

Parte Prima

Privacy: disposizioni generali

di *Giovanni Guerra*

con la collaborazione di *Salvatore Barresi*

Capitolo 1

Il Codice privacy: principi e regole

SOMMARIO: 1. Il Codice in materia di protezione dei dati personali. – 2. Le definizioni del codice. – 2.1. La nozione di dato personale. – 2.2. La natura dei dati. – 2.3. I concetti di trattamento e di banca dati. – 2.4. I ruoli soggettivi: titolare, responsabile ed incaricato. – 3. Adempimenti e presupposti. – 3.1. I principi generali. – 3.2. L’informativa. – 3.3. I presupposti di liceità: il consenso. – 3.4. I casi di esclusione del consenso. – 3.5. Presupposti del trattamento dei dati sensibili. – 3.6. Il trasferimento di dati all’estero. – 3.7. La notificazione. – 4. Misure di sicurezza. – 4.1. Il regime della sicurezza dei dati. – 4.2. Le recenti semplificazioni. – 5. I diritti dell’interessato. – 5.1. I diritti di accesso e controllo dei dati. – 5.2. Limiti all’esercizio dei diritti. – 5.3. I diritti relativi ai dati valutativi. – 5.4. Modalità di esercizio dei diritti. – 5.5. Riscontro all’interessato. – 6. Forme di tutela. – 6.1. Tutela amministrativa. – 6.2. Il reclamo e la segnalazione. – 6.3. Il ricorso. – 6.4. La tutela giurisdizionale. – 7. Provvedimenti del Garante. – 8. I codici deontologici in materia di privacy. – 8.1. I codici di deontologia e di buona condotta. – 8.2. Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive. – 9. Le autorizzazioni del Garante. – 9.1. Le autorizzazioni generali. – 9.2. Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro. – 9.3. Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale. – 9.4. Autorizzazione al trattamento dei dati sensibili da parte dei liberi professionisti. – 9.5. Autorizzazione al trattamento dei dati sensibili da parte degli investigatori privati. – 9.6. Autorizzazione al trattamento dei dati giudiziari. – 9.7. Autorizzazione al trattamento dei dati genetici. – 10. Le responsabilità per la violazione della privacy.

1. *Il Codice in materia di protezione dei dati personali*

La disciplina sulla tutela della privacy o, meglio, sulla protezione dei dati personali fa la sua prima apparizione nel nostro Paese l’8 maggio 1997, con l’entrata in vigore della legge 31 dicembre 1996, n. 675, emanata in attuazione di disposizioni comunitarie (direttiva quadro 95/46/CE)¹ ed internazionali (Convenzione di Strasburgo n. 108 del 1981)².

¹ V. la direttiva 46/95/CE del Parlamento europeo e del Consiglio relativa “alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”.

² Sottoscritta nell’ambito del Consiglio d’Europa, la Convenzione per la protezione delle persone in relazione all’elaborazione automatica dei dati di carattere personale prevede che ogni Paese aderente presti assistenza sia a propri cittadini sia a quelli stranieri, in materia di ban-

L'introduzione di tale specifica disciplina in Italia, pur arrivando in ritardo rispetto a quanto avvenuto in altri Paesi europei che si erano già dotati di specifiche legislazioni in materia già a partire dagli anni '70 (come la Svezia e la Francia), si è subito caratterizzata nel contesto comunitario per l'elevato e rigoroso livello di garanzie e misure poste a tutela dei diritti alla riservatezza, identità e dignità delle persone, che ancora oggi non trova pari in altri sistemi.

Gli operatori in ogni campo, economico e giuridico, hanno dunque particolarmente risentito di questo passaggio "epocale" da una situazione di completa assenza di disposizioni legislative ad un complesso sistema di regole ed eccezioni sul tema, del tutto nuovo, del diritto alla protezione dei dati personali. Passaggio che ha richiesto un periodo di lungo rodaggio a livello applicativo ed interpretativo e che si è rivelato tutt'altro che indolore anche per cittadini, professionisti ed imprese che ancora faticano a prendere confidenza con gli innovativi strumenti di tutela basati su un avanzato livello di consapevolezza e di partecipazione attiva da parte degli individui.

