa le veci[51], previo ascolto del minorenne ove capace di discernimento.

Non può non evidenziarsi che, nel contesto digitale del consenso ai *cookie* qui analizzato può ben capitare che la limitazione suddetta rimanga spesso non rispettata, né può tantomeno richiedersi al titolare del trattamento un onere di controllo esorbitante. Il GDPR prevede infatti che il titolare si adoperi "in ogni modo ragionevole" per verificare, nei casi di minore al di sotto della soglia di età minima, che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale, in considerazione delle tecnologie disponibili (art. 8, par. 2).

Ad ogni modo, nella *mens legis*, pare presumersi l'assenza di maturità, di piena consapevolezza e, dunque, di libertà del minore infraquattordicenne[52]. Rimane chiaro che la libertà del consenso del minorenne dovrà in ogni caso essere valutata, prendendo in considerazione le modalità con cui il consenso è stato prestato e le altre circostanze rilevanti in tal senso.

La disposizione codicistica prosegue, statuendo che, in relazione all'offerta dei servizi suddetti, "*il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi*". Il consenso deve, quindi, "significare" qualcosa, e questo significato pare doversi rintracciare proprio nella consapevolezza e libertà della decisione.

Il GDPR manifesta una chiara attenzione al rischio di un consenso indebitamente coartato, indicando taluni requisiti che le richieste di trattamento devono rispettare. Il considerando n. 32 specifica che la richiesta del consenso non deve *interferire immotivatamente con il servizio per il quale il consenso è espresso*. Analogamente, il considerando n. 43 e l'art. 7, par. 4[53] del Regolamento prevedono che il consenso si presume non liberamente espresso ove l'esecuzione di un contratto e la prestazione di un servizio siano subordinate al consenso sebbe-

[47] Questo era previsto anche dal Codice della Privacy, il cui art. 23, co. 2, stabiliva che il consenso al trattamento è validamente prestato solo se è "espresso liberamente".

[48] Una simile lettura, infatti, priverebbe il requisito della libertà di ogni autonomia concettuale rispetto agli altri previsti dalla normativa.

[49] Così S. THOBANI, *I requisiti del consenso*, cit., 44.

[50] Cit. G. BUTTARELLI, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1996, 285.

[51] Si evidenzia che il legislatore europeo ha stabilito, quale età minima per la validità del consenso dei minori, i 16 anni, lasciando agli Stati la possibilità di stabilire un'età inferiore, non minore di 13 anni (art. 8, par. 1, GDPR).

[52] Per un approfondimento del tema della capacità dei minorenni rispetto alla prestazione del consenso al trattamento, si rinvia a: S. PATTI, *Sub art. 23*, in *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («codice della privacy»)*, C.M. Bianca, F.D. Busnelli (a cura di), Padova, 2007, I, 544 ss.; S. THOBANI, *I requisiti del consenso*, cit., 17 ss.

[53] L' art. 7, par. 4, del GDPR, non vieta in assoluto di subordinare l'esecuzione di un contratto o la prestazione di un servizio al consenso al trattamento, ma impone di tenere tale circostanza nella "massima considerazione". Ciò può rappresentare una ulteriore conferma della negoziabilità dei dati commerciali.

ne esso non sia necessario per le stesse (pratiche cd. di "tying"); tale indicazione risulta in linea con gli orientamenti già precedentemente espressi dal Garante per la protezione dei dati personali a proposito della libertà del consenso, come vedremo più avanti.

Ancora, il considerando n. 42 evidenzia che il consenso non dovrebbe essere considerato liberamente espresso se l'interessato *"non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio"*.

Si tratta di disposizioni che, formulate in generale per ogni forma di trattamento, possono ritenersi ben applicabili al caso dei *cookie* e della relativa richiesta di consenso contenuta nei banner informativi. Ciò trova conferma, come vedremo nel prosieguo, nelle recenti Linee Guida "in materia di cookie ed altri strumenti di tracciamento" del Garante per la protezione dei dati personali.

E' dato di comune coscienza che in molte circostanze, soprattutto nel mondo digitale, al consenso non si accompagni quella base di consapevolezza e libertà ritenuta necessaria dalla disciplina in materia di privacy. In altre parole, il consenso inteso come *atto* non corrisponde sempre al consenso inteso come *atteggiamento*, dunque ad una reale volontà. Come detto sopra, infatti, occorre verificare se la decisione affermativa sia frutto di un effettivo percorso libero del soggetto agente: tale percorso spesso è compromesso in ragione della difficoltà conoscitiva dell'individuo, il quale, oltre che venire a contatto continuamente con una pluralità di trattamenti e di richieste di consenso, non è sempre in grado di comprendere a pieno l'informativa ricevuta, tenendo conto anche delle modalità in cui questa è fornita.

Laddove manchi una reale consapevolezza da parte dell'interessato, ritenere che il semplice consenso-atto prescinda dall'esigenza di una necessaria, effettiva, informazione della decisione sul trattamento rischierebbe di rendere la libertà informata di autodeterminazione una mera illusione.

Lo stesso vale, evidentemente, per tutte le ipotesi digitali in cui il consenso dell'utente è "estorto" attraverso forme di indebita pressione, come i *banner* forzatamente inseriti nella pagina di navigazione o le altre forme di consenso al trattamento in qualche modo imposte all'utente.

Che ciò non sia in linea né con una libertà di autodeterminazione né con una effettiva informazione – elementi centrali per esaminare la legittimità di un trattamento – appare con evidenza ad ogni osservatore. I *cookie*, in questi termini, rappresentano forse il fenomeno più delicato e rischioso, e per questo occorre una loro adeguata considerazione giuridica.

4. *Cookie* e consenso al trattamento dei dati personali

Uno degli strumenti più diffusi all'interno del panorama digitale è certamente quello dei *cookie,* presenza ormai costante in ogni sito visitato dagli utenti del web[54].

La ricerca competitiva dell'attenzione dei consumatori *online* ha indotto le imprese a fornire, mediante la piattaforma digitale, servizi sempre più ritagliati sulle preferenze del singolo cliente, onde incrementare le proprie possibilità di vendita. In questo senso, i *cookie* rappresentano il principale strumento con cui le imprese raccolgono i *big data*, con particolare attenzione alle abitudini personali e alle preferenze dei diversi consumatori.

Dunque, l'evoluzione tecnologica ha aperto nuove vie alla profilazione degli individui, attraverso il monitoraggio delle loro attività nel contesto telematico e l'accumulo, sempre crescente, delle relative informazioni[55]. E ciò non solo da parte degli operatori del mercato, ma anche dei soggetti pubblici, non senza stimolare ulteriori, importanti, dibattiti tra gli studiosi della materia.

Un riferimento ai *cookie* è contenuto nel considerando n. 30 del GDPR, il quale prevede che "*le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*".

[54] In dottrina, a proposito dei cookie vedi: M. Borghi, F. Ferretti e S. Karapapa, *Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK*, in *International Journal of Law and Information Technology*, Vol. 21, 2, 2013, 109 ss.; D. Clifford, *Consent and the Cookie Monster - Tracking the crumbs of online user behaviour*, *JIPITEC*, 194, 2014, par. 1; N. van Eijk, N. Helberger, L. Kool, A. van der Plas e B. van der Sloot, *Online tracking: questioning the power of informed consent*, in *Info*, Vol. 14 No. 5, 2012, 57 ss.; A. Mantelero, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies*, in *Dir. informatica*, fasc. 4-5, 2012, 781; A. Reinalter e S. Vale, *Cookie e consenso dell'utente (commento a sent. CGUE 1 ottobre 2019 in C-673/17)*, in *Giur. It.*, 8/9, 2020, 79 ss.; E. M. Tripodi, *A proposito di privacy: le informative dei siti web*, in *Disc. comm. e servizi*, 2020, I, 9 ss.;

[55] Sulla natura di dato personale delle informazioni raccolte attraverso il tracciamento online cfr. Article 29 *Data Protection Working Party*, Parere n. 2/2010 sulla pubblicità comportamentale online, adottato il 22 giugno 2010, p. 3.

