

## GRUPPO DI LAVORO PER LA TUTELA DEI DATI EX ART. 29

*Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE.» l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE. Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio LX-46 01/190.*

### **Parere n. 15/2011 - WP187** **sulla definizione di consenso** adottato il 13 luglio 2011

#### **Sintesi**

Il presente parere fornisce un'analisi dettagliata della nozione di consenso attualmente impiegata nella direttiva in materia di protezione dei dati e nella direttiva relativa alla vita privata e alle comunicazioni elettroniche. Facendo tesoro dell'esperienza dei membri del Gruppo di lavoro "Articolo 29", il parere fornisce numerosi esempi di consenso valido e non valido, soffermandosi su elementi chiave quali il significato di "manifestazione", "manifestazione di volontà libera", "specifico", "inequivocabile", "esplicito", "informato", ecc. Il parere chiarisce ulteriormente alcuni aspetti correlati alla nozione di consenso, come il momento in cui dev'essere ottenuto il consenso, la differenza tra diritto a opporsi e consenso, ecc.

Il consenso è uno dei vari motivi che legittimano il trattamento dei dati personali. Svolge un ruolo importante, ma non esclude la possibilità che, a seconda del contesto, possano essere invocati altri fondamenti giuridici forse più appropriati, dalla prospettiva sia del titolare del trattamento sia dell'interessato. Se usato correttamente, il consenso rappresenta uno strumento che offre all'interessato una forma di controllo sul trattamento dei dati che lo riguardano. Se utilizzato in maniera errata, il controllo dell'interessato sul trattamento dei dati che lo riguardano è soltanto illusorio e il consenso costituisce un fondamento inadeguato per legittimare il trattamento.

Il presente parere è stato redatto anche per rispondere a una richiesta di contributi della Commissione nell'ambito della revisione in corso della direttiva in materia di protezione dei dati. Pertanto, contiene raccomandazioni di cui si dovrà tener conto nell'ambito della revisione, tra cui:

- (i) fare chiarezza sul significato del concetto di consenso "inequivocabile" e spiegare che soltanto il consenso fondato su dichiarazioni o azioni intese a esprimere accettazione costituisce un valido consenso;
- (ii) obbligare i responsabili dei dati a mettere a punto meccanismi per dimostrare di aver effettivamente ottenuto il consenso (nell'ambito di un obbligo generale di rendiconto);
- (iii) aggiungere una prescrizione esplicita relativa alla qualità e all'accessibilità delle informazioni che costituiscono il fondamento per il consenso;
- (iv) una serie di suggerimenti relativi ai minori e ad altri soggetti privi della capacità di agire.

**IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI,**

istituito con direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, visto l'articolo 29 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, della suddetta direttiva, visto il proprio regolamento interno,

**HA ADOTTATO IL SEGUENTE PARERE:**

**I. Introduzione**

La nozione di "consenso dell'interessato" è sempre stata fondamentale nella sfera della protezione dei dati; nonostante ciò, non sempre è chiaro quando il consenso sia necessario e quali condizioni debbano essere soddisfatte perché possa essere considerato valido. Di conseguenza, ciò può portare, nei diversi Stati membri, ad approcci diversi e pareri divergenti per quanto concerne le buone prassi. Questa situazione può indebolire la posizione degli interessati. Il problema si è fatto più critico da quando il trattamento dei dati personali è divenuto un elemento via via più importante della società moderna, negli ambienti online così come in quelli off-line, un elemento che spesso vede il coinvolgimento di Stati membri diversi. Ecco perché il Gruppo di lavoro "Articolo 29", nell'ambito del suo programma di lavoro per il 2010-2011, ha deciso di esaminare attentamente tale situazione.

Il consenso è anche uno degli argomenti in merito ai quali la Commissione ha chiesto contributi esterni nell'ambito della revisione della direttiva 95/46/CE. Nella comunicazione della Commissione intitolata "Un approccio globale alla protezione dei dati personali nell'Unione europea"<sup>1</sup> si legge: "La Commissione esaminerà come rendere più chiare e rafforzare le norme sul consenso".

La comunicazione fornisce la seguente ulteriore spiegazione<sup>2</sup>:

è questo il caso della pubblicità comportamentale, dove le impostazioni del browser esprimono, secondo alcuni ma non secondo tutti, il consenso dell'utente."» quindi opportuno fare chiarezza sulle condizioni per il consenso, onde garantire che questo sia dato sempre con conoscenza di causa e che l'interessato ne sia pienamente consapevole e sappia per quale trattamento lo sta accordando, come prevede l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. Disposizioni essenziali chiare possono inoltre favorire lo sviluppo di iniziative di autoregolamentazione e la ricerca di soluzioni pratiche conformi al diritto dell'UE."

Per rispondere alla richiesta di contributi formulata dalla Commissione e per dare attuazione al suo programma di lavoro per il periodo 2010-2011, il Gruppo di lavoro "Articolo 29" si è impegnato a redigere un parere. Scopo del parere è chiarire gli aspetti critici al fine di offrire una comprensione comune del quadro giuridico attuale. Al tempo stesso, questo intervento segue la logica di precedenti pareri vertenti su altre disposizioni fondamentali della direttiva<sup>3</sup>. Poiché l'introduzione di potenziali modifiche al quadro attuale richiederà ancora del tempo, il fatto di chiarire la nozione attuale di "consenso" e i suoi elementi principali non è privo di meriti e vantaggi. Inoltre, fare chiarezza sulle disposizioni attuali contribuirà a mettere in evidenza i punti ancora perfettibili. Pertanto, sulla base dell'analisi effettuata, il parere tenterà di formulare raccomandazioni politiche per assistere la Commissione e i responsabili politici nella definizione di modifiche al quadro giuridico applicabile in materia di protezione dei dati.

I contenuti fondamentali del parere sono i seguenti: dopo aver fornito una panoramica della storia legislativa e del ruolo del consenso nella legislazione in materia di protezione dei dati, saranno esaminati i vari elementi e requisiti che devono essere soddisfatti affinché il consenso possa essere considerato valido ai sensi della legislazione applicabile, comprese alcune parti pertinenti della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche. L'analisi è illustrata con esempi pratici raccolti dalle esperienze nazionali. Tale esercizio suffraga le raccomandazioni contenute nella parte conclusiva del presente parere, in base alle quali, per richiedere e ottenere un consenso

valido ai sensi della direttiva, devono essere presenti alcuni elementi. Esso fornisce inoltre raccomandazioni politiche da sottoporre all'attenzione dei responsabili politici nell'ambito della revisione della direttiva 95/46/CE.

## **II. Osservazioni Generali e aspetti relativi alla politica in esame**

### **II.1. Breve panoramica**

Benché in alcune leggi nazionali in materia di protezione dei dati/vita privata adottate negli anni '70 il consenso figurasse tra i fondamenti giuridici che legittimano il trattamento dei dati personali<sup>4</sup>, questa situazione non ha trovato riscontro nella successiva convenzione n. 108 del Consiglio d'Europa<sup>5</sup>. Non esiste alcun motivo palese per cui la convenzione non riservi al consenso un ruolo più preminente<sup>6</sup>.

A livello di Unione europea, al contrario, il consenso come criterio per la legittimazione di operazioni di trattamento dei dati è stato previsto sin dall'inizio del processo legislativo che si è concluso con l'adozione della direttiva 95/46/CE. Nel 1990, l'articolo 12 della proposta della Commissione<sup>7</sup> definiva le caratteristiche che il consenso doveva avere per legittimare le operazioni di trattamento dei dati: esso cioè doveva essere "fornito espressamente" ed essere "specifico".

L'articolo 17, in materia di dati sensibili, prescriveva che il consenso fosse "espresso e scritto". Nel 1992 la proposta modificata della Commissione<sup>8</sup> introduceva un testo simile alla definizione di "consenso dell'interessato" contenuta nell'odierno articolo 2, lettera g), che sostituisce l'originale articolo 12. La proposta stabiliva che il consenso dovesse essere "libero e specifico". Le parole "fornito espressamente" sono state sostituite dal concetto di consenso come "espressa indicazione della sua [dell'interessato] volontà". Il memorandum esplicativo che accompagna la proposta modificata del 1992 stabiliva che il consenso dovesse essere ottenuto oralmente o preiscritto. Nel caso dei dati sensibili, il requisito del consenso "scritto" rimaneva valido. Nel 1992 la proposta modificata della Commissione ristrutturava la precedente proposta e introduceva un articolo 7 che elencava i criteri di liceità del trattamento. L'articolo 7, lettera a), stabiliva che i dati potessero essere trattati qualora "la persona interessata [avesse] dato il suo consenso"; l'elenco originale comprendeva, così come comprende tuttora, cinque altri fondamenti giuridici (oltre al consenso) in base ai quali può essere legittimato il trattamento dei dati.

In sintesi, dalla storia legislativa, soprattutto riferita all'UE, emerge che il consenso ha rivestito un ruolo importante per le nozioni di protezione dei dati e di vita privata. Parallelamente, emerge che il consenso non è stato considerato come l'unico fondamento giuridico per la legittimazione delle operazioni di trattamento dei dati. Dai lavori preparatori della direttiva 95/46/CE si evince un relativo accordo sulle condizioni che soddisfano la nozione di valido consenso, nel senso che il consenso può dirsi tale se è libero, specifico e informato. Tuttavia, non mancano le incertezze riguardo alle modalità con cui il consenso può essere espresso, se cioè debba essere esplicito, scritto, ecc. Tale situazione è analizzata più nel dettaglio nelle pagine seguenti.

### **II.2. Ruolo della nozione di consenso: motivo di liceità**

#### **Motivo generico/specifico:**

Nella direttiva il consenso è utilizzato sia come criterio generico di liceità (articolo 7) sia come criterio specifico in alcuni contesti particolari (articolo 8, paragrafo 2, lettera a), articolo 26, paragrafo 1, lettera a)). L'articolo 7 cita il consenso come il primo di sei diversi principi in base ai quali il trattamento dei dati personali è considerato legittimo, mentre l'articolo 8 contempla la possibilità di utilizzare il consenso per legittimare il trattamento riguardante categorie particolari di dati (sensibili), che

altrimenti sarebbe vietato. In quest'ultimo caso la norma per ottenere il consenso è più rigorosa, poiché trascende la norma generale e impone che il consenso sia "esplicito".

Inoltre, la direttiva permette un'interazione con altre norme, come si evince dal considerando 23: "(...) gli Stati membri sono autorizzati ad assicurare la messa in opera della tutela delle persone sia mediante una legge generale relativa alla tutela delle persone contro il trattamento dei dati personali, sia mediante leggi settoriali (...)". Il funzionamento di questo sistema a livello pratico è complesso: gli Stati membri hanno adottato ciascuno un loro approccio e, in alcuni casi, ciò ha prodotto discrepanze.

La nozione di consenso non è sempre stata trasposta fedelmente a livello nazionale. A titolo di esempio, la nozione generica di consenso non compare nella normativa francese in materia di protezione dei dati, ma il significato del termine è stato spiegato con precisione e coerenza nella giurisprudenza dell'autorità per la protezione dei dati (CNIL), in relazione alla definizione contenuta nella direttiva sulla protezione dei dati. Nel Regno Unito il concetto di consenso è stato sviluppato dalla common law con riferimento al testo della direttiva. In alcuni settori, inoltre, il consenso è stato talvolta definito in maniera esplicita, per esempio nell'ambito della vita privata e delle comunicazioni elettroniche, della pubblica amministrazione online e dei servizi sanitari in rete. La nozione elaborata nella normativa specifica è quindi destinata a interagire con quella sviluppata nella legislazione generica in materia di protezione dei dati.

La nozione di consenso è richiamata anche in altri rami del diritto, in particolare nel diritto contrattuale. In questo ambito, per assicurare che un contratto sia valido, sono presi in considerazione criteri diversi rispetto a quelli menzionati nella direttiva, tra cui l'età, l'influenza indebita, ecc. Il campo di applicazione del diritto civile e quello della direttiva, tuttavia, non sono in contrasto tra loro, ma si sovrappongono: la direttiva cioè non contempla le condizioni generali della validità del consenso nel contesto del diritto civile, ma nemmeno le esclude. Ciò significa, per esempio, che per valutare la validità di un contratto nell'ambito dell'articolo 7, lettera b), della direttiva si dovrà tener conto delle norme di diritto civile. Perché possa essere considerato valido ai sensi del diritto civile, oltre all'applicazione delle condizioni generali, il consenso previsto dall'articolo 7, lettera a), dev'essere anche interpretato alla luce dell'articolo 2, lettera h), della direttiva.

Tale interazione con altre legislazioni non è evidente soltanto a livello nazionale ma anche a livello europeo. Un'interpretazione analoga degli elementi della direttiva è stata fornita in altri contesti, come si evince da una sentenza della Corte di giustizia nel settore del diritto del lavoro<sup>12</sup>: in tal caso il consenso era necessario per rinunciare a un diritto sociale. La Corte ha interpretato la nozione di consenso nell'ambito della direttiva 93/104/CE concernente taluni aspetti dell'organizzazione dell'orario di lavoro, stabilendo che fosse necessario ottenere "il consenso del lavoratore" (quindi non di un sindacato per conto del lavoratore), e interpretando il termine "consenso" (...) come libero assenso informato. Ha inoltre statuito che, qualora il lavoratore sottoscriva un contratto di lavoro contenente un riferimento a un contratto collettivo che autorizza un superamento dell'orario massimo, le prescrizioni relative alla necessità che il consenso sia esplicitamente e liberamente espresso, in piena cognizione di causa, non sono soddisfatte. Tale interpretazione della nozione di consenso in un contesto specifico collima quasi pienamente con il testo della direttiva 95/46/EC.

La direttiva presenta chiaramente il consenso come un motivo di liceità. Alcuni Stati membri, tuttavia, lo annoverano tra i motivi preferenziali, talvolta di portata analoga a quella di un principio costituzionale, correlato allo status di diritto fondamentale riconosciuto alla protezione dei dati. Altri Stati membri possono intenderlo come una di sei diverse opzioni, un obbligo valido a fini operativi che non è più importante delle sue alternative. Fare chiarezza sul rapporto del consenso rispetto agli altri

motivi di liceità (per esempio, in relazione ai contratti, alle missioni di interesse pubblico o agli interessi legittimi del titolare del trattamento, e al diritto di opporsi) contribuirà a porre in evidenza il ruolo del consenso in circostanze specifiche.

