ARTICOLO 29 GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI

01248/07/IT
WP 136

Parere 4/2007 sul concetto di dati personali

adottato il 20 giugno

istituito a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1],

visti gli articoli 29 e 30, paragrafo 1, lettera a), e paragrafo 3 della richiamata direttiva, e l'articolo 15, paragrafo 3 della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002,

visto l'articolo 255 del trattato CE e il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione,

visto il proprio regolamento interno,

HA ADOTTATO IL SEGUENTE PARERE:

[1] Gazzetta ufficiale L 281 del 23.11.1995, pag. 31, consultabile su: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. INTRODUZIONE

Il Gruppo è consapevole della necessità di condurre un'analisi approfondita del concetto di dati personali. Le informazioni sulle prassi attualmente in uso negli Stati membri dell'UE indicano incertezze e diversità da uno Stato all'altro in relazione a importanti aspetti di tale concetto, che potrebbero avere ripercussioni sul corretto funzionamento dell'attuale quadro giuridico sulla protezione dei dati a seconda dei contesti. L'esito di questa analisi, che verte su un elemento cruciale per l'applicazione e l'interpretazione delle norme sulla protezione dei dati, è destinato ad avere un forte impatto su varie questioni importanti, in particolare per alcune tematiche come la gestione dell'identità nel quadro dell'*e-Government* e dell'*e-Health* e della tecnologia RFID.

Obiettivo del presente parere è arrivare a una comprensione comune del concetto di dati personali, delle situazioni in cui andrebbe applicata la legislazione nazionale sulla protezione dei dati e delle relative modalità di applicazione. Formulare una definizione comune del concetto di dati personali equivale a definire ciò che rientra e ciò che non rientra nell'ambito di applicazione della normativa sulla protezione dei dati. Corollario di questo lavoro è dare un orientamento su come applicare la normativa nazionale sulla protezione dei dati ad alcune categorie di situazioni a livello europeo, contribuendo così all'applicazione uniforme di tali norme, che è poi una funzione centrale del Gruppo ex articolo 29.

Il presente documento si avvale di esempi tratti dalla pratica nazionale delle autorità europee per la protezione dei dati personali, per sostenere e illustrare l'analisi. Molti degli esempi sono stati adattati ai fini esclusivi del presente contesto.

II. CONSIDERAZIONI GENERALI E QUESTIONI POLITICHE

La direttiva contiene una nozione ampia di dati personali

La definizione di dati personali contenuta nella direttiva 95/46/CE (nel prosieguo «la direttiva sulla protezione dei dati» o «la direttiva») recita:

"Per «dati personali» si intende qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".

Si noti che questa definizione rispecchia la volontà del legislatore europeo di avere un'ampia nozione di «dati personali» in tutto il processo legislativo. La proposta originale della Commissione spiegava che "*come per la convenzione 108, viene adottata un'ampia definizione al fine di comprendere tutte le informazioni che possono essere connesse ad una persona*"[2]. La proposta modificata della Commissione precisava inoltre che "*la proposta modificata soddisfa la volontà del Parlamento di avere una definizione di «dati personali» il più generale possibile, al fine di includere tutte le informazioni riguardanti una persona identificabile*"[3], volontà che anche il Consiglio ha tenuto in considerazione nella sua posizione comune[4].

Obiettivo delle norme contenute nella direttiva è tutelare le persone

Gli articoli 1 della direttiva 95/46/CE e della direttiva 2002/58/CE dichiarano chiaramente lo scopo ultimo di tali norme: proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla privacy, in relazione al trattamento dei dati personali. Questo importantissimo elemento va tenuto presente nell'interpretazione e nell'applicazione delle norme di entrambi gli strumenti, in quanto può svolgere un ruolo sostanziale nel determinare come vada applicata la direttiva ad una serie di situazioni in cui i diritti degli individui non sono a rischio, e può mettere in guardia contro interpretazioni che lascerebbero le persone prive di un'adeguata tutela.

L'ambito di applicazione della direttiva esclude diverse attività e la flessibilità contraddistingue il testo ai fini una risposta giuridica appropriata a seconda delle specifiche circostanze

Nonostante l'ampio concetto di «dati personali» e di «trattamento» contenuto nella direttiva, il semplice fatto che una data situazione possa essere considerata come implicante «il trattamento di dati personali» nel senso della definizione non è di per sé sufficiente per determinare l'applicazione delle norme della direttiva, in particolare ai sensi dell'articolo 3. A parte le esenzioni dovute alle competenze del diritto

2 COM (90) 314 def. del 13.9.1990, pag. 19 (commento all'articolo 2)
3 COM (92) 422 def. del 28.10.1992, pag. 10 (commento all'articolo 2)
4 Posizione comune (CE) n. 1/95, adottata dal Consiglio il 20 febbraio 1995, GU C 93 del 13.4.1995, pag. 20

comunitario, le esenzioni dell'articolo 3 tengono conto della modalità tecnica di trattamento (manuale non strutturata) e della finalità d'uso (per attività a carattere esclusivamente personale o domestico di una persona fisica). Anche in caso di trattamento dei dati personali nell'ambito della direttiva, non si applicheranno necessariamente tutte le norme in quella contenute. Diverse disposizioni della direttiva lasciano un margine sostanziale di flessibilità per raggiungere un giusto equilibrio tra la protezione dei diritti della persona interessata e i legittimi interessi dei responsabili del trattamento dei dati, di terzi e dell'interesse pubblico eventuale. Esempi di tali disposizioni figurano all'articolo 6 (conservazione dei dati nell'arco di tempo necessario al conseguimento delle finalità per le quali sono rilevati), all'articolo 7, lettera f) (equilibrio degli interessi che giustifichi il trattamento), all'ultima frase dell'articolo 10, lettera c) e all'articolo 11, paragrafo 1, lettera c) (informazioni alla persona interessata per garantire un trattamento leale), oppure all'articolo 18 (esonero dall'obbligo di notificazione), per citarne solo alcuni.

Non bisogna ampliare troppo l'ambito di applicazione delle norme sulla protezione dei dati

Un effetto indesiderato sarebbe che le norme di protezione dei dati si applichino a situazioni che non erano destinate ad essere disciplinate da tali norme e per le quali il legislatore non le aveva previste. Le esenzioni materiali di cui al richiamato articolo 3 e le chiarificazioni dei considerando 26 e 27 della direttiva mostrano come il legislatore intenda vedere applicata la protezione dei dati.

Una limitazione riguarda il modo di trattare i dati. Al riguardo è utile ricordare i motivi per cui sono nate le prime leggi sulla protezione dei dati negli anni Settanta: le nuove tecnologie sotto forma di trattamento elettronico dei dati permettevano infatti un accesso più semplice e diffuso ai dati personali rispetto alle tradizionali forme di trattamento. Di conseguenza, la protezione dei dati ai sensi della direttiva mira a proteggere le forme di trattamento che tipicamente presentano un rischio più alto di "facile accesso ai dati personali" (considerando 27). Il trattamento non automatizzato di dati personali rientra nell'ambito di applicazione della direttiva soltanto se i dati sono contenuti o destinati a figurare negli archivi (articolo 3).

Un'altra limitazione generale all'applicazione della protezione dei dati a norma della direttiva sarebbe il trattamento dei dati in circostanze in cui non "possono essere ragionevolmente utilizzati" (considerando 26) i mezzi necessari per identificare la persona interessata. Tale questione verrà discussa più avanti.

Ma bisogna anche evitare un'indebita restrizione dell'interpretazione del concetto di dati personali

Nei casi in cui un'applicazione meccanicistica di ogni singola disposizione della direttiva comporti a priori conseguenze estremamente gravose o addirittura assurde, occorre verificare 1) se la situazione rientra nel campo di applicazione della direttiva, in particolare ai sensi dell'articolo 3; 2) qualora rientri in tale campo, se la direttiva stessa o le disposizioni nazionali di applicazione non ammettono esenzioni o semplificazioni in situazioni particolari, e ciò per dare una risposta giuridica appropriata che protegga i diritti della persona e gli interessi in gioco. È preferibile non restringere indebitamente l'interpretazione della definizione di dati personali, ma notare piuttosto che vi è molta flessibilità nell'applicazione delle norme ai dati.

Le autorità nazionali per la protezione dei dati personali svolgono un ruolo essenziale al riguardo nel quadro della loro missione di controllo dell'applicazione delle norme sulla protezione dei dati, interpretando le disposizioni giuridiche e dando un orientamento concreto ai responsabili del trattamento dei dati e alle persone interessate. Esse dovrebbero approvare una definizione sufficientemente ampia da anticipare le evoluzioni e cogliere tutte le "zone d'ombra" nel suo campo di applicazione, facendo un uso legittimo della flessibilità offerta dalla direttiva. Di fatto, il testo della direttiva invita allo sviluppo di una politica che combini un'ampia interpretazione della nozione di dati personali con un adeguato equilibrio nell'applicazione delle norme della direttiva.

III. ANALISI DELLA DEFINIZIONE DI "DATI PERSONALI" SECONDO LA DIRETTIVA SULLA PROTEZIONE DEI DATI

La definizione nella direttiva contiene quattro elementi fondamentali che verranno analizzati separatamente ai fini del presente documento:

- "qualsiasi informazione"
- "concernente"
- "persona fisica"
- "identificata o identificabile"

I quattro elementi fondamentali sono strettamente connessi fra loro e si alimentano reciprocamente. Tuttavia, ai fini della metodologia del presente documento, ciascun elemento sarà trattato separatamente.

