



844/14/IT  
WP 217

**Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE**

**adottato il 9 aprile 2014**

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È 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 MO-59 02/13.

Sito Internet: [http://ec.europa.eu/justice/data-protection/index\\_it.htm](http://ec.europa.eu/justice/data-protection/index_it.htm)

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

## Indice

<b>Sintesi</b> .....	3
I. <b>Introduzione</b> .....	5
II. <b>Osservazioni generali e questioni di natura politica</b> .....	7
II.1. Breve excursus .....	7
II.2. Ruolo dell'articolo 7, lettera f).....	11
II.3. Nozioni correlate .....	12
II.4. Contesto e conseguenze strategiche .....	14
III. <b>Analisi delle disposizioni</b> .....	16
III.1. Panoramica dell'articolo 7 .....	16
III.1.1. Consenso o "necessario per..." .....	16
III.1.2. Relazione con l'articolo 8 .....	17
III.2. Articolo 7, lettere da a) a e).....	19
III.2.1. Consenso .....	19
III.2.2. Contratto.....	20
III.2.3. Obbligo legale .....	22
III.2.4. Interesse vitale.....	24
III.2.5. Compito di interesse pubblico.....	25
III.3. Articolo 7, lettera f): interesse legittimo .....	27
III.3.1. Interesse legittimo del responsabile del trattamento (oppure del o dei terzi cui vengono comunicati i dati).....	28
III.3.2. Interesse o diritti dell'interessato .....	34
III.3.3. Introduzione all'applicazione del test comparativo .....	36
III.3.4. Fattori chiave da considerare nell'applicazione del test comparativo.....	39
III.3.5. Responsabilità e trasparenza .....	51
III.3.6. Il diritto di opposizione e oltre .....	52
IV. <b>Osservazioni finali</b> .....	57
IV.1. Conclusioni.....	57
IV. 2. Raccomandazioni .....	60
<b>Allegato 1. Guida rapida allo svolgimento del test comparativo di cui all'articolo 7, lettera f)</b>	
65	
<b>Allegato 2. Esempi pratici volti a illustrare l'applicazione del test comparativo di cui all'articolo 7, lettera f)</b> .....	68

## Sintesi

Il presente parere analizza i principi relativi alla legittimazione del trattamento dei dati di cui all'articolo 7 della direttiva 95/46/CE. Concentrandosi sull'interesse legittimo del responsabile del trattamento, fornisce indicazioni sulle modalità di applicazione dell'articolo 7, lettera f), nell'ambito dell'attuale quadro giuridico e formula raccomandazioni per futuri miglioramenti.

L'articolo 7, lettera f), è l'ultimo dei sei criteri che legittimano il trattamento dei dati personali. Di fatto, prevede che l'interesse legittimo del responsabile del trattamento, oppure dei terzi cui vengono comunicati i dati, sia valutato rispetto agli interessi o ai diritti fondamentali dell'interessato. L'esito di questo test comparativo permetterà di stabilire se l'articolo 7, lettera f), può essere invocato come fondamento giuridico per il trattamento.

Il Gruppo di lavoro "articolo 29" riconosce l'importanza e l'utilità del criterio di cui all'articolo 7, lettera f), che nelle giuste circostanze e in presenza di adeguate garanzie potrebbe contribuire a evitare che si faccia eccessivamente affidamento ad altre basi giuridiche. L'articolo 7, lettera f), non deve essere trattato come "estremo rimedio" per situazioni rare o imprevedute in cui non si ritengono applicabili altri fondamenti giuridici per il trattamento legittimo dei dati. Tuttavia, non si deve decidere automaticamente di avvalersi di tale articolo né se ne deve ampliare indebitamente l'utilizzo in base alla percezione che sia meno vincolante rispetto agli altri criteri.

Una corretta valutazione dell'articolo 7, lettera f), non è un semplice test comparativo consistente soltanto nel confrontare tra loro due "pesi" facilmente quantificabili e comparabili. Per eseguire il test occorre invece valutare appieno una serie di fattori affinché sia possibile garantire che gli interessi e i diritti fondamentali degli interessati siano tenuti nella debita considerazione. Al tempo stesso, il test comparativo è adattabile, può variare da semplice a complesso e non deve risultare indebitamente gravoso. Tra i fattori di cui tenere conto nell'esecuzione del test comparativo figurano:

- la natura e l'origine dell'interesse legittimo nonché l'eventualità che il trattamento dei dati sia necessario per l'esercizio di un diritto fondamentale o altrimenti per l'esecuzione di un compito di interesse pubblico o sia riconosciuto dalla comunità interessata;

- l'impatto sugli interessati e le loro ragionevoli aspettative su ciò che accadrà ai loro dati, nonché la natura dei dati e le modalità di trattamento;

- garanzie supplementari che potrebbero limitare l'indebito impatto sull'interessato, quali la minimizzazione dei dati, le tecnologie di rafforzamento della tutela della vita privata, una maggiore trasparenza, il diritto generale e incondizionato di revoca ("opt-out") e la portabilità dei dati.

Per il futuro, il Gruppo di lavoro "articolo 29" raccomanda di inserire nella proposta di regolamento un considerando sui fattori chiave di cui tenere conto nell'applicazione del test comparativo. Il Gruppo di lavoro "articolo 29" raccomanda altresì di aggiungere un considerando che imponga al responsabile del trattamento, ove opportuno, di documentare la sua valutazione nell'interesse di una maggiore responsabilità. Infine, il Gruppo di lavoro "articolo 29" sarebbe inoltre favorevole all'introduzione di una disposizione sostanziale che imponga ai responsabili del trattamento di spiegare agli interessati perché ritengono che gli

interessi e i diritti e le libertà fondamentali degli interessati non prevalgano sui loro interessi.

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

istituito dalla 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 PRESENTE PARERE:**

### **I. Introduzione**

Il presente parere analizza i principi relativi alla legittimazione del trattamento dei dati di cui all'articolo 7 della direttiva 95/46/CE<sup>1</sup> (la "direttiva") concentrandosi, in particolare, sull'interesse legittimo del responsabile del trattamento di cui all'articolo 7, lettera f).

I criteri elencati all'articolo 7 si riferiscono al concetto più generale di "liceità" enunciato all'articolo 6, paragrafo 1, lettera a), secondo cui i dati personali devono essere trattati "lealmente e lecitamente".

Ai sensi dell'articolo 7, il trattamento di dati personali può essere effettuato soltanto quando è legittimato da almeno uno dei sei fondamenti giuridici elencati in tale articolo. In particolare, i dati personali possono essere trattati esclusivamente (a) sulla base del consenso inequivocabile dell'interessato<sup>2</sup> o, in sintesi<sup>3</sup>, qualora il trattamento sia necessario:

- (b) all'esecuzione del contratto concluso con la persona interessata;
- (c) per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento;
- (d) per la salvaguardia dell'interesse vitale della persona interessata;
- (e) per l'esecuzione di un compito di interesse pubblico; o
- (f) per il perseguimento dell'interesse legittimo del responsabile del trattamento, subordinatamente a un test comparativo supplementare tra tale interesse e i diritti e l'interesse della persona interessata.

L'ultimo criterio ammette il trattamento "necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o<sup>4</sup> i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1". In altre parole, l'articolo 7, lettera f), ammette il trattamento subordinatamente a un test comparativo, che

---

<sup>1</sup> Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

<sup>2</sup> Cfr. il parere 15/2011 del Gruppo di lavoro "articolo 29" sulla definizione di consenso, adottato il 13 luglio 2011 (WP 187).

<sup>3</sup> Queste disposizioni sono discusse più approfonditamente più avanti.

<sup>4</sup> Come spiegato nella sezione III.3.2, la versione inglese della direttiva sembra contenere un refuso: nel testo dovrebbe figurare l'espressione "interests or fundamental rights" (l'interesse o i diritti [e le libertà] fondamentali) anziché "interests for fundamental rights" (l'interesse per i diritti e [le libertà] fondamentali).

valuti l'interesse legittimo del responsabile del trattamento (oppure del o dei terzi cui vengono comunicati i dati) rispetto agli interessi o ai diritti fondamentali degli interessati<sup>5</sup>.

### *Necessità di un approccio più coerente e armonizzato in Europa*

Sia gli studi condotti dalla Commissione nel quadro della revisione della direttiva<sup>6</sup> che la cooperazione e lo scambio di pareri tra le autorità nazionali di protezione dei dati hanno evidenziato che non esiste un'interpretazione armonizzata dell'articolo 7, lettera f), della direttiva; tale carenza ha dato luogo a divergenze di applicazione negli Stati membri. In particolare, benché in alcuni Stati membri sia necessario effettuare un vero e proprio test comparativo, l'articolo 7, lettera f), è talvolta erroneamente considerato come una "porta aperta" per legittimare tutti i trattamenti di dati che non rientrano in uno degli altri fondamenti giuridici.

L'assenza di un approccio coerente può determinare una mancanza di certezza del diritto e prevedibilità, può indebolire la posizione degli interessati e può inoltre imporre inutili oneri normativi alle imprese e ad altre organizzazioni operanti a livello transfrontaliero. Tali incongruenze hanno già dato luogo a controversie dinanzi alla Corte di giustizia dell'Unione europea ("CGUE")<sup>7</sup>.

Mentre prosegue il lavoro verso un nuovo regolamento generale sulla protezione dei dati, è pertanto particolarmente opportuno comprendere meglio il sesto fondamento che legittima il trattamento dei dati personali (riguardante "l'interesse legittimo") nonché la sua relazione con gli altri criteri di liceità del trattamento. Nello specifico, il fatto che siano in gioco i diritti fondamentali degli interessati comporta la necessità che l'applicazione di tutti e sei i criteri tenga conto, in debita e uguale misura, del rispetto di tali diritti. L'articolo 7, lettera f), non deve diventare una scappatoia per eludere il rispetto della normativa in materia di protezione dei dati.

Per questi motivi, nell'ambito del suo programma di lavoro 2012-2013, il Gruppo di lavoro "articolo 29" per la protezione dei dati (il "Gruppo di lavoro") ha deciso di esaminare attentamente la questione e, per dare attuazione a tale programma di lavoro<sup>8</sup>, si è impegnato a redigere il presente parere.

---

<sup>5</sup> Il riferimento all'articolo 1, paragrafo 1, non deve essere interpretato come inteso a limitare la portata degli interessi e dei diritti e delle libertà fondamentali dell'interessato. Questo riferimento ha invece il ruolo di evidenziare l'obiettivo generale sia delle norme in materia di protezione dei dati che della direttiva stessa. In realtà, l'articolo 1, paragrafo 1, non si riferisce esclusivamente alla tutela della vita privata, ma anche alla protezione di tutti gli altri "diritti e libertà fondamentali delle persone fisiche", di cui la vita privata è solo uno degli aspetti.

<sup>6</sup> Il 25 gennaio 2012 la Commissione europea ha adottato un pacchetto per riformare il quadro europeo della protezione dei dati. Il pacchetto è costituito da (i) una "comunicazione" (COM(2012)9 definitivo), (ii) una proposta di "regolamento generale sulla protezione dei dati" (la "proposta di regolamento") (COM(2012)11 definitivo) e (iii) una proposta di "direttiva" sulla protezione dei dati nell'ambito dell'applicazione del diritto penale (COM(2012)10 definitivo). La "valutazione d'impatto", contenente 10 allegati, è illustrata in un documento di lavoro della Commissione (SEC(2012)72 definitivo). Cfr., in particolare, lo studio intitolato "Evaluation of the implementation of the Data Protection Directive" (Valutazione dell'attuazione della direttiva sulla protezione dei dati), che costituisce l'allegato 2 alla valutazione d'impatto che accompagna il pacchetto di riforma della protezione dei dati della Commissione europea.

<sup>7</sup> Cfr. pagina 9, alla sezione "II.1 Breve excursus", "Attuazione della direttiva; la sentenza ASNEF e FECEMD".

<sup>8</sup> Cfr. il programma di lavoro 2012-2013 del Gruppo di lavoro "articolo 29" per la protezione dei dati, adottato il 1° febbraio 2012 (WP 190).

## *Applicare il quadro giuridico vigente e preparare il quadro futuro*

Il programma di lavoro stesso ha dichiarato chiaramente due obiettivi: “assicurare la corretta applicazione del quadro giuridico vigente” e “preparare il quadro futuro”.

Di conseguenza, il primo obiettivo del presente parere è assicurare una comprensione comune del quadro giuridico attuale. Tale obiettivo segue la logica di precedenti pareri vertenti su altre disposizioni fondamentali della direttiva<sup>9</sup>. In secondo luogo, sulla base dell’analisi effettuata, il parere formulerà inoltre raccomandazioni politiche di cui tenere conto durante la revisione del quadro giuridico sulla protezione dei dati.

### *Struttura del parere*

Dopo aver fornito un breve excursus della storia e del ruolo del legittimo interesse e di altri criteri di liceità del trattamento nel capitolo II, il capitolo III esaminerà e interpreterà le pertinenti disposizioni della direttiva, tenendo conto della base comune nella loro attuazione a livello nazionale. L’analisi, illustrata con esempi pratici tratti dalle esperienze nazionali, suffraga le raccomandazioni fornite nel capitolo IV sia sull’applicazione del quadro giuridico vigente che nel contesto della revisione della direttiva.

## **II. Osservazioni generali e questioni di natura politica**

### **II.1. Breve excursus**

Il presente excursus si concentra sul modo in cui sono stati sviluppati il concetto di liceità e i fondamenti giuridici che legittimano il trattamento. Spiega in particolare come la necessità di una base giuridica sia stata inizialmente utilizzata come obbligo nell’ambito delle deroghe ai diritti alla tutela della vita privata e successivamente sia diventata una prescrizione a se stante nell’ambito della protezione dei dati.

#### *Convenzione europea dei diritti dell’uomo (“CEDU”)*

L’articolo 8 della Convenzione europea dei diritti dell’uomo, adottata nel 1950, incorpora il diritto alla tutela della vita privata, ossia il diritto di ogni persona al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Vieta qualsiasi ingerenza nell’esercizio di tale diritto a meno che sia “prevista dalla legge” e costituisca una misura che, “in una società democratica, è necessaria” a soddisfare talune esigenze imperative, espressamente elencate, che perseguono un obiettivo di interesse generale.

L’articolo 8 della CEDU si concentra sulla tutela della vita privata e stabilisce che qualsiasi ingerenza nell’esercizio di tale diritto deve essere giustificata. Tale approccio si basa su un divieto generale di ingerenza nel diritto alla tutela della vita privata e prevede deroghe solo a

---

<sup>9</sup> Tra questi figurano il parere 3/2013 sul principio di limitazione delle finalità, adottato il 3 aprile 2013 (WP 203), il parere 15/2011 sulla definizione di consenso, adottato il 13 luglio 2011 (WP 187), citato alla nota a piè di pagina 2, il parere 8/2010 sul diritto applicabile, adottato il 16 dicembre 2010 (WP 179) e il parere 1/2010 sui concetti di “responsabile del trattamento” e “incaricato del trattamento”, adottato il 16 febbraio 2010 (WP 169).

condizioni rigorosamente definite. Nei casi di “ingerenza nella vita privata” occorre indicare una base giuridica nonché precisare un fine legittimo quale requisito per valutare la necessità dell’ingerenza. Da questo approccio si evince che la CEDU non fornisce un elenco dei possibili criteri di liceità, ma si concentra sulla necessità di una base giuridica e sulle condizioni che tale base giuridica deve soddisfare.

#### *Convenzione n. 108*

La Convenzione n. 108 del Consiglio d’Europa<sup>10</sup>, aperta alla firma nel 1981, introduce la protezione dei dati personali come concetto separato. L’idea sottesa all’epoca non era che il trattamento dei dati personali dovesse essere sempre considerato come una “ingerenza nella vita privata”, bensì che per *proteggere* i diritti e le libertà fondamentali di ogni persona, e in particolare il diritto di ognuno alla tutela della vita privata, il trattamento dei dati personali dovesse sempre soddisfare determinate condizioni. L’articolo 5 stabilisce pertanto i principi fondamentali della normativa in materia di protezione dei dati, compreso il requisito secondo cui “i dati a carattere personale oggetto di elaborazione automatica devono essere: (a) ottenuti ed elaborati lealmente e legalmente”. Tuttavia, la Convenzione non stabilisce criteri di liceità del trattamento dettagliati<sup>11</sup>.

#### *Linee guida dell’OCSE<sup>12</sup>*

Le linee guida dell’OCSE, elaborate contestualmente alla Convenzione n. 108 e adottate nel 1980, condividono analoghe idee di “liceità”, anche se il concetto è espresso in maniera differente. Le linee guida sono state aggiornate nel 2013, senza apportare modifiche sostanziali al principio di liceità. L’articolo 7 delle linee guida dell’OCSE stabilisce in particolare che “devono esistere limiti alla raccolta di dati personali e che tali dati devono essere ottenuti lealmente e lecitamente e, ove opportuno, con la conoscenza o il consenso dell’interessato”. In questo caso il fondamento giuridico del consenso è espressamente indicato come un’opzione, da utilizzare “ove opportuno”. A tal fine sarà necessario esaminare gli interessi e i diritti in gioco nonché valutare il livello di invasività del trattamento. In questo senso l’approccio dell’OCSE mostra alcune analogie con i criteri, molto più elaborati, definiti nella direttiva 95/46/CE.

#### *Direttiva 95/46/CE*

Quando è stata adottata nel 1995, la direttiva si basava su precedenti strumenti di protezione dei dati, compresa la Convenzione n. 108 e le linee guida dell’OCSE. Si era tenuto conto anche della precedente esperienza in materia di protezione dei dati in alcuni Stati membri.

Oltre al più ampio requisito enunciato all’articolo 6, paragrafo 1, lettera a), secondo cui i dati personali devono essere tratti “lealmente e lecitamente”, la direttiva ha aggiunto un insieme

---

<sup>10</sup> Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

<sup>11</sup> Il progetto di testo della Convenzione modernizzata adottato dalla riunione plenaria del comitato consultivo T-PD del novembre 2012 afferma che i dati a carattere personale possono essere trattati in base al consenso della persona interessata o a “un altro fondamento legittimo previsto dalla legge”, analogamente a quanto prescritto dalla Carta dei diritti fondamentali dell’Unione europea citata di seguito a pagina 9.

<sup>12</sup> Linee guida dell’OCSE sulla protezione della vita privata e dei flussi transfrontalieri di dati personali, 11 luglio 2013.

specifico di requisiti aggiuntivi, non ancora presenti in quanto tali né nella Convenzione n. 108 né nelle linee guida dell'OCSE: il trattamento dei dati personali deve basarsi su uno dei sei fondamenti giuridici indicati all'articolo 7.

### *Attuazione della direttiva; la sentenza ASNEF e FECEMD<sup>13</sup>*

La relazione della Commissione intitolata “*Evaluation of the implementation of the Data Protection Directive*” (Valutazione dell’attuazione della direttiva sulla protezione dei dati)<sup>14</sup> sottolinea che il recepimento delle disposizioni della direttiva negli ordinamenti nazionali è stato talvolta insoddisfacente. Nell’analisi tecnica della trasposizione della direttiva negli Stati membri<sup>15</sup>, la Commissione fornisce ulteriori dettagli sull’attuazione dell’articolo 7. L’analisi spiega che, benché nella maggior parte degli Stati membri le disposizioni nazionali enuncino i sei fondamenti giuridici in termini relativamente simili a quelli utilizzati nella direttiva, di fatto la flessibilità di tali principi ha dato luogo a divergenze di applicazione.

In tale contesto, riveste particolare importanza il fatto che, nella sentenza *ASNEF e FECEMD* del 24 novembre 2011, la CGUE abbia stabilito che la Spagna non aveva recepito correttamente l’articolo 7, lettera f), della direttiva, richiedendo che, in assenza del consenso della persona interessata, tutti i dati pertinenti utilizzati figurino in fonti accessibili al pubblico. La sentenza ha inoltre stabilito che l’articolo 7, lettera f), ha effetto diretto. La sentenza limita il margine discrezionale di cui dispongono gli Stati membri nell’applicazione dell’articolo 7, lettera f). In particolare, gli Stati membri non devono oltrepassare la sottile linea di confine tra la precisazione, da un lato, e l’imposizione di requisiti supplementari, che modificherebbero la portata dell’articolo 7, lettera f), dall’altro.

Chiarendo che nei loro ordinamenti nazionali gli Stati membri non possono prevedere restrizioni e requisiti supplementari unilaterali riguardo ai fondamenti giuridici per il trattamento legittimo dei dati, la sentenza ha conseguenze considerevoli. I tribunali nazionali e gli altri organismi competenti devono interpretare le disposizioni nazionali alla luce di questa sentenza disapplicando, se necessario, tutte le norme e le pratiche nazionali contrastanti.

Alla luce della sentenza, è ancora più importante che le autorità nazionali di protezione dei dati e/o i legislatori europei giungano a un’interpretazione chiara e comune sull’applicabilità dell’articolo 7, lettera f). Tale obiettivo deve essere raggiunto in maniera equilibrata, senza limitare o ampliare indebitamente il campo di applicazione di questa disposizione.

### *La Carta dei diritti fondamentali*

Da quando il trattato di Lisbona è entrato in vigore il 1° dicembre 2009, la Carta dei diritti fondamentali dell’Unione europea (la “Carta”) ha “lo stesso valore giuridico dei trattati”<sup>16</sup>. La

---

<sup>13</sup> Corte di giustizia dell’Unione europea, sentenza 24 novembre 2011, cause riunite C-468/10 e C-469/10 (*ASNEF e FECEMD*).

<sup>14</sup> Cfr. l’allegato 2 alla valutazione d’impatto che accompagna il pacchetto di riforma della protezione dei dati della Commissione europea, citato nella precedente nota a piè di pagina 6.

<sup>15</sup> “*Analysis and impact study on the implementation of Directive EC 95/46 in Member States*” (Analisi e studio d’impatto sull’attuazione della direttiva 95/46/CE negli Stati membri). Cfr. [http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf).

<sup>16</sup> Cfr. l’articolo 6, paragrafo 1, del TUE.

Carta sancisce la protezione dei dati personali all'articolo 8 quale diritto fondamentale distinto dal rispetto della vita privata e della vita familiare di cui all'articolo 7. L'articolo 8 fissa l'obbligo di trattare i dati personali sulla base di un fondamento legittimo. In particolare, stabilisce che i dati personali devono essere trattati "in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge"<sup>17</sup>. Queste disposizioni rafforzano sia l'importanza del principio della liceità che la necessità di una base giuridica adeguata per il trattamento dei dati personali.

#### *La proposta di regolamento sulla protezione dei dati*

Nell'ambito del processo di revisione del quadro giuridico dell'UE sulla protezione dei dati, il campo di applicazione dei criteri di liceità del trattamento di cui all'articolo 7 e, in particolare, la portata dell'articolo 7, lettera f), sono attualmente oggetto di discussione.

L'articolo 6 della proposta di regolamento elenca i fondamenti che legittimano il trattamento dei dati personali. Con alcune eccezioni (come sarà illustrato più avanti), i sei fondamenti disponibili rimangono sostanzialmente invariati rispetto a quelli attualmente enunciati all'articolo 7 della direttiva. La Commissione ha tuttavia proposto di fornire ulteriori indicazioni sotto forma di atti delegati.

È interessante osservare che, nell'ambito del lavoro svolto in seno alla competente commissione del Parlamento europeo<sup>18</sup>, sono stati compiuti tentativi per chiarire il concetto di interesse legittimo nella proposta di regolamento stessa. Sono stati redatti un elenco di casi in cui l'interesse legittimo del responsabile del trattamento prevarrebbe, di regola, sugli interessi legittimi e sui diritti e sulle libertà fondamentali dell'interessato e un secondo elenco di casi in cui gli interessi legittimi e i diritti e le libertà fondamentali dell'interessato prevarrebbero, di norma, sull'interesse legittimo del responsabile del trattamento. Tali elenchi, redatti nelle disposizioni o nei considerando, forniscono un importante contributo alla valutazione dell'equilibrio tra i diritti e gli interessi del responsabile del trattamento e dell'interessato e sono presi in considerazione nel presente parere<sup>19</sup>.

---

<sup>17</sup> Cfr. l'articolo 8, paragrafo 2, della Carta.

<sup>18</sup> Progetto di relazione della commissione per le libertà civili, la giustizia e gli affari interni (LIBE) sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), datato 16 gennaio 2013 ("progetto di relazione della commissione LIBE"). Cfr., in particolare, gli emendamenti 101 e 102 nonché gli emendamenti adottati dalla commissione il 21 ottobre 2013 nella sua relazione finale ("relazione finale della commissione LIBE").

<sup>19</sup> Cfr. la sezione III.3.1, in particolare i punti a pag. 29, contenenti un elenco non esaustivo di alcuni degli ambiti più comuni in cui può porsi la questione dell'interesse legittimo ai sensi dell'articolo 7, lettera f).

## II.2. Ruolo dell'articolo 7, lettera f)

*Interesse legittimo del responsabile del trattamento: test comparativo come ultima opzione?*

L'articolo 7, lettera f), è elencato come ultima opzione tra i sei criteri che legittimano il trattamento dei dati personali. Prevede l'esecuzione di un test comparativo: ciò che è necessario per l'interesse legittimo del responsabile del trattamento (oppure del o dei terzi cui vengono comunicati i dati) deve essere valutato rispetto agli interessi o ai diritti e alle libertà fondamentali dell'interessato. L'esito del test comparativo permette di stabilire se l'articolo 7, lettera f), può essere invocato come fondamento giuridico per il trattamento.

Il carattere indeterminato di questa disposizione solleva molte questioni importanti riguardo alla sua esatta portata e applicazione, che saranno a loro volta analizzate nel presente parere. Tuttavia, come sarà illustrato di seguito, ciò non significa necessariamente che si debba ricorrere solo moderatamente a questa opzione come "estremo rimedio" al fine di colmare lacune nel caso di situazioni rare e impreviste o come ultima possibilità qualora non sia possibile applicare alcun altro criterio. Analogamente, questa opzione non deve essere privilegiata rispetto alle altre né se ne deve ampliare indebitamente l'utilizzo in base alla percezione che sia meno vincolante rispetto agli altri criteri.

È invece molto probabile che l'articolo 7, lettera f), abbia il suo naturale campo di pertinenza e che possa svolgere un ruolo molto utile come criterio di liceità del trattamento, purché sia soddisfatta una serie di condizioni fondamentali.

Nelle giuste circostanze e in presenza di adeguate garanzie, il corretto utilizzo dell'articolo 7, lettera f), potrebbe inoltre contribuire a evitare che gli altri fondamenti giuridici siano utilizzati in maniera impropria o che si faccia eccessivamente affidamento ad essi.

I primi cinque criteri elencati all'articolo 7 considerano motivi di liceità il consenso dell'interessato, l'accordo contrattuale, un obbligo legale o altri fondamenti espressamente indicati. Quando si basa su uno di questi cinque fondamenti, il trattamento è considerato legittimo a priori e pertanto è subordinato solo all'osservanza delle altre disposizioni normative applicabili. In altre parole, si presume che esista un equilibrio tra i differenti diritti e interessi in gioco, compresi quelli sia del responsabile del trattamento che dell'interessato, sempreché, ovviamente, siano rispettate tutte le altre disposizioni in materia di protezione dei dati. D'altro canto, l'articolo 7, lettera f), prevede l'esecuzione di un test *specifico* per i casi che non rientrano negli scenari predefiniti di cui ai criteri elencati alle lettere da a) a e). Garantisce che, al di fuori di tali scenari, tutti i trattamenti di dati soddisfino il requisito di un test comparativo, tenendo nella debita considerazione gli interessi e i diritti fondamentali dell'interessato.

In seguito a questo test si può giungere alla conclusione che in determinati casi il bilanciamento penda a favore degli interessi e dei diritti fondamentali degli interessati e che, di conseguenza, non sia possibile effettuare l'attività di trattamento. D'altro canto, una valutazione adeguata del bilanciamento degli interessi ai sensi dell'articolo 7, lettera f), spesso accompagnata dalla possibilità di revocare il consenso al trattamento, potrebbe in altri casi rappresentare una valida alternativa all'uso improprio, per esempio, del fondamento del "consenso" o del criterio della "necessità ai fini dell'esecuzione del contratto". Considerato in questo modo, l'articolo 7, lettera f), presenta garanzie complementari, che richiedono misure adeguate, rispetto agli altri criteri di liceità prestabiliti. Non deve quindi essere ritenuto

“l’anello più debole” o una “porta aperta” per legittimare tutte le attività di trattamento dei dati che non rientrano in uno degli altri fondamenti giuridici.

Il Gruppo di lavoro ribadisce che, nell’interpretare il campo di applicazione dell’articolo 7, lettera f), intende conseguire un approccio equilibrato, che garantisca la necessaria flessibilità ai responsabili del trattamento in situazioni in cui non sussiste un indebito impatto sugli interessati, fornendo contemporaneamente loro una certezza del diritto e garanzie sufficienti che questa disposizione indeterminata non sarà utilizzata in maniera impropria.

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

#### *Relazione tra l’articolo 7, lettera f), e altri criteri di liceità del trattamento*

L’articolo 7 inizia elencando il consenso e prosegue citando gli altri criteri di liceità del trattamento, tra cui i contratti e gli obblighi legali, fino ad arrivare gradualmente al test comparativo dell’interesse legittimo, che è l’ultimo dei sei fondamenti disponibili. L’ordine in cui sono elencati i fondamenti giuridici all’articolo 7 è stato talvolta interpretato come un’indicazione della rispettiva importanza dei differenti criteri di liceità. Tuttavia, come è già stato evidenziato nel parere del Gruppo di lavoro sulla nozione di consenso<sup>20</sup>, il testo della direttiva non opera una distinzione giuridica tra i sei criteri di liceità del trattamento né suggerisce l’esistenza di una gerarchia fra loro. Non esistono indicazioni secondo cui l’articolo 7, lettera f), deve essere applicato solo in casi eccezionali né dal testo si evince altrimenti che l’ordine specifico dei sei fondamenti giuridici avrà effetti giuridicamente vincolanti. Al contempo, il significato preciso dell’articolo 7, lettera f), e la sua relazione con altri criteri di liceità del trattamento sono da tempo poco chiari.

Alla luce delle precedenti osservazioni e considerando le diversità storiche e culturali nonché il linguaggio indeterminato della direttiva, sono stati sviluppati approcci differenti: alcuni Stati membri hanno la tendenza a considerare l’articolo 7, lettera f), come il fondamento giuridico meno preferito, volto a colmare le lacune solo in alcuni casi eccezionali quando nessuno degli altri cinque criteri di liceità troverebbe o potrebbe trovare applicazione<sup>21</sup>. Altri Stati membri, invece, la ritengono solo una delle sei opzioni, né più né meno importante rispetto alle altre, e che potrebbe trovare applicazione in un’ampia serie e in una grande varietà di situazioni, purché siano soddisfatte le condizioni necessarie.

Considerando queste diversità, e anche alla luce della sentenza *ASNEF e FECEMD*, è importante chiarire la relazione del criterio dell’“interesse legittimo” sia con gli altri criteri di liceità (ovvero la sua relazione sia con il consenso, i contratti, i compiti di interesse pubblico) che con il diritto di opposizione dell’interessato. Tale precisazione potrebbe permettere di definire meglio il ruolo e la funzione del criterio dell’interesse legittimo e contribuire pertanto alla certezza del diritto.

È inoltre opportuno osservare che il criterio dell’interesse legittimo, insieme agli altri fondamenti giuridici ad esclusione del consenso, prevede l’esecuzione di un test di

---

<sup>20</sup> Cfr. la precedente nota a piè di pagina 2.