L'ordine in cui i motivi legittimanti sono elencati all'articolo 7, pur essendo importante, non significa che il consenso costituisce sempre il motivo più appropriato per legittimare il trattamento dei dati personali. L'articolo 7 inizia elencando il consenso e prosegue citando gli altri criteri, tra cui i contratti e gli obblighi legali, fino ad arrivare gradualmente all'equilibrio degli interessi. Si deve notare che, per gli altri cinque motivi diversi dal consenso, è richiesta la prova della "necessità", che limita rigorosamente il contesto in cui tali motivi possono trovare applicazione. Ciò tuttavia non significa che, per l'obbligo relativo al consenso, sia garantito un margine di manovra maggiore rispetto agli altri motivi menzionati nell'articolo 7.

Inoltre, l'ottenimento del consenso non esonera il titolare del trattamento dagli obblighi di cui all'articolo 6 con riferimento ai principi di lealtà, necessità e proporzionalità, oltre che di qualità dei dati. Per esempio, anche qualora il trattamento dei dati personali poggi sul consenso dell'utilizzatore, ciò di per sé non legittima una raccolta dei dati supplementare rispetto allo scopo specifico.

Né l'ottenimento del consenso consente di aggirare altre disposizioni, come l'articolo 8, paragrafo 5. Soltanto in casi estremamente limitati il consenso può legittimare attività di trattamento dei dati che altrimenti sarebbero vietate, per esempio per quanto concerne il trattamento di taluni dati sensibili (articolo 8) o per autorizzare l'uso di dati personali ai fini dell'ulteriore trattamento, indipendentemente dal fatto che ciò sia compatibile con lo scopo originale. In linea di principio, il consenso non dev'essere considerato come una forma di esonero dagli altri principi di protezione dei dati, bensì come una salvaguardia. Esso è, in prima linea, un motivo di liceità e non comporta una rinuncia all'applicazione di altri principi.

La scelta del motivo legittimante più appropriato non è sempre ovvia, soprattutto nel caso dell'articolo 7, lettere a) e b). Secondo l'articolo 7, lettera b), il trattamento è necessario per eseguire un contratto o misure precontrattuali prese su richiesta dell'interessato, e non altro. Un titolare del trattamento che si avvale dell'articolo 7, lettera b), come motivo legittimante nell'ambito della conclusione di un contratto non può ampliare tale fondamento per giustificare un trattamento di dati che va oltre quanto necessario: deve invece legittimare tale trattamento supplementare con un consenso specifico al quale si applicano le disposizioni dell'articolo 7, lettera a). Questa è la dimostrazione che, nei termini contrattuali, è necessaria maggiore granularità. Nella pratica, ciò significa che può essere necessario ottenere il consenso come ulteriore condizione per dar corso ad alcune parti del trattamento. O il trattamento è necessario all'esecuzione del contratto oppure è indispensabile ottenere il (libero) consenso. In alcune operazioni potrebbero trovare applicazione più motivi legittimanti contemporaneamente. In altri termini, un qualsiasi trattamento dei dati personali deve sempre essere conforme a uno o più motivi di liceità. Ciò non esclude l'uso simultaneo di più criteri, purché siano utilizzati nel contesto appropriato. Nell'ambito del contratto con l'interessato può essere necessario raccogliere alcuni dati e procedere a un ulteriore trattamento – articolo 7, lettera b); altre forme di trattamento possono essere necessarie per adempiere a un obbligo legale – articolo 7, lettera c); per la raccolta di ulteriori informazioni può essere necessario ottenere un consenso specifico – articolo 7, a); in-fine, altre forme ancora di trattamento potrebbero essere legittimate anche ai fini dell'equilibrio degli interessi – articolo 7, lettera f).

### **Esempio: acquisto di un'automobile**

Il titolare del trattamento può essere autorizzato a trattare i dati personali per scopi diversi e sulla base di motivazioni diverse: - dati necessari per l'acquisto dell'automobile: articolo 7, lettera b); - per la

preparazione dei documenti dell'automobile: articolo 7, lettera c); - ai fini dei servizi di assistenza al cliente (per esempio, per garantire l'assistenza per il veicolo in diverse società affiliate nell'UE): articolo 7, lettera f); - ai fini del trasferimento dei dati a terzi per la realizzazione delle attività di marketing di questi ultimi: articolo 7, lettera a).

### **II.3. Nozioni correlate**

#### **Controllo**

La nozione di consenso è tradizionalmente correlata all'idea che l'interessato debba poter controllare l'uso che si fa dei suoi dati. Dalla prospettiva dei diritti fondamentali, il controllo esercitato attraverso il consenso è un concetto importante. Al tempo stesso, e dalla medesima prospettiva, la decisione di un individuo di accettare un'operazione di trattamento dei dati dovrebbe essere soggetta a rigorosi criteri, soprattutto se si tiene conto del fatto che, così facendo, un individuo potrebbe rinunciare ad un suo diritto fondamentale.

Benché il consenso sia un elemento importante per conferire agli interessati il controllo dei propri dati, esso non rappresenta l'unico strumento utile a tal fine. La direttiva fornisce altri mezzi di controllo, in particolare il diritto di opporsi al trattamento, ma questo strumento è diverso e può essere utilizzato in una fase diversa del trattamento, ossia dopo che il trattamento è iniziato e sulla base di un diverso fondamento giuridico.

Il consenso è collegato alla nozione di autodeterminazione delle informazioni. L'autonomia dell'interessato è sia una preconditione sia una conseguenza del consenso: essa conferisce all'interessato una certa influenza sul trattamento dei dati. Tuttavia, come si avrà modo di dimostrare nel seguente capitolo, tale principio possiede dei limiti, e vi sono casi in cui l'interessato non è in condizione di prendere realmente una decisione. Il titolare del trattamento potrebbe voler sfruttare il consenso dell'interessato come mezzo per trasferire a quest'ultimo la sua propria responsabilità giuridica. Per esempio, l'interessato che ha autorizzato la pubblicazione dei dati personali in Internet, o il trasferimento degli stessi a un soggetto dubbio in un paese terzo, potrebbe subire danni ma il titolare del trattamento potrebbe sostenere che tale situazione altro non è se non la conseguenza dell'assenso fornito dall'interessato. Per tale ragione è importante rammentare che un consenso pienamente valido non solleva il titolare del trattamento dai suoi obblighi e non legittima un trattamento che sarebbe altrimenti sleale ai sensi dell'articolo 6 della direttiva.

La nozione di controllo è inoltre correlata al fatto che l'interessato dovrebbe poter revocare il suo consenso. La revoca del consenso non è retroattiva, ma in linea di principio dovrebbe servire a impedire l'ulteriore trattamento dei dati dell'interessato da parte del titolare del trattamento. Il modo in cui ciò avviene nella pratica sarà esaminato di seguito (capitolo III).

#### **Trasparenza**

Una seconda dimensione del consenso riguarda le informazioni: la trasparenza nei confronti dell'interessato. La trasparenza è una condizione per avere il controllo dei propri dati e il presupposto in base al quale il consenso è reso valido. La trasparenza, in quanto tale, non è sufficiente per legittimare il trattamento dei dati personali, ma costituisce una condizione essenziale per avere la certezza che il consenso sia valido.

Per essere valido, il consenso dev'essere informato. Ciò presuppone che tutte le informazioni necessari e debbano essere fornite al momento in cui è richiesto il consenso e che tali informazioni debbano riguardare gli aspetti sostanziali del trattamento che si intende legittimare attraverso la richiesta di consenso. Tra queste solitamente figurano le informazioni elencate all'articolo 10 della direttiva, ma esse dipendono anche dal momento e dalle circostanze in cui è richiesto il consenso.

Indipendentemente dal fatto che il consenso sia o meno accordato, la trasparenza del trattamento dei dati è anche una condizione di lealtà, il cui valore permane anche dopo che sono state fornite le informazioni iniziali.

#### **Attività/tempistiche: modalità di manifestazione del consenso**

Questa terza dimensione si riferisce al modo in cui è esercitato il controllo: in che modo è possibile esprimere il consenso e quando dovrebbe essere richiesto per avere la certezza che si tratti di un consenso reale? Queste domande hanno un impatto decisivo sulle modalità di esercizio e d'interpretazione del consenso.

Benché la direttiva non specifichi il momento in cui dev'essere richiesto il consenso, dal testo delle varie disposizioni è evidente che, ingenerale, il consenso deve essere rilasciato prima dell'inizio del trattamento<sup>13</sup>. Ottenere il consenso prima dell'inizio del trattamento dei dati è un requisito fondamentale per legittimare il trattamento dei dati stessi. Questo aspetto è ulteriormente approfondito nel capitolo III.B, in cui è esaminata la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche. dopo che è avvenuto"<sup>14</sup>.

Per tali ragioni, il diritto di opposizione ai sensi dell'articolo 14 della direttiva non dovrebbe essere confuso con il consenso. Quest'ultimo rappresenta una motivazione per legittimare il trattamento dei dati personali in conformità dell'articolo 7, lettera a), dell'articolo 8, paragrafo 2, lettera a), dell'articolo 26, paragrafo 1, o secondo quanto previsto in svariate disposizioni della direttiva 2002/58/CE.

#### **II.4. Uso appropriato del consenso come fondamento giuridico**

E' opportuno precisare che il consenso non rappresenta sempre lo strumento principale o quello più auspicabile per legittimare il trattamento dei dati personali.

Talvolta il consenso è un debole fondamento per giustificare il trattamento dei dati personali e perde il suo valore quando viene esteso o limitato al fine di adattarlo a situazioni in cui non era destinato a essere utilizzato.» indispensabile quindi ricorrere al consenso "nel contesto adatto". Se utilizzato in circostanze inadeguate, perché è improbabile che siano presenti gli elementi che costituiscono un consenso valido, si verrebbe a creare una situazione di estrema vulnerabilità e, nella pratica, ciò finirebbe per indebolire la posizione dell'interessato.

Questa impostazione è già stata condivisa dal gruppo di lavoro e dal GEDP nei contributi rispettivamente forniti al dibattito sul nuovo quadro giuridico in materia di protezione dei dati. Si è dichiarato, in particolare, che "non è sempre possibile stabilire con chiarezza in che cosa consista un consenso vero e univoco. Alcuni responsabili del trattamento dei dati sfruttano questa incertezza affidandosi a metodi inadeguati per l'espressione di un consenso vero e univoco"<sup>15</sup> in violazione delle condizioni dell'articolo 6 della direttiva. Sulla stessa linea, il Gruppo di lavoro "Articolo 29" ha osservato che la complessità delle pratiche di raccolta dei dati, dei modelli commerciali, delle relazioni tra fornitori e delle applicazioni tecnologiche sovrasta molto spesso la capacità o la volontà dell'individuo di prendere decisioni, mediante una scelta attiva, per controllare l'utilizzo e la condivisione di informazioni<sup>16</sup>. » dunque importante chiarire i limiti del consenso e assicurare che soltanto il consenso interpretato secondo la legge sia considerato tale.<sup>17</sup> 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". Tale definizione contiene alcuni diversi elementi fondamentali che saranno discussi di seguito.

"... qualsiasi ... manifestazione di volontà ... accetta ..."

In linea di principio, non esistono limiti alla forma che può assumere il consenso. Per essere valido ai sensi della direttiva, tuttavia, il consenso dev'essere una manifestazione. Benché possa trattarsi di "qualsiasi" "forma di manifestazione, andrebbe chiarito che cosa esattamente ricade nella definizione di manifestazione.

La direttiva non specifica la forma che deve assumere la manifestazione (ossia il modo in cui è espressa la volontà). Per ragioni di flessibilità, nel testo definitivo si è evitato il riferimento al consenso "scritto".» bene ribadire che la direttiva contempla "qualsiasi" manifestazione di volontà. Ciò implica la possibilità di un'ampia interpretazione del campo di applicazione di tale manifesta-zione. L'espressione minima di una manifestazione potrebbe essere qualsiasi tipo di segnale che sia sufficientemente chiaro da indicare la volontà dell'interessato e che possa essere comprensibile per il titolare del trattamento. I termini "manifestazione" e "accetta" puntano nella direzione di un'azione che è effettivamente necessaria (rispetto a una situazione in cui il consenso potrebbe essere dedotto dall'assenza un'azione).

Il consenso dovrebbe prevedere qualsiasi manifestazione di una volontà con cui l'interessa-to accetta ossia esprime il suo assenso: potrebbe trattarsi di una firma apposta manualmente in calce a un modulo cartaceo, ma anche una dichiarazione orale che esprima accettazione, o un comportamento dal quale si possa ragionevolmente dedurre il consenso dell'interessato. Oltre al classi-co esempio della firma, potrebbe rientrare in questa definizione anche il fatto di lasciare a qualcuno-no un biglietto da visita. Lo stesso vale nel caso in cui una persona trasmetta un'organizzazione il proprio nome e indirizzo per avere informazioni sull'organizzazione stessa. In questo caso la sua azione dovrebbe essere intesa come un'accettazione al trattamento di tali dati essendo tale trattamento necessario per poter evadere e dar corso alla richiesta stessa.

Nel suo parere sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto (WP 115), il Gruppo di lavoro ha valutato in che modo le persone dovrebbero essere messe nelle condizioni di esprimere il proprio consenso a ricevere servizi che ne richiedano la localizzazione-ne automatica (per esempio, la possibilità di telefonare ad un numero specifico per ottenere informazioni sulle condizioni metereologiche del luogo in cui cisi trova). In tal caso ha riconosciuto che, a condizione che gli utenti ricevano preventivamente informazioni complete sul trattamento dei dati relativi all'ubicazione, chiamare un determinato numero equivarrebbe ad acconsentire a essere localizzati.

### **Esempio: pannelli pubblicitari di dispositivi dotati di Bluetooth**

In fase di sviluppo uno strumento pubblicitario costituito da pannelli che inviano ai passanti richieste di autorizzazione a stabilire una connessione Bluetooth per poter inviare messaggi pubblicitari. I messaggi sono trasmessi alle persone che hanno attivato i dispositivi Bluetooth sui loro tele-foni cellulari. La mera attivazione della funzione Bluetooth non costituisce un consenso valido (poiché la funzione Bluetooth potrebbe essere stata attivata per altri scopi). Al tempo stesso, se-qualcuno è informato del servizio e si avvicina a pochi centimetri dal pannello con il suo cellulare, sussiste, normalmente, una manifestazione di volontà: tale comportamento dimostra quali persone sono realmente interessate a riceverei messaggi pubblicitari. Si dovrebbe ritenere che soltanto queste persone hanno manifestato il proprio consenso e i messaggi dovrebbero essere inviati solo ai cellulari di queste persone.