I *cookie*, in particolare, possono definirsi come "piccoli file di testo che i siti visitati dagli utenti inviano ai loro terminali, ove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla visita successiva"[56]. In questo modo, il sito invia all'utente una sorta di captatore di informazioni personali le quali vengono poi recuperate dal sito il quale le utilizza o per studi di settore o per profilare i contenuti proposti ad ogni singolo utente secondo le preferenze manifestate durante la navigazione web[57].

I "*cookie* tecnici" sono quelli utilizzati dal fornitore di un servizio al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica e di fornire all'utente i propri servizi (art. 122, co. 1, del Codice). Essi sono direttamente installati dal gestore del sito visitato e non vengono utilizzati per scopi ulteriori rispetto a quelli necessari per l'uso del sito. Possono essere suddivisi in: "*cookie* di navigazione", che garantiscono la normale navigazione e fruizione del sito web (permettendo, ad esempio, di realizzare un acquisto o autenticarsi per accedere ad aree riservate); "*cookie* di funzionalità", i quali consentono la navigazione in funzione di una serie di criteri selezionati (ad esempio, la lingua, i prodotti selezionati per l´acquisto) al fine di migliorare il servizio reso ai singoli utenti; "*cookie analytics*", assimilati ai *cookie* tecnici laddove utilizzati direttamente dal gestore del sito per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come questi visitano il sito stesso. Quanto a questi ultimi, come precisato recentemente dal Garante, la loro identificazione come cookie tecnici può aversi solo a condizione che non si pervenga, mediante l'utilizzo degli stessi, alla diretta individuazione dell'interessato (cd. *single out*), come nel caso della produzione di statistiche aggregate.

Per l'installazione dei *cookie* tecnici non è richiesto il preventivo consenso degli utenti, salvo restando l'obbligo di dare l´informativa ai sensi dell´art. 13 del Codice, che il gestore del sito, qualora utilizzi soltanto tali dispositivi, potrà adempiere con le modalità che ritiene più idonee.

Diversa è la categoria dei "cookie di profilazione", così chiamati perché volti a creare profili relativi all'utente, solitamente utilizzati al fine di inviare messaggi pubblicitari (ma non solo) in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete[58].

Un particolare tipo di *cookie* sono, infine, i "*cookie* delle terze parti", i quali sono impostati da un sito web diverso da quello che l'utente sta visitando, in grado di captare le informazioni rilasciate da quest'ultimo. In tal caso, dunque, ad ottenere ed utilizzare i dati non è (quanto meno non solamente) il sito visitato, ma terzi soggetti che dal sito traggono informazioni utili per la propria attività: si tratta, principalmente, di imprese con finalità di marketing.

Per quanto riguarda le ultime due categorie di *cookie* (quelli di profilazione di prime e di terze parti), la loro installazione necessita del consenso dell'utente, la sussistenza dei cui requisiti - necessari per rendere il trattamento dei dati personali legittimo – deve opportunamente valutarsi ponendo attenzione alle particolarità di tale specifica modalità di trattamento dei dati. Dunque, in quanto strumentali al trattamento dei dati, i *cookie* saranno soggetti alle regole (alcune delle quali viste sopra) previste in generale dal GDPR, a cui si aggiungono talune particolari disposizioni che, nella sostanza, non ne mutano il regime giuridico.

L'articolo 22, par. 2, lettera *c)*, del *GDPR*, stabilisce che "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*". In questo modo, si ribadisce la necessità di un preventivo consenso dell'utente nel caso in cui il trattamento consista nella sua profilazione, con la precisazione che il consenso deve essere anche "esplicito" nel senso visto sopra, dunque comunicato mediante dichiarazione espressa, ancorché in una forma digitalizzata.

La necessità di un preventivo consenso alla profilazione è ribadita dall´art. 122 del Codice della Privacy, introdotto dalla Dir. 2002/58/CE, laddove prevede, analogamente all'art. 5, par. 3 della Direttiva, che "*l´archiviazione delle informazioni nell´apparecchio terminale di un contraente o di un utente o l´accesso a informazioni già archiviate sono consentiti unicamente a condizione che il con-*

[56] Definizione presa dal sito del Garante per la Privacy, consultabile al link seguente https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3585077.

[57] Una definizione alternativa dei cookie è quella data dalla Corte di Giustizia dell'Unione Europea, secondo cui essi sono "strumenti utilizzati per raccogliere informazioni generate da un sito web e salvate da un browser di un utente internet, che consentono al medesimo di memorizzare le azioni o le preferenze dell'utente nel corso del tempo" (v. CGUE, 5 giugno 2018, C-210/16; CGUE, 13 febbraio 2014, C-466/12).

[58] Il GDPR definisce la "profilazione" come "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*" (art. 4, n. 4).

traente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13, comma 3".

Mediante tale disposizione, introdotta dalla Dir. 2009/136/CE, è stata stabilita per i *cookie* la regola dell'*opt-in* fatta propria, successivamente, dal *GDPR*: in base ad essa, il consenso non può essere prestabilito da parte di colui che tratta i dati, ma deve essere di volta in volta conferito dall'utente per ogni specifico trattamento. In altre parole, non si ammette che si pre-configuri l'accettazione del trattamento da parte del gestore di un sito.

Come giustamente rilevato, deve tenersi presente che la nozione di "informazioni" di cui alla disposizione suddetta va intesa in senso esteso, non riferita alle sole informazioni sui dati personali, poiché "l'aspetto rilevante non è l'informazione in sé, bensì la sfera privata che viene individuata nell'ambito di impiego del dispositivo di comunicazione"[59].

Quanto alle "modalità semplificate" di informazione, si tratta di forme di volta in volta stabilite dal Garante con proprio provvedimento.

Ancora, l'art 5, par. 3, della Direttiva *ePrivacy* consente l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un utente - quindi il trattamento mediante *cookie* - "*unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE*[60] *e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento*".

In sintesi, accanto alla imprescindibile informazione preventiva, chiara e completa, la disposizione precisa la necessità di assicurare all'utente anche la possibilità di rifiutare il trattamento mediante i *cookie*, non sempre garantita nella prassi, tantomeno con le stesse modalità con cui è dato il consenso, come invece richiesto dall'art. 7, par. 3, del *GDPR*.

A conferma dell'importanza e della complessità del fenomeno dei cookie, il Garante per la protezione dei dati personali ha introdotto dapprima un documento su "*Informativa e consenso per l'uso dei cookie*"[61], nel 2014 un ulteriore provvedimento generale sull'"*Individuazione delle modalità semplificate per l'informazione e l'acquisizione del consenso per l'uso dei cookie*"[62], e nel giugno 2021 le "*Linee Guida sull'Utilizzo di cookie e di altri strumenti di tracciamento*" [63]. Queste ultime hanno preso spunto dalle *Linee Guida n. 5/2020 sul consenso ai sensi del Regolamento UE 2016/679*, emanate dal Comitato Europeo per la protezione dei dati il 4 maggio 2020.

Le suddette fonti introducono importanti precisazioni in merito al rispetto dei limiti normativi al trattamento nel contesto digitale, con chiarimenti su numerosi profili coinvolti nel fenomeno dei *cookie*. Per tali ragioni, le stesse saranno oggetto di analisi nel prosieguo della trattazione.

Deve evidenziarsi che nella maggior parte dei siti internet odierni la richiesta di accettare i *cookie* (anche non tecnici), contenuta nel *banner* della pagina web, oltre a risultare spesso priva delle minime informazioni necessarie al consenso, si pone quale condizione per usufruire del sito internet. In alcuni casi ciò avviene in modo espresso e/o comunque palese, non essendo consentito materialmente l'accesso ad alcun *link* del sito visitato; in altri, invece, il condizionamento è più velato, traducendosi in un sostanziale disturbo continuo, da parte del *banner*, della navigazione del sito internet da parte dell'utente.

Non meno rilevante è, poi, la circostanza che quello dei *cookie* rappresenta pur sempre un trattamento per il quale il consenso risulta estremamente semplificato, consistendo in un semplice *click*. Tra l'altro, anche l'estetica del banner può assumere un ruolo nell'indurre un determinato comportamento degli utenti: secondo l'approccio della *privacy by design* – come sottolineato anche dal Garante nelle recenti Linee Guida – deve evitarsi che la decisione circa il consenso sia influenzata, come spesso avviene, da scelte estetiche del gestore del sito che spingano, in ragione dei caratteri utilizzati, a preferire l'accettazione del trattamento.