<sup>21</sup> È inoltre opportuno osservare che, al suo emendamento 100, il progetto di relazione della commissione LIBE aveva proposto di separare l’articolo 7, lettera f), dal resto dei fondamenti giuridici, suggerendo altresì obblighi aggiuntivi laddove si ricorra a questa base giuridica, tra cui una trasparenza e una responsabilità maggiori, come sarà illustrato più avanti.

“necessità” che limita rigorosamente il contesto in cui ciascuno di essi può essere applicato. La Corte di giustizia ha ritenuto che la “necessità” sia una nozione autonoma del diritto comunitario<sup>22</sup>. Anche la Corte europea dei diritti dell’uomo ha fornito orientamenti utili<sup>23</sup>.

Inoltre, disporre di un fondamento giuridico appropriato non esonera il responsabile del trattamento dagli obblighi di cui all’articolo 6 con riferimento ai principi di lealtà, liceità, necessità e proporzionalità, oltre che di qualità dei dati. Per esempio, anche qualora il trattamento dei dati personali poggi sul criterio dell’interesse legittimo, o sull’esecuzione di un contratto, ciò di per sé non legittimerebbe una raccolta dei dati eccedente rispetto alla finalità perseguita.

L’interesse legittimo e gli altri criteri di liceità del trattamento di cui all’articolo 7 sono fondamenti giuridici alternativi e, di conseguenza, è sufficiente che trovi applicazione uno solo di essi. Tuttavia, sono cumulabili non solo con gli obblighi di cui all’articolo 6, ma anche con tutti gli altri principi e requisiti in materia di protezione dei dati che potrebbero essere applicabili.

#### *Altri test comparativi*

L’articolo 7, lettera f), non è l’unico test comparativo previsto nella direttiva. Ai sensi dell’articolo 9, per esempio, occorre trovare un equilibrio tra il diritto alla protezione dei dati personali e la libertà d’espressione. Questo articolo consente agli Stati membri di prevedere le esenzioni e le deroghe necessarie per il trattamento di dati personali “effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria [...] qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d’espressione”.

Inoltre, molte altre disposizioni della direttiva prevedono a loro volta un’analisi caso per caso, il bilanciamento degli interessi e dei diritti in gioco nonché una valutazione multifattoriale flessibile. Tra queste, per citare solo qualche esempio, figurano le disposizioni in materia di necessità, proporzionalità e limitazione delle finalità, le deroghe di cui all’articolo 13 e la ricerca scientifica.

Di fatto, sembra che la direttiva sia stata concepita per lasciare un margine all’interpretazione e al bilanciamento degli interessi. Tale formulazione, ovviamente, aveva almeno in parte l’obiettivo di lasciare agli Stati membri un ulteriore margine per recepire la direttiva negli ordinamenti nazionali. Oltre a ciò, tuttavia, la necessità di una certa flessibilità deriva anche dalla natura stessa del diritto alla protezione dei dati personali e del diritto alla tutela della vita privata. Di fatto, questi due diritti, insieme alla maggior parte degli altri (ma non tutti) diritti

---

<sup>22</sup> Corte di giustizia, sentenza 16 dicembre 2008, causa C-524/06, *Heinz Huber c. Bundesrepublik Deutschland*, punto 52: “Pertanto, considerato l’obiettivo di garantire un livello di tutela equivalente in tutti gli Stati membri, la nozione di necessità come risultante dall’articolo 7, lettera e), della direttiva 95/46, che mira a delimitare con precisione una delle ipotesi in cui il trattamento di dati personali è lecito, non può avere un contenuto variabile in funzione degli Stati membri. Si tratta quindi di una nozione autonoma del diritto comunitario che deve essere interpretata in maniera tale da rispondere pienamente alla finalità di tale direttiva come definita dal suo articolo 1, paragrafo 1.”

<sup>23</sup> Corte europea dei diritti dell’uomo, sentenza 25 marzo 1983, *Silver e altri c. Regno Unito*, punto 97, che discute l’espressione “necessaria in una società democratica”: “l’aggettivo ‘necessaria’ non è sinonimo di ‘indispensabile’ né ha la flessibilità di termini quali ‘ammissibile’, ‘ordinaria’, ‘utile’, ‘ragionevole’ o ‘auspicabile’ [...]”.

fondamentali, sono considerati diritti umani relativi o qualificati<sup>24</sup>. Questi tipi di diritti devono essere sempre interpretati nel contesto. Fatte salve garanzie adeguate, possono essere bilanciati con i diritti altrui. In alcune situazioni, e sempre fatte salve garanzie adeguate, possono inoltre essere limitati per motivi di interesse generale.

#### **II.4. Contesto e conseguenze strategiche**

*Garantire la legittimità ma anche la flessibilità: mezzi per precisare il campo di applicazione dell'articolo 7, lettera f)*

Il testo attuale dell'articolo 7, lettera f), della direttiva è indeterminato. Questo significa che può essere invocato in un'ampia serie di situazioni, nella misura in cui siano soddisfatti gli obblighi da esso previsti, compreso il test comparativo. Tale flessibilità, tuttavia, potrebbe anche avere implicazioni negative. Per evitare che comporti un'applicazione incoerente a livello nazionale o una mancanza di certezza del diritto, sarebbe importante fornire ulteriori orientamenti.

La Commissione prevede di fornire tali orientamenti nella proposta di regolamento sotto forma di atti delegati. Fra le altre opzioni figura la possibilità di fornire chiarimenti e disposizioni dettagliate nel testo della proposta di regolamento stessa<sup>25</sup> e/o di affidare al comitato europeo per la protezione dei dati il compito di fornire ulteriori orientamenti in quest'ambito.

A sua volta, ognuna di queste opzioni presenta vantaggi e svantaggi. Se la valutazione dovesse essere effettuata caso per caso senza ulteriori orientamenti, si rischierebbe di incorrere in un'applicazione incoerente e in una mancanza di prevedibilità, come è avvenuto in passato.

D'altro canto, se si fornissero elenchi dettagliati ed esaurienti delle situazioni in cui gli interessi legittimi del responsabile del trattamento prevalgono, di norma, sui diritti fondamentali dell'interessato o viceversa nel testo della proposta di regolamento stessa, quest'ultima potrebbe risultare fuorviante, inutilmente prescrittiva o presentare entrambe le caratteristiche.

Tali approcci potrebbero nondimeno ispirare una soluzione equilibrata, rendendo più dettagliata la proposta di regolamento stessa e fornendo ulteriori indicazioni negli atti delegati o negli orientamenti del comitato europeo per la protezione dei dati<sup>26</sup>.

---

<sup>24</sup> Esistono solo alcuni diritti umani che non possono essere bilanciati con i diritti altrui o con gli interessi della comunità in generale. Si tratta dei diritti assoluti. Tali diritti non possono essere mai limitati, indipendentemente dalle circostanze, nemmeno in situazioni di guerra o di emergenza. Un esempio è il diritto a non essere sottoposti a tortura o a trattamenti inumani o degradanti. Non è mai ammissibile torturare o trattare qualcuno in maniera inumana o degradante, indipendentemente dalle circostanze. Tra gli esempi di diritti umani non assoluti figurano il diritto al rispetto della vita privata e della vita familiare, il diritto alla libertà d'espressione e il diritto alla libertà di pensiero, coscienza e religione.

<sup>25</sup> Cfr. la sezione II.1 Breve excursus, al paragrafo "*La proposta di regolamento sulla protezione dei dati*", a pagina 10.

<sup>26</sup> Per quanto riguarda gli atti delegati e gli orientamenti del comitato europeo per la protezione dei dati, il parere 8/2012 del Gruppo di lavoro che fornisce un ulteriore contributo alle discussioni sulla riforma in materia di protezione dei dati, adottato il 5 ottobre 2012 (WP 199), si è espresso nettamente a favore della possibilità che a occuparsi della questione sia il Comitato europeo per la protezione dei dati (cfr. pagg. 13-14).

Obiettivo dell'analisi presentata al capitolo III è gettare le basi per individuare tale approccio affinché non sia troppo generale da rivelarsi inutile né troppo specifico da risultare eccessivamente rigido.

### **III. Analisi delle disposizioni**

#### **III.1. Panoramica dell'articolo 7**

Ai sensi dell'articolo 7, il trattamento di dati personali può essere effettuato soltanto se si applica almeno uno dei sei fondamenti giuridici elencati in tale articolo. Prima di analizzare ognuno di tali fondamenti, la presente sezione III.1 fornisce una panoramica dell'articolo 7 e della sua relazione con l'articolo 8 sulle categorie particolari di dati.

##### **III.1.1. Consenso o “necessario per...”**

È possibile distinguere tra il caso in cui i dati personali sono trattati sulla base del consenso inequivocabile manifestato dalla persona interessata (articolo 7, lettera a)) e i cinque casi rimanenti (articolo 7, lettere da b) a f)). Questi cinque casi, in sintesi, descrivono scenari in cui il trattamento potrebbe essere necessario in un contesto specifico, quali l'esecuzione del contratto concluso con la persona interessata, l'adempimento di un obbligo legale al quale è soggetto il responsabile del trattamento, ecc.

Nel primo caso, ai sensi dell'articolo 7, lettera a), sono gli interessati stessi ad autorizzare il trattamento dei loro dati personali. Spetta a loro decidere se acconsentire o meno al trattamento dei dati personali che li riguardano. Al tempo stesso, il consenso non elimina la necessità di rispettare i principi di cui all'articolo 6<sup>27</sup>. Inoltre, per essere legittimo, il consenso deve comunque soddisfare talune condizioni essenziali, come illustrato nel parere 15/2011 del Gruppo di lavoro<sup>28</sup>. Poiché il trattamento dei dati dell'utente avviene, in ultima analisi, a sua discrezione, l'accento è posto sulla validità e sulla portata del consenso dell'interessato.

In altre parole, il primo fondamento giuridico, l'articolo 7, lettera a), si concentra sull'autodeterminazione dell'interessato quale motivo di liceità. Tutti gli altri criteri, invece, ammettono il trattamento, subordinatamente a garanzie e misure adeguate, in situazioni in cui, a prescindere dal consenso, è opportuno e necessario trattare i dati in un determinato contesto al fine di perseguire un interesse legittimo specifico.

Le lettere b), c), d) ed e) precisano ognuna un criterio che legittima il trattamento:

- (b) l'esecuzione del contratto concluso con la persona interessata;
- (c) l'adempimento di un obbligo legale al quale è soggetto il responsabile del trattamento;
- (d) la salvaguardia dell'interesse vitale della persona interessata;
- (e) l'esecuzione di un compito di interesse pubblico.

La lettera f) è meno specifica e si riferisce, più in generale, all'interesse legittimo (di qualsiasi tipo) perseguito dal responsabile del trattamento (in qualsiasi contesto). Questa disposizione

---

<sup>27</sup> Corte suprema dei Paesi Bassi, sentenza 9 settembre 2011, causa ECLI:NL:HR:2011:BQ8097, §3.3(e) in riferimento al principio di proporzionalità. Cfr. anche pagina 8 del parere 15/2011 del Gruppo di lavoro “articolo 29” citato alla precedente nota a piè di pagina 2: “... l'ottenimento del consenso non esonera il responsabile 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.”

<sup>28</sup> Cfr. pagg. 12-29 del parere 15/2011 citato alla precedente nota a piè di pagina 2.

generale è tuttavia espressamente subordinata a un test comparativo supplementare, finalizzato a tutelare gli interessi e i diritti degli interessati, come sarà illustrato di seguito nella sezione III.2.

La valutazione del rispetto dei criteri enunciati all'articolo 7, lettere da a) a f), è inizialmente effettuata, in tutti i casi, dal responsabile del trattamento dei dati, subordinatamente alla legislazione applicabile e agli orientamenti sulle modalità di applicazione della normativa. In secondo luogo, la legittimità del trattamento può essere soggetta a un'ulteriore valutazione ed eventualmente contestata dagli interessati, da altri attori, dalle autorità di protezione dei dati e, alla fine, giudicata dai tribunali.

Per completare questa breve panoramica, è opportuno ricordare che, come illustrerà la sezione III.3.6, l'interessato può esercitare il diritto di opposizione previsto dall'articolo 14<sup>29</sup> almeno nei casi indicati alle lettere e) e f). Ne scaturirà una nuova valutazione degli interessi in gioco o, nel caso di trattamento dei dati personali a fini di invio di materiale pubblicitario (articolo 14, lettera b)), il responsabile del trattamento sarà tenuto a interrompere il trattamento dei dati personali senza effettuare ulteriori valutazioni.

### **III.1.2. Relazione con l'articolo 8**

L'articolo 8 della direttiva disciplina ulteriormente i trattamenti riguardanti talune categorie particolari di dati personali. Nello specifico, si applica ai dati "che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale" (articolo 8, paragrafo 1)), e ai dati "relativi alle infrazioni o alle condanne penali" (articolo 8, paragrafo 5)).

In linea di principio, il trattamento di tali dati è vietato, fatte salve alcune eccezioni. L'articolo 8, paragrafo 2, prevede una serie di casi in cui non si applica tale divieto, alle lettere da a) a e). L'articolo 8, paragrafi 3 e 4, prevede ulteriori eccezioni. Alcune di queste disposizioni sono simili, ma non identiche, a quelle enunciate all'articolo 7, lettere da a) a f).

Le specifiche condizioni fissate dall'articolo 8, oltre al fatto che alcuni dei criteri elencati all'articolo 7 sono simili alle condizioni enunciate all'articolo 8, sollevano la questione della relazione esistente tra le due disposizioni.

Se è concepito come *lex specialis*, occorre valutare se l'articolo 8 escluda completamente l'applicabilità dell'articolo 7. In tal caso significherebbe che si possono trattare categorie particolari di dati senza rispettare l'articolo 7, purché si applichi una delle eccezioni di cui all'articolo 8. Tuttavia, è anche possibile che la relazione sia più complessa e che gli articoli 7 e 8 debbano essere applicati cumulativamente<sup>30</sup>.

---

<sup>29</sup> A norma dell'articolo 14, lettera a), questo diritto si applica "salvo disposizione contraria prevista dalla normativa nazionale". In Svezia, per esempio, l'ordinamento nazionale non prevede la possibilità di opporsi a un trattamento basato sull'articolo 7, lettera e).

<sup>30</sup> Poiché l'articolo 8 è istituito come un *divieto con deroghe*, tali deroghe possono essere considerate come obblighi che limitano soltanto il campo di applicazione del divieto senza però fornire, in sé e per sé, una base giuridica sufficiente per il trattamento. Secondo questa interpretazione, l'applicabilità delle deroghe di cui all'articolo 8 non esclude l'applicabilità degli obblighi previsti dall'articolo 7 e, se del caso, i due articoli devono essere applicati cumulativamente.

In ogni caso, è evidente che l'obiettivo politico è prevedere una protezione aggiuntiva per categorie particolari di dati. Di conseguenza, l'esito finale dell'analisi deve essere altrettanto chiaro: l'applicazione dell'articolo 8, di per sé o in maniera cumulativa con l'articolo 7, è volta a fornire un livello di protezione maggiore per categorie particolari di dati.

In pratica, benché in alcuni casi l'articolo 8 preveda obblighi più rigorosi (quali il consenso "esplicito" di cui all'articolo 8, paragrafo 2, lettera a), anziché il "consenso inequivocabile" di cui all'articolo 7), questa affermazione non è valida per tutte le disposizioni. Alcune deroghe previste dall'articolo 8 non sembrano equivalenti o più rigorose rispetto ai criteri elencati all'articolo 7. Sarebbe inappropriato concludere per esempio che il fatto che qualcuno abbia reso alcune categorie particolari di dati manifestamente pubbliche ai sensi dell'articolo 8, paragrafo 2, lettera e), sia (sempre in sé e per sé) una condizione sufficiente a consentire qualunque tipo di trattamento dei dati, senza effettuare un test comparativo degli interessi e dei diritti in gioco in conformità dell'articolo 7, lettera f)<sup>31</sup>.

In alcune situazioni, il fatto che il responsabile del trattamento dei dati sia un partito politico revocherebbe inoltre il divieto di trattare categorie particolari di dati ai sensi dell'articolo 8, paragrafo 2, lettera d). Tuttavia, ciò non significa che qualsiasi trattamento effettuato nel campo di applicazione di tale disposizione sia necessariamente legittimo. Occorre valutare separatamente questa disposizione e il responsabile del trattamento potrebbe dover dimostrare, per esempio, che il trattamento dei dati è necessario all'esecuzione di un contratto (articolo 7, lettera b)) o che prevale il suo interesse legittimo ai sensi dell'articolo 7, lettera f). In quest'ultimo caso è necessario effettuare il test comparativo di cui all'articolo 7, lettera f), dopo aver valutato che il responsabile del trattamento dei dati rispetta gli obblighi sanciti dall'articolo 8.

Analogamente, il semplice fatto che il "trattamento dei dati è necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura" e che tali dati sono trattati nel rispetto dell'obbligo del segreto (requisiti citati tutti all'articolo 8, paragrafo 3) implica che tale trattamento di dati sensibili è *esentato dal divieto* di cui all'articolo 8, paragrafo 1. Tuttavia, ciò non è necessariamente sufficiente a garantire anche la legittimità ai sensi dell'articolo 7 e richiederà un criterio di liceità quale l'esecuzione di un contratto con il paziente ai sensi dell'articolo 7, lettera b), l'adempimento di un obbligo legale ai sensi dell'articolo 7, lettera c), l'esecuzione di un compito di interesse pubblico ai sensi dell'articolo 7, lettera e), o un test comparativo ai sensi dell'articolo 7, lettera f).

In conclusione, il Gruppo di lavoro ritiene che debba essere effettuata un'analisi caso per caso valutando se l'articolo 8 preveda di per sé condizioni più rigorose e sufficienti<sup>32</sup> o se sia necessaria un'applicazione cumulativa degli articoli 8 e 7 al fine di garantire la piena

---

<sup>31</sup> Inoltre, l'articolo 8, paragrafo 2, lettera e), non deve essere interpretato *a contrario* nel senso che, quando i dati resi pubblici dall'interessato non sono sensibili, possono essere trattati senza alcuna condizione aggiuntiva. I dati disponibili al pubblico sono comunque dati personali soggetti ai requisiti di tutela dei dati, compreso il rispetto dell'articolo 7, indipendentemente dal fatto che siano o meno dati sensibili.

<sup>32</sup> Cfr. l'analisi effettuata al punto 3.3 del parere del Gruppo di lavoro concernente lo standard internazionale dell'Agenzia Mondiale Antidoping (WADA), che prende in considerazione sia l'articolo 7 che l'articolo 8 della direttiva: "Secondo parere 4/2009 concernente lo standard internazionale dell'Agenzia Mondiale Antidoping (WADA) per la protezione della privacy e dei dati personali, le disposizioni pertinenti del codice WADA e le altre questioni inerenti la vita privata nell'ambito della lotta contro il doping nello sport da parte della WADA e di altre organizzazioni (nazionali) antidoping", adottato il 6 aprile 2009 (WP 162).

protezione degli interessati. In nessun caso l'esito dell'esame deve comportare una minore protezione per categorie particolari di dati<sup>33</sup>.

Questo significa anche che, per legittimare un'attività di trattamento dei dati, un responsabile che tratta categorie particolari di dati non può mai invocare *soltanto* un fondamento giuridico ai sensi dell'articolo 7. Ove applicabile, l'articolo 7 non *prevarrà* ma si applicherà sempre in maniera *cumulativa* con l'articolo 8 al fine di garantire il rispetto di tutte le garanzie e le misure pertinenti. Si tratta di una precisazione ancor più pertinente qualora gli Stati membri decidano di stabilire ulteriori deroghe oltre a quelle previste dall'articolo 8, conformemente a quanto previsto dall'articolo 8, paragrafo 4.

### **III.2. Articolo 7, lettere da a) a e)**

La presente sezione III.2 fornisce una breve panoramica di ciascuno dei fondamenti giuridici di cui all'articolo 7, lettere da a) a e), della direttiva, prima che, nella sezione III.3, il parere si concentri sull'articolo 7, lettera f). L'analisi evidenzierà inoltre alcune delle interfacce più comuni tra tali fondamenti giuridici, quali, ad esempio, "l'esecuzione di un contratto", "l'adempimento di un obbligo legale" e "il perseguimento dell'interesse legittimo", a seconda del contesto particolare e delle circostanze del caso.

#### **III.2.1. Consenso**

Il consenso come fondamento giuridico è stato analizzato nel parere 15/2011 del Gruppo di lavoro sulla definizione di consenso. Le conclusioni principali del parere sono che il consenso è uno dei vari motivi che legittimano il trattamento dei dati personali, anziché il fondamento giuridico principale. 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 responsabile 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.

Fra le sue raccomandazioni, il Gruppo di lavoro ha insistito sulla necessità di chiarire il significato di "consenso inequivocabile": "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."<sup>34</sup> Ha inoltre raccomandato di obbligare i responsabili del trattamento dei dati a mettere a punto meccanismi per dimostrare di aver effettivamente ottenuto il consenso (nell'ambito di un obbligo generale di rendiconto) e ha chiesto al legislatore di aggiungere una prescrizione esplicita relativa alla qualità e all'accessibilità delle informazioni che costituiscono il fondamento per il consenso.

---

<sup>33</sup> Va da sé che, anche nel caso dell'applicazione dell'articolo 8, deve essere garantito il rispetto delle altre disposizioni della direttiva, tra cui l'articolo 6.

<sup>34</sup> Cfr. pagina 42 del parere 15/2011 del Gruppo di lavoro sulla definizione di consenso.

### III.2.2. Contratto

L'articolo 7, lettera b), è il fondamento giuridico che può essere invocato nei casi in cui il trattamento "è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona". Questa disposizione contempla due scenari differenti.

- i) Innanzitutto, l'articolo 7, lettera b), riguarda le situazioni in cui il trattamento è necessario all'esecuzione del contratto concluso con la persona interessata. In quest'ambito possono rientrare, per esempio, il trattamento dell'indirizzo dell'interessato affinché possa essere effettuata la consegna delle merci acquistate online o il trattamento degli estremi della carta di credito per l'esecuzione del pagamento. Nel contesto occupazionale, questo fondamento giuridico potrebbe permettere, per esempio, il trattamento di informazioni riguardanti lo stipendio e delle coordinate bancarie al fine di consentire il pagamento dei salari.

Questa disposizione deve essere interpretata rigorosamente e non contempla le situazioni in cui il trattamento non è effettivamente *necessario* all'esecuzione di un contratto, bensì imposto unilateralmente all'interessato dal responsabile del trattamento. Inoltre, il fatto che alcuni trattamenti di dati siano coperti da un contratto non significa automaticamente che tali trattamenti siano necessari alla sua esecuzione. Ad esempio, l'articolo 7, lettera b), non è un fondamento giuridico adeguato per creare un profilo dei gusti e delle scelte di stile di vita dell'utente sulla base della sequenza di clic che ha effettuato su un sito web e degli articoli che ha acquistato. Questo perché il responsabile del trattamento dei dati non ha firmato un contratto per elaborare profili, bensì per fornire beni e servizi particolari, per esempio. Anche se tali attività di trattamento sono espressamente menzionate in caratteri minuscoli nel contratto, questo fatto, da solo, non le rende "necessarie" all'esecuzione del contratto.

In questo caso esiste un chiaro collegamento tra la valutazione della necessità e il rispetto del principio di limitazione delle finalità. È importante stabilire la *ratio* esatta del contratto, ossia la sua sostanza e il suo obiettivo fondamentale, poiché sarà questa la base su cui si valuterà se il trattamento dei dati è necessario alla sua esecuzione.

In alcuni casi limite, stabilire se il trattamento è necessario all'esecuzione del contratto potrebbe essere sostenibile o richiedere accertamenti più specifici. Per esempio, la creazione di una banca dati aziendale con i recapiti dei dipendenti interni, in cui siano indicati il nome, l'indirizzo professionale, il numero di telefono e l'e-mail di tutti i dipendenti al fine di consentire a questi ultimi di contattare i loro colleghi, in alcune situazioni potrebbe essere considerata necessaria per l'esecuzione di un contratto ai sensi dell'articolo 7, lettera b), ma potrebbe anche essere legittima ai sensi dell'articolo 7, lettera f), qualora l'interesse prevalente del responsabile del trattamento sia dimostrato e siano adottate tutte le misure appropriate, compresa ad esempio l'opportuna consultazione dei rappresentanti dei dipendenti.

Altre situazioni, quali ad esempio il monitoraggio elettronico dell'utilizzo di Internet, della posta elettronica o del telefono da parte dei dipendenti o la videosorveglianza dei lavoratori costituiscono più chiaramente trattamenti che con ogni probabilità vanno oltre quanto necessario all'esecuzione di un contratto di lavoro, sebbene anche in questo caso ciò possa dipendere dalla natura dell'attività lavorativa. La prevenzione

delle frodi, che fra le altre attività potrebbe comprendere il monitoraggio e la creazione di profili dei clienti, è un altro tipico ambito che si potrebbe ritenere al di là di quanto necessario all'esecuzione di un contratto. Tale trattamento potrebbe dunque essere comunque legittimo ai sensi di un altro criterio di liceità di cui all'articolo 7, per esempio il consenso, se del caso, un obbligo legale o l'interesse legittimo del responsabile del trattamento (articolo 7, lettere a), c) o f))<sup>35</sup>. In quest'ultimo caso, il trattamento deve essere soggetto a garanzie e misure supplementari al fine di tutelare adeguatamente gli interessi o i diritti e le libertà degli interessati.

L'articolo 7, lettera b), si applica esclusivamente a ciò che è necessario all'*esecuzione* di un contratto. Non si applica a tutte le ulteriori azioni avviate a seguito di inosservanza o a tutti gli altri incidenti intervenuti nell'esecuzione di un contratto. Fintantoché riguarda la normale esecuzione di un contratto, il trattamento potrebbe rientrare nel campo di applicazione dell'articolo 7, lettera b). Qualora nell'esecuzione di un contratto si verifichi un incidente che determina un conflitto, il trattamento dei dati potrebbe seguire un corso diverso. Il trattamento delle informazioni di base dell'interessato, quali il nome, l'indirizzo e il riferimento ai restanti obblighi contrattuali per l'invio di solleciti formali dovrebbe comunque essere considerato come rientrante nel trattamento dei dati necessario all'esecuzione di un contratto. Quanto a trattamenti di dati più elaborati, che potrebbero prevedere o meno il coinvolgimento di terzi, quali il recupero del debito estero o la citazione in giudizio di un cliente che non ha pagato per un servizio, si potrebbe sostenere che tali trattamenti non avvengono più nell'ambito della "normale" esecuzione di un contratto e pertanto non rientrano nel campo di applicazione dell'articolo 7, lettera b). Tuttavia, ciò non renderebbe il trattamento illegittimo in quanto tale: è nell'interesse legittimo del responsabile del trattamento esperire mezzi di ricorso per garantire il rispetto dei suoi diritti contrattuali. Potrebbero essere invocati altri fondamenti giuridici, quali l'articolo 7, lettera f), fatte salve garanzie e misure adeguate e subordinatamente al soddisfacimento del test comparativo<sup>36</sup>.

- ii) In secondo luogo, l'articolo 7, lettera b), riguarda anche il trattamento che si effettua *prima* della conclusione di un contratto. In quest'ambito rientrano le relazioni precontrattuali, purché siano prese misure su richiesta dell'interessato, anziché su iniziativa del responsabile del trattamento o di terzi. Per esempio, se una persona chiede a un rivenditore al dettaglio di mandarle un'offerta per un prodotto, il trattamento effettuato a tal fine, tramite la conservazione dei dati relativi all'indirizzo e delle informazioni riguardanti la richiesta, per un periodo di tempo limitato, sarà appropriato ai sensi di questo fondamento giuridico. Analogamente, se una persona

---

<sup>35</sup> È possibile trovare un altro esempio di fondamenti giuridici multipli nel parere 15/2011 del Gruppo di lavoro sulla definizione di consenso (citato alla nota a piè di pagina 2). Per acquistare un'automobile, il responsabile 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).

<sup>36</sup> Per quanto riguarda le categorie particolari di dati, potrebbe essere necessario prendere in considerazione anche l'articolo 8, paragrafo 1, lettera e), "necessario per costituire, esercitare o difendere un diritto per via giudiziaria".

chiede un preventivo assicurativo per la propria automobile, l'assicuratore potrebbe trattare i dati necessari, per esempio la marca e l'età dell'autoveicolo nonché altri dati pertinenti e proporzionati, al fine di preparare il preventivo.

Tuttavia, verifiche dettagliate dei precedenti quali, ad esempio, il trattamento dei dati relativi a controlli medici prima che una società di assicurazioni stipuli un'assicurazione sulla salute o un'assicurazione sulla vita con un richiedente, non saranno considerate misure necessarie prese su richiesta dell'interessato. Anche le verifiche delle informazioni creditizie svolte prima della concessione di un prestito non sono effettuate su *richiesta* dell'interessato ai sensi dell'articolo 7, lettera b), bensì ai sensi dell'articolo 7, lettera f), o dell'articolo 7, lettera c), conformemente all'obbligo giuridico delle banche di consultare un elenco ufficiale di debitori registrati.

Non sarà nemmeno possibile inviare materiale pubblicitario su iniziativa del rivenditore al dettaglio/responsabile del trattamento sulla base di questo fondamento giuridico. In alcuni casi, fatte salve garanzie e misure adeguate e subordinatamente al soddisfacimento del test comparativo, un fondamento giuridico adeguato potrebbe essere rappresentato dall'articolo 7, lettera f), anziché dall'articolo 7, lettera b). In altri casi, compresi quelli che comportano la creazione di profili completi, la condivisione dei dati, l'invio di materiale pubblicitario online o la pubblicità comportamentale, occorre prendere in considerazione il consenso di cui all'articolo 7, lettera a), come si evince dall'analisi sottostante<sup>37</sup>.

### III.2.3. Obbligo legale

L'articolo 7, lettera c), è il fondamento giuridico che può essere invocato nei casi in cui il trattamento "è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento". Questa situazione potrebbe verificarsi, per esempio, quando i datori di lavoro devono comunicare i dati relativi agli stipendi dei loro dipendenti alle autorità tributarie o previdenziali o quando gli istituti finanziari sono tenuti a segnalare talune operazioni sospette alle autorità competenti ai sensi delle norme antiriciclaggio. Potrebbe anche essere un obbligo cui è soggetta un'autorità pubblica, poiché niente limita l'applicazione dell'articolo 7, lettera c), al settore privato o pubblico. Questo fondamento giuridico potrebbe ad esempio applicarsi alla raccolta di dati da parte di un'autorità locale per la gestione delle multe per sosta vietata.

L'articolo 7, lettera c), presenta analogie con l'articolo 7, lettera e), poiché spesso un compito di interesse pubblico si basa su una disposizione giuridica o deriva da essa. Il campo di applicazione dell'articolo 7, lettera c), è tuttavia rigidamente delimitato.

Affinché sia possibile applicare l'articolo 7, lettera c), l'obbligo deve essere imposto dalla legge (e non, per esempio, da una disposizione contrattuale). La legge deve soddisfare tutte le pertinenti condizioni volte a rendere l'obbligo valido e vincolante e deve altresì rispettare la

---

<sup>37</sup> Cfr. la sezione III.3.6 (b) al paragrafo "Esempio: l'evoluzione nell'approccio all'invio di materiale pubblicitario", pagg. 54-55.

normativa in materia di protezione dei dati, tra cui i requisiti di necessità, proporzionalità<sup>38</sup> e limitazione delle finalità.