Non è sicuro se, in circostanze estremamente specifiche (ossia in un contesto assolutamente privo di ambiguità), l'assenza di un comportamento– o meglio: un comportamento passivo – possa esse-re considerato una manifestazione. La nozione di "manifestazione" è ampia, ma sembra implicare la necessità di un'azione. Altri elementi della definizione di consenso, e il requisito aggiuntivo di cui all'articolo 7, lettera a), in base al quale il consenso dev'essere manifestato in maniera inequivocabile, suffragano questa interpretazione. L'indicazione che l'interessato deve esprimere un assenso quale



forma di "accettazione" sembra suggerire che la semplice inazione sia insufficiente e che, per configurare un consenso, sia necessaria una qualche forma di azione, benché siano possibili tipologie diverse di azioni, da valutare "nel contesto".

Nella pratica, in assenza di un comportamento attivo dell'interessato, è difficile per il titolare del trattamento stabilire se il silenzio dell'interessato significhi accettazione o consenso. Per esempio, un titolare del trattamento potrebbe non avere la certezza necessaria per dare per scontato un consenso nei seguenti casi: si immagina una situazione in cui, dopo aver inviato una lettera ai suoi clienti per informarli del previsto trasferimento dei loro dati in assenza di una loro risposta contraria entro 2 settimane, il titolare del trattamento ottenga una risposta soltanto dal 10% dei suoi clienti. In questo esempio, è improbabile che il 90% dei clienti che non hanno risposto abbia effettivamente accettato che i propri dati siano trasferiti. In un caso come questo il titolare del trattamento non ha ottenuto una chiara manifestazione dell'intenzione degli interessati. Inoltre, non dispone delle prove e, pertanto, non è in grado di dimostrare di aver ottenuto il consenso dei clienti. In pratica, l'ambiguità di una risposta passiva rende difficile ottemperare alle disposizioni della direttiva.

### **"... libera ..."**

Il consenso può essere valido soltanto se l'interessato è in grado di operare realmente una scelta, e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative nel caso in cui questa persona non manifesti il proprio consenso. Se le conseguenze del consenso minano la libertà di scelta dell'individuo, il consenso non può essere considerato libero. La direttiva stessa, all'articolo 8, paragrafo 2, lettera a), prevede che in alcuni casi, che devono essere determinati dagli Stati membri, il consenso espresso dall'interessato non è sufficiente per derogare al divieto relativo al trattamento di talune categorie specifiche di dati personali.

Ne è un esempio il caso in cui l'interessato è sotto l'influsso del titolare del trattamento, come nell'ambito di un rapporto di lavoro. In questo esempio, benché non necessariamente in tutti i casi, l'interessato può trovarsi in una situazione di dipendenza dal titolare del trattamento— per la natura del rapporto o per via di circostanze particolari —e potrebbe temere di essere trattata in maniera diversa nell'eventualità in cui rifiutasse il consenso al trattamento dei dati.

In svariati pareri il Gruppo di lavoro ha esaminato i limiti del consenso in situazioni in cui non sia possibile esprimerlo liberamente.» questo il caso, in particolare, dei pareri sulle cartelle cliniche elettroniche (WP 131), sul trattamento dei dati nel contesto dell'occupazione (WP 48) e sul trattamento dei dati da parte dell'Agenzia Mondiale Antidoping (WP 162).

Nel WP 131, il Gruppo di lavoro ha rammentato che "consenso 'libero' significa una decisione volontaria, presa da una persona in pieno possesso di tutte le sue facoltà e senza alcuna forma di coercizione, sociale, finanziaria, psicologica o d'altro tipo. Un consenso dato in una situazione medica sotto la minaccia di non essere curati o di ricevere cure peggiori non può essere considerato 'libero'. (...) qualora la situazione medica imponga in modo necessario e inevitabile all'operatore sanitario di trattare i dati personali in un sistema di CEE [cartelle cliniche elettroniche], è fuorviante che questi cerchi di legittimare tale operazione attraverso il consenso dell'interessato.

Il fatto di basarsi sul consenso dovrebbe essere limitato ai casi in cui la persona interessata è veramente libera di scegliere e può in seguito ritirare tale consenso senza venire danneggiata".<sup>18</sup>

Il Gruppo di lavoro ha adottato una posizione coerente sull'interpretazione di libero consenso nel contesto dell'occupazione<sup>19</sup>, sostenendo che se al lavoratore è richiesto un.

### **Esempio: immagini sulla Intranet**

» possibile che il consenso rilasciato nell'ambito dell'occupazione sia valido, come illustra il seguente esempio: una società decide di creare un'Intranet in cui saranno pubblicati i nomi e le principali funzioni dei dipendenti. A ciascun dipendente è chiesto se vuole far pubblicare la sua fotografia accanto al nome. Le persone che accettano sono invitate a inviare una loro fotografia a un determinato indirizzo. L'azione di una persona che, essendo stata adeguatamente informata, decide di inviare la sua fotografia sarebbe equiparata a un consenso. Se la società dispone di immagini digitali di ciascun dipendente e chiede a ognuno il consenso a caricare tali fotografie sull'intranet per gli scopi sopra descritti, il fatto che un dipendente clicchi su un tasto per fornire il suo consenso sarà parimenti considerato una forma di consenso valido. In entrambi i casi, la scelta del dipendente di accettare o meno che la propria fotografia sia caricata sull'Intranet è pienamente rispettata.

Il contesto dell'occupazione richiede una discussione specifica. In questo caso, infatti, entrano in gioco gli aspetti culturali e sociali del rapporto di lavoro, così come il modo in cui i principi della protezione dei dati interagiscono con altre leggi. Nel contesto dell'occupazione, i dati personali possono essere trattati per scopi diversi:

- o dati necessari perché il dipendente possa svolgere le proprie mansioni: applicazione dell'articolo 7, lettera b) – necessità per l'esecuzione del contratto;
- o per determinare il diritto dei dipendenti ad acquisire stock option: ciò potrebbe avvenire sia in base a un consenso - articolo 7, lettera a), o essere considerato un aspetto intrinseco agli aspetti amministrativi del contratto di lavoro - articolo 7, lettera b);
- o trattamento del numero di sicurezza sociale a scopi di sicurezza sociale: articolo 7, lettera c) – obbligo giuridico, o anche articolo 8, lettera b) – obblighi in materia di diritto del lavoro;
- o trattamento di dati di carattere etnico: in alcuni paesi, questo potrebbe essere un obbligo in materia di diritto di lavoro - articolo 8, lettera b), mentre in altri sarebbe rigorosamente vietato.

Benché, in contesti di questo genere, possa sussistere il forte sospetto che il consenso fornito sia debole, di per sé ciò non basta a escludere del tutto il ricorso al consenso, purché vi siano garanzie sufficienti che si tratti veramente di una manifestazione di volontà libera.

Se una situazione di subordinazione rappresenta sovente il principale motivo che impedisce al consenso di essere libero, esistono anche altre circostanze che possono influenzare la decisione dell'interessato. Tali aspetti possono essere, per esempio, correlati alla dimensione economica, o a una dimensione emotiva o pratica. Anche il fatto che la raccolta di dati sia espletata da un'autorità pubblica può influenzare in qualche modo l'interessato. Può tuttavia essere difficile distinguere tra un semplice incentivo e qualcosa che può realmente influenzare la libertà dell'interessato nell'operare una scelta. Gli esempi che seguono intendono illustrare la diversa natura degli sforzi o dei costi per gli interessati che potrebbero influenzarne la decisione.

### **Esempio– Cartelle cliniche elettroniche**

In molti Stati membri si sta cercando di creare una scheda elettronica sintetica delle cartelle cliniche dei pazienti. In questo modo gli operatori sanitari potranno accedere a informazioni fondamentali relative al paziente ogniqualvolta quest'ultimo necessiti di cure.

- Nel primo scenario, la creazione della scheda sintetica è assolutamente volontaria e il paziente continua a ottenere le cure, indipendentemente dal fatto che abbia consentito o meno alla creazione di tale scheda elettronica. In questo caso il consenso alla creazione della scheda sintetica è una manifestazione di volontà libera, perché non si prospettano svantaggi per il paziente nel caso in cui quest'ultimo non accordi il proprio consenso o decida di revocarlo.

- Nel secondo scenario, si propone un modesto incentivo economico a optare per la cartella clinica elettronica. I pazienti che sono contrari alla cartella clinica elettronica non vanno incontro a svantaggi, nel senso che le spese sanitarie loro imputate non subiscono variazioni. Anche in questa situazione si

potrebbe considerare che i pazienti sono liberi di accordare o meno il proprio consenso al nuovo sistema.

- Nel terzo scenario i pazienti che rifiutano il sistema dei servizi sanitari on-line sono costretti a pagare un notevole costo supplementare rispetto al precedente sistema tariffario e il trattamento del loro caso subisce notevoli ritardi. Ciò equivale a un netto svantaggio per le persone che non accettano il nuovo sistema, il cui scopo è indurre tutti i cittadini a optare per il sistema dei servizi sanitari online entro un determinato termine. Il consenso non può pertanto essere considerato una manifestazione sufficientemente libera di volontà. In tal caso si dovrebbe quindi valutare l'esistenza di altri motivi legittimanti per il trattamento dei dati personali o considerare l'applicazione dell'articolo 8, paragrafo 3, della direttiva 95/46/CE.

### **Esempio: scansionatori del corpo (body scanner)**

Il ricorso a body scanner si sta diffondendo in alcuni luoghi pubblici, in particolare negli aeroporti per l'accesso all'area di imbarco. Considerando che i dati dei passeggeri sono trattati al momento in cui avviene la scansione<sup>20</sup>, il trattamento deve essere conforme a uno dei motivi di liceità di cui all'articolo 7. Talvolta la scansione con il body scanner è presentata ai passeggeri come un'opzione, il che implicherebbe che il trattamento potrebbe essere giustificato dal consenso eventualmente accordato. Tuttavia, il rifiuto a sottoporsi alla scansione potrebbe creare sospetti o far scattare controlli supplementari, tra i quali una perquisizione personale. Molti passeggeri acconsentono alla scansione per evitare, così facendo, potenziali problemi o ritardi, laddove la loro massima priorità consiste nel salire a bordo puntualmente. Il consenso così espresso non rappresenta quindi una manifestazione sufficientemente libera di volontà. Poiché è obbligatorio dimostrare che il trattamento è necessario (per ragioni di sicurezza pubblica), il motivo legittimante non va rinvenuto nell'articolo 7, lettera a), bensì in un atto del legislatore – articolo 7, lettere c) o e) – risultante nell'obbligo a collaborare posto in capo ai passeggeri. Il fondamento giuridico per procedere al controllo con il body scanner dovrebbe pertanto essere la legislazione: tale legislazione potrebbe comunque prevedere la possibilità di scegliere tra la scansione e il controllo manuale, ma tale scelta verrebbe offerta al singolo soltanto a fini di integrazione, ossia nell'ambito di misure aggiuntive.

Anche la natura del titolare del trattamento può essere decisiva in relazione alla scelta del criterio che legittima il trattamento dei dati personali» questo il caso, in particolare, dei responsabili del trattamento del settore pubblico, dove il trattamento dei dati è solitamente collegato all'adempimento di un obbligo giuridico come specificato all'articolo 7, lettera c), o all'esecuzione di un compito di interesse pubblico, secondo il disposto dell'articolo 7, lettera e). Di conseguenza, il ricorso al consenso dell'interessato per legittimare il trattamento dei dati non rappresenta il fondamento giuridico appropriato. Ciò è particolarmente evidente nel caso del trattamento dei dati personali da parte delle autorità pubbliche dotate di potestà d'imperio, tra cui le autorità che agiscono nell'ambito delle proprie funzioni nel corso di attività di polizia e giudiziarie. Le autorità di polizia non possono avvalersi del consenso dell'interessato per mettere in atto misure che non sono previste, o che non sarebbero altrimenti consentite, dalla legge.

Si deve riconoscere tuttavia che, benché gli Stati possano essere giuridicamente obbligati al trattamento dei dati personali, non sempre l'interessato è tenuto a collaborare. Si può ipotizzare il caso in cui "servizi a valore aggiunto" sono offerti agli interessati, che possono decidere di utilizzarli o meno. Nella maggior parte dei casi, però, il trattamento è effettivamente obbligatorio. Spesso non è così semplice stabilire se il trattamento dei dati personali da parte delle autorità pubbliche poggia, legittimamente, sul consenso del soggetto interessato. Il trattamento di dati personali nel settore pubblico, pertanto, comporta sovente dei sistemi ibridi, che possono dare adito a incertezze e abusi, se erroneamente giustificati dal consenso.

Se il consenso può, in casi eccezionali, rappresentare un motivo valido addotto dagli Stati per legittimare il trattamento dei dati, sarebbe opportuno effettuare, caso per caso, un'attenta verifica atta a stabilire se il consenso sia effettivamente una manifestazione di volontà sufficientemente libera. Come dimostrano gli esempi seguenti, quando il titolare del trattamento è un'autorità pubblica, il fondamento giuridico che legittima il trattamento non è il consenso bensì la conformità all'obbligo giuridico di cui all'articolo 7, lettera c), o l'esecuzione di un compito di interesse pubblico ai sensi dell'articolo 7, lettera e).

### **Esempio: pubblica amministrazione on-line**

Negli Stati membri sono in fase di realizzazione nuove carte d'identità con funzionalità elettroniche incorporate in un chip. Attivare i servizi elettronici della carta può non essere obbligatorio. Tuttavia, l'utente che rinuncia all'attivazione potrebbe non avere accesso a taluni servizi amministrativi che altrimenti sarebbe estremamente difficile ottenere (trasferimento di alcuni servizi online, riduzione dell'orario di lavoro degli uffici). Non è possibile in tal caso dichiarare che il consenso rappresenta il motivo legittimante che giustifica il trattamento. Il fondamento giuridico dovrebbe essere, piuttosto, la legge che disciplina lo sviluppo dei servizi on line, unitamente a tutte le salvaguardie appropriate.

