TUTTO CIÒ PREMESSO IL GARANTE

a) autorizza, ai sensi dell'art. 124, comma 5, del Codice, a partire dal 1° luglio 2008, tutti i fornitori di servizi di comunicazione elettronica accessibili al pubblico, sempreché essi abbiano abilitato i propri utenti a effettuare comunicazioni e a richiedere servizi da qualsiasi terminale avvalendosi per il pagamento di modalità alternative alla fatturazione, a indicare nella fatturazione dettagliata richiesta dagli abbonati, i numeri completi delle comunicazioni, a condizione che essi forniscano a tutti i propri abbonati un'idonea informativa da inserire all'interno di almeno due fatture e nel proprio sito *web*. L'informativa dovrà:
   - menzionare la decisione del fornitore di avvalersi della presente autorizzazione, specificando che tutti gli abbonati che abbiano chiesto o chiederanno la fatturazione dettagliata la riceveranno "in chiaro", salvo che non richiedano il mascheramento delle ultime tre cifre;
   - contenere l'invito, rivolto a tutti gli abbonati, che abbiano chiesto o chiederanno la fatturazione dettagliata "in chiaro", a informare coloro che utilizzino l'utenza che la fatturazione perverrà completa di tutti i numeri chiamati relativi alle comunicazioni documentate nella fatturazione dettagliata;

b) dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia anche ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti, nonché, per opportuna conoscenza, all'Autorità per le garanzie nelle comunicazioni.

Roma, 13 marzo 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

39 Schema preliminare del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria (*)

20 marzo 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 135 del Codice con il quale è stato demandato al Garante il compito di promuovere, ai sensi dell'art. 12 del medesimo Codice, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o per far valere o difendere un diritto in sede giudiziaria, in particolare da liberi professionisti o da soggetti che esercitano un'attività di investigazione privata autorizzata in conformità alla legge;

Visto il provvedimento del 16 febbraio 2006 (in G.U. 1° marzo 2006, n. 50) con il quale il Garante ha promosso il predetto codice di deontologia e di buona condotta;

Rilevato che i soggetti menzionati nel verbale della riunione del 17 marzo 2008, conclusiva della prima fase dei lavori per la redazione del codice, hanno convenuto uno schema preliminare di codice che hanno sottoposto all'esame dell'Autorità;

Visto il provvedimento del Garante del 20 luglio 2006 (in G.U. 8 agosto 2006, n. 183) con il quale è stato adottato il regolamento n. 2/2006, recante la procedura per la sottoscrizione dei codici di deontologia e di buona condotta;

VISTI gli atti d'ufficio e rilevata, sulla base di una prima verifica, la non manifesta sussistenza di profili di non conformità del codice alla normativa vigente e la conseguente esigenza di darne notizia e diffusione nei modi previsti dall'art. 6, comma 2, del menzionato regolamento n. 2/2006;

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÓ PREMESSO IL GARANTE

a) dispone la pubblicazione sul sito Internet dell'Autorità www.garanteprivacy.it dello schema preliminare del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria;
b) invita in applicazione dell'art. 6, comma 2, del regolamento n. 2/2006 del Garante i soggetti interessati ai sensi dell'art. 12 del Codice a formulare eventuali osservazioni che dovranno pervenire all'Autorità per posta elettronica entro il 30 aprile 2008, all'indirizzo: *codiceforense@garanteprivacy.it*;
c) invita, altresì, i soggetti rappresentativi o interessati a dare ampia pubblicità al predetto schema preliminare;
d) dispone la trasmissione all'Ufficio pubblicazioni leggi e decreti del Ministero della

(*) [doc. *web* n. 1503511]

giustizia di un avviso da pubblicare nella *Gazzetta Ufficiale* della Repubblica italiana, volto a rendere nota l'inserzione del medesimo schema preliminare sul predetto sito Internet.

Roma, 20 marzo 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

SCHEMA PRELIMINARE DEL CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA
PER IL TRATTAMENTO DEI DATI PERSONALI
EFFETTUATO PER SVOLGERE INVESTIGAZIONI DIFENSIVE
O PER FAR VALERE O DIFENDERE UN DIRITTO IN SEDE GIUDIZIARIA
17 marzo 2008

Preambolo

I sottoindicati soggetti sottoscrivono il presente codice di deontologia e di buona condotta sulla base delle seguenti premesse:

1. diversi soggetti, in particolare gli avvocati e i praticanti avvocati iscritti nei relativi albi e registri e chi esercita un'attività di investigazione privata autorizzata in conformità alla legge, utilizzano dati di carattere personale per svolgere investigazioni difensive collegate a un procedimento penale (l. 7 dicembre 2000, n. 397) o, comunque, per far valere o difendere un diritto in sede giudiziaria. L'utilizzo di questi dati è imprescindibile per garantire una tutela piena ed effettiva dei diritti, con particolare riguardo al diritto di difesa e al diritto alla prova: un'efficace tutela di questi due diritti non è pregiudicata, ed è anzi rafforzata, dal principio secondo cui il trattamento dei dati personali deve rispettare i diritti, le libertà fondamentali e la dignità delle persone interessate, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (artt. 1 e 2 del Codice);

2. gli specifici adattamenti e cautele previsti dalla legge o dal presente codice deontologico non possono trovare applicazione se i dati sono trattati per finalità diverse da quelle di cui all'art. 1 del presente codice;

3. consapevoli del primario interesse al legittimo esercizio del diritto di difesa e alla tutela del segreto professionale, i predetti soggetti avvertono l'esigenza di individuare aspetti specifici delle loro attività professionali, in particolare rispetto alle informazioni personali di carattere sensibile o giudiziario. Ciò, al fine di valorizzare le peculiarità delle attività di ricerca, di acquisizione, di utilizzo e di conservazione dei dati, delle dichiarazioni e dei documenti a fini difensivi, specie in sede giudiziaria, e di prevenire talune incertezze applicative che si sono a volte sviluppate e che hanno portato anche a ipotizzare inutili misure protettive non previste da alcuna disposizione e anzi contrastanti con ordinarie esigenze di funzionalità. Il primario interesse al legittimo esercizio del diritto di difesa deve essere rispettato in ogni sede, anche in occasione di accertamenti ispettivi, tenendo altresì conto dei limiti normativi all'esercizio dei diritti dell'interessato (artt. 7, 8 e 9 del Codice) previsti per finalità di tutela del diritto di difesa;