In altre parole, come suggerito da taluni studiosi[64], l'informazione sui *cookie* dovrebbe essere facilmente accessibile e comprensibile, non nascosta in un *link* in fondo a un pagina che fa riferimento ad una vaga e illeggibile politica di privacy. Peraltro, il considerando 25 della Direttiva *ePrivacy* stabilisce che gli avvisi dovrebbero essere visualizzati in modo "chiaro e completo". L'*Article 29 Data Protection Working Party* ha ritenuto "chiaramente non sufficienti" dichiarazioni informative del tipo "gli

[59] Così A. MANTELERO, *Si rafforza la tutela dei dati personali,* cit. 784.

[60] Il richiamo alla Direttiva 95/46/CE deve ormai intendersi riferito al GDPR.

[61] Cfr. al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3585077.

[62] Cfr. al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3118884.

[63] Cfr. al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876.

[64] Come evidenziato da N. VAN EIJK, N. HELBERGER, L. KOOL, A. VAN DER PLAS e B. VAN DER SLOOT, *op. cit.*, 57 ss.

inserzionisti e altre terze parti possono anche utilizzare i propri cookie o tag di azione"[65].

Sembra, dunque, essere necessaria una maggiore chiarezza e specificità dell'informativa sui *cookie*, la quale deve, sin dall'accesso al sito, rendere (quanto meno in potenza) l'utente edotto dei diversi trattamenti che il sito e gli eventuali terzi effettueranno rispetto ai suoi dati.

In questo senso, non pare sufficiente un'accettazione effettuata in generale attraverso l'opzione di default del *browser* utilizzato, in quanto non chiarisce se il mantenimento di tale opzione derivi da una scelta consapevole o sia solo segno di indifferenza o inconsapevolezza. A ciò si aggiunga che, in questo caso, verrebbero altresì a mancare la specificità del consenso e la natura informata dello stesso rispetto al trattamento posto in essere attraverso l'impiego dei diversi *cookies* installati.

Altrettanto importante è, poi, il fattore temporale del consenso. Sul punto pare condivisibile l'interpretazione restrittiva data dall'*Article 29 Data Protection Working Party*, secondo cui occorre comunque delimitare la validità temporale del consenso prestato, fornire adeguate informazioni all'utente e renderlo edotto circa la possibilità di revocare in qualsiasi momento il consenso prestato[66].

In conclusione, come visto finora, il fenomeno dei *cookie*, nella sua singolare complessità, ha destato molteplici attenzioni normative ed istituzionali sotto il profilo del rispetto della privacy.

Esaminato il contesto normativo di riferimento, occorre ora analizzare la posizione delle autorità competenti in materia, dapprima guardando a quella del Garante per poi procedere con le più interessanti interpretazioni date, nelle recenti Linee Guida, dal Comitato Europeo per la protezione dei dati, e dalla Corte di Giustizia dell'Unione Europea in alcune sue recenti sentenze.

5. La posizione del Garante sulla libertà del consenso nel contesto digitale

La ricostruzione della posizione assunta dal Garante per la privacy sulla materia dei *cookie* richiede di far riferimento sia ai provvedimenti generali che l'Autorità nazionale ha specificamente dedicato a quest'ultima, sia a talune decisioni espresse in altri contesti. In particolare, molte pronunce giungono a conclusioni di non poca rilevanza per la materia qui in esame, in particolare per quanto riguarda la questione dell'ottenimento "forzato" del consenso al trattamento dei dati personali.

Una prassi diffusa, come già visto sopra, è quella di subordinare l'utilizzo di un servizio digitale da parte dell'utente alla necessaria prestazione del consenso al trattamento dei suoi dati personali, anche ove non necessari per l'erogazione del servizio medesimo. Il principale strumento utilizzato sono, appunto, i *cookie*.

5.1. La posizione del Garante sul consenso "forzato"

In molte delle sue decisioni, il Garante ha chiamato in causa il requisito della libertà del consenso in casi nei quali, in sede di accesso ad un servizio (principalmente digitale), il fornitore del servizio medesimo chiedeva all'interessato di prestare il consenso al trattamento dei dati per finalità estranee rispetto al servizio offerto, senza specificare in maniera chiara le conseguenze del rifiuto di acconsentire a tale ulteriore trattamento e senza permettere all'interessato la possibilità di prestare consensi separati e facoltativi per ciascuna finalità di trattamento.

In merito alla fattispecie appena menzionata, devono richiamarsi talune considerazioni con cui il Garante ha dimostrato di aver colto, con una certa attenzione, gli elementi cruciali coinvolti nel trattamento dei dati nel contesto digitale. Si tratta di conclusioni che, sebbene estrapolate da un contesto più ampio e in parte diverso, sono pienamente applicabili alla fattispecie dei *cookie*.

Innanzi tutto, il Garante ha stabilito che la capacità di autodeterminazione degli utenti (e quindi la libertà del relativo consenso) non è assicurata quando si assoggetta la fruizione delle prestazioni dedotte nel contratto alla contestuale autorizzazione a trattare i dati conferiti per il medesimo servizio per una finalità diversa, qual è quella promozionale e pubblicitaria[67]. In un'altra occasione[68] il Garante ha, altresì, affermato che il consenso può essere ritenuto effettivamente libero *solo se si presenta come manifestazione del diritto all'autodeterminazione informativa, e dunque al riparo da qualsiasi pressione*, e se non viene condizionato all'accettazione di clau-

[65] Così Article 29 *Data Protection Working Party*, Parere 2/2010 sulla Pubblicità comportamentale online, cit.

[66] Vedi Article 29 *Data Protection Working Party*, Parere 2/2010 sulla pubblicità comportamentale online, cit., dove si evidenzia la necessità che i fornitori di reti pubblicitarie "elaborino modalità per informare periodicamente le persone del monitoraggio in corso".

[67] Così Garante per la protezione dei dati personali, Provv. 27 ottobre 2016, 2016 n. 439, doc. web n. 5687770. Sul tema vedi altresì: Garante per la protezione dei dati personali, Provv. 13 maggio 2015 n. 291, doc. web n. 4337465; Provv. 24 novembre 2016, n. 488.

[68] Garante per la protezione dei dati personali, Provv. 28 maggio 1997, doc. web n. 40425.

sole che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto. Ciò è esattamente quanto avverrebbe *nel caso di un consenso generalizzato e fondato su informazioni generiche o insufficienti, accompagnate dall'esplicita previsione di una possibile rottura dei rapporti contrattuali*[69].

Il Garante ha altresì precisato[70], con riferimento a taluni modelli di informativa per il trattamento dei dati, che la parte relativa alla descrizione delle conseguenze di un eventuale rifiuto di fornire i dati presentava una formulazione non chiara, in quanto lasciava intendere che il diniego del consenso avrebbe potuto comportare la mancata esecuzione di prestazioni che, in verità, potevano essere eseguite comunque, anche in mancanza del consenso e che, dunque, avrebbe dovuto indicarsi come facoltativo il consenso finalizzato ad indagini di mercato, iniziative di marketing o di altro tipo. In tal modo, infatti, i dati personali, conferiti dall'utente per il perseguimento di una determinata finalità oggetto del rapporto contrattuale, vengono di fatto piegati ad un utilizzo diverso dallo scopo originario che ne aveva giustificato la raccolta, in violazione del principio di finalità[71].

In un provvedimento a carattere generale del 2013[72], il Garante ha ribadito che "*il consenso del contraente per l'attività promozionale deve intendersi libero quando non è preimpostato e non risulta — anche solo implicitamente in via di fatto — obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento*". Dunque, non è libero il consenso prestato quando la società condiziona la registrazione al suo sito web da parte degli utenti e, conseguentemente, anche la fruizione dei suoi servizi, al rilascio del consenso al trattamento per la finalità promozionale[73].

