Capitolo Primo

Nozione del dato personale e del trattamento dei dati

SOMMARIO: 1. Nozione di dato personale. – 2. Introduzione al concetto di dato personale nel Codice della Privacy e la sua evoluzione nel contesto sociale. – 3. Modelli possibili di classificazione di dato personale. – 4. Il modello di classificazione proposto dal Gruppo dei Garanti Europei per la protezione dei dati personali. – 5. Il problema di classificare l'*Internet Protocol* (IP) come dato personale e le contraddizioni nella recente giurisprudenza sulla tutela del diritto d'autore e della privacy. – 6. Quando il frammento di informazione diviene dato personale. – 7. Nozione di dato sensibile: nuovo approccio sulla sensibilità del dato nel Codice della Privacy e nel regolamento europeo. – 7.1. Le sottocategorie del dato personale: dati sensibili, giudiziari e semi-sensibili. – 7.2. Dati sensibili e soglia di sensibilità dei dati: analisi dei singoli casi. – 8. Nozione di dato giudiziario nel Codice della Privacy e nel regolamento europeo. – 9. Nozione di dato semisensibile: il *prior checking* (verifica preliminare). – 10. Nozione di trattamento dei dati. – 11. Oggetto e ambito di applicazione del Codice della Privacy e del regolamento europeo. – 11.1. Le reti telematiche e il trasferimento di dati all'estero: quale è il diritto per la protezione dei dati personali applicabile?

1. *Nozione di dato personale*

La normativa sulla privacy si prefigge lo scopo di tutelare la persona in senso ampio attraverso la nozione di trattamento dei dati personali al fine di garantire il rispetto dei diritti e delle libertà fondamentali, la dignità dell'interessato [1], la riser-

[1] Con tale espressione si intende generalmente tutto il corpus di libertà e diritti descritti nella Parte prima della Costituzione italiana, sono da includersi sia le libertà negative (dallo Stato), sia le libertà positive (nello Stato), e relative all'individuo nelle formazioni sociali; strettamente connessa alla nozione di libertà è quella di autonomia, entrambi i concetti esprimono un'idea di relazione, nel senso che si è liberi nei confronti di qualcosa, senza interferenze esterne e nell'esprimere e selezionare i propri interessi. Per un approfondimento sul tema delle libertà e dell'autonomia, T. MARTINES, *Diritto Costituzionale*, Giuffrè, 1994, p. 628. Questi diritti e libertà devono essere riconosciuti in particolare nelle relazioni che si istaurano nelle formazioni sociali, ampiamente intese come entità superindividuali a base associativa, come per esempio i sindacati che possono avere un ruolo di mediazione rispetto allo Stato, verso una cultura del pluralismo e dell'autonomia nelle formazioni sociali, P. RE-

vatezza [2], l'identità personale ed il diritto alla protezione dei dati personali [3].

In primo luogo si evidenzia come le esigenze di tutela della privacy siano state per lungo tempo intese come coincidenti con quelle di riservatezza; il diritto alla privacy era esclusivamente un diritto "negativo", volto a non rilevare informazioni sul nostro conto, ovvero qualcosa che, in ambito giuridico, legava in modo trasversale il diritto alla riservatezza, all'identità personale, e altri diritti di personalità [4].

Tuttavia, il progresso sociale, tecnologico e la globalizzazione con l'abbatti-

---

SCIGNO, *Persona e comunità*, Cedam, 1999, p. 58 ss. La nozione di dignità ricorre anche nell'art. 3 della Costituzione Italiana, in particolare il valore della dignità acquista il suo pieno significato nelle relazioni, infatti l'articolo poc'anzi menzionato recita "Tutti i cittadini hanno pari dignità sociale e sono uguali davanti alla legge […] È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, limitando di fatto la libertà e l'uguaglianza dei cittadini", in quest'articolo si vede come i valori costituzionali delle libertà e dignità siano indissolubilmente vincolati l'uno con l'altro, infatti senza un'uguaglianza sostanziale non esistono spazi di libertà ed autonomia individuale.

[2] A seguito di questa vicenda, nella *Harvard Law Review* del 1890 venne pubblicato un famoso articolo che fissa i principi cardine della Privacy, *The right to privacy*, scritto da Samuel D. Warren e Luis D. Brandais costituisce la prima vera riflessione sulla tutela della riservatezza come diritto inviolabile ed espresso magistralmente laddove si afferma che "These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone".

[3] Nella relazione di accompagnamento al Codice della Privacy viene descritto come segue: «*L'art. 1 introduce nell'ordinamento il 'diritto alla protezione dei dati personali', diritto fondamentale della persona, autonomo rispetto al più generale diritto alla riservatezza già richiamato dall'articolo 1 della legge n. 675/1996, come chiarisce anche il successivo art. 2. Un diritto che tiene conto delle molteplici prerogative legate al trattamento dei dati personali, oltre quelle attinenti al riserbo e alla tutela della vita privata. In tal modo il legislatore italiano si adegua al quadro normativo comunitario che, nella Carta dei diritti del cittadino europeo, garantisce già tale diritto fondamentale (art. 8) che si accinge ad assumere una connotazione ancora più solenne nel quadro dei lavori della Convenzione europea*». Il diritto alla protezione dei dati personali rappresenta pertanto un istituto giuridico ideato per garantire la più ampia tutela dell'individuo oltre la vita privata e quindi nelle formazioni e nelle relazioni sociali *lato sensu*, garantendo autodeterminazione decisionale e controllo sulla circolazione dei dati personali, questo istituto verrà analizzato più in dettaglio nel proseguo della trattazione.

[4] L'identità personale è l'espressione della personalità di ciascun individuo, che si manifesta nei diversi contesti e relazioni sociali, così tradizionalmente rientrano nell'identità personale, l'identità politica, l'identità religiosa, in cui l'aggettivo qualifica l'individuo come appartenente ad un determinato pensiero politico o credo religioso. Recentemente si è parlato anche dell'identità elettronica per contrapporla all'identità fisica/corporea, tramite i sistemi informatici e telematici infatti le persone acquistano diverse identità, si pensi ai forum o alle chat su internet, in cui ciascuno assume un nome utente spesso fittizio per non mostrare la propria identità reale, si ritiene peraltro che anche in questi casi siamo sempre in presenza di una manifestazione dell'identità personale. L'individuo infatti manifesta comunque il proprio pensiero attraverso uno strumento che consente di non identificarsi ovvero viene garantito l'anonimato, d'altronde il nickname altro non è che un falso nome. Le problematiche che si aprono riguardo l'identità elettronica sono molteplici, si pensi alla "sostituzione di persona" che si può verificare in particolare tramite un elaboratore elettronico, così impossessandosi del PIN di un bancomat e della carta (clonata o meno) si può accedere al conto corrente di un altro individuo prelevando denaro contante, anche tramite internet si possono intercettare i dati della carta di credito e spacciandosi per l'identità di un'altra persona si può sottrarre denaro illegalmente, il tema dell'identità personale e del furto dei dati saranno trattatati più in dettaglio nel proseguo del libro.

mento delle barriere fisiche, hanno comportato forti mutamenti di questi diritti mettendone a repentaglio la tutela e facendo sorgere un'impellente esigenza di rafforzamento della stessa.

In tal modo anche il diritto all'identità personale di ciascuno, a causa dell'influenza subita dalla diffusione della tecnologia, è stato sottoposto a forti cambiamenti. Da ciò consegue che la nozione di "Diritto alla Privacy" è legata alle relazioni sociali. Difatti le informazioni che riguardano la nostra persona sono contenute in banche dati differenti e riportano solo frammenti della nostra biografia, facendo sì che l'identità personale dei singoli coincida sempre più con le informazioni tramite cui l'altro ci identifica, ci vede, ci giudica, ed in cui il ruolo giocato dagli altri è sempre più decisivo [5].