4. il trattamento dei dati per l'attività di difesa concorre alla formazione permanente del professionista e contribuisce alla realizzazione di un patrimonio di precedenti giuridici che perdura nel tempo, per ipotizzabili necessità di difesa, anche dopo l'estinzione del rapporto di mandato, oltre a essere espressione della propria attività professionale;

5. norme di legge e provvedimenti attuativi prevedono già garanzie e accorgimenti da osservare per la protezione dei dati personali utilizzati per far valere o difendere un diritto in sede giudiziaria o per svolgere investigazioni difensive. Tali cautele, che non vanno osservate se i dati sono anonimi, hanno già permesso di chiarire, ad esempio, a quali condizioni

sia lecito raccogliere informazioni personali senza consenso e senza una specifica informativa, e che è legittimo utilizzarle in modo proporzionato per esigenze di difesa anche quando il procedimento civile o penale di riferimento non sia ancora instaurato. I predetti accorgimenti e garanzie possono comportare, se non sono rispettati, l'inutilizzabilità dei dati trattati (art. 11, comma 2, del Codice). Essi riguardano, in particolare:

a) l'informativa agli interessati, che può non comprendere gli elementi già noti alla persona che fornisce i dati e può essere caratterizzata da uno stile colloquiale e da formule sintetiche adatte al rapporto fiduciario con la persona assistita o, comunque, alla prestazione professionale; essa può essere fornita, anche solo oralmente e, comunque, *una tantum* rispetto al complesso dei dati raccolti sia presso l'interessato, sia presso terzi. Ciò, con possibilità di omettere l'informativa stessa per i dati raccolti presso terzi, qualora gli stessi siano trattati solo per il periodo strettamente necessario per far valere o difendere un diritto in sede giudiziaria o per svolgere investigazioni difensive, tenendo presente che non sono raccolti presso l'interessato i dati provenienti da un rilevamento lecito a distanza, ossia tale da non interagire direttamente con l'interessato (art. 13, comma 5, lett. *b*) del Codice);

b) il consenso dell'interessato, che non va richiesto per adempiere a obblighi di legge e che non occorre, altresì, per i dati anche di natura sensibile utilizzati per perseguire finalità di difesa di un diritto anche mediante investigazioni difensive. Ciò, sia per i dati trattati nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, anche al fine di verificare con le parti se vi sia un diritto da tutelare utilmente in sede giudiziaria, sia nella fase successiva alla risoluzione, giudiziale o stragiudiziale della lite. Occorre peraltro avere cura di rispettare, se si tratta di dati idonei a rivelare lo stato di salute e la vita sessuale, il principio del "pari rango", il quale giustifica il loro trattamento quando il diritto che si intende tutelare, anche derivante da atto o fatto illecito, è "di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile" (artt. 24, comma 1, lett. *f*) e 26, comma 4, lett. *c*) del Codice; aut. gen. nn. 2/2007, 4/2007 e 6/2007; *Provv.* 9 luglio 2003 [doc. *web* n. 29832]);

c) l'accesso ai dati personali e l'esercizio degli altri diritti da parte dell'interessato rispetto al trattamento dei dati stessi; diritti per i quali è previsto, per legge, un possibile differimento nel periodo durante il quale, dal loro esercizio, può derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria (art. 8, comma 2, lett. *e*) del Codice);

d) il flusso verso l'estero dei dati trasferiti solo per finalità di svolgimento di investigazioni difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria, per il tempo a ciò strettamente necessario, trasferimento che non è pregiudicato né verso Paesi dell'Unione europea, né verso Paesi terzi (artt. 42 e 43, comma 1, lett. *e*) del Codice);

e) la notificazione dei trattamenti, che non è richiesta per innumerevoli trattamenti di dati effettuati per far valere o difendere un diritto in sede giudiziaria, o per svolgere investigazioni difensive (art. 37, comma 1, del Codice; *Prov.* 31 marzo 2004, n. 1 [doc. *web* n. 852561] e nota di chiarimenti n. 9654/33365 del 23 aprile 2004 [doc. *web* n. 993385]);

f) la designazione di incaricati e di eventuali responsabili del trattamento, considerata la facoltà di avvalersi di soggetti che possono utilizzare legittimamente i dati (colleghi, collaboratori, corrispondenti, domiciliatari, sostituti, periti, ausiliari e consulenti che non rivestano la qualità di autonomi titolari del trattamento: artt. 29 e 30 del Codice);

g) i dati particolari quali quelli genetici, per i quali sono previste già alcune cautele in particolare per ciò che riguarda il principio di proporzionalità, le misure di sicurezza, il contenuto dell'informativa agli interessati e la manifestazione del consenso (art. 90 del Codice; aut. gen. del Garante del 22 febbraio 2007);

h) l'informatica giuridica, per la quale apposite disposizioni di legge hanno individuato opportune cautele per tutelare gli interessati senza pregiudicare l'informazione scientifico-giuridica (artt. 51 e 52 del Codice);

i) l'utilizzazione di dati pubblici e di altri dati e documenti contenuti in pubblici registri, elenchi, albi, atti o documenti conoscibili da chiunque, nonché in banche

di dati, archivi ed elenchi, ivi compresi gli atti dello stato civile, dai quali possono essere estratte lecitamente informazioni personali riportate in certificazioni e attestazioni utilizzabili a fini difensivi;

6. rispetto a questo quadro, il presente codice individua alcune regole complementari di comportamento le quali costituiscono una condizione essenziale per la liceità e la correttezza del trattamento dei dati, ma non hanno diretta rilevanza sul piano degli illeciti disciplinari; esse non pregiudicano, quindi, la distinta e autonoma valenza delle norme deontologiche professionali e le scelte adottate al riguardo dai competenti organismi di settore, in particolare rispetto al codice deontologico forense. Peraltro, l'inosservanza di quest'ultimo può assumere rilievo ai fini della valutazione della liceità e correttezza del trattamento dei dati personali;

7. utile supporto alla protezione dei dati proviene anche da ulteriori princìpi già riconosciuti, in materia, dal codice di procedura penale e dallo stesso codice deontologico forense (in particolare, per quanto riguarda il dovere di segretezza e riservatezza, anche nei confronti di *ex* clienti, la rivelazione di notizie riservate o coperte dal segreto professionale, la rivelazione al pubblico del nominativo di clienti, la registrazione di colloqui tra avvocati e la corrispondenza tra colleghi), nonché da altre regole di comportamento individuate dall'Unione delle camere penali italiane o da ulteriori organismi sottoscrittori del presente codice deontologico.