È inoltre importante sottolineare che l'articolo 7, lettera c), si riferisce alla legislazione dell'Unione europea o di uno Stato membro. Gli obblighi previsti dagli ordinamenti nazionali dei paesi terzi (quali, ad esempio, l'obbligo di istituire procedure per la denuncia delle irregolarità ai sensi della legge Sarbanes-Oxley, emanata dagli Stati Uniti nel 2002) non sono contemplati da questo fondamento giuridico. Per essere valido, un obbligo legale vigente in un paese terzo dovrà essere ufficialmente riconosciuto e integrato nell'ordinamento giuridico dello Stato membro interessato, per esempio sotto forma di accordo internazionale<sup>39</sup>. D'altro canto, la necessità di rispettare un obbligo vigente in un paese terzo potrebbe rappresentare un interesse legittimo del responsabile del trattamento, ma solo subordinatamente al test comparativo dell'articolo 7, lettera f), e purché siano predisposte garanzie adeguate come quelle adottate dall'autorità di protezione dei dati competente.

Il responsabile del trattamento non deve poter scegliere se adempiere o meno l'obbligo legale. Se va al di là di quanto prescritto dalla legge, il trattamento dei dati effettuato nell'ambito degli impegni volontari unilaterali e dei partenariati pubblico-privato non è pertanto contemplato dall'articolo 7, lettera c). Se, per esempio, senza avere un chiaro e specifico obbligo legale di agire in tal senso, un fornitore di servizi Internet decide di monitorare i suoi utenti nel tentativo di contrastare il download illegale di contenuti, l'articolo 7, lettera c), non rappresenta un fondamento giuridico adeguato a tal fine.

Inoltre, l'obbligo legale stesso deve essere sufficientemente chiaro riguardo al trattamento dei dati personali che richiede. Di conseguenza, l'articolo 7, lettera c), si applica sulla base delle disposizioni giuridiche che si riferiscono espressamente alla natura e all'oggetto del trattamento. Il responsabile del trattamento non deve avere un indebito potere discrezionale sulle modalità di adempimento dell'obbligo legale.

In alcuni casi la legislazione potrebbe fissare solo un obiettivo generale, imponendo obblighi più specifici a un livello differente, per esempio o nel diritto derivato o con una decisione vincolante di un'autorità pubblica in un caso concreto. Ne potrebbero altresì scaturire obblighi legali ai sensi dell'articolo 7, lettera c), purché la natura e l'oggetto del trattamento siano ben definiti e soggetti a una base giuridica adeguata.

Tuttavia, la situazione sarebbe diversa se un'autorità di regolamentazione stabilisse esclusivamente orientamenti politici generali nonché le condizioni alle quali potrebbe valutare l'opportunità di utilizzare i suoi poteri di esecuzione (ad esempio orientamenti normativi destinati agli istituti finanziari su taluni criteri di debita diligenza). In tali circostanze, le

---

<sup>38</sup> Cfr. anche il parere 1/2014 del Gruppo di lavoro sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto, adottato il 27 febbraio 2014 (WP 211).

<sup>39</sup> Cfr. a questo proposito la sezione 4.2.2 del parere 10/2006 del Gruppo di lavoro sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT), adottato il 20 novembre 2006 (WP 128), e il parere 1/2006 del Gruppo di lavoro relativo all'applicazione della normativa UE sulla protezione dei dati alle procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria, adottato il 1° febbraio 2006 (WP 117).

attività di trattamento dovrebbero essere valutate ai sensi dell'articolo 7, lettera f), ed essere considerate legittime solo subordinatamente all'ulteriore test comparativo<sup>40</sup>.

Come osservazione generale, è opportuno rilevare che alcune attività di trattamento potrebbero sembrare rientrare nella portata dell'articolo 7, lettere c) o b), senza rispettare appieno i criteri di applicazione di tali fondamenti giuridici. Questo non significa che tali attività di trattamento siano sempre necessariamente illegittime: talvolta potrebbero essere legittime, ma ai sensi dell'articolo 7, lettera f), subordinatamente all'ulteriore test comparativo.

#### **III.2.4. Interesse vitale**

L'articolo 7, lettera d), è il fondamento giuridico che può essere invocato nei casi in cui il trattamento “è necessario per la salvaguardia dell'interesse vitale della persona interessata”. La formulazione si discosta dal linguaggio utilizzato all'articolo 8, paragrafo 2, lettera c), che è più specifico e si riferisce a situazioni in cui “il trattamento sia necessario per salvaguardare un interesse vitale della persona interessata o di un terzo nel caso in cui la persona interessata è nell'incapacità fisica o giuridica di dare il proprio consenso”.

Entrambe le disposizioni sembrano tuttavia suggerire che l'applicazione di questo fondamento giuridico deve essere limitata. Innanzitutto, l'espressione “interesse vitale” sembra limitare l'applicazione di questo fondamento a questioni di vita e di morte o, quanto meno, a minacce che comportano un rischio per l'incolumità o la salute dell'interessato (o, nel caso dell'articolo 8, paragrafo 2, lettera c), anche di un terzo).

Il considerando 31 conferma che l'obiettivo di questo fondamento giuridico è “tutelare un interesse essenziale alla vita della persona interessata”. Tuttavia, la direttiva non indica con esattezza se la minaccia deve essere immediata. Questa mancanza di precisione solleva problemi riguardo al campo di applicazione della raccolta dei dati, per esempio come misura preventiva su larga scala, quale la raccolta dei dati dei passeggeri aerei nei casi in cui siano stati individuati un rischio di malattia epidemiologica o un incidente relativo alla sicurezza.

Il Gruppo di lavoro ritiene che questa disposizione debba essere interpretata in maniera restrittiva, conformemente allo spirito dell'articolo 8. Benché l'articolo 7, lettera d), non limiti espressamente l'utilizzo di questo fondamento ai casi in cui il consenso non può essere utilizzato come motivo di liceità, per le ragioni indicate all'articolo 8, paragrafo 2, lettera c), è ragionevole presumere che, nelle situazioni in cui sussistono la possibilità e la necessità di chiedere un consenso valido, il consenso debba essere effettivamente richiesto ogniqualvolta sia possibile. Di conseguenza l'applicazione di questa disposizione sarà inoltre limitata a un'analisi caso per caso e l'articolo 7, lettera d), non potrà di norma essere utilizzato per legittimare la raccolta e il trattamento di un'ingente quantità di dati personali. Laddove ciò fosse necessario, l'articolo 7, lettera c), o l'articolo 7, lettera e), sarebbero fondamenti giuridici più appropriati per il trattamento.

---

<sup>40</sup> Gli orientamenti forniti da un'autorità di regolamentazione possono comunque svolgere un ruolo importante nella valutazione dell'interesse legittimo del responsabile del trattamento (cfr. la sezione III.3.4, in particolare il paragrafo (a), a pagina 40).

### III.2.5. Compito di interesse pubblico

L'articolo 7, lettera e), è il fondamento giuridico che può essere invocato nei casi in cui il trattamento "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati".

È importante rilevare che, proprio come l'articolo 7, lettera c), anche l'articolo 7, lettera e), si riferisce all'interesse pubblico dell'Unione europea o di uno Stato membro. Analogamente, l'espressione "pubblici poteri" si riferisce a un mandato conferito dall'Unione europea o da uno Stato membro. In altre parole, i compiti eseguiti nell'interesse pubblico di un paese terzo o connessi all'esercizio di pubblici poteri conferiti in virtù del diritto estero non rientrano nel campo di applicazione di questa disposizione<sup>41</sup>.

L'articolo 7, lettera e), contempla due situazioni ed è pertinente sia per il settore pubblico che per quello privato. Innanzitutto, riguarda le situazioni in cui il responsabile del trattamento stesso è investito di pubblici poteri o svolge un compito di interesse pubblico (ma non è necessariamente soggetto anche all'adempimento di un obbligo legale per il trattamento dei dati) e il trattamento è necessario all'esercizio di tali poteri o all'esecuzione di quel compito. Per esempio, un'autorità tributaria può raccogliere e trattare i dati relativi alla dichiarazione dei redditi di una persona al fine di stabilire e verificare l'importo da versare a titolo di imposta. Oppure un'associazione professionale come un ordine forense o un ordine di professionisti del settore medico investiti di pubblici poteri per agire in tal senso possono avviare procedimenti disciplinari nei confronti di alcuni dei loro membri. Un altro esempio ancora potrebbe essere costituito da un ente pubblico locale quale un'amministrazione comunale cui sia stato affidato il compito di gestire un servizio di biblioteca, una scuola o una piscina comunale.

In secondo luogo, l'articolo 7, lettera e), contempla anche i casi in cui il responsabile del trattamento non è investito di pubblici poteri, ma è tenuto a comunicare i dati su richiesta di terzi insigniti di tali poteri. Per esempio, il funzionario di un ente pubblico responsabile delle indagini per reati penali potrebbe chiedere al responsabile del trattamento di cooperare a un'indagine in corso anziché ordinargli di ottemperare a una specifica richiesta di cooperazione. L'articolo 7, lettera e), può inoltre contemplare i casi in cui il responsabile del trattamento comunica proattivamente i dati a un terzo investito di pubblici poteri. Questa situazione può verificarsi, per esempio, quando un responsabile del trattamento constata che è stato commesso un reato e fornisce questa informazione alle autorità di contrasto competenti di sua iniziativa.

Diversamente da quanto avviene nel caso dell'articolo 7, lettera c), il responsabile del trattamento non è tenuto ad agire nell'ambito di un obbligo legale. Utilizzando l'esempio precedente, qualora si rendesse accidentalmente conto che sono stati commessi un furto o una frode, un responsabile del trattamento potrebbe non essere giuridicamente tenuto a darne comunicazione alla polizia, ma, ove opportuno, potrebbe tuttavia riferire volontariamente tali informazioni sulla base dell'articolo 7, lettera e).

---

<sup>41</sup> Cfr. la sezione 2.4 del documento di lavoro del Gruppo di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE del 24 ottobre 1995, adottato il 25 novembre 2005 (WP 114), che fornisce un'interpretazione analoga del concetto di "interesse pubblico rilevante" all'articolo 26, paragrafo 1, lettera d).

Tuttavia, il trattamento deve essere “necessario per l’esecuzione di un compito di interesse pubblico”. In alternativa, o il responsabile del trattamento o il terzo cui il responsabile del trattamento comunica i dati devono essere investiti di pubblici poteri e il trattamento dei dati deve essere necessario all’esercizio di tali poteri<sup>42</sup>. È inoltre importante sottolineare che questi pubblici poteri o compiti di interesse pubblico saranno stati di norma attribuiti dal diritto ordinario o da altre disposizioni giuridiche. Se il trattamento comporta un’ingerenza nella vita privata o se è altrimenti previsto ai sensi del diritto nazionale al fine di garantire la protezione delle persone interessate, la base giuridica deve essere specifica e sufficientemente precisa riguardo alla definizione del tipo di trattamento di dati che potrebbe essere consentito.

Queste situazioni stanno diventando sempre più comuni, anche oltre i confini del settore pubblico, se si considera la tendenza ad affidare compiti governativi a enti del settore privato, come avviene, per esempio, nell’ambito delle attività di trattamento nel settore dei trasporti o della salute (per esempio studi epidemiologici, ricerca). Questo fondamento giuridico potrebbe essere invocato anche in un contesto di attività di contrasto, come è già stato suggerito negli esempi precedenti. Tuttavia, per valutare la misura in cui a una società privata può essere consentito di cooperare con le autorità di contrasto, per esempio nella lotta contro la frode o contro i contenuti illeciti diffusi su Internet, deve essere effettuata un’analisi non solo ai sensi dell’articolo 7, ma anche ai sensi dell’articolo 6, considerando il principio della limitazione delle finalità e i requisiti di lealtà e liceità del trattamento<sup>43</sup>.

L’articolo 7, lettera e), ha potenzialmente un campo di applicazione molto vasto e, di conseguenza, occorre interpretare restrittivamente e individuare chiaramente, caso per caso, l’interesse pubblico in gioco e i pubblici poteri che giustificano il trattamento. Questo ampio campo di applicazione spiega anche perché, proprio come per l’articolo 7, lettera f), all’articolo 14 è stato previsto un diritto di opposizione nei casi in cui il trattamento si basa sull’articolo 7, lettera e)<sup>44</sup>. Garanzie e misure supplementari analoghe potrebbero pertanto essere applicate in entrambi i casi<sup>45</sup>.

In questo senso, l’articolo 7, lettera e), presenta analogie con l’articolo 7, lettera f), e in alcuni contesti, in particolare per quanto riguarda le autorità pubbliche, l’articolo 7, lettera e), può sostituire l’articolo 7, lettera f).

Nel valutare il campo di applicazione di queste disposizioni agli organismi del settore pubblico, specialmente alla luce delle modifiche proposte al quadro giuridico applicabile in materia di protezione dei dati, è utile rilevare che nel testo attuale del regolamento (CE)

---

<sup>42</sup> In altre parole, in questi casi la rilevanza pubblica dei compiti e la corrispondente responsabilità continueranno a essere presenti anche se l’esecuzione dei compiti è stata trasferita ad altri organi, anche di natura privata.

<sup>43</sup> Cfr., a tale proposito, il parere 10/2006 del Gruppo di lavoro sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT), citato alla precedente nota a piè di pagina 39, il parere 4/2003 del Gruppo di lavoro sul livello di protezione assicurato negli Stati Uniti per quanto riguarda la trasmissione di dati relativi ai passeggeri, adottato il 13 giugno 2003 (WP 78) e il documento di lavoro sulle questioni relative alla protezione dei dati per quanto riguarda i diritti di proprietà intellettuale, adottato il 18 gennaio 2005 (WP 104).

<sup>44</sup> Come precedentemente indicato, in alcuni Stati membri (per esempio la Svezia) non esiste la possibilità di opporsi a un trattamento dei dati basato sull’articolo 7, lettera e).

<sup>45</sup> Come sarà illustrato di seguito, il progetto di relazione della commissione LIBE ha suggerito l’introduzione di ulteriori garanzie, in particolare una maggiore trasparenza, nei casi in cui si applica l’articolo 7, lettera f).

n. 45/2001<sup>46</sup>, contenente le norme di protezione dei dati applicabili alle istituzioni e agli organismi dell'Unione europea, non figurano disposizioni paragonabili all'articolo 7, lettera f).

Tuttavia, il considerando 27 di tale regolamento stabilisce che “il trattamento di dati personali per l'esercizio delle funzioni svolte dalle istituzioni e dagli organismi comunitari *nel pubblico interesse* comprende il trattamento dei dati personali necessari alla gestione e al funzionamento di tali istituzioni e organismi”. Questa disposizione consente pertanto il trattamento dei dati sulla base dell'interpretazione estensiva del fondamento giuridico del “compito di interesse pubblico” in un'ampia varietà di casi, che avrebbero altrimenti potuto essere contemplati da una disposizione analoga all'articolo 7, lettera f). La videosorveglianza dei locali a fini di sicurezza, il controllo elettronico del traffico mail o le valutazioni del personale sono solo alcuni esempi di situazioni che potrebbero rientrare nell'ambito di questa disposizione di “funzioni svolte [...] nel pubblico interesse” interpretata in maniera estensiva.

Guardando al futuro, è inoltre importante tenere presente che, all'articolo 6, paragrafo 1, lettera f), la proposta di regolamento stabilisce espressamente che il fondamento giuridico dell'interesse legittimo “non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esercizio dei loro compiti”. Se questa disposizione sarà adottata e interpretata estensivamente, in modo che alle autorità pubbliche sia completamente preclusa la possibilità di utilizzare l'interesse legittimo come fondamento giuridico, allora i criteri del “compito di interesse pubblico” e dei “pubblici poteri” di cui all'articolo 7, lettera e), dovranno essere interpretati in modo da concedere alle autorità pubbliche una certa flessibilità, almeno per garantirne la corretta gestione e il buon funzionamento, analogamente a quanto avviene secondo l'attuale interpretazione del regolamento (CE) n. 45/2001.

In alternativa, la citata ultima frase dell'articolo 6, paragrafo 1, lettera f), della proposta di regolamento, potrebbe essere interpretata in modo che alle autorità pubbliche non sia completamente preclusa la possibilità di utilizzare l'interesse legittimo come fondamento giuridico. In tal caso, l'espressione “trattamento di dati effettuato dalle autorità pubbliche nell'esercizio dei loro compiti” di cui all'articolo 6, paragrafo 1, lettera f), della proposta di regolamento, dovrà essere interpretata restrittivamente. Secondo tale interpretazione restrittiva, il trattamento finalizzato a garantire la corretta gestione e il buon funzionamento di queste autorità pubbliche non rientrerebbe nel campo di applicazione dell'espressione “trattamento di dati effettuato dalle autorità pubbliche nell'esercizio dei loro compiti”. Di conseguenza, il trattamento finalizzato a garantire la corretta gestione e il buon funzionamento di queste autorità pubbliche potrebbe comunque essere possibile nell'ambito del criterio dell'interesse legittimo.

### **III.3. Articolo 7, lettera f): interesse legittimo**

L'articolo 7, lettera f)<sup>47</sup>, prevede l'esecuzione di un test comparativo: l'interesse legittimo del responsabile del trattamento (oppure del o dei terzi cui vengono comunicati i dati) deve essere valutato rispetto agli interessi o ai diritti e alle libertà fondamentali dell'interessato. L'esito

---

<sup>46</sup> Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

<sup>47</sup> Per il testo integrale dell'articolo 7, lettera f), cfr. pagina 5.

del test comparativo permette di stabilire in ampia misura se l'articolo 7, lettera f), può essere invocato come fondamento giuridico per il trattamento.

Già a questo punto è opportuno segnalare che non si tratta di un semplice test comparativo consistente soltanto nel confrontare tra loro due “pesi” facilmente quantificabili e comparabili. Invece, come sarà illustrato più dettagliatamente di seguito, per eseguire il test comparativo potrebbe essere necessario svolgere una complessa valutazione tenendo conto di una serie di fattori. Al fine di strutturare e semplificare la valutazione, abbiamo suddiviso il processo in più fasi in modo da garantire l'efficace svolgimento del test comparativo.

La sezione III.3.1 esamina innanzitutto uno dei due elementi da valutare ai fini del test comparativo: in che cosa consiste “l'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati”. La sezione III.3.2, invece, esamina l'altro elemento, ovvero in che cosa consistono “l'interesse o i diritti e le libertà fondamentali della persona interessata, che devono essere tutelati ai sensi dell'articolo 1, paragrafo 1”.

Le sezioni III.3.3 e III.3.4 forniscono orientamenti sulle modalità di svolgimento del test comparativo. La sezione III.3.3 fornisce un'introduzione generale avvalendosi di tre scenari differenti. Successivamente a tale introduzione, la sezione III.3.4 delinea le considerazioni più importanti di cui occorre tenere conto durante lo svolgimento del test comparativo, comprese le garanzie e le misure fornite dal responsabile del trattamento.

Le sezioni III.3.5 e III.3.6 esamineranno infine anche alcuni meccanismi particolari, quali il principio di responsabilità, la trasparenza e il diritto di opposizione, che possono contribuire ad assicurare, e a rafforzare ulteriormente, il giusto equilibrio tra i vari interessi che potrebbero essere in gioco.

### **III.3.1. Interesse legittimo del responsabile del trattamento (oppure del o dei terzi cui vengono comunicati i dati)**

#### *Il concetto di “interesse”*

Il concetto di “interesse” è strettamente correlato al concetto di “finalità” citato all'articolo 6 della direttiva, pur distinguendosene. In materia di protezione dei dati, per “finalità” si intendono il motivo specifico per cui si trattano i dati: l'obiettivo o lo scopo del trattamento dei dati. Un interesse, invece, è l'interesse più ampio che un responsabile può avere nel trattamento oppure il beneficio che il responsabile trae (o che potrebbe trarre la società) dal trattamento.

Per esempio, un'azienda potrebbe avere un *interesse* a tutelare la salute e la sicurezza del personale che lavora presso il suo impianto nucleare. Relativamente a questo aspetto, la *finalità* dell'impresa potrebbe essere l'attuazione di determinate procedure di controllo dell'accesso che giustifica il trattamento di taluni dati personali specifici al fine di contribuire a tutelare la salute e la sicurezza del personale.

Un interesse deve essere articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del responsabile del trattamento rispetto agli interessi e ai diritti fondamentali dell'interessato. Inoltre, l'interesse in questione deve anche essere “perseguito dal responsabile del trattamento”. A tal fine l'interesse deve

essere concreto ed effettivo, qualcosa che corrisponda alle attività in corso o ai benefici previsti nell'immediato futuro. In altre parole, gli interessi che sono troppo vaghi o teorici non saranno sufficienti.

La natura dell'interesse può variare. Alcuni interessi possono essere preminenti e vantaggiosi per la società in generale, quali ad esempio l'interesse della stampa a pubblicare informazioni sulla corruzione governativa o l'interesse a svolgere ricerca scientifica (fatte salve garanzie adeguate). Altri interessi possono essere meno preminenti per la società nel suo complesso o, in ogni caso, l'impatto del loro perseguimento sulla società potrebbe essere più eterogeneo o controverso. Questa situazione potrebbe verificarsi, per esempio, nel caso di un'impresa il cui interesse economico è venire a conoscenza del maggior numero possibile di informazioni sui suoi potenziali clienti al fine di pubblicizzare in maniera più mirata i suoi prodotti o servizi.

*Che cosa rende un interesse "legittimo" o "illegittimo"?*

L'obiettivo di questa domanda è individuare la soglia di ciò che costituisce un interesse legittimo. Se l'interesse del responsabile del trattamento dei dati è illegittimo, il test comparativo non sarà effettuato poiché non sarà stata raggiunta la soglia iniziale per l'utilizzo dell'articolo 7, lettera f).

A parere del Gruppo di lavoro, il concetto di interesse legittimo potrebbe comprendere un'ampia serie di interessi, sia di scarso rilievo che decisamente preminenti, evidenti oppure più controversi. Sarà poi in una seconda fase, quando si tratterà di valutare questi interessi rispetto agli interessi e ai diritti fondamentali degli interessati, che occorrerà adottare un approccio più restrittivo ed effettuare un'analisi più sostanziale.

Di seguito è riportato un elenco non esaustivo di alcuni degli ambiti più comuni in cui può porsi la questione dell'interesse legittimo ai sensi dell'articolo 7, lettera f). È presentato lasciando impregiudicata la possibilità che gli interessi del responsabile del trattamento prevalgano in ultima analisi sugli interessi e sui diritti degli interessati al momento dell'esecuzione del test comparativo.

- esercizio del diritto alla libertà di espressione e d'informazione, anche nei mezzi di comunicazione e di espressione artistica
- commercializzazione diretta tradizionale e altre forme di commercializzazione o pubblicità
- messaggi indesiderati non commerciali, anche a fini di campagne politiche o di raccolta fondi per scopi benefici
- esercizio di un diritto in via giudiziale, compreso il recupero del credito tramite procedure extragiudiziali
- prevenzione di frodi, uso improprio dei servizi o riciclaggio di denaro
- controllo del personale a fini di sicurezza o gestione
- procedure per la denuncia delle irregolarità
- sicurezza fisica, sicurezza informatica e sicurezza della rete
- trattamento di dati a scopi statistici o di ricerca storica o scientifica
- trattamento a scopi di ricerca (compresa la ricerca a fini commerciali)

Di conseguenza, un interesse può essere considerato legittimo nella misura in cui il responsabile del trattamento può perseguire tale interesse secondo modalità che sono

conformi alla legislazione in materia di protezione dei dati e ad altre normative. In altre parole, un interesse legittimo deve essere “ammesso dalla legge”<sup>48</sup>.

Di conseguenza, per essere pertinente ai sensi dell’articolo 7, lettera f), un “interesse legittimo” deve:

- essere lecito (ossia conforme al diritto nazionale e unionale applicabile);
- essere articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l’interesse legittimo del responsabile del trattamento rispetto agli interessi e ai diritti fondamentali dell’interessato (ossia sufficientemente specifico);
- rappresentare un interesse concreto ed effettivo (ossia non deve essere teorico).

Il fatto che il responsabile del trattamento abbia tale interesse legittimo nel trattamento di determinati dati non significa che possa necessariamente invocare l’articolo 7, lettera f), come fondamento giuridico per il trattamento. La legittimità dell’interesse del responsabile del trattamento dei dati è solo un punto di partenza, uno degli elementi che devono essere analizzati ai sensi dell’articolo 7, lettera f). La possibilità di invocare l’articolo 7, lettera f), dipenderà dall’esito del test comparativo che segue.

A titolo di esempio, i responsabili del trattamento possono avere un interesse legittimo a conoscere le preferenze dei loro clienti per poter personalizzare meglio le loro offerte e, in definitiva, offrire prodotti e servizi in grado di soddisfare meglio le esigenze e i desideri dei clienti. Alla luce di questa considerazione, l’articolo 7, lettera f), potrebbe essere un fondamento giuridico adeguato da utilizzare per alcuni tipi di attività di commercializzazione, sia online che offline, purché sussistano adeguate garanzie (compreso, fra l’altro, un meccanismo efficace che permetta di opporsi a tale trattamento ai sensi dell’articolo 14, lettera b), come sarà illustrato nella sezione III.3.6 *Il diritto di opposizione e oltre*).

Tuttavia, questo non significa che i responsabili del trattamento potranno avvalersi dell’articolo 7, lettera f), per controllare indebitamente le attività online o offline dei loro clienti, combinare grandi quantitativi di dati che li riguardano, dopo averli ricavati da varie fonti e averli inizialmente raccolti in altri contesti e per finalità differenti, e creare (e, ad esempio, grazie agli intermediari che forniscono dati, anche effettuare la compravendita di) profili complessi delle personalità e delle preferenze dei clienti a loro insaputa, senza un meccanismo efficace che permetta di opporsi al trattamento dei dati e tantomeno senza il loro

---

<sup>48</sup> Le osservazioni sulla natura della “legittimità” formulate nella sezione III.1.3 del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato alla precedente nota a piè di pagina 9) si applicano anche in questo caso, *mutatis mutandis*. Come alle pagine 19-20 del summenzionato parere, il concetto di ‘legge’ è utilizzato qui nel suo significato più ampio. Vi rientrano altre normative applicabili, fra cui leggi in materia di occupazione, contratti o tutela dei consumatori. Inoltre, il concetto di legge “comprende tutte le forme di diritto scritto e diritto comune, diritto primario e derivato, ordinanze comunali, precedenti giurisprudenziali, principi costituzionali, diritti fondamentali, altri principi legali nonché la giurisprudenza, poiché tale “legge” sarà interpretata e presa in considerazione dai tribunali competenti. Entro i confini della legge, per stabilire se una determinata finalità è legittima, possono essere presi in considerazione anche altri elementi quali codici doganali, codici di condotta, codici deontologici, accordi contrattuali nonché il contesto generale e gli elementi fattuali del caso. In quest’ambito rientrerà la natura, commerciale o di altro tipo, della relazione esistente tra il responsabile del trattamento e gli interessati”. Inoltre, ciò che può essere considerato come un interesse legittimo “può anche cambiare nel tempo, subordinatamente agli sviluppi scientifici e tecnologici e ai cambiamenti nella società e negli atteggiamenti culturali”.

consenso informato. È probabile che tale attività di profilazione costituisca una considerevole ingerenza nella vita privata del cliente e, in tal caso, sull'interesse del responsabile del trattamento prevarrebbero gli interessi e i diritti dell'interessato<sup>49</sup>.

Il parere sul trattamento dei dati personali da parte della Società per le telecomunicazioni finanziarie interbancarie mondiali (SWIFT)<sup>50</sup> contiene un ulteriore esempio: pur avendo riconosciuto l'interesse legittimo della società a soddisfare le richieste ufficiali a norma del diritto statunitense, per evitare il rischio di farsi infliggere sanzioni da parte delle autorità degli USA, il Gruppo di lavoro ha stabilito l'impossibilità di avvalersi dell'articolo 7, lettera f), come fondamento giuridico. Il Gruppo di lavoro ha ritenuto in particolare che, a causa degli effetti a lungo raggio che potrebbe avere sugli individui il trattamento dei dati effettuato "nascostamente, sistematicamente, in grandi proporzioni e nel lungo periodo", "gli interessi ed i diritti e libertà fondamentali dei numerosi individui ai quali si riferiscono i dati prevalgono sull'interesse della SWIFT di non farsi infliggere sanzioni dagli USA per non aver eventualmente soddisfatto le sue richieste ufficiali".

Come sarà illustrato più avanti, se l'interesse perseguito dal responsabile del trattamento non è preminente, è più probabile che l'interesse e i diritti dell'interessato prevalgano rispetto al legittimo, ma meno importante, interesse del responsabile del trattamento. Al contempo, questo non significa che l'interesse meno preminente del responsabile del trattamento non possa talvolta prevalere rispetto agli interessi e ai diritti degli interessati: in genere questa situazione si verifica quando anche l'impatto del trattamento sugli interessati è meno rilevante.

#### *Interesse legittimo nel settore pubblico*

Il testo attuale della direttiva non vieta espressamente ai responsabili del trattamento che sono autorità pubbliche di trattare dati avvalendosi dell'articolo 7, lettera f), come fondamento giuridico per il trattamento<sup>51</sup>.

Tuttavia, la proposta di regolamento<sup>52</sup> esclude questa possibilità per il "trattamento di dati effettuato dalle autorità pubbliche nell'esercizio dei loro compiti".

La modifica legislativa proposta evidenzia l'importanza del principio generale secondo cui le autorità pubbliche, di norma, devono trattare dati esclusivamente nell'esercizio dei loro compiti, purché siano opportunamente autorizzate dalla legge ad agire in tal senso. L'adesione a questo principio è particolarmente importante, ed espressamente prevista dalla giurisprudenza della Corte europea dei diritti dell'uomo, nei casi in cui è in gioco la vita

---

<sup>49</sup> La questione delle tecnologie di tracciamento e il ruolo del consenso di cui all'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche saranno discussi separatamente. Cfr. la sezione III.3.6 (b) al paragrafo "Esempio: l'evoluzione nell'approccio all'invio di materiale pubblicitario".

<sup>50</sup> Cfr. la sezione 4.2.3 del parere già citato alla precedente nota a piè di pagina 39. In questo caso l'interesse legittimo del responsabile del trattamento era collegato anche all'interesse pubblico di un paese terzo, situazione che non poteva essere fatta rientrare nel campo di applicazione della direttiva 95/46/CE.

<sup>51</sup> In origine la prima proposta di direttiva della Commissione disciplinava separatamente il trattamento dei dati nel settore privato e le attività di trattamento nel settore pubblico. Questa distinzione formale tra le norme che si applicano al settore pubblico e quelle applicabili al settore privato è stata abbandonata nella proposta modificata. Ciò potrebbe avere a sua volta determinato differenze nell'interpretazione e nell'attuazione da parte dei vari Stati membri.

<sup>52</sup> Cfr. l'articolo 6, paragrafo 1, lettera f), della proposta di regolamento.

privata degli interessati e le attività dell'autorità pubblica costituirebbero un'ingerenza nella loro vita privata.

È pertanto necessaria un'autorizzazione prevista dalla legge, anche ai sensi dell'attuale direttiva, sufficientemente *dettagliata e specifica* nel caso in cui il trattamento effettuato dalle autorità pubbliche costituisca un'ingerenza nella vita privata degli interessati. Tale prescrizione può assumere la forma di uno specifico obbligo giuridico per il trattamento dei dati, in grado di ottemperare all'articolo 7, lettera c), o di un'autorizzazione specifica (senza essere necessariamente un obbligo) al trattamento dei dati, che possa rispettare le prescrizioni dell'articolo 7, lettere e) o f)<sup>53</sup>.