Mentre la riservatezza viene comunemente intesa come interesse contrario alla comunicazione e alla diffusione di informazioni personali, tramite qualunque mezzo, riguardanti la vita privata della persona [6]. A tal riguardo i mass media, per il loro potenziale di diffusione delle informazioni, sono sicuramente l'arma più temuta.

La prima formulazione compiuta della nozione di riservatezza come tutela della vita privata, si fa risalire storicamente alla fine del XIX secolo ed è legata al caso Samuel Dennis Warren. La vicenda coinvolgeva la vita privata di un affermato avvocato di Boston il quale veniva rincorso continuamente da orde di giornalisti per una storia legata alla moglie e si vide costretto a tutelare la propria vita privata.

Il concetto di riservatezza così come concepito agli albori della normativa della privacy è stato oramai accostato, nell'Unione europea e nei paesi più industrializzati, alla nozione di dato personale.

Tale nozione rappresenta un aspetto innovativo che merita una particolare attenzione: il dato personale rappresenta uno strumento tecnico-giuridico attraverso il quale sia il legislatore europeo che quello italiano hanno scelto di tutelare quell'insieme di diritti collegati all'identità personale, alla riservatezza, al diritto alla pro-

---

[5] L'identità è così una identità non solo "dispersa" in tanti frammenti di informazioni dislocate, ma anche "in conoscibile" da parte dell'interessato, viene così effettuata un'astrazione della personalità di ciascuno dislocata nel mondo, diviene in tal modo estremamente difficile se non impossibile conoscere le informazioni che ci riguardano, per esempio possiamo essere del tutto ignari di essere presenti su un determinato sito web o su una banca dati pubblica o privata che sia, l'identità in tal modo è un'identità "instabile" fuori dal controllo dell'interessato, S. RODOTÀ, *Dal Soggetto alla Persona*, Editoriale Scientifica, 2007, p. 59 ss.

[6] Come è stato affermato magistralmente più di un secolo fa «se allora le decisioni indicano un diritto generale alla privacy relativo ai pensieri, emozioni e sensazioni, questi dovrebbero ricevere la stessa protezione siano essi espressi per iscritto, siano costituiti da un comportamento, una conversazione, un'attitudine od un'espressione del viso» («*If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression*»), al fine di tutelare la vita privata si prescinde perciò dalla forma di espressione dell'informazione (aspetto preso in considerazione dalla normativa sul diritto d'autore), *The right to privacy, ibid.* Tale diritto alla riservatezza è perciò un diritto tutelato in via autonoma rispetto ad altri diritti quali per esempio il diritto alla reputazione, all'immagine di una persona e all'onore.

tezione dei dati personali [7]. Il dato è perciò un contenitore vuoto all'interno del quale l'interprete inserisce di volta in volta uno specifico contenuto relativo al patrimonio informativo dell'interessato [8]. Come vedremo nel prosieguo nel corso degli anni il modello di dato personale non ha subito sostanziali modifiche anche le pronunce della Corte di Giustizia interpellate sulle questioni preliminari sembrano aver mantenuto un linea di continuità e coerenza sin da caso Lindquvist (C-101/01) sino ai più recenti casi come il caso *Patrick Breyer* (C-582/2014) su cui si è pronunciata la Corte il 19 ottobre 2016, nello stesso si conferma che gli *internet protocol* siano essi dinamici o statici sono comunque dati personali.

2. *Introduzione al concetto di dato personale nel Codice della Privacy e la sua evoluzione nel contesto sociale*

Il concetto di dato personale è estremamente importante nella normativa sulla privacy tanto da determinarne la portata applicativa. Il codice della Privacy (C.d.P.) si applica ai trattamenti dei dati personali effettuati nei territori soggetti alla sovranità dello stato, ne sono esclusi *ex* art. 5 C.d.P., i trattamenti effettuati per scopi esclusivamente personali che non siano soggetti ad una comunicazione o diffusione sistematica [9].

La metodologia di classificazione del dato personale rappresenta pertanto il principale elemento di discernimento tra l'obbligo di osservare il Codice e l'ambito di irrilevanza.

Per dato personale s'intende «*qualunque informazione relativa a persona fisica, persona giuridica ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*» (art. 4, lett. b).

Ne deriva che il dato personale è una categoria generale ed ampia che include quasi tutte le informazioni riferibili direttamente e indirettamente alla persona fisica o giuridica (ad es. nome e cognome, data di nascita, residenza, codice fiscale)

---

[7] Il nuovo diritto alla protezione dei dati personali, rappresenta effettivamente un'importante innovazione inserita con il Codice della Privacy rispetto alla legge 675/96, nell'art. 2 del Codice non si fa più solo riferimento alle persone fisiche o giuridiche ma indistintamente all'interessato, in questo modo si apre anche la possibilità di riconoscere come titolari di tali diritti una pluralità di soggetti, oltre ad aprire alla possibilità di tutelare diritti fondamentali riconosciuti in altra sede dall'ordinamento, *Relazione di accompagnamento al testo del "Codice in materia di protezione di dati personali"*.

[8] Appare condivisibile a questo riguardo quella parte della dottrina che considera il dato personale come un'entità neutra, un medio giuridico, ovvero un contenitore vuoto che è strutturalmente e funzionalmente deputato a recepire un contenuto informativo, allo stesso tempo è da considerarsi un bene giuridico di secondo grado, lo strumento tecnico per far conoscere al mondo esclusivamente quelle informazioni circoscritte e sotto il controllo del soggetto cui i dati si riferiscono.

[9] A titolo meramente informativo è opportuno sottolineare che per comunicazione di dati personali si intende portare a conoscenza degli stessi una o più persone diversi dall'interessato, mentre la diffusione si verifica quando i destinatari sono soggetti indeterminati.

compresi i suoni e le immagini. Un elenco esaustivo di tutte le informazioni che si possono ricomprendere in tale categoria è molto laborioso, così generalmente facendo degli esempi si preferisce procedere per esclusione indicando cosa viene omesso dalla stessa.

Tali informazioni, se considerate nel loro insieme e senza il riferimento al loro creatore o al loro inventore, ovvero senza riferimento agli interessati, non possono essere classificate come dati personali, ne sono un esempio l'archivio di cose, gli inventari di cose, i dati tecnici, il *know-how* e le informazioni tutelate nel codice della proprietà industriale e nella legge del diritto d'autore.

Tuttavia, come è facile immaginare la definizione contenuta nell'art. 4, lett. b), risulta a volte troppo generica e di scarso supporto per la risoluzione dei casi concreti, in tali situazioni occorre pertanto un maggiore sforzo ermeneutico per distinguere ciò che è identificabile come dato personale da cosa non lo è.

Procedendo per gradi nell'analisi della definizione, dobbiamo dapprima soffermarci sulla seguente locuzione "qualunque informazione relativa a persona fisica, persona giuridica ente od associazione", rispetto alla quale in via generale i dati personali possono distinguersi in due macrocategorie:

1. dati oggettivi, ad esempio: nome, cognome, età, sesso, componenti del sangue;
2. dati soggettivi, ad esempio opinioni o valutazioni (si pensi per esempio alle valutazioni effettuate per l'assunzione in azienda).

In tale concetto sono da includersi quindi tutte le informazioni grafiche, acustiche, numeriche, fotografiche purché siano riferibili ad una persona fisica o giuridica.