CAPO I - PRINCIPI GENERALI

Art. 1 - Ambito di applicazione

1. Le disposizioni del presente codice devono essere rispettate nel trattamento di dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sia nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla sua definizione, da parte di:

a) avvocati o praticanti avvocati iscritti ad albi territoriali o ai relativi registri, sezioni ed elenchi, i quali esercitino l'attività in forma individuale, associata o societaria svolgendo, anche su mandato, un'attività in sede giurisdizionale o di consulenza o di assistenza stragiudiziale, anche avvalendosi di collaboratori, dipendenti o ausiliari, nonché da avvocati stranieri esercenti legalmente la professione sul territorio dello Stato;

b) soggetti che, sulla base di uno specifico incarico anche da parte di un difensore (aut. gen. n. 6/2007, punto n. 2), svolgano in conformità alla legge attività di investigazione privata (art. 134 r.d. 18 giugno 1931, n. 773; art. 222 norme di coordinamento del c.p.p.).

2. Le disposizioni del presente codice si applicano, altresì, a chiunque tratti dati personali per le finalità di cui al comma 1, in particolare a altri liberi professionisti o soggetti che in conformità alla legge prestino, su mandato, attività di consulenza per le medesime finalità.

CAPO II - TRATTAMENTI DA PARTE DI AVVOCATI

Art. 2 - Modalità di trattamento

1. L'avvocato organizza il trattamento anche non automatizzato dei dati personali secondo le modalità che risultino più adeguate, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle libertà e della dignità degli interessati, applicando i princìpi di finalità, necessità, proporzionalità e non eccedenza sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste, nonché di un'analisi della quantità e qualità delle informazioni che utilizza e dei possibili rischi.

2. Le decisioni relativamente a quanto previsto dal comma 1 sono adottate dal titolare del trattamento il quale resta individuato, a seconda dei casi, in:

a) un singolo professionista;

b) una pluralità di professionisti, codifensori della medesima parte assistita o che, anche al di fuori del mandato di difesa, siano stati comunque interessati a concorrere all'opera professionale quali consulenti o domiciliatari;

c) un'associazione tra professionisti o una società di professionisti.

3. Nel quadro delle adeguate istruzioni da impartire per iscritto agli incaricati del tratta-

mento da designare e ai responsabili del trattamento prescelti facoltativamente (artt. 29 e 30 del Codice), sono formulate concrete indicazioni in ordine alle modalità che tali soggetti devono osservare, a seconda del loro ruolo di sostituto processuale, di praticante avvocato con o senza abilitazione al patrocinio, di consulente tecnico di parte, perito, investigatore privato o altro ausiliario che non rivesta la qualità di autonomo titolare del trattamento, nonché di tirocinante, stagista o di persona addetta a compiti di collaborazione amministrativa.

4. Specifica attenzione è prestata all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

a) acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;
b) scambio di corrispondenza, specie per via telematica;
c) esercizio contiguo di attività autonome all'interno di uno studio;
d) utilizzo di dati di cui è dubbio l'impiego lecito, anche per effetto del ricorso a tecniche invasive;
e) utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti (tabulati di flussi telefonici e informatici, consulenze tecniche e perizie, relazioni redatte da investigatori privati);
f) custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se consultabili anche telematicamente da uffici dello stesso titolare del trattamento situati altrove;
g) acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;
h) conservazione di atti relativi ad affari definiti.

5. Se i dati sono trattati per esercitare il diritto di difesa in sede giurisdizionale, ciò può avvenire anche prima della pendenza di un procedimento, sempreché i dati medesimi risultino strettamente funzionali all'esercizio del diritto di difesa, in conformità ai princìpi di proporzionalità, di pertinenza, di completezza e di non eccedenza rispetto alle finalità difensive (art. 11 del Codice).

6. Sono utilizzati lecitamente e secondo correttezza:

a) i dati personali contenuti in pubblici registri, elenchi, albi, atti o documenti conoscibili da chiunque, nonché in banche di dati, archivi ed elenchi, ivi compresi gli atti dello stato civile, dai quali possono essere estratte lecitamente informazioni personali riportate in certificazioni e attestazioni utilizzabili a fini difensivi;
b) atti, annotazioni, dichiarazioni e informazioni acquisite nell'ambito di indagini difensive, in particolare ai sensi degli articoli 391-*bis*, 391-*ter* e 391-*quater* del codice di procedura penale, evitando l'ingiustificato rilascio di copie eventualmente richieste. Se per effetto di un conferimento accidentale, anche in sede di acquisizione di dichiarazioni e informazioni ai sensi dei medesimi articoli 391-*bis*, 391-*ter* e 391-*quater*, sono raccolti dati eccedenti e non pertinenti rispetto alle finalità difensive, tali dati, qualora non possano essere estrapolati o distrutti, formano un unico contesto, unitariamente agli altri dati raccolti.

Art. 3 - Informativa unica

1. L'avvocato può fornire in un unico contesto, anche mediante affissione nei locali dello studio o pubblicazione sul proprio sito Internet e anche utilizzando formule sintetiche e colloquiali, l'informativa sul trattamento dei dati personali (art. 13 del Codice) e le notizie che deve indicare ai sensi della disciplina sulle indagini difensive.

Art. 4 - Conservazione e cancellazione dei dati

1. La definizione di un grado di giudizio o la cessazione dello svolgimento di un incarico non comportano un'automatica dismissione dei dati. Una volta estinto il procedimento o il relativo rapporto di mandato, atti e documenti attinenti all'oggetto della difesa o delle investigazioni difensive possono essere conservati, in originale o in copia e anche in formato elettronico, qualora risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del trattamento, ferma restando la loro utilizzazione in forma anonima per finalità scientifiche. La valutazione è effettuata tenendo conto della tipologia dei dati. Se è prevista una conservazione per adempiere a un obbligo normativo, anche in

materia fiscale e di contrasto della criminalità, sono custoditi i soli dati personali effettivamente necessari per adempiere al medesimo obbligo.