1. PRIMO ELEMENTO: "QUALSIASI INFORMAZIONE"

L'espressione "qualsiasi informazione" nella direttiva segnala chiaramente la volontà del legislatore di definire un ampio concetto di dati personali. La formulazione richiede un'ampia interpretazione.

Dal punto di vista della natura dell'informazione, il concetto di dati personali comprende qualsiasi tipo di affermazione su una persona; può quindi includere informazioni "oggettive" come la presenza di una data sostanza nel sangue di una persona, ma anche informazioni "soggettive" come opinioni o valutazioni. Quest'ultimo tipo di informazioni rappresenta un'ampia parte del trattamento dei dati personali nei settori bancario, per la valutazione dell'affidabilità di chi richiede un prestito ("Tizio è un cliente affidabile") e assicurativo ("Tizio probabilmente non morirà presto"), o nel mercato del lavoro ("Tizio è un buon lavoratore e merita una promozione").

Perché l'informazione diventi un 'dato personale' non è necessario che sia vera o dimostrata. In effetti le norme sulla protezione dei dati già prevedono che le informazioni possano non essere corrette e conferiscono all'interessato il diritto di accesso a quelle informazioni e di contestarle con mezzi d'impugnazione adeguati[5].

[5] La rettifica è possibile aggiungendo commenti o ricorrendo ad adeguati rimedi giuridici come i mezzi di impugnazione.

Dal punto di vista del contenuto dell'informazione, il concetto di dati personali comprende qualsiasi tipo d'informazioni, sia quelle personali, considerate "dati sensibili" all'articolo 8 della direttiva per via della natura rischiosa, sia quelle più generali. L'espressione "dati personali" comprende informazioni sulla vita privata e familiare in senso stretto, ma anche sulle attività di qualunque tipo, come sui rapporti di lavoro o sul comportamento economico e sociale, di una persona. I dati personali comprendono quindi informazioni sulle persone, a prescindere dalla posizione o dalle capacità (in quanto consumatori, pazienti, lavoratori, clienti, ecc.).

Esempio n. 1: Abitudini e pratiche professionali

Le informazioni sulle prescrizioni dei farmaci (ad esempio, numero identificativo, nome, potenza e produttore del farmaco, prezzo di vendita del farmaco, nuovo o ricarica, motivi dell'uso, nome, cognome e numero di telefono di chi effettua la prescrizione, ecc.), sia sotto forma di singola prescrizione o di elementi caratteristici tratti da una serie di prescrizioni, possono essere considerate dati personali relativi al medico che prescrive il farmaco, anche se il paziente resta anonimo. Pertanto, fornire informazioni su prescrizioni effettuate da medici identificati o identificabili a produttori di farmaci su prescrizione costituisce una comunicazione di dati personali a terzi ai sensi della direttiva.

Questa interpretazione trova conferma nella formulazione della stessa direttiva. Da un lato, è necessario considerare che il concetto di vita privata e vita familiare è ampio, come ha chiaramente statuito la Corte europea dei diritti umani[6]. Dall'altro, le norme sulla protezione dei dati personali vanno oltre la protezione dell'ampio concetto del diritto al rispetto della vita privata e familiare. Si noti che la Carta dei diritti fondamentali dell'Unione europea sancisce la protezione dei dati personali all'articolo 8 quale diritto autonomo, separato e differente dal rispetto della vita privata di cui all'articolo 7, e lo stesso avviene a livello nazionale in alcuni Stati membri. Questa interpretazione è conforme al disposto dell'articolo 1, paragrafo 1, che protegge i "diritti e le libertà fondamentali delle persone fisiche, e *in particolare* [ma non esclusivamente] il diritto alla vita privata". Di conseguenza, la direttiva fa specifico riferimento al trattamento dei dati personali al di là dei contesti domestici e familiari, come quello previsto dal diritto del lavoro (articolo 8, paragrafo 2, lettera b)), per le condanne penali, le sanzioni amministrative o i procedimenti civili (articolo 8, paragrafo 5), oppure per l'invio di materiale pubblicitario (articolo 14, lettera b)). La Corte di giustizia delle Comunità europee[7] ha approvato questo ampio approccio.

---

6 Sentenza della Corte europea dei diritti umani nella causa Amann/Switzerland del 16.2.2000, §65 : *"[...] il termine "vita privata" non va interpretato in modo restrittivo. In particolare, il rispetto della vita privata comprende il diritto a stabilire e sviluppare relazioni con altri esseri umani; inoltre, non vi è alcuna ragione di principio per giustificare l'esclusione di attività di natura professionale o imprenditoriale dalla nozione di "vita privata" (v. sentenza Niemietz/Germania del16 dicembre 1992, serie A n. 251-B, pagg. 33-34, § 29, e la sentenza Halford summenzionata, pagg. 1015-16, § 42). Quell'ampia interpretazione corrisponde a quella della convenzione del Consiglio d'Europa del 28 gennaio 1981 [...]*"

7 Sentenza della Corte di giustizia delle Comunità europee C-101/2001del 6.11.2003 (Lindqvist), §24: "*La nozione di «dati personali» accolta nell'articolo 3, n. 1, della direttiva 95/46 comprende, conformemente alla definizione che figura nell'articolo 2, lettera a), di questa, «qualsiasi informazione concernente una persona fisica identificata o identificabile». Tale nozione ricomprende certamente il nome di una persona accostato al suo recapito telefonico o ad informazioni relative alla sua situazione lavorativa o ai suoi passatempo*".

Dal punto di vista del formato dell'informazione o del supporto usato, il concetto di dati personali comprende le informazioni disponibili in qualsiasi forma, alfabetica, numerica, grafica, fotografica o acustica, le informazioni registrate su carta e le informazioni conservate nella memoria di un computer attraverso un codice binario o in una videocassetta. Questa è la logica conseguenza dell'includere il trattamento automatico dei dati personali nell'ambito di applicazione della direttiva. Da questo punto di vista, i dati in forma di suoni e immagini costituirebbero dati personali in quanto possono rappresentare informazioni su una persona. Al riguardo, il riferimento specifico ai dati sotto forma di suoni e immagini dell'articolo 33 della direttiva deve essere compreso come conferma e chiarificazione del fatto che questo tipo di dati rientra effettivamente nel suo ambito di applicazione (a condizione che ricorrano tutte le altre condizioni) e che la direttiva è ad essi applicabile. Di fatto, è questo il presupposto logico per la disposizione del richiamato articolo che cerca di valutare se le norme della direttiva danno risposte giuridiche adeguate in quei campi. Ciò viene chiarito ulteriormente nel considerano 14 che recita: "*considerando che la presente direttiva dovrebbe applicarsi al trattamento dei dati in forma di suoni e immagini relativi a persone fisiche, vista la notevole evoluzione in corso nella società dell'informazione delle tecniche per captare, trasmettere, manipolare, registrare, conservare o comunicare siffatti dati"*. D'altro canto, non è necessario che le informazioni siano considerate dati personali contenuti in una base dati o in un archivio strutturati. Anche le informazioni contenute sotto forma di testo libero in un documento elettronico possono essere considerate dati personali, a condizione che sussistano gli altri criteri della definizione di dati personali. Un messaggio di posta elettronica, ad esempio, contiene 'dati personali'.

Esempio n. 2: *Phone banking*

Nei servizi di *phone banking* il cliente dà istruzioni alla banca e la sua voce viene registrata su nastro; tali istruzioni dovrebbero essere considerate dati personali.

Esempio n. 3: Videosorveglianza

Le immagini registrate da un sistema di videosorveglianza possono essere dati personali nella misura in cui le persone riprese sono riconoscibili.

Esempio n. 4: Disegno di un bambino

Nell'ambito di un test neuropsichiatrico ai fini di un procedimento giudiziario per l'affidamento di una bambina, è stato presentato un suo disegno dei familiari. Il disegno dà informazioni sullo stato d'animo della bambina e sui suoi sentimenti per i diversi membri della famiglia. Queste informazioni possono di per sé costituire "dati personali" in quanto rivelano informazioni sulla bambina (la sua salute mentale), ma anche sul comportamento della madre o del padre. I genitori possono quindi, in questa fattispecie, esercitare il diritto di accesso a tale informazione specifica.

In questo contesto meritano un cenno particolare i dati biometrici. Questi dati possono essere definiti proprietà biologiche, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità. Esempi tipici di dati biometrici sono le impronte digitali, la struttura della retina, del volto, la voce, ma anche la forma della mano, gli elementi caratteristici delle vene o perfino alcune capacità profondamente

radicate nella persona o altre caratteristiche comportamentali (la firma, la pressione esercitata sui tasti, il modo particolare di camminare o parlare, ecc...)

Peculiarità dei dati biometrici è che li si può considerare sia come *contenuto* delle informazioni su una particolare persona (Tizio ha queste impronte digitali), sia come elemento atto a stabilire un *collegamento* tra un'informazione e una persona (questo oggetto è stato toccato da qualcuno che ha queste impronte digitali e queste impronte corrispondono a Tizio; quindi questo oggetto è stato toccato da Tizio). Possono quindi fungere da "identificatori". Di fatto, grazie al loro collegamento univoco ad una persona specifica, i dati biometrici possono essere impiegati per identificare una persona. Questa doppia natura si riscontra anche nei dati sul DNA che forniscono informazioni sul corpo umano e consentono l'identificazione univoca e inequivocabile di una persona.