Accanto e contestualmente alla legge n. 675/1996, contenente il corpo di principi e regole generali in tema di privacy, il Parlamento approvò all'epoca anche un'articolata legge delega, la n. 676/1996, per l'emanazione da parte del Governo di disposizioni integrative e correttive in specifici settori e materie (come P.A., giustizia, sanità, ricerca storica, statistica e scientifica, TLC), in cui era necessario rimodellare i suddetti principi in modo anche da non ostacolare il perseguimento dei rilevanti interessi perseguiti in tali ambiti.

Ciò ha comportato la proliferazione, nel corso degli anni, di un'articolata decretazione legislativa con la conseguente introduzione di una serie di disposizioni in vari campi³, finalizzate ad un'attuazione dei principi affermati nel

che dati e tutela della riservatezza, imponendo agli Stati membri di adottare una specifica normativa sulla protezione dei dati personali. La legge sulla privacy ha consentito di dare attuazione agli Accordi di Schengen (sottoscritti dall'Italia nel 1990) che prevedono la realizzazione di una struttura informatica alla quale possono accedere tutti i Paesi aderenti all'Accordo con lo scopo di favorire – per motivi di ordine e sicurezza – la circolazione dei dati riguardanti persone ricercate, espulse, scomparse o sottoposte a procedimenti penali. La partecipazione al Sistema di Informazione Schengen (SIS), imponeva il rispetto di standard minimi di protezione informatica (finalizzata ad evitare l'accesso incontrollato e non autorizzato alle banche dati) che devono essere garantiti da un'apposita Autorità.

³ V. i decreti legislativi n. 255/1997: "Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675, in materia di notificazione dei trattamenti di dati personali, a norma dell'articolo 1, comma 1, lettera f), della legge 31 dicembre 1996, n. 676"; n. 135/1998 e n. 389/1998: "Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici" n. 171/1998: "Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica"; n. 51/1999: "Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675, concernenti il personale dell'ufficio del Garante per la protezione dei dati perso-

1996, anche alla luce dell'esperienza applicativa via via maturata, che si sono venute a sovrapporre tra di loro e con le disposizioni dei regolamenti di esecuzione o attuazione nel frattempo adottati dal medesimo Governo⁴.

Dopo ben nove decreti legislativi in sette anni, in linea con gli orientamenti dell'epoca in tema di semplificazione legislativa, il Governo è stato infine delegato ad adottare un "testo unico"⁵, divenuto poi "codice" contenente tutte le disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni "connesse", al fine di coordinarvi le norme vigenti e di apportarvi le integrazioni o modificazioni necessarie sia a tale coordinamento, sia «per assicurarne la migliore attuazione».

Si arriva così al "Codice in materia di protezione dei dati personali" di cui al d.lgs. 30 giugno 2003, n. 196, in vigore dal 1° gennaio 2004⁶, che raccoglie tutte le principali norme in materia di privacy e costituisce quindi il testo base di riferimento per gli operatori del diritto.

Il Codice c.d. della privacy è dunque un unico testo di matrice solo legislativa (a differenza dei testi unici c.d. "misti", legislativo-regolamentari, precedentemente approvati), risultato di un complesso lavoro di riorganizzazione ed, in alcuni casi, di revisione delle norme, che va a sostituire tutte le precedenti normative.

Nel Codice sono previste diverse innovazioni ed armonizzazioni, con recepimento delle nuove norme comunitarie e degli indirizzi emersi a seguito dell'attività propria dell'Autorità Garante della protezione dei dati personali, nonché con integrazione di alcune normative di settore. Più che un riordino di norme preesistenti, il Codice rappresenta una vera e propria riorganizzazione della materia rispetto al previgente regime, che si muove con l'esplicito obiettivo di «assicurare un elevato livello di tutela ... nel rispetto dei principi di sem-

nali"; n. 135/1999: "Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici"; n. 281/1999: "Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica"; n. 282/1999: "Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario"; n. 467/2001: "Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'articolo 1 della legge 24 marzo 2001, n. 127".