### **Esempio: dati del codice di prenotazione (PNR)**

» stata discussa la questione se il consenso dei passeggeri possa essere validamente utilizzato per legittimare il trasferimento dei dati personali dei passeggeri ("Passenger Name Record, PNR") da parte delle compagnie aeree europee alle autorità statunitensi. Il Gruppo di lavoro è del parere che il consenso dei passeggeri non possa essere una manifestazione di volontà libera, poiché le compagnie aeree sono obbligate a inviare i dati prima della partenza del volo, e pertanto i passeggeri non hanno libertà di scelta se desiderano effettuare il volo.<sup>21</sup> Il fondamento giuridico qui non è tanto il consenso del passeggero bensì, conformemente all'articolo 7, lettera c), gli obblighi previsti dall'accordo internazionale stipulato tra l'UE e gli USA sul trattamento e sul trasferimento dei dati del passeggero.

### **"... specifica ..."**

Per essere valido, il consenso dev'essere specifico. In altri termini, un consenso totale, senza che sia specificato lo scopo preciso del trattamento, non è accettabile.

Per essere specifico, il consenso dev'essere comprensibile: dovrebbe cioè riferirsi chiaramente e precisamente al campo di applicazione e alle conseguenze del trattamento dei dati. Non può riferirsi a un insieme illimitato di attività di trattamento. Ciò significa, in altre parole, che il contesto al quale si applica il consenso è limitato.

Il consenso dev'essere accordato in relazione ai diversi aspetti del trattamento, chiaramente identificati.» necessario, in particolare, che siano specificati il tipo di dati oggetto di trattamento e le finalità del trattamento. Questa interpretazione dovrebbe essere fondata sulle aspettative ragionevoli delle parti. La nozione di "consenso specifico" è pertanto intrinsecamente correlata al fatto che il consenso deve essere informato. Sussiste un obbligo di articolazione del consenso per quanto concerne i vari elementi che costituiscono il trattamento dei dati: non si può pensare cioè che il consenso si riferisca a "tutti gli scopi legittimi" perseguiti dal titolare del trattamento. Il consenso si dovrebbe riferire alle forme di trattamento che risultano ragionevoli e necessarie rispetto allo scopo.

In linea di principio, per i responsabili del trattamento dovrebbe essere sufficiente ottenere il consenso una volta sola, per operazioni diverse, se queste rientrano nelle aspettative ragionevoli dell'interessato.

Recentemente la Corte di giustizia dell'Unione europea si è pronunciata in via pregiudiziale<sup>22</sup> in merito all'articolo 12, paragrafo 2, della direttiva relativa alla vita

privata e alle comunicazioni elettroniche, sulla necessità di ottenere nuovamente il consenso degli abbonati che abbiano già acconsentito alla pubblicazione dei propri dati personali in un elenco al trasferimento di tali dati personali ai fini della pubblicazione da parte di altri servizi di consultazione. La Corte ha stabilito che, quando un abbonato sia stato correttamente informato della possibilità della trasmissione dei dati personali che lo riguardano a un'impresa terza, e questi abbia acconsentito alla pubblicazione di tali dati in un simile elenco, la trasmissione degli stessi dati non deve essere nuovamente oggetto di un consenso da parte dell'abbonato, "qualora venga garantito che i dati in questione non saranno usati per scopi diversi da quelli per cui sono stati raccolti al fine della loro prima pubblicazione" (punto 65).

Può essere tuttavia necessario ottenere un distinto consenso se il titolare del trattamento intende trattare i dati per finalità diverse. Per esempio, l'interessato potrebbe acconsentire sia all'invio di informazioni su nuovi prodotti sia all'utilizzo dei suoi dati per specifiche azioni di promozione, poiché questa situazione potrebbe essere fatta rientrare nelle ragionevoli aspettative dell'interessato. Al contrario, si dovrebbe richiedere un consenso distinto e supplementare per essere autorizzati a trasmettere i dati dell'interessato a terzi. La necessità di ottenere un consenso articolato dovrebbe essere valutata caso per caso, a seconda degli scopi o dei destinatari dei dati.

Si rammenta che il trattamento potrebbe avere molti e diversi fondamenti giuridici: alcuni dati potrebbero essere sottoposti a trattamento perché necessari nell'ambito di un contratto concluso con l'interessato, per esempio per dare esecuzione a un ordine o per gestire il servizio di assistenza, mentre un consenso specifico potrebbe essere richiesto ai fini del trattamento per scopi che trascendono l'esecuzione del contratto, per esempio per valutare il grado di affidabilità creditizia (credit scoring) dell'interessato.

Il Gruppo di lavoro ha chiarito questo aspetto del consenso nel WP131 sulle cartelle cliniche elettroniche (CCE): "il consenso 'specifico' deve riferirsi a una situazione ben definita e concreta in cui si prevede un trattamento dei dati medici. Pertanto un 'consenso generale' dell'interessato – ad esempio alla raccolta dei suoi dati medici per una CCE e ai trasferimenti successivi di tali dati, passati e futuri, a operatori sanitari coinvolti nella cura – non costituisce un consenso conformemente all'articolo 2, lettera h) della direttiva".

Lo stesso ragionamento è espresso nel parere WP 115 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto: "[La] definizione esclude esplicitamente che il consenso possa essere prestato nel quadro dell'accettazione delle condizioni generali del servizio di comunicazioni elettroniche offerto. (...), a seconda del tipo di servizio offerto, il consenso può riguardare un'operazione specifica o può costituire un'accettazione del fatto di essere localizzati su base continuativa".

Nella decisione della Corte menzionata al capitolo II, "Ruolo del consenso", anche se il termine "specifico" non viene esplicitamente usato, la motivazione insiste anche sulla necessità che il consenso sia specifico sostenendo che "non è sufficiente che il contratto di lavoro dell'interessato faccia riferimento a un contratto collettivo che consente tale superamento".

### **Esempio: i social network**

L'accesso ai servizi di social network è spesso condizionato al rilascio di un'autorizzazione a forme diverse di trattamento dei dati personali.» possibile che, per potersi registrare a un servizio di social network, l'utente debba accettare l'invio di pubblicità comportamentali, senza la possibilità di ricevere ulteriori chiarimenti o di avere opzioni alternative. Considerando l'importanza acquisita da alcuni socialnetwork, talune categorie di utenti (come gli adolescenti) accetteranno di ricevere messaggi di pubblicità comportamentale per evitare il rischio di essere parzialmente esclusi dalle interazioni sociali. L'utente dovrebbe essere messo in condizione di dare un consenso libero e specifico in merito

all'invio di messaggi di pubblicità comportamentale, indipendentemente dall'accesso al servizio di social network. Per concedere all'utente questa possibilità si potrebbe utilizzare una finestra pop-up. Il servizio di social network offre la possibilità di usare applicazioni esterne. In pratica, all'utente viene spesso impedito di usare un'applicazione se non acconsente alla trasmissione dei suoi dati allo sviluppatore dell'applicazione stessa per una varietà di scopi, tra cui la pubblicità comportamentale e la trasmissione a parti terze. Poiché l'applicazione può funzionare senza che vi sia un trasferimento di dati allo sviluppatore dell'applicazione stessa, il Gruppo di lavoro invita a prevedere una maggiore granularità nell'ottenimento del consenso dell'utente, vale a dire che lo sviluppatore deve ottenere un distinto consenso per ciascuno dei vari scopi. Diversi meccanismi, ad esempio finestre pop-up, possono essere utilizzati per consentire all'utente di scegliere il tipo di utilizzo dei dati che lo riguardano (trasferimento allo sviluppatore; servizi a valore aggiunto; pubblicità comportamentale; trasferimento a terzi; ecc.).

In molti casi il consenso è ottenuto al momento della raccolta dei dati personali, ossia quando ha inizio il trattamento. In tal caso, le informazioni da fornire coincidono con quelle elencate all'articolo 10 della direttiva. Il consenso, tuttavia, può anche essere richiesto "a valle", quando cioè si hanno variazioni nelle finalità del trattamento. In tal caso le informazioni da fornire dovranno limitarsi a quanto necessario nel contesto specifico, in relazione alla finalità del trattamento.

Il consenso informato è particolarmente decisivo nell'ambito dei trasferimenti di dati personali a paesi terzi, dove l'obbligo di informazione "prescrive che l'interessato sia informato adeguatamente sul rischio specifico che i suoi dati vengano trasferiti in un paese che non garantisce una tutela adeguata"<sup>24</sup>. Qualità dell'informazione – Il modo in cui è fornita l'informazione (mediante un linguaggio chiaro, privo di espressioni gergali, comprensibile, manifesto) è fondamentale per stabilire se il consenso è "informato". Il modo in cui le informazioni devono essere fornite dipende dal contesto: dovrebbero cioè essere comprensibili a un utente regolare/medio.

Accessibilità e visibilità delle informazioni – le informazioni devono essere fornite direttamente agli individui interessati. Non è sufficiente che le informazioni siano "disponibili" da qualche parte. Su questo punto ha insistito la Corte di giustizia nella sua sentenza del 2004<sup>25</sup>, riferendosi a un contratto di lavoro che non precisava le condizioni di lavoro ma rinviava ad altri documenti.

Le informazioni devono essere chiaramente visibili (tipo e dimensioni dei caratteri), rilevanti ed esauritive. Possono essere utilizzate finestre di dialogo per fornire informazioni specifiche al momento della richiesta del consenso. Come si è detto riguardo al "consenso specifico", gli strumenti di informazione on-line sono particolarmente utili per i servizi di social network, perché garantiscono sufficienti granularità e chiarezza per le situazioni concernenti la vita privata. Anche gli avvisi a più livelli possono essere un utile strumento a questo proposito, poiché contribuiscono a fornirle giuste informazioni in maniera facilmente accessibile.

Con il passare del tempo possono sorgere dubbi sulla validità del consenso originariamente rilasciato sulla base di informazioni valide e sufficienti. Per una serie di motivi, la gente spesso cambia idea, vuoi perché le scelte iniziali sono state avventate, vuoi perché le circostanze sono cambiate, come nel caso di un adolescente che, crescendo, è maturato<sup>26</sup>. Ecco perché i responsabili del trattamento, di prassi, dovrebbero sforzarsi di rivedere periodicamente le scelte di un individuo, per esempio mettendoli al corrente della loro scelta attualmente valida e offrendo loro la possibilità di confermare il consenso o di revocarlo<sup>27</sup>. L'intervallo di tempo in questione dipende ovviamente dal contesto e dalle circostanze del caso. "La presa d'atto di un preavviso secondo cui avrà luogo un qualche tipo di pubblicazione non equivale a manifestare 'senza ambiguità' il proprio consenso a un certo tipo di pubblicazione particolareggiata. Né può essere propriamente descritta come una 'manifestazione libera e

specifica 'della volontà dei richiedenti secondo la definizione del consenso della persona interessata di cui all'art. 2, lettera h)". L'avvocato generale ha pertanto ritenuto che i ricorrenti non avessero manifestato il proprio consenso al trattamento (vale a dire, alla pubblicazione) dei loro dati personali ai sensi dell'articolo 7, lettera a), della direttiva 95/46/CE.<sup>29</sup>

Il consenso esplicito può anche essere manifestato nell'ambiente online. Proprio come avviene offline, esistono mezzi perfettamente adatti a manifestare il consenso in maniera inequivocabile, come bene illustra il seguente esempio.

**Esempio: consenso on-line a essere arruolato in un programma di fedeltà**

Il sito web di un albergo contiene un modulo di prenotazione che permette ai visitatori di effettuare la prenotazione anticipata di una camera on-line. Il modulo on-line in cui l'interessato inserisce le date previste per il soggiorno e le informazioni sulle modalità di pagamento contiene anche una casella visibile, che l'interessato può selezionare se desidera che i suoi dati siano utilizzati per l'arruolamento in un programma di fedeltà. Il fatto di selezionare la casella, dopo aver ricevute informazioni del caso, equivarrebbe alla manifestazione di un consenso esplicito in maniera inequivocabile, poiché tale azione è sufficientemente chiara da non lasciare adito a dubbi circa la volontà dell'interessato a essere arruolato nel programma di fedeltà.

Il consenso esplicito può inoltre essere fornito verbalmente, mediante dichiarazioni volte a manifestare l'assenso. Il consenso esplicito fornito verbalmente potrebbe essere manifestato in una situazione analoga alla seguente.

**Esempio: consenso verbale a ricevere informazioni promozionali**

Durante le operazioni di saldo del conto effettuate dai clienti di un albergo in partenza, l'impiegato alla reception chiede ai clienti l'autorizzazione a utilizzare il loro indirizzo da parte dell'albergo ai fini dell'invio di materiale promozionale. I clienti che, dopo aver ricevuto tutte le informazioni necessarie, accettano di comunicare il proprio indirizzo postale manifestano il proprio consenso esplicito. L'azione di fornire il proprio indirizzo può costituire una manifestazione inequivocabile della volontà del soggetto interessato. Il titolare del trattamento, tuttavia, potrebbe decidere di ricorrere a meccanismi che gli permettono di dimostrare in maniera più affidabile che il consenso è stato accordato.

In alcune circostanze il consenso inequivocabile potrebbe essere dedotto da talune azioni, come nel caso, in particolare, di azioni da cui si può concludere senza tema di errore che il consenso è stato concesso. Ciò, tuttavia, è correlato all'effettiva trasmissione di informazioni pertinenti sul trattamento dei dati, che permettano all'interessato di prendere una decisione al riguardo (in relazione all'identità del titolare del trattamento, alle finalità del trattamento, ecc.).

**Esempio: consenso a essere fotografati**

Durante le procedure di accettazione dei clienti in un albergo, l'impiegato alla reception informa gli ospiti che, nel pomeriggio, nel bar dell'albergo saranno scattate delle fotografie. Le immagini selezionate saranno utilizzate a scopo promozionale, in particolare per la produzione di opuscoli cartacei dell'albergo. Se gli ospiti dell'albergo desiderano essere fotografati, sono invitati a presentarsi nel bar negli orari indicati. Al contrario, chi non desidera comparire sulle fotografie può utilizzare l'altro bar dell'albergo.

Si può ritenere che gli ospiti che, essendo stati informati al riguardo, decidono di recarsi al bar nell'orario indicato per il servizio fotografico abbiano manifestato il proprio consenso a essere fotografati. La manifestazione del consenso è deducibile dall'atto di recarsi nel bar in cui è in corso il servizio fotografico nell'orario stabilito. La frequentazione del bar in questo orario costituisce una manifestazione della volontà dell'interessato, che in linea di principio può essere considerata inequivocabile,

giacché non vi è dubbio che la persona che si reca nel bar desidera essere fotografata. L'albergo, tuttavia, potrebbe ritenere prudente disporre di prove documentali del consenso ottenuto, nell'eventualità in cui in futuro la validità del consenso espresso possa essere contestata.