Si evidenzia incidentalmente come sulla questione in esame sia intervenuta, con meno rigore, la Corte di Cassazione civile[74], che – in un caso in cui l'offerta di un determinato servizio da parte del gestore di un sito Internet era condizionato al rilascio del consenso all'utilizzo dei dati personali per il successivo invio, da parte di terzi, di messaggi pubblicitari – ha evidenziato la necessità di valutare l'intensità del condizionamento, ritenendolo tanto più sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo "infungibile" ed "irrinunciabile" per l'interessato. Dunque, la Corte ha ammesso che, per un servizio fungibile a cui l'utente possa rinunziare senza alcun sacrificio gravoso, il gestore possa condizionare l'uso del servizio al consenso al trattamento dei dati per finalità pubblicitarie, purché vi sia una informazione chiara ed il consenso sia specificamente prestato per le singole finalità pubblicitarie. Non può non scorgersi il rischio che una simile posizione incentivi la prassi di obbligare l'utente di un servizio a cedere le proprie informazioni, anche quando non necessarie per il servizio stesso, con un sostanziale svuotamento della piena ed effettiva libertà del consenso al trattamento dei dati.

Tornando alla posizione del Garante, dunque, perché il consenso sia considerato "libero" esso non solo non può essere condizione per l'accesso o la fruizione di un servizio, ma deve anche essere manifestato esplicitamente, e non mediante esclusiva conferma di condizioni generali preimpostate.

Si tratta di considerazioni antesignane rispetto a quanto successivamente introdotto dal GDPR ai considerando nn. 32, 42 e 43, oltre che all'art. 7 co. 4, analizzati prima. Esse muovono da una duplice esigenza: da un lato, evitare una concentrazione eccessiva di dati personali in capo ad un unico soggetto privato, idonei a consentirgli la profilazione di molte persone; dall'altro, compensare la disparità, informativa e negoziale, sussistente tra titolare del trattamento e soggetto interessato, la quale, anche grazie all'utilizzo di tecnologie pervasive, può ben indurre ad un consenso privo di adeguata ponderazione[75].

Seppur elaborate in ambiti parzialmente differenti, le medesime considerazioni risultano pienamente valevoli con riguardo ai *cookie*, spesso imposti quale condizione, espressamente o comunque di fatto, per l'accesso e l'utilizzo dei siti. Se applicate rigorosamente, le suddette statuizioni potrebbero risultare idonee a comprimere la gran parte delle modalità applicative dei *cookie* poste in essere dai siti internet odierni.

Tra l'altro, proprio i *cookie* rientrano tra quelle nuove tecnologie verso le quali prima il Garante ed ora anche il Regolamento UE 679/2016 muovono una particolare attenzione, in quanto idonee a determinare "*un rischio elevato per i diritti e le libertà*

[69] *Ibidem*.
[70] Vedi Garante per la protezione dei dati personali, Provv. 8 settembre 1997, doc. web. n. 1055101.
[71] Cosi Garante per la protezione dei dati personali, Provv. 12 ottobre 2005, doc. web n. 1179604.
[72] Garante per la protezione dei dati personali, Provv. 4 luglio 2013, doc. web. n. 2542348.
[73] Sulle questioni più strettamente contrattuali inerenti al rapporto tra la prestazione del servizio e la cessione dei dati, si rinvia a S. THOBANI, *Diritti della personalità e contratto,* cit., 171 ss.
[74] Cass., 2 luglio 2018, n. 17278, cit.
[75] Evidenzia tali profili di rischio S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1984, 763, e ID. *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 600.

delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità" (considerando 89).

5.2. La posizione del Garante nel provvedimento generale del 2014

Con il provvedimento generale sull'"*Individuazione delle modalità semplificate per l'informazione e l'acquisizione del consenso per l'uso dei cookie*" del 2014, il Garante, che pur ha manifestato una approfondita conoscenza tecnica del fenomeno in esame, ha assunto un approccio meno rigoroso rispetto alle modalità di richiesta ed ottenimento del consenso poste in essere nel digitale.

L'Autorità nazionale ha previsto che possa ritenersi una "soluzione efficace" impostare il consenso su due livelli: nel momento in cui l'utente accede a un sito web, deve essergli presentata una prima informativa "breve" (I livello), contenuta in un *banner* a comparsa immediata sulla *home page* (o altra pagina tramite la quale l´utente può accedere al sito), integrata poi da un´informativa "estesa" (II livello), alla quale l'utente può accedere attraverso un *link*. Solo la seconda informativa deve contenere tutti gli elementi previsti dall´art. 13 del Codice, descrivere in maniera specifica e analitica le caratteristiche e le finalità dei *cookie* installati dal sito e consentire all´utente di selezionare/deselezionare i singoli *cookie*[76].

Ai fini della semplificazione, si ritiene necessario che la richiesta di consenso all´uso dei *cookie* sia inserita proprio nel *banner* contenente l´informativa breve. Gli utenti che desiderano avere maggiori e più dettagliate informazioni, e differenziare le proprie scelte in merito ai diversi *cookie* archiviati tramite il sito visitato, possono accedere ad altre pagine del sito, contenenti, oltre al testo dell'informativa estesa, la possibilità di esprimere scelte più specifiche.

Il *banner* contenente l'informativa breve, oltre che ben distinguibile dal resto della pagina visitata, deve in ogni caso contenere le seguenti indicazioni: a) che il sito utilizza *cookie* di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall´utente nell´ambito della navigazione in rete; b) che il sito consente anche l´invio di *cookie* a "terze parti" (laddove ciò ovviamente accada); c) il link all´informativa estesa, ove è possibile differenziare il consenso in relazione ai diversi tipi di *cookie*; d) l´indicazione che alla pagina dell´informativa estesa è possibile negare il consenso all´installazione di qualunque *cookie*; e) che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un´immagine o di un link) comporta la prestazione del consenso all´uso dei cookie[77] (cd. *scrolling down*).

Per quanto riguarda le informazioni richieste, anche nell'informativa breve, si ritiene che quelle suggerite dal Garante siano sufficienti per assicurare una minima consapevolezza agli utenti. Ove chiaramente fornite, infatti, le stesse consentirebbero all'utente di comprendere le possibili modalità di trattamento dei dati che l'uso del sito può comportare e di decidere, mediante accesso all'informativa estesa, a quali *cookie* acconsentire.

E' pur vero che taluni studi sperimentali hanno dimostrato che l'estrema semplificazione del contenuto informativo della richiesta di consenso non consente di raggiungere il risultato auspicato dalla normativa, dunque la scelta consapevole da parte dell'utente: i risultati hanno evidenziato che quest'ultimo spesso non comprende l'informativa, non è consapevole di condividere i propri dati o di quali siano i suoi diritti in materia[78].

Concentrandoci, in particolare, sull'ultima informazione richiesta dal Garante, da essa si evince come quest'ultimo ammetta un'accettazione mediante lo *scrolling down*, dunque con la semplice navigazione nel sito o la selezione di uno qualsiasi dei suoi *link*.

Si precisa che il *banner*, oltre a dover presentare dimensioni sufficienti a ospitare l´informativa, seppur breve, "deve essere parte integrante dell´azione positiva nella quale si sostanzia la manifestazione del consenso dell´utente". In altre parole, secondo il Garante esso dovrebbe "determinare una discontinuità, seppur minima, dell´esperienza di navigazio-

[76] All'interno di tale informativa, deve essere inserito anche il *link* aggiornato alle informative e ai moduli di consenso delle terze parti con le quali l´editore ha stipulato accordi per l´installazione di *cookie* tramite il proprio sito. Qualora l´editore abbia contatti indiretti con le terze parti, dovrà *linkare* i siti dei soggetti che fanno da intermediari tra lui e le stesse terze parti. Non si esclude l´eventualità che tali collegamenti con le terze parti siano raccolti all´interno di un unico sito web gestito da un soggetto diverso dall´editore, come nel caso dei concessionari.

[77] Così riportate nel Provvedimento, consultabile sul sito del Garante al link indicato nella nota 27.

[78] Cfr. O. Ben Shahar e A. Milton, *Simplification of Privacy Disclosures: An Experimental Test*, in *Coase-Sandor Working Paper Series in Law and Economics*, 737, 2016, 1 ss. Gli autori hanno evidenziato che – se è pur vero che in talune ipotesi di concentrazione cognitiva del lettore la comprensione aumenta con una buona presentazione dei materiali – quando l'agente è impegnato in un compito diverso, la presentazione accidentale di informazioni semplificate non influisce sul suo comportamento. In questo senso, auspicabile sarebbe un'informativa da un lato non troppo complessa, ma al contempo non estremamente semplificata, caratterizzata da chiarezza ed evidenza degli elementi decisivi per la scelta dell'utente.

ne: il superamento della presenza del banner al video deve essere possibile solo mediante un intervento attivo dell´utente (appunto attraverso la selezione di un elemento contenuto nella pagina sottostante il banner stesso)".