⁴ V. il d.P.R. n. 501/1998: "Regolamento recante norme per l'organizzazione ed il funzionamento dell'Ufficio del Garante per la protezione dei dati personali, a norma dell'articolo 33, comma 3, della legge 31 dicembre 1996, n. 675" e il d.P.R. n. 318/1999: "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675".

⁵ V. la legge delega n. 127/2001: "Differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996 n. 676 in materia di trattamento di dati personali".

⁶ Anche se alcune disposizioni transitorie hanno previsto termini ulteriori per l'esecuzione di adempimenti nuovi o modificati: v. gli artt. 180 e 181 del d.lgs. n. 196/2003.

plificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento» (così come sancito dall'art. 2, comma 2 del Codice stesso).

In particolare, il Codice privacy si compone di ben 186 articoli, suddivisi in tre parti.

La prima parte si occupa delle **disposizioni generali**, riguardanti i principi generali, le definizioni e le regole “sostanziali” della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, salvo eventuali regole specifiche per i trattamenti effettuati da soggetti pubblici o privati.

La seconda parte contiene le **disposizioni relative a specifici settori** consistenti in disposizioni particolari per specifici trattamenti, ad integrazione o eccezione alle disposizioni generali.

La terza parte infine è relativa alla **tutela dell'interessato e sanzioni** e contiene appunto le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio.

Con una tecnica senza dubbio innovativa, il Codice privacy reca infine in allegato diversi codici di deontologia e di buona condotta⁷ adottati nel corso degli anni⁸ (che si caratterizzano per la loro particolare natura giuridica, come si avrà modo di spiegare nel prosieguo), nonché il disciplinare tecnico delle c.d. misure minime di sicurezza, il quale potrà essere soggetto ad adeguamento periodico, con riferimento anche all'evoluzione tecnica ed all'esperienza maturata nel settore, con successivi decreti interministeriali di natura non regolamentare (art. 36).

2. *Le definizioni del codice*

2.1. *La nozione di dato personale*

Nell'accezione comune è frequente, come abbiamo visto, l'uso della terminologia “*legge sulla privacy*” o “*codice della privacy*”, ma in realtà tale disciplina normativa⁹, impropriamente associata al concetto, più diffuso in ambito

⁷ In relazione ai codici di deontologia e di buona condotta, cfr. *infra*, par. 8.

⁸ Ai sensi dell'art. 12, comma 2, Codice privacy, i codici deontologici sono pubblicati in *Gazzetta Ufficiale* a cura del Garante e riportati nell'allegato A del medesimo Codice, con decreto del Ministero della giustizia.

⁹ Il d.lgs. n. 196/2003, e successive modificazioni ed integrazioni, recante il “Codice in materia della protezione dei dati personali”.

letterario e giornalistico, della tutela della *privacy*, ha a specifico oggetto la protezione dei dati personali (art. 1 del Codice).

Dunque, la nozione di dato personale è il perno attorno al quale ruota tutto l'impianto normativo a livello internazionale, comunitario e nazionale: è infatti attraverso l'individuazione di cautele ed accorgimenti nella gestione e circolazione di tali dati che, nella c.d. società dell'informazione¹⁰ caratterizzata appunto dalla forte espansione e diffusione delle tecnologie informatiche e telematiche (*Information and Communication Technologies – ICT: in primis*, l'Internet), possono trovare efficace tutela i diritti fondamentali della persona, quali appunto il diritto alla riservatezza, alla dignità umana ed all'identità personale (v. art. 2, comma 1, d.lgs. n. 196/2003).