Come si è detto, i medesimi requisiti, anche in materia di manifestazione del consenso in maniera inequivocabile, si applicano tanto offline quanto on-line. Nonostante ciò, il Gruppo di lavoro osserva che il rischio che un consenso possa essere considerato ambiguo è maggiore in un'ambiente on-line, e questo aspetto merita perciò un'attenzione specifica. Il prossimo esempio illustra un caso in cui il consenso dedotto da un determinato comportamento (partecipazione a un gioco on-line) non soddisfa i requisiti per un valido consenso.

### **Esempio: gioco online**

Un fornitore di giochi online chiede ai visitatori che desiderano partecipare al gioco di specificare età, nome e cognome e indirizzo (i giocatori vengono suddivisi per età e indirizzi). Il sito web riporta un avviso, accessibile attraverso un link (benché l'accesso a tale avviso non sia obbligatorio per poter partecipare al gioco), in cui si precisa che utilizzando il sito web (e quindi fornendo le informazioni) i giocatori acconsentono al trattamento dei dati da parte del fornitore del gioco online e di parti terze ai fini dell'invio di informazioni commerciali.

L'accesso e la partecipazione al gioco non possono essere equiparati alla manifestazione inequivocabile del consenso al trattamento delle informazioni personali per finalità diverse dalla partecipazione al gioco. Il fatto che l'interessato partecipi al gioco non implica che egli intende acconsentire al trattamento dei suoi dati al di là di quanto necessario ai fini del gioco. Questo tipo di comportamento non costituisce una manifestazione inequivocabile della volontà dell'interessato ad accettare l'utilizzo dei suoi dati per finalità commerciali.

### **Esempio: impostazioni di default e vita privata**

Le impostazioni di default di un socialnetwork, a cui gli utenti non necessariamente devono accedere per utilizzare la rete, consentono all'intera categoria "amici degli amici" di rendere visibili le informazioni personali di ciascun utente a tutti gli "amici degli amici". Agli utenti che non desiderano che le proprie informazioni siano visualizzate dagli "amici degli amici" è richiesto di cliccare un tasto. Il titolare del trattamento riterrà che le persone che adottano un atteggiamento passivo, o non compiono l'operazione consistente nel cliccare un tasto, abbiano acconsentito alla visualizzazione dei propri dati. Tuttavia, è dubbio che il fatto di non cliccare sul tasto significhi che la stragrande maggioranza delle persone acconsentano di rendere accessibili le informazioni che le riguardano a tutti gli amici degli amici. Per via dell'incertezza circa la possibilità che una mancata azione possa equivalere a una manifestazione di consenso, il fatto di non cliccare non può essere considerato una manifestazione di consenso in maniera inequivocabile.

L'esempio precedente illustra un caso in cui l'interessato rimane passivo (per esempio, mancata azione o "silenzio"). Un consenso inequivocabile al si concilia con procedure per l'ottenimento del consenso basate sull'inazione o sul silenzio degli interessati: il silenzio o l'inazione di una parte è caratterizzato da un'ambiguità intrinseca (l'interessato cioè potrebbe aver avuto l'intenzione di manifestare il suo consenso o semplicemente potrebbe essere stato intenzionato a non eseguire l'azione). L'esempio seguente spiega più chiaramente questo concetto.

Sussiste ambiguità nella circostanza in cui si ritiene che una persona abbia manifestato il proprio consenso per il fatto di non aver risposto a una lettera con cui veniva informata che un mancato riscontro equivaleva un'espressione di assenso. In questo genere di circostanza, il comportamento in-



dividuale (o piuttosto la mancata azione) solleva forti dubbi sull'intenzione del soggetto di manifestare il proprio assenso. Il fatto che il soggetto in questione non abbia compiuto alcuna azione attiva non è sufficiente per concludere che l'assenso sia stato accordato. Pertanto, questa forma di consenso non soddisfa i requisiti della manifestazione inequivocabile del consenso. Oltretutto, come si avrà modo di dimostrare di seguito, sarà anche estremamente difficile per il titolare del trattamento fornire le prove a conferma della manifestazione di assenso dell'interessato.

Il Gruppo di lavoro ha già ribadito l'inadeguatezza di un consenso fondato sul silenzio degli interessati nel contesto dell'invio di comunicazioni tramite posta elettronica a fini di commercializzazione diretta: "Il consenso implicito a ricevere tali messaggi non è compatibile con la definizione di consenso stabilita dalla direttiva 95/46/CE (...). Analogamente, neppure le caselle preselezionate, ad esempio nei siti web, sono compatibili con la definizione della direttiva"<sup>30</sup>. Il seguente esempio conferma tale posizione:

#### **Esempio: consenso non valido ai fini di utilizzi supplementari di dati dei clienti**

Un rivenditore di libri online invia un messaggio di posta elettronica ai clienti partecipanti al suo programma di fedeltà, informandoli che i loro dati saranno trasmessi a una società pubblicitaria, che è intenzionata a utilizzarli a scopo di marketing. Gli utenti hanno due settimane di tempo per rispondere al messaggio di posta elettronica. Essi sono informati che il mancato riscontro sarà considerato alla stregua di un consenso al trasferimento dei dati. Questo tipo di meccanismo, in base al quale il consenso è ottenuto dall'assenza di una risposta da parte degli interessati, non permette di ottenere un consenso valido e privo di ambiguità. Non è possibile, infatti, stabilire senza ombra di dubbio che, con il mancato riscontro, gli interessati abbiano accettato il trasferimento dei dati.

Da quanto precede deriva che, alla luce dell'obbligo concernente la manifestazione di un consenso inequivocabile, i responsabili del trattamento sono incoraggiati di fatto a mettere a punto procedure e meccanismi che non lascino dubbi circa la manifestazione del consenso, vuoi sulla base di un'azione esplicita dell'interessato, vuoi deducendolo chiaramente da un comportamento dell'interessato.

Come si è detto in precedenza, per buona pratica i responsabili del trattamento dovrebbero considerare l'opportunità di mettere in opera misure e procedure pertinenti per dimostrare che il consenso è stato rilasciato. Più è complicato l'ambiente in cui operano, maggiori saranno le misure che sarà necessario attuare per garantire che il consenso sia verificabile. Su richiesta, tali informazioni dovrebbero essere messe a disposizione dell'autorità per la protezione dei dati.

#### **III.A.3. Articolo 8, paragrafo 2, lettera a)**

L'articolo 8 della direttiva conferisce una protezione speciale a "categorie particolari di dati" che per loro natura sono considerati estremamente sensibili. Il trattamento di tali dati è vietato a meno che non si applichi almeno una delle deroghe elencate. L'articolo 8, paragrafo 2, lettera a), stabilisce che il divieto non si applica se l'interessato ha dato il proprio consenso esplicito al trattamento.

Nel linguaggio giuridico, l'espressione "consenso esplicito" (explicit) equivale all'espressione "consenso manifesto" (express). Essa cioè comprende tutte le situazioni in cui agli interessati è proposto di accettare o rifiutare un particolare utilizzo oppure l'oscuramento di informazioni personali che li riguardano ed essi rispondono attivamente a tale proposta, verbalmente o per iscritto.

Generalmente, il consenso esplicito o manifesto è concesso per iscritto ed è accompagnato da una firma scritta a mano. Per esempio, il consenso esplicito è dato quando gli interessati firmano un modulo per il consenso che specifica chiaramente le ragioni per cui un titolare del trattamento desidera raccogliere e trattare i loro dati personali.

Sebbene tradizionalmente il consenso esplicito sia manifestato in forma scritta, su carta o in formato elettronico, come si è avuto modo di precisare nel precedente capitolo III.A.2, la forma scritta non è indispensabile, pertanto, il consenso può essere manifestato anche verbalmente. Ciò è confermato dal fatto che la prescrizione relativa al consenso in forma scritta originariamente prevista dall'articolo 8 è stata successivamente soppressa nel testo definitivo della direttiva. Vero è, però, come si è avuto modo di spiegare nel medesimo capitolo, che potrebbe essere difficile dimostrare a posteriori di aver effettivamente ottenuto un consenso verbale, per cui nella pratica si suggerisce ai responsabili del trattamento di ricorrere al consenso scritto a scopo probatorio.

L'obbligo di ottenere un consenso esplicito significa che il consenso dedotto dalle circostanze non soddisfa normalmente il disposto dell'articolo 8, paragrafo 2. A tale proposito, vale la pena rammentare il parere del Gruppo di lavoro "Articolo 29" sulle cartelle cliniche elettroniche<sup>31</sup>, laddove esso recita che "Diversamente da quanto disposto dall'articolo 7 della direttiva, nel caso di dati personali sensibili, e quindi delle CCE, il consenso deve essere esplicito. Non soddisfa il criterio del carattere 'esplicito' la soluzione del silenzio-assenso (opt-out)."

#### **Esempio: dati medici a scopo di ricerca**

Il caso di un paziente che viene informato da una clinica sul fatto che il suo fascicolo medico sarà trasmesso a un ricercatore a meno che il paziente non sollevi obiezioni in tal senso (chiamando un numero) non soddisfa il requisito del consenso esplicito.

Come si è detto al capitolo II.A.2, gli interessati possono dare un consenso esplicito, verbalmente e anche per iscritto, intraprendendo un'azione positiva per manifestare la propria volontà di accettare una certa forma di trattamento dei dati. Nell'ambiente on-line il consenso esplicito può essere manifestato con la firma elettronica o digitale. Può anche tuttavia essere dato cliccando un tasto a seconda del contesto, per esempio per inviare messaggi di conferma o cliccando su un'icona, ecc.<sup>32</sup> L'approvazione di procedure che implicano un'azione deliberata da parte dell'interessato è implicitamente riconosciuta dal considerando 17 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, in base al quale "Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet".<sup>33</sup> Il bisogno di disporre di prove indiscutibili

un ambiente on-line, in modo da potervi accedere per un riferimento futuro.<sup>34</sup>

Alla luce di quanto precede, si ritiene che i moduli di registrazione online da compilare con informazioni personali necessarie all'identificazione e al fine di manifestare il consenso al trattamento dei dati soddisfino il requisito riguardante il consenso esplicito, a condizione che siano rispettati tutti gli altri requisiti. Per esempio, per aprire un fascicolo medico on-line personalizzato, i pazienti possono dare il proprio consenso fornendo il proprio recapito e cliccando su un'apposita casella in segno di accettazione del trattamento dei dati. Ovviamente il ricorso a metodi d'autenticazione più rigorosi, come l'uso della firma digitale, permetterà di ottenere il medesimo risultato e costituirà una prova più solida<sup>35</sup>.

#### **III.A.4. Articolo 26, paragrafo 1**

L'articolo 26, paragrafo 1, lettera a), introduce il consenso inequivocabile tra le deroghe al divieto di trasferimento di dati a paesi terzi che non garantiscono un livello di protezione adeguato. Le riflessioni formulate in precedenza in merito all'articolo 7, lettera a), valgono anche in questa circostanza, nel senso che, oltre alle condizioni necessarie per il consenso valido a norma dell'articolo 2, lettera g), il consenso deve anche essere manifestato in maniera inequivocabile.

Il Gruppo di lavoro "Articolo 29" si è espresso più volte fornendo indicazioni sull'applicazione dell'articolo 25 e dell'articolo 26 della direttiva, ivi compresa la deroga del consenso. A tale proposito vale la pena menzionare il documento del gruppo di lavoro WP1236, che precisa il significato di consenso inequivocabile: "Poiché il consenso dev'essere inequivocabile, anche il dubbio sul fatto che esso sia stato dato rende la deroga inapplicabile. Ciò potrebbe significare che molte situazioni in cui il consenso è implicito (ad esempio perché un individuo è stato informato su un trasferimento e non si è opposto) non giustificano questa deroga".

Nel documento WP 11437, in relazione all'uso del consenso per il trasferimento di dati, il Gruppo di lavoro ha dichiarato di ritenere che "(...) il consenso non possa fornire un quadro adeguato a lungo termine per i responsabili del trattamento in caso di trasferimenti ripetuti o anche strutturali per il trattamento in questione. Infatti, specialmente se il trasferimento è parte intrinseca del trattamento principale (ad es. la centralizzazione di una banca dati di risorse umane a livello mondiale, che, per essere operativa, deve essere alimentata da trasferimenti di dati continui e sistematici), i responsabili del trattamento potrebbero trovarsi in situazioni irrisolvibili se solo una delle persone interessate decidesse di ritirare il proprio consenso. A rigor di termini, i dati relativi a una persona che abbia revocato il consenso non potrebbero più essere trasferiti; in mancanza di ciò, il trasferimento continuerebbe ad essere parzialmente basato sul consenso delle persone interessate, ma dovrebbe essere trovata una soluzione alternativa (contratto, NVI, ecc.) per i dati delle persone che hanno revocato il consenso. Il ricorso al consenso può pertanto rivelarsi una 'falsa buona soluzione', a prima vista semplice ma in realtà complessa e onerosa."

### **III.A.5. Consenso fornito da soggetti privi della piena capacità di agire**

La direttiva 95/46/CE non contiene disposizioni specifiche sulla manifestazione del consenso da parte di persone prive della capacità di agire, tra cui i minori. » importante che questo aspetto sia considerato nel contesto della revisione della direttiva in materia di protezione dei dati. Oltre alle problematiche sollevate fin qui, il consenso di queste persone presenta sue proprie complessità specifiche.

Per quanto concerne i minori, le condizioni per il rilascio di un consenso valido variano da Stato membro a Stato membro. In più occasioni il Gruppo di lavoro "Articolo 29" ha avuto modo di riflettere sulla questione del consenso dei minori e ha preso in esame le prassi in vigore a livello nazionale<sup>38</sup>.

Dai precedenti lavori emerge che, per richiedere il consenso di un minore, la legge può prevedere che si ottenga il consenso del minore e del suo rappresentante, oppure il solo consenso del minore se questi è già maturo. Le età a cui si applica l'uno o l'altro caso sono diverse. Non esistono procedure armonizzate per verificare l'età di un minore.

L'assenza di norme generali in tal senso è la causa della frammentarietà dell'approccio in uso ed esclude la necessità di una protezione specifica per il minore in circostanze particolari, sia per la sua vulnerabilità sia per le incertezze giuridiche che ne scaturiscono, in particolare in merito alle modalità con cui il consenso del minore viene ottenuto.