### *Interesse legittimo dei terzi*

Il testo attuale della direttiva non fa soltanto riferimento al “perseguimento dell'interesse legittimo del responsabile del trattamento”, ma permette di avvalersi dell'articolo 7, lettera f), anche quando l'interesse legittimo è perseguito dal o dai “terzi cui vengono comunicati i dati”<sup>54</sup>. Gli esempi riportati di seguito illustrano alcuni dei contesti in cui potrebbe essere applicata questa disposizione.

*Pubblicazione dei dati a fini di trasparenza e responsabilità.* Un contesto importante in cui l'applicazione dell'articolo 7, lettera f), potrebbe essere pertinente è il caso della pubblicazione di dati a fini di trasparenza e responsabilità (per esempio, gli stipendi degli alti dirigenti di una società). In questo caso si può ritenere che la divulgazione pubblica sia effettuata essenzialmente non nell'interesse del responsabile del trattamento che pubblica i dati, bensì nell'interesse di altre parti interessate, quali i dipendenti dell'azienda, i giornalisti o il grande pubblico, cui sono comunicati i dati.

Dal punto di vista della protezione dei dati e della tutela della vita privata, e per garantire la certezza del diritto in generale, è consigliabile che i dati personali siano comunicati al pubblico sulla base di una legge che consenta e, ove opportuno, specifichi chiaramente i dati che devono essere pubblicati, le finalità della pubblicazione e tutte le garanzie necessarie<sup>55</sup>. Questo significa anche che, quando i dati personali sono comunicati a fini di trasparenza e

---

<sup>53</sup> A tale proposito, cfr. anche la precedente sezione III.2.5 sul compito di interesse pubblico (pagg. 25-27) nonché le questioni affrontate nel prosieguo alla rubrica *Interesse legittimo dei terzi* (pagg. 32-34). Cfr. anche le riflessioni sui limiti della “applicazione delle norme su iniziativa dei privati” a pagina 41, alla rubrica “interesse pubblico/interesse della collettività”. In tutte queste situazioni, è particolarmente importante garantire che siano rispettati appieno i limiti sia dell'articolo 7, lettera f), che dell'articolo 7, lettera e).

<sup>54</sup> La proposta di regolamento intende limitare l'utilizzo di questo fondamento al “perseguimento del legittimo interesse del responsabile del trattamento”. Dal solo testo non si riesce a evincere se con l'espressione proposta si voglia meramente semplificare il testo o se si intenda escludere le situazioni in cui un responsabile del trattamento potrebbe comunicare i dati nell'interesse legittimo altrui. Il testo è comunque non definitivo. L'interesse dei terzi è stato per esempio reintrodotta nella relazione finale della commissione LIBE in occasione del voto del 21 ottobre 2013 sugli emendamenti di compromesso della commissione LIBE del Parlamento europeo. Cfr. l'emendamento 100 all'articolo 6. Il Gruppo di lavoro è favorevole alla reintroduzione dell'interesse dei terzi nella proposta poiché il suo utilizzo potrebbe continuare a essere appropriato in alcune situazioni, tra cui quelle descritte di seguito.

<sup>55</sup> Questa raccomandazione sulle migliori pratiche non deve pregiudicare le norme giuridiche nazionali in materia di trasparenza e accesso del pubblico ai documenti.

responsabilità, potrebbe essere preferibile utilizzare come base giuridica l'articolo 7, lettera c), anziché l'articolo 7, lettera f)<sup>56</sup>.

Tuttavia, in assenza di un obbligo giuridico specifico o di un'autorizzazione a pubblicare i dati, sarà comunque possibile comunicare i dati personali alle pertinenti parti interessate. Ove opportuno, sarà anche possibile pubblicare i dati personali a fini di trasparenza e responsabilità.

In entrambi i casi, ossia a prescindere che i dati personali siano comunicati sulla base di una legge che ne autorizza la divulgazione o meno, la loro diffusione dipende direttamente dall'esito del test comparativo di cui all'articolo 7, lettera f), nonché dall'attuazione di garanzie e misure adeguate<sup>57</sup>.

Inoltre, l'ulteriore utilizzo, ai fini di una maggiore trasparenza, di dati personali già divulgati (per esempio, la ripubblicazione dei dati da parte della stampa oppure l'ulteriore diffusione, in maniera più innovativa e semplice, della serie di dati pubblicata inizialmente da parte di una ONG) potrebbe essere anch'esso auspicabile. La possibilità di ripubblicare e riutilizzare i dati dipenderà a sua volta dall'esito del test comparativo, che dovrà tenere conto, tra l'altro, della natura delle informazioni e dell'effetto della ripubblicazione o del riutilizzo sulle persone<sup>58</sup>.

*Ricerca storica o altri tipi di ricerca scientifica.* Altri contesti importanti in cui potrebbe essere pertinente comunicare i dati nell'interesse legittimo di terzi sono la ricerca storica o altri tipi di ricerca scientifica, in particolare laddove sia necessario accedere a determinate banche dati. La direttiva riconosce espressamente tali attività, fatte salve garanzie e misure adeguate<sup>59</sup>, ma è opportuno ricordare che il fondamento che legittima queste attività sarà spesso un utilizzo ben ponderato dell'articolo 7, lettera f)<sup>60</sup>.

---

<sup>56</sup> Di fatto, in alcuni Stati membri devono essere rispettate norme differenti riguardo al trattamento effettuato da soggetti pubblici e privati. Ai sensi del Codice italiano in materia di protezione dei dati personali, per esempio, la diffusione di dati personali da parte di un soggetto pubblico è ammessa unicamente quando è prevista da una norma di legge o di regolamento (articolo 19, comma 3).

<sup>57</sup> Come spiegato nel parere 6/2013 del Gruppo di lavoro sui dati aperti (cfr. pagg. 9-10 del suddetto parere, citato di seguito nella nota a piè di pagina 88), qualsiasi pratica o normativa nazionale in materia di trasparenza "deve osservare l'articolo 8 della CEDU e gli articoli 7 e 8 della Carta dell'UE. Ne consegue, come ha affermato la Corte di giustizia nelle sentenze *Österreichischer Rundfunk* e *Schecke*, che si dovrebbe verificare se la divulgazione sia necessaria per realizzare la finalità legittima perseguita e che non sia sproporzionata alla luce di tale obiettivo". Cfr. Corte di giustizia, sentenza 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01, *Rundfunk*, e Corte di giustizia dell'Unione europea, sentenza 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke*.

<sup>58</sup> Il principio di limitazione delle finalità riveste parimenti grande importanza in questo caso. A pagina 21 del parere 6/2013 del Gruppo di lavoro sui dati aperti (citato di seguito nella nota a piè di pagina 88), il Gruppo di lavoro "articolo 29" raccomanda "che qualsiasi normativa che richieda l'accesso pubblico a una serie di dati specifici con chiarezza le finalità della diffusione di dati personali. Se ciò non avvenisse, o avvenisse solo in termini vaghi e generici, ne deriverebbe un pregiudizio per la certezza e la prevedibilità del diritto. In particolare, in merito a qualsiasi richiesta finalizzata al riutilizzo, sarebbe molto difficile per l'ente pubblico e i potenziali riutilizzatori interessati stabilire quali fossero gli scopi iniziali previsti della pubblicazione e, conseguentemente, quali altri scopi sarebbero compatibili con quelli iniziali. Come è già stato affermato, anche se vengono pubblicati dati personali su Internet, non è detto che tali dati possano essere ulteriormente trattati per ogni finalità possibile".

<sup>59</sup> Cfr., per esempio, l'articolo 6, paragrafo 1, lettere b) ed e).

<sup>60</sup> Come spiegato nel parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato nella precedente nota a piè di pagina 9), l'ulteriore utilizzo dei dati per finalità secondarie deve essere sottoposto a un duplice test. Innanzitutto, si dovrà garantire che i dati saranno utilizzati per finalità compatibili. In secondo luogo, occorrerà garantire che il trattamento si fondi su una base giuridica adeguata ai sensi dell'articolo 7.

*Interesse pubblico generale o interesse dei terzi.* Infine, anche l'interesse legittimo dei terzi potrebbe essere pertinente in una maniera differente. Questa circostanza si verifica quando un responsabile del trattamento, talvolta incoraggiato dalle autorità pubbliche, persegue un interesse che corrisponde a un interesse pubblico generale o a un interesse dei terzi. In quest'ambito possono rientrare i casi in cui un responsabile del trattamento va oltre gli obblighi giuridici specifici che è tenuto a rispettare conformemente a leggi e regolamenti al fine di contribuire all'impegno profuso dalle autorità di contrasto e dai soggetti privati per combattere le attività illegali, quali il riciclaggio di denaro, l'adescamento di minori o la condivisione illegale di file online. In queste situazioni, tuttavia, è particolarmente importante garantire che siano rispettati appieno i limiti dell'articolo 7, lettera f)<sup>61</sup>.

*Il trattamento deve essere necessario al conseguimento della/e finalità perseguita/e*

Infine, il trattamento dei dati personali deve anche essere "necessario per il perseguimento dell'interesse legittimo" del responsabile del trattamento o, nel caso della comunicazione dei dati, del/dei terzo/i. Questa condizione integra il requisito della necessità di cui all'articolo 6 e prevede un collegamento fra il trattamento e gli interessi perseguiti. Questo requisito della "necessità" si applica in tutte le situazioni indicate all'articolo 7, lettere da b) a f), ma è particolarmente pertinente nel caso della lettera f) per garantire che il trattamento dei dati basato sull'interesse legittimo non porti a un'interpretazione indebitamente ampia della necessità di trattare i dati. Come negli altri casi, questo significa che occorre valutare se esistono altri mezzi meno invasivi per conseguire lo stesso obiettivo.

### **III.3.2. Interesse o diritti dell'interessato**

*Interesse o diritti (anziché interesse per i diritti)*

La versione inglese della direttiva, all'articolo 7, lettera f), recita: "the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)".

Confrontando le differenti versioni linguistiche della direttiva, il Gruppo di lavoro ha tuttavia constatato che l'espressione "interests for" ("interesse per") è stata tradotta come "interests or" ("interesse o") in altre lingue fondamentali utilizzate all'epoca della negoziazione del testo<sup>62</sup>.

Da un'ulteriore analisi si evince che il testo inglese della direttiva è semplicemente il risultato di un errore di ortografia: anziché "or" ("o") era stato erroneamente digitato "for" ("per")<sup>63</sup>.

---

<sup>61</sup> A tale proposito cfr., per esempio, il documento di lavoro sulle questioni relative alla protezione dei dati per quanto riguarda i diritti di proprietà intellettuale, adottato il 18 gennaio 2005 (WP 104).

<sup>62</sup> Per esempio, "l'intérêt ou les droits et libertés fondamentaux de la personne concernée" in francese, "l'interesse o i diritti e le libertà fondamentali della persona interessata" in italiano, "das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person" in tedesco.

<sup>63</sup> Il Gruppo di lavoro osserva che nel testo della versione inglese grammaticalmente corretta sarebbe dovuta figurare l'espressione "interests in" ("interesse a") anziché "interests for" ("interesse per"), se il significato previsto era questo. Inoltre, l'espressione "interests for" ("interesse per") o "interest in" ("interesse a") sembra essere ridondante, innanzitutto perché di norma sarebbe dovuto essere sufficiente citare "i diritti e le libertà fondamentali", se il significato previsto era questo. L'interpretazione secondo cui è stato commesso un errore di ortografia è inoltre confermata dal fatto che anche nella posizione comune (CE) n. 1/95 definita dal Consiglio il

Di conseguenza, nel testo corretto dovrebbe figurare l'espressione "interests or fundamental rights and freedoms" ("l'interesse o i diritti e le libertà fondamentali").

*Necessità di interpretare estensivamente i concetti di "interesse" e "diritti"*

"L'interesse o i diritti e le libertà fondamentali" di cui all'articolo 7, lettera f), della direttiva hanno un impatto diretto sul campo di applicazione della disposizione. Tale riferimento garantisce una maggiore protezione dell'interessato; in particolare, stabilisce che si tengano in considerazione non solo i diritti e le libertà fondamentali dell'interessato, ma anche il suo "interesse". Ciononostante, non esistono elementi per ritenere che la restrizione di cui all'articolo 7, lettera f), ai diritti fondamentali "che richiedono tutela ai sensi dell'articolo 1, paragrafo 1", e di conseguenza l'espresso riferimento all'oggetto della direttiva<sup>64</sup>, non si applichi anche al termine "interesse". Il messaggio chiaro è comunque che devono essere tenuti in considerazione tutti i pertinenti interessi dell'interessato.

Questa interpretazione del testo ha senso non solo grammaticalmente, ma anche se si tiene conto dell'interpretazione estensiva del concetto di "interesse legittimo" del responsabile del trattamento. Se il responsabile del trattamento, o i terzi in caso di comunicazione dei dati, possono perseguire qualsiasi interesse purché legittimo, allora tutte le categorie di interessi dell'interessato devono essere prese in considerazione e valutate comparativamente rispetto a quelle del responsabile del trattamento, nella misura in cui siano pertinenti nell'ambito del campo di applicazione della direttiva.

In un'epoca in cui lo squilibrio del "potere informativo" è sempre maggiore, in cui governi e organizzazioni imprenditoriali in ugual misura ammassano quantità di dati senza precedenti e sono sempre più in grado di elaborare profili dettagliati che permetteranno di prevedere il comportamento delle persone (accentuando lo squilibrio informativo e riducendone l'autonomia), è sempre più importante garantire che sia tutelato l'interesse delle persone a preservare la loro vita privata e la loro autonomia.

Infine, è importante rilevare che, diversamente da quanto avviene nel caso dell'interesse del responsabile del trattamento, "l'interesse" dell'interessato non è seguito dall'aggettivo "legittimo". Di conseguenza, il campo di applicazione per la tutela dell'interesse e dei diritti delle persone è più ampio. Anche le persone dedite ad attività illegali non devono essere soggette a un'ingerenza sproporzionata nei loro diritti e interessi<sup>65</sup>. Per esempio, l'interesse di una persona che potrebbe aver commesso un furto in un supermercato potrebbe comunque prevalere rispetto alla pubblicazione della sua fotografia e del suo indirizzo privato sulle pareti del supermercato e/o su Internet da parte del proprietario dell'esercizio commerciale.

---

20 febbraio 1995 è contenuta l'espressione "interests or fundamental rights and freedoms" ("l'interesse o i diritti e le libertà fondamentali). Infine, il Gruppo di lavoro osserva anche che la Commissione intendeva correggere questo errore di ortografia nella proposta di regolamento; l'articolo 6, paragrafo 1, lettera f), infatti, recita: "the interests or fundamental rights and freedoms of the data subject which require protection of personal data" ("gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali) anziché "interests for" (interesse per tali diritti).

<sup>64</sup> Cfr. l'articolo 1, paragrafo 1, della direttiva, che recita: "Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali."

<sup>65</sup> Ovviamente, una delle conseguenze della criminalità potrebbe essere la raccolta e la possibile pubblicazione dei dati personali degli autori dei reati e dei sospetti. Tali provvedimenti devono però essere subordinati a rigorose condizioni e garanzie.

### III.3.3. Introduzione all'applicazione del test comparativo

È utile immaginare su uno spettro sia l'interesse legittimo del responsabile del trattamento che l'impatto sull'interesse e sui diritti dell'interessato. L'interesse legittimo può avere diversi gradi di rilevanza: da irrilevante a piuttosto importante fino a preminente. Analogamente, l'impatto sull'interesse e sui diritti degli interessati può essere più o meno rilevante e andare da poco importante a molto significativo.

L'interesse legittimo del responsabile del trattamento, quando è poco rilevante e scarsamente preminente può, in generale, prevalere rispetto all'interesse e ai diritti degli interessati solo nei casi in cui l'impatto su tali diritti e interessi è ancora più irrilevante. D'altro canto, un interesse legittimo importante e preminente può, in alcuni casi e fatte salve determinate garanzie e misure, giustificare anche una notevole ingerenza nella vita privata oppure un altro impatto considerevole sugli interessi o sui diritti degli interessati<sup>66</sup>.

A tale proposito è importante sottolineare il ruolo speciale che possono svolgere le garanzie<sup>67</sup> nella riduzione dell'indebito impatto sugli interessati, modificando in tal modo l'equilibrio tra i diritti e gli interessi in misura tale che l'interesse legittimo degli interessati non prevalga sull'interesse legittimo del responsabile del trattamento dei dati. Il solo utilizzo delle garanzie non è ovviamente sufficiente a giustificare qualsiasi tipo di trattamento in qualunque contesto. Inoltre, le garanzie in questione devono essere adeguate e sufficienti e devono indiscutibilmente e significativamente ridurre l'impatto sugli interessati.

#### *Scenari introduttivi*

Prima di passare a fornire orientamenti sulle modalità di svolgimento del test comparativo, i tre scenari introduttivi illustrati di seguito possono dare una prima indicazione di come potrebbero essere bilanciati interessi e diritti nella vita reale. Tutti e tre gli esempi si basano su un semplice e innocuo scenario che inizia con un'offerta speciale riguardante un cibo italiano da asporto. Gli esempi introducono gradualmente nuovi elementi che dimostrano come l'equilibrio si sbilancia man mano che aumenta l'impatto sugli interessati.

#### Scenario 1: offerta speciale da parte di una catena di pizza

Claudia ordina una pizza tramite un'applicazione mobile sul suo smartphone, ma non

<sup>66</sup> Cfr., a titolo illustrativo, le motivazioni fornite dal Gruppo di lavoro in alcuni pareri e documenti di lavoro:

- parere 4/2006 relativo alla Comunicazione di proposta di legge del Dipartimento della sanità e dei servizi umani degli Stati Uniti sul controllo delle malattie trasmissibili e sulla raccolta di informazioni sui passeggeri del 20 novembre 2005 (Controllo delle malattie trasmissibili - Proposta 42 CFR Parti 70-71), adottato il 14 giugno 2006 (WP 121), che esamina gravi minacce specifiche per la salute pubblica;
- parere 1/2006 relativo alle procedure interne per la denuncia delle irregolarità (citato precedentemente alla nota a piè di pagina 39), in cui la gravità di una presunta violazione è uno degli elementi del test comparativo;
- documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, adottato il 29 maggio 2002 (WP 55), che bilancia il diritto del datore di lavoro di gestire la sua azienda con una certa efficienza con la dignità umana del lavoratore nonché con il diritto alla segretezza della corrispondenza.

<sup>67</sup> Le garanzie possono comprendere, fra l'altro, rigorose limitazioni alla quantità di dati raccolti, l'immediata cancellazione dei dati dopo il loro utilizzo, misure tecniche e organizzative volte a garantire la separazione funzionale, l'adeguato utilizzo di tecniche di anonimizzazione, l'aggregazione dei dati nonché tecnologie di rafforzamento della tutela della vita privata, ma anche una maggiore trasparenza, responsabilità e la possibilità di revocare il proprio consenso al trattamento. Cfr. anche la sezione III.3.4 (d) e oltre.

disattiva l'opzione relativa all'invio di materiale pubblicitario sul sito web. Il suo indirizzo e i dati della carta di credito sono conservati ai fini della consegna. Alcuni giorni dopo Claudia riceve buoni sconto per prodotti simili nella buca delle lettere di casa sua.

Breve analisi: la catena di pizza ha un interesse legittimo, ma non particolarmente preminente, a cercare di vendere un maggior numero di prodotti ai suoi clienti. D'altro canto, non sembrano registrarsi una considerevole ingerenza nella vita privata di Claudia o un indebito impatto di altro tipo sui suoi interessi e diritti. I dati e il contesto sono relativamente innocui (il consumo di pizza). La catena di pizza ha istituito alcune garanzie: si utilizzano solo informazioni relativamente limitate (i recapiti) e l'invio dei buoni sconto avviene per posta tradizionale. Inoltre, è prevista un'opzione di facile utilizzo che permette di opporsi all'invio di materiale pubblicitario sul sito web.

Nel complesso, e considerando anche le garanzie e le misure previste (tra cui uno strumento di facile utilizzo per opporsi all'invio di materiale pubblicitario), l'interesse e i diritti dell'interessato non sembrano prevalere rispetto all'interesse legittimo della catena di pizza di effettuare questo minimo trattamento dei dati.

## Scenario 2: pubblicità mirata per la stessa offerta speciale

Il contesto è lo stesso, ma questa volta la catena di pizza non conserva solo l'indirizzo e i dati della carta di credito di Claudia, ma anche la sua cronologia degli ordini recenti (relativa agli ultimi tre anni). Inoltre, la cronologia degli acquisti è combinata con i dati del supermercato in cui Claudia effettua acquisti online, di cui è titolare la stessa società che gestisce la catena di pizza. La catena di pizza invia a Claudia offerte speciali e annunci pubblicitari mirati basati sulla sua cronologia degli ordini effettuati per i due differenti servizi. Claudia riceve i messaggi pubblicitari e le offerte speciali sia online che offline, per posta tradizionale e per posta elettronica nonché tramite inserzioni sul sito web della società e su quelli di una serie di partner selezionati (quando accede a tali siti sul suo computer o tramite il suo cellulare). Vengono inoltre tracciati la cronologia delle sue esplorazioni (sequenza di clic) e, tramite il suo cellulare, anche i dati relativi alla sua ubicazione. Un software analitico scorre i dati e predice le sue preferenze nonché gli orari e i luoghi in cui sarà più probabile che Claudia effettui acquisti maggiori, sia disponibile a pagare un prezzo più elevato nonché suscettibile di essere influenzata da una determinata percentuale di sconto o i momenti in cui desidera più intensamente i suoi dessert o i suoi piatti pronti preferiti<sup>68</sup>. Claudia è assolutamente infastidita dai messaggi che continuano a comparire sul suo cellulare quando controlla gli orari dell'autobus mentre torna a casa e che pubblicizzano le ultime offerte di cibo da asporto alle quali sta cercando di resistere. Non è riuscita a trovare informazioni di facile consultazione o un semplice modo per disattivare questi messaggi pubblicitari, nonostante la società sostenga che a livello settoriale esiste un sistema che consente di revocare il proprio consenso alla loro ricezione. Ha inoltre constatato con stupore che, dopo essersi trasferita in un quartiere meno benestante, non ha più ricevuto le offerte speciali a lei destinate. Di conseguenza, ha speso circa il 10% in più per la spesa alimentare mensile. Un amico più esperto di lei in ambito tecnologico le ha indicato alcuni pareri espressi su un blog online secondo cui il supermercato imponeva un prezzo superiore per gli ordini provenienti dai quartieri meno benestanti, sulla base del rischio statisticamente più elevato di utilizzo fraudolento di carte di credito nei casi in questione. La società non ha formulato osservazioni al riguardo e ha sostenuto che la politica aziendale in materia di sconti nonché l'algoritmo utilizzato per la fissazione dei prezzi sono esclusivi e non possono essere divulgati.

Breve analisi: la natura dei dati e del contesto rimane relativamente innocua. Tuttavia, la portata della raccolta dei dati e le tecniche utilizzate per influenzare Claudia (tra cui varie tecniche di tracciamento, la previsione degli orari e dei luoghi in cui la sua voglia di cibo sarà maggiore e il fatto che in tali orari Claudia è più soggetta a soccombere alla tentazione) sono fattori di cui tenere conto nel valutare l'impatto del trattamento. La mancanza di trasparenza riguardo alla logica sottesa al trattamento dei dati da parte della società, che può avere di fatto determinato una discriminazione dei prezzi sulla base del luogo in cui viene effettuato un ordine, e il considerevole impatto finanziario potenziale sui clienti sbilanciano in definitiva l'equilibrio anche nel contesto relativamente innocuo del cibo da asporto e dell'acquisto di generi alimentari. Anziché offrire semplicemente la possibilità di opporsi a questo tipo di elaborazione dei profili e di pubblicità mirata, sarebbe necessario un consenso informato, ai sensi sia dell'articolo 7, lettera a), che dell'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Di conseguenza, l'articolo 7, lettera f), non deve essere invocato come fondamento giuridico per il trattamento.

<sup>68</sup> Cfr., per esempio, <http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review->

### Scenario 3: utilizzo degli ordini di prodotti alimentari per adeguare i premi di assicurazione sanitaria

Le abitudini di consumo di pizza di Claudia, compresi gli orari e il carattere degli ordini di prodotti alimentari, sono vendute dalla catena a una società di assicurazioni che utilizza questi dati per adeguare i suoi premi di assicurazione sanitaria.

Breve analisi: la società di assicurazione sanitaria potrebbe avere un interesse legittimo, nella misura in cui i regolamenti applicabili lo consentano, a valutare i rischi per la salute dei suoi clienti e ad applicare premi differenziati a seconda dei vari rischi. Tuttavia, le modalità di raccolta dei dati e la portata della raccolta dei dati in sé sono eccessive. Se si fosse trovata nella situazione di Claudia, una persona ragionevole non si sarebbe probabilmente aspettata che le informazioni relative al suo consumo di pizza sarebbero state utilizzate per calcolare i suoi premi di assicurazione sanitaria.

Oltre al carattere eccessivo dell'attività di profilazione e alle possibili deduzioni sbagliate (la pizza potrebbe essere ordinata per qualcun altro), la deduzione di dati sensibili (dati sanitari) da dati apparentemente innocui (ordini di cibi da asporto) contribuisce a sbilanciare l'equilibrio a favore dell'interesse e dei diritti dell'interessato. Infine, il trattamento ha anche un considerevole impatto finanziario su Claudia.

Nel complesso, in questo caso specifico l'interesse e i diritti dell'interessato prevalgono rispetto all'interesse legittimo della società di assicurazione sanitaria. Di conseguenza, l'articolo 7, lettera f), non deve essere invocato come fondamento giuridico per il trattamento. È inoltre controverso se l'articolo 7, lettera a), possa essere utilizzato come fondamento giuridico, considerando l'eccessiva portata della raccolta dei dati ed eventualmente anche le ulteriori restrizioni specifiche previste dalla normativa nazionale.

Gli scenari precedenti e la possibile introduzione di variazioni con altri elementi evidenziano la necessità di un numero limitato di fattori chiave che possono contribuire a mirare la valutazione nonché la necessità di un approccio pragmatico che consenta di utilizzare ipotesi pratiche (“regole empiriche”) basate essenzialmente su ciò che una persona ragionevole troverebbe accettabile in determinate circostanze (“aspettative ragionevoli”) nonché sulle conseguenze dell'attività di trattamento dei dati per gli interessati (“impatto”).

#### **III.3.4. Fattori chiave da considerare nell'applicazione del test comparativo**

---

boards: *“Recent research suggests that willpower is a finite resource that can be depleted or replenished over time.[10] Imagine that concerns about obesity lead a consumer to try to hold out against her favourite junk food. It turns out there are times and places when she cannot. Big data can help marketers understand exactly how and when to approach this consumer at her most vulnerable—especially in a world of constant screen time in which even our appliances are capable of a sales pitch”* (“Da recenti ricerche emerge che la forza di volontà è una risorsa finita che può esaurirsi o ricostituirsi nel tempo[10]. Immaginate che la preoccupazione per l'obesità induca un consumatore a cercare di resistere al suo cibo spazzatura preferito. Di fatto ci sono volte e luoghi in cui è impossibile non cedere a tale tentazione. I megadati possono aiutare gli operatori di mercato a capire esattamente come e quando rivolgersi a questo consumatore nel momento in cui si trova in condizioni di massima vulnerabilità, specialmente in un mondo di costante esposizione al video in cui anche i nostri elettrodomestici sono in grado di promuovere la vendita di un determinato prodotto”).

Gli Stati membri hanno sviluppato una serie di fattori utili da considerare nell'esecuzione del test comparativo. Tali fattori sono discussi nella presente sezione nell'ambito delle quattro rubriche principali elencate di seguito: (a) valutazione dell'interesse legittimo del responsabile del trattamento, (b) impatto sugli interessati, (c) bilanciamento provvisorio e (d) garanzie supplementari applicate dal responsabile del trattamento per evitare qualsiasi indebito impatto sugli interessati<sup>69</sup>.

Per eseguire il test comparativo è innanzitutto importante considerare, da un lato, la natura e l'origine dell'interesse legittimo e, dall'altro, l'impatto sugli interessati. Questa valutazione deve già tenere conto delle misure che il responsabile del trattamento prevede di adottare per ottemperare alla direttiva (per esempio, garantire la limitazione delle finalità e la proporzionalità ai sensi dell'articolo 6 o fornire informazioni agli interessati ai sensi degli articoli 10 e 11).

Dopo aver analizzato e valutato comparativamente i due elementi, è possibile giungere a un "bilanciamento" provvisorio. Quando in seguito all'esito della valutazione permangono dubbi, il passo successivo consisterà nel valutare se, assicurando una maggiore protezione all'interessato, eventuali garanzie supplementari potrebbero far pendere il bilanciamento a favore della legittimazione del trattamento.

#### (a) Valutazione dell'interesse legittimo del responsabile del trattamento

Considerando che il concetto di interesse legittimo è piuttosto ampio, come spiegato nella precedente sezione III.3.1, la sua natura svolge un ruolo cruciale quando si tratta di bilanciare l'interesse del responsabile del trattamento e i diritti e gli interessi degli interessati. Benché sia impossibile formulare giudizi di valore riguardo a tutti gli interessi legittimi possibili, si possono fornire alcuni orientamenti. Come precedentemente indicato, tali interessi possono essere sia di scarso rilievo che preminenti nonché evidenti oppure più controversi.

##### i) Esercizio di un diritto fondamentale

Tra i diritti e le libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea (la "Carta")<sup>70</sup> e dalla Convenzione europea dei diritti dell'uomo (la "CEDU"), alcuni possono entrare in conflitto con il diritto alla tutela della vita privata e con il diritto alla protezione dei dati personali, quali la libertà di espressione e d'informazione<sup>71</sup>, la libertà delle arti e delle scienze<sup>72</sup>, il diritto d'accesso ai documenti<sup>73</sup> nonché, per esempio, il diritto alla libertà e alla sicurezza<sup>74</sup>, la libertà di pensiero, di coscienza e di religione<sup>75</sup>, la libertà

---

<sup>69</sup> Considerata la loro importanza, alcune questioni specifiche riguardanti le garanzie saranno ulteriormente discusse nell'ambito di rubriche separate nelle sezioni III.3.5 e III.3.6.

<sup>70</sup> Le disposizioni della Carta si applicano alle istituzioni e agli organi dell'Unione nel rispetto del principio di sussidiarietà, come pure alle autorità nazionali esclusivamente nell'attuazione del diritto dell'Unione.

<sup>71</sup> Articolo 11 della Carta e articolo 10 della CEDU.

<sup>72</sup> Articolo 13 della Carta e articoli 9 e 10 della CEDU.

<sup>73</sup> Articolo 42 della Carta. "Qualsiasi cittadino dell'Unione o qualsiasi persona fisica o giuridica che risieda o abbia la sede sociale in uno Stato membro ha il diritto di accedere ai documenti del Parlamento europeo, del Consiglio e della Commissione". In alcuni Stati membri esistono diritti d'accesso analoghi per quanto riguarda i documenti detenuti da organismi pubblici in tali Stati membri.

<sup>74</sup> Articolo 6 della Carta e articolo 5 della CEDU.

<sup>75</sup> Articolo 10 della Carta e articolo 9 della CEDU.

d'impresa<sup>76</sup>, il diritto di proprietà<sup>77</sup>, il diritto a un ricorso effettivo e a un giudice imparziale<sup>78</sup> o la presunzione di innocenza e diritti della difesa<sup>79</sup>.

Affinché prevalga l'interesse legittimo del responsabile del trattamento, il trattamento dei dati deve essere "necessario" e "proporzionato" al fine di esercitare il diritto fondamentale in questione.