I campioni di tessuti umani (un campione di sangue) sono fonti da cui vengono estratti dati biometrici, ma non sono di per sé dati biometrici (le impronte digitali sono dati biometrici, non il dito). Ne consegue che l'estrazione di informazioni da campioni equivale a una raccolta di dati personali, e che ad essa si applicano le norme della direttiva. La raccolta, la conservazione e l'impiego di campioni di tessuti possono di per sé essere soggetti a una serie di norme specifiche[8].

2. SECONDO ELEMENTO: “CONCERNENTE”

Questo elemento fondamentale della definizione è d'importanza cruciale, poiché è molto importante stabilire con precisione le relazioni/i collegamenti che contano, e come distinguerli.

Il linea generale, un'informazione si può considerare “concernente” una persona se la *riguarda* .

In molte situazioni questa relazione può essere stabilita facilmente. Per esempio, i dati registrati nel fascicolo personale di una certa persona presso l'ufficio del personale “concernono” la sua situazione in qualità di impiegato. Lo stesso avviene per i risultati di un test medico di un paziente contenuti nella sua cartella clinica, o per l'immagine di una persona filmata nel corso di un'intervista.

Possono essere menzionate diverse altre situazioni, però, in cui non è sempre facile, come nei casi precedenti, determinare se le informazioni “concernono” una persona.

In alcune situazioni le informazioni trasmesse dai dati concernono in primo luogo oggetti e non persone. Questi oggetti appartengono di solito a qualcuno o possono subire l’influenza particolare di persone o esercitare un'influenza particolare su persone, oppure possono avere una sorta di vicinanza fisica o geografica a persone o ad altri oggetti. Solo indirettamente si può quindi considerare che tali informazioni concernono quelle persone o quegli oggetti.

Esempio n. 5: Valore di una casa

Il valore di una casa specifica costituisce un'informazione su un oggetto. Beninteso, le norme sulla protezione dei dati non si applicano se l’informazione è usata soltanto per

[8] Vedi raccomandazione del Consiglio d'Europa, Rec (2006) 4 del Comitato dei ministri agli Stati membri relativa alla ricerca sul materiale biologico di origine umana, del 15.3.2006.

illustrare il livello dei prezzi immobiliari in un dato quartiere. Però, in alcune circostanze, tale informazione meriterebbe di essere considerata anche come dato personale: la casa è in effetti una proprietà e in quanto tale servirà per determinare in che misura il proprietario è tassabile. Da questo punto di vista l'informazione costituisce indiscutibilmente un dato personale.

Una simile analisi vale anche quando i dati riguardano in primo luogo processi o eventi, ad esempio informazioni sul funzionamento di una macchina in cui è necessario l'intervento dell'uomo. Queste informazioni possono pertanto considerarsi "concernenti" una persona.

Esempio n. 6: Servizio di manutenzione di un'automobile

Il registro clienti di un meccanico o di un'officina contiene informazioni sull'automobile, sul chilometraggio, sulle date dei controlli, sui problemi tecnici e sulle condizioni materiali. Queste informazioni sono associate ad un numero di targa e a un numero di motore, che a loro volta possono essere collegati al proprietario. Quando un'officina stabilisce un nesso tra veicolo e proprietario, per la fatturazione, l'informazione "concernerà" il proprietario o il conducente. Se il nesso viene fatto con il meccanico che ha lavorato sul veicolo, per accertarne la produttività, l'informazione "concernerà" anche il meccanico.

Il Gruppo si è già interessato ai casi in cui un'informazione può essere considerata "concernente" una persona. Nel quadro delle discussioni sulla protezione dei dati in relazione alle etichette RFID, il Gruppo ha osservato che "*i dati concernono una persona se si riferiscono all'identità, alle caratteristiche o al comportamento di questa persona, o se tali informazioni vengono impiegate per stabilire o influenzare il modo in cui quella persona viene trattata o valutata*[9]".

Considerando i casi sopra indicati e su quella falsa riga, si potrebbe affermare che, per stabilire se i dati "concernono" una persona, dovrebbe ricorrere un elemento di "**contenuto**" OPPURE di "**finalità**" OPPURE di "**risultato**".

L'elemento di "**contenuto**" è presente nei casi in cui – secondo il senso più ovvio e più diffuso della parola "concernere" – l'informazione riguardante una particolare persona è fornita a prescindere dalla finalità del responsabile del trattamento o di terzi, o dal suo impatto sulla persona interessata. Un'informazione "concerne" una persona quando la "riguarda", e questo deve essere valutato alla luce delle circostanze del caso di specie. Ad esempio, i risultati di un'analisi medica concernono chiaramente il paziente, così come le informazioni contenute in un fascicolo sotto il nome di un dato cliente concernono chiaramente quel cliente. Ancora, le informazioni contenute in un'etichetta RFID o in un codice a barre incorporato nel documento d'identità di un dato individuo concernono quella persona, al pari delle informazioni contenute nei futuri passaporti con chip RFID.

Anche un elemento di "**finalità**" può far sì che le informazioni "concernano" una data persona. Tale elemento può essere considerato presente quando i dati sono usati o lo saranno probabilmente, tenendo conto di tutte le circostanze del caso di specie, al fine

[9] Documento del Gruppo n. WP 105: *Working document on data protection issues related to RFID technology*, adottato il 19.1.2005, pag. 8.

di valutare, trattare in un dato modo o influire sullo stato o sul comportamento di una persona.

Esempio n. 7: Registro chiamate di un telefono

Il registro chiamate di un telefono in una data società fornisce informazioni sulle chiamate effettuate da quel telefono collegato a una certa linea. Queste informazioni possono concernere diversi soggetti. Da un lato, la linea è a disposizione della società e questa è tenuta per contratto a pagare le chiamate. L'apparecchio telefonico è sotto il controllo di un impiegato negli orari di lavoro e si presume che le chiamate vengano effettuate da quell'impiegato. Il registro chiamate può anche fornire informazioni sulla persona chiamata. Il telefono può essere usato pure da altro personale autorizzato in assenza dell'impiegato (ad esempio, addetti alle pulizie). Per scopi diversi, le informazioni sull'utilizzo di quell'apparecchio possono essere messe in relazione con la società, l'impiegato o il personale addetto alle pulizie (ad esempio, per verificare l'ora in cui l'addetto alle pulizie lascia il luogo di lavoro, poiché è tenuto a confermare per telefono a che ora lascia i locali prima di chiuderli a chiave). Si noti che il concetto di dati personali qui si estende sia alle chiamate in entrata che a quelle in uscita, nella misura in cui entrambe contengono informazioni sulla vita privata, sui rapporti sociali e sulle comunicazioni delle persone.

Un terzo tipo di "concernente" una persona specifica emerge quando è presente un elemento di "**risultato**". Nonostante l'assenza di elementi di "contenuto" o di "finalità", è possibile considerare che i dati "concernono" una persona quando il loro impiego può avere un impatto sui diritti e sugli interessi di quella persona, tenendo conto di tutte le circostanze del caso di specie. Si noti che non è necessario che il risultato potenziale abbia un impatto importante. È sufficiente che la persona sia trattata in modo diverso rispetto ad altre in seguito al trattamento di tali dati.

Esempio n. 8: Impatto sui tassisti del controllo della posizione dei taxi per ottimizzarne il servizio

Una società di taxi installa un sistema di localizzazione satellitare per localizzare i taxi disponibili in tempo reale. Obiettivo del trattamento è offrire un servizio migliore e risparmiare carburante, assegnando ad ogni cliente il veicolo che si trova più vicino al suo indirizzo. Strettamente parlando, i dati necessari al funzionamento del sistema sono dati relativi ad automobili, non ai conducenti. La finalità del trattamento non è valutare le prestazioni dei tassisti, ad esempio ottimizzandone gli itinerari. Eppure, il sistema permette di monitorare le prestazioni dei tassisti e di controllare se rispettano i limiti di velocità, se scelgono itinerari adeguati, se sono al volante o se stanno facendo una pausa, ecc. Il sistema quindi può esercitare un forte impatto su queste persone e si può considerare che i dati da quello elaborati concernono anche persone fisiche. Il loro trattamento dovrebbe essere quindi soggetto alle norme sulla protezione dei dati.

Questi tre elementi (contenuto, finalità, risultato) vanno intesi come condizioni alternative e non già cumulative. In particolare, quando è presente l'elemento di contenuto non è necessario che siano presenti anche gli altri elementi perché si consideri che le informazioni concernono una persona. Oltre a ciò, la stessa informazione può concernere simultaneamente persone diverse, a seconda dell'elemento presente in relazione a ciascuna di esse: può concernere Tizio per via dell'elemento di "contenuto" (i dati riguardano chiaramente Tizio), e Caio per via dell'elemento di "finalità" (sarà usata al fine di trattare Caio in un determinato modo) e

Sempronio per via dell'elemento di "risultato" (avrà un probabile impatto sui diritti e sugli interessi di Sempronio). In altri termini, non è necessario che i dati siano "focalizzati" su una persona perché si possano considerare concernenti tale persona. Stando a questa analisi è indispensabile verificare, per ciascun dato specifico in base alle sue qualità, se concerne una data persona o meno. Allo stesso modo, il fatto che un'informazione possa concernere persone diverse deve essere tenuto presente nell'applicazione delle norme sostanziali (ad esempio, sulla portata del diritto di accesso).