Il Gruppo di lavoro è del parere che tale mancanza di armonizzazione abbia conseguenze in termini di certezza del diritto. La decisione di armonizzare le condizioni necessarie per consentire a soggetti privi della capacità di agire di esercitare i propri diritti a livello di UE, soprattutto per quanto concerne la soglia di età, offrirebbe senz'altro nuove garanzie. Tuttavia, il Gruppo di lavoro è consapevole che questa decisione potrebbe travalicare l'ambito di applicazione della protezione dei dati, poiché riguarda, più in generale, questioni di diritto civile. Il Gruppo di lavoro richiama l'attenzione della Commissione sulle sfide sollevate in questo ambito.

Inoltre, il Gruppo di lavoro "Articolo 29" ritiene che gli interessi dei minori e di altri soggetti privi della capacità di agire sarebbero meglio tutelati se la direttiva contenesse ulteriori disposizioni, concernenti in particolare la raccolta e il trattamento supplementare dei dati che riguardano tali soggetti. Tali disposizioni potrebbero contemplare le circostanze in cui è richiesto il consenso del rappresentante, unitamente o in sostituzione del consenso del soggetto privo della capacità di agire, e potrebbero prevedere casi in cui non dovrebbe essere possibile utilizzare il consenso come fondamento per legittimare il trattamento dei dati personali. Dovrebbero inoltre formulare l'obbligo di utilizzare meccanismi on-line per la verifica dell'età. Esistono al riguardo meccanismi diversi e diverse soglie di età. Per esempio, la verifica dell'età, anziché essere soggetta a un'unica norma, potrebbe essere fondata su un approccio basato su una scala progressiva, per cui il meccanismo da utilizzare dipenderebbe dalle circostanze, per esempio il tipo di trattamento (le sue finalità), il suo grado di pericolosità, il tipo di dati raccolti, gli utilizzi fatti di questi dati (se i dati sono destinati a essere divulgati), ecc.

### **III.B. Direttiva 2002/58/CE**

La direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva 2002/58/CE)<sup>39</sup> è una *lex specialis* rispetto alla direttiva 95/46/CE, nel senso che stabilisce un regime giuridico per un settore specifico, vale a dire la vita privata e le comunicazioni elettroniche. La maggior parte delle sue disposizioni si applicano esclusivamente a fornitori di servizi di comunicazione elettronica accessibili al pubblico (per esempio, fornitori di servizi di telefonia, fornitori di servizi Internet, ecc.).

Alcune disposizioni della direttiva 2002/58/CE menzionano il consenso come fondamento giuridico su cui i fornitori di servizi di comunicazione elettronica accessibili al pubblico possono fare affidamento ai fini del trattamento dei dati<sup>40</sup>. » questo il caso, per esempio, dell'uso di dati relativi al traffico o all'ubicazione.

Il Gruppo di lavoro "Articolo 29" ritiene utile formulare osservazioni su taluni aspetti particolarmente interessanti correlati all'uso del consenso ai sensi della direttiva 2002/58/CE. In particolare, saranno considerati i seguenti cinque aspetti:

- a) il rapporto tra la definizione e il significato generale di consenso tra la direttiva 95/46/CE e la direttiva 2002/58/CE. Tale analisi è effettuata sulla base dell'articolo 2, paragrafo 2, lettera f), di quest'ultima direttiva.
- b) La questione se, per violare la segretezza delle comunicazioni (per esempio, al fine di controllare o intercettare una comunicazione telefonica), sia necessario ottenere il consenso di una o entrambe le parti che partecipano alla comunicazione. Tale situazione è disciplinata dall'articolo 6, paragrafo 3, e dall'articolo 5, paragrafo 1.
- c) La questione relativa al momento in cui deve essere ottenuto il consenso. Si tratta di un aspetto disciplinato da varie disposizioni della direttiva 2002/58/CE, tra cui in particolare l'articolo 5, paragrafo 3, e gli articoli 6 e 13.
- d) L'ambito di applicazione del diritto a opporsi al trattamento dei dati e la distinzione tra tale diritto e consenso. Tale distinzione può essere analizzata ai sensi dell'articolo 13 della direttiva 2002/58/CE.
- e) La possibilità di revocare il consenso esplicitamente prevista dall'articolo 6, paragrafo 3, e dall'articolo 9, paragrafi 3 e 4, della direttiva 2002/58/CE.

#### **III.B.1. Articolo 2, lettera f) - Definizione di consenso in relazione alla direttiva 95/46/CE "consenso dell'utente o dell'abbonato"**

L'articolo 2 della direttiva 2002/58/CE stabilisce esplicitamente che le definizioni della direttiva 95/46/CE si applicano anche alla presente direttiva. L'articolo 2, lettera f), così recita "consenso dell'utente dell'abbonato: corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE".

Ciò significa che, laddove si ha necessità di ottenere un consenso ai sensi della direttiva 2002/58/CE, i criteri per stabilire se il consenso è valido sono gli stessi previsti dalla direttiva 95/46/CE, ossia la definizione di cui all'articolo 2, lettera g), e gli aspetti specifici contemplati dall'articolo 7, lettera a). L'opinione che il consenso di cui trattasi nella direttiva 2002/58/CE sia da intendersi con riferimento all'articolo 2, lettera g), e all'articolo 7, lettera a), in combinato disposto, è confermata dal considerando 1741.

### **III.B.2. Articolo 5, paragrafo 1 - Sesià necessario ottenere il consenso di una o entrambe le parti "... consenso di questi ultimi ..."**

L'articolo 5, paragrafo 1, della direttiva 2002/58/CE tutela la riservatezza delle comunicazioni vietando ogni genere di intercettazione o di sorveglianza delle comunicazioni senza il consenso di tutti gli utenti interessati.

In tal caso, l'articolo 5, paragrafo 1, fa riferimento al consenso di tutti gli utenti interessati o, per dirla altrimenti, dei due interlocutori che prendono parte alla comunicazione. Il consenso di una sola parte non è sufficiente.

Durante l'elaborazione del suo parere 2/200642, il Gruppo di lavoro "Articolo 29" ha esaminato alcuni servizi che comportavano lo screening dei contenuti di messaggi di posta elettronica e, in alcuni casi, la verifica dell'eventuale apertura dei messaggi di posta elettronica. Il Gruppo di lavoro ha espresso timori in merito al fatto che, per l'erogazione di tali servizi, una delle due parti della comunicazione non veniva informata. Perché tali servizi siano conformi all'articolo 5, paragrafo 1, è necessario il consenso di entrambe le parti.

L'articolo 6, paragrafo 3, della direttiva 2002/58/CE contiene un riferimento esplicito alla necessità di ottenere il previo consenso dell'abbonato o dell'utente interessato, formulando l'obbligo di fornire informazioni e di ottenere il previo consenso prima di procedere al trattamento dei dati sul traffico al fine della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto. Per taluni tipi di servizi, il consenso può essere ottenuto dall'abbonato anche al momento della sottoscrizione al servizio. In altri casi, il consenso potrebbe essere ottenuto direttamente dall'utente. Un approccio di questo genere è contenuto all'articolo 9, che riguarda il trattamento di dati relativi all'ubicazione diversi dai dati relativi al traffico.

Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento. L'articolo 13 prevede l'obbligo di ottenere il consenso preliminare degli abbonati a utilizzare sistemi automatizzati di chiamata senza intervento di un operatore, del telefax o della posta elettronica a fini di commercializzazione diretta.

L'articolo 5, paragrafo 3, stabilisce una norma specifica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un utente, anche allo scopo di verificare le attività online dell'utente. Benché l'articolo 5, paragrafo 3, non usi il termine "preliminare", il riferimento a un momento precedente il trattamento è chiaramente e ovviamente deducibile dal testo della disposizione.

Ottenere il consenso prima dell'inizio del trattamento dei dati è una questione di buon senso. In caso contrario, il trattamento effettuato nel periodo di tempo che intercorre tra il momento in cui tale operazione ha avuto inizio e il momento in cui il consenso è stato ottenuto sarebbe illegale, perché privo di un fondamento giuridico. Tra l'altro, qualora in un caso del genere l'interessato decidesse di opporsi

al trattamento, ogni forma di trattamento dei dati già operata sarebbe illegale anche per questo motivo.

Dal che ne consegue che, se il consenso è obbligatorio, esso dev'essere richiesto prima dell'inizio del trattamento dei dati. La decisione di avviare il trattamento senza aver preliminarmente ottenuto il consenso è legittima soltanto laddove la direttiva in materia di protezione dei dati o la direttiva relativa alla vita privata e alle comunicazioni elettroniche, anziché prescrivere il consenso, offrono un motivo alternativo e fanno riferimento al diritto dell'interessato di opporsi o di rifiutare il trattamento. Questi meccanismi sono palesemente diversi dal consenso. In questi casi, infatti, il trattamento potrebbe essere già stato avviato e l'interessato avrebbe il diritto di opporvisi o di rifiutarlo.

Ne è un esempio l'articolo 5, paragrafo 3, della precedente direttiva sulla vita privata e le comunicazioni elettroniche, laddove esso recita (sottolineatura aggiunta): "l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito 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 e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del titolare del trattamento". Questo testo dovrebbe essere paragonato con il nuovo testo dell'articolo 5, paragrafo 3, della direttiva, modificata dalla direttiva 2009/136/CE<sup>43</sup>, in cui si legge 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 (...)". Le conseguenze di questa modifica nella formulazione dell'articolo 5, paragrafo 3, sono già state spiegate dal Gruppo di lavoro "Articolo 29" nel suo parere 2/2010 sulla pubblicità comportamentale online<sup>44</sup>. Nel prossimo capitolo si discuterà anche della differenza tra rifiuto e consenso.

In molti casi in cui la direttiva sulla vita privata e le comunicazioni elettroniche o la direttiva in materia di protezione dei dati prevede la possibilità di rifiutare il trattamento dei dati personali, ciò è possibile perché il fondamento giuridico del trattamento iniziale dei dati riguarda motivi di legittimità diversi dal consenso, tra cui per esempio l'esistenza di un contratto. Si avrà modo di discutere questo aspetto nella prossima sezione, che formula osservazioni in merito all'articolo 13 della direttiva 2002/58/CE.

#### **III.B.4. Articolo 13, paragrafi 2 e 3 – Diritto a opporsi e differenza rispetto al consenso "...ai clienti sia offerta in modo chiaro e distinto la possibilità di opporsi ..."**

L'articolo 13 della direttiva 2002/58/CE prevede il ricorso al consenso ai fini dell'invio di comunicazioni elettroniche a scopo legittimo di commercializzazione diretta, facendo affidamento su un principio standard e su una disposizione specifica.

In merito all'uso di dispositivi automatici di chiamata, telefax o posta elettronica, impone l'obbligo di ottenere preliminarmente il consenso dell'interessato.

Se il destinatario della comunicazione commerciale è un cliente già acquisito e la comunicazione si prefigge lo scopo di promuovere i prodotti o i servizi del fornitore o prodotti e servizi analoghi, non è necessario richiedere il consenso bensì fare in modo che agli interessati sia offerta "la possibilità di opporsi" ai sensi dell'articolo 13, paragrafo 2. Il considerando 41 spiega il motivo per cui il legislatore, in questo caso, non ha previsto il ricorso al consenso: "Nel contesto di una relazione di clientela già esistente è ragionevole consentire l'uso delle coordinate elettroniche per offrire prodotti o servizi analoghi". Pertanto, in linea di principio, la relazione contrattuale tra l'interessato e il fornitore di servizi

costituisce il motivo legittimante che permette il primo contatto mediante posta elettronica. Gli interessati, tuttavia, dovrebbero avere la possibilità di opporsi a ulteriori contatti. Come il Gruppo di lavoro ha già avuto modo di spiegare: "Tale opportunità dovrebbe continuare ad essere offerta gratuitamente per ogni successivo messaggio a scopi di commercializzazione diretta, ad eccezione degli eventuali costi relativi alla trasmissione del servizio".<sup>45</sup>

Si dovrebbe fare una distinzione tra l'obbligo a ottenere il consenso e il diritto a opporsi. Come si è detto nel capitolo III.A.2, il consenso fondato sulla mancata azione dell'interessato, per esempio mediante caselle preselezionate, non soddisfa i requisiti per il consenso valido ai sensi della direttiva 95/46/CE. La stessa conclusione si trae nei confronti di impostazioni del browser che per default permetterebbero la trasmissione all'utente (mediante l'uso di cookies). Sulla stessa linea è anche il nuovo testo dell'articolo 5, paragrafo 3, citato sopra al capitolo III.B.3. In questi due esempi non sono soddisfatti, in particolare, i requisiti per una manifestazione della volontà univoca dell'interessato. » fondamentale che all'interessato sia offerta l'opportunità di prendere una decisione e di manifestare la propria volontà, per esempio selezionando la casella di propria iniziativa, in vista delle finalità del trattamento dei dati.

Nel suo parere sulla pubblicità comportamentale il Gruppo di lavoro ha concluso che "è di estrema importanza che i browsers siano dotati di impostazioni di default a tutela della privacy o, in altre parole, che siano provvisti dell'impostazione di 'non accettazione e non trasmissione di cookie terzi'. A integrazione di ciò e ai fini di una maggiore efficacia, alla prima installazione o al momento dell'aggiornamento del browser, quest'ultimo dovrebbe richiedere all'utente di procedere attraverso una procedura guidata relativa alla privacy, offrendo così un modo semplice per esercitare la scelta durante l'uso"<sup>46</sup>.

### **III.B.5. Articolo 6, paragrafo 3, e articolo 9, paragrafi 3 e 4 – Possibilità di revocare il consenso "... possibilità di ritirare il loro consenso ... in qualsiasi momento..."**

La possibilità di revocare il consenso in qualsiasi momento, che è implicita nella direttiva 95/46/CE, è espressa in varie disposizioni della direttiva 2002/58/CE. Lo stesso concetto è stato esplicitamente formulato nel parere del Gruppo di lavoro sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto<sup>47</sup>:

"Ai sensi dell'articolo 9 della direttiva 2002/58/CE, coloro che hanno dato il proprio consenso al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico possono ritirare il loro consenso in qualsiasi momento e devono avere la possibilità di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati. Il gruppo di lavoro considera tali diritti – che possono essere considerati un'applicazione del diritto di opposizione al trattamento dei dati relativi all'ubicazione – come fondamentali, vista la natura delicata di tali dati. Il gruppo di lavoro ritiene che l'informazione delle persone – non solo quando si abbonano ad un servizio ma anche quando lo utilizzano – sia una condizione preliminare per l'esercizio di tali diritti. Nel caso in cui un servizio necessiti del trattamento continuativo dei dati relativi all'ubicazione, il gruppo di lavoro ritiene che il fornitore di servizi debba far presente periodicamente alla persona interessata che il suo terminale è stato, sarà o può essere localizzato. Ciò consentirà a tale persona di esercitare il diritto di revoca ai sensi dell'articolo 9 della direttiva 2002/58/CE, qualora essa lo desideri."

