Per un consenso (veramente) informato: la Corte di giustizia UE inizia l'inversione di rotta

Emilio Girino
Avvocato in Milano – Managing Partner, Studio Ghidini, Girino & Associati – Docente CUOA Finance – già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

Franco Estrangeros
Avvocato in Milano – Partner, Studio Ghidini, Girino & Associati – già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

Trappole della rete e consenso inesigibile: l'urgenza di una svolta

Mentre le bozze del nostro ultimo intervento in questa Rivista[1] stavano per andare in stampa, apparve, con le fattezze di un *δαίμων*, la sentenza della Grande Sezione della Corte di Giustizia dell'Unione Europea nel caso Planet49 [2]. Fummo costretti a riacciuffare le bozze per apporre un *post scriptum*: ciò che auspicavamo nelle ultime righe sembrava essere stato telepaticamente avviato dalla Corte. Un rapido passo indietro. Il menzionato intervento operava un'ampia ricognizione dello stato dell'arte tecnica raffrontandolo all'asimmetria di quello dell'arte giuridica. La navigazione in rete comporta svariati rischi, in termini soprattutto di tracciamento dell'utente e di sua connessa e indesiderata profilazione comportamentale, con conseguente inarrestabile assedio informatico-pubblicitario o, più spesso, vera e propria invasione. *Banner*, *pop-up*,

[1] E. Girino, F. Estrangeros, M. Bedarida, *Liberi di navigare ma senza porti sicuri: perché il diritto soccombe alla tecnologia. Una proposta di inversione*, in *Privacy&, n. 3/2019*.
[2] Sentenza 1 ottobre 2019, Corte di Giustizia dell'Unione Europea (Causa C-673/17) in https://www.garanteprivacy.it/temi/cookie.

trojan e *malware* consimili, algoritmi di decrittazione nei blog e affini non sono che alcuni dei più importuni arieti di sfondamento della riservatezza dell'utente, ma è indiscutibilmente il cookie il grimaldello più efficace anche e soprattutto perché non illegittimo, anzi necessario nella sua mera declinazione tecnica (strumento di interconnessione funzionale fra utente e siti), più subdolo ove indossi il cappello del profilatore a scopi commerciali e no. L'uso del cookie per fini diversi da quelli tecnici è naturalmente sottoposto alle stringenti disposizioni di derivazione unionista (prima la Direttiva 2002/58 e oggi il GDPR del 2016) in punto di consenso libero, specifico, informato e inequivocabile (come recita il Considerando 32 del Regolamento). Tuttavia la disciplina, un po' per sottaciuta connivenza, un po' per tema d'esser aggirata, non s'azzarda a stabilire le precise modalità con cui la libera e cosciente manifestazione volontaristica debba essere acquisita. Nella quotidianità della navigazione in rete prevale ormai la nota prassi di far comparire, in prima visita[3], un'avvertenza in cima o in fondo di pagina, con cui si chiede il consenso dell'utente all'impiego dei cookie, peraltro in svariate declinazioni. I siti che si limitano ad impiegare cookie tecnici e innocui ne danno diretta notizia nel *disclaimer* e chiedono il click sul pulsante "OK" o il consenso (necessario) esprimibile anche soltanto attraverso la mera prosecuzione della navigazione. La più parte dei siti, specie (ma non solo) quelli tipicamente commerciali, ricorrono allo stesso metodo anche se i biscottini servono a profilare l'utente e le sue preferenze. Tutti i siti rinviano ad una lettura delle avvertenze privacy, cui è istantaneo accedere restando invece biblicamente infinito il tempo di una lettura accurata e di una connessa scelta consapevole [4]. In altre parole, il paradigma informativo, (apparentemente) legittimato dal GDPR e in fondo non troppo dissimile da quello pregresso, si traduce in una non-informazione o, se si preferisce, in un'informazione la cui fruizione richiede un comportamento obiettivamente inesigibile e, in fin dei conti, radicalmente antitetico all'eguale e contrario paradigma della velocità di navigazione. Si torna quindi al tautologico e inefficiente modello di pseudo-informazione[5].

[3] E solo in quella se non si siano nel frattempo attivati strumenti di anti-tracciamento o di eliminazione dei cookie a fine navigazione.

[4] Sempre nel nostro menzionato scritto riferivamo gli esiti di una "prova pratica". La visita di 3 siti web – l'uno per comprare una applique, l'altro per un'informazione giornalistica, l'altro ancora per un abbonamento televisivo, dedicando un tempo massimo di 30 minuti ivi inclusa l'accurata lettura delle privacy policy e la cosciente opzione di cosa concedere o meno alla domanda profilativa – restituiva esiti desolanti: i 30 minuti stimati per l'intera operazione risultavano consumati dalla solo parziale e incerta lettura della policy del primo sito.

[5] Icasticamente stigmatizzato da G. Arnò, *Ti informo di averti informato*, in *Privacy&, n. 2/2019*.