2. Fermo restando quanto previsto dal codice deontologico forense in ordine alla restituzione al cliente dell'originale degli atti da questi ricevuti, e salvo quanto diversamente stabilito dalla legge, è consentito, previa comunicazione alla parte assistita, distruggere, cancellare o consegnare all'avente diritto o ai suoi eredi o aventi causa la documentazione integrale dei fascicoli degli affari trattati e le relative copie.

3. In caso di revoca o di rinuncia al mandato fiduciario o del patrocinio, la documentazione acquisita è rimessa, in originale ove detenuta in tale forma, al difensore che subentra formalmente nella difesa.

4. La titolarità del trattamento non cessa per il solo fatto della sospensione o cessazione dell'esercizio della professione. In caso di cessazione anche per sopravvenuta incapacità e qualora manchi un altro difensore anche succeduto nella difesa o nella cura dell'affare, la documentazione dei fascicoli degli affari trattati, decorso un congruo termine dalla comunicazione all'assistito, è consegnata al Consiglio dell'ordine di appartenenza ai fini della conservazione per finalità difensive.

Art. 5 - Comunicazione e diffusione di dati

1. Nei rapporti con i terzi e con la stampa possono essere rilasciate informazioni non coperte da segreto qualora sia necessario per finalità di tutela dell'assistito, ancorché non concordato con l'assistito medesimo, nel rispetto dei princìpi di finalità, liceità, correttezza, indispensabilità, pertinenza e non eccedenza di cui al Codice (art. 11), nonché dei diritti e della dignità dell'interessato e di terzi, di eventuali divieti di legge e del codice deontologico forense.

Art. 6 - Accertamenti riguardanti documentazione detenuta dal difensore

1. In occasione di accertamenti ispettivi che lo riguardano l'avvocato ha diritto ai sensi dell'articolo 159, comma 3, del Codice che vi assista il presidente del competente Consiglio dell'ordine forense o un consigliere da questo delegato. Allo stesso, se interviene e ne fa richiesta, è consegnata copia del provvedimento.

2. In sede di istanza di accesso o richiesta di comunicazione dei dati di traffico relativi a comunicazioni telefoniche in entrata ai sensi degli artt. 8, comma 2, lett. *f*) e 24, comma 1, lett. *f*) del Codice, l'avvocato attesta al fornitore di servizi di comunicazione elettronica accessibili al pubblico la sussistenza del pregiudizio effettivo e concreto che deriverebbe per lo svolgimento delle investigazioni difensive dalla mancata disponibilità dei dati, senza menzionare necessariamente il numero di repertorio di un procedimento penale.

CAPO III - TRATTAMENTI DA PARTE DI ALTRI LIBERI PROFESSIONISTI E ULTERIORI SOGGETTI

Art. 7 - Applicazione di disposizioni riguardanti gli avvocati

1. Le disposizioni di cui agli articoli 2 e 5 si applicano, salvo quanto applicabile per legge unicamente all'avvocato:

a) a liberi professionisti che prestino o su mandato dell'avvocato o unitamente a esso o, comunque, nei casi e nella misura consentita dalla legge, attività di consulenza e assistenza per far valere o difendere un diritto in sede giudiziaria o per lo svolgimento delle investigazioni difensive;

b) agli altri soggetti, di cui all'art. 1, comma 2, salvo quanto risulti obiettivamente incompatibile in relazione alla figura soggettiva o alla funzione svolta.

CAPO IV - TRATTAMENTI DA PARTE DI INVESTIGATORI PRIVATI

Art. 8 - Modalità di trattamento

1. L'investigatore privato organizza il trattamento anche non automatizzato dei dati personali secondo le modalità di cui all'articolo 2, comma 1.

2. L'investigatore privato non può intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta dei dati. Tali attività possono essere eseguite esclusivamente sulla base di apposito incarico conferito per iscritto e solo per le finalità di cui al presente codice.

3. L'atto d'incarico deve menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione è collegata, nonché i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole entro cui questa deve essere conclusa.

4. L'investigatore privato deve eseguire personalmente l'incarico ricevuto e può avvalersi solo di altri investigatori privati indicati nominativamente all'atto del conferimento dell'incarico, oppure successivamente in calce a esso qualora tale possibilità sia stata prevista nell'atto di incarico e non siano trattati dati sensibili.

5. Nel caso in cui si avvalga di collaboratori interni designati quali responsabili o incaricati del trattamento in conformità a quanto previsto dagli artt. 29 e 30 del Codice, l'investigatore privato formula concrete indicazioni in ordine alle modalità da osservare e vigila, con cadenza almeno settimanale, sulla puntuale osservanza delle norme di legge e delle istruzioni impartite. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione a essi richiesta.

6. Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova.

Art. 9 - Altre regole di comportamento

1. L'investigatore privato si astiene dal porre in essere prassi elusive di obblighi e di limiti di legge e, in particolare, conforma ai princìpi di liceità e correttezza del trattamento sanciti dal Codice:

a) l'acquisizione di dati personali presso altri titolari del trattamento, anche mediante mera consultazione, verificando che si abbia titolo per ottenerli;

b) il ricorso ad attività lecite di rilevamento, specie a distanza, e di audio/videoripresa;

c) la raccolta di dati biometrici.

2. L'investigatore privato rispetta nel trattamento dei dati le disposizioni di cui all'articolo 2, commi 4, 5 e 6 del presente codice.

Art. 10 - Conservazione e cancellazione dei dati

1. Nel rispetto dell'art. 11, comma 1, lett. *e*) del Codice i dati personali trattati dall'investigatore privato possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto. A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all'incarico conferito.

2. Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico, i quali possono consentire, anche in sede di mandato, l'eventuale conservazione temporanea di materiale strettamente personale di chi ha curato l'attività svolta, ai soli fini dell'eventuale dimostrazione della liceità e correttezza del proprio operato. Se è stato contestato il trattamento il difensore o il soggetto che ha conferito l'incarico possono anche fornire all'investigatore il materiale necessario per dimostrare la liceità e correttezza del proprio operato, per il tempo a ciò strettamente necessario.

