Provvedimenti del Garante

24. Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

Visto l'art. 27 della direttiva n. 95/46/Ce del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visti gli artt. 12 e 154, comma 1, lett. e) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), i quali attribuiscono al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto l'art. 135 del Codice con il quale è stato demandato al Garante il compito di promuovere la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuati per svolgere le 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;

Vista la deliberazione n. 31- *bis* del 20 luglio 2006 con la quale il Garante ha adottato in base all'articolo 156, comma 3, lett. a) del Codice il regolamento n. 2/2006 concernente la proce-

(*) Provvedimento del Garante n. 60 del 6 novembre 2008, Gazzetta Ufficiale 24 novembre 2008, n. 275 [doc. *web* n. 1565171]

dura per la sottoscrizione dei codici di deontologia e di buona condotta;

Vista la deliberazione n. 3 del 16 febbraio 2006, pubblicata nella Gazzetta Ufficiale della Repubblica italiana del 1° marzo 2006, con la quale il Garante ha promosso la sottoscrizione del predetto codice di deontologia e di buona condotta;

Viste le comunicazioni pervenute al Garante in risposta al citato provvedimento con le quali soggetti pubblici e privati hanno manifestato la volontà di partecipare all'adozione di tale codice e rilevato che si è anche formato un apposito gruppo di lavoro composto da rappresentanti dei predetti soggetti, ai sensi dell'art. 4 del predetto regolamento n. 2/2006;

Considerato che il testo del codice di deontologia e di buona condotta è stato oggetto di ampia diffusione anche attraverso la sua pubblicazione sul sito Internet di questa Autorità, resa nota tramite avviso sulla Gazzetta Ufficiale della Repubblica italiana dell'8 aprile 2008, n. 83, al fine di favorire il più ampio dibattito e di permettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

Viste le osservazioni pervenute a seguito di tale avviso e le modifiche apportate allo schema del codice, poi sottoscritto il 27 ottobre 2008;

Constatata la conformità del codice di deontologia e di buona condotta alle leggi e ai regolamenti anche in relazione a quanto previsto dall'art. 12 del Codice;

Visto il verbale della riunione collegiale del 2 ottobre 2008 e il successivo verbale di sottoscrizione del predetto codice del 27 ottobre 2008;

Rilevato che il rispetto delle disposizioni contenute nel codice di deontologia e di buona condotta costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici (art. 12, comma 3, del Codice);

Considerato che, ai sensi dell'art. 12, comma 2, del Codice e dell'art. 9 del menzionato regolamento n. 2/2006, il codice di deontologia e di buona condotta deve essere pubblicato a cura del Garante nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, riportato nell'Allegato A. al medesimo Codice;

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. Giuseppe Chiaravalloti;

TUTTO CIÒ PREMESSO IL GARANTE

dispone la trasmissione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere le 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, sottoscritto il 27 ottobre 2008 e che figura in allegato, quale parte integrante della presente deliberazione, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonché al Ministro della giustizia per essere riportato nell'Allegato A. al Codice.

Roma, 6 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive

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, soprattutto quando non sia tale da 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 con-

ciliazione, 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. del Garante del 9 luglio 2003);

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; del. 31 marzo 2004, n. 1 e nota di chiarimenti n. 9654/33365 del 23 aprile 2004);

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 (artt. 90 del Codice; aut. gen. del Garante del 22 febbraio 2007);

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

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 assistenza o 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 trattamento 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 e, se ne dispone, pubblicazione sul proprio sito Internet, 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 o 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 intervenuto 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. Restano ferme le prescrizioni relative al trattamento dei dati sensibili contenute in atti autorizzativi del Garante.

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 dei soggetti che hanno curato l'attività svolta, a i soli fini dell'eventuale dimostrazione della liceità e corr ettezza 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 dimostrar e la liceità e corr ettezza del pr oprio operato, per il tempo a ciò str ettamente necessario.

3. La sola pendenza del pr ocedimento al quale l'investigazione è collegata, o vvero 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 decorr ere dal 1° gennaio 2009.

25. Linee-guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero (*)

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);

Ritenuta la necessità di provvedere in relazione ai rischi connessi al trattamento di dati personali effettuato da consulenti tecnici e periti ausiliari del giudice e del pubblico ministero nell'ambito di procedimenti in sede civile, penale e amministrativa;

Rilevata l'esigenza di individuare un quadro unitario di misure e di accorgimenti necessari e opportuni, volti a fornire orientamenti utili per i professionisti interessati;

Viste le pertinenti disposizioni del codice di procedura civile (in particolare gli articoli da 61 a 64 e da 191 a 200) e del codice di procedura penale (in particolare gli articoli da 220 a 232, 359 e 360);

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

Relatore il dott. Giuseppe Chiaravalloti;

DELIBERA:

1. di adottare le "Linee-guida" contenute nel documento allegato quale parte integrante della presente deliberazione;
2. di inviare copia del presente provvedimento al Ministero della giustizia e al Consiglio superiore della magistratura, per opportuna conoscenza nonché –per quanto di rispettiva competenza– per l'adozione di ogni iniziativa ritenuta idonea alla massima diffusione presso gli uffici giudiziari interessati;

(*) Deliberazione n. 46 del 26 giugno 2008, Gazzetta Ufficiale 31 luglio 2008, n. 178 [doc. *web* n. 1534086]

3. ai sensi dell'art. 143, comma 2, del Codice, di trasmettere al Ministero della giustizia-Ufficio pubblicazione leggi e decreti copia del presente provvedimento, unitamente alle menzionate "Linee-guida", per la loro pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 26 giugno 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

LINEE-GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI DA PARTE DEI CONSULENTI TECNICI E DEI PERITI AUSILIARI DEL GIUDICE E DEL PUBBLICO MINISTERO

1. PREMESSA

1.1. *Scopo delle linee guida*

I consulenti tecnici e i periti ausiliari del giudice e del pubblico ministero coadiuvano e assistono l'autorità giudiziaria nello svolgimento delle proprie funzioni, quando ciò si rende necessario per compiere atti o esprimere valutazioni che richiedono particolari e specifiche competenze tecniche (art. 61 c.p.c.; artt. 220 e 359 c.p.p.).

L'attività svolta dai consulenti tecnici e dai periti è strettamente connessa e integrata con l'attività giurisdizionale, di cui mutua i compiti e le finalità istituzionali.

Nell'espletamento delle relative incombenze, il consulente e il perito di regola vengono a conoscenza e devono custodire, contenuti nella documentazione consegnata dall'ufficio giudiziario, anche dati personali di soggetti coinvolti a diverso titolo nelle vicende giudiziarie (quali le parti di un giudizio civile o le persone sottoposte a procedimento penale), e possono acquisire altre informazioni di natura personale nel corso delle operazioni (cfr. ad esempio, art. 194 c.p.c., richiesta di chiarimenti alle parti e assunzione di informazioni presso terzi; art. 228, comma 3, c.p.p., richiesta di notizie all'imputato, alla persona offesa o ad altre persone). L'attività dell'ausiliario comporta quindi il trattamento di diversi dati personali, talvolta di natura sensibile o di carattere giudiziario (art. 4, comma 1, lettere d) ed e) del Codice), di uno o più soggetti, persone fisiche o giuridiche.

A tali trattamenti, in quanto direttamente correlati alla trattazione giudiziaria di affari e di controversie, si applicano le norme del Codice relative ai trattamenti effettuati presso uffici giudiziari di ogni ordine e grado "per ragioni di giustizia" (art. 47, comma 2, del Codice; *cfr.* Provv. del Garante 31 dicembre 1998, [doc. *web* n. 39608]; Provv. 27 marzo 2002, [doc. *web* n. 1063421]).

Le presenti linee guida mirano a fornire indicazioni di natura generale ai professionisti nominati consulenti tecnici e periti dall'autorità giudiziaria nell'ambito di procedimenti civili, penali e ammi-

nistrativi al fine esclusivo di garantire il rispetto dei princìpi in materia di protezione dei dati personali ai sensi del Codice in materia protezione dei dati personali (d.lg. 30 giugno 2003, n. 196).

1.2. *Ambito considerato*

Le predette indicazioni non incidono sulle forme processuali che gli ausiliari devono rispettare nello svolgimento delle attività e nell'adempimento degli obblighi derivanti dall'incarico e dalle istruzioni ricevuti dall'autorità giudiziaria, come disciplinati dalle pertinenti disposizioni codicistiche.

All'interno del paragrafo 6. sono poi formulate alcune indicazioni applicabili anche ai trattamenti di dati personali effettuati dai soggetti nominati consulenti tecnici dalle parti private con riferimento a procedimenti giudiziari (artt. 87, 194, 195 e 201 c.p.c.; artt. 225 e ss., 233 e 360 c.p.p.).

2. IL RISPETTO DEI PRINCÌPI DI PROTEZIONE DEI DATI PERSONALI

2.1. *Considerazioni generali*

La peculiare disciplina posta dal Codice con riguardo ai trattamenti svolti per ragioni di giustizia (art. 47) rende non applicabili alcune disposizioni del medesimo Codice relative alle modalità di esercizio dei diritti da parte dell'interessato (art. 9), al riscontro da fornire al medesimo (art. 10), ai codici di deontologia e di buona condotta (art. 12), all'informativa agli interessati (art. 13), alla cessazione del trattamento (art. 16), al trattamento svolto da soggetti pubblici (artt. da 18 a 22), alla notificazione al Garante (artt. 37 e 38, commi da 1 a 5), a determinati obblighi di comunicazione all'Autorità, alle autorizzazioni e al trasferimento dei dati all'estero (artt. da 39 a 45), nonché ai ricorsi al Garante (artt. da 145 a 151).

Sono invece pienamente applicabili le altre pertinenti disposizioni del Codice. In particolare, il trattamento dei dati effettuato a cura di consulenti tecnici e periti deve avvenire:

- nel rispetto dei princìpi di liceità e che riguardano la qualità dei dati (art. 11);
- adottando le misure di sicurezza idonee a preservare i dati da alcuni eventi, tra i quali accessi e utilizzazioni indebite (artt. 31 e ss. e disciplinare tecnico Allegato B. al Codice).