A titolo illustrativo, a seconda delle circostanze del caso, per un giornale potrebbe essere necessario e proporzionato pubblicare determinate informazioni incriminanti sulle abitudini di spesa di un funzionario governativo di alto livello coinvolto in un presunto scandalo di corruzione. D'altro canto, non deve esistere un'autorizzazione generalizzata che permetta ai mezzi di comunicazione di pubblicare qualsiasi informazione irrilevante sulla vita privata di personalità pubbliche. Questi e altri casi analoghi danno generalmente luogo a complesse questioni di valutazione e, per contribuire a orientare la valutazione, una legislazione e una giurisprudenza specifiche, orientamenti mirati nonché codici di condotta e altre norme formali o meno formali potrebbero svolgere tutti un ruolo importante<sup>80</sup>.

Ove opportuno, anche in questo contesto le garanzie supplementari potrebbero svolgere un ruolo importante e contribuire a individuare le modalità secondo cui l'equilibrio degli interessi, talvolta fragile, deve essere raggiunto.

#### ii) Interesse pubblico/interesse della collettività

In alcuni casi il responsabile del trattamento potrebbe voler invocare l'interesse pubblico o l'interesse della collettività (a prescindere che ciò sia previsto o meno nelle normative o nei regolamenti nazionali). Per esempio, un ente di beneficenza o un'associazione senza scopo di lucro potrebbero trattare dati personali rispettivamente a fini di ricerca medica e di sensibilizzazione sulla corruzione governativa.

Può anche succedere che l'interesse imprenditoriale privato di un'azienda coincida in qualche misura con un interesse pubblico. Questa situazione potrebbe verificarsi, per esempio, nel caso della lotta alle frodi finanziarie o ad altri usi fraudolenti dei servizi<sup>81</sup>. Un fornitore di servizi può avere un interesse imprenditoriale legittimo a garantire che i suoi clienti non utilizzino il servizio in maniera impropria (o che non possano ottenere i servizi senza aver pagato per fruirne) e, al tempo stesso, i clienti dell'impresa, i contribuenti e il pubblico in

---

<sup>76</sup> Articolo 16 della Carta.

<sup>77</sup> Articolo 17 della Carta e articolo 1 del protocollo n.°1 della CEDU.

<sup>78</sup> Articolo 47 della Carta e articolo 6 della CEDU.

<sup>79</sup> Articolo 48 della Carta e articoli 6 e 13 della CEDU.

<sup>80</sup> Quanto ai criteri da applicare nei casi riguardanti la libertà di espressione, anche la giurisprudenza della Corte europea dei diritti dell'uomo fornisce indicazioni utili. Cfr., per esempio, Corte EDU, sentenza 7 febbraio 2012, *von Hannover c. Germania* (n. 2), in particolare i punti 95-126. Occorre inoltre tenere presente che l'articolo 9 della direttiva (intitolato *Trattamento di dati personali e libertà d'espressione*) permette agli Stati membri di prevedere "per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, le esenzioni o le deroghe [a talune disposizioni della direttiva]" qualora si rivelino "necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione".

<sup>81</sup> Cfr., a titolo illustrativo, "Esempio 21: Dati dei sistemi di misurazione intelligenti estrapolati per individuare un uso fraudolento dell'energia" a pagina 67 del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato precedentemente alla nota a piè di pagina 9).

generale hanno a loro volta un interesse legittimo a garantire che le attività fraudolente siano scoraggiate e individuate quando si verificano.

In generale, il fatto che un responsabile del trattamento agisca non solo nel proprio interesse legittimo (per esempio, nell'interesse dell'impresa), ma anche nell'interesse della collettività, può attribuire maggior "peso" a tale interesse. Quanto più preminenti saranno l'interesse pubblico o l'interesse della collettività e quanto più la collettività e gli interessati si aspetteranno e riconosceranno chiaramente che il responsabile del trattamento può intervenire e trattare i dati al fine di perseguire tali interessi, tanto maggiore sarà il peso di questo interesse legittimo nel bilanciamento.

D'altra parte, "l'applicazione delle norme su iniziativa dei privati" non deve essere utilizzata per legittimare pratiche invasive che, se fossero attuate da un'organizzazione governativa, sarebbero proibite ai sensi della giurisprudenza della Corte europea dei diritti dell'uomo in quanto le attività dell'autorità pubblica lederebbero il diritto al rispetto della vita privata degli interessati senza soddisfare il rigoroso criterio di cui all'articolo 8, paragrafo 2, della CEDU.

### iii) Altri interessi legittimi

In alcuni casi, come è già stato illustrato nella sezione III.2, il contesto in cui può aversi un interesse legittimo può essere simile a uno dei contesti in cui potrebbero essere applicati alcuni degli altri criteri di liceità del trattamento, in particolare i fondamenti giuridici di cui all'articolo 7, lettera b) (contratto), all'articolo 7, lettera c) (obbligo legale) o all'articolo 7, lettera e) (compito di interesse pubblico). Per esempio, un'attività di trattamento dei dati potrebbe non essere strettamente necessaria, ma potrebbe comunque essere pertinente per l'esecuzione di un contratto, oppure una legge potrebbe solo permettere, ma non prescrivere, il trattamento di taluni dati. Come abbiamo constatato, può non essere sempre semplice tracciare una netta linea di separazione tra i vari fondamenti, ma proprio per questo è ancora più importante inserire nell'analisi il test comparativo di cui all'articolo 7, lettera f).

Anche in questo caso, come in tutte le altre possibili situazioni non menzionate finora, quanto più preminente sarà l'interesse del responsabile del trattamento e quanto più la collettività si aspetterà e riconoscerà chiaramente che il responsabile del trattamento può intervenire e trattare i dati al fine di perseguire tale interesse, tanto maggiore sarà il peso di questo interesse legittimo nel bilanciamento<sup>82</sup>. Questa considerazione ci porta al punto seguente, di carattere più generale.

### iv) Riconoscimento giuridico e culturale/sociale della legittimità dell'interesse

In tutti i contesti precedenti, un aspetto indubbiamente pertinente è anche l'eventualità che la legislazione dell'UE o la normativa di uno Stato membro consentano espressamente (pur non prescrivendolo) ai responsabili del trattamento di adottare misure volte a perseguire l'interesse pubblico o privato in questione. L'esistenza di orientamenti non vincolanti, opportunamente adottati, emessi da organi autorevoli, per esempio da agenzie di regolamentazione, che incoraggiano i responsabili del trattamento a trattare i dati al fine di perseguire l'interesse in questione è a sua volta pertinente.

---

<sup>82</sup> Ovviamente, nella valutazione occorre anche riflettere sull'eventuale danno subito dal responsabile del trattamento, dai terzi o dalla collettività in caso di mancato trattamento dei dati.

Il rispetto di tutti gli orientamenti non vincolanti forniti dalle autorità di protezione dei dati o da altri organismi competenti riguardo alle modalità di trattamento dei dati contribuirà probabilmente a sua volta a una valutazione favorevole del bilanciamento degli interessi. Anche quando non trovano direttamente riscontro negli strumenti legislativi o normativi, le aspettative culturali e sociali potrebbero svolgere a loro volta un ruolo importante e contribuire a far pendere il bilanciamento in un senso o nell'altro.

Quanto più il fatto che i responsabili del trattamento possono intervenire e trattare i dati al fine di perseguire un particolare interesse sarà espressamente riconosciuto nel diritto, in altri strumenti normativi (siano essi vincolanti o meno per il responsabile del trattamento) o addirittura nella cultura di una determinata collettività in generale senza una specifica base giuridica, tanto maggiore sarà il peso di questo interesse legittimo nel bilanciamento<sup>83</sup>.

(b) Impatto sugli interessati

Esaminando l'altro elemento da valutare ai fini del test comparativo, l'impatto del trattamento sull'interesse o sui diritti e sulle libertà fondamentali dell'interessato è un criterio cruciale. La prima sottosezione riportata di seguito discute in termini generali come valutare l'impatto sull'interessato.

A tale proposito possono rivelarsi utili alcuni elementi che saranno analizzati in sottosezioni successive, tra cui la natura dei dati personali, le modalità di trattamento delle informazioni, le ragionevoli aspettative degli interessati nonché lo status del responsabile del trattamento e dell'interessato. Affronteremo inoltre brevemente le questioni connesse alle potenziali fonti di rischio che potrebbero avere un impatto sulle persone interessate, la gravità dell'eventuale impatto sulle persone interessate e la probabilità che tale impatto si concretizzi.

---

<sup>83</sup> Questo interesse, tuttavia, non può essere utilizzato per legittimare pratiche invasive che altrimenti non soddisferebbero il criterio di cui all'articolo 8, paragrafo 2, della CEDU.

## i) Valutazione dell'impatto

Nel valutare l'impatto<sup>84</sup> del trattamento, occorre considerare le conseguenze sia positive che negative. Queste possono comprendere potenziali azioni o decisioni future di terzi nonché situazioni in cui il trattamento potrebbe comportare l'esclusione o la discriminazione di persone, la diffamazione o, in senso più ampio, situazioni in cui esiste il rischio di danneggiare la reputazione, il potere negoziale o l'autonomia dell'interessato.

Oltre a esiti negativi che possono essere specificamente previsti, occorre tenere conto anche delle più ampie conseguenze emotive, quali l'irritazione, la paura e l'ansia che può provare un interessato che non abbia più il controllo dei suoi dati personali o che si sia reso conto che tali informazioni sono state o possono essere utilizzate in maniera impropria o compromesse, per esempio mediante l'esposizione su Internet. Occorre tenere nella debita considerazione anche l'effetto dissuasivo sui comportamenti protetti, quali la libertà di ricerca o la libertà di espressione, che potrebbe derivare da continue attività di monitoraggio/tracciamento.

Il Gruppo di lavoro sottolinea che è fondamentale capire che "l'impatto" pertinente è un concetto molto più ampio rispetto al nocumento o al danno che possono essere arrecati a uno o più interessati specifici. Il termine "impatto" quale utilizzato nel presente parere comprende tutte le possibili (potenziali o effettive) conseguenze del trattamento dei dati. A fini di chiarezza sottolineiamo inoltre che il concetto non è correlato alla nozione di violazione dei dati ed è molto più ampio rispetto alle conseguenze che potrebbero derivare da una violazione dei dati. Il concetto di impatto quale utilizzato nel presente parere, invece, contempla i vari modi in cui il trattamento dei dati personali potrebbe incidere, positivamente o negativamente, su un interessato<sup>85</sup>.

È inoltre importante comprendere che il più delle volte una serie di fatti correlati e non correlati può determinare cumulativamente l'impatto negativo sull'interessato e potrebbe essere difficile individuare l'attività di trattamento mediante la quale il responsabile del trattamento ha svolto un ruolo fondamentale nell'impatto negativo.

Considerando che spesso in questo contesto per gli interessati è difficile avviare una procedura di risarcimento per il nocumento o il danno subito, anche quando l'effetto in sé è molto concreto, è ancora più importante concentrarsi sulla prevenzione e garantire che le

---

<sup>84</sup> Questa valutazione dell'impatto deve essere interpretata nel contesto dell'articolo 7, lettera f). In altre parole, non facciamo riferimento a una "analisi dei rischi" o a una "valutazione d'impatto sulla protezione dei dati" nel senso della proposta di regolamento (articoli 33 e 34) e dei vari emendamenti formulati al riguardo dalla commissione LIBE. La questione di quale metodologia debba essere seguita nell'ambito di una "analisi dei rischi" o di una "valutazione d'impatto sulla protezione dei dati" esula dall'ambito di applicazione del presente parere. D'altro canto, occorre tenere presente che, in un modo o nell'altro, l'analisi dell'impatto ai sensi dell'articolo 7, lettera f), può essere una parte importante di qualsiasi "valutazione dei rischi" o "valutazione d'impatto sulla protezione dei dati" e può inoltre contribuire a individuare le situazioni in cui è necessario consultare l'autorità di protezione dei dati.

<sup>85</sup> Occorre sempre tenere nella debita considerazione il rischio di danno finanziario, per esempio, qualora in seguito a una violazione di dati siano divulgate informazioni che dovevano trovarsi in un ambiente sicuro e ciò comporti in definitiva un furto d'identità o altre forme di frode o il rischio di lesioni personali, dolore, sofferenza e un peggioramento della qualità della vita che potrebbero infine scaturire, per esempio, da un'alterazione non autorizzata dei dati medici e dal successivo trattamento inadeguato di un paziente, sebbene tale rischio sia tutt'altro che limitato alle situazioni che rientrano nel campo di applicazione dell'articolo 7, lettera f). Al contempo, tali rischi non sono gli unici di cui tenere conto nel valutare l'impatto ai sensi dell'articolo 7, lettera f).

attività di trattamento dei dati possano essere svolte solo a patto che non comportino rischi o comportino un rischio molto basso di indebito impatto negativo sull'interesse o sui diritti e sulle libertà fondamentali degli interessati.

Nella valutazione dell'impatto potrebbero risultare in certa misura utili la terminologia e la metodologia utilizzate nella tradizionale valutazione dei rischi e pertanto alcuni elementi di tale metodologia saranno brevemente descritti di seguito. Tuttavia, una metodologia globale per la valutazione dell'impatto, nel contesto dell'articolo 7, lettera f), o in un ambito più ampio, esulerebbe dal campo di applicazione del presente parere.

In questo come in altri contesti è importante individuare le fonti del potenziale impatto sugli interessati.

La probabilità che un rischio possa concretizzarsi è uno degli elementi da tenere in considerazione. Per esempio, l'accesso a Internet, gli scambi di dati con siti al di fuori dell'UE, le interconnessioni con altri sistemi e un elevato livello di eterogeneità o variabilità del sistema possono rappresentare vulnerabilità che potrebbero essere sfruttate dagli hacker. Questa fonte di rischio comporta una probabilità relativamente elevata che si materializzi il rischio di compromissione dei dati. Viceversa, un sistema omogeneo, stabile, privo di interconnessioni e disconnesso da Internet comporta una probabilità decisamente inferiore di compromissione dei dati.

Un altro elemento della valutazione dei rischi è la gravità delle conseguenze di un rischio divenuto realtà. I livelli di questa gravità possono variare, andando da bassi (quali la fastidiosa necessità di inserire nuovamente i recapiti personali smarriti dal responsabile del trattamento) a molto elevati (come la perdita della vita quando i modelli di localizzazione personale di persone protette finiscono nelle mani di criminali o quando la fornitura energetica è interrotta da remoto tramite contatori intelligenti in condizioni meteorologiche o di salute personale critiche).

Questi due elementi fondamentali (la probabilità che il rischio si concretizzi, da una parte, e la gravità delle conseguenze, dall'altra) contribuiscono entrambi alla valutazione globale dell'impatto potenziale.

Infine, nell'applicare la metodologia è opportuno ricordare che la valutazione dell'impatto ai sensi dell'articolo 7, lettera f), non può dare luogo a un esercizio meccanico e puramente quantitativo. Negli scenari tradizionali di valutazione dei rischi, la "gravità" può tenere conto del numero di persone su cui il trattamento può potenzialmente avere un impatto. Ciononostante, occorre tenere presente che il trattamento di dati personali che ha un impatto su una minoranza di interessati (o anche solo su una singola persona) richiede nondimeno un'analisi molto accurata specialmente se tale impatto su ciascuna persona interessata è potenzialmente significativo.

#### ii) Natura dei dati

Sarebbe innanzitutto importante valutare se il trattamento riguarda dati sensibili, o perché appartengono alle categorie particolari di dati di cui all'articolo 8 della direttiva, o per altri motivi, come nel caso dei dati biometrici, delle informazioni genetiche, dei dati sulle

comunicazioni, dei dati relativi all'ubicazione e di altri tipi di informazioni personali che richiedono una protezione speciale<sup>86</sup>.

A titolo di esempio, a parere del Gruppo di lavoro, di norma l'utilizzo di dati biometrici per i requisiti generali di sicurezza di immobili o persone è considerato un interesse legittimo su cui prevarrebbero l'interesse o i diritti e le libertà fondamentali dell'interessato. D'altro canto, dati biometrici quali le impronte digitali e/o la scansione dell'iride potrebbero essere utilizzati per la sicurezza di un'area ad alto rischio come un laboratorio che effettua ricerche su virus pericolosi, a patto che il responsabile del trattamento abbia fornito prove concrete dell'esistenza di un rischio considerevole<sup>87</sup>.

In generale, quanto più saranno sensibili i dati in questione, tanto più numerose potrebbero essere le conseguenze per l'interessato. Ciononostante, questo non significa che i dati che in sé e per sé potrebbero sembrare innocui possano essere trattati liberamente sulla base dell'articolo 7, lettera f). Anzi, anche quei dati, a seconda del modo in cui sono trattati, possono avere un impatto considerevole sulle persone, come sarà illustrato nella successiva sottosezione (iii).

A tale proposito, potrebbe essere pertinente che i dati siano già stati resi accessibili al pubblico o meno dall'interessato o da terzi. In questo caso è innanzitutto importante sottolineare che, anche se sono stati resi accessibili al pubblico, i dati personali continuano a essere considerati tali e, di conseguenza, per il loro trattamento continuano a essere necessarie garanzie adeguate<sup>88</sup>. Non esiste un'autorizzazione generalizzata a riutilizzare e a sottoporre a ulteriore trattamento dati personali resi accessibili al pubblico ai sensi dell'articolo 7, lettera f).

Detto questo, il fatto che i dati personali siano accessibili al pubblico potrebbe essere considerato come un elemento di valutazione, specialmente se la pubblicazione è stata effettuata senza una ragionevole aspettativa in merito all'ulteriore utilizzo dei dati per determinate finalità (per esempio, a scopi di ricerca o a fini di trasparenza e responsabilità).

### iii) Modalità di trattamento dei dati

Per valutare l'impatto in senso più ampio potrebbe essere necessario esaminare se i dati sono resi pubblici o altrimenti resi accessibili a un ampio numero di persone o se grandi quantità di dati personali sono trattate o combinate con altri dati (per esempio, nel caso dell'elaborazione

---

<sup>86</sup> I dati biometrici e i dati genetici sono considerati categorie particolari di dati nella proposta di regolamento sulla protezione dei dati della Commissione, in combinato disposto con gli emendamenti della commissione LIBE. Cfr. l'emendamento 103 all'articolo 9 nella relazione finale della commissione LIBE. Per quanto riguarda la relazione tra gli articoli 7 e 8 della direttiva 95/46/CE, cfr. la precedente sezione III.1.2 alle pagine 17-19.

<sup>87</sup> Cfr. il parere 3/2012 del Gruppo di lavoro "articolo 29" sugli sviluppi nelle tecnologie biometriche (WP 193). A titolo di ulteriore esempio, nel suo parere 4/2009 concernente lo standard internazionale dell'Agenzia Mondiale Antidoping (WADA) (citato precedentemente alla nota a piè di pagina 32), il Gruppo di lavoro ha sottolineato che l'articolo 7, lettera f), non sarebbe un motivo valido per trattare i dati medici e i dati relativi alle infrazioni nel contesto di indagini antidoping, alla luce della "gravità delle intrusioni nella vita privata". Il trattamento dei dati deve essere previsto dalla legge e soddisfare i requisiti di cui all'articolo 8, paragrafi 4 o 5, della direttiva.

<sup>88</sup> Cfr. il parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato alla precedente nota a piè di pagina 9) e il parere 6/2013 del Gruppo di lavoro sui dati aperti e sul riutilizzo delle informazioni del settore pubblico ("ISP"), adottato il 5 giugno 2013 (WP 207).

di profili, a fini commerciali, a fini di contrasto o per altri scopi). Dati apparentemente innocui, se trattati su vasta scala e combinati con altri dati, potrebbero dare luogo a deduzioni su dati più sensibili, come è stato dimostrato precedentemente nello scenario 3, che illustra la relazione tra modelli di consumo di pizza e premi di assicurazione sanitaria.

Oltre a poter comportare il trattamento di dati più sensibili, tale analisi potrebbe anche dare luogo a strane, imprevedute e talvolta anche errate previsioni, per esempio riguardo al comportamento o alla personalità delle persone interessate. A seconda della loro natura e dell'impatto che possono avere, queste previsioni potrebbero essere estremamente invasive per la vita privata dell'interessato<sup>89</sup>.

Il Gruppo di lavoro ha inoltre evidenziato in un precedente parere i rischi comportati da talune soluzioni a tutela della sicurezza (tra cui firewall, programmi antivirus o antispyware), poiché potrebbero dare luogo a un uso esteso di dispositivi di filtraggio DPI, che sarebbero in grado di influire significativamente sulla valutazione del bilanciamento dei diritti<sup>90</sup>.

In generale, quanto più negativo o incerto potrà essere l'impatto del trattamento, tanto più sarà improbabile che, nel complesso, il trattamento sia considerato legittimo. La disponibilità di metodi alternativi per raggiungere gli obiettivi perseguiti dal responsabile del trattamento, con un impatto meno negativo per l'interessato, dovrà sicuramente essere una considerazione importante in quest'ambito. Ove opportuno, è possibile utilizzare valutazioni di impatto sulla tutela della vita privata e sulla protezione dei dati per stabilire se questa sia una possibilità.

#### iv) Ragionevoli aspettative dell'interessato

Le ragionevoli aspettative dell'interessato riguardo all'utilizzo e alla comunicazione dei dati sono anch'esse estremamente pertinenti a questo riguardo. Come è stato evidenziato anche in merito all'analisi del principio di limitazione delle finalità<sup>91</sup>, è "importante valutare se lo status del responsabile del trattamento<sup>92</sup>, la natura della relazione o il servizio fornito<sup>93</sup> o gli obblighi giuridici o contrattuali applicabili (o altre promesse formulate al momento della raccolta dei dati) potrebbero dare luogo a ragionevoli aspettative riguardo a una riservatezza più rigorosa e a limitazioni più severe in merito all'ulteriore utilizzo. In generale, quanto più specifico e restrittivo sarà il contesto in cui si effettua la raccolta dei dati, tanto più numerose saranno probabilmente le limitazioni di utilizzo. Anche in questo caso è necessario tenere conto del contesto fattuale anziché fare semplice affidamento al testo in minuscolo.

#### v) Status del responsabile del trattamento dei dati e dell'interessato

---

<sup>89</sup> Cfr. la sezione III.2.5 e l'allegato 2 (Megadati e dati aperti) del parere sul principio di limitazione delle finalità (citato precedentemente alla nota a piè di pagina 9).

<sup>90</sup> Cfr. la sezione 3.1 del parere 1/2009 del Gruppo di lavoro sulle proposte recanti modifica della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (WP 159).

<sup>91</sup> Cfr. pagg. 24-25 del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato precedentemente alla nota a piè di pagina 9).

<sup>92</sup> "Quale, per esempio, un avvocato o un medico".

<sup>93</sup> "Quali, per esempio, servizi di cloud computing per la gestione di documenti personali, servizi di posta elettronica, agende, e-reader dotati di funzioni che consentono di scrivere annotazioni e varie applicazioni che permettono di registrare ogni momento della propria vita (life-logging) che potrebbero contenere informazioni molto personali".

Anche lo status dell'interessato e del responsabile del trattamento è un elemento pertinente ai fini della valutazione dell'impatto del trattamento. A seconda che il responsabile del trattamento sia una persona o un'organizzazione di piccole dimensioni, una grande impresa multinazionale o un ente pubblico e in base alle circostanze specifiche, la sua posizione potrebbe essere più o meno dominante rispetto all'interessato. Una grande impresa multinazionale, per esempio, potrebbe avere più risorse e un potere negoziale maggiore rispetto al singolo interessato e, di conseguenza, potrebbe trovarsi in una posizione migliore per imporre all'interessato ciò che ritiene sia nel suo "interesse legittimo", tanto più se l'impresa detiene una posizione dominante sul mercato. L'eventuale assenza di controlli al riguardo potrebbe andare a discapito dei singoli interessati. Così come le norme in materia di tutela dei consumatori e di concorrenza contribuiscono ad assicurare che tale potere non sia utilizzato in maniera impropria, la legislazione sulla protezione dei dati potrebbe svolgere a sua volta un ruolo importante nel garantire che i diritti e gli interessi degli interessati non siano indebitamente pregiudicati.

D'altro canto, anche lo status dell'interessato è pertinente. Benché in linea di principio il test comparativo debba essere effettuato prendendo in considerazione un individuo medio, situazioni specifiche devono comportare l'adozione di un approccio basato maggiormente su una valutazione caso per caso: per esempio, potrà essere pertinente esaminare se l'interessato è un minore<sup>94</sup> o, in caso contrario, se appartiene a una categoria più vulnerabile della popolazione che richiede una protezione speciale, come per esempio le persone affette da malattie mentali, i richiedenti asilo o gli anziani. Deve essere indubbiamente pertinente anche esaminare se l'interessato è un lavoratore dipendente, uno studente, un paziente o se esiste altrimenti uno squilibrio nella relazione tra la posizione dell'interessato e quella del responsabile del trattamento. È importante valutare l'impatto dell'effettivo trattamento su determinati individui.

Infine, è importante sottolineare che non tutto l'impatto negativo sugli interessati "pesa" allo stesso modo sul bilanciamento. Il test comparativo di cui all'articolo 7, lettera f), non è finalizzato a evitare qualsiasi impatto negativo sull'interessato. Il suo scopo è invece evitare un impatto sproporzionato. Questa è una differenza fondamentale. Per esempio, la pubblicazione di un articolo di giornale accurato e fondato su ricerche esaurienti sulla presunta corruzione governativa potrebbe danneggiare la reputazione dei funzionari di governo coinvolti e avere conseguenze considerevoli, tra cui la perdita di reputazione, la perdita delle elezioni o la reclusione; ciononostante, potrebbe comunque trovare un fondamento nell'articolo 7, lettera f)<sup>95</sup>.

### (c) Bilanciamento provvisorio

Quando si valutano comparativamente gli interessi e i diritti in gioco come precedentemente descritto, le misure adottate dal responsabile del trattamento per assolvere gli obblighi generali che è tenuto a rispettare ai sensi della direttiva, anche in termini di proporzionalità e trasparenza, contribuiranno in ampia misura a garantire che il responsabile del trattamento dei

---

<sup>94</sup> Cfr. il parere 2/2009 del Gruppo di lavoro sulla protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole), adottato l'11 febbraio 2009 (WP 160). Tale parere insiste sulla specifica vulnerabilità del minore e, qualora il minore si faccia rappresentare, sulla necessità di tenere conto dell'interesse superiore del minore e non di quello del suo rappresentante.

<sup>95</sup> Come precedentemente spiegato, occorre tenere conto anche di tutte le deroghe pertinenti per il trattamento di dati personali effettuato a scopi giornalistici ai sensi dell'articolo 9 della direttiva.

dati ottemperi ai requisiti di cui all'articolo 7, lettera f). Per “pieno rispetto” si deve intendere che l'impatto sulle persone è ridotto, che esistono *meno probabilità* di ingerenze negli interessi o nei diritti e nelle libertà fondamentali degli interessati e che di conseguenza è *più probabile* che il responsabile del trattamento possa invocare l'articolo 7, lettera f). Ciò dovrebbe incoraggiare i responsabili del trattamento a impegnarsi maggiormente per rispettare tutte le disposizioni orizzontali della direttiva<sup>96</sup>.

Tuttavia, ciò non significa che il rispetto di questi requisiti orizzontali sarà in quanto tale sempre sufficiente a garantire una base giuridica fondata sull'articolo 7, lettera f). Anzi, se così fosse, l'articolo 7, lettera f), sarebbe superfluo o diventerebbe una scappatoia che priverebbe di significato l'intero articolo 7, che richiede una specifica base giuridica adeguata per il trattamento.

Per questo motivo è importante svolgere un'ulteriore valutazione nell'ambito del test comparativo nei casi in cui, sulla base dell'analisi preliminare, non è chiaro in quale modo deve essere operato il bilanciamento. Il responsabile del trattamento potrebbe valutare la possibilità di introdurre misure supplementari, che vadano oltre il rispetto delle disposizioni orizzontali della direttiva, per contribuire a ridurre l'indebito impatto del trattamento sugli interessati.

Tra le misure supplementari potrebbe figurare, per esempio, la disponibilità di un meccanismo facilmente accessibile ed efficace volto ad assicurare agli interessati la possibilità incondizionata di revocare il proprio consenso al trattamento dei dati. In alcuni casi (ma non in tutti) queste misure supplementari potrebbero contribuire a far pendere il bilanciamento in un senso o nell'altro e a garantire che il trattamento possa basarsi sull'articolo 7, lettera f), tutelando al contempo anche i diritti e gli interessi degli interessati.

#### (d) Garanzie supplementari applicate dal responsabile del trattamento

Come precedentemente spiegato, il modo in cui il responsabile del trattamento applicherà le misure adeguate potrebbe, in alcune situazioni, contribuire a “far pendere il bilanciamento in un senso o nell'altro”. L'accettabilità del risultato dipenderà dalla valutazione nel suo complesso. Quanto più sarà rilevante l'impatto sull'interessato, tanto maggiore dovrà essere l'attenzione da riservare alle garanzie pertinenti.

Tra gli esempi delle misure pertinenti potrebbero figurare, tra l'altro, una rigorosa limitazione della quantità di dati raccolti e l'immediata cancellazione dei dati dopo il loro utilizzo. Alcune di queste misure potrebbero essere già obbligatorie ai sensi della direttiva; ciononostante, spesso sono adattabili e lasciano ai responsabili del trattamento la flessibilità necessaria a garantire una migliore protezione degli interessati. Per esempio, il responsabile del trattamento potrebbe raccogliere meno dati o fornire informazioni supplementari rispetto a quelle espressamente elencate agli articoli 10 e 11 della direttiva.

---

<sup>96</sup> Per quanto riguarda l'importante ruolo svolto dalla “conformità orizzontale”, cfr. anche pagina 54 del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità, citato nella precedente nota a piè di pagina 9.

In alcuni altri casi, le garanzie non sono *espressamente* prescritte a norma della direttiva, ma potrebbero esserlo in futuro ai sensi della proposta di regolamento, oppure sono prescritte solo in situazioni specifiche, quali:

- misure tecniche e organizzative volte a garantire che i dati non possano essere utilizzati per adottare decisioni o intraprendere altre azioni riguardo alle persone (“separazione funzionale” come spesso avviene in un contesto di ricerca)
- utilizzo estensivo di tecniche di anonimizzazione
- aggregazione dei dati
- tecnologie di rafforzamento della tutela della vita privata, tutela della vita privata fin dalla progettazione (“privacy by design”) nonché valutazioni di impatto sulla tutela della vita privata e sulla protezione dei dati
- maggiore trasparenza
- diritto generale e incondizionato di revoca (“opt-out”)
- portabilità dei dati e misure correlate volte a responsabilizzare gli interessati

Il Gruppo di lavoro osserva che, per quanto riguarda alcune questioni fondamentali, quali la separazione funzionale e le tecniche di anonimizzazione, sono già stati forniti alcuni orientamenti nelle pertinenti parti dei suoi pareri sul principio di limitazione delle finalità, sui dati aperti e sulle tecniche di anonimizzazione<sup>97</sup>.

Per quanto riguarda la pseudonimizzazione e la cifratura, il Gruppo di lavoro desidera sottolineare che, se i dati non sono direttamente identificabili, di per sé ciò non influisce sulla valutazione della legittimità del trattamento: non si deve interpretare tale circostanza nel senso che renda legittimo un trattamento illegittimo<sup>98</sup>.