3. La sola pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato.

Art. 11 - Informativa

1. L'investigatore privato può fornire l'informativa in un unico contesto ai sensi dell'articolo 3 del presente codice, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore, nonché la natura facoltativa del conferimento dei dati.

CAPO V - DISPOSIZIONI FINALI

Art. 12 - Monitoraggio dell'attuazione del codice

1. Ai sensi della art. 135 del Codice, i soggetti che sottoscrivono il presente codice avviano forme di collaborazione per verificare periodicamente la sua attuazione anche ai fini di un eventuale adeguamento alla luce del progresso tecnologico, dell'esperienza acquisita o di novità normative.

Art. 13 - Entrata in vigore

1. Il presente codice si applica a decorrere dal ... 2008.

40 Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (*)
14 giugno 2007

Registro delle deliberazioni
n. 23 del 14 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), anche in riferimento all'art. 154, comma 1, lett. *h*);

Esaminate le istanze (segnalazioni e quesiti) pervenute riguardo al trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico;

Ritenuta l'opportunità di individuare un quadro unitario di misure e di accorgimenti necessari e opportuni, volti a fornire orientamenti utili per cittadini e amministrazioni interessate;

Visto il testo unico delle leggi sull'ordinamento degli enti locali (d.lg. 18 agosto 2000, n. 267);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il dott. Mauro Paissan;

DELIBERA

1. di adottare le *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico"* contenute nel documento allegato quale parte integrante della presente deliberazione (Allegato 1);

2. che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 14 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

(*) *G.U.* 13 luglio 2007, n. 161
[doc. *web* n. 1417809]

LINEE-GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI DI LAVORATORI PER FINALITÀ DI GESTIONE DEL RAPPORTO DI LAVORO IN AMBITO PUBBLICO (*)

(Deliberazione n. 23 del 14 giugno 2007)

Sommario

1. Premessa
   1.1. Scopo delle linee-guida
   1.2. Ambiti considerati
2. Il rispetto dei princìpi di protezione dei dati personali
   2.1. Considerazioni generali
   2.2. Liceità, pertinenza, trasparenza
   2.3. Finalità
3. Titolare, responsabile e incaricati del trattamento
   3.1. Corretta individuazione delle figure
   3.2. Medico competente
4. Dati sensibili e rapporti di lavoro
5. Comunicazione di dati personali
   5.1. Comunicazione
   5.2. Rapporti con le organizzazioni sindacali
   5.3. Modalità di comunicazione
6. Diffusione di dati personali
   6.1. Dati relativi a concorsi e selezioni
   6.2. Dati relativi all'organizzazione degli uffici, alla retribuzione e ai titolari di cariche e incarichi pubblici
   6.3. Atti in materia di organizzazione degli uffici
   6.4. Cartellini identificativi
7. Impronte digitali e accesso al luogo di lavoro
   7.1. Princìpi generali
   7.2. Casi particolari
8. Dati idonei a rivelare lo stato di salute
   8.1. Dati sanitari
   8.2. Assenze per ragioni di salute
   8.3. Denuncia all'Inail
   8.4. Visite medico legali
   8.5. Abilitazione al porto d'armi e alla guida
   8.6. Altre informazioni relative alla salute
9. Dati idonei a rivelare le convinzioni religiose

1. Premessa

1.1. *Scopo delle linee-guida.* Per fornire indicazioni e raccomandazioni riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori alle dipendenze di datori di lavoro pubblici, il Garante ravvisa l'esigenza di adottare le presenti linee-guida, suscettibili di periodico aggiornamento, nelle quali si tiene conto di precedenti decisioni dell'Autorità.

Le presenti linee-guida seguono quelle adottate rispetto agli analoghi trattamenti effettuati da datori di lavoro privati [1], con le quali coincidono per molteplici aspetti che sono comunque riprodotti nel presente documento.

L'adozione di distinte linee-guida per il settore pubblico deriva dall'esigenza di evidenziare, nel quadro della tendenziale uniformità dei princìpi applicabili al rapporto di lavoro [2], alcune specificità che si pongono per i soggetti pubblici datori di lavoro (taluni presupposti del trattamento; speciali disposizioni che prevedono casi di necessaria comunicazione o diffusione di dati; situazioni particolari).

Come per il settore privato, le indicazioni fornite non pregiudicano l'applicazione delle disposizioni di legge o di regolamento che stabiliscono particolari divieti o limiti in relazione a taluni settori o a specifici casi di trattamento (artt. 113, 114 e 184, comma 3, del Codice).

(*) *Le note sono in calce al testo*

1.2. *Ambiti considerati.* Le tematiche prese in considerazione si riferiscono, in particolare, alla comunicazione e alla diffusione di dati e al trattamento delle informazioni sensibili (in specie, di quelli idonei a rivelare lo stato di salute e le convinzioni religiose) o di dati biometrici relativi a lavoratori alle dipendenze di pubbliche amministrazioni.

2. Il rispetto dei princìpi di protezione dei dati personali

2.1. *Considerazioni generali.* Anche per i datori di lavoro pubblici il trattamento dei dati personali è disciplinato assicurando un livello elevato di tutela dei diritti e delle libertà fondamentali e conformando il medesimo trattamento ai princìpi di semplificazione, armonizzazione ed efficacia, sia per le modalità di esercizio dei diritti, sia per l'adempimento degli obblighi da parte dei titolari del trattamento [3].

I lavoratori, nel rapporto con il proprio datore di lavoro pubblico, hanno diritto di ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei predetti diritti e libertà [4].

Assume quindi particolare rilievo la necessità che i soggetti pubblici colgano l'occasione della progressiva introduzione di nuove tecniche rispetto alle modalità tradizionali di trattamento dei dati su base cartacea per valutare preventivamente come rendere efficienti i propri sistemi informativi, individuando forme adeguate di trattamento che tutelino appieno i lavoratori.

Le cautele e gli accorgimenti devono essere opportunamente graduati tenendo conto anche delle diverse forme del trattamento e della differente natura dei dati comuni e sensibili.