Ma cosa si intende per “**dato personale**”? In base alla vigente normativa comunitaria ed italiana, dato personale è tutto ciò che, in termini informativi – a prescindere dal supporto, cartaceo o elettronico, in cui è contenuto e dalla forma con cui è rappresentato (anche un'immagine od un suono) –, sia riferito o riferibile ad una persona che sia già identificata o che possa comunque esserlo, anche indirettamente, ossia grazie alla presenza di altre informazioni (come, ad esempio, un codice numerico) che permettano comunque di poter risalire alla sua identità, pure se siano necessarie ulteriori operazioni, purché ragionevoli e possibili in termini organizzativi, tecnici ed economici.

Specificamente, l'art. 4, comma 1, lett. b), d.lgs. n. 196/2003 definisce come dato personale: «*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*».

Questa definizione, adottata sulla falsariga della direttiva 95/46/CE, è molto ampia e tale da ricomprendere, come detto, un'ampia quantità di informazioni e da rendere molto sottile la linea di demarcazione rispetto al c.d. “**dato anonimo**”, ovvero l'informazione che, in origine o a seguito di trattamento, non può in alcun modo essere associata ad una persona identificata od identificabile (art. 4, comma 1, lett. n)) e che, proprio per questo, fuoriesce completamente dall'ambito applicativo delle legislazioni in materia.

¹⁰ Con il termine società dell'informazione si indica uno dei tratti salienti della società moderna, caratterizzata dallo scambio ad altissima velocità di un enorme numero di informazioni (principalmente attraverso internet e la telefonia mobile) e nella quale l'economia si fonda ampiamente sulla produzione di servizi basati sul possesso e la manipolazione di informazioni come risorsa primaria. Il concetto è stato richiamato dalla direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico (“Direttiva sul commercio elettronico”), attuata in Italia con il d.lgs. 9 aprile 2003, n. 70.

L'identificabilità del soggetto è, quindi, la condizione base che determina se le informazioni trattate rientrano o meno nell'ambito di applicazione della norma. Questa identificabilità, come detto, è ancorata ad una sorta di regime di "ragionevolezza" in relazione ai mezzi necessari per poter identificare un soggetto, qualificati, in un altro specifico ambito (scopi statistici) ma con una definizione che qui può esser richiamata, come *«l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare l'interessato, anche in relazione alle conoscenze acquisite in base al progresso tecnico»* (art. 106, comma 2, lett. c), d.lgs. n. 196/2003)¹¹.

A determinare se i dati a disposizione sono sufficienti per effettuare l'identificazione è quindi il contesto della situazione specifica nella quale possono essere utilizzati vari criteri di combinazione/correlazione delle informazioni¹². Ciò porta ad evidenziare come il concetto di identificabilità non sia univoco, ma la sua mutevolezza rende sempre necessaria un'attenta valutazione in relazione alla situazione concreta¹³.

I diversi elementi che, accanto al presupposto dell'identificabilità della persona, portano all'individuazione di determinate informazioni come dati personali sono strettamente connessi tra loro, ma puntano tutti al concetto di "riferimento" o "riferibilità" del dato ad una persona, piuttosto che ad un concetto di "proprietà" del dato (per cui il dato può appartenere ad una persona ma, essendo riferito ad un'altra, potrà da quest'ultima essere conosciuto e controllato).

L'informazione deve essere "relativa" ad una persona (fisica o, come vedremo, giuridica), deve cioè riguardarla. In merito a questo concetto di relazione, a livello europeo il Gruppo di lavoro di cui all'art. 29 della direttiva 95/46/CE¹⁴ ha evidenziato che *«i dati concernono una persona se si riferiscono*

¹¹ V. anche il parere n. 4/2007 sul concetto di dati personali (WP 136), formulato dal Gruppo di lavoro di cui all'art. 29 della direttiva 95/46/CE.

¹² V. sempre il citato parere n. 4/2007 del Gruppo, art. 29, par. 3, p. 13, in cui si afferma che: *«Una persona può essere identificata (...) 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, etc.)»*.