Esempio n. 9: Informazioni contenute nel verbale di una riunione

Un esempio della necessità di effettuare la precedente analisi per ciascuna informazione separatamente riguarda le informazioni contenute nel verbale di una riunione, in cui tipicamente vengono registrate la presenza dei partecipanti Tizio, Caio e Sempronio, gli interventi di Tizio e Caio e una relazione dei lavori su alcune tematiche riassunti dall'autore del verbale, Sempronio. Come dato personale concernente Tizio si può considerare soltanto il fatto che ha partecipato alla riunione a una data ora e in un dato luogo e i suoi interventi. La presenza alla riunione di Caio, i suoi interventi e i suoi lavori su a una data questione riassunti da Sempronio NON sono dati personali di Tizio, anche se queste informazioni figurano nello stesso documento e anche se è stato Tizio a sollevare la questione da discutere alla riunione. Tali informazioni sono quindi escluse dal diritto di accesso di Tizio ai propri dati personali. Se e in che misura possano essere considerate dati personali di Caio e Sempronio dovrà essere determinato separatamente, usando l'analisi descritta in precedenza.

3. TERZO ELEMENTO: [PERSONA FISICA] “IDENTIFICATA O IDENTIFICABILE”

La direttiva impone che l'informazione riguardi una persona fisica “identificata o identificabile”. Da questo requisito derivano le seguenti considerazioni.

In linea generale, si può considerare “identificata” la persona fisica che, all'interno di un gruppo, è "distinta" da tutti gli altri membri. Di conseguenza, la persona fisica è “identificabile” quando, sebbene non sia stata ancora identificata, è possibile identificarla (come suggerisce il suffisso "-abile"). Questa seconda alternativa è quindi in pratica la condizione limite che determina se le informazioni rientrano nell'ambito di applicazione del terzo elemento.

L'identificazione si fonda di norma su informazioni particolari che possiamo chiamare “identificatori” e che hanno un rapporto particolarmente stretto e privilegiato con la persona interessata, ad esempio segni esterni riguardo all'aspetto, come l’altezza, il colore dei capelli, l'abbigliamento, ecc., oppure una qualità che non può essere percepita immediatamente, come la professione, una funzione, un nome, ecc. La direttiva fa riferimento a questi “identificatori” nella definizione di “dati personali” all'articolo 2 che afferma che una persona fisica *"può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"*.

Identificabile "direttamente" o "indirettamente"

Ulteriori chiarimenti sono contenuti nel commento agli articoli della proposta modificata della Commissione, per cui "*una persona può essere identificata direttamente attraverso il nome o indirettamente attraverso il numero di telefono, il numero identificativo della automobile, il numero di sicurezza sociale, del passaporto o una combinazione di criteri significativi che ne consentano il riconoscimento all'interno del gruppo al quale appartiene (età, occupazione, luogo di residenza, ecc.)".* Tale formulazione indica chiaramente che a determinare se questi identificatori sono sufficienti per effettuare l'identificazione è il contesto della situazione specifica. Un cognome molto comune non basterà a identificare una persona -cioè a distinguerla- tra l'intera popolazione di un paese, ma basterà con buone probabilità a identificare uno studente in una classe. Anche le informazioni ausiliarie, come "l'uomo che indossa un abito nero" possono permettere di identificare qualcuno fra i passanti fermi ad un semaforo. Pertanto, il fatto che una persona cui si riferisce l'informazione venga identificata o meno dipende dalle circostanze del caso.

Per quanto riguarda le persone identificate o identificabili "direttamente", il **nome** è evidentemente l'identificatore più comune e, in pratica, la nozione di "persona identificata" implica sovente un riferimento al nome di quella persona.

Al fine di accertare l'identità, il nome della persona deve talvolta essere combinato ad altre informazioni (data di nascita, nomi dei genitori, indirizzo o fotografia del volto) per evitare confusioni con eventuali omonimi. Ad esempio, l'informazione che Tizio è debitore di una somma di denaro si può considerare concernente una persona identificata poiché è connessa al nome di quella persona. Il nome è un'informazione che rivela che la persona utilizza quella combinazione di lettere e suoni per distinguersi o essere distinta da altri con cui ha rapporti. Il nome può anche essere il punto di partenza per ottenere informazioni sul luogo in cui vive o può essere trovata la persona, e può anche fornire informazioni sui suoi familiari (attraverso il cognome) e sui diversi rapporti giuridici e sociali associati a quel nome (attestati scolastici/di studio, cartelle cliniche, conti bancari). È perfino possibile conoscere l'aspetto di persona se al suo nome è associata una fotografia. Tutte queste nuove informazioni legate al nome possono permettere di "zumare" su una persona in carne ed ossa, e quindi attraverso gli identificatori l'informazione originale viene associata a una persona fisica che può essere distinta da altri individui.

Per quanto concerne le persone identificate o identificabili "indirettamente", questa categoria rimanda tipicamente al fenomeno delle "combinazioni uniche", siano esse ampie o ridotte. Nei casi in cui, a prima vista, gli identificatori disponibili non consentono di identificare una persona particolare, si può ancora considerare quella persona "identificabile" perché quelle informazioni combinate con altre (che siano o meno conservate dal responsabile del trattamento) consentiranno di distinguerla dalle altre. Questo intende la direttiva con "uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale". Alcune caratteristiche sono talmente uniche da permettere un'identificazione immediata ("l'attuale primo ministro spagnolo"), ma una combinazione di informazioni dettagliate a livello di categorie (fascia d'età, origine regionale, ecc.) può ugualmente essere decisiva in alcune circostanze, specie se si ha accesso a informazioni complementari specifiche. Questo fenomeno è stato ampiamente studiato dagli statistici che sono sempre attenti a non violare l'obbligo di riservatezza.

Esempio n. 10: Informazioni frammentarie nella stampa

Vengono pubblicate informazioni su un vecchio caso penale che all'epoca aveva fatto scalpore. Nella pubblicazione non figura nessuno degli identificatori tradizionalmente dati, in particolare non risulta il nome né la data di nascita delle persone coinvolte.

Non sembra irragionevolmente difficile ottenere informazioni complementari per scoprire chi sono le principali persone coinvolte, per esempio consultando la stampa di quel periodo. Di fatto, si può presumere che non è completamente improbabile che qualcuno segua un procedimento analogo (come leggere vecchi giornali) che gli consenta verosimilmente di scoprire i nomi e altri identificatori delle persone coinvolte. Sembra pertanto giustificato considerare le informazioni dell'esempio 'informazioni su persone identificabili' e quindi 'dati personali'.

A questo punto occorre notare che, mentre l'identificazione attraverso il nome è la pratica più corrente, il nome può non essere necessario in tutti i casi per identificare una persona. Ciò può accadere quando vengono usati altri "identificatori" per distinguere una persona. Di fatto, gli archivi computerizzati che registrano i dati personali di solito assegnano un identificatore unico alle persone registrate per evitare confusioni tra due persone in uno stesso archivio. Anche sul Web gli strumenti di sorveglianza del traffico permettono di identificare facilmente il comportamento di un computer e, quindi, quello del suo utente. Viene "ricostruita" così la personalità di una persona per attribuirle determinate decisioni. Senza neanche cercare il nome e l'indirizzo di un soggetto è possibile categorizzarlo sulla base di criteri socioeconomici, fisiologici, filosofici o di altro tipo, e attribuirgli alcune decisioni, tanto più che il punto di contatto (il computer) non richiede più necessariamente che ne sia svelata l'identità in senso stretto. In altre parole, la possibilità di identificare una persona non presuppone più necessariamente la possibilità di individuarne il nome. La definizione di dati personali rispecchia questa constatazione[10].

La Corte di giustizia delle Comunità europee si è espressa in tal senso quando ha considerato che "*fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce un «trattamento di dati personali [...] ai sensi dell'art. [...] della direttiva 95/46/CE*"[11].

Esempio n. 11: Richiedenti asilo

In un centro d'accoglienza è stato attribuito per scopi amministrativi un codice ai richiedenti asilo che nascondono il loro vero nome. Il codice serve come identificatore, in modo che le diverse informazioni riguardanti il soggiorno del richiedente asilo presso quel centro gli siano associate e, per mezzo di una fotografia o altri indicatori biometrici, il codice stabilisca una connessione diretta e immediata con quella persona

[10] «Report on the application of data protection principles to the worldwide telecommunication networks», di Yves POULLET e della sua équipe, per il comitato T-PD del Consiglio d'Europa, punto 2.3.1, T-PD (2004) 04 def.

[11] Sentenza della Corte di giustizia delle Comunità europee C-101/2001del 6.11.2003 (Lindqvist), punto 27.

fisica, consentendo di distinguerla dagli altri richiedenti asilo e di attribuirle diverse informazioni, che riguarderanno allora una persona fisica "identificata".

L'articolo 8, paragrafo 7 afferma inoltre: "Gli Stati membri determinano a quali condizioni un numero nazionale di identificazione o qualsiasi altro mezzo identificativo di portata generale può essere oggetto di trattamento". Vale la pena soffermarsi sul senso di questa disposizione, che non contiene indicazioni particolari sul tipo di condizioni che gli Stati membri dovrebbero adottare ma che figura comunque nell'articolo sui dati sensibili. Il considerando 33 fa riferimento a questo tipo di dati come "*dati che possono per loro natura ledere le libertà fondamentali o la vita privata*". Si può ragionevolmente supporre che il legislatore possa avere avuto dubbi analoghi in relazione ai numeri nazionali di identificazione, a causa della loro forte potenzialità di collegare facilmente e inequivocabilmente diverse informazioni su una data persona.