2.2. *Liceità, pertinenza, trasparenza.* Il datore di lavoro pubblico può lecitamente trattare dati personali dei lavoratori nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro, avendo cura di applicare le previsioni che riguardano le proprie funzioni istituzionali o il rapporto di lavoro, contenute in leggi, regolamenti, contratti e in accordi collettivi, in modo da avvalersi di informazioni personali e modalità di trattamento proporzionate ai singoli scopi.

Il Codice in materia di protezione dei dati personali, anche in attuazione di direttive comunitarie (nn. 95/46/Ce e 2002/58/Ce), prescrive che il trattamento di dati personali per la gestione del rapporto di lavoro avvenga, in particolare:

- rispettando i princìpi di necessità, di liceità e di qualità dei dati (artt. 3 e 11 del Codice);
- attenendosi alle funzioni istituzionali e applicando i presupposti e i limiti previsti da leggi e regolamenti rilevanti per il trattamento, in particolare in materia di pubblico impiego (art. 18 del Codice);
- dando applicazione effettiva e concreta al principio di indispensabilità nel trattamento dei dati sensibili e giudiziari, il quale vieta di trattare informazioni o di effettuare operazioni che non siano realmente indispensabili per raggiungere determinate finalità previste specificamente (artt. 4, comma 1, lett. *d*) ed *e*), 22, commi 3, 5 e 9, e 112 del Codice);
- limitando il trattamento di dati sensibili e giudiziari alle sole informazioni ed operazioni di trattamento individuate e rese pubbliche con l'atto regolamentare adottato in conformità al parere del Garante (artt. 20, 21, 112 e 154 del Codice);
- informando preventivamente e adeguatamente gli interessati (art. 13 del Codice);
- adottando adeguate misure di sicurezza, idonee a preservare i dati da alcuni eventi tra cui accessi ed utilizzazioni indebiti, rispetto ai quali l'amministrazione può essere chiamata a rispondere anche civilmente e penalmente (artt. 15 e 31 e ss. del Codice).

2.3. *Finalità.* Il trattamento dei dati personali, anche sensibili, riferibili ai lavoratori deve essere orientato in concreto all'esclusivo o prevalente scopo di adempiere agli obblighi e ai compiti in materia di rapporto di lavoro e di impiego alle dipendenze delle amministrazioni pubbliche.

Oltre alle leggi e ai regolamenti, anche i contratti collettivi (nazionali e integrativi) contengono alcune previsioni che permettono di trattare lecitamente informazioni di natura personale anche per ciò che attiene all'attività sindacale (ad esempio, per determinare il trattamento economico fondamentale ed accessorio, per fruire di permessi o di aspettative sindacali, per accedere a qualifiche, per la mobilità o per la responsabilità disciplinare).

Il trattamento effettuato dal soggetto pubblico deve attenersi in concreto a queste disposizioni e restare compatibile con le finalità per le quali i dati sono stati inizialmente raccolti o già trattati (art. 11, comma 1, lett. *b*), del Codice).

Particolare attenzione deve essere posta alle disposizioni dei contratti collettivi che prevedono la conoscenza di dati da parte di organizzazioni sindacali, avendo cura che il doveroso rispetto degli obblighi di informativa, consultazione, concertazione e contrattazione che comportano la comunicazione di informazioni alle medesime organizzazioni avvenga nel rispetto dei princìpi di necessità e proporzionalità.

I soggetti pubblici potrebbero peraltro cogliere l'occasione dei rinnovi dei contratti collettivi per verificare l'attualità e la chiarezza di tali previsioni contrattuali, verificando anche la loro adeguatezza rispetto a casi che si verificano in concreto (si pensi al problema della contestuale iscrizione dei lavoratori a più organizzazioni sindacali contestata da alcuna di esse).

In questo quadro occorre anche mantenere distinti i casi in cui è prevista specificamente la comunicazione solo di dati numerici aggregati da quelli in cui, in un'ottica di trasparenza e graduazione dell'accesso delle organizzazioni sindacali ad informazioni personali che risultino necessarie per verificare in conformità alla legge la concreta applicazione delle disposizioni del contratto collettivo da parte del datore di lavoro, è invece consentita (ed è giustificata in rapporto al caso concreto) la conoscenza di dati riferiti a singoli lavoratori.

In tale ottica, nell'ambito della disciplina contrattuale, si potrebbe pertanto prevedere di regola un accesso preliminare del sindacato a dati aggregati, riferiti all'intera struttura lavorativa o a singole unità organizzative ovvero a gruppi di lavoratori e, soltanto in presenza di successive anomalie o di specifiche esigenze di verifica, consentire (in casi espressamente previsti e circostanziati) all'organizzazione sindacale di conoscere anche informazioni personali relative a singoli o a gruppi di lavoratori. Ciò sempreché, nel caso concreto, sia effettivamente necessario per dimostrare la corretta applicazione dei criteri pattuiti e la comunicazione sia limitata alle informazioni pertinenti e non eccedenti rispetto a tale scopo. Resta fermo che l'eventuale successivo trattamento illecito o non corretto delle informazioni acquisite da parte dell'organizzazione sindacale si svolge nella sfera di responsabilità della medesima organizzazione [5].

3. Titolare, responsabile e incaricati del trattamento

3.1. Corretta individuazione delle figure. Resta importante individuare correttamente i soggetti che, a diverso titolo, possono trattare i dati nell'ambito della pubblica amministrazione "titolare" del trattamento ("incaricati"; eventuali "responsabili"), definendo chiaramente le rispettive attribuzioni (artt. 4, comma 1, lett. *f*), *g*) e *h*), 28, 29 e 30 del Codice).

Rinviando per brevità di esposizione ai numerosi pronunciamenti del Garante sul tema, giova ricordare che in linea di principio, per individuare il titolare del trattamento, occorre far riferimento all'amministrazione o ente centrale o locale nel suo complesso, anziché a singole articolazioni interne o alle persone fisiche che l'amministrano o la rappresentano (ad esempio, il ministro, il direttore generale o il presidente) [6].