¹³ V. il citato parere n. 4/2007, par. 3, p. 12: *«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")»*.

¹⁴ Si tratta appunto del Gruppo di lavoro per la protezione dei dati personali istituito ai sensi dell'art. 29 della direttiva 95/46/CE. È un organo europeo indipendente a carattere consultivo in materia di tutela dei dati e della vita privata. I suoi compiti sono illustrati all'art. 30 della direttiva 95/46/CE.

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»¹⁵.

È da notare poi che, a differenza della direttiva 95/46/CE¹⁶, la normativa italiana, estende la nozione di dato personale anche all'informazione riferita alla persona giuridica, oltre che alla persona fisica od umana (individuo). Pertanto, la disciplina del Codice della privacy trova applicazione nei confronti di tutte le attività che comportano un "maneggio" di dati relativi anche a società, enti od associazioni.

L'espressione "qualunque informazione" richiama un concetto molto ampio, senza limiti di carattere qualitativo o formale. Come è stato recentemente evidenziato dal Gruppo di lavoro *ex art. 29* con riferimento alla definizione contenuta nella medesima direttiva, in modo perfettamente calzante anche con riferimento al d.lgs. n. 196/2003: «*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*»¹⁷.

Le informazioni, oltre a poter avere qualsiasi forma (dati alfanumerici, suoni, immagini) ed essere contenute in qualsiasi supporto (elettronico, carta-

¹⁵ V. il citato parere n. 4/2007 sul concetto di dati personali, WP 136, par. 2, p. 10. Cfr. anche la Newsletter Garante privacy del 26 luglio 2007. L'informazione può quindi essere relativa ad una persona sotto vari aspetti. In questo senso ha evidenziato come una informazione possa riguardare una persona:

- perché l'oggetto dell'informazione è chiaramente una persona fisica (è il caso più semplice: i risultati di un esame medico "riguardano" il paziente che si è sottoposto all'esame);
- perché la finalità del dato raccolto è, alla luce delle circostanze specifiche, quella di "incidere" in qualche modo su una persona specifica (si pensi ad un elenco delle chiamate effettuate da una postazione telefonica in un ufficio);
- oppure, infine, perché l'informazione, se trattata, è suscettibile di generare risultati specifici sui diritti e gli interessi di una determinata persona (come nel caso del trattamento di dati di localizzazione effettuato da una società di taxi per migliorare la qualità del servizio, che però ha conseguenze importanti sui singoli tassisti in quanto il loro comportamento finisce per essere monitorabile).

¹⁶ La direttiva 95/46/CE prevede che il concetto di dato personale si riferisca solo alle persone fisiche: «*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.*

La Corte europea di giustizia ha chiarito che «*nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46/Ce a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcun'altra disposizione del diritto comunitario*» (Corte di giustizia delle Comunità europee, 6 novembre 2003, C-101/01).

¹⁷ V. il citato parere n. 4/2007 sul concetto di dati personali, WP 136, par. 1, p. 6.

ceo, biologico), possono consistere, pertanto, in considerazioni oggettive o soggettive, ossia i c.d. dati di tipo valutativo come giudizi, opinioni ed altri apprezzamenti di tipo soggettivo espressi in ambito, ad es., scolastico, professionale, medico, economico, ecc.¹⁸ – in proposito, è opportuno sottolineare come affinché un’informazione diventi “dato personale” non occorre che sia vera¹⁹ –.

2.2. La natura dei dati

Nell’ambito della più ampia nozione-contenitore di dato personale, sulla scia di quanto previsto a livello comunitario, il Codice della privacy effettua una distinzione tra alcune categorie di dati che, in ragione della loro specifica natura, sono considerate particolarmente delicate proprio per i riflessi che la loro conoscenza da parte di terzi può determinare nei confronti della vita e delle relazioni delle persone a cui si riferiscono e per i maggiori rischi che possono quindi derivare dal trattamento degli stessi dati.