Mezzi di identificazione

Il considerando 26 della direttiva presta particolare attenzione al termine "identificabile", quando dispone che "*per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona*". Ciò significa che la sola possibilità ipotetica di distinguere una persona non basta per considerare tale persona "identificabile". Se, tenendo conto dell'"*insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona*", quella possibilità non esiste o è trascurabile, la persona non dovrebbe essere considerata "identificabile", e le informazioni non configurerebbero "dati personali". Il criterio dell'"*insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri*" deve in particolare tenere conto di tutti i fattori in gioco. Il costo dell'identificazione è uno di questi fattori ma non l'unico. La finalità, il modo in cui viene strutturato il trattamento, il vantaggio atteso dal responsabile del trattamento, gli interessi dei singoli, come pure il rischio di disfunzioni organizzative (es. violazioni degli obblighi di riservatezza) e tecniche sono tutti elementi da prendere in considerazione. Per altro verso, questo test è dinamico, quindi bisognerebbe considerare lo stato dell'arte della tecnologia al momento del trattamento e le possibilità di sviluppo nel periodo per il quale saranno trattati i dati. Attualmente l'identificazione può non essere possibile con tutti i mezzi di cui è ragionevolmente possibile avvalersi oggi. Se i dati sono destinati a essere conservati per un mese, forse l'identificazione non è possibile nell'"arco di vita" dell'informazione, nel qual caso i dati non dovrebbero essere considerati dati personali. Se invece l'intenzione è conservare i dati per 10 anni, il responsabile del trattamento dovrebbe considerare la possibilità che l'identificazione avvenga anche al nono anno, il che li renderebbe dati personali in quel preciso momento. È importante che il sistema sia in grado di adattarsi a questi sviluppi, via via che si verificano, e di integrare quindi le misure tecniche e organizzative più appropriate in tempo utile.

Esempio n. 12: Pubblicazione di radiografie con il nome del paziente

Su una rivista scientifica viene pubblicata la radiografia di una donna insieme al suo nome, un nome alquanto raro. Il nome e il fatto che i suoi familiari o le sue conoscenze sapessero della patologia di cui soffriva hanno reso la donna identificabile per alcune persone, pertanto la lastra radiografica è stata considerata dato personale.

Esempio n. 13: Dati di ricerca farmaceutica

Ospedali o singoli medici trasferiscono dati dalle cartelle cliniche dei loro pazienti ad una società a fini di ricerca medica. Non vengono usati i nomi dei pazienti ma solo numeri di serie attribuiti a caso ad ogni caso clinico, per ragioni di coerenza e per evitare confusioni tra le informazioni dei diversi pazienti. Solo i medici, vincolati da segreto medico, posseggono i nomi dei loro pazienti. I dati non contengono altre informazioni che possano identificare i pazienti tramite combinazioni particolari. Inoltre, sono state adottate tutte le altre misure, giuridiche, tecniche e organizzative, per impedire che gli interessati siano identificati o diventino identificabili. In queste circostanze un'autorità per la protezione dei dati personali può considerare che esistano nel trattamento dei dati effettuato dalla società farmaceutica mezzi che possono essere ragionevolmente utilizzati per identificare le persone interessate.

Come si è già detto, un fattore rilevante per valutare "*tutti i mezzi che possono essere ragionevolmente utilizzati*" per identificare le persone sarà di fatto la finalità perseguita dal responsabile del trattamento nel trattare i dati. Le autorità nazionali per la protezione dei dati si sono trovate di fronte a casi in cui, da un lato, il responsabile del trattamento sostiene che vengono trattate solo informazioni sparse, senza riferimenti a nomi o altro identificatore diretto, e ritiene che i dati non dovrebbero essere assimilati a dati personali né dovrebbero essere soggetti alle norme di protezione dei dati; dall'altro, il trattamento di quelle informazioni ha senso soltanto se permette di identificare persone specifiche e di trattarle in un determinato modo. Nei casi in cui la finalità del trattamento implica l'identificazione di persone si può presumere che il responsabile del trattamento o altra persona coinvolta ha o avrà i mezzi che "possono essere ragionevolmente utilizzati" per identificare l'interessato. In effetti, pretendere che le persone non sono identificabili quando la finalità del trattamento è precisamente identificarle sarebbe una contraddizione in termini. Pertanto, è opportuno considerare le informazioni concernenti persone identificabili e subordinarne il trattamento alle norme sulla protezione dei dati.

Esempio n. 14: Videosorveglianza

Ciò è particolarmente pertinente per la videosorveglianza, settore nel quale i responsabili del trattamento sostengono spesso che l'identificazione avverrebbe soltanto in una piccola percentuale del materiale raccolto e che quindi, prima che l'identificazione in questi pochi casi abbia luogo, non vengano trattati dati personali. Poiché la finalità della videosorveglianza è però quella di identificare le persone che appaiono nelle immagini, nell'ipotesi che il responsabile del trattamento giudichi necessaria tale identificazione, l'intera applicazione configura trattamento dei dati di persone identificabili, anche se nella pratica alcune delle persone registrate non sono identificabili.

Esempio n. 15: Indirizzi IP dinamici

Il Gruppo considera gli indirizzi IP dati concernenti una persona identificabile. Al riguardo ha dichiarato che "*i fornitori di accesso Internet e i gestori delle reti LAN possono, utilizzando mezzi ragionevoli, identificare gli utenti Internet cui essi hanno attribuito indirizzi IP, poiché, normalmente, essi "registrano" in un apposito file la data, l'ora, la durata e l'indirizzo IP dinamico assegnato all'utente Internet. Lo stesso dicasi per i fornitori di servizi Internet, i quali detengono un registro sul server HTTP.*

In questi casi, non vi è dubbio sul fatto che si possa parlare di dati personali ai sensi dell'articolo 2 (a) della direttiva …)"[12]

In particolare, nei casi in cui il trattamento di indirizzi IP viene effettuato per identificare gli utenti di un computer (ad esempio, dal titolare di un diritto d'autore per perseguire l'utente di un computer per violazione di diritti di proprietà intellettuale), il responsabile del trattamento parte dal principio che i "mezzi che possono essere ragionevolmente utilizzati" per identificare le persone esistono, ad esempio nella figura del giudice del ricorso (altrimenti la raccolta delle informazioni non avrebbe senso), e quindi tali informazioni andrebbero considerate dati personali.

Un caso particolare è quello di alcuni tipi di indirizzi IP che, in alcune circostanze, non permettono effettivamente di identificare l'utente per vari motivi tecnici ed organizzativi. Si pensi per esempio agli indirizzi IP attribuiti a un computer di un internet café, dove non è richiesta l'identificazione dei clienti. Si potrebbe affermare che i dati raccolti sull'impiego del computer X per un certo lasso di tempo non consentono di identificare l'utente con mezzi ragionevoli, e quindi non si può parlare di dati personali. Tuttavia, occorre notare che i fornitori di servizi Internet molto probabilmente non sapranno se gli indirizzi IP in questione permettono l'identificazione o meno, e tratteranno i dati associati con quell'IP nello stesso modo in cui trattano le informazioni associate agli indirizzi IP degli utenti debitamente registrati e identificabili. Pertanto, a meno di poter distinguere con assoluta certezza che i dati corrispondano a utenti non identificabili, il fornitore di servizi Internet dovrà trattare tutte le informazioni IP come dati personali, per maggiore sicurezza.

Esempio n. 16: Danni causati dai graffiti

I veicoli per passeggeri di una società di trasporti subiscono danni a ripetizione a causa dei graffiti. Per valutare i danni e agevolare l'azione legale contro gli autori, la società tiene un registro contenente informazioni sulle circostanze dei danni, nonché immagini dei veicoli danneggiati e delle "tag" o "firme" dell'autore. Al momento di inserire le informazioni nel registro non sono noti né gli autori del danno, né le persone cui corrisponde la "firma". Può anche accadere che non si vengano mai a sapere. Tuttavia, la finalità del trattamento è proprio quella di identificare le persone cui si riferisce l'informazione, come gli autori del danno, in modo da denunciarli. Questo trattamento ha un senso se il responsabile del trattamento dei dati considera "ragionevolmente probabile" che un giorno vi saranno i mezzi per identificare la persona. Le informazioni contenute nelle immagini vanno considerate come concernenti persone "identificabili", le informazioni contenute nel registro come "dati personali" e il trattamento dovrebbe essere soggetto alle norme sulla protezione dei dati, che ne ammettono la legittimità in talune circostanze e con determinate garanzie.

Quando l'identificazione della persona interessata non rientra nella finalità del trattamento, molto importante è il ruolo delle misure tecniche per prevenire l'identificazione. È possibile che adottare appropriate misure tecniche e organizzative fra le più avanzate per proteggere i dati contro l'identificazione faccia la differenza nel ritenere che le persone non siano identificabili, considerati *tutti i mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento dei dati o da un'altra persona* per identificare le persone. In questo caso, l'attuazione di quelle

[12] WP 37: Tutela della vita private su Internet – Un approccio integrato dell'UE alla protezione dei dati on-line, adottato il 21.11.2000.

misure non è *conseguenza* di un obbligo giuridico derivante dall'articolo 17 della direttiva (che si applica soltanto se le informazioni sono, prima di tutto, dati personali), ma piuttosto una *condizione* affinché le informazioni non siano considerate dati personali e il loro trattamento non sia soggetto alla direttiva.

Dati pseudonimizzati

La "pseudonimizzazione" è il processo volto a mascherare l'identità. L'obiettivo è poter raccogliere dati complementari sulla stessa persona senza doverne conoscere l'identità. Tale aspetto è particolarmente pertinente nel contesto della ricerca e della statistica.