"*Identificati*" o "*identificabili*" sono invece due aggettivi che permettono di distinguere due importanti sottocategorie di informazioni:

1. dati personali che permettono *l'identificazione dell'interessato in modo diretto* (così definiti dall'art. 4, lett. c), C.d.P.), quali i dati anagrafici e quelli contrattuali, ovvero i dati presenti in ogni tipologia di elenco in cui si faccia menzione del nome e cognome di una persona;
2. informazioni attraverso le quali è possibile identificare la persona, per esempio con riferimento al contesto, le caratteristiche fisiche, colore dei capelli, statura, vestiario indossato da una persona che appartiene ad una classe o che partecipa ad un meeting.

L'altro elemento caratterizzante il dato personale è la diretta ed indiretta identificabilità dell'informazione. Mentre la diretta identificazione è un concetto di immediata comprensione, è direttamente identificabile un'informazione come il nome associato al cognome di una persona, ma in genere possono verificarsi casi dove frammenti di informazioni rendono la persona direttamente identificabile, come nel caso di una persona che possiede una macchina, una casa, un'azienda, ecc., questa informazione associata al nome può identificare direttamente la persona. La categoria delle informazioni indirettamente identificate o identificabili è invece particolarmente complessa. Si tratta infatti di una categoria di dati che non è oggetto di

una puntuale definizione nel Codice Privacy e verrà esaminata nel paragrafo seguente.

Il regolamento europeo prevede una definizione pienamente coerente con tale definizione sebbene specifichi meglio ciò che nel corso degli anno è stato chiarito dal Gruppo art. 29 (Gruppo europeo del Garanti privacy) e dalla Corte di Giustizia. L'art. 4 del regolamento al punto uno prevede che: «*"dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

La definizione del legislatore europeo sopra riportata conferma certamente la nozione presente nel Codice della Privacy ma indica in modo espresso che anche i dati di ubicazione e quindi di geolocalizzazione sono dati personali analogamente agli *internet protocol*, ai dati bimetrici, genetici, psichici, economici, culturali e sociali lo sono.

La conferma di quanto asserito sopra trova fondamento proprio nell'articolo 9 del regolamento UE 2016/679, il quale menziona tra i dati particolari (dati sensibili) i dati biometrici e genetici, mentre l'art. 4 lett. a) del regolamento menziona sia i dati relativi all'ubicazione e l'identificativo online dell'interessato.

3. *Modelli possibili di classificazione di dato personale*

Sulla nozione di dato personale e su quella di indiretta identificabilità delle informazioni alcuni anni fa è stato effettuato un autorevole studio condotto dall'Università di Sheffield e pubblicato sinteticamente in italiano tramite una newsletter del Garante per la protezione dei dati personali, newsletter 15-12 novembre 2004, n. 234.

La nozione di dato personale che emerge da questo prestigioso studio è basata su quanto prescritto dalla direttiva 95/46/CE, ed è il risultato di diversi modelli teorici di classificazione del dato personale, tra cui:

1. *Modello identificatore univoco*, secondo cui la valutazione del dato personale prescinde dal contesto. Questo modello riduce considerevolmente la quantità di dati classificabili, ne deriva una gerarchia di classi dal DNA e, via via, a tutti gli altri a seguire.

2. *Modello degli effetti indipendenti dal contesto*, il quale ha l'obiettivo di trovare un giudizio affidabile sugli effetti che una data informazione può avere su di una persona fisica a prescindere dal contesto. Alcuni studiosi hanno mosso delle critiche a questo modello in quanto esso prende a riferimento un contesto stabile e valevole per tutti e non tiene conto di aspetti dinamici quali quelli legati ai cambiamenti del contesto sociale. Secondo altri, inoltre, tale approccio non sarebbe aderente ai principi comunitari.

3. *Modello delle strategie dipendenti dal contesto*, il quale presenta rischi di eccessiva estensione della classificazione dei dati personali, perché in grado di identificare o avere effetti su una persona in base al contesto di riferimento.

Una soluzione ai problemi esposti riguardo quest'ultimo modello, potrebbe essere quella di correggerlo inserendo un grado di probabilità che tenga conto delle condizioni di riferimento future e necessarie per identificare l'interessato.

Per una strategia di classificazione affidabile gli autori sottolineavano l'esigenza di un approccio composto di più modelli. Il Garante per la protezione dei dati personali, sembra accogliere in alcune pronunce un approccio simile al modello delle strategie dipendenti dal contesto, considerando personale, per es., il dato biometrico conservato con algoritmi di criptazione.

In tal caso i dati sono infatti personali poiché dopo un certo lasso di tempo l'algoritmo può essere decifrato e pertanto l'informazione diviene personale (vedasi *ex multis*, provv. Garante del 21 luglio 2004). In tal senso si è espresso il CNIPA [10], tale orientamento trova conforto anche nella posizione assunta dal Gruppo dei Garanti Europei per la tutela dei dati personali [11].

Sono pertanto da considerarsi indirettamente identificativi i seguenti dati: codici fiscali, codici numerici e alfanumerici, dati biometrici, che sono conoscibili da altri i quali anche dopo un certo lasso di tempo e tramite altre informazioni possono risalire all'interessato. In particolare, il produttore dei dispositivi di riconoscimento biometrico è sempre in grado di associare il *template* registrato sul dispositivo all'identità dell'interessato. D'altro canto questa caratteristica risulta essere connessa alla funzione principale dei dispositivi biometrici, ossia garantire maggiore certezza dell'identità negli accessi.

4. *Il modello di classificazione proposto dal Gruppo dei Garanti Europei per la protezione dei dati personali*

In verità un recente documento del Gruppo dei Garanti Europei per la tutela dei dati personali del 2007 [12], chiarifica l'approccio metodologico corretto per la classificazione dei dati personali e presenta forti analogie con il modello dipendente dal contesto.

Tale documento al fine di classificare i dati fa riferimento alla Direttiva Comunitaria 46/95/CE, ed in particolare l'art. 2, lett. a), afferma che «*il dato personale* è *qualsiasi informazione concernente una persona fisica identificata o identificabi-*

---

[10] CENTRO NAZIONALE PER L'INFORMATICA DELLA PUBBLICA AMMINISTRAZIONE, *Linee Guida per l'impiego delle tecnologie biometriche*, Quaderno n. 9.

[11] Documento di lavoro sulla biometria, adottato il 1° agosto 2003.

[12] Opinion 4/2007 on the concept of personal data, documento adottato dal Gruppo Europeo dei Garanti per la protezione dei dati personali il 20 giugno 2007.

le». 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. Tale definizione è pressoché la medesima trasfusa nel Codice della Privacy italiano, i due testi presentano delle lievi differenze e a parere dello scrivente la norma italiana fornisce più dettagliatamente i criteri per l'individuazione dell'interessato, sebbene la normativa comunitaria non menzioni la persona giuridica.

Passando ad una descrizione più specifica del documento, la definizione di dato personale [13] deve essere suddivisa in quattro punti:

1. qualsiasi informazione;
2. concernente (l'interessato a cui si riferiscono i dati);
3. identificata o identificabile (riferito all'informazione);
4. persona fisica (riferito all'interessato).

L'avverbio concernente, caratterizza le relazioni tra le informazioni e l'interessato; l'informazione può essere riferita ad una cosa, un evento o altro, si pensi per esempio all'informazione relativa alla descrizione di una casa di valore utilizzata per fini fiscali, questa informazione può essere classificata come dato personale riferito al proprietario della casa.