Al tempo stesso, la pseudonimizzazione e la cifratura, analogamente a qualsiasi altra misura tecnica e organizzativa introdotta a tutela dei dati personali, svolgeranno un ruolo importante riguardo alla valutazione del potenziale impatto del trattamento sull’interessato e, di conseguenza, in alcuni casi potrebbero contribuire a far pendere il bilanciamento a favore del responsabile del trattamento. L’utilizzo di forme meno rischiose di trattamento dei dati personali (quali ad esempio la cifratura di dati personali in fase di conservazione o di transito oppure dati personali che sono meno direttamente e meno immediatamente identificabili) deve in generale significare che esistono minori probabilità di ingerenze negli interessi o nei diritti e nelle libertà fondamentali degli interessati.

Relativamente a tali garanzie, nonché alla valutazione comparativa generale del bilanciamento degli interessi, il Gruppo di lavoro desidera evidenziare tre questioni specifiche che spesso svolgono un ruolo fondamentale nel contesto dell’articolo 7, lettera f):

---

<sup>97</sup> Cfr. le sezioni III.2.3, III.2.5 e l’allegato 2 del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità, citato precedentemente alla nota a piè di pagina 9, sul trattamento successivo dei dati per scopi storici, statistici o scientifici, sui megadati e sui dati aperti; cfr. anche le parti pertinenti del parere 6/2013 del Gruppo di lavoro sui dati aperti (citato precedentemente alla nota a piè di pagina 88) e il parere 5/2014 sulle tecniche di anonimizzazione.

<sup>98</sup> Cfr. a tale proposito gli emendamenti votati dalla commissione LIBE nella sua relazione finale e in particolare l’emendamento 15 al considerando 38 in cui la pseudonimizzazione è associata alle legittime aspettative dell’interessato.

- la relazione tra il test comparativo, la trasparenza e il principio di responsabilità;
- il diritto dell'interessato a opporsi al trattamento e, oltre al diritto di opposizione, la possibilità di revocare il consenso al trattamento dei dati senza la necessità di fornire alcuna giustificazione, e
- la responsabilizzazione degli interessati: la portabilità dei dati e la disponibilità di meccanismi efficaci volti a permettere all'interessato di accedere ai suoi dati, modificarli, cancellarli, trasferirli o sottoporli altrimenti a un trattamento successivo (o permetterne l'ulteriore trattamento da parte di terzi).

Considerata la loro importanza, questi argomenti saranno trattati nell'ambito di rubriche distinte.

### **III.3.5. Responsabilità e trasparenza**

Innanzitutto, prima di effettuare un'operazione di trattamento sulla base dell'articolo 7, lettera f), il responsabile del trattamento ha la responsabilità di valutare se ha un interesse legittimo, se il trattamento è necessario per il perseguimento di quell'interesse legittimo e se nel caso specifico gli interessi e i diritti degli interessati prevalgono su detto interesse.

In tal senso, l'articolo 7, lettera f), si basa sul principio di responsabilità. Il responsabile del trattamento deve preventivamente eseguire un test meticoloso ed effettivo, basato sulle specifiche circostanze del caso, anziché operare in maniera astratta, tenendo altresì conto delle ragionevoli aspettative degli interessati. Come norma di buona pratica, ove opportuno, l'esecuzione di questo test deve essere documentata in maniera sufficientemente dettagliata e trasparente da permettere di verificare la completa e corretta applicazione del test, se del caso, da parte dei soggetti pertinenti, tra cui gli interessati e le autorità di protezione dei dati nonché, in ultima analisi, dei tribunali competenti.

Il responsabile del trattamento definirà innanzitutto l'interesse legittimo ed eseguirà il test comparativo, ma questa non sarà necessariamente la valutazione finale e definitiva: se, di fatto, l'interesse perseguito non è quello che era stato specificato dal responsabile del trattamento o se il responsabile del trattamento ha fornito solo una definizione scarsamente dettagliata dell'interesse, sarà necessario valutare nuovamente il bilanciamento, sulla base dell'interesse effettivo, che deve essere determinato o da un'autorità di protezione dei dati o da un tribunale<sup>99</sup>. Come nel caso di altri aspetti fondamentali della protezione dei dati, quali l'identificazione del responsabile del trattamento o la specificazione delle finalità<sup>100</sup>, ciò che conta è la realtà che si cela dietro qualsivoglia dichiarazione formulata dal responsabile del trattamento.

Il concetto di responsabilità è strettamente connesso al concetto di trasparenza. Per consentire agli interessati di esercitare i loro diritti e permettere un più ampio controllo pubblico da parte dei soggetti pertinenti, il Gruppo di lavoro raccomanda ai responsabili del trattamento di spiegare agli interessati, in maniera chiara e semplice, i motivi per cui ritengono che gli interessi o i diritti e le libertà fondamentali degli interessati non prevalgano sui loro interessi,

<sup>99</sup> Per esempio, in seguito a un ricorso o all'esercizio del diritto di opposizione ai sensi dell'articolo 14.

<sup>100</sup> Cfr. i pareri citati nella nota a piè di pagina 9.

illustrando altresì loro quali garanzie hanno adottato per tutelare i dati personali, compreso, se del caso, il diritto a revocare il proprio consenso al trattamento<sup>101</sup>.

A tale proposito il Gruppo di lavoro sottolinea che la normativa in materia di tutela dei consumatori, in particolare le norme che proteggono i consumatori da pratiche commerciali sleali, è a sua volta estremamente pertinente in questo caso.

Se un responsabile del trattamento occulta informazioni importanti in merito a un non previsto ulteriore utilizzo dei dati in termini legalistici nascosto nei caratteri minuscoli di un contratto, questo comportamento potrebbe costituire una violazione delle norme in materia di tutela dei consumatori riguardanti le clausole contrattuali abusive (compreso il divieto di utilizzare “clausole a sorpresa”) e inoltre non rispetterà i requisiti di cui all’articolo 7, lettera a), di un consenso valido e informato o i requisiti di cui all’articolo 7, lettera f), in termini di ragionevoli aspettative dell’interessato e di un bilanciamento degli interessi complessivamente accettabile. Solleverebbe ovviamente anche questioni di conformità con l’articolo 6 relativamente alla necessità di un trattamento leale e lecito dei dati personali.

In alcuni casi, per esempio, gli utenti di servizi “gratuiti” online, quali motori di ricerca, posta elettronica, mezzi di comunicazione sociale, archiviazione di documenti o altre applicazioni online o mobili, non sono pienamente consapevoli della misura in cui le loro attività sono registrate e analizzate al fine di generare valore per il fornitore di servizi e pertanto non si preoccupano dei rischi connessi.

Al fine di responsabilizzare gli interessati in queste situazioni, una prima condizione preliminare<sup>102</sup>, necessaria ma tutt’altro che sufficiente di per sé, è chiarire che i servizi non sono gratuiti e che, invece, i consumatori pagano utilizzando i loro dati personali. Le condizioni e le garanzie subordinatamente alle quali potrebbero essere utilizzati i dati devono a loro volta essere indicate chiaramente in ogni caso al fine di garantire la validità del consenso di cui all’articolo 7, lettera a), oppure un bilanciamento favorevole ai sensi dell’articolo 7, lettera f).

### **III.3.6. Il diritto di opposizione e oltre**

#### *(a) Il diritto di opposizione ai sensi dell’articolo 14 della direttiva*

L’articolo 7, lettera e), e l’articolo 7, lettera f), sono particolari nel senso che, pur basandosi essenzialmente su una valutazione oggettiva degli interessi e dei diritti in questione, permettono al contempo all’autodeterminazione dell’interessato di entrare in gioco con un

---

<sup>101</sup> Come spiegato a pagina 46 del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato precedentemente alla nota a piè di pagina 9), nel caso dell’elaborazione di profili e di processi decisionali automatizzati, “per garantire la trasparenza, gli interessati/i consumatori devono poter accedere ai loro ‘profili’ nonché alla logica sottesa al processo decisionale (algoritmo) che ha portato allo sviluppo del profilo. In altre parole, le organizzazioni devono rendere noti i loro criteri decisionali. Questa è una garanzia fondamentale, che riveste un’importanza ancora maggiore nel mondo dei megadati”. L’eventualità che un’organizzazione offra o meno questa trasparenza è un fattore estremamente importante da tenere parimenti in considerazione nel test comparativo.

<sup>102</sup> Per le ulteriori possibili garanzie riguardo alle situazioni sempre più comuni in cui i consumatori pagano con i loro dati personali, cfr. la sezione III.3.6, in particolare le pagine 55-57 sulle “Alternative ai servizi online ‘gratuiti’ compatibili con la protezione dei dati” e sulla “Portabilità dei dati, ‘Midata’ e questioni correlate”.

diritto di opposizione<sup>103</sup>: almeno nel caso di questi due fondamenti giuridici, l'articolo 14, lettera a), della direttiva stabilisce che ("salvo disposizione contraria prevista dalla normativa nazionale") la persona interessata può "opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano". Aggiunge che, se l'opposizione è giustificata, il trattamento non può più riguardare tali dati.

In linea di principio, a norma della legislazione in vigore, l'interessato dovrà pertanto dimostrare "interessi preminenti e legittimi" per interrompere il trattamento dei suoi dati personali (articolo 14, lettera a)), fuorché nel contesto delle attività di invio di materiale pubblicitario, in cui non è necessario giustificare l'opposizione (articolo 14, lettera b)).

Ciò non deve essere considerato in contraddizione con il test comparativo di cui all'articolo 7, lettera f), che è effettuato a priori: si tratta piuttosto di un'integrazione del bilanciamento, nel senso che, laddove il trattamento possa essere effettuato in seguito a una ragionevole e oggettiva valutazione dei differenti diritti e interessi in gioco, l'interessato ha comunque la possibilità *supplementare* di opporsi per motivi derivanti dalla sua situazione particolare. Di conseguenza dovrà essere effettuata una nuova valutazione che tenga conto delle specifiche argomentazioni addotte dall'interessato. In linea di principio tale valutazione sarà nuovamente sottoposta alla verifica di un'autorità di protezione dei dati o dei tribunali.

*(b) Oltre l'opposizione: il ruolo della revoca come garanzia supplementare*

Il Gruppo di lavoro sottolinea che, sebbene il diritto di opposizione di cui all'articolo 14, lettera a), debba essere giustificato dall'interessato, nulla vieta al responsabile del trattamento di offrire la possibilità di revocare il consenso che, oltre a costituire un'opzione più ampia, non comporterebbe la necessità di fornire una dimostrazione supplementare dell'interesse legittimo (preminente o di altro tipo) da parte dell'interessato. Non sarà necessario che tale diritto incondizionato si basi sulla situazione specifica degli interessati.

Di fatto, e in particolare nei casi limite in cui è difficile bilanciare gli interessi e i diritti in gioco, un meccanismo di revoca adeguatamente strutturato ed efficace, pur non fornendo necessariamente agli interessati tutti gli elementi atti a soddisfare il requisito di un consenso valido a norma dell'articolo 7, lettera a), potrebbe svolgere un ruolo importante nella salvaguardia dei diritti e degli interessi degli interessati.

A tal fine occorre adottare un approccio flessibile, che distingua i casi in cui è necessario un consenso esplicito ai sensi dell'articolo 7, lettera a), dai casi in cui un'opportunità praticabile di revocare il proprio consenso al trattamento (associata ad altre possibili misure supplementari) potrebbe contribuire a tutelare gli interessati ai sensi dell'articolo 7, lettera f).

---

<sup>103</sup> Questo diritto di opposizione non deve essere confuso con il consenso basato sull'articolo 7, lettera a), conformemente al quale il responsabile del trattamento non può trattare i dati prima di ottenere tale consenso. Nell'ambito dell'articolo 7, lettera f), il responsabile del trattamento può trattare i dati, subordinatamente a determinate condizioni e garanzie, purché l'interessato non si sia opposto. In questo senso, il diritto di opposizione può piuttosto essere considerato come una forma specifica di revoca del consenso. Per maggiori particolari, cfr. il parere 15/2011 del Gruppo di lavoro sulla definizione di consenso (citato alla nota a piè di pagina 2).

Quanto più ampiamente applicabile sarà il meccanismo di revoca del consenso e quanto più semplice sarà esercitarlo, tanto più tale meccanismo contribuirà a far pendere il bilanciamento a favore del trattamento al fine di trovare un fondamento giuridico nell'articolo 7, lettera f).

*Esempio: l'evoluzione nell'approccio all'invio di materiale pubblicitario*

Per illustrare in che modo si opera una distinzione tra i casi in cui è necessario un consenso a norma dell'articolo 7, lettera a), e i casi in cui si potrebbe ricorrere alla revoca quale garanzia ai sensi dell'articolo 7, lettera f), è utile avvalersi dell'esempio dell'invio di materiale pubblicitario, per cui l'articolo 14, lettera b), della direttiva prevede tradizionalmente una specifica disposizione di deroga al consenso. Per far fronte ai nuovi sviluppi tecnologici, questa disposizione è stata successivamente integrata da disposizioni specifiche nella direttiva relativa alla vita privata e alle comunicazioni elettroniche<sup>104</sup>.

Ai sensi dell'articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, per taluni tipi di attività (più invasive) di invio di materiale pubblicitario (quali la commercializzazione per posta elettronica e i dispositivi automatici di chiamata), il consenso è la norma. In deroga a tale disposizione, nei rapporti di clientela esistenti in cui un responsabile del trattamento pubblicizza i propri "analoghi" prodotti o servizi è sufficiente fornire una possibilità (incondizionata) di revoca del consenso senza giustificazione.

In seguito all'evoluzione delle tecnologie è stato necessario ricorrere a soluzioni analoghe, relativamente semplici, basate su una logica simile per le nuove pratiche di invio di materiale pubblicitario.

Innanzitutto, sono cambiate le modalità di invio del materiale pubblicitario: anziché semplici e-mail spedite alle caselle di posta elettronica, ora compaiono anche annunci comportamentali mirati sugli smartphone e sugli schermi dei computer. Nel prossimo futuro, gli annunci pubblicitari potranno anche essere integrati in oggetti intelligenti connessi nell'ambito dell'Internet degli oggetti.

In secondo luogo, gli annunci pubblicitari stanno diventando sempre più specificamente mirati: anziché basarsi sui semplici profili dei clienti, le attività dei consumatori sono sempre più frequentemente tracciate e conservate online e offline nonché analizzate con sistemi automatizzati più sofisticati<sup>105</sup>.

A seguito di tali sviluppi, l'oggetto del test comparativo è cambiato: non si tratta più di valutare il diritto alla libertà di espressione commerciale, ma sostanzialmente gli interessi economici delle organizzazioni imprenditoriali di conoscere i loro clienti tracciandone e controllandone le attività online and offline, che devono essere bilanciati con i diritti (fondamentali) alla vita privata e alla tutela dei dati personali di tali persone e il loro interesse a non essere indebitamente controllate.

---

<sup>104</sup> Riguardo all'articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, cfr. anche la sezione III.2.4 del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato precedentemente alla nota a piè di pagina 9).

<sup>105</sup> Cfr. la sezione III.2.5 e l'allegato 2 (Megadati e dati aperti) del parere 3/2013 del Gruppo di lavoro sul principio di limitazione delle finalità (citato precedentemente alla nota a piè di pagina 9).

Questo cambiamento nei modelli commerciali prevalenti e il maggior valore attribuito ai dati personali quale risorsa per le organizzazioni imprenditoriali spiega il recente obbligo del consenso in quest'ambito, conformemente all'articolo 5, paragrafo 3, e all'articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

Esistono pertanto regole specifiche differenti, a seconda della forma di commercializzazione, tra cui:

- il diritto incondizionato a opporsi all'invio di materiale pubblicitario (concepito per il contesto tradizionale di invio per posta e per la commercializzazione di prodotti simili) ai sensi dell'articolo 14, lettera b), della direttiva; in tal caso il fondamento giuridico potrebbe essere l'articolo 7, lettera f);
- l'obbligo del consenso a norma dell'articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche per l'uso di sistemi automatizzati di chiamata, fax, messaggi di testo e commercializzazione per posta elettronica (salvo eccezioni)<sup>106</sup> e l'applicazione *de facto* dell'articolo 7, lettera a), della direttiva sulla protezione dei dati;
- l'obbligo del consenso di cui all'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche (e all'articolo 7, lettera a), della direttiva sulla protezione dei dati) per la pubblicità comportamentale basata su tecniche di tracciamento come i cookie che archiviano informazioni nel terminale dell'utente<sup>107</sup>.

Sebbene i fondamenti giuridici applicabili siano chiari per quanto riguarda l'articolo 5, paragrafo 3, e l'articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, non tutte le forme di invio di materiale pubblicitario sono contemplate e sarebbe auspicabile disporre di orientamenti sulle situazioni per le quali occorre fornire il consenso di cui all'articolo 7, lettera a), e sulle situazioni per cui è stato raggiunto un equilibrio ai sensi dell'articolo 7, lettera f), compresa la possibilità di revoca.

A tale proposito è utile ricordare il parere del Gruppo di lavoro sul principio di limitazione delle finalità, in cui si afferma a chiare lettere che, “quando un'organizzazione vuole espressamente analizzare o prevedere le preferenze personali, il comportamento e le intenzioni dei singoli clienti, che successivamente informeranno 'le misure o le decisioni' adottate riguardo a tali clienti [...], sarà quasi sempre necessario ottenere un consenso libero, specifico, informato e inequivocabile, altrimenti l'uso successivo non potrà essere considerato compatibile. È importante sottolineare che tale consenso deve essere ottenuto, per esempio, per scopi di tracciamento e profilazione a fini di invio di materiale pubblicitario, pubblicità comportamentale, intermediazione di dati, pubblicità basata sulla localizzazione o ricerche di mercato digitali basate sul tracciamento<sup>108</sup>”.

#### *Alternative ai servizi online “gratuiti” compatibili con la protezione dei dati*

In un contesto in cui i clienti che sottoscrivono servizi online “gratuiti” di fatto “pagano per” tali servizi autorizzando l'utilizzo dei loro dati personali, contribuirebbe a sua volta a una

---

<sup>106</sup> Cfr. anche l'articolo 13, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche, che lascia agli Stati membri la possibilità di scegliere se accettare o rifiutare l'invio di materiale pubblicitario tramite altri mezzi.

<sup>107</sup> Per l'applicazione di questa disposizione, cfr. il parere 2/2010 del Gruppo di lavoro sulla pubblicità comportamentale online (WP 171).

<sup>108</sup> Cfr. l'allegato II (Megadati e dati aperti) del parere (citato alla precedente nota a piè di pagina 9), pagina 45.

valutazione favorevole del bilanciamento, o al riscontro dell'effettiva libertà di scelta del consumatore e pertanto del valido consenso da esso fornito ai sensi dell'articolo 7, lettera a), se il responsabile del trattamento offrisse anche una versione alternativa dei suoi servizi, in cui i "dati personali" non fossero utilizzati a fini di commercializzazione.

Finché tali servizi alternativi non saranno disponibili, sarà più difficile sostenere che è stato manifestato un consenso valido (liberamente espresso) ai sensi dell'articolo 7, lettera a), attraverso il semplice utilizzo di servizi gratuiti o che l'equilibrio degli interessi di cui all'articolo 7, lettera f), deve essere ottenuto a favore del responsabile del trattamento.

Le precedenti considerazioni evidenziano il ruolo importante che le garanzie supplementari, compreso un meccanismo efficace di revoca del consenso al trattamento, potrebbero svolgere nella modifica del bilanciamento provvisorio. Al tempo stesso, suggeriscono altresì che, in alcuni casi, l'articolo 7, lettera f), non può essere invocato come fondamento giuridico per il trattamento e che i responsabili del trattamento devono garantire un consenso valido ai sensi dell'articolo 7, lettera a), oppure ottemperare ad alcune altre condizioni della direttiva, affinché possa essere effettuato il trattamento.

#### *Portabilità dei dati, "Midata" e questioni correlate*

Tra le garanzie supplementari che potrebbero contribuire a far pendere il bilanciamento in un senso o nell'altro deve essere accordata una particolare attenzione alla portabilità dei dati e alle misure correlate, che potrebbero acquisire sempre maggiore importanza in un ambiente online. Il Gruppo di lavoro rimanda al suo parere sul principio di limitazione delle finalità, in cui ha sottolineato che "in molte situazioni, garanzie quali permettere agli interessati/ai clienti di accedere direttamente ai loro dati in un formato portabile, di facile utilizzo e leggibile meccanicamente potrebbe contribuire a responsabilizzarli e a ridurre lo squilibrio economico tra grandi società da una parte e interessati/consumatori dall'altra. Permetterebbe inoltre alle persone di 'condividere la ricchezza' creata dai megadati e incentiverebbe gli sviluppatori a offrire applicazioni e caratteristiche aggiuntive ai loro utenti<sup>109</sup>".

La disponibilità di meccanismi efficaci volti a permettere agli interessati di accedere ai loro dati, modificarli, cancellarli, trasferirli o sottoporli altrimenti a un trattamento successivo (o permetterne l'ulteriore trattamento da parte di terzi) li responsabilizzerà e consentirà loro di trarre maggiori benefici dai servizi digitali. Può inoltre promuovere un contesto di mercato più concorrenziale, permettendo ai clienti di cambiare fornitore più facilmente (per esempio nell'ambito dei servizi bancari online o nel caso dei fornitori di energia in un contesto di reti intelligenti). Infine, può altresì contribuire allo sviluppo di servizi supplementari a valore aggiunto da parte di terzi che potrebbero essere in grado di accedere ai dati dei clienti su richiesta e sulla base del consenso dei clienti. In quest'ottica, la portabilità dei dati è pertanto

---

<sup>109</sup> "Cfr. iniziative quali il progetto 'Midata' del Regno Unito, che si basano sul principio chiave secondo cui i dati devono essere restituiti ai consumatori. 'Midata' è un programma volontario, che nell'arco del tempo dovrebbe aumentare l'accesso dei consumatori ai loro dati personali in un formato portabile ed elettronico. L'idea fondamentale è che anche i consumatori debbano trarre beneficio dai megadati tramite l'accesso alle loro informazioni personali per poter compiere scelte migliori. Cfr. anche le iniziative "Green button", che permettono ai consumatori di accedere ai loro dati sull'uso dell'energia". Per maggiori informazioni sulle iniziative intraprese nel Regno Unito e in Francia, cfr. <http://www.midatalab.org.uk/> e <http://mesinfos.fing.org/>.

positiva non solo per la protezione dei dati, ma anche per la concorrenza e la tutela dei consumatori<sup>110</sup>.

## **IV. Osservazioni finali**

Nel presente parere il Gruppo di lavoro ha analizzato i principi relativi alla legittimazione del trattamento dei dati di cui all'articolo 7 della direttiva. Oltre a fornire orientamenti sull'interpretazione e sull'applicazione pratica dell'articolo 7, lettera f), nell'ambito dell'attuale quadro giuridico, il presente parere è volto a formulare raccomandazioni politiche per aiutare i responsabili decisionali a valutare le modifiche da apportare al quadro giuridico attuale in materia di protezione dei dati. Prima di esprimere tali raccomandazioni, di seguito sono riassunte le principali conclusioni riguardanti l'interpretazione dell'articolo 7.

### **IV.1. Conclusioni**

#### *Panoramica dell'articolo 7*

Ai sensi dell'articolo 7, il trattamento di dati personali può essere effettuato soltanto se si applica almeno uno dei sei fondamenti giuridici elencati in tale articolo.

Il primo fondamento, l'articolo 7, lettera a), si concentra sul consenso dell'interessato quale motivo di liceità. I restanti criteri, invece, ammettono il trattamento, subordinatamente a garanzie adeguate, in situazioni in cui, a prescindere dal consenso, è opportuno e necessario trattare i dati in un determinato contesto al fine di perseguire un interesse legittimo specifico.

Le lettere b), c), d) ed e) precisano ognuna un contesto specifico in cui il trattamento dei dati personali può essere considerato legittimo. Le condizioni che si applicano in ciascuno di questi differenti contesti richiedono particolare attenzione poiché definiscono il campo di applicazione dei vari fondamenti che legittimano il trattamento. Più precisamente, i criteri "necessario all'esecuzione del contratto concluso con la persona interessata", "necessario per adempiere un obbligo legale", "necessario per la salvaguardia dell'interesse vitale della persona interessata" e "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri" contengono requisiti differenti, che sono stati discussi nella sezione III.2.

La lettera f) si riferisce, più in generale, all'interesse legittimo (di qualsiasi tipo) perseguito dal responsabile del trattamento (in qualsiasi contesto). Questa disposizione generale è tuttavia espressamente subordinata a un test comparativo supplementare, il quale prevede che l'interesse legittimo del responsabile del trattamento (oppure del o dei terzi cui vengono comunicati i dati) sia valutato rispetto agli interessi o ai diritti fondamentali degli interessati.

#### *Ruolo dell'articolo 7, lettera f)*

Non si deve considerare l'articolo 7, lettera f), come un fondamento giuridico al quale si può ricorrere solo moderatamente come "estremo rimedio" al fine di colmare lacune nel caso di situazioni rare e impreviste o come ultima possibilità qualora non sia possibile applicare alcun

---

<sup>110</sup> Riguardo al diritto alla portabilità dei dati, cfr. l'articolo 18 della proposta di regolamento.

altro criterio. Analogamente, questa opzione non deve essere privilegiata rispetto alle altre né se ne deve ampliare indebitamente l'utilizzo in base alla percezione che sia meno vincolante rispetto agli altri criteri. Si tratta invece di uno strumento valido quanto gli altri fondamenti per legittimare il trattamento dei dati personali.

Nelle giuste circostanze e in presenza di adeguate garanzie, il corretto utilizzo dell'articolo 7, lettera f), potrebbe contribuire a evitare che gli altri fondamenti giuridici siano utilizzati in maniera impropria o che si faccia eccessivamente affidamento ad essi. Una valutazione adeguata del bilanciamento degli interessi ai sensi dell'articolo 7, lettera f), spesso accompagnata dalla possibilità di revocare il consenso al trattamento, potrebbe in alcuni casi rappresentare una valida alternativa all'uso improprio, per esempio, del fondamento del "consenso" o del criterio della "necessità ai fini dell'esecuzione del contratto". Considerato in questo modo, l'articolo 7, lettera f), presenta garanzie complementari rispetto agli altri criteri di liceità prestabiliti. Non deve quindi essere ritenuto "l'anello più debole" o una "porta aperta" per legittimare tutte le attività di trattamento dei dati che non rientrano in uno degli altri fondamenti giuridici.

#### *Interesse legittimo del responsabile del trattamento/interessi o diritti fondamentali dell'interessato*

Il concetto di "interesse" è l'interesse più ampio che un responsabile può avere nel trattamento oppure il beneficio che il responsabile trae (o che potrebbe trarre la società) dal trattamento. L'interesse potrebbe essere preminente, evidente oppure più controverso. Nelle situazioni contemplate dall'articolo 7, lettera f), potrebbero pertanto rientrare sia l'esercizio di diritti fondamentali o la protezione di importanti interessi personali o sociali che altri contesti meno ovvi o addirittura problematici.

Per essere considerato "legittimo" ed essere pertinente ai sensi dell'articolo 7, lettera f), l'interesse dovrà essere lecito, ossia conforme al diritto nazionale e unionale. Dovrà inoltre essere abbastanza specifico e articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del responsabile del trattamento rispetto agli interessi e ai diritti fondamentali dell'interessato. Dovrà altresì rappresentare un interesse concreto ed effettivo, ossia non essere teorico.

Se il responsabile del trattamento, o il terzo cui devono essere comunicati i dati, ha tale interesse legittimo, questo non significa necessariamente che possa invocare l'articolo 7, lettera f), come fondamento giuridico per il trattamento. La possibilità di invocare l'articolo 7, lettera f), dipenderà dall'esito del test comparativo che segue. Il trattamento deve inoltre essere "necessario per il perseguimento dell'interesse legittimo" del responsabile del trattamento o, nel caso della comunicazione dei dati, del/dei terzo/i. Devono pertanto essere sempre privilegiati mezzi meno invasivi per conseguire lo stesso obiettivo.

La definizione del concetto di "interessi" degli interessati è addirittura più ampia poiché non prevede un elemento di "legittimità". Se il responsabile del trattamento o il terzo possono perseguire qualsiasi interesse, purché legittimo, per contro tutte le categorie di interessi dell'interessato devono essere prese in considerazione e valutate comparativamente rispetto a quelle del responsabile del trattamento o del terzo, nella misura in cui siano pertinenti nell'ambito del campo di applicazione della direttiva.

### *Applicazione del test comparativo*

Nell'interpretare il campo di applicazione dell'articolo 7, lettera f), il Gruppo di lavoro intende conseguire un approccio equilibrato, che garantisca la necessaria flessibilità ai responsabili del trattamento in situazioni in cui non sussiste un indebito impatto sugli interessati, fornendo contemporaneamente loro una certezza del diritto e garanzie sufficienti che questa disposizione indeterminata non sarà utilizzata in maniera impropria.

Per eseguire questo test comparativo è innanzitutto importante considerare, da un lato, la natura e l'origine dell'interesse legittimo nonché l'eventualità che il trattamento sia necessario per il perseguimento di tali interessi e, dall'altro, l'impatto sugli interessati. Questa valutazione iniziale deve tenere conto delle misure, quali la trasparenza o la raccolta limitata di dati, che il responsabile del trattamento prevede di adottare per ottemperare alla direttiva.

Dopo aver analizzato e valutato comparativamente i due elementi, è possibile giungere a un "bilanciamento" provvisorio: si può concludere in via preliminare se l'interesse legittimo del responsabile del trattamento prevale sui diritti e sugli interessi degli interessati. Potrebbero tuttavia esistere casi in cui l'esito del test comparativo è dubbio e non è chiaro se prevale l'interesse legittimo del responsabile del trattamento (o del terzo) e se il trattamento può basarsi sull'articolo 7, lettera f).

Per questo motivo è importante svolgere un'ulteriore valutazione nell'ambito del test comparativo. In questa fase, il responsabile del trattamento potrebbe valutare se è in grado di introdurre misure supplementari, che vadano oltre il rispetto delle disposizioni orizzontali della direttiva, per contribuire a proteggere gli interessati. Tra le misure supplementari potrebbe figurare, per esempio, la disponibilità di un meccanismo facilmente accessibile ed efficace volto ad assicurare agli interessati la possibilità incondizionata di revocare il proprio consenso al trattamento dei dati.

### *Fattori chiave da considerare nell'applicazione del test comparativo*

Sulla base delle precedenti considerazioni, tra i fattori utili da considerare nell'esecuzione del test comparativo figurano:

- la natura e l'origine dell'interesse legittimo, tra cui:
  - l'eventualità che il trattamento dei dati sia necessario per l'esercizio di un diritto fondamentale, o
  - altrimenti necessario per l'esecuzione di un compito di interesse pubblico o sia riconosciuto a livello sociale, culturale o giuridico/normativo dalla comunità interessata;
- l'impatto sugli interessati, tra cui:
  - la natura dei dati, ad esempio l'eventualità che il trattamento riguardi dati che potrebbero essere considerati sensibili o che sono stati ottenuti da fonti accessibili al pubblico;
  - le modalità di trattamento dei dati, tra cui l'eventualità che i dati siano resi pubblici o altrimenti resi accessibili a un ampio numero di persone o che grandi quantità di dati

personali siano trattate o combinate con altri dati (per esempio, nel caso dell'elaborazione di profili, a fini commerciali, a fini di contrasto o per altri scopi);

- le ragionevoli aspettative dell'interessato, specialmente riguardo all'utilizzo e alla comunicazione dei dati nel contesto pertinente;
- lo status del responsabile del trattamento e dell'interessato, tra cui il bilanciamento dei poteri tra l'interessato e il responsabile del trattamento o l'eventualità che l'interessato sia un minore o altrimenti appartenga a una categoria più vulnerabile della popolazione.