A tali categorie di dati, così come definiti nel Codice, viene fatta corrispondere, poi, la previsione a livello normativo di specifiche disposizioni volte ad integrare il quadro dei principi e regole comuni con apposite, ulteriori garanzie al fine di assicurare un più rigoroso livello di tutela.

Si tratta, in primo luogo, dei c.d. **dati sensibili**. Con tale espressione vengono indicati i dati personali che sono “*idonei a rivelare*” i seguenti aspetti della persona:

¹⁸ V. l’art. 8, ultimo comma, d.lgs. n. 196/2003. Il tema dei dati di tipo valutativo è stato oggetto di particolare approfondimento nella giurisprudenza del Garante privacy, a partire dalla decisione del 2 giugno 1999 in relazione alla possibilità di considerare quali dati personali i giudizi dal datore di lavoro in note di qualifica e schede di valutazione predisposte nei confronti del dipendente.

Cfr. inoltre il citato parere n. 4/2007 sul concetto di dati personali, WP 136, par. 1, pp. 7 e 8. In merito alla forma che le informazioni possono assumere è stato puntualizzato che «*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*». In relazione al contenuto delle informazioni «*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.)*».

¹⁹ Le norme poste a protezione dei dati personali prevedono la possibilità che le informazioni non siano corrette ed attribuiscono all’interessato il diritto di accedervi nonché gli strumenti per contestarle.

- l'origine razziale ed etnica,
- le convinzioni religiose, filosofiche o di altro genere,
- le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,
- lo stato di salute e la vita sessuale (art. 4, comma 1, lett. d), d.lgs. n. 196/2003).

Pur se in presenza di un'elencazione tassativa delle categorie di informazioni che sono ricomprese nella nozione dei dati sensibili l'attività di loro concreta individuazione è resa piuttosto elastica dall'espressione "idoneo a rivelare" che consente di far rientrare in tale ambito anche informazioni che non indicano direttamente uno stato, un'appartenenza od un'altra delle situazioni dell'interessato espressamente indicate nella norma, ma che sono sufficienti a permettere comunque di ricavarle o desumerle. Ciò può avvenire, ad esempio, quando il trattamento di informazioni "comuni" permetta di risalire a dati sensibili in ragione della modalità di trattamento, della quantità di informazioni disponibili, nonché dell'abbinamento con altre informazioni – ad esempio: l'indicazione della "malattia", senza specificazione di alcuna patologia, come causale dell'assenza dal lavoro, della confessione religiosa od altro ente cui venga versato l'"otto per mille" o dell'origine razziale o etnica ricavabile, in alcuni casi, da nominativo, fotografia e paese di provenienza presenti in un documento di riconoscimento –.

Altra particolare caratteristica del dato sensibile è quella di venire a contraddistinguere in modo specifico l'identità della persona rispetto alle altre ed, alle volte, in modo tale da poter provocare discriminazioni od eventuali riflessi di carattere negativo (per cui, ad es., indicare che un individuo sta bene, gode di ottima salute o è idoneo allo svolgimento di un'attività agonistica non è considerato un dato sensibile). In tal senso, la dottrina e la giurisprudenza hanno elaborato in questi anni la definizione di dati *iper* o *super* sensibili per il sottoinsieme dei dati sulla salute e sulla vita sessuale, a causa del più rigoroso regime di tutela stabilito per il loro trattamento da alcune disposizioni del Codice (in special modo, per quanto attiene alla possibilità di loro utilizzo per la difesa giudiziaria di diritti di c.d. "pari rango": art. 26, comma 4, lett. c)).

Con riferimento ai **dati genetici**²⁰, intesi come i dati che, indipendentemente dalla tipologia, riguardino la costituzione genotipica di un individuo, ovvero i caratteri genetici trasmissibili nell'ambito di un gruppo di individui legati da vincoli di parentela, gli stessi possono essere considerati in alcuni casi alla stregua di dati sensibili, in quanto idonei a rivelare lo stato di salute degli interessati, ma non sempre perché possono essere circoscritti solo agli elementi

²⁰ Provv. Garante 22 febbraio 2007, in *G.U.* 19 marzo 2007, n. 65.

che permettono di identificare l'individuo o la famiglia genetica di appartenenza²¹.