Il nostro orizzonte aspirava ad un'inversione di rotta, lungo tre direttrici. Più precisamente:

1. un rovesciamento dell'impostazione tecnica attuale: navigazione di default in totale anonimato legalmente garantito attraverso una "presunzione di rifiuto" alla raccolta e alla profilazione, fatta salva la facoltà del cliente di accettare dei cookie profilativi anche nella prospettiva di fruire di maggiori servizi;
2. l'obbligo dei provider di impedire, nell'impostazione di default o in caso di revoca del consenso, che parti terze (inserzionisti o fornitori di beni e servizi) possano effettuare tracciamenti e di dover cancellare quelli pregressi e di eliminare le ulteriori tracce (comandi vocali, registrazioni, geolocalizzazioni, documenti o immagini);
3. il potenziamento dello strumentario ispettivo e sanzionatorio delle Autorità di controllo con la previsione di periodici e regolari accessi (attivabili in automatico in presenza di fondati reclami dei proprietari dei dati) presso provider e imprese al fine di sorvegliare l'effettivo rispetto della presunzione di rifiuto di profilazione.

In tempi pressoché inattesi, la pronuncia della Corte di Giustizia del 1° ottobre 2019 spiana la via al processo di inversione, sia pur in termini non ancora risolutivi ma, come si noterà, lungo un percorso argomentativo che, muovendo da un'ineccepibile ricostruzione della reale portata delle norme, addita implicitamente sia il vuoto normativo che affligge il sistema attuale sia la sua invocata soluzione.

Il caso di specie e i motivi di rinvio

Il caso risolto dalla decisione in parola vedeva coinvolta una società gerente un sito tedesco di giochi a premi, basato sul rilascio di consenso al trattamento dei dati personali secondo un meccanismo alquanto singolare.
L'utente che intendesse partecipare all'operazione era tenuto a fornire il proprio codice postale venendo così automaticamente reindirizzato ad altra pagina in cui si richiedeva l'inserzione di nome e indirizzo. In calce a tale pagina comparivano due "didascalie" accompagnate da altrettante caselle di spunta.
Con la spunta della prima casella l'utente acconsentiva a ricevere informazioni per posta, per telefono, per posta elettronica o via SMS da sponsor e partner di Planet49. I termini sponsor e partner incorporavano un link rimandante ad un elenco nel quale comparivano i nominativi di varie imprese che l'utente aveva facoltà di eliminare: in caso di eliminazione mancata

o effettuata in "numero insufficiente", la scelta dei partner legittimati ad inviare messaggistica commerciale sarebbe stata effettuata autonomamente dal gestore del sito per un massimo di 30 nominativi.
La seconda didascalia recava invece una casella di spunta preselezionata, con la quale l'utente accettava – in tal modo per *default* – di sottoporsi ad un servizio di analisi web (denominato Remintrex), in forza del quale il gestore del sito avrebbe installato cookie finalizzati a verificare le navigazioni web dell'utente e le visite ai siti Internet dei partner commerciali e ad inviare pubblicità coerente agli interessi così identificati. Il tutto seguito da un invito a verificare ulteriori dettagli con consueto link "qui". Tale ultima connessione, se cliccata, portava all'evidenziazione di un ulteriore *disclaimer* nel quale si avvertiva l'utente circa la natura dei cookie specificandosi che, a seguito dell'installazione così autorizzata, le visite del sito di uno dei partner avrebbero comportato l'automatico rilevamento delle visite stesse, del prodotto per il quale l'utente avesse mostrato interesse o che avesse eventualmente acquistato. Seguivano rassicurazioni sulla possibilità di revocare il consenso, sul fatto che le informazioni sarebbero state impiegate esclusivamente per la pubblicità dei prodotti dei partner pubblicitari, l'esclusione di profilazione dell'utente destinata a più partner pubblicitari, il fatto che i partner non avrebbero ricevuto dati personali, la facoltà di cancellazione dei cookie via browser, l'assenza del rischio che i cookie potessero esportare programmi o trasferire virus.
La partecipazione al gioco, si legge testualmente nella sentenza, era possibile "*solo dopo aver selezionato quanto meno la prima casella di spunta*" (enfasi nostre).
In sintesi, il meccanismo di adesione imponeva all'utente, per un verso, di spuntare la prima casella, dunque di aderire ad una richiesta di invio di messaggi e materiale promozionale da parte degli sponsor del gestore con la facoltà di limitarne il numero attraverso una mirata eliminazione di una quantità sufficiente (ma apparentemente non specificata) di nominativi (prima casella da selezionare), mentre, per altro verso, accordava la facoltà all'utente di rifiutare una vera e propria profilazione (al di là del fatto che tale effetto venisse negato nel *disclaimer*) solo deselezionando la seconda casella già preselezionata.
Una federazione consumeristica, dopo aver inutilmente diffidato la società gerente, proponeva azione di fronte al Tribunale del Land di Francoforte sostenendo che entrambe le condizioni sarebbe state contrarie alle norme civilistiche e settoriali riguardanti la formazione del libero consenso e chiedendone l'inibitoria. Richiesta parzialmente accolta dal Tribunale. La decisione veniva appellata da Planet49 dinanzi al Tribunale superiore del

Land di Francoforte (*Oberlandesgericht Frankfurt am Main*), che ribaltava il verdetto del primo grado osservando come, in considerazione della sufficiente chiarezza grafica del *disclaimer*, l'utente fosse a conoscenza della possibilità di deselezionare la casella del "consenso". La federazione ricorreva quindi per la cassazione (*Revision*) della pronuncia di secondo grado dinanzi alla Corte federale di giustizia (*Bundesgerichtshof*). Quest'ultima riteneva necessaria una corretta interpretazione del combinato disposto dell'articolo 5, paragrafo 3, e dell'articolo 2, lettera f), della Direttiva 2002/58, dell'articolo 2, lettera h), della Direttiva 1995/46, nonché dell'articolo 6, paragrafo 1, lettera a), del GDPR. Di conseguenza, la questione veniva sottoposta al vaglio della Corte di giustizia proponendo due distinti e articolati quesiti.