Si afferma che in genere ci sono tre caratteristiche affinché un'informazione identifichi l'interessato: A) il contenuto della stessa; B) la finalità per la quale viene trattata; C) il risultato.

Il primo elemento ricorre quando un'informazione concerne direttamente una persona, (per esempio il referto medico indica il paziente) e il frammento di informazione si ricollega inequivocabilmente all'interessato a prescindere dalle finalità del trattamento.

Il secondo elemento, quello della finalità, ricorre quando, tenuto conto di tutte le circostanze del caso, quel trattamento è probabile che abbia influenza sullo stato o sul comportamento dell'interessato. Per fare un esempio possiamo pensare alle informazioni contenute nel registro dei log di chiamate in entrata e in uscita in una azienda che possono, a seconda dei casi, riferirsi al personale interno, esterno, ovvero ai clienti di una azienda, quindi a seconda della finalità per la quale l'informazione viene trattata cambia anche l'interessato a cui si riferiscono.

Il terzo elemento è molto simile al precedente ma tiene conto del risultato che questa informazione potrebbe avere nella sfera giuridica dell'interessato in assenza degli altri elementi. Per esempio un sistema di rilevazione satellitare con la funzione che solo il tassista più vicino al cliente accetti la chiamata, può portare alla profilazione delle scelte operate dal tassista ed in genere ad informazioni sul suo comportamento anche solo effettuando un monitoraggio sui tragitti scelti dallo stesso.

[13] Ci si riferisce all'art. 2, lett. a) della direttiva comunitaria 46/95/CE.

Anche se l'argomento verrà trattato più avanti è opportuno chiarire fin da ora che l'identificazione può essere diretta o indiretta. Quella diretta si verifica generalmente quando nell'informazione compare il nome e cognome dell'interessato, ovvero in riferimento al contesto, l'identificazione diretta si può verificare fornendo delle caratteristiche fisiologiche e comportamentali di un individuo appartenente ad un certo gruppo limitato.

Quello che sembra decisivo nella logica dei Garanti è che per poter classificare un'informazione come dato personale si deve ricorrere ad un'unità di misura chiamata identificatore, che consiste nel frammento di informazione idoneo a fornire notizie sufficienti sull'identità dell'interessato.

In buona sostanza solo tutti i frammenti di informazione (identificatori) combinati tra loro, tenuto conto delle circostanze del contesto, sono in grado di dire se l'informazione risultante possa essere considerata o meno dato personale. È possibile quindi affermare che fornire informazioni sul primo ministro di stato costituisce un dato personale, mentre fornire una descrizione sull'età, sesso, colore dei capelli, costituisce un dato personale solo in un contesto limitato, come per esempio un gruppo di poche persone in cui è possibile distinguere l'individuo interessato dagli altri.

Con riferimento a quest'ultimo caso per citare un esempio possiamo pensare alla trasmissione televisiva "le Iene" [14], i cui autori avevano fatto prelevare dei campioni di sudore ad un gruppo di parlamentari al fine di verificare l'assunzione di droghe.

Il Garante Italiano ha affermato che nonostante la trasmissione "Le Iene" sostenesse di garantire il pieno anonimato dei campioni di sudore, questi, uniti ad altre informazioni come per esempio le circostanze di luogo e di tempo (che i parlamentari si trovassero davanti a Montecitorio ad una data ora ed altre informazioni), non consentivano il pieno anonimato ovvero tali campioni potevano portare all'identificazione di qualche parlamentare trattandosi di un gruppo limitato. Questo caso, inoltre, per la natura delle informazioni coinvolte rientrava tra quelli idonei a rilevare uno stato di salute, e come tale ancora più doveroso di tutela.

Allo stesso modo pubblicare in una rivista scientifica un referto medico con il solo nome del paziente può costituire dato personale quando quel nome resta raro nella società e anche se l'informazione è conosciuta solo da parenti e amici stretti, il contesto di riferimento unito alla quantità e qualità del frammento di informazione risultano determinanti nel classificare il dato personale.

Il contesto di riferimento viene poi ulteriormente caratterizzato dai Garanti Europei i quali considerano dato personale l'informazione che consente di identificare l'interessato tenuto conto di «*tutti i mezzi il cui utilizzo è da considerarsi ragionevolmente probabile*».

---

[14] Provvedimento del Garante, *Informazione televisiva e raccolta di dati genetici dei parlamentari: blocco del trattamento*, 10 ottobre 2006, in *Bollettino*, n. 76, ottobre 2006.

Così le impronte registrate da un dispositivo di riconoscimento ad impronte digitali per l'accesso ad un'area aziendale sono da considerarsi un dato personale poiché l'identificazione dell'interessato è ragionevolmente probabile da parte dell'incaricato o vigilatore dei dati, oppure da parte dell'impresa costruttrice del dispositivo e anche da parte del titolare del trattamento. Se il dispositivo è sicuro ed il *template* registrato viene criptato da un algoritmo complesso, è ragionevolmente probabile che il vigilatore dei dati, l'impresa costruttrice ed il titolare possano associare comunque il *template* non solo ad un codice anonimo ma al nominativo dell'interessato ed utilizzare tali dati biometrici per finalità non afferenti all'accesso in azienda [15].

Allo stesso modo un indirizzo IP è da ritenersi un dato personale, sia con riferimento all'identificabilità operata dall'amministratore di sistema di rete Lan sia con riferimento ai log file registrati dagli ISP. In particolare il dato personale sussiste qualora, tenuto conto di tutte le circostanze del caso, risulti ragionevolmente probabile che si ottengano altre informazioni che consentono l'identificazione dell'interessato, lo stesso si verifica per esempio nelle cause giudiziarie volte a far valere il diritto d'autore verso una sospetta riproduzione abusiva delle opere di ingegno. Come sopra accennato il criterio di "tutti i mezzi il cui utilizzo è da considerarsi ragionevolmente probabile" si è consolidato nel corso oltre un decennio, anche il caso Patrick Breyer (C-582/2014) su cui si è pronunciata la Corte il 19 ottobre 2016 ha confermato tale criterio e che gli Internet Protocol (IP) sono appunto dati personali nonostante i tentativi di relativizzare i dati rispetto ad uno specifico contesto e centro di imputazione di interessi giuridici.

5. *Il problema di classificare l'*Internet Protocol *(IP) come dato personale e le contraddizioni nella recente giurisprudenza sulla tutela del diritto d'autore e della privacy*

Il problema di classificare l'IP come dato personale si inserisce nel conflitto che si è aperto tra sostenitori della tutela del diritto d'autore e sostenitori della privacy. Il problema come poc'anzi accennato, si pone ad esempio per chi vuole tutelare il diritto d'autore avendo la necessità di individuare chi ha scaricato un'opera tutelata dallo stesso diritto. Per ottenere questa informazione è necessario rivolgersi all'ISP (Internet Service Provider), ossia al fornitore della connettività il quale può associare l'IP dell'utente che avrebbe scambiato illegalmente file musicali all'utenza telefonica.

---

[15] A questo riguardo il Garante italiano ha sostanzialmente escluso l'utilizzazione di dispositivi di riconoscimento di impronte digitali per la rilevazione delle presenze dei dipendenti in azienda, in tal senso si è espresso il recente provvedimento nel quale si esclude che l'accesso in banca sia esclusivamente vincolato al rilascio delle impronte digitali, Provvedimento del Garante, in *Bollettino*, n. 91, gennaio 2008.