Proprio in ragione della maggiore invasività e rischiosità per i diritti degli interessati, come detto, il trattamento dei dati sensibili richiede l'adozione di particolari garanzie e misure rispetto agli altri dati personali, anche a livello di sicurezza, ed, in particolare, per quanto concerne i soggetti privati che intendono utilizzarli è ammissibile solo sulla base del consenso scritto della persona e delle autorizzazioni generali del Garante (mentre per i soggetti pubblici è richiesta un'attenta ricognizione delle finalità di rilevante interesse pubblico che, a livello legislativo, ne legittimano il trattamento e la conseguente adozione di regolamenti attuativi: v. l'art. 20 del Codice)²².

Nell'ambito del Codice godono di una tutela pressoché equivalente a quella prevista per i dati sensibili i c.d. **dati giudiziari**, ossia «*i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale*» (art. 4, lett. e), d.lgs. n. 196/2003).

Tale definizione, collegata tecnicamente al testo unico in materia di casellario giudiziale, pur essendo stata integrata con il riferimento alla qualità di imputato o di indagato, non ha però preso in considerazione i dati relativi anche a violazioni amministrative, in attuazione di quanto previsto dalla direttiva 95/46/CE (art. 8, comma 5, il quale si riferisce ai trattamenti riguardanti "infrazioni").

Si tratta, sostanzialmente, dei soli dati che attengono ad eventuali provvedimenti giudiziari penali a carico dell'interessato che rilevano dalle iscrizioni del casellario giudiziale o procedimenti penali nei quali il medesimo interessato risulti indagato od imputato (come le informazioni desumibili eventualmente da un certificato dei carichi pendenti o riguardanti la notizia dell'avvenuta iscrizione al registro degli indagati, della comunicazione di un avviso di garanzia o di un rinvio a giudizio).

Mentre non rientrano nella categoria di dati giudiziari ai sensi del Codice della privacy le informazioni che siano relative a provvedimenti giudiziari in ambito civile ed amministrativo (quali, ad es., interdizioni, inabilitazioni, fallimenti).

Anche per il trattamento di tali dati, in modo pressoché identico ai dati

²¹ V. *infra*, par. 9.7.

²² V. *infra*, par. 3.5 sui presupposti del trattamento dei dati sensibili ed il successivo e par. 9 in relazione alle autorizzazioni del Garante.

sensibili, sono previste dal Codice garanzie particolari ed ulteriori rispetto a quelle indicate per i dati personali (come verrà illustrato nei successivi paragrafi).

I dati personali, che non rientrano nelle suddette nozioni di dati sensibili e di dati giudiziari, sono spesso indicati, nella prassi interpretativa, come dati “**comuni**”, anche se non esiste una tale definizione nel Codice privacy. Possono così essere definiti quali dati “comuni”, tutti i dati non sensibili e giudiziari che sono oggetto di trattamento quali, ad esempio, nome e cognome, indirizzo, numero di telefono, titolo di studio, codice fiscale, coordinate bancarie, ecc.

Nella prassi interpretativa è stata identificata anche la nozione dei dati c.d. “**semi-sensibili**”, con riferimento a trattamenti di dati particolari che, pur non rientrando nella definizione di “sensibili” o “giudiziari”, presentano «*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 (...)*» (art. 17, comma 1, Codice privacy). In realtà, si tratta di una definizione – quella di dati semi-sensibili – anch'essa non prevista dal legislatore e dai contorni molto incerti, perché fa riferimento ad ambiti ben più complessi, soggetti alla c.d. verifica preliminare del Garante (*prior checking* in base all'art. 20 della direttiva 95/46/CE), in cui non rileva tanto o solo la tipologia di dato, quanto la peculiarità della modalità seguita o l'impatto dell'attività svolta.