2.2. *Liceità, finalità, esattezza, pertinenza*

Il consulente e il perito possono trattare lecitamente dati personali, nei limiti in cui ciò è necessario per il corretto adempimento dell'incarico ricevuto e solo nell'ambito dell'accertamento deman-

dato dall'autorità giudiziaria; devono rispettare, altresì, le disposizioni sulle funzioni istituzionali della medesima autorità giudiziaria contenute in leggi e regolamenti, avvalendosi in particolare di informazioni personali e di modalità di trattamento proporzionate allo scopo perseguito (art. 11, comma 1, lett. a) e b)), nel rigoroso rispetto delle istruzioni impartite dall'autorità giudiziaria.
In tale quadro, l'eventuale utilizzo incrociato di dati può ritenersi consentito se è chiaramente collegato alle indagini delegate ed è stato autorizzato dalle singole autorità giudiziarie dinanzi alle quali pendono i procedimenti o, se questi si sono conclusi, che ebbero a conferire l'incarico o da altra autorità giudiziaria competente.
Nel pieno rispetto dell'ambito e della natura dell'incarico ricevuto, il consulente e il perito sono tenuti ad acquisire, utilizzare e porre a fondamento delle proprie operazioni e valutazioni informazioni personali che, con riguardo all'oggetto dell'indagine da svolgere, siano idonee a fornire una rappresentazione (finanziaria, sanitaria, patrimoniale, relazionale, ecc.) corretta, completa e corrispondente ai dati di fatto anche quando vengono espresse valutazioni soggettive di ciascun interessato, persona fisica o giuridica. Ciò, non solo allo scopo di fornire un riscontro esauriente in relazione al compito assegnato, ma anche al fine di evitare che, da un quadro inesatto o comunque inidoneo di informazioni possa derivare nocumento all'interessato, anche nell'ottica di una non fedele rappresentazione della sua identità (art. 11, comma 1, lett. c)).
Particolare attenzione deve essere inoltre posta dal consulente e dal perito nell'acquisire e utilizzare solo le informazioni che risultino effettivamente necessarie in riferimento alle specifiche finalità di accertamento perseguite. In ossequio al principio di pertinenza nel trattamento dei dati, le relazioni e le informative fornite al magistrato ed eventualmente alle parti non devono né riportare dati, specie se di natura sensibile o di carattere giudiziario o comunque di particolare delicatezza, chiaramente non pertinenti all'oggetto dell'accertamento peritale, né contenere ingiustificatamente informazioni personali relative a soggetti estranei al procedimento (art. 11, comma 1, lett. d)).

3. COMUNICAZIONE DEI DATI

Le informazioni personali acquisite nel corso dell'accertamento possono essere comunicate alle parti, come rappresentate nel procedimento (ad esempio, attraverso propri consulenti tecnici),

con le modalità e nel rispetto dei limiti fissati dalla pertinente normativa posta a tutela della segretezza e riservatezza degli atti processuali. Fermo l'obbligo per l'ausiliare di mantenere il segreto sulle operazioni compiute (art. 226 c.p.p.; cfr. anche art. 379-*bis* c.p.), eventuali comunicazioni di dati a terzi, ove ritenute indispensabili in funzione del perseguimento delle finalità dell'indagine, restano subordinate a quanto eventualmente direttamente stabilito per legge o, comunque, a preventive e specifiche autorizzazioni rilasciate dalla competente autorità giudiziaria.

4. CONSERVAZIONE E CANCELLAZIONE DEI DATI

In riferimento ai trattamenti di dati svolti per ragioni di giustizia non è applicabile la disposizione del Codice (art. 16) relativa alla cessazione del trattamento di dati personali, evenienza che, nel caso del trattamento effettuato dal consulente e dal perito, di regola coincide con l'esaurimento dell'incarico.

Trova, peraltro, applicazione anche ai trattamenti di dati personali effettuati per ragioni di giustizia il dettato dell'art. 11, comma 1, lett. e), del Codice il quale prevede che i dati non possono essere conservati per un periodo di tempo superiore a quello necessario al perseguimento degli scopi per i quali essi sono stati raccolti e trattati.

Ne consegue che, espletato l'incarico e terminato quindi il connesso trattamento delle informazioni personali, l'ausiliario deve consegnare per il deposito agli atti del procedimento non solo la propria relazione, ma anche la documentazione consegnatagli dal magistrato e quella ulteriore acquisita nel corso dell'attività svolta, salvo quanto eventualmente stabilito da puntuali disposizioni normative o da specifiche autorizzazioni dell'autorità giudiziaria che dispongano legittimamente ed espressamente in senso contrario.

Ove non ricorrano tali ultime due ipotesi, il consulente e il perito non possono quindi conservare, in originale o in copia, in formato elettronico o su supporto cartaceo, informazioni personali acquisite nel corso dell'incarico concernenti i soggetti, persone fisiche o giuridiche, nei cui confronti hanno svolto accertamenti.

Analogamente, la documentazione acquisita nel corso delle operazioni peritali deve essere restituita integralmente al magistrato in caso di revoca o di rinuncia all'incarico da parte dell'ausiliario.

Qualora sia prevista una conservazione per adempiere a uno specifico obbligo normativo (ad

esempio, in materia fiscale o contabile), possono esser e custoditi i soli dati personali effettiv amente necessari per adempiere tale obbligo.

Eventuali, ulteriori informazioni dev ono essere quindi cancellate, oppur e trasformate in forma anonima anche per finalità scientifiche o statistiche, tale da non poter esser e comunque riferita a soggetti identificati o identificabili, anche indir ettamente, mediante riferimento a qualsiasi altra informazione (art. 4, comma 1, lett. b), del Codice).

Tutto ciò non pregiudica l'espletamento di eventuali ulteriori attività dell'ausiliare, conseguenti a richieste di chiarimenti o di supplementi di indagine, che il consulente e il perito possono soddisfare acquisendo dal fascicolo processuale, in conformità alle regole poste dai codici di rito, la documentazione necessaria per fornire i nuovi riscontri.

5. MISURE DI SICUREZZA

5.1. *Misure idonee e misure minime*

Limitatamente all'espletamento degli accertamenti, l'attività dell'ausiliare è connotata da peculiari caratteri di autonomia, in r elazione alla natura squisitamente tecnica delle indagini che si svolgono, di regola, senza l'intervento del magistrato.

Ricevuto l'incarico e sino al momento della consegna al giudice o al pubblico minister o delle risultanze dell 'attività sv olta, incombono concr etamente al consulente tecnico e al perito, riguardo ai dati personali acquisiti all 'atto dell'incarico e alle ulteriori informazioni raccolte nel corso delle operazioni, le responsabilità e gli obblighi relativi al profilo della sicurezza prescritti dal Codice.

L'ausiliare è tenuto quindi a impiegar e tutti gli accorgimenti idonei a evitar e un'indebita divulgazione delle informazioni e, al contempo, la loro perdita o distruzione, adottando, a tal fine, le misure atte a garantir e la sicur ezza dei dati e dei sistemi ev entualmente utilizzati. E gli dev e curare personalmente, con il grado di autonomia riconosciuto per legge o con l 'incarico ricevuto, sia le " misure idonee e pr eventive" cui fa riferimento l 'art. 31 del Codice, sia le " misure minime" specificamente indicate negli ar ticoli da 33 a 35 e nel disciplinar e tecnico Allegato B. al Codice, la cui mancata adozione costituisce fattispecie penalmente sanzionata (ar t. 169 del Codice). Ove reso necessario dal trattamento di dati sensibili o giudiziari effettuato con l 'ausi-

lio di strumenti elettronici, nell'ambito delle misure minime (art. 33, comma 1, lett. g) del Codice) deve essere redatto il documento programmatico sulla sicurezza, con le modalità e i contenuti previsti al punto 19. del citato disciplinare tecnico.

5.2. *Incaricati*

L'obbligo di preporre alla custodia e al trattamento dei dati personali raccolti nel corso dell'accertamento solo il personale specificamente incaricato per iscritto resta fermo anche nel caso in cui il consulente e il perito si avvalgano dell'opera di collaboratori, anche se addetti a compiti di collaborazione amministrativa (art. 30 del Codice). L'attività di tali incaricati deve essere oggetto di precise istruzioni oltre che sulle modalità e sull'ambito del trattamento consentito, anche in ordine alla scrupolosa osservanza della riservatezza relativamente ai dati di cui vengono a conoscenza.

6. I CONSULENTI TECNICI DI PARTE NEI PROCEDIMENTI GIUDIZIARI

Ferma restando ogni altra disposizione contenuta nel Codice, nei provvedimenti generali adottati dal Garante e in un codice deontologico concernente le condizioni e i limiti applicabili ai trattamenti di dati personali effettuati dai consulenti tecnici di parte nei procedimenti giudiziari, anche a tali trattamenti trovano applicazione i princìpi di liceità e che riguardano la qualità dei dati (art. 11 del Codice) e le disposizioni in materia di misure di sicurezza volte alla protezione dei dati stessi (artt. 31 e ss. e disciplinare tecnico Allegato B. al Codice).

In particolare, il consulente di parte:

- può trattare lecitamente i dati personali nei limiti in cui ciò è necessario per il corretto adempimento dell'incarico ricevuto dalla parte o dal suo difensore ai fini dello svolgimento delle indagini difensive di cui alla legge n. 397/2000 o, comunque, per far valere o difendere un diritto in sede giudiziaria (art. 11, comma 1, lett. a) e b)); dati sensibili o giudiziari possono essere utilizzati solo se ciò è indispensabile;
- può acquisire e utilizzare solo i dati personali comunque pertinenti e non eccedenti rispetto alle finalità perseguite con l'incarico ricevuto, avvalendosi di informazioni personali e di modalità di trattamento proporzionate allo scopo perseguito (art. 11, comma 1, lett. d));
- salvi i divieti di legge posti a tutela della segretezza e riservatezza delle informazioni acqui-

site nel corso di un procedimento giudiziario (cfr., ad esempio, l'art. 379-*bis* c.p.p.) e i limiti e i doveri derivanti dal segreto professionale e dal fedele espletamento dell'incarico ricevuto (cfr. artt. 380 e 381 c.p.), può comunicare a terzi dati personali solo ove ciò risulti necessario per finalità di tutela dell'assistito, limitatamente ai dati strettamente funzionali all'esercizio del diritto di difesa della parte e nel rispetto dei diritti e della dignità dell'interessato e di terzi;

- relativamente ai dati personali acquisiti e trattati nell'espletamento dell'incarico ricevuto da una parte, assume personalmente le responsabilità e gli obblighi relativi al profilo della sicurezza prescritti dal Codice, relativamente sia alle "misure idonee e preventive" (art. 31) sia alle "misure minime" (artt. da 33 a 35 e disciplinare tecnico Allegato B. al Codice; art. 169 del Codice); ove l'incarico comporti il trattamento con strumenti elettronici di dati sensibili o giudiziari, è tenuto a redigere il documento programmatico sulla sicurezza (art. 33, comma 1, lett. g) e punto 19. del disciplinare tecnico Allegato B.);
- deve incaricare per iscritto gli eventuali collaboratori, anche se adibiti a mansioni di carattere amministrativo, che siano addetti alla custodia e al trattamento, in qualsiasi forma, dei dati personali (art. 30 del Codice), impartendo loro precise istruzioni sulle modalità e l'ambito del trattamento loro consentito e sulla scrupolosa osservanza della riservatezza dei dati di cui vengono a conoscenza.