Nelle amministrazioni più articolate, specie di grandi dimensioni o ramificate sul territorio, è possibile che alcune figure o unità organizzative siano dotate in conformità alla legge di poteri decisionali effettivamente del tutto autonomi riguardo ai trattamenti di dati personali. In tal caso, rispettando in concreto quanto previsto dal Codice (art. 28), tali articolazioni possono essere considerate lecitamente quali "titolari" autonomi o eventuali "contitolari del trattamento" (si pensi, ad esempio, ad una singola direzione generale o area geografica di un'amministrazione ministeriale di particolare complessità organizzativa [7]).

Nel rispetto dei princìpi generali sopra richiamati in materia di trattamento di dati personali (*cfr.* punto 2), le amministrazioni devono disciplinare le modalità del trattamento, designando gli eventuali soggetti responsabili e, in ogni caso, le persone fisiche incaricate, che possono acquisire lecitamente conoscenza dei dati inerenti alla gestione del rapporto di lavoro, attenendosi alle funzioni svolte e a idonee istruzioni scritte (artt. 4, comma 1, lett. *g*) e *h*), 29 e 30).

È, infatti, facoltà delle amministrazioni designare alcuni soggetti (persone fisiche o giuridiche, enti od organismi) quali "responsabili" del trattamento, delineandone analiticamente e per iscritto i compiti attribuiti, e individuando al loro interno, se del caso, ulteriori livelli di responsabilità in base all'organizzazione delle divisioni e degli uffici o alle tipologie di trattamenti, di archivi e di dati, sempreché ciascuno di questi dimostri l'esperienza, la capacità e l'affidabilità richieste dalla legge (art. 29 del Codice).

È necessario invece che ogni lavoratore sia preposto per iscritto, in qualità di "incaricato", alle operazioni di trattamento e sia debitamente istruito in ordine all'accesso e all'utilizzo delle informazioni personali di cui può venire a conoscenza nello svolgimento della propria prestazione lavorativa. La designazione degli incaricati può essere effettuata nominativamente o, specie nell'ambito di strutture organizzative complesse, mediante atti di preposizione del lavoratore a unità organizzative per le quali venga altresì previamente individuato, per iscritto, l'ambito del trattamento consentito (art. 30 del Codice).

3.2. *Medico competente.* Anche il datore di lavoro pubblico deve svolgere alcuni trattamenti di dati in applicazione della disciplina in materia di igiene e sicurezza del lavoro (art. 1, commi 1 e 2, d.lg. n. 626/1994 e successive modificazioni e integrazioni).

Tale disciplina, che attua anche alcune direttive comunitarie e si colloca nella cornice più ampia delle misure necessarie a tutelare l'integrità psico-fisica dei lavoratori, pone direttamente in capo al medico competente in materia di igiene e sicurezza nei luoghi di lavoro la sorveglianza sanitaria obbligatoria (e, ai sensi degli artt. 16 e 17 del d.lg. n. 626/1994, il correlato trattamento dei dati contenuti in cartelle cliniche).

In questo ambito il medico competente effettua accertamenti preventivi e periodici sui lavoratori (art. 33 d.P.R. n. 303/1956; art. 16 d.lg. n. 626/1994) e istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio (in conformità alle prescrizioni contenute negli artt. 17, 59-*quinquiesdecies*, comma 2, lett. b), 59-*sexiesdecies*, 70, 72-*undecies* e 87 d.lg. n. 626/1994).

Detta cartella è custodita presso l'amministrazione "con salvaguardia del segreto professionale, e consegnata in copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne fa richiesta" (artt. 4, comma 8, e 17, comma 1, lett. d), d.lg. n. 626/1994); in caso di cessazione del rapporto di lavoro le cartelle sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro-Ispesl (artt. 59-*sexiesdecies*, comma 4, 70, comma 4, 72-*undecies*, comma 3 e 87, comma 3, lett c), d.lg. n. 626/1994), in originale e in busta chiusa [8].

In relazione a tali disposizioni, al medico competente è consentito trattare dati sanitari dei lavoratori anche mediante annotazione nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate. Ciò, quale che sia il titolare del trattamento effettuato a cura del medico.

Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali dell'amministrazione (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti) ma, come detto, "con salvaguardia del segreto professionale" [9].

Il datore di lavoro pubblico è tenuto, su parere del medico competente (o qualora quest'ultimo lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati; in questo specifico contesto il datore di lavoro può accedere al giudizio di idoneità del lavoratore allo svolgimento di date mansioni, anziché alle specifiche patologie accertate [10].

Il medico può farsi assistere da personale sanitario, anche dipendente dello stesso datore di lavoro pubblico, che deve essere designato quale incaricato del trattamento dei dati personali impartendo ad esso specifiche istruzioni per salvaguardare la segretezza delle informazioni trattate (art. 30 del Codice). In tal caso, a prescindere da quale sia il titolare del trattamento e dagli eventuali obblighi in tema di segreto d'ufficio, il medico competente deve predisporre misure idonee a garantire il rispetto del segreto professionale da parte dei propri collaboratori che non siano tenuti per legge al segreto professionale, mettendoli ad esempio a conoscenza di tali disposizioni e delle relative sanzioni (art. 10 del codice di deontologia medica del 16 dicembre 2006; art. 4 del codice deontologico per gli infermieri del maggio del 1999) [11].

4. Dati sensibili e rapporto di lavoro

Le pubbliche amministrazioni devono adottare maggiori cautele se le informazioni personali sono idonee a rivelare profili particolarmente delicati della vita privata dei propri dipendenti quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere e l'origine razziale ed etnica (art. 4, comma 1, lett. *d*), del Codice).

In linea generale il datore di lavoro pubblico può utilizzare informazioni sensibili relative al proprio personale in attuazione della normativa in materia di instaurazione e gestione di rapporti di lavoro di qualunque tipo, per finalità di formazione, nonché per concedere benefici economici e altre agevolazioni (artt. 112, 95 e 68 del Codice).

Come sopra ricordato, il datore di lavoro pubblico deve limitare il trattamento dei dati sensibili e giudiziari alle sole informazioni ed operazioni individuate e rese pubbliche con l'atto regolamentare adottato in conformità al parere del Garante (artt. 20, 21, 112 e 154 del Codice) [12].