Come si è detto, ciò implica che il diritto di revoca è esercitato in riferimento al futuro, e non in relazione al trattamento di dati che già è avvenuto in passato, nel periodo in cui i dati sono stati raccolti in maniera legittima. Quindi, le decisioni prese o i processi avviati in precedenza in base a tali infor-

mazioni non possono essere semplicemente annullati. Tuttavia, qualora non sussistesse un altro fondamento giuridico per legittimare l'ulteriore archiviazione dei dati, questi dovrebbero essere cancellati dal titolare del trattamento.

#### **IV. Conclusioni**

Il presente parere esamina il quadro giuridico relativo all'uso del consenso ai sensi della direttiva 95/46/CE e della direttiva 2002/58/CE. L'obiettivo di tale documento è duplice: in primo luogo, esso mira a chiarire gli obblighi di legge esistenti e a illustrare in che modo essi si applicano nella pratica. In secondo luogo, così facendo offre una riflessione sull'adeguatezza del quadro esistente alla luce delle numerose nuove modalità di trattamento dei dati personali o sulla necessità di introdurre modifiche.

##### **IV.1. Chiarimento degli aspetti fondamentali del quadro attuale**

L'articolo 2, lettera h), della direttiva 95/46/CE definisce il consenso 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". L'articolo 7 della direttiva, che stabilisce il fondamento giuridico per il trattamento dei dati personali, individua tra i motivi di liceità il consenso manifestato in maniera inequivocabile. L'articolo 8 prescrive la necessità di ottenere un consenso esplicito per legittimare il trattamento dei dati sensibili. L'articolo 26, paragrafo 1, della direttiva 95/46/CE e svariate disposizioni della direttiva 2002/58/CE impongono l'obbligo di ottenere il consenso per poter intraprendere attività specifiche di trattamento dei dati che ricadono nell'ambito di applicazione delle direttive stesse. I punti sviluppati nel presente parere mirano a chiarire i vari elementi di tale quadro giuridico, allo scopo di facilitarne l'applicazione da parte delle parti interessate in generale.

##### **Elementi/osservazioni di natura generale**

Il consenso è uno dei sei criteri che legittimano il trattamento dei dati personali (uno dei cinque per quanto concerne il trattamento dei dati sensibili); esso è un elemento importante, poiché conferisce all'interessato una forma di controllo sul trattamento dei dati che lo riguardano. L'importanza del consenso a garanzia dell'autonomia dell'autodeterminazione dell'individuo è subordinata al fatto che esso sia utilizzato nel giusto contesto e con gli elementi necessari.

In generale, il quadro giuridico della direttiva 95/46/CE si applica ogniqualvolta viene richiesto il consenso all'interessato, sia nel mondo off-line sia in quello on-line. Si prenda l'esempio di un rivenditore di mattoni e malte che desidera chiedere alla sua clientela di aderire a un programma di fedeltà: le stesse regole si applicherebbero sia nel caso in cui questi ricorresse a un modulo carta-CEO, sia nell'eventualità in cui si avvallesse a tal fine del proprio sito Internet. Inoltre, la direttiva 2002/58/CE elenca alcune operazioni di trattamento dei dati che sono subordinate al rilascio del consenso: esse riguardano perlopiù il trattamento dei dati in relazione alla fornitura di servizi di comunicazione elettronica accessibili al pubblico. Gli obblighi previsti dalla direttiva 2002/58/CE affinché il consenso possa essere considerato valido sono gli stessi indicati nella direttiva 95/46/CE.

Le situazioni nelle quali il titolare del trattamento usa il consenso per legittimare il trattamento dei dati personali non andrebbero confuse con le situazioni in cui il titolare del trattamento invoca altri motivi per legittimare il trattamento che comportano il diritto dell'interessato a opporsi. » il caso, per esempio, di un'operazione di trattamento che poggia sull'"interesse legittimo" del titolare del trattamento ai sensi dell'articolo 7, lettera f), della direttiva 95/46/CE, nei confronti del quale l'interessato ha il diritto di opporsi a norma dell'articolo 14, lettera a), della direttiva 95/46/CE. Un altro esempio è quello di un titolare del trattamento che invia comunicazioni di posta elettronica ai suoi clienti per promuovere prodotti o servizi propri o simili: in tal caso gli interessati hanno diritto a opporsi al



trattamento ai sensi dell'articolo 13, paragrafo 2, della direttiva 2002/58/CE. In entrambi i casi l'interessato ha diritto a opporsi al trattamento e questa situazione non può essere equiparata al consenso.

Il fatto di ottenere il consenso al trattamento dei dati personali non solleva il titolare del trattamento dall'obbligo di rispettare le altre prescrizioni del quadro giuridico in materia di protezione dei dati, per esempio il principio di proporzionalità di cui all'articolo 6, paragrafo 1, lettera c), la sicurezza del trattamento a norma dell'articolo 17, ecc.

Un consenso valido presuppone la capacità di un individuo di manifestare il proprio consenso. Le norme che disciplinano la capacità di manifestare il consenso non sono armonizzate e, pertanto, possono variare da Stato membro a Stato membro.

Le persone che hanno manifestato il proprio consenso dovrebbero avere la possibilità di revocar-lo, al fine di impedire un trattamento supplementare dei dati che le riguardano. Tale principio è confermato anche dalla direttiva 2002/58/CE nel caso di operazioni specifiche di trattamento dei dati legittimate dal consenso, come il trattamento di dati relativi all'ubicazione diversi dai dati relativi al traffico.

Il consenso deve essere fornito prima che abbia inizio il trattamento dei dati personali, ma può anche essere obbligatoriamente ottenuto una seconda volta nel corso del trattamento, se la finalità dello stesso dovesse cambiare. Tale obbligo è sottolineato più volte dalla direttiva 2002/58/CE, sia mediante il ricorso al termine "preliminare" (per esempio, articolo 6, paragrafo) sia nella formulazione delle sue disposizioni (per esempio, articolo 5, paragrafo 3).

### **Elementi specifici del quadro giuridico relativo al consenso**

Perché il consenso sia valido, esso dev'essere una manifestazione di volontà libera. Ciò significa che non dev'esserci il rischio di raggiri, intimidazioni o conseguenze negative significative per l'interessato che decide di non dare il proprio consenso. Per alcune operazioni di trattamento dei dati in un contesto di lavoro in cui vi sia un elemento di subordinazione, nonché nel contesto di servizi governativi come il servizio sanitario, potrebbe essere necessario svolgere un'attenta analisi per stabilire se gli interessati siano realmente liberi di accettare il trattamento.

Il consenso deve essere specifico. Un consenso totale, senza che siano specificate le finalità esatte del trattamento, non soddisfa questo principio. Nel caso di un contratto, tale requisito obbliga il titolare del trattamento a introdurre specifiche clausole relative al consenso, chiaramente distinte dalle condizioni generali, evitando dunque di inserire le informazioni sul trattamento dei dati nelle condizioni generali.

Il consenso deve essere informato. Gli articoli 10 e 11 della direttiva elencano le tipologie di informazioni che devono necessariamente essere fornite agli interessati. In ogni caso, le informazioni fornite devono essere sufficienti per permettere agli interessati di adottare decisioni informate sul trattamento dei dati personali che li riguardano. La necessità che il consenso sia "informato" implica altri due requisiti aggiuntivi. In primo luogo, le modalità con cui sono fornite le informazioni devono garantire l'uso di un linguaggio adeguato, affinché gli interessati siano consapevoli delle attività che accettano e delle finalità da queste perseguite. Ciò dipende dal contesto. Il ricorso a un linguaggio giuridico o tecnico oltremodo astruso non sarebbe compatibile con tali requisiti di legge. In secondo luogo, le informazioni fornite agli utenti dovrebbero essere chiare e sufficientemente esaustive, in maniera tale che gli utenti non possano ignorarle. Le informazioni devono essere fornite direttamente agli interessati. Non è sufficiente che esse siano meramente disponibili in qualche luogo.

Quanto alle modalità con cui il consenso dev'essere manifestato, l'articolo 8, paragrafo 2, lettera a), prescrive l'obbligo di ottenere un consenso esplicito per poter procedere al trattamento di dati sensibili; ciò significa che l'interessato deve rispondere attivamente, verbalmente o per iscritto, per manifestare la sua volontà di accettare il trattamento dei dati che lo riguardano per determinate finalità. Ne consegue che non è possibile ottenere un consenso esplicito mediante il ricorso a una casella pre-selezionata. L'interessato deve compiere un'azione positiva per manifestare il proprio consenso e deve quindi essere libero di negarlo.

Per i dati diversi dai dati sensibili, l'articolo 7, lettera a), prevede che il consenso sia manifestato in maniera inequivocabile. Il termine "inequivocabile" impone il ricorso all'uso di meccanismi per l'ottenimento del consenso che non lasciano adito a dubbi quanto all'intenzione dell'interessato di accettare il trattamento. A livello pratico, tale obbligo permette ai responsabili del trattamento di utilizzare vari tipi di meccanismi per ottenere il consenso, dalle dichiarazioni di assenso (consenso esplicito) ai meccanismi che fanno affidamento su azioni finalizzate a esprimere un assenso.

L'inazione o il silenzio dell'interessato intesi come manifestazioni di consenso solitamente non-rappresentano un consenso valido, soprattutto in un contesto on-line. Il problema sorge, in particolare, in caso di utilizzo di impostazioni di default che l'interessato è tenuto a modificare per negare il trattamento. Ne è un esempio l'uso di caselle pre-selezionate o di impostazioni dei browser che sono predisposte per default alla raccolta di dati.

## **IV.2 Valutazione del quadro attuale e della possibile necessità di modifiche**

### **Valutazione generale**

Il Gruppo di lavoro ritiene che l'attuale quadro giuridico in materia di protezione dei dati contenga un insieme di norme ben concepite che stabiliscono le condizioni per considerare valido il consenso al fine delegittimare le operazioni di trattamento dei dati. Tali norme si applicano al mondo off-line così come a quello online. Più nello specifico: il quadro giuridico garantisce l'equilibrio rispetto a una serie di problematiche. Da un lato, assicura che soltanto un consenso reale e informato sia considerato tale. A tale proposito, l'articolo 2, lettera h), con cui esplicitamente si prevede che il consenso sia libero, specifico e informato, è rilevante e soddisfacente. Dall'altro lato, tale obbligo non rappresenta una camicia di forza, ma fornisce una flessibilità sufficiente, evitando norme specifiche sotto il profilo tecnico. Ne è un esempio lo stesso articolo 2, lettera h), laddove definisce il consenso una qualsiasi manifestazione della volontà dell'interessato. Ciò offre un sufficiente margine di manovra in termini di modalità per fornire tale manifestazione di volontà. Gli articoli 7 e 8, che prescrivono rispettivamente un consenso inequivocabile esplicito, rispecchiano perfettamente la necessità di garantire un equilibrio tra le due opposte questioni, quella cioè di offrire flessibilità ed evitare strutture oltremodo rigide e quella di garantire protezione.

Il risultato è un quadro normativo che, se adeguatamente applicato e attuato, è in grado di tenere il passo con l'ampia varietà di operazioni di trattamento dei dati che spesso sono rese possibili dagli sviluppi tecnologici.

Nella pratica, tuttavia, non è sempre facile stabilire quando è necessario ottenere il consenso dell'interessato e, più in particolare, individuare i requisiti che rendono valido il consenso, nonché le modalità permetterli concretamente in atto, e ciò a causa di una mancanza di uniformità tra Stati membri. A livello nazionale l'attuazione delle direttive è avvenuta sulla base di approcci diversi.

Gli elementi critici più specifici che sono emersi durante le discussioni condotte dal Gruppo di lavoro "Articolo 29", che hanno portato all'elaborazione del presente parere, sono descritti di seguito in maniera più dettagliata.

## **Possibili modifiche**

La nozione di consenso inequivocabile è utile per definire un sistema che non sia oltremodo rigido macché possa comunque fornire una robusta protezione. Tuttavia, se è vero che sussistono le potenzialità per sviluppare un sistema ragionevole, altrettanto certo è che, purtroppo, il suo significato viene spesso frainteso o semplicemente ignorato. Le indicazioni e gli esempi forniti nel presente parere dovrebbero contribuire a migliorare la certezza del diritto e la protezione dei diritti degli interessati nel caso in cui il consenso sia utilizzato come fondamento giuridico; al tempo stesso, il quadro tracciato sembra necessitare di alcune modifiche.

Più in particolare, il Gruppo di lavoro "Articolo 29" ritiene che la formulazione stessa ("in maniera inequivocabile") potrebbe beneficiare di ulteriori chiarimenti nell'ambito di una revisione del quadro normativo generale in materia di protezione dei dati. I chiarimenti introdotti dovrebbero avere lo scopo di spiegare che il consenso manifestato in maniera inequivocabile prevede l'uso di meccanismi che non lascino dubbi circa l'intenzione dell'interessato di manifestare il proprio assenso. Al tempo stesso occorrerebbe precisare che l'uso di soluzioni di default che l'interessato dovrebbe modificare per poter negare il trattamento (consenso fondato sul silenzio) di per sé non costituisce un consenso inequivocabile. Ciò vale in particolare per l'ambiente on-line.

Oltre al chiarimento di cui sopra, il Gruppo di lavoro 29 suggerisce quanto segue:

**i.** In primo luogo, includere nella definizione di consenso di cui all'articolo 2, lettera h), il termine "inequivocabile" (o un termine equivalente) allo scopo di rafforzare il concetto che soltanto un consenso fondato su dichiarazioni o azioni intese a esprimere accettazione costituisce un valido consenso. Oltre ad aggiungere chiarezza, ciò permetterebbe di allineare la nozione di consenso di cui all'articolo 2, lettera h), con le prescrizioni riguardanti il consenso valido di cui all'articolo 7. Inoltre, il significato del termine "inequivocabile" potrebbe essere ulteriormente precisato in un considerando del futuro quadro giuridico.