Non può sfuggire la difficoltà di concepire il *banner* come "parte integrante dell'azione positiva del consenso": basti considerare, tra l'altro, che non proprio il consenso deve raggiungersi con l'"intervento attivo dell'utente", ma semplicemente "il superamento della presenza del banner", come lo stesso Garante deve infine ammettere.

Ad ogni modo, la lettura suddetta – che pure contrastava già con l'art. 23 del Codice della privacy – è stata rivista dal Garante a seguito del *GDPR*, che ha riconosciuto un preciso valore al requisito dell'inequivocabilità del consenso, prevedendo anche un suo necessario carattere esplicito nel caso della profilazione ai sensi dell'art. 22, par. 2, lett. *c)*.

In questo senso, se è pur vero che un consenso "classico" possa essere sostituito, nel contesto informatico, con un comportamento digitale alternativo, rimane escluso – tanto nella lettura più recente del Garante quanto in quella del Comitato Europeo per la protezione dei dati del maggio 2020 – il riconoscimento del valore di accettazione ad un comportamento rientrante nella semplice utilizzazione del sito internet, sia esso consistente nello *scrolling* o nel *click* su elementi della pagina.

5.3. La posizione del Garante nelle "Linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento"

Nella Linee Guida del 10 giugno 2021 "*sull'utilizzo dei cookie e di altri strumenti di tracciamento*", l'Autorità di settore è tornata sulla questione dello *scrolling down*, prendendo in considerazione le disposizioni del GDPR *medio tempore* entrato in vigore e richiamando le Linee Guida emanate a maggio dello stesso anno da parte del Comitato Europeo per la privacy, analizzate nel prosieguo. Le conclusioni indicate nella proposta suddetta hanno trovato una sostanziale conferma nel testo definitivo delle Linee Guida, successivamente approvate il 10 giugno 2021.

Pur richiamando il considerando n. 32 del Regolamento ed ammettendo l'insufficienza, di per sé, dello *scrolling down* a rappresentare un idoneo consenso ai *cookie*, il Garante ha evidenziato come lo stesso possa validamente rappresentare una componente di un più articolato processo di formazione del consenso da parte dell'utente. In altre parole, secondo il Garante, ove lo *scrolling*, combinato ad altri elementi, permetta di registrare presso il server del gestore del sito un evento qualificabile come *azione positiva inequivocabile* dell'utente in termini di consenso, esso deve ritenersi "in linea con i requisiti di legge"[79].

All'utente deve essere quindi consentito di segnalare al titolare del sito, con la generazione di un preciso *pattern*, una scelta inequivoca e consapevole, che sia al tempo stesso registrabile e dunque documentabile, volta a prestare il proprio consenso all'uso dei cookie o di altri strumenti di tracciamento, come richiesto dalle norme vigenti[80].

Tra gli eventi significativi, alla luce del paradigma del "web dinamico", il Garante aveva indicato, nella Proposta delle Linee Guida del 26 novembre 2020, ad esempio "i movimenti del mouse all'interno del sito", a cui "potrebbero corrispondere (…) cambiamenti di stato di specifiche aree del sito (quali cambiamenti di colore, formato, posizione, etc.) e/o delle informazioni in esse presenti, cambiamenti che, in funzione del tipo di evento che li ha generati, potrebbero essere codificati dal sito ed interpretati anche come una forma di registrazione del consenso espresso dall'utente per l'installazione dei cookie"[81].

Deve comunque trattarsi, come precisato, di eventi realizzati in modo tale "da rendere inequivoco anche per l'utente l'effetto finale prodotto dalla propria azione". In altre parole, l'utente medesimo deve poter ricollegare alla propria azione positiva il significato di accettazione del trattamento.

Occorrerebbe valutare, anche analizzando le concrete modalità di funzionamento dei siti, quale possa essere il "più articolato processo di formazione del consenso" delineato dal Garante.

Rimane da chiarire, infatti, come possa dimostrarsi che un'azione digitale dell'utente (tra cui il movimento del mouse, o anche un qualsiasi *click* sulla pagina) diversa dall'accettazione espressa possa diventare consenso se combinata ad eventi di contesto come la modifica del colore, del formato o della posizione di elementi della pagina (richiamati, a titolo di esempio, dall'Autorità nazionale). Ancora più difficoltoso, per il gestore del sito, potrebbe risultare l'onere di provare la consapevolezza, da parte dell'utente, degli effetti autorizzativi delle proprie azioni digitali, come richiesto dal medesimo Garante.

E' più semplice che sia il gestore del sito ad "interpretarli anche come una forma di registrazione del consenso" per l'installazione dei cookie, a meno che non vi siano, all'interno della pagina già conformata all'azione dell'utente, indizi tali da suggeri-

[79] Cfr. Linee Guida, p. 7.
[80] Così nelle Linee Guida, a p. 8.
[81] Così il Garante a p. 7 della Proposta di Linee Guida del 26 novembre 2020.

re chiaramente a quest'ultimo di aver accettato diverse tipologie di cookie, espressamente indicate.

Il sistema ipotizzato dal Garante – che ha tratto certamente spunto dalle Linee Guida del Comitato Europeo, più precise in tal senso – deve pur sempre confrontarsi, da un lato con il requisito del carattere esplicito del consenso alla profilazione *ex art*. 22, e dall'altro con la necessaria specificità del consenso, difficilmente ipotizzabile nel caso di un'accettazione desunta complessivamente da un procedimento articolato di eventi comprensivi di comportamenti dell'utente e di reazioni della pagina web, diversi dall'accettazione espressa di singoli trattamenti.

Nelle medesime Linee Guida, il Garante ha rivolto la propria attenzione anche su altre questioni coinvolte nel fenomeno dei *cookie*. Lo stesso, ad esempio, è tornato sul tema del cd. *cookie wall*, ovvero quel meccanismo, più volte visto analizzato sopra, per cui l'utente è obbligato ad acconsentire ai cookie di profilazione, pena l'impossibilità di usufruire del sito. Il Garante, in linea con i precedenti, ha dichiarato tale trattamento illecito, considerando in particolare l'art. 4, punto 11, del GDPR, facendo salva l'ipotesi in cui il gestore del sito consenta di accedere ad alternative equivalenti anche nel caso di rifiuto dell'utente all'uso dei *cookie*.

L'Autorità nazionale ha inoltre evidenziato l'opportunità di rivalutare la validità dell'acquisizione del consenso mediante *banner* alla luce del principio di specificità di cui all'art. 25 del GDPR. In applicazione di quest'ultimo, il titolare deve garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari alle finalità del trattamento: per cui, in ragione dell'accesso al sito internet, il trattamento deve limitarsi al minimo indispensabile per la fruizione del medesimo, mentre deve essere rimesso interamente all'interessato un effettivo, concreto potere di scelta circa la possibilità di estendere il trattamento ad altre finalità.

In altre parole, l'impostazione predefinita del sito dovrebbe assicurare che "al momento del primo accesso dell'utente a un sito *web*, nessun *cookie* diverso da quelli tecnici" venga installato[82]. Ciò significa che, nel rispetto degli obblighi di *privacy by default*, le possibili decisioni dell'utente devono essere inizialmente tutte preimpostate, escluso per i cookie tecnici, sul diniego all'installazione.

Quindi, l'azione positiva dell'utente al primo accesso al sito deve essere esclusivamente volta al consenso, secondo il sistema di cd. *opt-in*, e non invece al diniego, come invece avviene per i meccanismi cd. *opt-out*.

Per consentire tale soluzione, il Garante suggerisce ai gestori dei siti di applicare un sistema in base a cui l'utente, accedendo alla *home page* (o ad altra pagina) del sito *web*, possa visualizzare "immediatamente un'area di dimensioni sufficienti da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che sta visitando", tramite la quale, pur senza escludere il mantenimento delle impostazioni di *default*, si consenta all'utente l'azione positiva della manifestazione del consenso. Ove l'utente, dunque, decidesse di chiudere tale finestra, ciò implicherebbe l'installazione dei soli *cookie* tecnici – in linea con la normativa, per la quale solo questa categoria di *cookie* non richiede il consenso – e non di quelli di profilazione.