26. Il sistema Eurodac (*)

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 regolamento (Ce) n. 2725/2000 del Consiglio dell'11 dicembre 2000 che istituisce l'Eurodac per il confronto delle impronte digitali ai fini dell'efficace applicazione della Convenzione di Dublino (Convenzione sulla determinazione dello Stato competente per l'esame di una domanda di asilo presentata in uno degli Stati membri delle Comunità europee);

Visto il Codice in materia di protezione dei dati personali (d. lg. 30 giugno 2003, n. 196);

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. Giuseppe Fortunato;

PREMESSO

Il Garante per la protezione dei dati personali è l'autorità indipendente incaricata di esercitare il controllo sul trattamento dei dati a carattere personale effettuato sul territorio nazionale ai sensi del regolamento comunitario n. 2725/2000 e di verificare che la trasmissione dei dati alla banca dati centrale informatizzata, gestita dall'unità centrale istituita presso la Commissione europea, avvenga lecitamente (art. 154, comma 2, lett. d), del Codice; art. 19 reg. n. 2725/2000).

Il Garante europeo della protezione dei dati, cui sono state conferite funzioni di supervisione dell'Eurodac già svolte dall'autorità comune di controllo prevista all'articolo 20 del citato regolamento, ha individuato, in accordo con le autorità nazionali di protezione dei dati, linee di azione utili per svolgere in parallelo indagini in ciascuno Stato, concentrate su alcuni aspetti considerati prioritari che concernono: a) le cd. "ricerche speciali", ovvero le richieste che gli Stati membri inviano alla predetta unità centrale in relazione all'art. 18 del menzionato regolamento

(*) [doc. *web* n. 1537606]

(in tema di accesso dell'interessato) e che risultano variare da paese a paese; b) le possibilità di uso dei dati a fini diversi da quelli consentiti dal regolamento; c) la qualità –sotto il profilo tecnico– dei dati.

Sulla base di tali indicazioni, in una prima fase il Garante ha inoltrato al Ministero dell'interno una richiesta preliminare di informazioni in relazione agli aspetti sopra evidenziati.

Al fine di completare l'azione richiesta, in una seconda fase il Garante ha deliberato di procedere ai sensi dell'art. 160 del Codice, anche con visita in loco presso i competenti uffici del Ministero dell'interno, centrali e periferici, a una verifica delle informazioni ottenute e riscontrare, in particolare, la sussistenza della base giuridica necessaria per l'inserimento dei dati dattiloscopici nella banca dati centrale e per l'interrogazione del sistema, nonché l'adeguatezza delle misure di sicurezza adottate nel trattamento. Con la medesima deliberazione l'Autorità ha, inoltre, ritenuto necessario svolgere accertamenti più ampi sulla liceità e correttezza dei trattamenti comunque effettuati in attuazione della Convenzione di Dublino.

Gli uffici interessati hanno prestato la propria collaborazione fornendo anche gli elementi e la documentazione richiesti.

Concluse le verifiche, il presente provvedimento viene adottato anche con riguardo alle raccomandazioni formulate dal Garante europeo a seguito del riscontro fornito dall'Autorità al termine della prima fase di accertamenti.

OSSERVA

1. IL SISTEMA EURODAC

Il regolamento n. 2725/2000 istituisce il sistema Eurodac, che si compone dell'unità centrale, di una banca dati centrale informatizzata e dei mezzi di trasmissione dei dati tra gli Stati membri e tale banca dati centrale. Gli Stati membri, direttamente o attraverso l'unità centrale, inseriscono nella banca dati centrale i dati personali (impronte digitali e sesso) appartenenti a tre tipologie di soggetti di età non inferiore a quattordici anni: a) richiedenti asilo; b) stranieri fermati in relazione all'attraversamento irregolare di una frontiera esterna; c) stranieri presenti irregolarmente in uno Stato membro.

I dati vengono inseriti affinché siano confrontati con i dati dei richiedenti l'asilo registrati già presso l'unità centrale, al fine di concorrere alla determinazione dello Stato membro compe-

tente, ai sensi della Convenzione (oggi regolamento) di Dublino, per l'esame di una domanda di asilo presentata in uno Stato membro.

Il regolamento n. 2725/2000 prevede che le norme cui è soggetto il sistema Eurodac si applicano anche alle operazioni effettuate dagli Stati membri, dal momento della trasmissione dei dati all'unità centrale fino all'utilizzazione dei risultati del confronto; specifica inoltre che, fatta salva l'utilizzazione delle informazioni destinate all'Eurodac da parte dello Stato membro d'origine nell'ambito di banche dati istituite ai sensi della propria legislazione nazionale, i dati sulle impronte digitali e le altre informazioni personali possono esser e trattati nell'Eurodac solo per gli scopi pr evisti dall'articolo 15, paragrafo 1, della Convenzione di Dublino (art. 1 reg. n. 2725/2000).

Con riferimento al trattamento dei dati effettuato in Italia, la procedura si articola in due fasi distinte.

La prima si svolge interamente nell'ambito del Dipartimento della pubblica sicurezza del Ministero dell'interno, in particolare attraverso le questure e il Servizio di polizia scientifica, ed è rivolta alla presentazione e ricezione della domanda di asilo, alla raccolta delle informazioni necessarie (tra cui il fotosegnalamento e le verifiche sugli archivi nazionali), alla valutazione dell'ammissibilità della domanda e al suo invio alla Commissione per il riconoscimento dello status di rifugiato, alla trasmissione dei dati alla banca dati centrali Eurodac e, in caso di riscontro positivo, all'Unità Dublino.

Le direttive di carattere tecnico-operativo e di rilievo giuridico vengono impartite dalla Direzione centrale dell'immigrazione e della polizia delle frontiere del Dipartimento della pubblica sicurezza, che cura, su richiesta dell'Unità Dublino, gli approfondimenti necessari ai fini della verifica di eventuali reati a carico dello straniero, nonché ogni altra informazione circa la presenza regolare o meno dello stesso sul territorio nazionale.

La seconda fase fa capo al Dipartimento delle libertà civili e l'immigrazione del Ministero dell'interno, che espleta la procedura di accettazione/rinvio della richiesta prevista dalla Convenzione di Dublino.

In particolare, all'esito degli accertamenti svolti risulta accertata la seguente procedura.

1.1. *Invio dei dati alla banca dati centrale*

Su richiesta dell'ufficio immigrazione presso le questure il Gabinetto provinciale di polizia scientifica della Polizia di Stato effettua il fotosegnalamento dell'interessato al fine dell'inserimento in A.f.i.s. (Automated fingerprint identification system) e in Eurodac, qualora ricorra una delle fattispecie previste dal regolamento n. 2725/2000 sopra precisate alle lett. a), b) e c). Il cartellino fotosegnaletico viene quindi inviato presso il Gabinetto regionale di polizia scientifica, che provvede al controllo della sua qualità tecnica e lo inserisce effettivamente in A.f.i.s. e, se richiesto dal Gabinetto provinciale, nell'Eurodac. L'invio avviene mediante il Servizio di polizia scientifica sito presso il Dipartimento della pubblica sicurezza, designato dall'Italia quale unico punto di accesso nazionale per l'interscambio dei dati con l'unità centrale sita a Bruxelles.

1.2. *Riscontro dell'unità centrale*

In caso di confronto positivo ("risposta pertinente" secondo l'art. 4 reg. n. 2725/2000) l'unità centrale invia i rilievi dattiloscopici al competente gabinetto di polizia scientifica per la conferma della corrispondenza con i rilievi già presenti nella banca dati. A seguito di tale conferma la questura interessata invia la richiesta di asilo, corredata dalla pertinente documentazione, sia alla Commissione per il riconoscimento dello status di rifugiato territorialmente competente a decidere nel merito, sia all'Unità Dublino, ufficio del Dipartimento per le libertà civili e l'immigrazione del Ministero dell'interno che ha il compito di intrattenere i rapporti e curare lo scambio di informazioni con altri omologhi uffici nazionali al fine di individuare lo Stato membro competente a decidere sulla richiesta di asilo. L'Unità Dublino tratta anche i casi in cui la richiesta di asilo è presentata in un altro Stato membro e nel sistema risultano le impronte digitali della persona inserite dall'Italia.

2. PROFILI CRITICI E PRESCRIZIONI DEL GARANTE

Il regolamento n. 2725/2000 e il Codice pongono precisi obblighi in relazione ai trattamenti di dati personali effettuati in funzione dell'applicazione della Convenzione di Dublino.

Le informazioni acquisite, anche attraverso gli accertamenti in loco, hanno permesso di verificare che alcuni di questi obblighi non sono stati attuati correttamente.

In relazione a tali aspetti il Garante rileva per tanto la necessità di impartire ai sensi degli

artt. 154 e 160 del Codice le necessarie modificazioni e integrazioni da apportare al trattamento, di cui, in relazione agli obblighi di controllo ad essa affidati, questa Autorità si riserva di verificare periodicamente l'attuazione ai sensi del medesimo art. 160.