La pseudonimizzazione può comportare tracciabilità se si usano liste di corrispondenza delle identità con i relativi pseudonimi, o algoritmi crittografici bidirezionali per la pseudonimizzazione. È inoltre possibile mascherare l'identità rendendo impossibile la reidentificazione, per esempio con la crittografia unidirezionale che crea in genere dati anonimi.

L'efficacia di questo procedimento dipende da una serie di fattori: lo stadio in cui viene applicato, il grado di sicurezza contro il tracciamento inverso, il volume di popolazione in cui è mascherata la persona, la capacità di collegare singole transazioni/registrazioni alla stessa persona, ecc. I pseudonimi devono essere casuali e imprevedibili e il numero dei pseudonimi possibili così ampio che uno stesso pseudonimo non possa essere mai selezionato casualmente due volte. Per garantire un alto livello di sicurezza, occorre che la serie di potenziali pseudonimi sia quanto meno pari alla gamma dei valori delle funzioni di hash crittografiche[13].

I dati pseudonimizzati con sistema tracciabile possono essere assimilati a informazioni su persone *identificabili indirettamente*. In effetti, usare uno pseudonimo significa permettere di risalire alla persona per scoprirne l'identità, ma solo in circostanze predefinite. In questo caso, pur applicandosi le norme di protezione dei dati, i rischi per le persone in relazione al trattamento delle informazioni indirettamente identificabili saranno per lo più bassi, cosicché l'applicazione di tali norme sarà a ragione più flessibile che nel caso di trattamento di informazioni su persone direttamente identificabili.

Dati codificati con chiave

I dati codificati con chiave sono un classico esempio di pseudonimizzazione. Le informazioni si riferiscono a persone contrassegnate da un codice, mentre la chiave che crea la corrispondenza tra il codice e i comuni identificatori (il nome, data di nascita, indirizzo) è tenuta separata.

Esempio n. 17: Dati non aggregati a fini statistici

Un esempio dell'importanza di tenere conto di tutte le circostanze per valutare se i mezzi di identificazione "possano essere ragionevolmente utilizzati" sono forse le informazioni personali trattate dall'istituto nazionale di statistica dove, a un certo stadio, le informazioni sono tenute in forma non aggregata e riguardano persone specifiche, benché designate da un codice anziché da un nome (per esempio, la persona

[13] Vedi il documento di lavoro *Privacy-enhancing technologies* del Gruppo di lavoro "Tecnologie volte a migliorare la protezione dei dati" del comitato "Questioni tecniche e organizzative della protezione dei dati" dei commissari federali tedeschi e di Stato per la protezione dei dati (ottobre 1997), pubblicato su http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

con codice X1234 beve un bicchiere di vino più di 3 volte a settimana). L'istituto di statistica tiene separata la chiave dei codici (la lista che associa i codici con i nomi delle persone). Se si considera che la chiave può essere "ragionevolmente utilizzata" dall'istituto statistico, allora le informazioni connesse alle persone possono essere considerate dati personali e l'istituto deve sottostare alle norme di protezione dei dati. Ora possiamo immaginare che una lista di dati sulle abitudini di consumo del vino venga trasferita all'associazione nazionale dei produttori di vino affinché difenda l'immagine dei suoi associati con dati statistici. Per determinare se questa lista contiene dati personali, bisogna appurare se possono essere identificati i singoli consumatori di vino "*prendendo in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri*".

Se i codici usati sono unici per ogni persona specifica, il rischio di identificazione sussiste quando è possibile accedere alla chiave di criptaggio. Pertanto, i rischi di pirateria, la probabilità cioè che qualcuno dell'organizzazione speditrice – nonostante il segreto professionale – fornisca la chiave *e* la possibilità di un'identificazione indiretta, sono tutti fattori di cui tener conto per stabilire se le persone possono essere identificate *prendendo in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri*, e quindi se le informazioni debbano essere considerate "dati personali". Se così è, si applicheranno le norme di protezione dei dati. Una questione diversa è quella per cui le norme di protezione dei dati potrebbero valutare il livello di rischio per le persone, subordinando il trattamento a condizioni più o meno rigide sulla base della flessibilità concessa dalle norme della direttiva.

Se invece i codici non sono unici ma lo stesso numero di codice (per esempio "123") è usato per designare persone in città differenti e dati relativi ad anni diversi (distinguendo una specifica persona solo nell'ambito di un anno e di un campione della stessa città), il responsabile del trattamento o un terzo sarebbero in grado di identificare una persona specifica solo sapendo a quale anno e a quale città si riferiscono i dati. Se queste informazioni complementari scompaiono, ed è ragionevolmente improbabile che vengano recuperate, si può ritenere che le informazioni disponibili non riguardino persone identificabili e che quindi non siano soggette alle norme di protezione dei dati.

Questo tipo di dati viene comunemente utilizzato nei test clinici dei medicinali. Disciplina queste attività il quadro normativo istituito dalla direttiva 2001/20/CE, del 4 aprile 2001, relativa all'applicazione della buona pratica clinica nell'esecuzione della sperimentazione clinica[14]. Il professionista/ricercatore medico ("investigatore") che effettua i test dei medicinali raccoglie dati sui risultati clinici di ogni paziente, contrassegnandolo con un codice. Il ricercatore comunica le informazioni alla società farmaceutica o a terzi interessati ("sponsor") solo nella forma codificata, poiché sia all'una che agli altri interessano solo le informazioni biostatistiche. Tuttavia, l'investigatore tiene separatamente la chiave che associa il codice alle informazioni generali per identificare i pazienti separatamente. Per proteggere la salute dei pazienti nel caso in cui i medicinali presentino rischi, l'investigatore è obbligato a conservare la chiave in modo da poter identificare i singoli pazienti e somministrare loro, in caso di necessità, la terapia appropriata.

In questo caso, il punto è stabilire se i dati usati per il test clinico siano da considerarsi concernenti persone fisiche "identificabili" e debbano quindi essere soggetti alle norme

[14] GU L 121 dell'1.5.2001, pag. 34.

di protezione dei dati. Secondo la precedente analisi, per stabilire se una persona è identificabile occorre tener conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificarla. Nella fattispecie, l'identificazione delle persone (per somministrare la terapia appropriata in caso di necessità) è uno dei fini del trattamento dei dati codificati con chiave. La società farmaceutica ha previsto i mezzi per il trattamento, comprese le misure organizzative e le sue relazioni con il ricercatore che detiene la chiave in modo che l'identificazione delle persone non sia soltanto qualcosa che *può* accadere, ma piuttosto qualcosa che *deve* accadere in alcune circostanze. L'identificazione dei pazienti costituisce quindi parte integrante delle finalità e dei mezzi del trattamento. In questo caso, si può concludere che i dati codificati con chiave costituiscono informazioni concernenti persone fisiche identificabili per tutte le parti eventualmente coinvolte nell'identificazione, e vanno sottoposti alle norme di protezione dei dati. Questo non significa tuttavia che altri responsabili del trattamento che stiano lavorando sugli stessi dati codificati stiano effettivamente trattando dati personali se il regime specifico nel quale questi altri responsabili operano esclude esplicitamente la reidentificazione e sono state adottate misure tecniche adeguate al riguardo.

In altri settori della ricerca o di uno stesso progetto, è possibile che nella concezione di protocolli e procedure sia esclusa la reidentificazione della persona interessata, magari perché non sono coinvolti aspetti terapeutici. Per ragioni tecniche o di altro tipo può essere ancora possibile scoprire quali dati clinici corrispondono a quali persone, ma in nessun caso si presuppone né ci si aspetta che tale identificazione avvenga, e sono predisposte misure tecniche appropriate (per esempio, l'hash irreversibile crittografico) perché ciò non accada. In un caso come questo, dove tutti i protocolli e le misure non possono comunque impedire l'identificazione di certe persone interessate (a causa di circostanze imprevedibili come la combinazione accidentale di loro caratteristiche che ne rivelano l'identità), è possibile non considerare le informazioni trattate dal responsabile del trattamento iniziale come concernenti persone identificate o identificabili, prendendo in considerazione *l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri*. Il loro trattamento non sarà quindi soggetto alle disposizioni della direttiva. Diversa è la situazione del nuovo responsabile del trattamento che ha effettivamente avuto accesso ai dati identificabili, che saranno senza dubbio da considerarsi "dati personali".

FAQ 14-7 sui principi di approdo sicuro (Safe Harbour)

La questione dei dati codificati nella ricerca farmaceutica è stata affrontata nell'ambito dei principi di approdo sicuro[15]. La FAQ 14-7 recita:

FAQ 14 – Medicinali e prodotti farmaceutici

7. D: Per non rivelare l'identità dei singoli partecipanti lo sperimentatore principale assegna invariabilmente ai dati della ricerca un codice di accesso unico. Le aziende farmaceutiche che promuovono tale ricerca non ricevono il codice di accesso. Soltanto il ricercatore ne è in possesso per poter essere in grado d'identificare il partecipante in circostanze particolari (ad esempio quando è necessario un supplemento d'assistenza medica). Un trasferimento dall'UE agli Stati Uniti di dati codificati in questo modo costituisce un trasferimento di dati personali soggetto ai principi dell'approdo sicuro?