Proseguendo, sotto il profilo contenutistico, il Garante specifica che il *banner* deve includere: i) l'indicazione di una informativa minima relativa al fatto che il sito utilizza *cookie* tecnici e potrà, esclusivamente previa acquisizione del consenso dell'utente, utilizzare anche *cookie* di profilazione o altri strumenti di tracciamento per finalità specificate nel medesimo banner; ii) il link alla *privacy policy*, ovvero ad una informativa estesa posizionata in un *second layer* ove vengano fornite in maniera chiara e completa almeno tutte le indicazioni di cui agli artt. 12 e 13 del Regolamento; iii) l'indicazione che la prosecuzione della navigazione mediante un "atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano…", che produca un evento informatico registrabile, comporta la prestazione del consenso alla profilazione; iv) un comando attraverso il quale sia possibile esprimere il proprio consenso alla profilazione accettando il posizionamento di tutti i cookie o l'impiego di altre tecniche di tracciamento; v) il link ad una ulteriore area dedicata nella quale sia possibile selezionare, in modo analitico, soltanto le funzionalità, le "terze parti" ed i *cookie*, anche eventualmente raggruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire.

Infine, il Garante auspica l'introduzione, all'interno della stessa informativa breve, di un comando che consenta di revocare, anche in blocco, il consenso precedentemente espresso.

Ciò appare in linea con la normativa, che, come visto nel primo paragrafo, include tra i diritti riconosciuti agli utenti quello di revocare il consenso (art. 7 GDPR), secondo il presupposto per cui un consenso irrevocabile non sarebbe un consenso libero. Ne consegue logicamente che, in un sistema in cui il consenso può esprimersi mediante semplice *click*, l'espressione del dissenso debba avvenire nella medesima modalità semplificata.

[82] Così il Garante nelle Linee Guida a pagina 10.

6. I *cookie* alla luce dell'interpretazione del GDPR da parte del Comitato Europeo per la protezione dei dati e della Corte di Giustizia dell'UE

Dopo aver analizzato la posizione dell'autorità nazionale sulla materia dei cookie appare opportuno rivolgere l'attenzione al contesto applicativo europeo.

Come già anticipato sopra, il Comitato europeo per la protezione dei dati ha adottato, con il provvedimento n. 5 del 4 maggio 2020, delle "*Linee Guida sul consenso ai sensi del Regolamento UE/2016/679*", da cui ha preso spunto il Garante per l'emanazione delle Linee Guida in materia di *cookie*.

Come precisato nella relativa parte introduttiva, tali linee guida prendono le mosse dal parere n. 15/2011 del Gruppo di lavoro Articolo 29 sul consenso, ampliandolo ed integrandolo.

Il Comitato Europeo ha innanzi tutto ribadito la necessità di salvaguardare, in ogni trattamento anche digitale, tutti i requisiti del consenso indicati dal *GDPR*.

Quanto alla libertà, si è precisato che essa implica che l'interessato effettui una scelta effettiva ed abbia il pieno controllo sui propri dati. Ne consegue che, se l'interessato "si sente obbligato ad acconsentire oppure subirà conseguenze negative se non acconsente, il consenso non sarà valido"[83]. Dunque, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio. Un esempio di pregiudizio fornito dal Comitato è quello dell'impossibilità di usare un servizio principale per cui il trattamento richiesto (e rifiutato) non risulti necessario: ciò, infatti, si porrebbe in contrasto tanto con l'art. 7, par. 4, quanto con il considerando 43 del GDPR, che stabiliscono, in questa ipotesi, una presunzione di non libertà[84]. Come visto sopra, ad una simile conclusione il Garante per la privacy era pervenuto già ben prima del Regolamento europeo.

In particolare, il Comitato ha ritenuto opportuno chiarire la questione della validità del consenso espresso nell'interazione con i cosiddetti *cookie walls*, estendendo a questi ultimi le medesime condizioni di cui sopra. Più precisamente, il Comitato ha ritenuto non liberamente espresso, e dunque non valido, il consenso espresso mediante un'accettazione dei cookie nel caso in cui il sito web imponga all'utente uno *script* (o *banner*) che blocchi la visualizzazione (e dunque l'utilizzo) del contenuto e faccia apparire solo la richiesta di accettare i cookie con le relative informazioni[85].

In altre parole, se la finestra contenente la richiesta di consenso ai cookie non permetta, fino all'accettazione, l'uso del sito visitato, il consenso non può ritenersi libero.

Quanto ai requisiti della *specificità* e *granularità* del consenso, il Comitato ha ribadito la necessità di consentire all'interessato, di fronte alla richiesta di trattamento dei dati, di scegliere il singolo trattamento con la relativa finalità: anche in questo caso, la libertà del consenso si presume assente ove il titolare del trattamento imponga di esprimere un unico consenso per tutte le finalità, senza consentire una differenziazione delle preferenze[86].

Ad esempio, si ritiene non granulare, e dunque illegittimo, richiedere agli utenti il consenso unitario a utilizzare i loro dati per inviare comunicazioni di marketing tramite posta elettronica e per condividere i dati con altre società del gruppo. In tal caso, si impone una distinzione per tali due finalità, a cui deve conseguire la possibilità per l'utente di esprimere un consenso differenziato[87].

In sintesi, il rispetto del requisito della specificità del consenso di cui all'art. 6, par. 1, lett. *a)*, impone al titolare del trattamento le seguenti condizioni: la specificazione delle finalità come garanzia contro la "function creep", ossia l'estensione indebita delle funzionalità; la granularità nelle richieste di consenso; una chiara separazione delle informazioni sull'ottenimento del consenso per le attività di trattamento dei dati rispetto alle informazioni su altre questioni[88].

Tale impostazione risulta di grande importanza in quanto strettamente strumentale al requisito dell'informazione; occorre, in sostanza, consentire all'interessato di avere contezza del trattamento dei propri dati e di avere il controllo sui medesimi. Da questo deriva che, nel caso in cui il titolare abbia ottenuto il consenso per un certo trattamento, ove intenda utilizzare i dati anche per altre finalità (ad esempio di marketing) deve chiedere all'utente un ulteriore, specifico, consenso.

[83] Così *Linee Guida sul consenso ai sensi del Regolamento (UE) 2016/679*, punto 13.

[84] Ad ogni modo, l'onere della prova riguardo all'articolo 7, paragrafo 4, incombe al titolare del trattamento, secondo quanto previsto, più in generale, dall'art. 7, par. 1 del GDPR. Dunque, se quest'ultimo riesce a dimostrare che il servizio consente di revocare il consenso senza conseguenze negative, ad esempio senza che il livello della prestazione del servizio venga diminuito a scapito dell'utente, allora il consenso deve ritenersi libero.

[85] Cfr. *Linee Guida sul consenso ai sensi del Regolamento (UE) 2016/679,* punto 40.

[86] *Ibidem*, punto 44.

[87] *Ibidem*, punto 45.

[88] *Ibidem*, punto 55.

Proprio con riguardo all'informazione, il Comitato ha precisato che le informazioni valide possono essere presentate in vari modi, ad esempio sotto forma di dichiarazioni scritte o verbali oppure di messaggi audio o video. E' necessario, in ogni caso, che il titolare adotti un linguaggio chiaro e semplice, idoneo a consentire all'interessato di identificare facilmente chi è il titolare del trattamento e di comprendere le specifiche finalità dello stesso[89].

Quanto al requisito dell'inequivocabilità del consenso, il Comitato europeo l'ha interpretato nel senso di una necessaria dichiarazione o, comunque, di una manifestazione attiva da parte dell'utente che possa significare un'accettazione "ovvia" del trattamento[90].

Tornando sul tema delle modalità semplificate di manifestazione del consenso, il Comitato ha stabilito espressamente che "*l'uso di caselle di adesione preselezionate non è valido ai sensi del regolamento*", e che "*il silenzio o l'inattività da parte dell'interessato, così come il semplice procedere all'uso di un servizio, non possono essere considerati una manifestazione attiva di scelta*"[91].