Il primo espresso nei seguenti termini:

a. se sussista un consenso efficace ai sensi dell'articolo 5, paragrafo 3, e dell'articolo 2, lettera f), della Direttiva 2002/58, in combinato disposto con l'articolo 2, lettera h), della Direttiva 1995/46, nel caso in cui la memorizzazione di informazioni ovvero l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un utente siano consentiti tramite una casella preselezionata che l'utente deve deselezionare per negare il suo consenso;
b. se, ai fini dell'applicazione dell'articolo 5, paragrafo 3, e dell'articolo 2, lettera f), della Direttiva [2002/58], in combinato disposto con l'articolo 2, lettera h), della Direttiva 1995/46, la situazione differisca nel caso in cui le informazioni archiviate o consultate consistano in dati personali o no;
c. se, in presenza delle circostanze indicate nella prima questione pregiudiziale, [lettera a),] sussista un consenso efficace ai sensi dell'articolo 6, paragrafo 1, lettera a), del GDPR.

Il secondo quesito era invece così formulato: quali informazioni debbano essere comunicate dal fornitore di servizi all'utente, affinché quest'ultimo sia informato, in termini chiari e completi ai sensi dell'articolo 5, paragrafo 3, della Direttiva 2002/58 e se, fra tali informazioni, rientrino altresì la durata della funzione dei cookie e il fatto che terzi abbiano accesso ai cookie stessi.

Lo snodo argomentativo della sentenza: a) la ricognizione del quadro normativo

La risposta ai quesiti[6] è preceduta da un'efficace ricostruzione del quadro normativo di riferimento, che vale la pena di sinteticamente richiamare con specifico riferimento alla tematica del consenso, aggiungendovi qualche nostra nota di precisazione. La decisione richiama *in primis* le definizioni contenute nell'art. 2 della Direttiva 1995/46[7] sulla nozione di dati personali[8], di trattamento[9] e di consenso dell'interessato, quest'ultimo da intendersi come "qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento", non senza rammentare che, ai sensi dell'art. 7, siffatta manifestazione di consenso deve essere "inequivocabile". In coerenza alla premessa, ai sensi della Direttiva 2002/58[10] la Corte evoca due Considerando (17 e 24) troppo spesso "dimenticati" in fase applicativa. Il Considerando 17, in particolare, tocca il nervo scoperto dell'intero sistema là dove esso afferma che "il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet".

[6] Risposta che presupponeva la preliminare risoluzione di un problema di successione di norme nel tempo. I fatti oggetto di lite risalivano a data anteriore all'entrata in vigore del GDPR e si riferivano anche a una Direttiva (1995/46) abrogata dal primo a decorrere dal 28 maggio 2018, mentre il quesito evocava anche il nuovo Regolamento. La "diacronia" normativa viene tuttavia agevolmente superata dalla Corte (pur demandando al giudice del rinvio la decisione finale), in ragione della natura del provvedimento inibitorio, come tale proteso ad assicurare l'efficacia della decisione anche in futuro, dunque in piena vigenza del GDPR.

[7] Si tratta della Direttiva "madre" sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla loro libera attuazione, alla quale lo Stato Italiano diede attuazione con la pubblicazione della ben nota legge 675/1996 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".

[8] "Qualsiasi informazione concernente una persona fisica identificata o identificabile ('persona interessata'); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".

[9] "Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione".

[10] Si tratta della Direttiva pubblicata il 31 luglio 2002, con specifico riferimento al "Trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche" e più nota con la definizione "Direttiva relativa alla vita privata e alle comunicazioni elettroniche".

In tutta evidenza, la disposizione, introducendo la possibilità di assentire tramite la spunta (selezione) di una casella, si trasforma in una locuzione ambigua sulla quale, si noterà, finiscono con l'incentrarsi gli sforzi interpretativi della Corte.

Non minor rilievo assume il Considerando 24, a mente del quale nella "sfera privata dell'utente" ricadono non solo, come ovvio, le apparecchiature terminali dell'utente stesso, ma anche "*qualsiasi informazione archiviata in tali apparecchiature*". Il Considerando in parola dà altresì atto della possibilità che software spia, bachi invisibili (cc.dd. *web bugs*), identificatori occulti ed altri dispositivi analoghi possano introdursi nel terminale a insaputa dell'utente per catturare dati, archiviare occultamente nuove informazioni o tracciare l'utente stesso potendo con ciò "*costituire una grave intrusione nella vita privata*".

A suo turno, l'articolo 5, co. 3, della Direttiva in parola impone agli Stati membri d'assicurare che "l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della Direttiva 95/46, tra l'altro sugli scopi del trattamento".