Il problema che si pone con riguardo all'ostensione del nome del titolare dell'utenza telefonica può comportare la violazione della privacy dello stesso; l'accesso a tali informazioni è possibile solo con una pronuncia del giudice che ordina l'esibizione dei nominativi ad un terzo: l'ISP detentore del nominativo del titolare dell'utenza telefonica.

Ci sono ovviamente molti aspetti della privacy da considerare, in questa sede verrà considerato solo l'aspetto della classificazione dei dati personali coinvolto nella fattispecie.

La fattispecie analizzata è per alcuni aspetti analoga al caso giudiziario Peppermint, una società tedesca che per tutelare le proprie opere di ingegno nella distribuzione on line, nella specie file musicali scambiati in P2P, aveva conferito incarico ad uno studio legale trentino per individuare gli autori degli "scarichi illegali" di materiale on-line.

Il problema nodale è che per poter rintracciare il presunto colpevole occorre comprimere una serie di diritti, come il diritto alla riservatezza e alla protezione dei dati personali dell'utente che naviga su internet.

Dall'altra parte, gli ISP, per la legge comunitaria ed italiana, devono conservare i dati telematici *ex* art. 132 C.d.P. solo per permettere che vengano perseguiti determinati reati gravi come quelli per fini terroristici ovvero quelli a danno dei sistemi informatici e telematici e non anche per tutelare reati meno gravi come quelli previsti per la riproduzione abusiva delle opere ed in genere per tutti i reati sul diritto d'autore.

La vicenda è molto complessa, da parte dei giudici di merito ci sono state due soluzioni contrastanti. Inizialmente in un paio di ordinanze il Tribunale di Roma ha affermato la prevalenza del diritto d'autore a scapito del diritto alla protezione dei dati personali, concedendo l'ordine di esibizione dei nominativi corrispondenti agli IP di scambio delle opere di ingegno protette nei confronti degli ISP, unici soggetti che detengono tali informazioni. Successivamente, in un'altra ordinanza, il Tribunale di Roma ha rifiutato di concedere l'ostensione dei nominativi degli utenti sospettati, ai quali si voleva accedere al fine di perseguire gli autori del presunto illecito [16].

La questione che veniva prospettata riguardava effettivamente l'IP come dato personale, quindi si doveva verificare se fosse necessario farsi rilasciare un consenso da parte del titolare del trattamento dei dati personali, ovvero se si ricadesse in un'ipotesi di deroga dallo stesso. A tal riguardo l'art. 24 C.d.P. prevede i casi in cui il consenso al trattamento dei dati personali è da escludersi (c.d. esimente del consenso), lo stesso recita che il consenso non è richiesto quando «*riguarda dati relativi allo svolgimento di attività economiche [...] o comunque, per far valere o difendere un diritto in sede giudiziaria*».

---

[16] Tribunale ordinario di Roma, sezione IX civile, ordinanza di rigetto dell'ostensione dei dati del 16 luglio 2007, Peppermint Jam Records GmbH e Techland sp. Z o.o. contro Wind Telecommunication S.p.a. Il Tribunale di Roma aveva deciso invece in senso contrario con due ordinanze del 9 febbraio 2007 e del 19 agosto 2006, disponendo per l'ostensione dei dati a favore della Peppermint.

Il rilascio del consenso al trattamento dei dati sarebbe dovuto inoltre essere preceduto da una corretta informativa sulle finalità e modalità del trattamento [17]. Senza addentrarsi troppo nelle questioni tecniche, cosa inopportuna in questa sede, si può accennare che entrambi gli adempimenti del consenso e dell'informativa possono essere derogati qualora il titolare del trattamento utilizzi i dati al fine di far valere o difendere un diritto in sede giudiziaria, questa tesi ha portato alla concessione dell'ordinanza di esibizione relativa ai nomi degli utenti.

Nell'ordinanza di segno opposto, in cui si rifiuta il rilascio dell'ordinanza di esibizione dei nominativi, si sostiene la tesi dell'esistenza dell'obbligo del consenso dovuto al fatto che per trattare i dati, anche con la finalità di far valere un diritto in sede giudiziaria, sarebbe necessario già possederli per un legittimo titolo [18], allo stesso tempo sostengono, a ragione, che l'acquisizione del dato personale sia soggetta all'obbligo di notificazione.

L'obbligo di notificazione *ex* art. 37 C.d.P. ricorre qualora vi sia un trattamento di dati personali operato al fine di definire il profilo o la personalità dell'interessato. Il monitoraggio dei file Mp3 scambiati on line non è altro che l'analisi delle scelte di consumo operate sui partecipanti al P2P, quest'attività fornisce indubbiamente informazioni che consentono la profilazione degli interessati [19].

Il caso esaminato coinvolgeva poi delle altre problematiche, da una parte vi era il problema della tutela dei terzi, l'ordine di esibizione dei dati veniva concesso non nei confronti degli autori dell'illecito bensì nei confronti degli ISP terzi rispetto alla vicenda, allo stesso tempo l'obbligo di conservazione dei dati telematici a carico degli ISP era un obbligo specifico previsto solo per determinati reati contro il terrorismo e per reati contro sistemi informatici e telematici.

Su un piano tecnico, si sollevano inoltre dubbi riguardo al metodo utilizzato per il monitoraggio degli utenti nel P2P, si sostiene infatti che il metodo sia indiscriminato coinvolgendo anche dati di utenti che svolgevano un'attività del tutto legittima. In questo quadro generale, il perno della vicenda ruotava intorno alla

---

[17] L'informativa sulla privacy come sarà meglio esposto nel proseguo, rappresenta un momento essenziale e sempre necessario salvo alcune ipotesi specifiche, ed è volta a garantire i diritti dell'interessato. L'art. 13 del C.d.P. elenca gli elementi essenziali di cui si compone l'informativa, tra i quali compaiono le finalità del trattamento dei dati, le modalità del trattamento, gli elementi identificativi del titolare e le informazioni per il suo reperimento al fine di far valere i diritti dell'interessato *ex* art. 7.

[18] Peraltro tale tesi non convince, laddove si afferma che da una parte occorre il consenso per trattare l'IP degli utenti e dall'altra si afferma che il solo IP sarebbe da considerarsi almeno inizialmente un frammento di informazione diverso da un dato personale. Seguendo questo ragionamento di l'IP sarebbe, anche se temporaneamente, un'informazione anonima, in quanto tale non soggetta a principi stabiliti dal Codice della Privacy.

[19] Tra i casi soggetti all'obbligo di notificazione al Garante per la tutela dei dati personali *ex* art. 37 C.d.P. vi è quello indicato alla lett. d): dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti.

definizione di dato personale che trova in particolare fondamento nei documenti ufficiali dei Garanti europei e in quelli del Garante italiano, che doveva necessariamente essere stabile e comprensiva dell'IP in qualunque situazione lo si rilevi.

6. *Quando il frammento di informazione diviene dato personale*

Secondo quanto delineato dal recente documento adottato dai Garanti europei, un frammento di informazione va sempre riferito al contesto in cui si trova. In genere un nome fornisce direttamente l'identità di una persona ed associato con altre informazioni come luogo di residenza, età, colore dei capelli, fornisce ulteriori notizie su dove abita, come trovare la sua abitazione e di quali proprietà è titolare.