Pur partendo da tale presupposto – che di per sé renderebbe inidonei, in termini di consenso al trattamento dei dati, comportamenti diversi rispetto all'accettazione espressa, sia pure mediante semplice *click* – il Comitato ammette la possibilità per il titolare del trattamento di progettare meccanismi di consenso alternativi, a condizione che gli stessi operino in maniera chiara per gli interessati. In questo senso, la necessaria chiarezza semantica dell'azione digitale esclude, in ogni caso, che la prosecuzione dell'uso normale del sito possa interpretarsi come consenso[92].

In particolare, 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[93].

L'azione con cui viene espresso il consenso deve, infatti, essere distinta da altre azioni.

Appare in linea con tale interpretazione la posizione assunta dal Garante nella recente proposta di Linee Guida vista sopra: in essa si è riconosciuta rilevanza ad azioni quali lo scrolling o il click su elementi della pagina solo nel caso in cui essi si combinino con altri eventi digitali idonei ad identificare, anche agli occhi dell'utente, un consenso al trattamento.

Tra gli esempi di comportamenti digitali che potrebbero, invece, equivalere a consenso il Comitato indica il "far scorrere una barra su uno schermo", il "muovere la mano davanti a una telecamera intelligente", il "ruotare lo smartphone in senso orario o (il) fargli compiere un movimento a otto". E' in ogni caso necessario che all'interessato siano fornite informazioni inequivocabili e che gli sia chiaro che con l'azione in questione acconsente a una richiesta specifica[94].

Il titolare del trattamento deve essere in grado di dimostrare che il consenso è stato ottenuto in questo modo e l'interessato deve poter revocare il consenso con la stessa facilità con cui lo ha espresso (art 7, par. 3). Come suggerito dal Comitato, quando il "consenso viene prestato con un solo click di mouse, un solo scorrimento o premendo un tasto, l'interessato deve, in pratica, poterlo revocare con altrettanta facilità". Si evidenzia come nella prassi ciò avvenga solo di rado, essendo solitamente necessario, per negare un consenso espresso mediante semplice click, seguire operazioni più lunghe e macchinose, quali la modifica delle impostazioni del *browser* per impedire l'installazione, o l'accesso ad altre pagine web, spesso in lingua straniera.

Ancora, se il consenso è espresso attraverso un'interfaccia utente specifica (ad esempio un sito web, un'applicazione o un account protetto), l'interessato deve poterlo revocare tramite la medesima interfaccia elettronica, risultando uno sforzo eccessivo il passaggio a un'altra interfaccia per la sola revoca[95].

Ad esempio, non rispetta l'art. 7, par. 3, del GDPR il titolare che, dopo aver ottenuto un consenso mediante semplice click, imponga, per la revoca, di chiamare un call center. O ancora, dovrebbe ritenersi parimenti illegittimo prevedere un'accettazione generica di tutti i cookie di profilazione con un solo click, imponendo per la revoca la necessità di deflaggare, per ogni singolo trattamento, la relativa casella. Si tratta di condotte molto diffuse nella prassi del digitale, evidentemente volte a disincentivare il dissenso o la revoca di un consenso precedentemente espresso.

Come evidenziato dal Comitato, nel caso in cui il consenso venga revocato, tutti i trattamenti dei dati basati sullo stesso avvenuti prima della revoca (e in conformità con il regolamento) rimangono leciti, salvo l'obbligo del titolare di interrompere le

[89] *Ibidem*, punti 66, 67 e 68.
[90] *Ibidem*, punto 75.
[91] *Ibidem*, punto 79.
[92] *Ibidem*, punto 84.
[93] *Ibidem*, punto 86.
[94] *Ibidem*, punto 85, che prevede, quale istruzione esemplificativa, la seguente: "se fai scorrere questa barra verso sinistra acconsenti all'uso delle informazioni X per la finalità Y. Ripeti il movimento per confermare".
[95] *Ibidem*, punto 114.

attività di trattamento interessate. Quest'ultimo, inoltre, dovrebbe cancellare i dati trattati, ove non sussista un'altra base legittima per il trattamento dei medesimi, come potrebbe essere l'esecuzione di un contratto per cui i dati risultino necessari[96].

6.1. Segue: la posizione della Corte di Giustizia dell'Unione Europea

In conclusione, appare interessante far riferimento a due recenti decisioni della Corte di Giustizia dell'Unione Europea in materia di cookie, le quali suggeriscono, se analizzate congiuntamente, la posizione raggiunta dalla medesima su particolari profili di criticità diffusi nella prassi dei siti internet.

La prima sentenza da analizzare è stata emanata a fine 2019 nel caso "*Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV contro Planet49 GmbH*"[97].

Il caso valutato dalla Corte riguardava un sito online di scommesse che faceva uso di *cookie*, anche di terze parti a fini pubblicitari, la cui accettazione era già stabilita dal gestore mediante la preselezione di caselle.

Il Giudice europeo, dopo aver preliminarmente precisato che i *cookie*, contendo un codice numerico associato ai dati di registrazione forniti dai singoli utenti, rientrano nella nozione di trattamento di dati personali – da ciò conseguendo l'applicazione di tutte le disposizioni previste dal GDPR – si è soffermato sull'interpretazione dell'articolo 5, par. 3, della Direttiva 2002/58. Lo stesso ha quindi osservato che, sebbene tale disposizione preveda esplicitamente che l'utente deve aver «*espresso preliminarmente il proprio consenso*» all'installazione e alla consultazione di *cookie* nella propria apparecchiatura terminale, la stessa non contiene, invece, indicazioni relative al modo in cui tale consenso debba essere espresso. Quest'ultimo, come rileva la Corte, può ben essere dato anche mediante selezione di apposita casella di un sito, come d'altronde previsto dal considerando n. 17 della Dir. 02/28/CE ed implicitamente ammesso dal legislatore italiano all'art. 122, co. 2, Cod. Privacy, che prevede un consenso mediante programmi o dispositivi informatici di facile e chiara utilizzabilità.

Nonostante ciò, prosegue la Corte, i termini «*espresso preliminarmente il proprio consenso*» si prestano ad un'interpretazione letterale secondo cui un'azione dell'utente è necessaria per esprimere il suo consenso[98], non bastando in questi termini un atto di negazione.

A tale proposito, dal considerando 17 della Direttiva 2002/58 emerge che il consenso dell'utente, ai fini della normativa, può essere fornito secondo qualsiasi modalità appropriata che consenta allo stesso di esprimere liberamente e in coscienza di causa i suoi desideri specifici, in particolare, attraverso la selezione di un'apposita casella nel caso di un sito Internet.

Ancora, data la definizione di consenso come manifestazione di volontà libera, informata e specifica (secondo il GDPR e, analogamente, la precedente Dir. 95/46/CE) – come altresì confermato dall'Avvocato Generale – "*il requisito della «manifestazione» della volontà della persona interessata evoca chiaramente un comportamento attivo e non uno passivo*". Orbene, a parere della Corte, *"il consenso espresso mediante una casella di spunta preselezionata non implica un comportamento attivo da parte dell'utente di un sito Internet*". Solo un comportamento attivo dell'utente mirante alla manifestazione del proprio consenso è idoneo a soddisfare il requisito dell'inequivocabilità richiesto dalla normativa[99].

Ciò significa che – secondo una lettura coerente con i recenti arresti del Comitato Europeo e del Garante della Privacy – il *click* su un qualsiasi *link* o la navigazione sul sito visitato non possono interpretarsi come consenso univoco ai *cookie* non tecnici, in quanto ciò presupporrebbe una pre-accettazione, da parte del gestore del sito, dei *cookie* di profilazione. In particolare, rimane la necessità di un comportamento digitale specifico, separato dal semplice utilizzo di un sito, idoneo ad identificare la volontà dell'utente di accettare uno o più trattamenti mediante cookie.

Accanto al *click* su un apposito tasto digitale chiaramente identificato come accettazione del trattamento, si potrebbero ammettere, come suggerito dalle autorità di settore nazionale ed europea, anche comportamenti diversi, purché preceduti da

[96] *Ibidem*, punto 117.