D'acchito quasi privo di spessore, il combinato disposto del Considerando 24 e dell'art. 5 cit. nasconde, se letto con la dovuta lucidità, un'innegabile regola positiva. Così grezzamente riassumibile: se il terminale è mio e se ciò che ci sta dentro è mio, anche ciò che i terzi v'immettono, pur senza il mio permesso, diventa mio. *Ergo*, la proprietà dei cookie malevoli e non espressamente permessi, è parimenti mia, sicché è mio anche il diritto di neutralizzarli. Non diversamente da quanto accadrebbe se qualcuno, Stato compreso, immettesse illegittimamente in casa mia microspie o altri invasivi strumenti. Posto che ciò che è mio è mio e ciò che, senza il mio consenso o il salvacondotto d'una superiore legge, viene introdotto in casa mia parimenti diventa mio, il mio diritto si estende non soltanto alla protezione del "mio originario" ma anche del "mio illegalmente introdotto" fra le mie mura. Ne consegue il mio diritto non solo di espellere ciò che è stato inserito in casa mia (nel gergo dei detective: "bruciare le spie") ma anche di adottare accorgimenti che ne impediscano la reintroduzione: antica teoretica degli *offendicula*, sui quali i nostri amici penalisti potrebbero intrattenerci a lungo ma con la certezza di non doversi misurare col sacrosanto principio di equilibrio fra beni materiali e vita umana, bensì fra equivalenti beni costituiti da dati informatici, ovverosia, in quanto tali, così come liberamente scambiabili, altrettanto liberamente distruggibili.

Diverrà chiaro oltre il senso di ciò che parrebbe avere il sembiante di una pura provocazione dialettica.
Si giunge così al terzo insegnamento della Corte: la corretta lettura del GDPR. Secondo il Considerando 32 del Regolamento 2016/679, "il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle".
A parte il richiamo al concetto di libertà, specificità, informazione e inequivocabilità del consenso, che riecheggia il dettato del cit. art. 7 della Direttiva 1995/46, il Considerando esclude espressamente la possibilità di manifestare passivamente il consenso, bandendo con ciò dal concetto di inequivocabilità il silenzio, l'inattività o la preselezione di caselle.
Aumentiamo però il gradiente di sfida ermeneutica. L'articolo 4 del GDPR, replicando lo stilema della Direttiva 1995/46, qualifica come consenso "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento". Fa eco l'articolo 6 del Regolamento quando prevede che "il trattamento è lecito solo se e nella misura in cui […] l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità". Mentre l'articolo 7, comma 4, del medesimo Regolamento rammenta che, nel valutare se il consenso sia stato liberamente prestato, "si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".
Quest'ultimo combinato normativo implica un paio di riflessioni. Prima: il consenso non può essere generalizzato bensì deve essere *specifico*. Seconda: il consenso obbligatorio deve essere effettivamente tale, *alias*: non può spacciarsi per obbligato, nel senso di imprescindibile per l'esecuzione del contratto, un consenso artatamente contrabbandato per tale fine.
Completano il quadro le previsioni dell'art. 13 co. 1 e 2 del GDPR che impongono al titolare del trattamento di dati personali già ottenuti, l'obbligo di

comunicare all'interessato *(i)* i destinatari o le categorie di destinatari dei dati e *(ii)* il periodo di conservazione dei dati personali o, se non possibile, i criteri utilizzati per determinarlo (elementi questi non espressamente contemplati dalla Direttiva 1995/46).

(*segue*): b) la preselezione quale antitesi del consenso informato e l'incompleta teorizzazione del "comportamento attivo"

In applicazione delle suesposte disposizioni, la Corte perviene alla conclusione per cui il consenso espresso mediante una casella di spunta preselezionata, non implicando un "comportamento attivo" da parte dell'utente, non sia idoneo a soddisfare il requisito della inequivocabilità del rilascio.
Il percorso logico si fonda su una precisa lettura storica dell'art. 5 co. 3 della Direttiva 2002/58, interpretato dalla Corte sia richiamando espressamente la modifica introdotta al suddetto comma dalla Direttiva 2009/136[11], sia riferendosi ai contenuti del "consenso della persona interessata" siccome espressi nella Direttiva 1995/46 e utilizzabili in tema di cookies in considerazione del richiamo operato dall'articolo 2 lett. f) della Direttiva 2002/58 alla Direttiva poc'anzi citata. Con la conseguenza che il consenso dell'utente non può ritenersi presunto dovendo invece risultare da un comportamento attivo.
Sul punto assume un particolare rilievo l'osservazione empirica della Corte (§ 56 della pronuncia): "risulta praticamente impossibile determinare in modo oggettivo se, non deselezionando una casella preselezionata, l'utente di un sito Internet abbia effettivamente manifestato il proprio consenso al trattamento dei suoi dati personali, nonché, in ogni caso, se tale consenso sia stato manifestato in modo informato. 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".
Tale costatazione, in apparenza discutibile secondo lo stilema dell'*imputet sibi* da "bugiardino farmaceutico" (per quanto lungo e noioso, chi non lo legge poi non si lamenti), cattura invece, in modo acuto e sintetico, il fenomeno caratteristico della navigazione in Internet. Affermare che non è oggettivamente possibile dimostrare che la scelta di non deselezione della casella sia seguita ad una cosciente lettura del testo o che tale lettura non sia avvenuta o che l'utente non abbia neppure notato la casella, non equivale

[11] Che ha introdotto la formula del "consenso preventivo" alla installazione di cookies in sostituzione del solo diritto, prima concesso, al rifiuto all'installazione dei cookies.

certo a introdurre un principio di deresponsabilizzazione del navigatore, sulla scia di un malinteso, indistinto e spesso abusato *favor* per la parte presuntamente debole del rapporto. È invero alquanto significativo che, nella fredda valutazione della Corte, non compaia alcun richiamo a condizioni di asimmetria informativa o di rapporti di forza economica o contrattuale, bensì un lucido riscontro di quella condizione di oggettiva inesigibilità di un comportamento improntato all'accuratezza informativa nel momento dell'uso di un mezzo come la rete che, per sua natura, si pone come veicolo di rapida consultazione o fruizione.