Si pensi per esempio al furto avvenuto per strada di una borsa, in cui c'è una carta di identità, con l'indirizzo, le chiavi della macchina, quelle di casa e le carte di credito. Le informazioni anagrafiche danno immediatamente l'identità dell'individuo, mentre il luogo, l'indirizzo di residenza e relativi dati anagrafici, ci rivelano dove abita e come reperire la persona, tali dati possono essere poi utilizzati per le finalità più diverse, contattare semplicemente la persona, e quindi per svolgere un'attività legale o compiere un'attività illegale come introdursi nella macchina per rubare oggetti o la macchina stessa ovvero introdursi nell'abitazione di una persona per il medesimo scopo; infine i dati contenuti sulla carta di credito ci forniscono ulteriori informazioni sul suo conto permettendoci contemporaneamente l'accesso al conto corrente ed alla sua identità elettronica, si aprono in tal caso tutte le problematiche connesse al furto dei dati e al furto di identità, di cui si tratterà nel proseguo del presente volume.

Con questi esempi, si è voluto mostrare come il concetto di dato personale sia dinamico nel senso che il frammento di informazione, per es., l'indirizzo dell'abitazione o dell'ufficio associati ad indizi come il semplice nome o le chiavi di un'auto connessi ad un certo luogo, se considerati isolatamente siano inizialmente informazioni che non consentono l'identificazione diretta della persona a cui si riferiscono, tuttavia associate ad altre informazioni come documenti, ricerche sul luogo ivi incluse le risposte dei passanti, consentono di identificare l'immagine di una persona ovvero il cognome diventando in tal modo dati personali estremamente delicati che se utilizzati in modo "improprio" potrebbero intaccare aspetti materiali ed immateriali della persona.

In tutti questi casi, siamo di fronte a dati identificativi che se utilizzati da terzi potrebbero sottrarre spazi di riservatezza e creare notevoli problemi più o meno ampi a seconda del contesto in cui vengono utilizzati.

Le informazioni che vengono acquisite senza il nome, come per esempio i connotati fisici, tipo di vestiti indossati e luogo di incontro, sono definite *indirettamente identificative*, infatti quante persone si incontrano riconoscendosi dal tipo di indumento portato in un dato incontro e allo stesso modo un numero può essere utilizzato per risalire all'identità della persona, si pensi al codice fiscale o al numero di telefono.

Il nodo cruciale è proprio quello di definire quando si è in presenza di un'informazione identificativa, quest'informazione, quando identifica la persona, è un dato personale e come tale soggetto alla tutela del C.d.P.

Tuttavia l'analisi di qualche esempio concreto mostra un certo grado di complessità nell'individuare un criterio standard che fa propendere verso un criterio di relatività [20], si pensi ad esempio, ad un individuo collocato in un gruppo di persone che può essere distinto dagli altri, come un alunno con i capelli rossi all'interno di una classe in cui è l'unico con quel colore di capelli.

Guardando l'altra faccia della medaglia, quando si fanno studi di statistica il problema è di raccogliere dati nel più assoluto anonimato, così l'età di un individuo e la sua professione, possono costituire frammenti di informazione anonimi. Ma considerati tutti i fattori in gioco, su cui si aggiunge il luogo in cui vive, la grandezza della città ed il livello di diffusione della professione, si può configurare un dato personale, si pensi per esempio al notaio di un piccolo paese.

Tra i fattori di cui si deve tenere conto c'è anche il fattore temporale, in tal modo qualora dopo un certo numero di tentativi di accesso ai dati, ovvero un certo lasso di tempo, sia comunque possibile risalire all'identità di un individuo, l'informazione viene qualificata come personale.

In base a tale impostazione, i dati memorizzati nella forma di *template* apparentemente anonimi su di un sistema di riconoscimento biometrico ad impronte digitali, sono da ritenersi invece dati personali per il semplice fatto che esiste una possibilità reale per alcuni soggetti di associare il *template* delle impronte delle dita al nominativo della persona, in tal senso vi è anche l'orientamento ormai consolidato del Garante italiano.

A tal riguardo, di importanza fondamentale è il considerando 26 della Direttiva 96/45/CE, il quale recita «*l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona*».

Come verrà analizzato nel proseguo del presente volume in particolare con riferimento ai dati biometrici, l'avverbio "ragionevolmente" riferito all'utilizzo dei mezzi fa propendere per un modello molto ampio di dato personale a supporto del modello poc'anzi descritto.

---

[20] A parere di chi scrive la relatività del criterio in questione sta nel fatto che l'identificatività dell'informazione è una qualità che si acquisisce in base al contesto e all'aspetto temporale, l'informazione diviene ragionevolmente identificativa quando un determinato contesto anche soggettivo lo consente ed anche se per un breve tempo, in quel momento si è in presenza di un dato personale identificativo, mentre la qualità di dato personale è assoluta nel senso che la tutela deve essere *erga omnes*, non solo nei confronti di coloro che rendono identificativa quell'informazione (per es,. l'alunno con i capelli rossi all'interno della classe consente di essere identificato solo da chi lo vede, questo dato personale potrebbe tuttavia comportare rischi per l'interessato se in possesso di terzi malintenzionati e deve essere pertanto tutelato secondo i principi del Codice nei confronti di tutti).

7. *Nozione di dato sensibile: nuovo approccio sulla sensibilità del dato nel Codice della Privacy e nel regolamento europeo*

7.1. *Le sottocategorie del dato personale: dati sensibili, giudiziari e semi-sensibili*

I dati personali sono perciò una macro-categoria all'interno della quale la legge distingue diverse sottocategorie. L'esigenza non è solo puramente nomenclatrice in quanto la diversa natura del dato personale necessita di un grado maggiore o minore di cautela nel compiere le operazioni di trattamento.

La legge elenca espressamente due sottocategorie: i dati sensibili e i dati giudiziari; una terza sottocategoria, sebbene non definita dal legislatore, trova origine grazie soprattutto alla prassi decisoria del Garante e verrà chiamata dato semisensibile.

7.2. *Dati sensibili e soglia di sensibilità dei dati: analisi dei singoli casi*

Il dato sensibile è un dato idoneo a rilevare determinate informazioni dell'interessato, tali informazioni per essere sensibili devono soddisfare il particolare requisito di essere attinenti ad una sfera più intima della persona, perciò la tutela di questi dati ha come scopo generale quello di garantire la libertà personale attraverso la libertà di pensiero e di opinione [21]. Mentre infatti i dati personali comuni hanno il principale scopo identificativo, i dati sensibili rilevano le convinzioni religiose, gli orientamenti politici e sindacali, fino ad arrivare ai dati "supersensibili" idonei a rilevare lo stato di salute e la vita sessuale delle persone.

Il dato sensibile ha una caratteristica peculiare che consiste nel riferirsi solo alle persone fisiche. Questa tesi sembra emergere chiaramente dal testo normativo, tra i molti esempi che si possono citare vi è l'art. 43 C.d.P. il quale prescrive i casi in cui il trasferimento dei dati all'estero (fuori dall'Unione europea) è consentito; nella lett. a) dello stesso articolo si asserisce che il trattamento è consentito quando l'interessato ha manifestato il consenso espresso e qualora si tratti di dati sensibili è richiesta la forma scritta, alla lett. h) invece si asserisce che i trattamenti di dati concernenti le persone giuridiche, associazioni ed enti sono consentiti a prescindere da un consenso espresso. Mettendo in relazione le due affermazioni si ricava che alle persone giuridiche, associazioni, enti non si riconoscono dati sensibili, e i loro dati possono essere trasferiti fuori dall'Unione europea senza il loro consenso.