Il Codice prevede, infatti, che in tali casi il trattamento dei dati è permesso solo nel rispetto di misure ed accorgimenti che sono prescritti dal Garante a tutela dell'interessato, in applicazione dei principi sanciti dallo stesso Codice, nell'ambito di una verifica preliminare effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello da parte dei titolari coinvolti.

L'indicazione di dato semi-sensibile è emersa, inizialmente, con riferimento al trattamento dei c.d. **dati biometrici**, oggetto delle prime attività di verifica preliminare effettuate dal Garante privacy. Per la loro natura, in effetti, i dati biometrici, ossia le informazioni che possono essere ricavate dalle caratteristiche fisiche o comportamentali delle persone (ad esempio, l'immagine dell'impronta digitale, l'immagine dell'iride o della retina, la registrazione della voce), a seguito di un apposito procedimento in parte automatizzato, al fine di identificarli in modo univoco²³, si prestano teoricamente a possibili studi ed elabo-

²³ V. per la voce “Verifica preliminare” (art. 17 del Codice) – 23 novembre 2005, *Bollettino* n. 66, novembre 2005, doc. web n. 1202254, “Divieto del Garante” [art. 154, 1 d) del Codice] – 21 luglio 2005, *Bollettino* n. 63, luglio 2005, doc. web n. 1150679. Cfr. anche il Documento di lavoro sulla biometria, WP 80, del Gruppo, art. 29 e il par. 4 della deliberazione Garante n. 53

razioni diretti ad identificare anche aspetti relativi allo stato di salute degli interessati.

I dati biometrici sono in genere riportati in un modello di riferimento (c.d. *template*), che consiste in un insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.

È utile infine soffermare brevemente l'attenzione su un'ulteriore categoria di dati personali a cui il Codice Privacy dedica una specifica disciplina (nella Parte II, Titolo X, Capo I concernente il settore delle comunicazioni elettroniche): i **dati relativi al traffico** che sono appunto le informazioni riferibili ad un abbonato od utente necessarie per la trasmissione delle relative comunicazioni telefoniche e/o via internet e della loro fatturazione (art. 4, comma 2, lett. h) del Codice).

In linea con la corrispondente legislazione comunitaria²⁴, la predetta disciplina pone alcuni limiti all'utilizzo di tali dati, imponendo ai fornitori di servizi di comunicazione elettronica la regola generale di cancellarli o renderli anonimi dopo l'inoltro di ogni comunicazione (art. 123, comma 1), con talune tassative eccezioni relative alla possibilità di conservarli:

- a) per sei mesi «*a fini di documentazione in caso di contestazione della fatturazione o per la pretesa del pagamento*» e «*salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale*» (art. 123, comma 2)²⁵;
- b) per gli ulteriori periodi di tempo previsti dalla legge esclusivamente «*per finalità di accertamento e repressione dei reati*» (art. 132)²⁶.

del 23 novembre 2006, "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", doc. web n. 1364099.

²⁴ V. art. 5, par. 1, direttiva 2002/58/CE.

²⁵ Già previsto ai parr. 2 e 3 dell'art. 6 della citata direttiva 2002/58/CE. V. anche il parere n. 1/2003 sulla memorizzazione ai fini della fatturazione dei dati relativi al traffico, adottato il 29 gennaio 2003 dal Gruppo di lavoro per la tutela dei dati personali, art. 29.

²⁶ I tempi di conservazione dei dati di traffico da parte delle società telefoniche e degli altri operatori del settore per finalità di "giustizia penale" sono stati disciplinati specificamente dal d.lgs. n. 109/2008, con il quale è stata recepita in Italia la direttiva comunitaria 2006/24/CE volta ad «*armonizzare le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, relativi alla conservazione di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi*». Le disposizioni di tale decreto 109/2008 prevedono che siano conservati: (i) i dati di traffico telefonico per venti-