Siamo pressoché certi che, in caso di sottoscrizione di un contratto bancario o finanziario, la Corte non avrebbe usato altrettanta indulgenza verso il cliente pur a fronte di un contratto lungo e complesso: come del resto non la usano abitualmente le Corti nazionali che, semmai, s'ingegnano di scovare vizi di forma dell'accordo o difettosità contenutistiche di singole clausole (vessatorietà, indeterminatezza e simili) ma giammai s'avvalgono d'una sorta di "presunzione statistica" che conduca all'incolpevolezza per ragioni di difficoltà di lettura o financo di mancata lettura.

In effetti, nel "contratto fisico", vige ancora la presunzione statistica eguale e contraria – quanto poi corrispondente al vero è discorso che qui ci porterebbe troppo lontano – di avvenuta, preventiva lettura. Al contrario – e qui sta il grande passo in avanti compiuto dalla sentenza in commento – la presunzione di incolpevole omissione di lettura dell'informativa privacy discende propriamente dalla tipologia del mezzo virtuale e dall'ambiente ipervelocizzato in cui esso consente di operare.

Sul piano normativo, la Corte rafforza il suo convincimento addentellandosi alle ancor più specifiche disposizioni del GDPR, in particolare al Considerando 32 e alla ivi esplicitata nozione di "*azione positiva inequivocabile*" nonché alla irrilevanza del *silenzio*, dell'*inattività* o della *preselezione* di caselle (§§ 62-63 della sentenza).

Quanto precede instilla un paio di dubbi, invero piuttosto "scomodi". Il primo: se la non deselezione non è garanzia di aver letto o visto l'informativa, non potrebbe dirsi altrettanto nel caso della selezione? Il secondo: quali requisiti deve rivestire il comportamento perché lo si possa effettivamente definire attivo? Più precisamente, la continuazione di navigazione, pur senza selezionare o deselezionare casella alcuna, può qualificarsi alla stregua di un comportamento attivo ai fini del rilascio del consenso?

I due dubbi sono evidentemente e strettamente annodati l'uno all'altro. Muoviamo dal secondo che, come ci accingiamo a notare, è invece un *prius* logico.

Se il GDPR boccia silenzio, inattività e preselezione quali efficaci manife-

stazioni di un consenso informato, potrebbe dialetticamente arguirsi che la prosecuzione pura e semplice di navigazione sia un comportamento indubbiamente attivo e tale da esprimere, implicitamente ma inequivocamente, la formulazione di un consenso.
La Corte sembra di avviso opposto. Nei §§ 58-59 della pronuncia, si rammenta che la manifestazione di volontà di cui all'art. 2, lettera h), della Direttiva 1995/46 deve rivestire il requisito della specificità "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". Per poi precisare (così smontando e smentendo l'argomento opposto dalla società gerente) che "il fatto che l'utente attivi il pulsante di partecipazione al gioco a premi organizzato da detta società non può essere, pertanto, sufficiente per ritenere che l'utente abbia validamente espresso il suo consenso all'installazione di cookie". La prosecuzione di navigazione, anzi nella specie l'attivazione specifica del servizio offerto dal sito, non è dunque sufficiente allo scopo in quanto ha un oggetto *distinto* (navigare o partecipare al gioco), cioè *diverso* dallo specifico oggetto (consenso al trattamento dei dati personali) su cui deve formarsi l'accettazione dell'utente ai fini privacy. Ne consegue che l'inattività non può ritenersi esclusa dalla prosecuzione di navigazione e financo dalla fruizione specifica del servizio.
Il ragionamento della Corte non fa grinze e merita piena condivisione. Quantunque il GDPR non si sospinga sino al punto di offrire una precisa definizione di inattività, la lettura sistematica del principio di specificità non può condurre ad altra razionale conclusione. La quale, a ben vedere, riposa nel trilogismo contenuto nel menzionato Considerando: silenzio-inattività-preselezione. Rapportati al contesto in discorso, il silenzio, ossia il non dire, e la preselezione della casella, ossia l'accettare il dire della controparte, sono condotte che certamente ineriscono lo specifico atto di manifestazione del consenso, per cui non v'è ragione, né semantica né ermeneutica, che possa giustificare un diverso ruolo funzionale del concetto di inattività.
Ne consegue, dal punto di vista pratico, l'insufficienza, ai fini di una corretta acquisizione del consenso all'impiego dei cookie (esclusi quelli meramente tecnici), di quei numerosi *disclaimer,* tuttora adottati da molti siti anche particolarmente seri e insospettabili, con cui si avverte l'utente che la prosecuzione di navigazione, ancorché colui o colei non accetti espressamente, implica il consenso implicito all'uso di *tutti* i cookie, salvo poi accorgersi, se si ha tempo e pazienza di leggere l'informativa per intero, che fra essi compaiono anche quelli di profilazione. E il problema si fa ancor più serio nel caso in cui il *disclaimer* sia semplicemente accompagnato dalla casella o dal tasto "OK", "Accetto" o simili, ma non anche da tasti che consentano

il rifiuto selettivo, posto che in tal caso (escludendosi qui – perché irrilevante ai fini dell'acquisizione del consenso da parte del sito – la facoltà dell'utente di bloccare attraverso i browser tutti i cookie[12]) l'utente non ha realisticamente altra scelta che accettare o continuare la navigazione, la quale, pertanto e *a fortiori*, non costituisce, non può costituire una libera, specifica, informata e inequivocabile manifestazione di consenso.