2.1. *Titolare ed eventuali responsabili del trattamento*

Profili critici

La complessità della procedura descritta, con l'intervento di molteplici organi facenti capo a diverse articolazioni del Ministero dell'interno, non consente una chiara individuazione delle diverse responsabilità nel trattamento dei dati per le finalità proprie del sistema Eurodac.

L'imputabilità a più soggetti delle operazioni da svolgere, con la conseguente, mancata individuazione di un unico interlocutore, ha determinato anche ritardi e difficoltà nello stesso svolgimento degli accertamenti deliberati dal Garante.

Prescrizioni

L'art. 13 del regolamento n. 2725/2000 pone precisi obblighi a carico di ciascuno Stato membro, il quale è tenuto a garantire "la legalità del rilevamento delle impronte digitali" e della loro trasmissione all'unità centrale, l'esattezza e l'attualità delle informazioni al momento della trasmissione, "la legalità della registrazione, conservazione, rettifica e cancellazione dei dati nella banca dati centrale", "la legalità dell'uso dei risultati del confronto dei dati sulle impronte trasmessi dall'unità centrale" (paragrafo 1), nonché la sicurezza dei dati in ogni fase del trattamento (paragrafo 2).

Tali obblighi impongono la necessità di identificare chiaramente le responsabilità dei diversi servizi che utilizzano il sistema Eurodac nell'ambito del Ministero dell'interno, ivi compreso il servizio competente per l'accertamento dell'età del soggetto ai fini dell'inserimento delle impronte digitali nel sistema. In particolare, devono essere individuati il titolare (o i co-titolari) del trattamento dei dati, nonché eventuali responsabili; i relativi estremi identificativi devono essere comunicati al Garante, al fine di consentire a questa Autorità di svolgere efficacemente il ruolo di controllo attribuitole (art. 19 reg. cit.).

A questo fine, va posta particolare attenzione al fatto che la descritta attività è "servente" rispetto alla procedura di asilo; pertanto, è richiesto il rigoroso rispetto del principio di finalità del trattamento per tutte le operazioni compiute, dalla raccolta all'utilizzo, alla conservazione e alla comunicazione dei dati.

2.2. *Soggetti che hanno accesso ai dati registrati nell'Eurodac*

Profili critici

L'articolo 15, paragrafo 2, del regolamento Eurodac prevede che ciascuno Stato membro designi "le autorità" che possono accedere ai dati dallo stesso trasmessi e registrati nella banca dati centrale, e comunichi l'elenco di tali autorità alla Commissione europea. Solo tali autorità possono modificare, rettificare, integrare o cancellare i dati da esse inseriti (paragrafo 3).

L'Italia risulta avere designato il Servizio di polizia scientifica che, per sua stessa precisazione, fornisce solo il supporto tecnico alle attività di competenza degli uffici titolari della gestione delle pratiche di asilo e di quelle relative agli accertamenti Eurodac e non è, pertanto, in grado di assumere le responsabilità per le operazioni di trattamento indicate nell'art. 15, nonché per le attività, precisate al punto 2.1, che l'art. 13 del regolamento prevede a carico degli Stati membri e delle autorità da questi designate.

Prescrizioni

Ferme restando le attribuzioni di carattere tecnico del Servizio di polizia scientifica, devono essere individuati dal titolare (o dai co-titolari) del trattamento i soggetti ("le autorità") che assicurino il giusto livello di responsabilità richiesto dagli artt. 13 e 15 del regolamento nelle decisioni di modifica, rettifica, integrazione e cancellazione dei dati inseriti nell'Eurodac.

Sempre al fine dell'espletamento delle necessarie attività di controllo, gli estremi identificativi dei soggetti investiti di tale responsabilità devono essere anch'essi comunicati al Garante, come pure i soggetti che hanno accesso ai risultati delle ricerche in Eurodac, in particolare a quelle relative ai confronti con le categorie b) e c) indicate al punto 1. del presente provvedimento.

2.3. *Finalità dell'accesso al sistema Eurodac*

Profili critici

I rilievi esposti ai punti che precedono evidenziano la mancanza di una chiara definizione dei livelli di responsabilità delle diverse autorità che partecipano al sistema e di una procedura definita e formalizzata che consenta di monitorare il grado di corretta applicazione delle regole che disciplinano il trattamento dei dati da parte dei diversi uffici abilitati, sul territorio nazionale, ad assumere decisioni rilevanti riguardo ai diritti delle persone e a inserire, correggere, richiamare, utilizzare i dati personali conservati nella base di dati gestita dall'unità centrale.

In particolare, per quanto riguarda l'Italia, la Commissione europea e il Garante europeo hanno segnalato l'alto numero di accessi nella base dati centrale giustificati ai sensi dellart. 18 del regolamento (le cd. "ricerche speciali"), il quale prevede che in ciascuno Stato membro l'interessato può esercitare i diritti di accesso, comunicazione, rettifica e cancellazione dei dati personali che lo riguardano. Nel corso degli accertamenti è risultato che in nessuno dei casi segnalati l'accesso ai dati era stato effettuato su richiesta dell'interessato; né, sono state presentate a questa Autorità istanze di interessati volte a esercitare i diritti conferiti dall'art. 18. In risposta alla richiesta dell'Autorità di verificare la legittimità degli accessi, il Servizio di polizia scientifica presso il Dipartimento della pubblica sicurezza è intervenuto assicurando di avere disattivato per gli uffici periferici tale possibilità di accesso ai dati, che attualmente potrebbe essere effettuato solo presso il Servizio stesso. Nonostante tale assicurazione, e benché il numero di tali casi sia diminuito fortemente, la Commissione europea, nei suoi report trimestrali, ha continuato a segnalare richieste di accesso ai sensi dell'art. 18 non basate su istanze degli interessati.

Prescrizioni

Il titolare e gli eventuali responsabili del trattamento, che vanno individuati ai sensi della prescrizione di cui al punto 2.1, devono adottare un'idonea regolamentazione volta a garantire che l'accesso ai dati gestiti dall'unità centrale sia limitato alle sole finalità previste dal regolamento Eurodac. In particolare, va garantita la conoscibilità di ogni accesso per le *cd.* "ricerche speciali" previste dall'art. 18 del regolamento; deve essere altresì assicurato che solo le autorità competenti per la procedura di asilo possano accedere ai risultati del confronto tra i dati dei soggetti appartenenti alle categorie c) e b) e quelli dei soggetti appartenenti alla categoria a) di cui al punto 1 del presente provvedimento.

2.4. *Formazione del personale e diritti degli interessati*

Profili critici

Con circolare del gennaio 2003 il Dipartimento della pubblica sicurezza ha informato gli uffici di polizia sul territorio dell'imminente entrata in vigore del regolamento Eurodac e ha impartito le relative istruzioni. La circolare fa riferimento alla necessità di garantire i diritti delle persone e reca in allegato un modulo per l'informativa da rendere agli interessati, redatto in più lingue, che viene consegnato alla persona e da questa sottoscritto allatto del fotosegna-

lamento. Nel corso dell'accertamento del Garante le suddette istruzioni sono state reiterate. Dalle informazioni acquisite non risulta peraltro che finora alcun interessato –direttamente o attraverso il proprio legale o organizzazioni umanitarie– abbia esercitato i diritti conferiti dall'art. 18.

Mancano inoltre informazioni certe sull'effettivo utilizzo del modulo da parte di tutte le questure.

Prescrizioni

Il titolare e gli eventuali responsabili del trattamento devono garantire un'adeguata formazione del personale, in particolare in merito all'uso legittimo delle cd. "ricerche speciali", e assicurare che l'intera procedura, dall'identificazione della persona alla decisione sulla richiesta di asilo avvenga nel rispetto della dignità dell'interessato.

In coerenza con quanto previsto dal regolamento Eurodac, il titolare e gli eventuali responsabili del trattamento devono assicurare il puntuale rispetto di quanto previsto nell'articolo 18, fornendo le informazioni previste e precisando le relative procedure al fine di mettere l'interessato nella condizione di esercitare i diritti riconosciutigli. Al riguardo, l'informativa non risulta del tutto adeguata rispetto a quanto prescritto dall'art. 18, con particolare riferimento all'indicazione del titolare (o co-titolari) del trattamento dai dati (linformativa attualmente fornita indica come responsabile del trattamento dei dati il Gabinetto di polizia scientifica che procede all'operazione di fotosegnalamento), degli specifici diritti che possono essere esercitati dagli interessati e delle autorità (Garante e autorità giudiziaria) a cui presentare un eventuale ricorso.

Si rende quindi necessario aggiornare il testo dell'informativa attualmente fornita con l'inserimento di tali ulteriori informazioni.

2.5. *Misure di sicurezza*

In relazione agli elementi acquisiti, la particolare natura dei dati induce a evidenziare la necessità che, fermo restando le cautele attualmente previste dagli artt. 31 e ss. e dall'Allegato B. al Codice, vengano adottate, da parte degli organi interessati dalla procedura, ulteriori misure e accorgimenti, di seguito indicati, volti a rafforzare il livello di protezione delle informazioni oggetto di trattamento, anche in attuazione dell'obbligo di garantire la sicurezza dei dati prima, durante e dopo la trasmissione all'unità centrale, nonché dei dati ricevuti dall'unità centrale che l'art. 13, paragrafo 2, del regolamento n. 2725/2000 pone a carico di ogni Stato membro.

2.5.1. *Credenziali di autenticazione presso il Servizio di polizia scientifica*

Profili critici

Presso il Servizio di polizia scientifica del Dipartimento della pubblica sicurezza vengono conservati i log file relativi al tracciamento delle operazioni effettuate sulle impronte digitali destinate a confluire in Eurodac (e in A.f.i.s) dai gabinetti provinciali e regionali della polizia scientifica. Nei log vengono memorizzate le attività svolte, il nome dell'utente, il codice della postazione client di provenienza della richiesta, il numero originario identificativo dell'operazione effettuata dal client e il codice A.f.i.s..

L'accesso alla sala macchine che ospita il server centrale è consentito mediante badge profilato.

L'accesso degli amministratori al database dei log Eurodac (e A.f.i.s.) avviene mediante credenziali di autenticazione (username e password) condivise tra il personale dell'area Gruppo sistemistico sezione A.f.i.s..