[97] Corte Giust. UE, 1 ottobre 2019, C-673/2017, ECLI:EU:C:2019:801. Sul tema, cfr. S. El Sabi, *La Corte di Giustizia vieta le caselle di spunta preselezionate per il consenso all'uso dei cookie, nota a sentenza del 19 febbraio 2020*, in *Giustizia Civile.com*, 2/2020; A. Reinalter e S. Vale, *op. cit.*, 79 ss.

[98] Ciò risulterebbe confermato dal fatto la versione iniziale di tale disposizione prevedeva solo il requisito che l'utente avesse la «*possibilità di rifiutare*» l'installazione di *cookie*, dopo essere stato informato in modo chiaro e completo sugli scopi del trattamento. La frase normativa è stata sostituita, appunto, con la formulazione "espresso preliminarmente", in ciò implicando la necessità di un comportamento attivo

[99] La questione della necessaria "attività" del consenso era già stata affrontata in diverse cause da parte della Corte di Giustizia, tra cui: CGUE 24 novembre 2011, C-468/10 e C-469/10, punto 30, nonché CGUE 19 ottobre 2016, C-582/14, punto 57.

un'informativa chiara e seguiti da effetti digitali altrettanto palesi, anche all'utente, in termini di inizio del trattamento dei dati.

Il suddetto orientamento è stato confermato anche in un'altra recente decisione della Corte[100] (causa *Orange România SA* contro *ANSPDCP*), riguardante un contratto relativo alla fornitura di servizi di telecomunicazioni che conteneva una clausola secondo la quale la persona interessata era stata informata ed aveva acconsentito alla raccolta e alla conservazione di una copia del suo documento di identità a fini di identificazione. Il Giudice europeo si chiedeva se il trattamento fosse idoneo a dimostrare che tale persona avesse prestato validamente il proprio consenso, nell'accezione della normativa, a tale raccolta e a tale conservazione.

Rispondendo al quesito, la Corte ha ritenuto che la formulazione dell'articolo 4, punto 11, del *GDPR* consente di affermare la inequivocabile necessità di un consenso attivo, precisando che, sebbene il considerando 32 precisi che l'espressione del medesimo possa essere tra l'altro realizzata mediante la selezione di una casella durante la consultazione di un sito web, esso esclude invece espressamente che configuri un consenso "il silenzio, l'inattività o la preselezione di caselle". La medesima Corte – richiamando le stesse ragioni già addotte dalla decisione precedente e facendo riferimento all'art 7, par. 1 *GDPR*, che pone l'onere probatorio del consenso sul titolare del trattamento – ha concluso in questo modo: "dal momento che, secondo tali indicazioni, non sembra che i clienti interessati avessero essi stessi selezionato la casella relativa a detta clausola, il mero fatto che tale casella sia stata spuntata non è idoneo a dimostrare una manifestazione positiva del consenso di tali clienti a che una copia della loro carta d'identità sia raccolta e conservata". Infatti, a parere della stessa, "la circostanza che detti clienti abbiano sottoscritto i contratti contenenti la casella selezionata non consente, di per sé, di dimostrare un siffatto consenso, in assenza di indicazioni che confermino che tale clausola è stata effettivamente letta e assimilata"[101].

Infatti, secondo il combinato disposto di cui agli artt. 2, lettera *h)*, 7, lett. *a)* della Dir. 95/46, 4, punto 11, e 6, paragrafo 1, lett. *a)* del GDPR, spetta proprio al responsabile del trattamento dimostrare che la persona interessata, mediante un comportamento attivo, ha manifestato il proprio consenso al trattamento dei suoi dati e che la stessa ha previamente ottenuto un'informazione alla luce di tutte le circostanze che corredano tale trattamento, in forma comprensibile e facilmente accessibile e con un linguaggio semplice e chiaro, che le consenta di individuare agevolmente le conseguenze del consenso prestato, affinché sia garantito che questo sia espresso con piena cognizione di causa. Dunque, sul responsabile del trattamento grava un onere probatorio di non poco momento: lo stesso deve dimostrare tanto che il consenso sia stato manifestato mediante un comportamento attivo, quanto che esso sia stato prestato a seguito di una informazione chiara e facilmente accessibile. Solo in questo modo può ritenersi dimostrata, infatti, la "piena cognizione di causa" necessaria a rendere il consenso libero, univoco ed informato.

Ha precisato la Corte, nella prima decisione esaminata, che "non può, infatti, essere escluso che detto utente non abbia letto l'informazione che accompagna la casella preselezionata, o addirittura che lo stesso non abbia visto tale casella, prima di continuare la propria attività sul sito Internet che visita"[102].

Il Giudice eurounitario ha evidenziato altresì che la manifestazione di volontà concretizzante il consenso deve, in particolare, essere "specifica", "nel senso che deve riferirsi precisamente al trattamento dei dati interessati e non può essere desunta da una manifestazione della volontà avente un oggetto distinto". Ciò non si riteneva sussistente nel caso di specie, dal momento che l'attivazione, da parte dell'utente, del pulsante di partecipazione al gioco a premi non poteva essere considerato sufficiente ed equivalente ad un consenso validamente espresso ai fini dell'installazione dei *cookie*.

In questo senso, pare che l'azione positiva non possa essere surrogata – sia per il suo carattere *univoco* che per quello *informato* – da un altro gesto che possa configurare un semplice utilizzo del servizio, come il click su un qualsiasi *link* presente sul sito visitato.

Parimenti, nella decisione più recente sul caso Orange Romania, già richiamata, la Corte ha considerato non idonea a dimostrare il valido consenso dell'interessato la semplice presenza, nel contratto relativo alla fornitura di servizi di telecomunicazione, di una clausola secondo cui l'interessato è stato informato e ha acconsentito al trattamento dei propri dati – nel caso di specie alla raccolta e alla conservazione di una copia del suo documento di identità a fini di identificazione – ove ricorra una delle seguenti circostanze*:* "la casella relativa a tale clausola sia stata selezionata dal responsabile del trattamento dei dati prima della sottoscrizione di tale contratto; le clausole contrattuali di detto contratto possano indurre in errore la persona interessata cir-

[100] Corte Giust. UE, 11 novembre 2020, C-61/19, ECLI:EU:C:2020:901.
[101] *Ibidem*.
[102] Corte Giust. UE, 1 ottobre 2019, C-673/2017, cit.

ca la possibilità di stipulare il contratto in questione anche se essa rifiuta di acconsentire al trattamento dei suoi dati; o la libera scelta di opporsi a tale raccolta e a tale conservazione sia indebitamente pregiudicata da detto responsabile esigendo che la persona interessata, per rifiutare il proprio consenso, compili un modulo supplementare che attesti tale rifiuto".

In considerazione di ciò, deve escludersi che la preselezione di caselle sia idonea a fondare un valido consenso; inoltre, questo non può ritenersi sussistente nemmeno quando l'utente venga indotto – anche per il tramite di procedure complesse o in ogni caso articolate, come la sottoscrizione di moduli aggiuntivi – a ritenere l'accettazione dei *cookie*, senza la distinzione di quelli tecnici, una condizione imprescindibile per l'utilizzo del sito.

La Corte di Giustizie, con le pronunce suddette, ha dunque ribadito come il rispetto di tutti i requisiti del consenso impongano, nel contesto digitale, di dover escludere il valore di accettazione ad ogni attività diversa rispetto alla manifestazione informata (dunque consapevole), libera, specifica ed univoca da parte dell'utente.

Il requisito dell'univocità, in uno con la necessità che il consenso alla profilazione sia esplicito, richiede un comportamento affermativo chiaramente distinguibile rispetto all'uso del servizio scelto. In mancanza di una simile espressione positiva, il trattamento da parte del gestore del sito dovrebbe limitarsi ai semplici *cookie* necessari al suo funzionamento, per i quali non è richiesto il consenso.

Eppure, a ben vedere, la maggior parte dei siti internet – ammettendo un consenso mediane semplice scorrimento della pagina, chiusura del banner o apertura di un qualsiasi link al suo interno – risulta attualmente non in linea con i requisiti suddetti, come stabiliti dal GDPR ed interpretati recentemente dalle autorità competenti. Non può escludersi, infatti, che l'utente, proseguendo con l'uso del sito, non abbia neanche letto l'informativa breve né, dunque, compreso di aver ceduto i propri dati personali.