- garanzie supplementari volte a evitare un indebito impatto sugli interessati, tra cui:
  - la minimizzazione dei dati (ad esempio rigorose limitazioni della quantità di dati raccolti e l'immediata cancellazione dei dati dopo il loro utilizzo);
  - misure tecniche e organizzative volte a garantire che i dati non possano essere utilizzati per adottare decisioni o intraprendere altre azioni riguardo alle persone ("separazione funzionale");
  - utilizzo estensivo di tecniche di anonimizzazione, aggregazione dei dati, tecnologie di rafforzamento della tutela della vita privata, tutela della vita privata fin dalla progettazione ("privacy by design") nonché valutazioni di impatto sulla tutela della vita privata e sulla protezione dei dati;
  - maggiore trasparenza, diritto generale e incondizionato di revoca ("opt-out"), portabilità dei dati e misure correlate volte a responsabilizzare gli interessati.

#### *Responsabilità, trasparenza, il diritto di opposizione e oltre*

Relativamente a queste garanzie, nonché alla valutazione comparativa generale del bilanciamento degli interessi, tre questioni svolgono spesso un ruolo cruciale nel contesto dell'articolo 7, lettera f), e richiedono pertanto un'attenzione speciale:

- l'esistenza di alcune misure supplementari e l'eventuale necessità di prevederne altre ai fini di una maggiore trasparenza e responsabilità;
- il diritto dell'interessato a opporsi al trattamento e, oltre al diritto di opposizione, la possibilità di revocare il consenso al trattamento dei dati senza la necessità di fornire alcuna giustificazione;
- la responsabilizzazione degli interessati: la portabilità dei dati e la disponibilità di meccanismi efficaci volti a permettere all'interessato di accedere ai suoi dati, modificarli, cancellarli, trasferirli o sottoporli altrimenti a un trattamento successivo (o permetterne l'ulteriore trattamento da parte di terzi).

#### **IV. 2. Raccomandazioni**

Il testo attuale dell'articolo 7, lettera f), della direttiva è indeterminato. Questa formulazione flessibile lascia un ampio margine all'interpretazione e, come ha dimostrato l'esperienza, talvolta ha dato luogo a una mancanza di prevedibilità e di certezza del diritto. Tuttavia, se utilizzato nel giusto contesto e con l'applicazione dei giusti criteri, quali illustrati nel presente parere, l'articolo 7, lettera f), può svolgere un ruolo fondamentale come fondamento giuridico per il legittimo trattamento dei dati.

Il Gruppo di lavoro sostiene pertanto l'attuale approccio di cui all'articolo 6 della proposta di regolamento, che mantiene l'equilibrio degli interessi come fondamento giuridico separato. Sarebbero tuttavia auspicabili ulteriori orientamenti per garantire un'applicazione adeguata del test comparativo.

#### *Margini e mezzi per ulteriori specificazioni*

Un requisito fondamentale è che la disposizione rimanga sufficientemente flessibile e che rifletta i punti di vista sia del responsabile del trattamento che dell'interessato nonché la dinamicità dei pertinenti contesti. Per questo motivo il Gruppo di lavoro ritiene che non sia opportuno fornire, nel testo della proposta di regolamento o negli atti delegati, elenchi dettagliati ed esaustivi delle situazioni in cui un interesse sarebbe considerato di fatto legittimo. Il Gruppo di lavoro ritiene analogamente inopportuno definire i casi in cui l'interesse o il diritto di una parte devono prevalere *in linea di principio* o *come presunzione* sull'interesse o sul diritto dell'altra parte, unicamente in virtù della natura di tale interesse o diritto o perché sono state adottate talune misure di protezione, ad esempio i dati sono stati semplicemente pseudonimizzati. Tale approccio rischierebbe di essere sia fuorviante che inutilmente prescrittivo.

Anziché formulare sentenze definitive sui meriti dei differenti diritti e interessi, il Gruppo di lavoro insiste sul *ruolo cruciale del test comparativo* nella valutazione dell'articolo 7, lettera f). Sussiste la necessità di mantenere la flessibilità del test, ma le modalità di esecuzione devono essere rese più efficaci nella pratica e consentire un'osservanza più rigorosa. Ciò deve tradursi in un *maggior* obbligo di *responsabilità* per i responsabili del trattamento dei dati, nel cui ambito il responsabile del trattamento ha la responsabilità di *dimostrare* che gli interessi e i diritti dell'interessato non prevalgono sul suo interesse.

#### *Orientamenti e responsabilità*

A tal fine, il Gruppo di lavoro raccomanda che nella proposta di regolamento siano forniti orientamenti nel modo indicato di seguito.

- 1) Sarebbe utile individuare e indicare in un considerando un elenco non esaustivo dei fattori chiave da considerare nell'applicazione del test comparativo, quali la natura e l'origine dell'interesse legittimo, l'impatto sugli interessati e le garanzie supplementari che potrebbero essere applicate dal responsabile del trattamento per evitare qualsiasi indebito impatto del trattamento sugli interessati. Tali garanzie possono comprendere, fra le altre,
  - la separazione funzionale dei dati, l'utilizzo adeguato di tecniche di anonimizzazione, della cifratura e di altre misure tecniche e organizzative volte a limitare i rischi potenziali per gli interessati;
  - ma anche misure volte a garantire agli interessati una maggiore trasparenza e una scelta più ampia, tra cui, se del caso, la possibilità incondizionata di revocare il proprio consenso al trattamento, gratuitamente e secondo modalità che possano essere invocate in maniera semplice ed efficace.

- 2) Il Gruppo di lavoro apprezzerrebbe inoltre se nella proposta di regolamento fossero forniti ulteriori chiarimenti sul modo in cui il responsabile del trattamento potrebbe *dimostrare*<sup>111</sup> una maggiore responsabilità.

La modifica delle condizioni alle quali gli interessati esercitano il diritto di opposizione di cui all'articolo 19 della proposta di regolamento è già un elemento di responsabilità importante. Se l'interessato si oppone al trattamento dei suoi dati a norma dell'articolo 7, lettera f), ai sensi della proposta di regolamento spetterà al responsabile del trattamento dimostrare che prevale il suo interesse. Il Gruppo di lavoro è fortemente favorevole a questa inversione dell'onere della prova poiché contribuisce a rafforzare l'obbligo di una maggiore responsabilità.

L'impossibilità del responsabile del trattamento dei dati di dimostrare all'interessato in un caso specifico che prevale il suo interesse potrebbe anche avere conseguenze più ampie per l'intero trattamento, non solo per l'interessato che si è opposto. Pertanto il responsabile del trattamento potrebbe mettere in discussione il trattamento o decidere di riorganizzarlo, ove opportuno, a beneficio non solo dell'interessato specifico, ma anche di tutti gli altri interessati che potrebbero trovarsi in una situazione analoga<sup>112</sup>.

Questo requisito è necessario ma non sufficiente. Per garantire la protezione fin dall'inizio ed evitare l'elusione dell'inversione dell'onere della prova<sup>113</sup>, è importante che siano adottate misure *prima* dell'inizio del trattamento e non solo nel corso delle procedure "di opposizione" *ex post*.

Si propone pertanto che, nella prima fase di qualsiasi attività di trattamento, il responsabile del trattamento intraprenda alcune azioni. Le prime due azioni potrebbero essere elencate in un considerando della proposta di regolamento e la terza in una disposizione specifica:

- condurre una valutazione<sup>114</sup>, che dovrebbe comprendere le varie fasi dell'analisi definite nel presente parere e riassunte nell'allegato 1. Il responsabile del trattamento

---

<sup>111</sup> Tale dimostrazione deve rimanere ragionevole e concentrarsi sul risultato anziché sul processo amministrativo.

<sup>112</sup> Oltre all'inversione dell'onere della prova, il Gruppo di lavoro approva altresì che, ai sensi della proposta di regolamento, il diritto di opposizione non dovrà più essere esercitato "per motivi *preminenti* e legittimi, derivanti dalla sua situazione particolare [dell'interessato]". Conformemente alla proposta di regolamento, invece, sarà sufficiente fare riferimento a qualsiasi motivo legittimo (non necessariamente "preminente") connesso alla situazione particolare dell'interessato. In realtà, un'altra opzione, che era stata proposta nella relazione finale della commissione LIBE, consiste nell'eliminare anche l'obbligo che il diritto di opposizione sia connesso alla situazione particolare dell'interessato. Il Gruppo di lavoro sostiene questo approccio nel senso che raccomanda che gli interessati siano in grado di sfruttare una delle due opportunità oppure entrambe, se del caso, ossia di opporsi al trattamento o sulla base della loro situazione particolare o di un contesto più generale, e in quest'ultima circostanza senza essere tenuti a fornire una giustificazione specifica. Cfr. a tale proposito l'emendamento 114 all'articolo 19, paragrafo 1, della proposta di regolamento nella relazione finale della commissione LIBE.

<sup>113</sup> I responsabili del trattamento dei dati, per esempio, potrebbero essere tentati di evitare di dimostrare caso per caso che prevale il loro interesse avvalendosi di giustificazioni standard o potrebbero rendere altrimenti farraginoso l'esercizio del diritto di opposizione.

<sup>114</sup> Tale valutazione, come precedentemente indicato alla nota a piè di pagina 84, non deve essere confusa con una valutazione generale dell'impatto sulla protezione dei dati e sulla tutela della vita privata. Attualmente non esistono orientamenti generali sulle valutazioni d'impatto a livello europeo, benché in alcuni settori, in particolare per quanto riguarda le applicazioni RFID e i sistemi di misurazione intelligenti, sia stata compiuta

dovrà espressamente individuare l'interesse/gli interessi superiori in gioco e specificare perché prevalgono sugli interessi degli interessati. Tale valutazione preliminare non dovrà essere eccessivamente gravosa e rimane *adattabile*: potrebbe essere limitata ai criteri essenziali se l'impatto del trattamento sugli interessati è a prima vista irrilevante; invece, se è stato difficile bilanciare gli interessi, dovrà essere svolta più approfonditamente e richiederà per esempio l'adozione di alcune garanzie supplementari. Ove opportuno, ovvero quando il trattamento presenta rischi specifici per i diritti e le libertà degli interessati, dovrà essere svolta una valutazione più generale dell'impatto sulla protezione dei dati personali e sulla tutela della vita privata (ai sensi dell'articolo 33 della proposta di regolamento), di cui la valutazione ai sensi dell'articolo 7, lettera f), potrebbe diventare una parte importante;

- documentare questa valutazione. Così com'è *adattabile* il livello di dettaglio con cui deve essere svolta la valutazione, deve essere adattabile anche l'entità della documentazione. Detto ciò, deve essere disponibile una documentazione di base in tutti i casi fuorché nei più insignificanti, a prescindere dalla valutazione dell'impatto del trattamento sulla persona. È sulla base di tale documentazione che la valutazione del responsabile del trattamento potrà essere ulteriormente esaminata ed eventualmente contestata;
- rendere trasparenti e visibili queste informazioni agli interessati e ad altri soggetti pertinenti. La trasparenza deve essere garantita sia nei confronti degli interessati e delle autorità di protezione dei dati nonché, ove opportuno, verso il pubblico in generale. Quanto agli interessati, il Gruppo di lavoro richiama il progetto di relazione della commissione LIBE<sup>115</sup>, in cui si affermava che il responsabile del trattamento deve informare l'interessato delle ragioni per cui ritiene che gli interessi o i diritti e le libertà fondamentali dell'interessato non prevalgono sui suoi interessi. A parere del Gruppo di lavoro, tali informazioni devono essere fornite agli interessati insieme a quelle che il responsabile del trattamento deve comunicare ai sensi degli articoli 10 e 11 della direttiva vigente (articolo 11 della proposta di regolamento). In tal modo l'interessato avrà eventualmente la possibilità di opporsi al trattamento in una seconda

---

una serie di lodevoli sforzi volti a definire una metodologia/un quadro (e/o un modello) settoriale che potrebbe essere applicato in tutta l'Unione europea. Cfr. la "Proposta dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID" e il "Modello di valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti elaborato dal gruppo di esperti n. 2 della task force della Commissione per le reti intelligenti". Il Gruppo di lavoro ha formulato più pareri riguardo a entrambe queste metodologie.

Sono state inoltre avviate alcune iniziative volte a definire una generica metodologia per la valutazione d'impatto sulla protezione dei dati di cui potrebbero beneficiare sforzi compiuti a livello settoriale. Cfr., per esempio, il progetto PIAF (*Privacy Impact Assessment Framework for data protection and privacy rights*, quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati) all'indirizzo <http://www.piafproject.eu/>.

Inoltre, per orientamenti a livello nazionale, cfr., per esempio, la metodologia della *Commission nationale de l'informatique et des libertés* (Commissione nazionale dell'informatica e delle libertà, CNIL) all'indirizzo <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf> nonché il *Privacy Impact Assessment Handbook* (Manuale sulla valutazione d'impatto sulla tutela della vita privata) pubblicato dall'ICO (*Information Commissioner's Office*) all'indirizzo [http://ico.org.uk/pia\\_handbook\\_html\\_v2/files/PIAhandbookV2.pdf](http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf).

<sup>115</sup> Progetto di relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

fase, mentre il responsabile del trattamento potrà fornire una giustificazione supplementare caso per caso degli interessi superiori. Inoltre, la documentazione su cui il responsabile del trattamento ha basato la propria valutazione dovrà essere messa a disposizione delle autorità di protezione dei dati, su richiesta, al fine di consentire l'eventuale verifica e applicazione, se del caso.

Il Gruppo di lavoro sarebbe lieto se queste tre fasi fossero espressamente incluse nella proposta di regolamento secondo le modalità precedentemente illustrate. Il ruolo specifico dei fondamenti giuridici troverebbe così riconoscimento nella valutazione della legittimità e chiarirebbe l'importanza del test comparativo nel più ampio contesto delle misure di responsabilità e delle valutazioni dell'impatto nel nuovo quadro giuridico proposto.

Il Gruppo di lavoro ritiene altresì opportuno affidare al comitato europeo per la protezione dei dati la formulazione di ulteriori orientamenti, ove necessario, sulla base di questo quadro. Tale approccio permetterà di rendere sia sufficientemente chiaro il testo che sufficientemente flessibile la sua attuazione.

## **Allegato 1. Guida rapida allo svolgimento del test comparativo di cui all'articolo 7, lettera f)**

### **Fase 1: valutare quale fondamento giuridico potrebbe potenzialmente essere applicato ai sensi dell'articolo 7, lettere da a) a f)**

Il trattamento dei dati può essere effettuato solo qualora sia applicabile uno o più dei sei fondamenti, lettere da a) a f), dell'articolo 7 (è possibile invocare fondamenti differenti in fasi differenti della stessa attività di trattamento). Se, a prima vista, sembra che l'articolo 7, lettera f), potrebbe costituire una base giuridica appropriata, passare alla fase 2.

#### *Suggerimenti rapidi:*

- l'articolo 7, lettera a), si applica solo se è stato fornito un consenso libero, informato, specifico e inequivocabile; il fatto che una persona non si sia opposta a un trattamento ai sensi dell'articolo 14 non va confuso con il consenso di cui all'articolo 7, lettera a); tuttavia, un semplice meccanismo per opporsi a un trattamento potrebbe essere considerato una garanzia importante ai sensi dell'articolo 7, lettera f);
- l'articolo 7, lettera b), riguarda il trattamento che è necessario all'esecuzione del contratto; il semplice fatto che il trattamento dei dati sia connesso al contratto, o previsto in qualche punto delle condizioni contrattuali, non significa necessariamente che sia possibile applicare questo fondamento; se del caso, valutare l'opportunità di ricorrere all'articolo 7, lettera f), in alternativa;
- l'articolo 7, lettera c), riguarda esclusivamente chiari e specifici obblighi legali ai sensi delle normative dell'UE o di uno Stato membro; in caso di orientamenti non vincolanti (ad esempio di agenzie di regolamentazione) o di un obbligo legale straniero, valutare l'opportunità di ricorrere all'articolo 7, lettera f), in alternativa.

### **Fase 2: classificare un interesse come “legittimo” o “illegittimo”**

Per essere considerato legittimo, un interesse deve soddisfare cumulativamente le seguenti condizioni:

- essere lecito (ossia conforme al diritto nazionale e unionale);
- essere articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del responsabile del trattamento rispetto agli interessi e ai diritti dell'interessato (ossia sufficientemente specifico);
- rappresentare un interesse concreto ed effettivo (ossia non deve essere teorico).

### **Fase 3: stabilire se il trattamento è necessario per il perseguimento dell'interesse**

Per soddisfare questo requisito, valutare se esistono altri mezzi meno invasivi per conseguire lo scopo specifico del trattamento e rispondere all'interesse legittimo del responsabile del trattamento dei dati.

### **Fase 4: definire un bilanciamento provvisorio valutando se gli interessi o i diritti fondamentali degli interessati prevalgono sull'interesse del responsabile del trattamento**

- Considerare la natura degli interessi del responsabile del trattamento (diritto fondamentale, altro tipo di interesse, interesse pubblico);

- valutare l'eventuale danno subito dal responsabile del trattamento, dai terzi o dalla collettività in generale qualora non sia effettuato il trattamento dei dati;
- tenere conto della natura dei dati (sensibili in senso stretto o in senso più ampio?);
- considerare lo status dell'interessato (minore, lavoratore dipendente, ecc.) e del responsabile del trattamento (ad esempio se un'organizzazione imprenditoriale si trova in una posizione dominante sul mercato);
- tenere conto della modalità di trattamento dei dati (vasta scala, estrapolazione dei dati, profilazione, comunicazione a un ampio numero di persone o pubblicazione);
- individuare i diritti fondamentali e/o gli interessi dell'interessato su cui potrebbe incidere il trattamento;
- considerare le ragionevoli aspettative degli interessati;
- valutare l'impatto sull'interessato e confrontarlo con i benefici che il responsabile del trattamento dei dati prevede di trarre dal trattamento.

*Suggerimento rapido:* valutare l'effetto che il trattamento vero e proprio potrebbe avere su persone specifiche (questa analisi non deve essere considerata come un esercizio astratto o ipotetico).

#### **Fase 5: definire un bilanciamento definitivo tenendo conto di garanzie supplementari**

Individuare e attuare garanzie supplementari adeguate derivanti dall'obbligo di sollecitudine e di diligenza, quali:

- minimizzazione dei dati (ad esempio, rigorose limitazioni della quantità di dati raccolti e l'immediata cancellazione dei dati dopo il loro utilizzo)
- misure tecniche e organizzative volte a garantire che i dati non possano essere utilizzati per adottare decisioni o intraprendere altre azioni riguardo alle persone ("separazione funzionale")
- utilizzo estensivo di tecniche di anonimizzazione, aggregazione dei dati, tecnologie di rafforzamento della tutela della vita privata, tutela della vita privata fin dalla progettazione ("privacy by design") nonché valutazioni di impatto sulla tutela della vita privata e sulla protezione dei dati;
- maggiore trasparenza, diritto generale e incondizionato di opposizione (revoca del consenso), portabilità dei dati e misure correlate volte a responsabilizzare gli interessati.

*Suggerimento rapido:* l'utilizzo di tecnologie e approcci di rafforzamento della tutela della vita privata può contribuire a far pendere il bilanciamento a favore del responsabile del trattamento dei dati nonché a proteggere le persone.

#### **Fase 6: dimostrare la conformità e garantire la trasparenza**

- Tracciare un piano delle fasi da 1 a 5 per giustificare il trattamento prima del suo avvio.
- Informare gli interessati dei motivi per cui si ritiene che il bilanciamento degli interessi sia a favore del responsabile del trattamento.
- Mantenere la documentazione a disposizione delle autorità di protezione dei dati.

*Suggerimento rapido:* questa fase è *adattabile* e, pertanto, i dettagli della valutazione e della documentazione devono essere adeguati alla natura e al contesto del trattamento. La portata di queste misure sarà maggiore se sarà trattata una grande quantità di informazioni su molte persone in un modo che potrebbe incidere considerevolmente su di esse. Una valutazione generale dell'impatto sulla protezione dei dati personali e sulla tutela della vita privata (ai sensi dell'articolo 33 della proposta di regolamento) sarà necessaria solo nel caso in cui

un'operazione di trattamento presenti rischi specifici per i diritti e le libertà degli interessati. Nei casi in questione, la valutazione di cui all'articolo 7, lettera f), potrebbe diventare una parte fondamentale di questa più ampia valutazione dell'impatto.

**Fase 7: che cosa fare se l'interessato esercita il suo diritto di opposizione?**

- Se come garanzia esiste solo un diritto qualificato di opporsi al trattamento (espressamente previsto ai sensi dell'articolo 14, lettera a), come garanzia minima): qualora l'interessato si opponga al trattamento, occorre garantire l'esistenza di un meccanismo adeguato e di facile utilizzo grazie al quale sia possibile valutare nuovamente il bilanciamento degli interessi per quanto riguarda la persona interessata e interrompere il trattamento dei suoi dati se dalla nuova valutazione emerge che prevalgono i suoi interessi.

- Se come garanzia supplementare è previsto un diritto incondizionato di revoca del consenso (o perché espressamente prescritto ai sensi dell'articolo 14, lettera b), o perché tale diritto è altrimenti considerato una garanzia supplementare necessaria o utile): qualora l'interessato si opponga al trattamento, si deve garantire che la sua scelta sia rispettata, senza la necessità di adottare altre misure o procedere a ulteriori valutazioni.

## **Allegato 2. Esempi pratici volti a illustrare l'applicazione del test comparativo di cui all'articolo 7, lettera f)**

Questo allegato fornisce esempi riguardanti alcuni degli ambiti più comuni in cui può porsi la questione dell'interesse legittimo ai sensi dell'articolo 7, lettera f). Nella maggior parte dei casi abbiamo raggruppato due o più esempi correlati che vale la pena di confrontare nell'ambito di un'unica rubrica. Molti degli esempi si basano su casi concreti o su elementi di casi concreti gestiti dalle autorità di protezione dei dati nei differenti Stati membri. Tuttavia, talvolta abbiamo modificato in certa misura i fatti per riuscire a illustrare meglio le modalità di svolgimento del test comparativo.

Gli esempi sono forniti al fine di illustrare il *processo di riflessione* (il metodo da utilizzare per svolgere il test comparativo multifattoriale). In altre parole, gli esempi *non* intendono fornire una valutazione *definitiva* dei casi descritti. Anzi, in molti casi, modificando in qualche modo le circostanze fattuali (per esempio, se il responsabile del trattamento dovesse adottare garanzie supplementari quali un'anonimizzazione più completa, misure di sicurezza migliori, una maggiore trasparenza e una scelta più autentica per gli interessati), l'esito del test comparativo potrebbe cambiare<sup>116</sup>.

Ciò dovrebbe incoraggiare i responsabili del trattamento a impegnarsi maggiormente per rispettare tutte le disposizioni orizzontali della direttiva e a offrire una protezione aggiuntiva, ove opportuno, sulla base della protezione dei dati e della tutela della vita privata fin dalla progettazione. Quanto più i responsabili del trattamento si preoccupano di proteggere i dati personali in generale, tanto maggiori saranno le probabilità che soddisfino il test comparativo.

***Esercizio del diritto alla libertà di espressione e d'informazione<sup>117</sup>, anche nei mezzi di comunicazione e di espressione artistica***

### **Esempio 1: una ONG ripubblica le spese dei parlamentari**

Un'autorità pubblica, in virtù di un obbligo legale (articolo 7, lettera c)), pubblica le spese dei parlamentari; una ONG a difesa della trasparenza, a sua volta, analizza e ripubblica i dati in una versione annotata accurata, proporzionata, ma più informativa, contribuendo a una maggiore trasparenza e responsabilità.

Supponendo che ripubblichi le spese dei parlamentari in una versione annotata, in maniera accurata e proporzionata, adotti garanzie adeguate e, in senso più ampio, rispetti i diritti delle persone interessate, l'ONG dovrebbe essere in grado di invocare l'articolo 7, lettera f), come fondamento giuridico per il trattamento. Fattori quali la natura dell'interesse legittimo (un diritto fondamentale alla libertà di espressione o d'informazione), l'interesse del pubblico relativo alla trasparenza e alla responsabilità e il fatto che i dati siano già stati pubblicati e

<sup>116</sup> La corretta applicazione dell'articolo 7, lettera f), potrebbe dare luogo a complesse questioni di valutazione e, per contribuire a orientare la valutazione, una legislazione e una giurisprudenza specifiche, orientamenti mirati nonché codici di condotta e altre norme formali o meno formali potrebbero svolgere tutti un ruolo importante.

<sup>117</sup> Per quanto riguarda la libertà di espressione e d'informazione, cfr. pagina 40 del parere. Occorre tenere conto anche di tutte le deroghe pertinenti previste dal diritto nazionale per il trattamento di dati personali effettuato a scopi giornalistici ai sensi dell'articolo 9 della direttiva.

riguardino dati personali (relativamente meno sensibili) connessi alle attività dei parlamentari pertinenti per l'esercizio delle loro funzioni pubbliche<sup>118</sup> depongono tutti a favore della legittimità del trattamento. Il fatto che la pubblicazione iniziale sia stata prevista dalla legge e che di conseguenza le persone si aspettassero che i loro dati sarebbero stati pubblicati contribuisce a sua volta a una valutazione favorevole. Esaminando l'altro elemento da valutare ai fini del test comparativo, l'impatto sulla persona potrebbe essere considerevole: per esempio, a causa del controllo del pubblico, potrebbe essere messa in discussione l'integrità personale di alcune persone, che di conseguenza potrebbero perdere le elezioni o, in alcuni casi, essere oggetto di indagini penali per attività fraudolente. L'insieme dei fattori precedenti, tuttavia, dimostra che, nel complesso, gli interessi del responsabile del trattamento (e gli interessi del pubblico al quale sono comunicati i dati) prevalgono sugli interessi degli interessati.

### **Esempio 2: un consigliere comunale nomina sua figlia come assistente speciale**

Un giornalista pubblica su un giornale locale online un articolo contenente dati conformi ai fatti e fondato su ricerche esaurienti da cui emerge che un consigliere comunale ha partecipato solo a una delle ultime undici riunioni del consiglio comunale e che probabilmente non sarà rieletto a causa di un recente scandalo scaturito dalla nomina della sua figlia diciassettenne come assistente speciale.

Anche in questo caso si applica un'analisi simile a quella fornita nell'*Esempio 1*. Per quanto riguarda i fatti, rientra negli interessi legittimi del giornale in questione pubblicare le informazioni. Benché siano stati rivelati dati personali riguardanti il consigliere comunale, il diritto alla tutela della sua vita privata non prevale sul diritto fondamentale alla libertà di espressione e di pubblicare la storia sul giornale. Questo perché i diritti alla tutela della vita privata delle personalità pubbliche sono relativamente limitati rispetto alle loro attività pubbliche nonché per la speciale importanza della libertà di espressione, in particolare nei casi in cui la pubblicazione di una storia sia di interesse pubblico.

### **Esempio 3: tra i primi risultati di ricerca continua a figurare la notizia di un reato penale minore**

L'archivio online di un giornale contiene un vecchio articolo riguardante una persona, un tempo una celebrità locale, il capitano di una squadra di calcio amatoriale di una piccola città. La persona è identificata con il suo nome completo e la storia si riferisce al suo coinvolgimento in un procedimento penale per un reato relativamente minore (stato di ubriachezza molesta). Ora la sua fedina penale è pulita e non riporta più il reato commesso in passato, per il quale la persona in questione ha scontato la sua pena alcuni anni orsono. Ciò che più infastidisce l'interessato è che, cercando il suo nome attraverso i comuni motori di ricerca online, il collegamento a questa vecchia notizia figura tra i primi risultati che lo riguardano. Nonostante la sua richiesta, il giornale si rifiuta di adottare misure tecniche che limiterebbero la più ampia disponibilità della notizia riguardante l'individuo in questione. Per esempio, il giornale si rifiuta di adottare misure tecniche e organizzative intese a limitare

<sup>118</sup> Non si può escludere che alcune spese possano rivelare dati più sensibili, quali dati sanitari. In tal caso, i dati in questione dovranno essere innanzitutto espunti dall'insieme di dati prima della sua pubblicazione. È buona prassi adottare un "approccio proattivo" e offrire alle persone l'opportunità di riesaminare i loro dati prima che siano pubblicati nonché informarle chiaramente riguardo alle possibilità e alle modalità della pubblicazione.

(nella misura consentita dalla tecnologia) l'accesso alle informazioni da motori di ricerca esterni che utilizzano il nome della persona come categoria di ricerca.

Questo è un altro caso volto a illustrare il possibile conflitto tra la libertà di espressione e la vita privata. Dimostra altresì che in alcuni casi le garanzie supplementari (tra cui quella che, almeno nel caso di un'opposizione giustificata ai sensi dell'articolo 14, lettera a), della direttiva, garantisce che la parte pertinente degli archivi del giornale non sarà più accessibile da parte di motori di ricerca esterni o che il formato utilizzato per mostrare le informazioni non consentirà di effettuare ricerche basate sul nome) possono svolgere un ruolo fondamentale nel bilanciare adeguatamente i due diritti fondamentali in questione. Ciò non pregiudica alcuna delle altre misure che potrebbero essere intraprese da motori di ricerca o da altri terzi<sup>119</sup>.

### *Commercializzazione diretta tradizionale e altre forme di commercializzazione o pubblicità*

#### **Esempio 4: un negozio di computer invia ai suoi clienti messaggi pubblicitari riguardanti prodotti simili a quelli da loro acquistati**

Un negozio di computer ottiene i recapiti dei suoi clienti nell'ambito della vendita di un prodotto e utilizza tali recapiti per commercializzare altri suoi prodotti simili tramite la posta tradizionale. Il negozio vende anche prodotti online e invia e-mail promozionali quando una nuova linea di prodotti arriva in magazzino. I clienti sono chiaramente informati in merito alla loro possibilità di opporsi, in maniera facile e gratuita, al momento della raccolta dei loro recapiti e all'invio di ogni messaggio, qualora non abbiano manifestato inizialmente la loro opposizione.

La trasparenza del trattamento, il fatto che il cliente può ragionevolmente aspettarsi di ricevere offerte per prodotti analoghi in quanto cliente del negozio e che ha il diritto di opporsi contribuiscono a rafforzare la legittimità del trattamento e a salvaguardare i diritti delle persone. Esaminando l'altro elemento da valutare ai fini del test comparativo, non sembra sussistere un impatto sproporzionato sul diritto alla tutela della vita privata della persona (in questo caso abbiamo supposto che il negozio di computer non abbia creato profili complessi dei suoi clienti, per esempio utilizzando un'analisi dettagliata dei dati provenienti da flussi di clic).