Nel perseguire tali finalità occorre comunque rispettare i princìpi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo di dati personali e, quando non si possa prescindere dall'uso di informazioni personali sensibili o giudiziarie, di trattare dati solo in riferimento ai tipi di dati e di operazioni indispensabili in relazione alla specifica finalità di gestione del rapporto di lavoro (artt. 3 e 22 del Codice).

Scaduto il termine transitorio del 28 febbraio 2007, il trattamento da parte di un soggetto pubblico che non sia previsto da tali fonti normative è ora illecito e, oltre all'inutilizzabilità dei dati trattati, può comportare l'adozione di provvedimenti anche giudiziari di blocco o di divieto del trattamento (art. 154 del Codice; art. 3 d.l. 24 giugno 2004, n. 158, come modificato dalla l. 27 luglio 2004, n. 188; art. 11, commi 1, lett. a) e 2, del Codice) [13].

Resta ferma la possibilità per le amministrazioni che non abbiano eventualmente adottato i necessari atti regolamentari entro il suddetto termine, di provvedervi comunque con sollecitudine, al fine rendere leciti i trattamenti dei dati sensibili e giudiziari.

5. Comunicazione di dati personali

5.1. *Comunicazione.* Specifiche disposizioni legislative o regolamentari individuano i casi in cui l'amministrazione pubblica è legittimata a comunicare informazioni che riguardano i lavoratori a terzi, soggetti pubblici o privati (art. 19 del Codice).

Quando manca una tale previsione specifica non possono essere quindi comunicati dati personali del dipendente (ad esempio, quelli inerenti alla circostanza di un'avvenuta assunzione, allo status o alla qualifica ricoperta, all'irrogazione di sanzioni disciplinari, a trasferimenti del lavoratore come pure altre informazioni contenute nei contratti individuali di lavoro) a terzi quali associazioni (anche di categoria), conoscenti, familiari e parenti.

Devono ritenersi in linea generale lecite le comunicazioni a terzi di informazioni di carattere sensibile relative ad uno o più dipendenti, quando esse siano realmente indispensabili per perseguire le finalità di rilevante interesse pubblico connesse all'instaurazione e alla gestione di rapporti di lavoro da parte di soggetti pubblici di cui all'art. 112 del Codice. Tali comunicazioni possono avere ad oggetto dati individuati nei pertinenti atti regolamentari

dell'amministrazione e che siano in concreto indispensabili, pertinenti e non eccedenti in rapporto ai compiti e agli adempimenti che incombono al soggetto pubblico in qualità di datore di lavoro in base alla normativa sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche (artt. 20 e 22 del Codice) [14].

La disciplina di protezione dei dati consente inoltre al datore di lavoro pubblico di rendere conoscibili a terzi dati personali del dipendente in attuazione delle disposizioni che definiscono presupposti, modalità e limiti per l'esercizio del diritto d'accesso a documenti amministrativi (contenenti dati personali) [15] o che prevedono un determinato regime di conoscibilità per talune informazioni [16], ovvero in virtù di una delega conferita dall'interessato.

Oltre a designare i soggetti che possono venire lecitamente a conoscenza dei dati inerenti alla gestione del rapporto di lavoro, quali incaricati o responsabili del trattamento, il datore di lavoro deve adottare particolari cautele anche nelle trasmissioni di informazioni personali che possono intervenire tra i medesimi incaricati o responsabili nelle correnti attività di organizzazione e gestione del personale. In tali flussi di dati occorre evitare, in linea di principio, di fare superflui riferimenti puntuali a particolari condizioni personali riferite a singoli dipendenti, specie se riguardanti le condizioni di salute, selezionando le informazioni di volta in volta indispensabili, pertinenti e non eccedenti (artt. 11 e 22 del Codice) [17].

A tal fine, può risultare utile esplicitare delicate situazioni di disagio personale solo sulla base di espressioni generiche e utilizzando, in casi appropriati, codici numerici, come pure riportare tali informazioni -quale presupposto degli atti adottati- solo nei provvedimenti messi a disposizione presso gli uffici per eventuali interessati e controinteressati (limitandosi quindi a richiamarli anche nelle comunicazioni interne e indicando gli estremi o un estratto del loro contenuto) [18].

5.2 *Rapporti con le organizzazioni sindacali.* Le pubbliche amministrazioni possono comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o a gruppi di lavoratori: si pensi al numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate nelle varie articolazioni organizzative, agli importi di trattamenti stipendiali o accessori individuati per fasce o qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative.

Sulla base delle disposizioni dei contratti collettivi, i criteri generali e le modalità inerenti a determinati profili in materia di gestione del rapporto di lavoro sono oggetto di specifici diritti di informazione sindacale preventiva o successiva.

Ad esclusione dei casi in cui il contratto collettivo applicabile preveda espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale per verificare la corretta attuazione di taluni atti organizzativi [19], l'amministrazione può fornire alle organizzazioni sindacali dati numerici o aggregati e non anche quelli riferibili ad uno o più lavoratori individuabili [20]. É il caso, ad esempio, delle informazioni inerenti ai sistemi di valutazione dell'attività dei dirigenti, alla ripartizione delle ore di straordinario e alle relative prestazioni, nonché all'erogazione dei trattamenti accessori [21].

Resta disponibile per l'organizzazione sindacale anche la possibilità di presentare istanze di accesso a dati personali attinenti ad uno o più lavoratori su delega o procura (art. 9, comma 2, del Codice), come pure la facoltà di esercitare il diritto d'accesso a documenti amministrativi in materia di gestione del personale, nel rispetto delle condizioni, dei limiti e delle modalità previsti dalle norme vigenti e per salvaguardare un interesse giuridicamente rilevante di cui sia portatore il medesimo sindacato (artt. 59 e 60 del Codice) [22]. Il rifiuto, anche tacito, dell'accesso ai documenti amministrativi, è impugnabile presso il tribunale amministrativo regionale, la Commissione per l'accesso presso la Presidenza del Consiglio dei ministri o il difensore civico (artt. 25 e ss. l. 7 agosto 1990, n. 241; art. 6 d.P.R. 12 aprile 2006, n. 184).

L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti, in conformità alle pertinenti disposizioni del contratto applicabile [23] e alle misure di sicurezza previste dal Codice (artt. 31-35).