Prescrizioni

Per l'accesso al database Eurodac (e A.f.i.s.), a ogni incaricato deve essere assegnata o associata individualmente almeno una credenziale di autenticazione costituita da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi.

2.5.2. *Conservazione dei fascicoli cartacei presso l'Unità Dublino*

Profili critici

Presso l'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione vengono conservati, in numero di oltre 90.000, i fascicoli cartacei relativi ai soggetti i cui dati personali vengono trattati dall'Unità in relazione ai compiti da questa svolti nell'ambito della procedura che disciplina Eurodac. Si tratta di dati anche biometrici (le impronte digitali contenute nei cartellini dattiloscopici) e di carattere giudiziario, tra i quali le informazioni relative agli interessati acquisite dal Centro elaborazioni dati del Dipartimento della pubblica sicurezza.

Allo stato, i fascicoli sono sistemati in armadi privi di chiusura collocati in stanze non chiuse a chiave. Sono in corso attività volte a dotare di serrature gli armadi e le stanze.

É installato un impianto di rilevazione incendi e un sistema di videosorveglianza, che entra in funzione al di fuori dell'orario di lavoro del personale.

Prescrizioni

I dati personali contenuti nei fascicoli cartacei devono essere custoditi e controllati con modalità che riducano al minimo i rischi di distruzione o perdita o di accesso non autorizzato.

L'accesso ai locali ove sono custoditi i fascicoli va consentito previa adozione di un sistema di controllo basato sull'utilizzo di una tessera individuale (ad esempio, un badge profilato) a disposizione dei soli soggetti incaricati del trattamento delle informazioni.

I fascicoli devono essere collocati in armadi ignifughi dotati di idonee serrature di sicurezza.

I varchi di accesso ai locali devono essere anch'essi dotati di idonee serrature di sicurezza.

2.5.3 *Trattamento dei dati con strumenti elettronici presso l'Unità Dublino*

Profili critici

Lo scambio di informazioni e documentazione con uffici esterni all'Unità (omologhi uffici di Stati membri e questure) avviene mediante posta elettronica certificata e non, posta tradizionale e fax, con esclusione, quanto al fax, della trasmissione dei cartellini dattiloscopici, causa la cattiva risoluzione dell'immagine.

L'accesso alle postazioni informatiche da parte del personale avviene mediante credenziali di autenticazione personale di dominio Windows.

L'accesso all'applicazione web DubliNET, attraverso cui l'Unità gestisce i dati e le comunicazioni con gli Stati membri, avviene attraverso un sito non Ssl (Secure Socket Layer) e, quindi, senza certificato di sicurezza.

Le credenziali di autenticazione (username e password) per l'accesso all'applicazione DubliNET sono condivise fra i vari operatori.

La documentazione scaricabile dal sistema DubliNET (ad esempio, in formato Pdf), ivi compresi i cartellini dattiloscopici, viene firmata digitalmente dal mittente, ma le postazioni informatiche in uso al personale dell'Unità non sono dotate del sistema di verifica della firma digitale (all'interno del file nell'area dedicata alla firma digitale risulta presente un punto interrogativo).

Gli accessi all'applicazione DubliNET e le operazioni compiute sui dati vengono tracciate.

Prescrizioni

Lo scambio di informazioni e documentazione da e verso l'Unità Dublino deve avvenire con modalità che assicurino la provenienza della comunicazione e l'integrità del suo contenuto.

Le comunicazioni devono quindi avvenire esclusivamente attraverso posta elettronica certificata e i documenti trasmessi devono essere cifrati.

Per l'accesso all'applicazione web DubliNET, a ogni incaricato deve essere assegnata o associata individualmente almeno una credenziale di autenticazione costituita da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi.

3. TERMINE PER ATTUARE LE PRESCRIZIONI DEL GARANTE

Attesa la particolare delicatezza dei dati in questione, il Garante constata la necessità che le prescritte modificazioni e integrazioni da apportare al trattamento siano adottate entro termini brevi, decorrenti dalla data di ricezione del presente provvedimento, che risulta congruo fissare:

a) in trenta giorni, relativamente alle misure di sicurezza concernenti l'adozione delle credenziali individuali di autenticazione da parte del personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e degli operatori dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione;

b) in sei mesi, relativamente alle altre modificazioni e integrazioni, ivi comprese le ulteriori misure di sicurezza prescritte (punto 2.5).

Il Ministero, che allo stato risulta titolare del trattamento, è invitato a fornire riscontro al decorso di ciascuno di tali termini circa l'attuazione delle presenti prescrizioni.

TUTTO CIÒ PREMESSO IL GARANTE

1) ai sensi degli artt. 154, comma 1, lett. c) e 160 del Codice dispone che il Ministero dell'interno adotti le prescritte modificazioni e integrazioni al trattamento dei dati personali effettuati in attuazione del regolamento n. 2725/2000 istitutivo del sistema Eurodac e della Convenzione di Dublino relativamente a:

   a) individuazione e comunicazione al Garante degli estremi identificativi del titolare (o co-titolari) e eventuali responsabili del trattamento, con indicazione dei compiti e delle responsabilità dei vari soggetti che effettuano il trattamento dei dati nellambito della procedura, al fine di assicurare la liceità del trattamento, la correttezza e sicurezza dei dati e il rigoroso rispetto del principio di finalità del trattamento per tutte

le operazioni compiute, dalla raccolta all'utilizzo, alla conservazione e alla comunicazione dei dati (punto 2.1);

b) individuazione e comunicazione al Garante degli estremi identificativi dei soggetti ("le autorità") che assicurino il livello di responsabilità richiesto dagli artt. 13 e 15 del regolamento n. 2725/2000 nelle decisioni di modifica, rettifica, integrazione e cancellazione dei dati registrati presso la banca dati centrale e che possono accedere ai risultati delle ricerche nel sistema, in particolare a quelle relative ai confronti con le categorie b) e c) indicate al punto 1 del presente provvedimento (punto 2.2);

c) adozione di una idonea regolamentazione volta a garantire che l'accesso ai dati gestiti dall'unità centrale sia limitato alle sole finalità previste dal regolamento n. 2725/2000 e alle sole autorità competenti per la procedura di asilo, con particolare riferimento alle cd. "ricerche speciali" di cui all'art. 18 del regolamento (punto 2.3);

d) formazione del personale in relazione al trattamento dei dati effettuato nel corso della procedura, con particolare riferimento all'uso legittimo delle cd. "ricerche speciali"; aggiornamento del testo dell'informativa da rendere all'interessato con particolare riferimento all'inserimento dell'indicazione del titolare (o co-titolari) del trattamento dei dati e degli specifici diritti che possono essere esercitati dagli interessati e delle autorità (Garante e autorità giudiziaria) a cui presentare un eventuale ricorso (punto 2.4);

2) ai sensi degli artt. 154, comma 1, lett. c) e 160 del Codice dispone che il Ministero dell'interno adotti adeguate misure di sicurezza nel trattamento dei dati, volte a rafforzare il livello di protezione delle informazioni trattate nell'ambito del sistema Eurodac, con particolare riferimento a (punto 2.5):

a) assegnazione al personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e del personale dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione di credenziali individuali di autenticazione costituite da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi;

b) conservazione dei fascicoli cartacei presso l'Unità Dublino del Dipartimento per le

libertà civili e l'immigrazione in armadi ignifughi dotati di serrature di sicurezza collocati in locali con accesso consentito previa adozione di un sistema di controllo basato sull'utilizzo di una tessera individuale (ad esempio, un badge profilato) a disposizione dei soli soggetti incaricati del trattamento delle informazioni e con varchi dotati di idonee serrature di sicurezza;

c) trattamento dei dati con strumenti elettronici presso la medesima Unità mediante comunicazioni basate sull'uso esclusivo di posta elettronica certificata e sulla trasmissione di documenti cifrati;

3) ai sensi delle medesime disposizioni prescrive che le suesposte modificazioni e integrazioni da apportare al trattamento siano adottate entro il termine, decorrente dalla data di ricezione del presente provvedimento, di trenta giorni relativamente alle misure di sicurezza concernenti l'adozione delle credenziali individuali di autenticazione da parte del personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e del personale dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione, e di sei mesi relativamente alle altre modificazioni e integrazioni, ivi comprese le ulteriori misure di sicurezza prescritte, fornendo riscontro a questa Autorità circa la loro attuazione al decorso dei medesimi termini.

Roma, 29 maggio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

27. Recepimento normativo in tema di dati di traffico telefonico e telematico (*)

ALLEGATO A

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, 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, di seguito, "Codice");

Visti in particolare gli artt. 17, 123 e 132, comma 5, del Codice;

Vista la deliberazione del 19 settembre 2007 con la quale l'Autorità ha avviato una procedura di consultazione pubblica su un documento, adottato in pari data, riguardante "Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione di reati" e pubblicato, unitamente alla medesima deliberazione, sul sito web dell'Autorità;

Visti i commenti e le osservazioni pervenuti a questa Autorità a seguito della consultazione pubblica per la quale era stato fissato il termine del 31 ottobre 2007;

Considerate le risultanze dei diversi incontri, anche di carattere tecnico, intercorsi con alcune associazioni di categoria che lo avevano richiesto;

Vista la documentazione in atti;

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

Relatore il prof. Francesco Pizzetti;

PREMESSO

1. CONSIDERAZIONI PRELIMINARI

Il trattamento dei dati di traffico telefonico e telematico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

(*) Gazzetta Ufficiale 13 agosto 2008, n. 189 [doc. *web* n. 1538237], in inglese [doc. *web* n. 1542849]

Tali informazioni hanno una natura particolarmente delicata e la loro impropria utilizzazione può avere importanti ripercussioni sulla sfera personale di più soggetti interessati; possono avere un'"accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore" e la loro conoscibilità richiede adeguate garanzie (cfr., fra l'altro, Corte cost. 11 marzo 1993, n. 81 e 14 novembre 2006 n. 372).

I dati relativi al traffico telefonico e telematico dovrebbero peraltro riguardare solo alcune caratteristiche esteriori di conversazioni, chiamate e comunicazioni, senza permettere di desumerne i contenuti.