Per i dati "supersensibili" ossia dati inerenti la salute e la vita sessuale, la questione relativa al loro riferimento esclusivo alle sole persone fisiche è immediata-

[21] Non sono infatti lontani gli anni in cui alcune aziende italiane effettuavano vere e proprie indagini sui propri dipendenti per conoscere tutte le informazioni personali, dall'orientamento politico a quello sindacale, un dipendente con idee riformatrici avrebbe probabilmente creato problemi all'azienda, la quale preferiva quindi assumere altre persone. Sono queste le preoccupazioni di fondo che hanno portato il legislatore ad approvare l'art. 8 sull'insindacabilità dell'opinione dei dipendenti nello statuto dei lavoratori (legge n. 300/1970).

mente intuitiva, infatti non avrebbe senso parlare di stato di salute di una persona giuridica, se non con riferimento allo stato economico-patrimoniale, né tanto meno avrebbe senso porsi il problema della sessualità di una persona giuridica. Riflessioni importanti sulla sensibilità dei dati sono riportati nella sentenza della Corte di Giustizia europea C 101/01, i giudici di Lussemburgo si sono trovati a dover decidere se l'immagine prodotta su internet di una signora ferita ad un piede fosse da ritenersi in primo luogo trattamento di dati personali nell'ambito della direttiva 45/96/CE. A tal riguardo, l'Avvocato generale affermava quanto segue: «*Ai sensi dell'art. 3, n. 2, primo trattino, della direttiva 95/46/CE, non rientra nel campo di applicazione della direttiva stessa un trattamento di dati personali consistente nella creazione, senza alcun intento di sfruttamento economico, di una home page del tipo di quella in esame, che sia destinata esclusivamente a supportare l'attività di catechesi svolta, a titolo gratuito e al di fuori di qualsiasi rapporto lavorativo, in seno alla comunità parrocchiale*».

I giudici al punto 3 del dispositivo hanno affermato che il riferimento al fatto che un individuo sia ferito ad un piede è da considerarsi un dato personale rientrante nei "dati particolari dell'art. 8 comma 1 della direttiva" che concernono la salute. In questo caso i giudici di Lussemburgo hanno adottato un criterio di sensibilità dei dati, nel senso che non tutte le immagini sono sensibili, ma solo quelle che indicano determinati aspetti dell'individuo a cominciare dalla salute, ma anche la vita sessuale, opinioni politiche, l'adesione al sindacato, ecc.

Tuttavia la Corte, essendosi pronunciata limitatamente al caso a lei sottoposto, non fornisce indicazioni solide in ordine alla sensibilità del dato.

A tal riguardo, per lo studioso della materia, è interessante chiedersi come un concetto "relativo" di dato sensibile, basato sulla dicotomia dato normale-dato diverso, conduca a considerare sensibile per esempio l'immagine di un individuo che indossa abiti religiosi in un luogo pubblico, in tal caso non si ritiene che vi siano dati sensibili dal momento che la persona indossa quei determinati abiti per esercitare la sua professione, mentre un'immagine di una persona che si accinge ad entrare in un luogo di culto per assistere ad una cerimonia religiosa presenta un grado di sensibilità maggiore poiché rappresenta un indice della scelta religiosa effettuata.

D'altro canto, una nozione di sensibilità assoluta porterebbe a considerare gli esempi appena descritti come dati sempre sensibili, con conseguente obbligo di dare consenso in forma scritta e nell'impossibilità di diffondere il dato, questa nozione contrasterebbe con la nozione di sensibilità comunemente intesa e comporterebbe non pochi problemi pratici [22].

Alla luce di quanto sopra esposto, sembra che la sensibilità dell'informazione

[22] Si ricorda che in Italia infatti i dati sensibili richiedono che il consenso al trattamento dei dati stessi debba avere necessariamente forma scritta, mentre per il dato identificativo è sufficiente la forma orale, salvo poi in quest'ultimo caso dover dimostrare che il consenso sia stato effettivamente rilasciato dall'interessato.

personale debba essere intesa in senso relativo e valutata caso per caso con riferimento al contesto e alla natura intrinseca dell'informazione.

Così per proseguire con qualche esempio un'attestazione di idoneità rilasciata dal medico competente per svolgere una certa mansione aziendale non è da ritenersi dato idoneo a rilevare lo stato di salute, l'idoneità psico-fisica [23] non contiene infatti referti o diagnosi, allo stesso modo un certificato medico comunicato all'azienda non contenendo una diagnosi non può ritenersi dato sensibile.

Analogamente, sebbene siano doverosi gli opportuni distinguo in riferimento alla privacy attenuata dei personaggi pubblici, non avrebbe senso ritenere che l'immagine di un politico ritratta con il simbolo del partito di appartenenza fosse da ritenersi un dato sensibile.

È sensibile invece l'informazione di una persona che viene fotografata all'ingresso di una chiesa ovvero di una moschea, qualora l'immagine venga diffusa per una qualunque finalità su di un giornale e sempre che non vi sia consenso.

In tal caso si verificherebbe un trattamento illecito di dati sensibili, si può facilmente immaginare infatti che qualora quella persona insegni in una scuola religiosa particolarmente rigorosa nell'osservare i propri precetti etici possa ricevere contestazioni o addebiti disciplinari oltre che questioni relativi ai rapporti interpersonali sul luogo di lavoro. Allo stesso modo, si può ritenere sensibile, l'immagine di una persona comune ritratta all'ingresso di una sede di un partito politico.

Nel regolamento europeo non vi sono sostanziali cambiamenti, l'art. 9 del regolamento prevede che: «*1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*».

Come è noto già il legislatore europeo del 1995 aveva seguito l'impostazione di indicare come vietati i trattamenti relativi ai dati personali salvo non ricorrano le condizioni di legittimità previste, l'unica novità rilevante riguarda i dati biometrici che non solo sono dati personali ma sono dati particolari ovvero sensibili e pertanto

---

[23] La tesi proposta della non sensibilità delle informazioni contenute nel certificato di idoneità psicofisica, sembra contrastare tuttavia con quanto asserito nell'autorizzazione al trattamento dei dati sensibili (Autorizzazione generale 19 giungo 2008, in *Bollettino*, n. 96, giugno 2008, *Trattamento dei dati sensibili nel rapporto di lavoro*), tra le categorie di dati sensibili trattati per adempiere obblighi di legge ovvero contrattuale compaiono infatti i seguenti dati «*dati idonei a rivelare lo stato di salute, i dati raccolti e ulteriormente trattati in riferimento a invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psico-fisica a svolgere determinate mansioni, all'appartenenza a determinate categorie protette, nonché i dati contenuti nella certificazione sanitaria attestante lo stato di malattia, anche professionale dell'interessato, o comunque relativi anche all'indicazione della malattia come specifica causa di assenza del lavoratore*». A questo riguardo, quello che non appare condivisibile è che, mentre le altre informazioni sono idonee a rilevare uno stato di salute come l'indicazione di una specifica malattia, un attestato di idoneità psicofisica in cui non compare la valutazione del medico competente indica solo l'idoneità ad un certo mestiere ma non uno stato di salute, non ci sono pertanto dati sensibili.

necessitano di ulteriori cautele di cui occorrerà tenere conto sia nell'analisi dei rischi che nell'individuazione del livello adeguato di protezione e volto a mitigare i rischi.

Per quanto attiene al regolamento europeo non vi sono cambiamenti rilevanti ai fini della classificazione del dato come sensibile, l'art. 9 individua i trattamenti di categorie particolari di dati che possono essere viste come equivalenti ai dati sensibili definiti nel Codice, con la differenza della menzione dei dati biometrici. Questa categoria come specificato nel considerando 51 del regolamento individua tutte qui dati personali il cui trattamento presenta rischi significativi e per i quali come si è detto sono necessarie particolari cautele. Tuttavia, il considerando n. 51 prescrive che le fotografie non costituiscono trattamenti di dati biometrici e quindi dati particolari o sensibili (questi due aggettivi da intendersi con significato intercambiabile), essendo necessario che il trattamento avvenga con dispositivi di riconoscimento biometrico.