[15] Decisione della Commissione 2000/520/CE del 26.7.2000 - GU L 215 del 25.8.2000, pag. 7

7. R: No. Questo modo di procedere non costituisce un trasferimento di dati personali soggetto ai principi in questione.

Il Gruppo ritiene che questa affermazione nell'ambito dei principi *Safe Harbour* non è incoerente con il ragionamento esposto, per cui tali informazioni andrebbero considerate dati personali soggetti alla direttiva. In realtà questa FAQ non è abbastanza precisa poiché non indica né il destinatario, né le modalità di trasferimento dei dati. Secondo il Gruppo la FAQ si riferisce al caso in cui i dati codificati sono trasmessi a un destinatario negli USA (ad esempio, una società farmaceutica) che riceve solo i dati codificati e non conoscerà mai l'identità dei pazienti, che è e sarà nota solo al ricercatore/professionista medico nell'UE, nel caso sia necessaria una terapia, ma mai alla società statunitense.

Dati anonimi

Con "dati anonimi" ai sensi della direttiva si intendono le informazioni concernenti una persona fisica che non può essere identificata né dal responsabile del trattamento né da altri, *prendendo in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri* per identificarla. I "dati anonimizzati" sarebbero quindi dati anonimi già corrispondenti a una persona identificabile ma che non ne permettono più l'identificazione. Il considerando 26 fa inoltre riferimento a questo concetto quando precisa che "*i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile*". Una volta di più valutare se i dati consentano l'identificazione di un soggetto e se le informazioni possano essere considerate anonime o meno dipende dalle circostanze, e si impone un'analisi caso per caso specie per verificare in qual misura i mezzi possono essere ragionevolmente utilizzati per l'identificazione, come descrive il considerando 26. Ciò è particolarmente pertinente in ambito statistico nel quale, nonostante le informazioni possano essere presentate come dati aggregati, il campione originale non è sufficientemente ampio e altre informazioni possono consentire l'identificazione delle persone.

Esempio n. 18: Sondaggi statistici e combinazione di informazioni sparse

Al di là dell'obbligo generale di rispettare le norme di protezione dei dati per assicurare l'anonimato dei sondaggi statistici, gli statistici sono soggetti all'obbligo specifico del segreto professionale e, in virtù di quelle norme, hanno il divieto di pubblicare dati non anonimi. Sono quindi obbligati a pubblicare dati statistici aggregati che non possono in nessun modo essere attribuiti a una persona identificata attraverso le statistiche. Questa norma è particolarmente pertinente in relazione alla pubblicazione dei dati dei censimenti. In ogni situazione dovrebbe essere determinata una soglia al di sotto della quale si ritiene possibile identificare le persone interessate. Se risulta che un criterio porti a un'identificazione in una data categoria di persone, per quanto ampia (per esempio, solo un dottore opera in una città di 6 000 abitanti), bisognerà eliminare tale criterio "discriminatorio" o aggiungere altri criteri per "diluire" i risultati su una data persona, così da garantire il segreto statistico.

Esempio n. 19: Pubblicazione di immagini di videosorveglianza

Un negoziante installa un sistema di videosorveglianza nel suo negozio e pubblica, nel negozio, le immagini dei ladri colti in flagrante dal sistema di videosorveglianza. Dopo l'intervento della polizia, cancella i volti dei ladri oscurandoli. Tuttavia, nonostante la

precauzione, è ancora possibile che le persone sulle foto siano riconosciute da loro amici, parenti o vicini, perché il portamento, il taglio di capelli o i vestiti sono ancora riconoscibili.

4. QUARTO ELEMENTO: "PERSONA FISICA"

La protezione fornita dalle norme della direttiva si applica alle persone fisiche, ossia agli esseri umani. Il diritto alla protezione dei dati personali è, in tal senso, un diritto universale che non è limitato ai cittadini o ai residenti di un dato paese. Il considerando 2 della direttiva dice esplicitamente che "*i sistemi di trattamento dei dati sono al servizio dell'uomo*" e che "*indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse*".

Il concetto di persona fisica figura all'articolo 6 della Dichiarazione universale dei diritti dell'uomo, che recita "*Ogni individuo ha diritto, in ogni luogo, al riconoscimento della sua personalità giuridica*". La legislazione degli Stati membri, generalmente nel diritto civile, descrive in modo più preciso il concetto di personalità degli esseri umani, intesa come la capacità dell'individuo di essere soggetto di rapporti giuridici, dalla nascita fino alla morte. I dati personali sono pertanto, in linea di principio, dati che si riferiscono a *persone viventi* identificate o identificabili. Ciò solleva diverse questioni ai fini della presente analisi.

Dati relativi a persone decedute

Le informazioni relative a persone decedute non sono da considerarsi, in linea di principio, dati personali soggetti alle norme della direttiva poiché, per il diritto civile, i defunti non sono più persone fisiche. Eppure, i dati dei defunti possono, in alcuni casi, beneficiare ancora indirettamente di una protezione.

Primo, il responsabile del trattamento dei dati può non essere nelle condizioni di accertare se la persona cui si riferiscono i dati è ancora viva o è deceduta e, anche se può farlo, le informazioni sui defunti possono essere trattate secondo lo stesso regime valido per i vivi, senza distinzioni. Poiché il responsabile del trattamento è soggetto agli obblighi di protezione dei dati imposti dalla direttiva in riferimento ai dati dei vivi, gli sarà probabilmente più facile, nella pratica, trattare anche i dati dei defunti ai sensi delle norme di protezione dei dati, piuttosto che separare le due serie di dati.

Secondo, è possibile che le informazioni sui defunti possono fare riferimento anche a persone viventi. Ad esempio, l'informazione che la defunta Gaia soffriva di emofilia indica che suo figlio Tizio soffre della stessa malattia, che è connessa a un gene presente nel cromosoma X. Pertanto, quando le informazioni costituenti dati di un defunto possono considerarsi concernenti nel contempo anche persone viventi e configurare dati personali soggetti alla direttiva, i dati personali del defunto possono godere indirettamente della protezione delle norme della direttiva.

Terzo, le informazioni sui defunti possono beneficiare di una protezione specifica ai sensi di norme diverse da quelle sulla protezione dei dati, delineando quel che alcuni definiscono la *personalitas praeterita*. L'obbligo di riservatezza del personale medico non termina con la morte del paziente. La legislazione nazionale sul diritto alla propria immagine e al proprio onore può ugualmente tutelare la memoria dei defunti.

Quarto, nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcuna altra disposizione del diritto comunitario, come ha osservato la Corte di giustizia delle Comunità europee[16]. È possibile che un legislatore nazionale decida di estendere le disposizioni delle leggi nazionali sulla protezione dei dati ad alcuni aspetti riguardanti il trattamento dei dati dei defunti, qualora un interesse legittimo lo giustifichi[17].

Nascituri

L'applicabilità delle norme sulla protezione dei dati prima della nascita dipende dalla posizione generale dei sistemi giuridici nazionali circa la tutela dei nascituri. Se guardiamo principalmente ai diritti di successione, alcuni Stati membri riconoscono il principio secondo cui i bambini concepiti ma non ancora nati sono da considerarsi nati ai fini di alcuni diritti (possono per esempio ricevere un'eredità o accettare una donazione), a condizione che nascano effettivamente. In altri Stati membri godono di una protezione specifica disposta da particolari norme giuridiche, subordinata anch'essa alla medesima condizione. Per determinare se le disposizioni nazionali sulla protezione dei dati proteggono anche le informazioni relative ai nascituri, occorre considerare l'approccio generale del sistema giuridico nazionale, tenendo ben presente che lo scopo delle norme di protezione dei dati è proteggere la persona.

Un secondo problema emerge in relazione alla risposta generale del sistema giuridico, che dà per assunto che la situazione del nascituro sia limitata nel tempo alla durata della gravidanza. Non si tiene quindi conto del fatto che tale situazione possa durare molto più a lungo, come nel caso degli embrioni congelati. Infine, è possibile trovare risposte giuridiche specifiche in particolari disposizioni sulle tecniche riproduttive che si occupano dell'impiego di informazioni mediche o genetiche sugli embrioni.

Persone giuridiche

Poiché la definizione di dati personali si riferisce all'individuo, più precisamente alla persona fisica, le informazioni sulle persone giuridiche non sono in linea di principio disciplinate dalla direttiva, e quindi non godono della protezione da questa disposta[18]. Ciò nondimeno, alcune norme di protezione dei dati possono, in certe circostanze, applicarsi indirettamente alle informazioni concernenti imprese o persone giuridiche.

Alcune disposizioni della direttiva 2002/58/CE sulla protezione della vita privata nel settore delle comunicazioni elettroniche si estendono alle persone giuridiche. All'articolo 1 si legge: "*2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche*". Di conseguenza, gli articoli 12 e 13 estendono l'applicazione di certe disposizioni sugli elenchi degli abbonati e sulle comunicazioni indesiderate anche alle persone giuridiche.

---

16 Sentenza della Corte di giustizia delle Comunità europee C-101/2001 del 6/11/2003 (Lindqvist), punto 98

17 Verbale del Consiglio dell'Unione europea, 8.2.1995, documento 4730/95: "All'articolo 2(a) "*Il Consiglio e la Commissione confermano che è compito degli Stati membri stabilire se e in quale misura questa direttiva debba essere applicata alle persone decedute*".