**ii.** In secondo luogo, nell'ambito di un obbligo generale di rendiconto, i responsabili del trattamento dovrebbero essere nella condizione di dimostrare che il consenso è stato ottenuto. Infatti, se l'onere della prova sarà rafforzato in modo da imporre ai responsabili del trattamento l'obbligo di dimostrare di aver effettivamente ottenuto il consenso dell'interessato, questi saranno tenuti ammettere in atto pratiche e meccanismi standard volti a ricercare e dimostrare un consenso inequivocabile. Il tipo di meccanismo dipenderà dal contesto e dovrebbero tener conto dei fatti e delle circostanze del trattamento, più in particolare dei suoi rischi.

Il Gruppo di lavoro "Articolo 29" non è convinto della necessità di introdurre nel quadro il concetto di "consenso esplicito" come regola generale per tutte le operazioni di trattamento, comprese quelle attualmente contemplate dall'articolo 7 della direttiva. Esso è del parere, infatti, che il consenso inequivocabile, che comprende il consenso esplicito ma anche il consenso derivante da azioni inequivocabili, dovrebbe rimanere la norma. Tale scelta offre maggiore flessibilità ai responsabili dei dati nella raccolta del consenso e la procedura generale potrebbe essere più rapida e di più agevole applicazione.

Vari aspetti del quadro giuridico che si applicano al consenso possono essere dedotti dal tenore degli atti in questione o dalla sua storia legislativa, oppure sono scaturiti dalla giurisprudenza e dai pareri del Gruppo di lavoro "Articolo 29". Se tali aspetti fossero espressamente integrati nel nuovo quadro legislativo in materia di protezione dei dati, si avrebbe una maggiore certezza del diritto. Potrebbero essere presi in considerazione i seguenti elementi:

**i.** l'inclusione di una clausola esplicita che istituisca il diritto degli interessati a revocare il consenso.

**ii.** Il rafforzamento della nozione che il consenso dev'essere manifestato prima dell'inizio del trattamento, o prima di qualsiasi eventuale ulteriore utilizzo dei dati per finalità diverse rispetto a quelle per le quali era stato ottenuto il consenso iniziale, nell'eventualità in cui non vi siano altri fondamenti giuridici che legittimano il trattamento.

**iii.** L'inclusione di obblighi espliciti in materia di qualità (obbligo a fornire informazioni sul trattamento dei dati in modo che siano facilmente comprensibili, in un linguaggio chiaro e semplice) e di accessibilità delle informazioni (obbligo di fornire informazioni esaustive, rilevanti e direttamente accessibili). Ciò è fondamentale per consentire agli interessati di adottare decisioni informate.

Infine, per quanto riguarda le persone prive della capacità di agire, si potrebbero prevedere disposizioni che garantiscono una maggiore protezione, tra cui:

**i.** chiarimenti in merito alle circostanze in cui è richiesto il consenso dei genitori o rappresentanti di un soggetto privo della capacità di agire, compresa la soglia di età al di sotto della quale tale consenso sarebbe obbligatorio.

**ii.** Definizione dell'obbligo di utilizzare meccanismi di verifica dell'età, che potrebbero cambiare a seconda delle circostanze come l'età di minori, il tipo di trattamento, il grado di rischio implicato, la destinazione finale delle informazioni (se cioè saranno custodite dal titolare del trattamento messe a disposizione di terzi).

**iii.** L'obbligo di adattare le informazioni ai minori, se ciò fosse utile per consentire a tali soggetti di comprendere le implicazioni della raccolta di informazioni che li riguardano, e quindi della manifestazione del consenso.

**iv.** Specifiche salvaguardie che identifichino le attività di trattamento dei dati, come la pubblicità comportamentale, nell'ambito delle quali il consenso non dovrebbe essere un fondamento possibile per legittimare il trattamento dei dati personali.

Il Gruppo di lavoro "Articolo 29" riesaminerà la questione del consenso. Più in particolare, le autorità nazionali per la protezione dei dati, oltre che il Gruppo di lavoro, potrebbero decidere in un secondo tempo di redigere linee guida per approfondire il presente parere, fornendo nuovi esempi pratici connessi all'uso del consenso.

Fatto a Bruxelles, 13 luglio 2011  
Per il Gruppo di lavoro,  
Il Presidente Jacob KOHNSTAMM

## **NOTE**

**1** COM (2010) 609 definitivo del 4.11.2010.

**2** La prima relazione della Commissione sull'applicazione della direttiva sulla tutela dei dati(95/46/CE) (COM (2003) 265 definitivo), già menzionata a pag. 17: "Soprattutto la nozione di 'consenso in maniera inequivocabile' (articolo 7, lettera a)), se paragonata alla nozione di 'consenso esplicito di cui all'articolo 8, richiede un ulteriore chiarimento e un'interpretazione più uniforme. » necessario che gli operatori sappiano che cosa si debba intendere per valido consenso, in particolare nelle situazioni in linea."

**3** Tra questi il parere 8/2010 sul diritto applicabile, adottato il 16.12.2010 (GL 179), e il parere 1/2010 sulle nozioni di "titolare del trattamento" e "incaricato del trattamento", adottato il 16.2.2010 (GL 169).

**4** Cfr., per esempio, l'articolo 31 della Legge n. 78-17 del 6 gennaio 1978 "relative à l'informatique, aux fichiers et aux libertés".

**5** La Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (denominata "Convenzione n. 108") è entrata in vigore l'1 ottobre 1985.

**6** La Convenzione n.108 ha introdotto le nozioni di "trattamento legittimo" e di "fine legittima"(articolo 5), ma a differenza della direttiva 95/46/CE non contiene un elenco di criteri da soddisfare per illegittimo trattamento dei dati. Il consenso dell'interessato gioca un ruolo specifico soltanto nell'ambito dell'assistenza reciproca (articolo 15). Tuttavia, il requisito del "consenso" è stato menzionato successivamente in più occasioni in varie raccomandazioni del Comitato dei ministri.

**7** Proposta di direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali, COM (90), 314 definitivo, SYN 287 e 288, Bruxelles, 13 settembre 1990.

**8** Proposta modificata di direttiva del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, COM(92) 422 DEF- SYN 287, Bruxelles, 15 ottobre 1992.

**9** Cfr. la pag. 11 della proposta modificata di direttiva del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, COM (92) 422 DEF-SYN 287, Bruxelles, 15 ottobre 1992.

**10** Posizione comune del Consiglio concernente la proposta di direttiva del Parlamento e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, (00/287) COD, adottata il 15 marzo 1995.

**11** Cfr. la pagina 4 della posizione comune.

**12** Sentenza della Corte (grande sezione) del 5 ottobre 2004, Pfeiffer, Roith, S,fl, Winter, Nestvogel, Zeller, D'bele, nelle cause riunite da C-397/01 a C-403/01.

**13** A titolo di esempio, la versione tedesca della direttiva (così come la legge federale tedesca in materia di protezione dei dati) ricorre alla nozione di "Einwilligung". Nel codice civile tedesco il termine è definito come "previa autorizzazione".

**14** WP 114 – Documento di lavoro del Gruppo di lavoro articolo 29 su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995.

**15** Parere del Garante europeo della protezione dei dati del 14 gennaio 2011 sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – "Un approccio globale alla protezione dei dati personali nell'Unione europea".

**16** Parere n. 168 del Gruppo di lavoro articolo 29 sul futuro della vita privata, contributo congiunto alla consultazione della Commissione europea sul quadro legale per il diritto fondamentale alla protezione dei dati personali, adottato il 1 dicembre 2009.

**17** Parere del Garante europeo della protezione dei dati del 14 gennaio 2011, op. cit.

**18** Il WP 162 sull'Agenda Mondiale Antidoping perviene alla medesima conclusione: "Tenuto conto delle sanzioni e delle conseguenze previste nell'eventualità che i partecipanti si sottraggano agli obblighi imposti dal codice (ad esempio fornire le informazioni sul luogo di permanenza), il Gruppo di lavoro non può in nessun caso considerare libero il consenso dato".

**19** WP 48 sul trattamento dei dati personali nel contesto dell'occupazione. A tale riguardo è pertinente anche il WP 114 – Documento di lavoro del Gruppo di lavoro articolo 29 su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995.

**20** Cfr. la lettera dell'11 febbraio 2009 inviata dal presidente del Gruppo di lavoro articolo 29 al sig. Daniel CAL-LEJA CRESPO, direttore della DG TREN, sulla questione dei body scanner, in risposta alla consultazione della Commissione sul tema "l'impatto dell'uso dei body scanner nel campo della sicurezza aerea sui diritti dell'uomo, sulla vita privata, sulla dignità personale, sulla salute e sulla protezione dei dati". Disponibile all'indirizzo-[http://ec.europa.eu/justice/policies/privacy/working-group/wpdocs/2009-others\\_en.htm](http://ec.europa.eu/justice/policies/privacy/working-group/wpdocs/2009-others_en.htm).

**21** Cfr. il parere 6/2002 del Gruppo di lavoro articolo 29 relativo alla trasmissione da parte delle compagnie aeree d'informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti.

**22** Sentenza della Corte 5 maggio 2011, Deutsche Telekom AG (causa C-543/09). La causa è iniziata con il rinvio operato dal tribunale amministrativo federale tedesco in merito agli elenchi telefonici e, in particolare, all'interpretazione dell'articolo 25, paragrafo 2, della direttiva relativa al servizio universale (2002/22/CE) e dell'articolo 12, paragrafo 2, della direttiva relativa alla vita privata e alle comunicazioni elettroniche (2002/58/CE). Essa è chiaramente collegata al ruolo specifico degli elenchi di cui trattasi nella direttiva relativa al servizio universale.

**23** WP 131 – Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche.

**24** WP 12 – Documento di lavoro. Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati. Cfr. anche il WP 114 – Documento di lavoro del Gruppo di lavoro articolo 29 concernente un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995.

**25** Cfr. la nota 12 (capitolo II.2)

**26** Documento di lavoro 1/2008 sulla protezione dei dati personali dei minori, WP 147, 18 febbraio 2008.

**27** Il Gruppo di lavoro articolo 29 ha formulato una raccomandazione simile nel suo parere 2/2010 sulla pubblicità comportamentale online, adottato il 22 giugno 2010 (WP171).

**28** Il Fondo europeo agricolo di garanzia (FEAGA) e il Fondo europeo agricolo per lo sviluppo rurale (FEASR).

**29** Conclusioni dell'avvocato generale Sharpston del 17 giugno 2010, Volker und Markus SchickeGmbH, nelle cause riunite C-92/09 e C-93/09. Si deve osservare che, nella sentenza del 9 novembre

2010, la Corte ha stabilito che il trattamento dei dati non era fondato sul consenso: "63. La normativa dell'Unione in questione, che si limita a disporre che i beneficiari di aiuti saranno preventivamente informati della pubblicazione dei dati che li riguardano, non mira dunque a fondare il trattamento dei dati personali da essa previsto sul consenso dei beneficiari interessati."

**30** Parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell'articolo 13 della direttiva 2002/58/CE, adottato il 27 febbraio 2004 (WP 90).

**31** WP 131 – Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE).

**32** Tale interpretazione è in linea con la legislazione dell'UE, prevalentemente sul commercio elettronico e sul più ampio uso delle firme digitali, che ha costretto gli Stati membri a modificare la propria legislazione contenente obblighi formali sulla necessità che i documenti siano "in forma scritta" e "scritti a mano" per rendere accettabili anche i documenti elettronici, a condizione che siano soddisfatte determinate condizioni.

**33** A tale proposito, cfr. per esempio la legislazione greca e tedesca sui requisiti previsti per la trasmissione del consenso con mezzi elettronici, che impone l'obbligo di registrare il consenso in maniera sicura, che prevede la possibilità di essere contattati dall'utente o dall'abbonato in qualsiasi momento e secondo cui il consenso può essere revocato in qualsiasi momento (articolo 5, paragrafo 3, della legge greca 3471/2006 sulla protezione dei dati personali nel settore delle comunicazioni elettroniche; articolo 13, paragrafo 2, della legge tedesca sui servizi telematici, articolo 94 della legge tedesca sulle telecomunicazioni articolo 28, paragrafo 3 bis della legge federale tedesca in materia di protezione dei dati).

**34** L'analisi delle condizioni tecniche che devono essere soddisfatte affinché documenti elettronici e firme digitali abbiano analogo valore probatorio degli equivalenti manoscritti esula dall'ambito di applicazione del presente parere. Si tratta di una questione che trascende la legislazione in materia di protezione dei dati e che è già stata disciplinata a livello di UE.

**35** Questo perché si presume automaticamente che l'uso di alcuni tipi di firma digitale (firme elettroniche avanzate basate su un certificato qualificato e che sono prodotte da un dispositivo per la creazione di una firma sicura) abbia il medesimo valore legale come prova degli equivalenti scritti.

**36** WP 12 – Documento di lavoro. Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati, adottato il 24 luglio 1998.

**37** Documento di lavoro concernente un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995, adottato il 25 novembre 2005.

**38** WP 147 – Documento di lavoro 1/2008 sulla protezione dei dati a carattere personale dei minori (Principi generali e caso specifico delle scuole); WP 160 – Parere 2/2009 sulla protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole).

**39** Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei

dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, 18.12.2009.

**40** L'espressione "dati sul traffico" si riferisce al trattamento dei dati al fine di trasmettere una comunicazione su una rete di comunicazioni elettroniche o per la fatturazione di tale comunicazione, tra cui i dati riguardanti l'instradamento del traffico, la durata o l'ora di una comunicazione.

**41** Nel quale si legge: "Ai fini della presente direttiva il consenso (..) dovrebbe avere lo stesso significato del con-senso della persona interessata come definito ed ulteriormente determinato nella direttiva 95/46/CE".

**42** Parere 2/2006 sugli aspetti di tutela della vita privata inerenti ai servizi di screening dei messaggi di posta elettronica, adottato il 21 febbraio 2006 (WP 118).

**43** Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (Testo rilevante ai fini del SEE), GU L 337 del 18.12.2009, pag. 11

**44** Parere del 22 giugno 2010, WP 171: la questione se il consenso possa essere manifestato mediante "l'uso delle opportune impostazioni di un motore di ricerca o di un'altra applicazione" [considerando 66 della direttiva 2009/136/CE] è esplicitamente esaminata al punto 4.1.1 del WP 171.

**45** Parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell'articolo 13 della direttiva 2002/58/CE, adottato il 27 febbraio 2004.

**46** Parere del 22 giugno 2010, WP 171, op. cit.

**47** Parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto, adottato il 25 novembre 2005 (WP 115).