8. *Nozione di dato giudiziario nel Codice della Privacy e nel regolamento europeo*

I dati giudiziari sono dati personali idonei a rivelare: i provvedimenti iscritti nel casellario giudiziale [24]; le sanzioni amministrative dipendenti da reato e relativi carichi pendenti; i dati personali idonei a rilevare la qualità di indagato o imputato. Sono pertanto da escludersi da tale definizione di dato giudiziario le informazioni relative a provvedimenti civili o amministrativi non attinenti a reati. Sono invece dati giudiziari i provvedimenti definitivi di condanna penale relativi a delitti, i provvedimenti di espulsione e di riabilitazione dei minori.

Il trattamento dei dati giudiziari è disciplinato da diverse disposizioni del C.d.P. e segue la ripartizione per i soggetti pubblici da una parte e soggetti privati ed enti pubblici economici dall'altra.

Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo per espressa autorizzazione della legge che specifichi le finalità di rilevante interesse pubblico, la tipologia dei dati e le operazioni di trattamento sui dati. Qualora la legge non contenga una disciplina dettagliata, l'ente pubblico deve adottare un regolamento interno previo parere del Garante che disciplini questi aspetti. L'art. 21 del C.d.P. disciplina i principi applicabili al trattamento dei dati giudiziari e dispone che siano applicabili i commi 2 e 4 dell'art. 20 sul trattamento dei dati sensibili in ambito pubblico.

---

[24] Sono tali ai sensi delle lett. a), o), r) e u) del d.p.r. 14 novembre 2002, n. 313, così richiamato dell'art. 4 del C.d.P., i provvedimenti giudiziari penali di condanna definitivi, anche pronunciati da autorità straniere, fatte salve le convenzioni per le quali la legge ammette la definizione per via amministrativa ovvero l'oblazione di cui all'art. 162 c.p., sono in ogni caso da iscriversi nel casellario giudiziale tutti i provvedimenti con i quali sia concessa la sospensione condizionale della pena. Sono da includere altresì i provvedimenti di riabilitazione speciali relativi ai minori, i provvedimenti di espulsione a titolo di sanzione sostitutiva.

Con riguardo al trattamento dei dati giudiziari così per il trattamento dei dati sensibili, i soggetti pubblici devono ricorrere a modalità del trattamento dei dati che garantiscano i diritti e le libertà fondamentali e la dignità dell'interessato. Inoltre, il titolare del trattamento deve osservare il principio di necessità, di esattezza e aggiornamento delle informazioni, di pertinenza e la conservazione delle informazioni non deve avvenire per un tempo eccessivo.

Per quanto attiene ai soggetti privati ed enti pubblici economici, l'art. 27 C.d.P. riporta *verbatim* quanto disposto dall'art. 20 con riguardo all'autorizzazione della legge, con la previsione aggiuntiva di un possibile intervento del Garante in merito alla definizione delle finalità di rilevante interesse pubblico, alla tipologia dei dati e alle operazioni compiute sui dati stessi.

L'aspetto che merita particolare attenzione con riferimento al trattamento dei dati giudiziari è la mancanza di un'esplicita menzione dei dati giudiziari nella disciplina del consenso, nell'art. 23 C.d.P. si disciplinano infatti i requisiti del consenso del trattamento dei dati personali, stabilendo la forma scritta per i soli dati sensibili.

L'aver omesso il consenso al trattamento dei dati giudiziari potrebbe far propendere a considerare sufficiente il solo consenso documentato (e quindi, una semplice nota documentativa sulla attività informativa svolta, escludendo la sottoscrizione autografa del consenso da parte dell'interessato) con un forte abbassamento del potere di controllo sulla circolazione dei dati giudiziari.

D'altro canto, del fatto che si tratti di un'omissione involontaria del legislatore ve ne è conferma anche nella relazione di accompagnamento al Codice della Privacy, in cui si afferma che il consenso al trattamento dei dati sensibili e giudiziari è manifestato in forma scritta [25].

Perciò mentre l'interpretazione letterale dell'art. 23 porta a ritenere che sia sufficiente il semplice consenso documentato, ciò tenendo conto in primo luogo dell'intenzione del legislatore ed in secondo luogo, che la scelta del consenso in forma scritta rispecchia una ratio di fondo del Codice volta ad equiparare le garanzie dei dati sensibili e dei dati giudiziari.

Una conferma di questa equiparazione vi è anche nell'allegato B del Codice il quale prescriveva al punto 19 (abrogato nel 2012) che il titolare di un trattamento dei dati sensibili o giudiziari era tenuto a redigere il Documento Programmatico per la Sicurezza (D.P.S.), questo documento garantiva che il titolare del trattamento dei dati sensibili e/o giudiziari adotti una serie di misure logiche, fisiche ed organizzative volte ad assicurare la sicurezza dei trattamenti dei dati personali. Per maggiori dettagli si

---

[25] Il commento riferito all'art. 23 C.d.P. afferma che «*Coerentemente con l'esigenza di razionalizzare e coordinare meglio dal punto di vista sistematico la materia, le pertinenti disposizioni di questo capo, ove possibile, sono state accorpate. In tal senso, nel medesimo art. 23 è stato aggiunto un comma il quale precisa che il consenso al trattamento dei dati sensibili e giudiziari è manifestato in forma scritta, come già previsto nella norma generale sul trattamento dei dati sensibili (art. 26, comma 1)*», Relazione parlamentare di accompagnamento al testo "Codice in materia di protezione dei dati personali".

rimanda alla parte sugli adempimenti e sulle misure di sicurezza nel quale si analizza con maggiore dettaglio il DPS e sul Registro della attività di trattamento.

Nel regolamento europeo non si ravvisa alcun cambiamento sul piano definitorio, l'art. 10 del regolamento recita infatti come segue: «*Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica*».

9. *Nozione di dato semisensibile: il* prior checking *(verifica preliminare)*

Si tratta di una categoria residuale che non è stata volutamente definita dal legislatore, la caratteristica principale è che a differenza delle altre categorie dei dati sensibili e giudiziari si tratta di una categoria maggiormente dinamica. In altri termini, mentre le altre due categorie trovano nelle definizioni legali le rotaie sulle quali viaggiare, per i dati semisensibili questo non accade.

Essi vengono definiti dalla prassi decisoria del Garante per la protezione dei dati personali nell'ambito del sistema di *prior checking* ovvero verifica preliminare ai sensi dell'art. 17 C.d.P. rubricato come "*Trattamento che presenta rischi specifici*".

Tale articolo dispone che «*Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti (comma 1). Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare (comma 2)*».

Il Garante per la protezione dei dati personali si è pronunciato diverse volte ai sensi dell'art. 17 del Codice in ordine al riconoscimento dei dati biometrici in azienda [26].

La mancanza di una definizione legale nel C.d.P. rende tuttavia incerta questa categoria, e fino ad ora non sembra che il corpus di pronunce in materia sia sufficiente a sopperire questa lacuna legislativa.

Il problema pratico a tal riguardo rimane il fatto che nell'incertezza interpretati-

[26] Cfr. provv. Garante 19 novembre 1999, in *Bollettino*, n. 10, p. 68; provv. Garante 21 luglio 2005, in *Bollettino*, n. 63), che ai sistemi televisivi interattivi (cfr. prescrizione del Garante 26 luglio 2006, in *Bollettino*, n. 74.