Inoltre, le stesse caratteristiche esteriori permettono di individuare analiticamente quando, tra chi e come sono intercorsi contatti telefonici o per via telematica, o sono avvenute determinate attività di accesso all'informazione in rete e persino il luogo dove si trovano i detentori di determinati strumenti.

L'intensità dei flussi di comunicazione comporta la formazione e, a volte, la conservazione di innumerevoli informazioni che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali e istituzionali, e di formare anche delicati profili interpersonali. Ciò, specie quando i dati sono conservati massivamente dai fornitori per un periodo più lungo di quello necessario per prestare servizi a utenti e abbonati, al fine di adempiere a un distinto obbligo di legge collegato a eccezionali necessità di giustizia.

Per le comunicazioni telematiche, poi, si pongono ulteriori e più specifiche criticità rispetto alle comunicazioni telefoniche tradizionalmente intese, in quanto il dato apparentemente "esterno" a una comunicazione (ad es., una pagina web visitata o un indirizzo Ip di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: può permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati.

Eventuali abusi (quali quelli emersi nel recente passato, allorché sono stati constatati gravi e diffusi fatti di utilizzazione illecita di dati), possono comportare importanti ripercussioni sulla sfera privata degli individui o anche violare specifici segreti attinenti a determinate attività, relazioni e professioni.

Emerge quindi la necessità, in attuazione di quanto previsto per legge, di assicurare che la con-

servazione di tali dati da parte dei fornitori, laddove essa sia necessaria per prestare un servizio o in quanto imposta dalla legge, avvenga comunque in termini adeguati per garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone.

Per tali motivi, a prescindere dalle garanzie previste in termini più generali nell'ordinamento anche sul piano costituzionale e processuale, il legislatore all'art. 132 del Codice ha demandato al Garante per la protezione dei dati personali l'individuazione delle misure e degli accorgimenti che i fornitori dei servizi di comunicazione elettronica devono adottare a fronte della conservazione dei dati di traffico telefonico e telematico, allo stato prescritta per finalità di accertamento e repressione dei reati.

Il presente provvedimento è rivolto appunto a individuare le elevate cautele che devono essere osservate dai fornitori nella formazione e nella custodia dei dati del traffico telefonico e telematico

Prima di indicare quali cautele risultano necessarie a seguito del complesso procedimento di accertamento curato dal Garante, sono opportune alcune altre premesse sull'attuale quadro normativo, sui fornitori e sui dati personali coinvolti.

2. QUADRO DI RIFERIMENTO

2.1. *Normativa comunitaria*

La direttiva europea n. 2002/58/Ce, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, impone agli Stati membri di proteggere la riservatezza delle comunicazioni elettroniche e vieta la conservazione dei dati relativi al traffico generati nel corso delle comunicazioni, a eccezione della conservazione espressamente autorizzata per i fini indicati nella direttiva medesima.

La direttiva riguarda (art. 3) il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione. I dati relativi al traffico sono definiti, in questa sede, quali quelli sottoposti a trattamento "ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione" (cfr. art. 2 e considerando n. 15 della direttiva 2002/58/Ce).

La medesima direttiva, nell'imporre agli Stati membri l'adozione di disposizioni di legge nazionali che assicurino la riservatezza delle comunicazioni effettuate tramite la rete pubblica di

comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, pone l'accento sui dati di traffico generati dai ser vizi medesimi (art. 5); tali dati, trattati e memorizzati dal fornitore della rete pubblica o del servizio pubblico di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunica - zione, fatte salve alcune tassative eccezioni (cfr. art. 6, par. 2 , 3 e 5 e ar t. 15, par. 1; v., fra gli altri, il Parere n. 1/2003 sulla memorizzazione ai fini di fatturazione dei dati r elativi al traffico, adottato il 29 gennaio 2003 dal G ruppo dei garanti europei per la tutela dei dati personali).

L'art. 15, par. 1, della direttiva consente che gli Stati membri possano adottare disposizioni legislative volte a limitar e i diritti e gli obblighi di cui ai pr edetti ar ticoli 5 e 6 solo quando tale restrizione costituisca " una misura necessaria, oppor tuna e pr oporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioé della sicurezza dello Stato), della difesa, della sicurezza pubblica e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettr onica". A tal fine, gli Stati membri possono, tra l 'altro, adottar e misur e legislative le quali pr evedano che, per tali motivi, i dati siano conser vati per un periodo di tempo limitato.

2.2. *Normativa nazionale*

La direttiva 2002/58/Ce è stata r ecepita con il Codice in materia di pr otezione dei dati personali (Titolo X ("Comunicazioni elettr oniche"); cfr. art. 184). Nel Capo I di tale Titolo, intitolato "Servizi di comunicazione elettronica", è stata introdotta una nuova disciplina sulla conservazione dei dati di traffico telefonico.

Da un lato, l'art. 123 del Codice ha ridotto a sei mesi il previgente limite temporale per la conservazione dei dati di traffico telefonico per finalità di fatturazione, pagamenti in caso di interconnessione e di commer cializzazione di ser vizi, termine che era in pr ecedenza individuabile nella misura massima di cinque anni in base a quanto pr evisto dal d.lg. n. 171/1998.

Dall'altro, l'art. 132 del medesimo Codice, modificato prima della sua entrata in vigore (d.l. 24 dicembre 2003, n. 354, conv ertito in l., con modificazioni, dall 'art. 1 l. 26 febbraio 2004, n. 45) ha introdotto un distinto obbligo per i fornitori di ser vizi di comunicazione elettr onica di conservare per finalità di accer tamento e repressione dei reati dati di traffico telefonico r elativi ai servizi offerti.

Tutto ciò, sullo sfondo del principio cardine in materia secondo cui i dati non devono essere formati se non sono necessari e proporzionati ai fini della funzionalità della rete o della prestazione del servizio (artt. 3 e 11 del Codice).

Dal contesto sopra riassunto emerge che è stata nel complesso vietata una conservazione generalizzata dei dati relativi al traffico (art. 123, comma 1, cit.), con le seguenti eccezioni:

- è stato consentito il trattamento di dati strettamente necessario a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione (nei limiti e con le modalità di cui all'art. 123, comma 2) o, previo consenso dell'abbonato o dell'utente, a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto (art. 123, comma 3);
- è stata però prescritta in termini distinti la conservazione temporanea dei dati di traffico telefonico per esclusive finalità di accertamento e repressione dei reati per due periodi di ventiquattro mesi ciascuno (art. 132 del Codice).

Un successivo provvedimento d'urgenza del 2005 (d.l. 27 luglio 2005, n. 144, convertito in l., con modificazioni, dall'art. 1 della l. 31 luglio 2005, n. 155) ha poi introdotto, tra l'altro:

a) l'obbligo di conservare i dati di traffico telematico, escludendone i contenuti, per due periodi di sei mesi ciascuno;

b) l'obbligo di conservare dati relativi alle chiamate telefoniche senza risposta;

c) con riferimento ai primi ventiquattro mesi di conservazione dei dati del traffico telefonico e ai primi sei mesi di conservazione dei dati del traffico telematico, la previsione che la richiesta giudiziaria volta ad acquisirli, rivolta al fornitore, venga effettuata dal "pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private e non già dal giudice su istanza del pubblico ministero";

d) un regime transitorio in virtù del quale è stata sospesa temporaneamente l'applicazione di qualunque disposizione che prescriva o consenta la cancellazione dei dati di traffico, anche se non soggetti a fatturazione (termine originariamente stabilito al 31 dicembre 2007, ma successivamente prorogato al 31 dicembre 2008 con l'art. 34 del recente d.l. 31 dicembre 2007, n. 248, in fase di conversione in legge);

e) per i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie, che si limi-

tino a porre a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale, alcuni specifici obblighi di identificazione e monitoraggio delle operazioni compiute dai clienti (cfr. anche il d.m. 16 agosto 2005, in G.U. 17 agosto 2005, n. 190, attuativo di tale previsione).

Il decreto legge del 2005 ha quindi, da un lato, emendato l'art. 132 del Codice (punti a), b) e c) sopra indicati) e, dall'altro, ha introdotto un regime transitorio per la conservazione dei dati, nonché la predetta disciplina speciale applicabile solo a determinati soggetti.

Fermo restando il predetto regime, che prevedeva temporaneamente la conservazione (lett. d) sopra citata), la normativa di riferimento prescriveva ai fornitori di servizi di comunicazione elettronica di conservare comunque, per finalità di accertamento e repressione di reati, i dati relativi al traffico telefonico (inclusi quelli concernenti le chiamate senza risposta) e quelli inerenti al traffico telematico (esclusi i contenuti delle comunicazioni), rispettivamente per ventiquattro e sei mesi (art. 132, comma 1, del Codice).

La stessa normativa prescriveva inoltre, ai medesimi fornitori, di conservare tali dati per un periodo ulteriore, rispettivamente di ventiquattro e sei mesi, per l'accertamento e la repressione dei delitti tassativamente individuati dall'art. 407, comma 2, lett. a), c.p.p., nonché dei delitti in danno di sistemi informatici o telematici (art. 132, comma 2).

Infine, introduceva la prescrizione, tutt'ora vigente, che la conservazione dei predetti dati fosse effettuata nel rispetto di specifici accorgimenti e misure a garanzia degli interessati. L'individuazione di tali cautele, oggetto del presente provvedimento, è stata appunto demandata al Garante per la protezione dei dati personali (cfr. artt. 17 e 132, comma 5, del Codice).

2.3. *Altra disciplina comunitaria: la direttiva 2006/24/Ce*

Al fine di armonizzare le disposizioni degli Stati membri sul tema della conservazione dei dati di traffico per finalità di accertamento e repressione di reati è poi intervenuta la direttiva n. 2006/24/Ce del Parlamento europeo e del Consiglio del 15 marzo 2006, che doveva essere recepita entro il 15 settembre 2007.

Tale direttiva contiene specifiche indicazioni sul risultato convenuto a livello comunitario con riferimento sia ai tempi di conservazione dei dati di traffico (minimo sei mesi e massimo due

anni), sia alla corretta e uniforme individuazione delle "categorie di dati da conservare" (analiticamente elencate nell'art. 5 della direttiva medesima); ciò, in relazione agli specifici servizi ivi enucleati, ovvero di telefonia di rete fissa e di telefonia mobile, di accesso a Internet, di posta elettronica in Internet e di telefonia via Internet.