Sciolto il secondo dubbio, veniamo al primo, decisamente più arduo da dissipare. La selezione della casella di accettazione può ritenersi sufficiente espressione di un comportamento attivo?

A rigor di logica e in una chiave di lettura sistematica delle norme, si dovrebbe negarlo. Non si trova infatti ragione alcuna per distinguere fra il selezionare e il non deselezionare: la possibilità, fors'anche la certezza, che l'utente non abbia letto l'informativa e che la sua manifestazione di volontà sia quanto meno né specifica né informata è rintracciabile in entrambe le ipotesi. La selezione, rispetto alla non deselezione, comporta un gesto aggiuntivo da parte dell'utente, ma si tratta di un gesto ormai automatico, pressoché scontato, un fastidio minimo e "accettabile per l'utente" che corrisponde ad un semplice click. L'incolpevole omissione di lettura o l'altrettanto e incolpevole frettolosa lettura si concretano in entrambi i casi.

La coerenza di tale interpretazione si scontra, tuttavia, contro il dato positivo. Sia la Direttiva del 2002 sia il GDPR ammettono esplicitamente che il consenso possa essere reso attraverso la selezione di una casella. Ed è qui, è proprio qui, che il sistema appalesa la sua più profonda incoerenza. Ed è parimenti qui che la teorizzazione del "comportamento attivo" si rivela necessariamente incompleta.

Necessariamente incompleta, poiché non ci si poteva certo attendere dalla Corte europea una lettura che forzasse il dettato normativo sino a stravolgerne il significato o a implicitamente abrogarlo. Non ci si poteva attendere tanto vuoi perché ciò non ricade nei poteri della Corte, vuoi perché la questione non fu neppure sollevata nel corso del procedimento da cui originò il rinvio né fu inclusa nel quesito sollevato dalla Cassazione tedesca. E non lo fu perché tanto chi agiva quanto chi decideva era ben conscio del predetto, invalicabile limite normativo.

Si conferma con ciò la "diagnosi" contenuta nel nostro precedente scritto. Il ponderoso e poderoso impianto normativo reca un'aporia intrinseca: per un verso, esso esalta la necessità di un comportamento attivo dell'utente nella manifestazione del consenso attraverso il predetto trilogismo "silenzio-inat-

[12] Facoltà, a onor del vero, poco sfruttata perché spesso il blocco totale dei cookie include anche quelli tecnici precludendo la funzionalità minima di molti siti.

tività-preselezione"; per altro verso, esso depotenzia quello stesso comportamento ammettendo il surrogato di una vera manifestazione di consenso tradotta nella selezione di una casella. Tratta cioè diversamente, proibendo l'una e ammettendo l'altra, condotte dei gestori che nondimeno pervengono allo stesso risultato: acquisire il consenso dell'utente in modo sostanzialmente elusivo degli specifici obblighi di informazione e libera scelta dell'utente.
Per eliminare tale aporia non resta che completare l'inversione di rotta in via normativa[13], pervenendo dunque al rovesciamento del meccanismo nei termini da noi suggeriti: nessun cookie di default (sempre esclusi quelli meramente tecnici) e la possibilità per l'utente di scegliere attivamente i cookie desiderati – dove per "attivamente" non deve intendersi la spunta di una o più caselle predisposte dal gestore e condizionanti la navigazione, bensì un'azione autenticamente volitiva dell'utente, rispetto alla quale il gestore non dovrà offrire alcun incentivo d'adesione automatica, ferma la possibilità di "negoziare" il consenso con funzionalità e servizi diversi e aggiuntivi rispetto a quelli contenuti nel sito.
Se la Corte non poteva arrivare a tanto, certamente essa ha però tracciato una linea di correzione inequivoca che il legislatore comunitario, se solo veramente lo volesse, potrebbe agevolmente seguire per riparare questa stortura, restituire coerenza al sistema ma soprattutto conferire all'impianto normativo quell'autentico valore di tutela della libertà e di protezione della sfera privata che esso pur solennemente proclama. E in ciò quella sentenza costituisce e costituirà un indelebile monito.
Il perché tale correzione non sia ancora avvenuta lo abbiamo chiarito nell'ultimo paragrafo del nostro precedente scritto. Non ci ripeteremo perché non vogliamo tediare i nostri Lettori, ai quali chiediamo invece la pazienza di seguirci nelle prossime righe, dove potranno cogliere un ulteriore, crediamo interessante spunto di riflessione.