#### **Esempio 5: una farmacia online crea profili completi dei suoi clienti**

Una farmacia online svolge attività di commercializzazione sulla base dei medicinali e di altri prodotti acquistati dai clienti, tra cui prodotti ottenuti con prescrizione medica. Analizza queste informazioni (in combinazione con dati demografici relativi ai clienti, per esempio il genere e l'età) al fine di elaborare un profilo "salute e benessere" dei singoli clienti. Utilizza anche i dati provenienti da flussi di clic, che sono raccolti non solo riguardo ai prodotti acquistati dai clienti, ma anche riguardo ad altri prodotti e informazioni di cui i clienti hanno effettuato la ricerca navigando sul sito web. I profili dei clienti contengono informazioni o previsioni da cui si evince che una determinata cliente è incinta, soffre di una particolare malattia cronica o sarebbe interessata ad acquistare integratori alimentari, creme solari o altri

<sup>119</sup> Cfr. anche Corte di giustizia dell'Unione europea, causa C-131/12 *Google Spain c. Agencia Española de Protección de Datos*, attualmente all'esame della Corte di giustizia dell'Unione europea.

prodotti per la cura della pelle in certi periodi dell'anno. Gli analisti della farmacia online utilizzano queste informazioni per offrire medicinali non soggetti a prescrizione medica, integratori alimentari e altri prodotti a persone specifiche tramite posta elettronica. In questo caso la farmacia non può invocare i suoi interessi legittimi quando crea e utilizza i profili dei suoi clienti a fini di commercializzazione. L'attività di creazione di profili descritta pone alcuni problemi. I dati sono particolarmente sensibili e possono rivelare molte informazioni su questioni che molte persone si aspetterebbero rimanessero private<sup>120</sup>. La misura e la maniera in cui sono creati i profili (utilizzo di dati provenienti da flussi di clic, algoritmi predittivi) suggeriscono inoltre un elevato livello di invasività. Il consenso basato sull'articolo 7, lettera a), e sull'articolo 8, paragrafo 2, lettera a), (nel caso in cui siano coinvolti dati sensibili) potrebbe essere tuttavia considerato un'alternativa ove appropriato.

***Messaggi indesiderati non commerciali, anche a fini di campagne politiche o di raccolta fondi per scopi benefici***

**Esempio 6: una candidata alle elezioni comunali utilizza in modo mirato le liste elettorali**

Una candidata alle elezioni comunali utilizza le liste elettorali<sup>121</sup> per inviare a ogni potenziale elettore del suo distretto elettorale una lettera di presentazione volta a promuovere la sua campagna per le prossime elezioni. La candidata utilizza i dati ottenuti dalle liste elettorali solo per inviare la lettera e non conserva i dati al termine della campagna elettorale.

Tale utilizzo delle liste elettorali figura tra le ragionevoli aspettative delle persone quando è effettuato nel periodo preelettorale: l'interesse del responsabile del trattamento è chiaro e legittimo. L'utilizzo limitato e mirato delle informazioni contribuisce inoltre a far pendere il bilanciamento a favore dell'interesse legittimo del responsabile del trattamento. Tale utilizzo delle liste elettorali potrebbe inoltre essere disciplinato dalla legge a livello nazionale, in un'ottica di interesse pubblico, prevedendo norme, restrizioni e garanzie specifiche riguardo all'utilizzo delle liste elettorali. In tal caso, occorre rispettare queste norme specifiche anche per garantire la legittimità del trattamento.

**Esempio 7: un organismo senza fini di lucro raccoglie informazioni per scopi di targeting**

Un'associazione filosofica dedita allo sviluppo umano e sociale decide di organizzare attività di raccolta fondi sulla base del profilo dei suoi membri. A tal fine raccoglie dati sui siti di socializzazione mediante un software ad hoc che individua le persone che hanno assegnato un "mi piace" alla pagina dell'associazione o ai messaggi che l'associazione ha pubblicato sulla sua pagina, che hanno "condiviso" questi messaggi, che hanno consultato periodicamente alcuni articoli o hanno "ritwittato" i messaggi dell'associazione. Successivamente manda messaggi e newsletter ai suoi membri sulla base dei loro profili. Per esempio, proprietari di cani anziani che hanno assegnato un "mi piace" ad articoli su rifugi per animali ricevono

<sup>120</sup> Oltre a tutte le restrizioni imposte dalle norme di protezione dei dati, anche la pubblicità di prodotti soggetti a prescrizione medica è rigorosamente regolamentata nell'UE ed esistono altresì alcune restrizioni riguardanti la pubblicità dei medicinali non soggetti a prescrizione. Inoltre, si deve tenere conto anche degli obblighi previsti dall'articolo 8 riguardo a categorie particolari di dati (quali dati sanitari).

<sup>121</sup> Si presuppone che negli Stati membri in cui si applica questo esempio l'esistenza di liste elettorali sia prevista dalla legge.

differenti appelli di raccolta fondi da famiglie con bambini piccoli; persone appartenenti a gruppi etnici differenti ricevono a loro volta messaggi differenti.

Poiché sono trattate categorie particolari di dati (convinzioni filosofiche), deve essere rispettato l'articolo 8, una condizione che sembra essere soddisfatta in quanto il trattamento è effettuato nell'ambito delle attività legittime dell'associazione. Tuttavia, questa non è una condizione sufficiente nel caso di specie: il modo in cui sono utilizzati i dati va oltre le ragionevoli aspettative delle persone. La quantità di dati raccolti, la mancanza di trasparenza riguardo alla raccolta e il riutilizzo dei dati per una finalità differente rispetto a quella per cui i dati erano stati pubblicati inizialmente contribuiscono alla conclusione che in questo caso non può essere invocato l'articolo 7, lettera f). Il trattamento non deve quindi essere consentito a meno che non sia possibile avvalersi di un altro fondamento, per esempio il consenso degli interessati a norma dell'articolo 7, lettera a).

### ***Esercizio di un diritto in via giudiziale, compreso il recupero del credito tramite procedure extragiudiziali***

#### **Esempio 8: controversia sulla qualità dei lavori di ristrutturazione**

Un cliente contesta la qualità dei lavori di ristrutturazione della cucina e si rifiuta di pagare il prezzo totale. L'impresa edile trasferisce i dati pertinenti e proporzionati al suo avvocato affinché possa ricordare al cliente la necessità di effettuare il pagamento e trovi una soluzione negoziale alla controversia con il cliente qualora quest'ultimo continui a rifiutarsi di pagare.

In questo caso, le misure preliminari adottate dall'impresa edile che ha utilizzato informazioni di base dell'interessato (quali il nome, l'indirizzo, il numero di riferimento del contratto) per inviargli un sollecito (direttamente o tramite il suo avvocato, come in questo caso) potrebbero comunque rientrare nel trattamento necessario all'esecuzione del contratto (articolo 7, lettera b)). Le ulteriori misure adottate<sup>122</sup>, tra cui il coinvolgimento di una società di recupero crediti, devono tuttavia essere valutate ai sensi dell'articolo 7, lettera f), considerando, fra l'altro, l'invasività e l'impatto sugli interessati, come sarà illustrato nell'esempio fornito di seguito.

#### **Esempio 9: un cliente scompare con un'auto acquistata a credito**

Un cliente non paga le rate che è tenuto a versare per una costosa auto sportiva acquistata a credito e poi "scompare". Il concessionario assume un "agente terzo di riscossione". L'agente di riscossione svolge un'indagine invasiva "in stile attività di contrasto" avvalendosi, tra l'altro, di pratiche quali la videosorveglianza discreta e le intercettazioni telefoniche.

Benché gli interessi del concessionario e dell'agente di riscossione siano legittimi, il bilanciamento degli interessi non pende a loro favore a causa dei metodi invasivi utilizzati per raccogliere le informazioni, alcuni dei quali sono espressamente vietati dalla legge (le intercettazioni telefoniche). La situazione sarebbe diversa se, per esempio, il concessionario o l'agente di riscossione avessero svolto solo controlli limitati per avere conferma dei recapiti dell'interessato al fine di avviare un procedimento giudiziario.

<sup>122</sup> Attualmente tra i vari Stati membri esiste una certa disomogeneità riguardo alle misure che potrebbero essere considerate necessarie all'esecuzione di un contratto.

**Esempio 10: verifica dei dati dei clienti prima dell'apertura di un conto bancario**

Un istituto bancario segue procedure ragionevoli e proporzionate (secondo le linee guida non vincolanti della competente autorità nazionale di vigilanza finanziaria) al fine di verificare l'identità di tutte le persone che intendono aprire un conto e conserva le informazioni utilizzate per verificare l'identità delle persone.

L'interesse del responsabile del trattamento è legittimo, il trattamento dei dati riguarda solo informazioni limitate e necessarie (secondo la normale prassi del settore, che gli interessati devono ragionevolmente attendersi e le autorità competenti devono raccomandare). Esistono garanzie adeguate per limitare qualsivoglia impatto indebito e sproporzionato sugli interessati. Il responsabile del trattamento può dunque avvalersi dell'articolo 7, lettera f). In alternativa, e nella misura in cui le azioni adottate siano espressamente previste dalla legislazione applicabile, potrebbe essere applicato l'articolo 7, lettera c).

**Esempio 11: scambio di informazioni per combattere il riciclaggio di denaro**

Un istituto finanziario, previa consultazione dell'autorità di protezione dei dati competente, attua procedure basate su criteri specifici e limitati finalizzate allo scambio di dati riguardanti il presunto abuso delle norme antiriciclaggio con altre società dello stesso gruppo, con rigorose limitazioni all'accesso, sicurezza e il divieto di utilizzare successivamente tali informazioni per altre finalità.

Per ragioni analoghe a quelle illustrate nell'esempio precedente, e a seconda delle circostanze del caso, il trattamento dei dati potrebbe basarsi sull'articolo 7, lettera f). In alternativa, e nella misura in cui le azioni adottate siano espressamente previste dalla legislazione applicabile, il trattamento potrebbe fondarsi sull'articolo 7, lettera c).

**Esempio 12: lista nera di tossicodipendenti aggressivi**

Un gruppo di ospedali crea una lista nera comune di "soggetti" aggressivi in cerca di stupefacenti al fine di vietare loro l'accesso a tutte le strutture mediche dei nosocomi aderenti all'iniziativa.

Benché l'interesse dei responsabili del trattamento a mantenere sicure le strutture ospedaliere sia legittimo, tale interesse deve essere valutato rispetto al diritto fondamentale alla tutela della vita privata e ad altre preoccupazioni preminenti, quali la necessità di non escludere le persone interessate dall'accesso all'assistenza sanitaria. Il fatto che siano trattati dati sensibili (ad esempio dati sanitari connessi alla tossicodipendenza) corrobora altresì la conclusione che in questo caso è improbabile che il trattamento sia ammissibile ai sensi dell'articolo 7, lettera f)<sup>123</sup>. Il trattamento potrebbe essere ammissibile se dovesse essere per esempio disciplinato da una legge che preveda garanzie specifiche (verifiche e controlli, trasparenza, divieto di

<sup>123</sup> Si deve tenere conto anche degli obblighi previsti dall'articolo 8 riguardo alle categorie particolari di dati (quali dati sanitari).

decisioni automatizzate) volte a garantire che tale trattamento non darà luogo a discriminazioni o violazioni dei diritti fondamentali delle persone<sup>124</sup>. In quest'ultimo caso, a seconda che tale legge specifica preveda o permetta soltanto il trattamento, potrebbero essere invocati come fondamento giuridico l'articolo 7, lettera c), oppure l'articolo 7, lettera f).

### **Controllo del personale a fini di sicurezza o gestione**

#### **Esempio 13: ore di lavoro di avvocati utilizzate a fini sia di fatturazione che per la determinazione di premi**

Il numero di ore fatturabili lavorate dagli avvocati di uno studio legale è trattato sia a fini di fatturazione che per la determinazione dei premi annuali. Il sistema è spiegato in maniera trasparente ai dipendenti che hanno il diritto esplicito di esprimere il loro disaccordo con le conclusioni in termini sia di fatturazione che di pagamento del premio, di cui dovranno successivamente discutere con i loro dirigenti.

Il trattamento sembra necessario per gli interessi legittimi del responsabile del trattamento e non sembrano esistere mezzi meno invasivi per conseguire l'obiettivo in questione. L'impatto sui dipendenti è altresì limitato grazie alle garanzie e ai processi attuati. L'articolo 7, lettera f), potrebbe pertanto costituire un fondamento giuridico adeguato in questo caso. Si potrebbe altresì sostenere che il trattamento per una o per entrambe le finalità è inoltre necessario all'esecuzione del contratto.

#### **Esempio 14: monitoraggio elettronico dell'uso di Internet<sup>125</sup>**

Il datore di lavoro controlla l'utilizzo di Internet da parte dei dipendenti durante le ore di lavoro per verificare che non facciano un uso personale eccessivo degli strumenti informatici dell'azienda. I dati raccolti comprendono file temporanei e cookie generati sui computer dei dipendenti, da cui si può risalire ai siti visitati e ai download effettuati durante le ore lavorative. I dati sono trattati senza aver prima consultato gli interessati e i rappresentanti sindacali/i comitati aziendali. Inoltre, alle persone interessate non sono fornite sufficienti informazioni su queste prassi.

La quantità e la natura dei dati raccolti rappresenta una considerevole ingerenza nella vita privata dei dipendenti. Oltre alle questioni relative alla proporzionalità, un altro fattore importante da considerare è la trasparenza sulle prassi adottate, strettamente connessa alle ragionevoli aspettative degli interessati. Anche se il datore di lavoro ha un interesse legittimo a limitare il tempo trascorso dai dipendenti a visitare siti web non direttamente pertinenti per il loro lavoro, i metodi utilizzati non soddisfano i criteri del test comparativo di cui all'articolo 7, lettera f). Il datore di lavoro deve ricorrere a metodi meno invasivi (ad esempio limitando l'accessibilità di determinati siti), che, come buona prassi, siano discussi e concordati con i rappresentanti dei lavoratori e comunicati ai dipendenti in maniera trasparente.

### ***Procedure per la denuncia delle irregolarità***

<sup>124</sup> Cfr. il documento di lavoro sulle liste nere (WP 65) adottato il 3 ottobre 2002.

<sup>125</sup> Alcuni Stati membri ritengono che un certo monitoraggio elettronico limitato potrebbe essere "necessario all'esecuzione del contratto" e che, di conseguenza, potrebbe essere basato sul fondamento giuridico dell'articolo 7, lettera b), anziché sull'articolo 7, lettera f).

### **Esempio 15: procedura per la denuncia delle irregolarità in ottemperanza agli obblighi giuridici vigenti nei paesi extra UE**

Una filiale UE di un gruppo statunitense istituisce una procedura limitata per la denuncia delle irregolarità volta a riscontrare gravi violazioni delle norme nel settore contabile e finanziario. Le entità del gruppo sono soggette a un codice di buona governance che prevede un rafforzamento delle procedure di controllo interno e gestione del rischio. In virtù delle sue attività internazionali, la filiale dell'UE è tenuta a fornire dati finanziari affidabili ad altri membri del gruppo negli Stati Uniti. La procedura è concepita in modo tale da essere conforme sia alla normativa degli USA che agli orientamenti forniti dalle autorità nazionali di protezione dei dati nell'UE.

Tra le garanzie, i dipendenti ricevono chiare indicazioni riguardo alle circostanze in cui deve essere utilizzata la procedura, sia mediante sessioni di formazione che con altri mezzi. Il personale è invitato a non abusare della procedura, per esempio formulando affermazioni false o infondate nei confronti di altri membri; ai dipendenti si spiega altresì che, se preferiscono, possono utilizzare la procedura in maniera anonima o che, se lo desiderano, possono identificarsi. In quest'ultimo caso, i dipendenti sono informati delle circostanze in cui i dati che li identificano saranno trasmessi al loro datore di lavoro o trasferiti ad altre agenzie.

Se la procedura dovesse essere istituita ai sensi del diritto dell'UE o del diritto di uno Stato membro dell'Unione europea, il trattamento potrebbe fondarsi sull'articolo 7, lettera c). Tuttavia, gli obblighi giuridici vigenti nei paesi extra UE non sono considerati come un obbligo giuridico ai fini dell'articolo 7, lettera c), e di conseguenza tale obbligo non potrebbe legittimare il trattamento ai sensi dell'articolo 7, lettera c). Ciononostante, il trattamento potrebbe essere basato sull'articolo 7, lettera f), qualora esista, per esempio, un interesse legittimo a garantire la stabilità dei mercati finanziari o a combattere la corruzione e a patto che la procedura preveda garanzie sufficienti, conformemente agli orientamenti forniti dalle competenti autorità di regolamentazione nell'UE.

### **Esempio 16: procedura “interna” per la denuncia delle irregolarità priva di procedure coerenti**

Una società di servizi finanziari decide di istituire una procedura per la denuncia delle irregolarità poiché sospetta che tra il personale i furti e la corruzione siano diffusi e intende incoraggiare i dipendenti a fornire informazioni gli uni sugli altri. Per risparmiare, la società decide di gestire la procedura internamente affidandola a membri del suo ufficio “Risorse umane”. Per incentivare i dipendenti a utilizzare la procedura, offre una ricompensa in denaro “senza richiesta di specifiche condizioni” ai dipendenti le cui attività di denuncia delle irregolarità portino all'individuazione di comportamenti scorretti e al recupero degli importi.

La società ha effettivamente un interesse legittimo a individuare e a prevenire i furti e la corruzione. Tuttavia, la sua procedura per la denuncia delle irregolarità è talmente mal concepita e priva di garanzie che rispetto agli interessi della società prevalgono sia gli interessi che il diritto alla tutela della vita privata dei suoi dipendenti, in particolare di coloro che potrebbero essere vittime di false segnalazioni fornite esclusivamente per ottenere un profitto finanziario. Il fatto che la procedura sia gestita internamente anziché in maniera indipendente rappresenta un altro problema in questo caso, al pari della mancanza di formazione e orientamenti sull'utilizzo della procedura.

**Esempio 17: controlli biometrici in un laboratorio di ricerca**

Un laboratorio di ricerca scientifica che lavora con virus letali utilizza un sistema di accesso biometrico a causa del rischio elevato che sussisterebbe per la salute pubblica nel caso in cui questi virus dovessero uscire dalla struttura. Sono applicate garanzie adeguate, compreso il fatto che i dati biometrici sono conservati sui tesserini personali dei dipendenti e non in un sistema centralizzato.

Benché i dati siano sensibili in senso ampio, il motivo per cui sono trattati è di interesse pubblico. Questo e il fatto che i rischi di utilizzo improprio siano ridotti dall'uso appropriato di garanzie rendono l'articolo 7, lettera f), una base adeguata per il trattamento.

**Esempio 18: utilizzo di telecamere nascoste per individuare visitatori e dipendenti che fumano**

Un'impresa utilizza telecamere nascoste per individuare dipendenti e visitatori che fumano in aree dell'edificio in cui non è consentito farlo.

Sebbene il responsabile del trattamento abbia un interesse legittimo a garantire il rispetto delle norme antifumo, i mezzi utilizzati per conseguire questo obiettivo sono, in linea generale, sproporzionati e inutilmente invasivi. Esistono metodi meno invasivi e più trasparenti (quali rilevatori di fumo e cartelli visibili). Il trattamento non è pertanto conforme all'articolo 6, che prevede che i dati non siano "eccedenti" rispetto alle finalità per le quali vengono rilevati o successivamente trattati. Al tempo stesso, il trattamento probabilmente non soddisferà i criteri del test comparativo di cui all'articolo 7, lettera f).

*Ricerca scientifica*

**Esempio 19: studi sugli effetti del divorzio e della disoccupazione genitoriale sul rendimento scolastico dei minori**

Nel quadro di un programma di ricerca adottato dal governo e autorizzato da un comitato etico competente, si effettua uno studio sulla relazione esistente tra divorzio, disoccupazione dei genitori e rendimento scolastico dei minori. Lo studio si concentra tuttavia su questioni che, pur non essendo classificate come "categorie particolari di dati", sarebbero ritenute informazioni personali molto intime da un gran numero di famiglie. Lo studio permetterà di destinare una speciale assistenza educativa ai minori che potrebbero altrimenti essere interessati dal fenomeno dell'assenteismo, registrare uno scarso rendimento scolastico, essere vittime della disoccupazione in età adulta o diventare soggetti a rischio di criminalità. La legge dello Stato membro interessato autorizza espressamente il trattamento dei dati personali (diversi dalle categorie particolari di dati) a fini di ricerca, purché lo studio sia necessario a salvaguardare interessi pubblici importanti e sia condotto nel rispetto di garanzie adeguate, che sono successivamente descritte nel dettaglio nella normativa di attuazione. Questo quadro giuridico prevede obblighi specifici, ma anche un quadro di responsabilità che permette di valutare caso per caso l'ammissibilità della ricerca (qualora sia svolta senza il consenso delle persone interessate) e le misure specifiche che devono essere adottate per proteggere gli interessati.

Il ricercatore gestisce uno strumento di ricerca sicuro e, in condizioni di sicurezza, ottiene le informazioni pertinenti da uffici anagrafici, tribunali, agenzie per l'occupazione e scuole. Il centro di ricerca esamina minuziosamente le identità delle persone affinché sia possibile collegare i dati relativi al divorzio, alla disoccupazione e all'istruzione, ma senza rivelare le identità "civiche" degli individui, ad esempio i loro nomi e indirizzi. Tutti i dati originali sono poi irrimediabilmente cancellati. Sono adottate anche altre misure volte a garantire la separazione funzionale (ossia i dati saranno utilizzati solo a fini di ricerca) e a ridurre qualsiasi ulteriore rischio di reidentificazione.

I membri del personale che lavorano presso il centro di ricerca ricevono una rigorosa formazione in materia di sicurezza e sono perseguibili a livello personale (eventualmente anche penale) per qualsivoglia violazione della sicurezza di cui sono responsabili. Si utilizzano misure tecniche e organizzative volte per esempio a garantire che il personale che adopera chiavette USB non possa rimuovere i dati personali dallo strumento.

È nell'interesse legittimo del centro di ricerca svolgere lo studio, che ha un forte interesse pubblico. È anche nell'interesse legittimo di enti per l'occupazione e l'istruzione nonché di altri organismi coinvolti nell'iniziativa, poiché li aiuterà a programmare e a fornire servizi a coloro che più ne hanno bisogno. Gli aspetti dello studio riguardanti la tutela della vita privata sono stati ben concepiti e le garanzie in atto indicano che sugli interessi legittimi delle organizzazioni che partecipano alla realizzazione dello studio non prevalgono gli interessi o i diritti alla tutela della vita privata dei genitori o dei minori i cui dati erano alla base della ricerca.

#### **Esempio 20: studio di ricerca sull'obesità**

Un'università vuole realizzare uno studio sui livelli di obesità infantile in alcune città e comunità rurali. Benché in generale abbia difficoltà ad avere accesso ai dati pertinenti da parte di scuole e altri istituti, l'università riesce di fatto a persuadere alcune decine di insegnanti scolastici a monitorare per un certo periodo di tempo gli alunni delle loro classi che appaiono obesi e a rivolgere loro domande riguardo alla dieta seguita, ai livelli di attività fisica praticata, all'utilizzo di giochi elettronici e così via. Questi insegnanti registrano anche i nomi e gli indirizzi degli alunni intervistati affinché possa essere inviato loro un buono per l'acquisto di musica online come ricompensa per avere preso parte alla ricerca. Successivamente i ricercatori compilano una banca dati correlando i livelli di obesità dei bambini con l'attività fisica e altri fattori. Le copie cartacee dei questionari completati (comunque in un formato tramite il quale è possibile individuare bambini specifici) sono conservate negli archivi dell'università per un periodo di tempo indeterminato e senza misure di sicurezza adeguate. Le fotocopie di tutti i questionari sono condivise su richiesta con tutti i laureati o i dottorandi in medicina dello stesso ateneo o di università partner nel mondo che sono interessati all'ulteriore utilizzo dei dati della ricerca.

Benché l'università abbia un interesse legittimo a condurre lo studio, esistono alcuni aspetti del progetto di ricerca da cui si evince che su tale interesse prevalgono gli interessi e i diritti alla tutela della vita privata dei minori. Oltre alla metodologia di ricerca, che è priva di rigore scientifico, il problema deriva in particolare dalla mancanza di approcci di rafforzamento della tutela della vita privata nel progetto di ricerca nonché dall'ampio accesso ai dati personali raccolti. I dati dei minori non sono mai codificati o anonimizzati e non sono adottate altre misure per garantire la sicurezza dei dati o la separazione funzionale. Non è stato

nemmeno ottenuto un consenso valido ai sensi dell'articolo 7, lettera a), e dell'articolo 8, paragrafo 2, lettera a), e non è chiaro se ai minori o ai loro genitori sia stato spiegato per quale finalità saranno utilizzati o con chi saranno condivisi i loro dati.

### ***Obbligo giuridico vigente in un paese terzo***

#### **Esempio 21: ottemperanza alle disposizioni fiscali di un paese terzo**

Le banche dell'UE raccolgono e trasferiscono alcuni dati dei loro clienti per consentire a questi ultimi di ottemperare agli obblighi fiscali vigenti in un paese terzo. La raccolta e il trasferimento sono specificati e avvengono alle condizioni e nel rispetto delle garanzie concordate tra l'UE e il paese estero nell'ambito di un accordo internazionale.

Benché di per sé un obbligo vigente in un paese terzo non possa essere considerato come una base legittima per il trattamento ai sensi dell'articolo 7, lettera c), tale obbligo potrebbe essere ritenuto un motivo di liceità se fosse sancito da un accordo internazionale. In quest'ultimo caso il trattamento potrebbe essere considerato necessario per adempiere un obbligo legale integrato nel quadro giuridico interno dall'accordo internazionale. Tuttavia, in assenza di accordi di questo tipo, la raccolta e il trasferimento dovranno essere valutati conformemente ai criteri di cui all'articolo 7, lettera f), e potranno essere ritenuti ammissibili solo qualora esistano garanzie adeguate come quelle approvate dall'autorità di protezione dei dati competente (cfr. anche il precedente *Esempio 15*).

#### **Esempio 22: trasferimento di dati relativi a dissidenti**

Una società dell'UE trasferisce, su richiesta, dati riguardanti residenti stranieri a un regime oppressivo di un paese terzo che vuole avere accesso ai dati di dissidenti (per esempio, i loro dati relativi al traffico di e-mail, il contenuto dei loro messaggi di posta elettronica, la cronologia delle loro esplorazioni o i loro messaggi privati sui social network).

In questo caso, a differenza dell'esempio precedente, non esiste un accordo internazionale che permetterebbe di applicare l'articolo 7, lettera c), come fondamento giuridico. Inoltre, alcuni elementi depongono a sfavore dell'articolo 7, lettera f), come fondamento adeguato per il trattamento. Anche se il responsabile del trattamento potrebbe avere un interesse economico a garantire che rispetta le richieste formulate da un governo straniero (altrimenti potrebbe ricevere dal governo del paese terzo un trattamento meno favorevole rispetto a quello riservato ad altre società), la legittimità e la proporzionalità del trasferimento sono estremamente discutibili nel quadro della Carta dei diritti fondamentali dell'UE. L'impatto potenzialmente enorme che il trattamento potrebbe avere sulle persone interessate (per esempio discriminazione, detenzione, pena di morte) fa a sua volta pendere il bilanciamento nettamente a favore degli interessi e dei diritti degli interessati.

### ***Riutilizzo di dati disponibili al pubblico***

#### **Esempio 23: valutazione di politici<sup>126</sup>**

<sup>126</sup> Cfr. e operare anche un confronto con il precedente esempio 7.

Una ONG a difesa della trasparenza utilizza i dati sui politici disponibili al pubblico (promesse formulate al momento della loro elezione e dati effettivi sul voto) per valutarli in funzione del grado di mantenimento delle loro promesse.

Anche se l'impatto sui politici interessati potrebbe essere considerevole, il fatto che il trattamento, chiaramente finalizzato ad aumentare la trasparenza e la responsabilità, si basi su informazioni pubbliche nonché riguardanti le loro responsabilità pubbliche fa pendere il bilanciamento a favore dell'interesse del responsabile del trattamento<sup>127</sup>.

### ***Minori e altre persone vulnerabili***

#### **Esempio 24: sito web di informazione per gli adolescenti**

Il sito web di una ONG che offre consigli agli adolescenti su questioni quali abuso di stupefacenti, gravidanza indesiderata e abuso di alcolici raccoglie, attraverso il proprio server, dati relativi ai visitatori del sito. Subito dopo li rende anonimi e li trasforma in dati statistici generali riguardanti le parti del sito web più consultate da visitatori provenienti da regioni geografiche differenti del paese.

L'articolo 7, lettera f), potrebbe essere utilizzato come fondamento giuridico anche se i dati interessati riguardano soggetti vulnerabili, poiché il trattamento è di interesse pubblico e sono poste in essere garanzie rigorose (i dati sono immediatamente anonimizzati e utilizzati solo per la creazione di statistiche), fattori che contribuiscono a far pendere il bilanciamento a favore del responsabile del trattamento.

### ***Soluzioni basate sul concetto di “privacy by design” (tutela della vita privata fin dalla progettazione) come garanzie supplementari***

#### **Esempio 25: accesso a numeri di cellulare di utenti e non utenti di un'applicazione: “confronta e dimentica”**

I dati personali di alcuni soggetti sono trattati per verificare se in passato tali persone avevano già fornito il loro consenso inequivocabile (ad esempio, “confronta e dimentica” come garanzia).

Uno sviluppatore di applicazioni è tenuto a ottenere il consenso inequivocabile degli interessati per trattare i loro personali: per esempio, lo sviluppatore di applicazioni vuole avere accesso all'intera rubrica elettronica degli utenti dell'applicazione, compresi i numeri di cellulare di recapiti che non utilizzano l'applicazione. Per poterlo fare, potrebbe prima dover valutare se i titolari dei numeri di cellulare contenuti nelle rubriche degli utenti dell'applicazione hanno fornito il loro consenso inequivocabile (ai sensi dell'articolo 7, lettera a)) al trattamento dei loro dati personali.

<sup>127</sup> Come negli *Esempi 1 e 2*, siamo partiti dal presupposto che la pubblicazione sia accurata e proporzionata; l'assenza di garanzie e altri fattori potrebbero modificare l'equilibrio degli interessi a seconda delle circostanze del caso.

Per questo trattamento iniziale limitato (ossia accesso in lettura a breve termine all'intera rubrica di un utente dell'applicazione), lo sviluppatore dell'applicazione potrebbe basarsi sul fondamento giuridico costituito dall'articolo 7, lettera f), fatte salve talune garanzie. Tali garanzie dovrebbero comprendere misure tecniche e organizzative volte a garantire che la società utilizzi questo accesso solo per aiutare l'utente a individuare quali dei suoi contatti sono già utenti e avevano pertanto già fornito in passato alla società il loro consenso inequivocabile a raccogliere e trattare i numeri di telefono a tal fine. I numeri di cellulare dei non utenti possono essere raccolti e utilizzati solo al fine strettamente limitato di verificare se tali persone hanno fornito il loro consenso inequivocabile al trattamento dei dati personali e devono essere immediatamente cancellati subito dopo.

### *Combinazione di dati personali tra servizi web*

#### **Esempio 26: combinazioni di dati personali tra servizi web**

Una società di Internet che fornisce vari servizi tra cui motori di ricerca, condivisione di video, siti di socializzazione, sviluppa una politica sulla tutela della vita privata contenente una clausola che le permette "di combinare tutte le informazioni personali" raccolte su ciascuno dei suoi utenti in relazione ai differenti servizi da essi utilizzati, senza definire alcun periodo di conservazione dei dati. La società sostiene di agire in tal senso al fine di "garantire la migliore qualità possibile del servizio".

La società mette alcuni strumenti a disposizione di differenti categorie di utenti affinché possano esercitare i loro diritti (ad esempio, disattivare la pubblicità mirata, opporsi all'impostazione di un tipo specifico di cookie).

Tuttavia, gli strumenti disponibili non permettono agli utenti di controllare effettivamente il trattamento dei loro dati: gli utenti non possono controllare le combinazioni specifiche dei loro dati tra i servizi né opporsi alla combinazione di dati che li riguardano. Nel complesso, esiste uno squilibrio tra l'interesse legittimo della società e la protezione dei diritti fondamentali degli utenti e l'articolo 7, lettera f), non deve essere invocato come fondamento giuridico per il trattamento. Sarebbe più opportuno utilizzare l'articolo 7, lettera a), come fondamento giuridico purché siano soddisfatte le condizioni per un consenso valido.