In questo quadro risulta necessario tener conto di tali indicazioni anche nell'ambito del presente provvedimento. Ciò, anche in considerazione del fatto che nell'attuale quadro normativo interno, pur sussistendo una definizione generale di "dati relativi al traffico" (art. 4, comma 2, lett. h) del Codice), tali dati non vengono enumerati, né vengono distinti espressamente i dati relativi al traffico "telefonico" da quelli inerenti al traffico "telematico".

Tale distinzione risulta, invece, necessaria in considerazione del fatto che il legislatore italiano, diversamente da quello comunitario, ha individuato due diversi periodi di conservazione in relazione alla natura "telefonica" o "telematica" del dato da conservare.

Ciò comporta l'esigenza di specificare l'ambito soggettivo di applicazione del presente provvedimento rispetto all'obbligo di conservazione dei dati.

La direttiva è stata recepita con il d.lg. 30 maggio 2008, n. 109, che ha previsto un periodo unico di conservazione pari a 24 mesi per i dati di traffico telefonico, a 12 mesi per i dati di traffico telematico e a 30 giorni per i dati relativi alle chiamate senza risposta, senza ulteriori distinzioni in base al tipo di reato.

La legge 18 marzo 2008, n. 48, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica fatta a Budapest il 23 novembre 2001 ha poi previsto una specifica ipotesi di conservazione temporanea dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati.

3. I FORNITORI TENUTI A CONSERVARE I DATI DI TRAFFICO

Il "fornitore" sul quale incombe l'obbligo di conservare i dati di traffico ai sensi del citato art. 132 del Codice è quello che mette a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione; per "servizi di comunicazione elettronica" devono intendersi quelli consistenti, esclusivamente o prevalentemente, "nella trasmissione di segnali su reti di comunicazioni elettroniche" (art. 4, comma 2, lett. d) e e), del Codice).

Ciò, deriva:

a) dalla collocazione del menzionato art. 132 all'interno del Titolo X, Capo I, del Codice e da quanto disposto dall'art. 121 del medesimo Codice il quale, nell'individuare i "Servizi interessati", chiarisce che le disposizioni del Titolo X "si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni";

b) da quanto stabilisce il citato decreto legge 27 luglio 2005, n. 144 nella parte in cui, nell'imporre la conservazione dei dati per il predetto regime transitorio, si riferisce ai "fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico".

Devono ritenersi quindi tenuti alla conservazione dei dati ai sensi del medesimo art. 132 i soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione (cfr. anche direttiva 2002/21/Ce del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (cd. direttiva quadro) e d.lg. n. 259/2003 recante il Codice delle comunicazioni elettroniche).

Al contrario non rientrano, ad esempio, nell'ambito applicativo del presente provvedimento:

- i soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche). Tali servizi, pur rientrando nelle definizione generale di "servizi di comunicazione elettronica", non possono essere infatti considerati come "accessibili al pubblico". Qualora la comunicazione sia instradata verso un utente che si trovi al di fuori della cd. "rete privata", i dati di traffico generati da tale comunicazione sono invece oggetto di conservazione (ad es., da parte del fornitore di cui si avvale il destinatario della comunicazione, qualora si tratti di un messaggio di posta elettronica; cfr. documento di lavoro "Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati online", adottato dal Gruppo di lavoro per la tutela dei dati personali il 21 novembre 2000);

- i soggetti che, pur offrendo servizi di comunicazione elettronica accessibili al pubblico, non generano o trattano direttamente i relativi dati di traffico;
- i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale;
- i gestori dei siti Internet che diffondono contenuti sulla rete (cd. "content provider"). Essi non sono, infatti, fornitori di un "servizio di comunicazione elettronica" come definito dall'art. 4, comma 2, lett. e) del Codice. Tale norma, infatti, nel rinviare, per i casi di esclusione, all'art. 2, lett. c) della direttiva 2002/21/Ce cit., esclude essa stessa i "servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica […]". Deve rilevarsi, inoltre, che i dati di traffico relativi alla comunicazione (come, ad esempio, la cd. "navigazione web" e le pagine visitate di un sito Internet) spesso identificano o rivelano nella sostanza anche il suo contenuto e pertanto l'eventuale conservazione di tali dati si porrebbe, in violazione di quanto disposto dall'art. 132 del Codice (come modificato dal citato d.l. n. 144/2005), laddove esclude dalla conservazione per finalità di giustizia i "contenuti" della comunicazione (cfr., in tal senso, anche l'art. 1, comma 2, della direttiva 2006/24/Ce, nella parte in cui esclude dal proprio ambito di applicazione la conservazione del "contenuto delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazioni elettroniche");
- i gestori di motori di ricerca. I dati di traffico telematico che essi trattano, consentendo di tracciare agevolmente le operazioni compiute dall'utente in rete, sono, comunque, parimenti qualificabili alla stregua di "contenuti".

4. I DATI DI TRAFFICO CHE DEVONO ESSERE CONSERVATI

L'obbligo di conservazione riguarda i dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, nonché i dati inerenti al traffico telematico, esclusi comunque i contenuti delle comunicazioni (art. 132 del Codice). In particolare, sono oggetto di conservazione

i dati che i fornitori sottopongono a trattamento per la trasmissione della comunicazione o per la relativa fatturazione (art. 4, comma 2, lett. h), del Codice).

Pertanto, i fornitori (come individuati nel precedente paragrafo 3) devono conservare, per esclusive finalità di accertamento e repressione di reati, solo i dati di traffico che risultino nella loro disponibilità in quanto derivanti da attività tecniche strumentali alla resa dei servizi offerti dai medesimi, nonché alla loro fatturazione. Ciò, in ossequio anche ai princìpi di pertinenza e non eccedenza stabiliti dagli artt. 3 e 11 del Codice.

In tal senso, si esprime anche il citato decreto legge 27 luglio 2005, n. 144 che, all'art. 6, riconduce l'obbligo di conservazione alle "informazioni che consentono la tracciabilità degli accessi, nonché, qualora disponibili, dei servizi". La direttiva 2006/24/Ce ribadisce che tale obbligo sussiste soltanto se i dati sono stati "generati o trattati nel processo di fornitura dei [...] servizi di comunicazione" del fornitore (cfr. considerando 23 e art. 3, par. 1, della direttiva 2006/24/Ce cit.).

L'art. 5 di tale direttiva contiene, poi, un'elencazione specifica delle informazioni da conservare e individua diverse categorie di dati di traffico, specificandone i contenuti a seconda che si tratti di traffico telefonico o telematico.

Nell'ambito dei servizi di comunicazione elettronica, occorre infatti distinguere i servizi "telefonici" da quelli "telematici".

Nei primi sono ricompresi:

- le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite telefax;
- servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata;
- la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-sms.

Nei secondi sono ricompresi:

- l'accesso alla rete Internet;
- la posta elettronica;
- i fax (nonché i messaggi sms e mms) via Internet;
- la telefonia via Internet (cd. Voice over Internet Protocol - VoIP).

Per quanto concerne specificamente la conservazione dei dati di traffico telefonico relativo alle "chiamate senza risposta", fermo restando allo stato quanto indicato dalla direttiva 2006/24/Ce

al considerando 12 (laddove esclude dal proprio ambito di applicazione i "tentativi di chiamata non riusciti"), il fornitore, in forza delle modifiche apportate dal d.l. n. 144/2005 all'art. 132 del Codice, deve conservare solo i dati generati da chiamate telefoniche che sono state collegate con successo, ma non hanno ottenuto risposta oppure in cui vi è stato un intervento del gestore della rete (cfr. art. 2, comma 2, lett. f), direttiva 2006/24/Ce).

5. FINALITÀ PERSEGUIBILI

Il vincolo secondo cui i dati conservati obbligatoriamente per legge possono essere utilizzati solo per finalità di accertamento e repressione di reati comporta una precisa limitazione per i fornitori nell'eventualità in cui essi ricevano richieste volte a perseguire scopi diversi.

Ad esempio:

a) i medesimi fornitori non possono corrispondere a eventuali richieste riguardanti tali dati formulate nell'ambito di una controversia civile, amministrativa e contabile;

b) sono tenuti a rispettare il menzionato vincolo di finalità anche l'interessato che acceda ai dati che lo riguardano esercitando il diritto di accesso di cui all'art. 7 del Codice (e che può utilizzare quindi i dati acquisiti solo in riferimento alle predette finalità penali), nonché, nel procedimento penale, il difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private (art. 132, comma 3, del Codice).

6. MODALITÀ DI ACQUISIZIONE DEI DATI

Il Codice individua le modalità con le quali possono essere acquisiti i dati di traffico conservati dai fornitori prescrivendo che la richiesta sia formulata con "decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altri parti private" (art. 132, comma 3, del Codice).

Al difensore dell'imputato o della persona sottoposta alle indagini è riconosciuta la facoltà di richiedere, direttamente, al fornitore i dati di traffico limitatamente ai dati che si riferiscano "alle utenze intestate al proprio assistito". La richiesta deve essere effettuata "con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale, fermerestando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante" (art. 132, comma 3, cit.). Tale ultimo

riferimento ai presupposti previsti dal Codice per l'accesso alle chiamate in entrata comporta, anche per i fornitori, la necessaria valutazione preliminare della circostanza che dalla mancata conoscenza dei dati richiesti possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397. A tale riguardo si richiama quanto rilevato nel provvedimento adottato dal Garante in materia il 3 novembre 2005, consultabile sul sito dell'Autorità (doc. web n. 1189488).

7. MISURE E ACCORGIMENTI DA PRESCRIVERE

Come premesso, il Garante è stato preposto per disposizione di legge a individuare accorgimenti e misure da porre a garanzia degli interessati nell'ambito della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione di reati (art. 132, comma 5, del Codice).

A tal fine, il Garante ha curato preliminarmente diversi approfondimenti tecnici con esperti del settore, nonché numerosi accertamenti ispettivi presso primari fornitori di servizi di comunicazione elettronica; ha, infine, indetto una specifica consultazione pubblica su un articolato documento indicante le misure e gli accorgimenti ritenuti idonei per la conservazione dei dati di traffico per finalità di giustizia.