Le ulteriori statuizioni della sentenza: l'informazione sui tempi di conservazione dei cookie e la protezione dei contenuti del terminale diversi dai dati personali

La sentenza contiene altre due linee interpretative.
La prima, più scontata e meno attraente, riguarda l'obbligo di comunicazione all'utente dell'arco temporale di conservazione dei cookie. La questione è

[13] Apparendo alquanto improbabile il successo di un eventuale ricorso in annullamento della disposizione del GDPR in parola, giacché, a tacer del resto, non sembra predicabile un contrasto con, o una violazione di, trattati unionisti o diritti fondamentali.

agevolmente risolta dalla Corte alla luce del GDPR che contiene una specifica disposizione al riguardo[14]. Alla stessa conclusione la sentenza perviene anche in relazione all'art. 10 della Direttiva 1995/96, che pur non contemplava espressamente questo genere di comunicazione. La Corte riesce ad includervelo grazie ad una lettura letterale e sostanziale della disposizione oggi abrogata. Sul piano letterale, la sentenza rammenta che l'elenco di informazioni da rendersi all'utente previsto dal cit. art. 10 non è da considerarsi tassativo né esaustivo data la premessa dell'avverbio "almeno" all'elenco delle informazioni. Sul piano della *ratio legis*, si afferma invece che il richiamo al principio del "trattamento leale" dei dati non può non includere l'informazione sulla tempistica di mantenimento dei cookie poiché "un lungo periodo di attività, o addirittura un periodo illimitato, implica la raccolta di numerose informazioni sulle abitudini di navigazione e sulla frequenza delle eventuali visite dell'utente ai siti dei partner pubblicitari". Soluzione molto "geometrica", indubbiamente corretta ma sostanzialmente inservibile in quanto ormai recepita *de plano* nel GDPR.

Molto più invogliante, non foss'altro perché atta a stimolare sottili e pungenti riflessioni, è la seconda statuizione.

Il quesito del giudice del rinvio parrebbe molto elaborato: "se l'articolo 2, lettera f), e l'articolo 5, paragrafo 3, della Direttiva 2002/58, letti in combinato disposto con l'articolo 2, lettera h), della Direttiva 95/46, nonché con l'articolo 4, punto 11 e l'articolo 6, paragrafo 1, lettera a), del Regolamento 2016/679, debbano essere interpretati in modo diverso a seconda che le informazioni archiviate o consultate nell'apparecchiatura terminale dell'utente di un sito Internet costituiscano o meno dati personali, ai sensi della Direttiva 95/46 e del Regolamento 2016/679". Nella sostanza il problema è più semplice di quel che sembri: nel § 45 della pronuncia si rappresenta che i cookie installati dal gestore nell'apparecchiatura terminale degli utenti includevano un codice numerico associato ai dati di registrazione degli utenti medesimi. Siffatto abbinamento induceva il giudice del rinvio a concludere nel senso della personalizzazione dei dati archiviati dai cookie cosicché la raccolta di questi dati si sarebbe risolta nel trattamento di dati personali. Dato peraltro confermato dal gestore che, in corso di processo, ammise che il consenso corrispondente alla seconda casella di spunta (quella preselezionata) fosse inteso ad autorizzare la raccolta e il trattamento di dati personali e non di informazioni anonime.

[14] All'articolo 13, par. 2°, del GDPR è espressamente richiesta, nell'informativa, l'indicazione del "periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo".

L'*affaire* poteva chiudersi lì, di fronte cioè ad una confessione inequivoca e inevitabile. Ciononostante la Corte non si sottrae all'obbligo di rendere il suo pensiero e getta il cuore non oltre ma al di qua dell'ostacolo, quest'ultimo non meritando manco l'onore del superamento. Nel contempo essa però riafferma un principio a sua volta capace di schiudere nuovi scenari.
Anche in questo frangente, la Corte lavora per geometrie ermeneutiche, senza dover ricorrere a *verve* creativa. Donde il seguente teorema:

a) l'art. 5, co. 3, Direttiva 2002/58 richiama l'"*archiviazione di informazioni*" e l'"*accesso a informazioni già archiviate*", senza darsi cura che tali informazioni corrispondano a dati personali nel senso definito dalla Direttiva. La *ratio* è lampante: la norma tutela l'utente da qualsiasi ingerenza nella sua vita privata, indipendentemente dal fatto che detta ingerenza riguardi o meno dati strettamente qualificabili come personali;
b) è lo stesso più volte citato Considerando 24 della Direttiva 2002/58 a chiarire che qualsiasi informazione archiviata nell'apparecchiatura terminale degli utenti appartiene alla sfera privata dell'utente: tutela applicabile, dunque, a qualsiasi informazione archiviata nel terminale, che si tratti o meno di dati personali, oppure volta a proteggere gli utenti dal rischio che *malware* e affini si introducano nell'apparecchiatura terminale dell'utente *malgré lui*; ergo
c) le succitate norme non devono essere interpretate in modo diverso a seconda che le informazioni archiviate o consultate nell'apparecchiatura terminale dell'utente di un sito Internet costituiscano o meno dati personali, ai sensi della Direttiva 1995/46 e del Regolamento 2016/679.