18 Considerando 24 della direttiva: "*Considerando che la presente direttiva lascia impregiudicate le normative relative alla tutela delle persone giuridiche riguardo al trattamento dei dati che le riguardano*"

Le informazioni sulle persone giuridiche possono considerarsi "concernenti" persone fisiche in virtù della loro situazione specifica, conformemente ai criteri stabiliti nel presente documento. È quel che accade quando il nome di una persona giuridica deriva dal nome di una persona fisica, oppure nel caso dell'indirizzo e-mail di un'impresa di norma usato da un dato dipendente, o delle informazioni su una piccola impresa (giuridicamente un "oggetto" piuttosto che una persona giuridica) che possono descrivere il comportamento del suo titolare. In tutti questi casi, in cui i criteri di "contenuto", "finalità" o "risultato" fan sì che le informazioni su una persona giuridica o su un'impresa possano considerarsi come "concernenti" una persona fisica, è opportuno considerare tali informazioni come dati personali e si applicano le norme di protezione dei dati.

La Corte di giustizia delle Comunità europee ha precisato che nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcuna altra disposizione del diritto comunitario[19]. Di conseguenza, alcuni Stati membri come l'Italia, l'Austria e il Lussemburgo hanno esteso l'applicazione di alcune disposizioni della legislazione nazionale adottata in conformità della direttiva (come quelle sulle misure di sicurezza) al trattamento dei dati sulle persone giuridiche.

Come per le informazioni sulle persone decedute, è possibile che, in conseguenza a modalità pratiche disposte dal responsabile del trattamento, i dati sulle persone giuridiche siano *de facto* soggetti alle norme di protezione dei dati. Quando il responsabile del trattamento raccoglie indistintamente dati sulle persone fisiche e giuridiche e li include negli stessi gruppi di dati, i meccanismi di trattamento dei dati e i sistemi di audit possono essere concepiti in modo da conformarsi alle norme di protezione dei dati. In effetti, può essere più semplice per il responsabile del trattamento applicare le norme sulla protezione dei dati a tutti i tipi di informazioni presenti nei suoi archivi, anziché cercare di distinguere fra informazioni inerenti a persone fisiche o a persone giuridiche.

IV. COSA ACCADE QUANDO I DATI NON RIENTRANO NEL CAMPO D'APPLICAZIONE DELLA DEFINIZIONE

Come abbiamo visto nel presente documento, le informazioni possono non essere considerate dati personali a seconda delle circostanze. È quel che accade quando i dati non si possono considerare concernenti una persona o quando la persona non può essere considerata identificata o identificabile. Quando le informazioni trattate non rientrano nel concetto di "dati personali", ne consegue che la direttiva non si applica a norma del suo articolo 3. Ciò non significa, peraltro, che le persone possano essere private di ogni forma di protezione in quella particolare situazione. Varranno invece le seguenti considerazioni.

Se la direttiva non è applicabile, è possibile che si applichi la legislazione nazionale in materia di protezione dei dati. Come stabilisce l'articolo 34, gli Stati membri sono destinatari della direttiva. Al di fuori della sua portata, gli Stati membri non sono soggetti agli obblighi che impone -in buona sostanza attuare le disposizioni legislative, regolamentari ed amministrative necessarie per conformarsi ad essa. Tuttavia, come ha precisato la Corte di giustizia delle Comunità europee, nulla impedisce che uno Stato

[19] Sentenza della Corte di giustizia delle Comunità europee C-101/2001 del 6.11.2003 (Lindqvist), punto 98.

membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcuna altra disposizione del diritto comunitario. Può quindi benissimo accadere che certe situazioni che non comportano trattamento di dati personali come definito dalla direttiva siano tuttavia soggette a misure di protezione ai sensi della legislazione nazionale. Ciò può valere, ad esempio, per i dati codificati con chiave, a prescindere che siano dati personali o meno.

Quando non si applicano le norme sulla protezione dei dati, alcune attività possono ancora comportare interferenze con l'articolo 8 della Convenzione europea sui diritti dell'uomo, che tutela il diritto alla vita privata e familiare, alla luce della vasta giurisprudenza della Corte europea dei diritti dell'uomo. Altri corpus normativi come il diritto civile, il diritto penale o il diritto antidiscriminatorio possono ugualmente dare protezione alle persone laddove non siano applicabili le norme di protezione dei dati e possano entrare in gioco interessi legittimi di vario tipo.

V. CONCLUSIONI

Nel presente parere il Gruppo ha formulato orientamenti su come interpretare, e applicare a seconda delle situazioni, il concetto di dati personali ai sensi della direttiva 95/46/CE e della legislazione comunitaria correlata.

La constatazione generale è che il legislatore europeo ha inteso adottare un concetto ampio di dati personali, ma non illimitato. Non bisogna perdere di vista che l'obiettivo delle norme contenute nella direttiva è proteggere i diritti e le libertà fondamentali delle persone, in particolare il diritto alla vita privata, in relazione al trattamento dei dati personali. Queste norme sono state pertanto concepite per applicarsi a situazioni in cui i diritti individuali potrebbero essere a rischio e necessitano pertanto protezione. Il campo d’applicazione delle norme di protezione dei dati personali non va esteso oltre misura, ma bisogna anche evitare di restringere indebitamente il concetto di dati personali. La direttiva ha definito il proprio campo di applicazione escludendo una serie di attività, e ammette una certa flessibilità nell’applicare le norme alle attività rientranti in tale campo. Le autorità per la protezione dei dati svolgono un ruolo essenziale nella ricerca di un equilibrio adeguato in questa applicazione (vedi parte II).

L'analisi del Gruppo si è incentrata su quattro elementi fondamentali, individuabili nella definizione di “dati personali”: “qualsiasi informazione”, “concernente”, “persona fisica”, “identificata o identificabile”. Questi quattro elementi sono strettamente connessi fra loro e si alimentano reciprocamente, ma presi insieme determinano se un'informazione debba essere assimilata a un “dato personale”. L'analisi è sostenuta da esempi tratti dalle pratiche nazionali delle autorità europee per la protezione dei dati.

- Il primo elemento – “qualsiasi informazione” – richiede un’interpretazione ampia del concetto, a prescindere dalla natura o dal contenuto delle informazioni e dal formato tecnico in cui vengono presentate. Ciò significa che le informazioni tanto oggettive che soggettive su una persona, di qualunque portata, possono essere considerate “dati personali” al di là del supporto tecnico usato. Il parere si sofferma inoltre sui dati biometrici e sulle distinzioni giuridiche con i campioni umani da cui possono essere estratte le informazioni (vedi punto III.1).

- Il secondo elemento – “concernente” – è stato finora sovente trascurato, sebbene svolga un ruolo cruciale nel determinare la portata sostanziale del concetto, in

particolare in relazione a oggetti e nuove tecnologie. Il parere propone di avvalersi di tre fattori alternativi -contenuto, finalità e risultato- per stabilire se le informazioni "concernono" una persona. Questo elemento riguarda anche le informazioni che possono avere un chiaro impatto sul modo in cui una persona viene trattata o valutata (vedi punto III.2).

- Il terzo elemento – [persona fisica] "identificata o identificabile" – focalizza l'attenzione sulle condizioni in cui un soggetto va considerato "identificabile" e sui "mezzi che possono essere ragionevolmente utilizzati" dal responsabile del trattamento o da altri per identificarlo. Il contesto particolare e le circostanze di un caso specifico sono determinanti in questa analisi. Il parere affronta inoltre la questione dei "dati pseudonimizzati" e dell'impiego dei "dati codificati con chiave" nella ricerca statistica o farmaceutica (vedi punto III.3).

- Il quarto elemento – "persona fisica" – si occupa del requisito secondo cui i "dati personali" riguardano "persone viventi". Il parere esamina anche le connessioni con i dati sulle persone decedute, sui nascituri e sulle persone giuridiche (vedi punto III.4).

In ultimo, il parere esamina cosa accade quando i dati non rientrano nel campo d'applicazione della definizione "dati personali". Diverse sono le soluzioni disponibili, anzitutto attraverso la legislazione nazionale al di fuori della portata della direttiva, purché siano rispettate le altre disposizioni comunitarie (vedi parte IV).

Il Gruppo invita tutte le parti interessate a esaminare attentamente gli orientamenti formulati nel presente parere e a tenerne conto nell'interpretazione e nell'applicazione delle disposizioni di diritto nazionale in conformità della direttiva 95/46/CE.

I membri del Gruppo, prevalentemente rappresentanti delle autorità di controllo nazionali per la protezione dei dati, si impegnano a sviluppare ulteriormente tali orientamenti nell'ambito delle loro attribuzioni e ad assicurare la corretta applicazione della loro legislazione nazionale in conformità della direttiva 95/46/CE.

Il Gruppo intende applicare e sviluppare gli orientamenti formulati nel presente parere ogni qualvolta necessario, e tenerne conto nel suoi futuri lavori, specie in relazione a problematiche come la gestione dell'identità nel quadro dell'*e-Government* e dell'*e-Health* e della tecnologia RFID. Su quest'ultimo punto, il Gruppo intende contribuire all'analisi di come le norme di protezione dei dati possono influire sull'impiego della tecnologia RFID, e dell'eventuale necessità di misure complementari per assicurare un adeguato rispetto dei diritti e degli interessi in materia di protezione dei dati.

Infine, il Gruppo apprezzerebbe un qualunque riscontro dalle parti interessate e dalle autorità di controllo sull'applicazione pratica degli orientamenti qui formulati, compresi eventuali esempi in aggiunta a quelli esposti nel documento. Il Gruppo intende ritornare sull'argomento a tempo debito, per una maggiore comprensione comune del concetto chiave di dati personali e per un'applicazione armonizzata e un migliore recepimento della direttiva 95/46/CE e della legislazione comunitaria correlata.

Per il Gruppo

Il presidente
Peter SCHAAR