Il *come dovevasi dimostrare* risulta quindi pianamente attuato dalla *consecutio* normativa. Tutto qui? Niente affatto.
Rievocando quella che appariva come una mera provocazione dialettica, ci si avvede che essa trova una granitica conferma nel dato normativo. Andando oltre la fattispecie ludica del caso concreto, il principio di fondo, insito nelle norme ma stabilito senza esitazione preconcetta dalla Corte, non è tanto la tutela della riservatezza (chimera ormai prossima alla consunzione per esaurimento funzionale) quanto la tutela della proprietà. L'allitterante equazione del "mio-uguale-mio" dianzi ipotizzata (*supra* § 3) sospinge il nostro discorso al di là della cortina di cartapesta del dato personale.
Non rileverebbe, secondo il verbo high-tecnologico, solo ciò che può indentificare e profilare un individuo ma anche ciò che un individuo possiede: anche quel ciò va tutelato e rispettato ancorché quel "ciò" non sia utile – secondo l'umana intelligenza e non la stupida ingenuità meccanicistica di un algoritmo – a profilare l'utente. Del resto, a ben vedere la stessa nozione di dato

personale, contenuta nella Direttiva abrogata ma fatta propria dal GDPR, che riconosce nel dato personale anche "*uno o più elementi caratteristici della* […] *identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*" dell'utente ben include anche elementi che, pur non costituendo in sé dati personali, possano diventarlo per effetto di profilazioni tanto arbitrarie quanto sciocche, perché incapaci di distinguere fra condivisione e conoscenza: il fatto che l'utente acquisti e conservi nel suo terminale tanto la copia di *Mein Kampf* quanto quella de *Il Capitale* non significa affatto che egli o ella siano simpatizzanti dell'ideologia nazionalsocialista e al contempo ferventi marxisti, ben potendo la presenza di quegli scritti testimoniare semplicemente un desiderio di conoscenza.

Il pregio indiscusso della sentenza è di aver sancito l'ineluttabile forza delle norme nell'affermazione del diritto proprietario di ciò che risiede in un terminale con contestuale negazione del diritto vuoi di appropriarsene vuoi di scongiurare stereotipi di un utente in funzione di ciò che si possiede in luogo di ciò che si pensa, e di precludere la sciagurata equazione che ne derivi secondo automatismi associativi. Dunque, tutto ciò che sta nel terminale è proprietà dell'utente.

Da qui un ovvio corollario: se ciò che sta nel terminale è di proprietà dell'utente, non fa, non può far differenza il fatto che il dato sia stato archiviato dal proprietario o fraudolentemente o meno immesso da terzi. Conta solo il fatto che quel dato, acquisito dall'utente o da terzi inoculato (parimenti qui non rileva se con consenso reale o indotto), diventa proprietà dell'utente.

Siffatta e ineccepibile usucapione dell'insinuato altrui, al di là d'ogni scettica e contraria convinzione, consegna (anzi: restituisce) all'utente il primordiale diritto di rivendicazione del "suo". Ma se ciò che è nel mio terminale è mio, l'equilibrio giuridico impone che il "mio", adulterato dall'altrui ingerenza, resti mio e quindi proteggibile dinanzi a vere o tentate manipolazioni.

Dove vogliamo arrivare? È molto semplice. In assenza di un intervento normativo che finalmente doni equilibrio al sistema, sarà inevitabile da parte degli utenti, almeno di quelli cui sta a cuore la propria sfera privata, il ricorso a strumenti di autodifesa. È già accaduto con i vari sistemi di blocco pubblicitario, di anti-spamming, di antivirus. Nulla vieta che ciò si ripeta attraverso tecnologie più sofisticate e verso nuovi obiettivi: *offendicula* high-tech che non solo distruggano gli intrusi ma che ne annichiliscano la potenza intrusiva, meccanismi per eliminare i cookie profilativi nell'esatto istante in cui essi s'installano e per creare barriere al loro rientro. Tanto proprio in forza del principio per cui anche il meccanismo profilativo installato nel terminale finisce con il ricadere nella proprietà dell'utente sicché quest'ultimo può farne ciò che crede.

È lievemente sconfortante e profondamente amaro dover costatare come, a fronte di un impianto normativo sempre più oneroso per i gestori seri e sempre meno tutelante per gli utenti, la "soluzione" continui a risiedere nella legittima difesa tecnologica. Il vero *core business* del futuro non starà nell'ingenua illusione di esaltare la tecnologia intrusiva ma nella capacità di neutralizzarla. Sennonché, di questo passo, il sistema cadrà in una sorta di interminabile guerra civil-cibernetica, dove le norme perderanno tutto il loro potenziale riequilibratore e il dilagare del conflitto finirà col deprimere le stesse migliori funzionalità della tecnologia. Una ponderata e attenta rilettura di questa sentenza sarebbe un gesto responsabile, saggio e previdente da parte del Parlamento e della Commissione europea[15].

[15] D'altra parte l'occasione legislativa per un intervento regolamentare "di svolta" sarebbe disponibile e "a portata di mano", visto che le bozze del ben noto, e sicuramente atteso, "Regolamento e-Privacy" circolano continuamente, senza trovare, almeno sino ad oggi, una soluzione comune e condivisa tra chi dovrebbe produrle ed i relativi destinatari. Ciò che è certo, è che il far-west cibernetico farebbe compiere un innegabile "passo indietro" al mercato del web: passo indietro che andrebbe a scontrarsi con l'esigenza di trasparenza e di riservatezza quali presupposti irrinunciabili di una costruttiva modernità.