Le cautele ipotizzate in sede di consultazione pubblica hanno trovato conforto all'esito della stessa, non essendo pervenuti all'Autorità sostanziali rilievi critici da parte dei soggetti interessati. Tutte le riflessioni e commenti pervenuti sono stati comunque oggetto di specifica analisi e considerazione nell'elaborazione del presente provvedimento.

Nell'individuare le seguenti cautele che il Garante prescrive ai fornitori interessati al presente provvedimento, l'Autorità ha tenuto conto dei parametri indicati negli artt. 17 e 132, comma 5, del Codice, nonché:

a) dell'esigenza normativa volta a prevedere specifiche cautele rapportate alla quantità e qualità dei dati da proteggere e ai rischi indicati nell'art. 31 del Codice, rischi che i fornitori devono già oggi prevenire rispettando i comuni obblighi di sicurezza collegati alle misure non solo minime previste dal Codice (artt. 31 e ss.; Allegato B.;

b) dell'opportunità di individuare, allo stato, misure protettive per i trattamenti svolti da

tutti i fornitori interessati che siano verificabili anche in sede ispettiva, ai fini di una più incisiva messa in sicurezza dei dati di traffico telefonico e telematico;

c) della necessità di tener e in considerazione i costi derivanti dall'adozione delle misure e degli accorgimenti prescritti con il presente provvedimento, anche in ragione della variegata capacità tecnica ed economica dei soggetti interessati;

d) del contesto europeo di riferimento, specie alla luce dei pareri resi dal Gruppo per la tutela dei dati personali (cfr. parere n. 4/2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/Ce; parere n. 3/2006 sulla direttiva 2006/24/Ce del Parlamento europeo e del Consiglio riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione che modifica la direttiva 2002/58/Ce; parere n. 8/2006 sulla revisione del quadro normativo per le reti ed i servizi di comunicazione elettronica, con particolare attenzione alla direttiva relativa alla vita privata e alle comunicazioni elettroniche);

e) dello stato dell'evoluzione tecnologica, alla luce del quale le seguenti prescrizioni devono pertanto ritenersi soggette ad aggiornamento periodico.

Di seguito, sono indicati gli accorgimenti e le misure prescritti dal Garante.

Tali misure e accorgimenti devono essere adottati dai fornitori di comunicazione elettronica anche in caso di conservazione temporanea dei dati relativi al traffico telematico a fini di svolgimento di investigazioni preventive o di accertamento e repressione di reati, ai sensi del menzionato art. 132, comma 4 ter, del Codice.

Per effetto del presente provvedimento:

7.1. *Sistemi di autenticazione*

Il trattamento dei dati di traffico telefonico e telematico da parte dei fornitori deve essere consentito solo agli incaricati del trattamento e unicamente sulla base del preventivo utilizzo di specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per

il trattamento, evitando che questo possa av er luogo senza che l 'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti.

Tale fase di autenticazione può essere realizzata con procedure strettamente integrate alle applicazioni informatiche con cui il fornitor e tratta i dati di traffico, oppur e con pr ocedure per la protezione delle singole postazioni di lavoro che si integrino alle funzioni di autenticazione proprie dei sistemi operativi utilizzati. N el secondo caso, il fornitor e deve assicurare che non esistano modalità di accesso alle applicazioni informatiche da par te dei propri incaricati di trattamento che consentano di eludere le procedure di strong authentication predisposte per l'accesso alla postazione di lavoro.

Per i dati di traffico conservati per esclusive finalità di accertamento e repressione dei reati (cioè quelli generati da più di sei mesi, oppure la totalità dei dati trattati per queste finalità se conservati separatamente dai dati trattati per le altre finalità fin dalla loro generazione), una di tali tecnologie dev e esser e basata sull 'elaborazione di caratteristiche biometriche dell 'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento.

Tali modalità di autenticazione dev ono essere applicate anche a tutti gli addetti tecnici (ammi - nistratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore.

Limitatamente a tali addetti tecnici, cir costanze legate a indifferibili inter venti per malfunzionamenti, guasti, installazioni har dware e softwar e, aggiornamento e riconfigurazione dei sistemi, possono determinare la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di autenticazione biometrica o di str ong-authentication per operazioni che comportano la presenza fisica dell'addetto che procede all'intervento in prossimità del sistema di elaborazione (per esempio, per lo svolgimento di operazioni di amministrazione da console locale che implichino la disabilitazione dei ser vizi di r ete e l 'impossibilità di gestir e operazioni di input/output tramite dispositivi accessori come quelli utilizzabili per la str ong authentication).

In caso di accesso da par te degli addetti tecnici nei termini anzidetti, fermo r estando l'obbligo di assicurare le misur e minime in tema di cr edenziali di autenticazione pr eviste dall'Allegato B. al Codice e, per quanto concerne i trattamenti di dati di traffico telefonico per esclusiv e finalità di

giustizia, quanto specificato al successivo paragrafo 7.3, dovrà essere tenuta preventivamente traccia in un apposito "registro degli accessi" dell'evento, nonché delle motivazioni che lo hanno determinato, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.

7.2. *Sistemi di autorizzazione*

Relativamente ai sistemi di autorizzazione devono essere adottate specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. Tali differenti funzioni non possono essere attribuite contestualmente a uno stesso soggetto.

I profili di autorizzazione da definire e da attribuire agli incaricati devono differenziare le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice).

7.3. *Conservazione separata*

I dati di traffico conservati per esclusive finalità di accertamento e repressione di reati vanno trattati necessariamente tramite sistemi informatici distinti fisicamente da quelli utilizzati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia nell'immagazzinamento dei dati (storage).

Più specificamente, i sistemi informatici utilizzati per i trattamenti di dati di traffico conservati per esclusiva finalità di giustizia devono essere differenti da quelli utilizzati anche per altre funzioni aziendali (come fatturazione, marketing, antifrode) ed essere, altresì, protetti contro il rischio di intrusione mediante idonei strumenti di protezione perimetrale a salvaguardia delle reti di comunicazione e delle risorse di memorizzazione impiegate nei trattamenti.

I dati di traffico conservati per un periodo non superiore a sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i

medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità, per l'elaborazione con sistemi dedicati a questo specifico trattamento.

Questa prescrizione lascia ai fornitori la facoltà di scegliere, sulla base di propri modelli organizzativi e della propria dotazione tecnologica, l'architettura informatica più idonea per la conservazione obbligatoria dei dati di traffico e per le ordinarie elaborazioni aziendali; permette infatti che i dati di traffico conservati sino a sei mesi dalla loro generazione possano essere trattati, per finalità di giustizia, con sistemi informatici non riservati esclusivamente a tali elaborazioni; oppure, che gli stessi dati vengano duplicati per effettuare un trattamento dedicato esclusivamente al perseguimento delle finalità di giustizia. In quest'ultimo caso le misure e gli accorgimenti prescritti per i dati conservati per esclusive finalità di giustizia si applicano sin dall'inizio del trattamento.

Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali.

Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico.

Devono essere adottate misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni.

7.4. *Incaricati del trattamento*

Gli incaricati che accedono ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo, devono essere designati specificamente in rapporto ai dati medesimi.

Il processo di designazione deve prevedere la frequenza di una periodica attività formativa con-

cernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. L'effettiva partecipazione al corso deve essere documentata.

Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico (menzionate anche nell'art. 132, comma 5, lett. c)), nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera f) del Codice, il titolare del trattamento deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo.

7.5. *Cancellazione dei dati*

Allo scadere dei termini previsti dalle disposizioni vigenti, i dati di traffico sono resi non disponibili per le elaborazioni dei sistemi informativi e le relative consultazioni; sono altresì cancellati o resi anonimi senza alcun ritardo, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente, documentando tali operazioni al più tardi entro trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice.

7.6. *Altre misure*

Audit log

Devono essere adottate soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati.

Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.

I sistemi di audit log devono garantire la completezza, l'immodificabilità e l'autenticità delle

registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi devono essere adottati, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche.

Le misure di cui al presente paragrafo sono adottate nel rispetto dei princìpi in materia di controllo dei lavoratori sull'uso di strumenti elettronici, con particolare riguardo all'informativa agli interessati (cfr. Provv. 1° marzo 2007, doc. web n. 1387522).

7.7. *Audit interno–Rapporti periodici*

La gestione dei dati di traffico per finalità di accertamento e repressione di reati deve essere oggetto, con cadenza almeno annuale, di un'attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.

L'attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati.

I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di Alerting e di Anomaly Detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione.

L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate.

L'esito dell'attività di controllo deve essere:

- comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari

livelli in base al proprio ordinamento interno, la volontà della società;

- richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza;
- messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria.

7.8. *Documentazione dei sistemi informativi*

I sistemi informativi utilizzati per il trattamento dei dati di traffico devono essere documentati in modo idoneo secondo i princìpi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione.

La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema.

La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati.

La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico.

7.9. *Cifratura e protezione dei dati*

I dati di traffico trattati per esclusive finalità di giustizia vanno protetti con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. In particolare, devono essere adottate soluzioni che rendano le informazioni, residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei database o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche.

Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, data base administrator e manuten-

tori hardware e software) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate.

Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire, più in generale, la sicurezza dei sistemi, evitando di esporli a vulnerabilità e a rischio di intrusione (a titolo esemplificativo, l'accesso interattivo in modalità "emulazione di terminale", anche per scopi tecnici, non deve essere consentito su canali non sicuri, così come deve essere evitata l'attivazione di servizi di rete non necessari che si possono prestare alla realizzazione di forme di intrusione).

7.10. *Tempi di adozione delle misure e degli accorgimenti*

Valutato il complesso delle misure e degli accorgimenti, tenuto conto del quadro delle cautele che emergono dalle risultanze ispettive essere già in atto presso i fornitori, nonché dei tempi tecnici necessari per completarne l'attuazione, anche alla luce di quanto emerso dalla consultazione pubblica, risulta dagli atti congruo fissare un termine transitorio per i trattamenti di dati in essere, prevedendo che tutti gli adempimenti di cui al presente punto 7 siano completati al più presto ed entro, e non oltre, il termine che è parimenti congruo stabilire per tutti i fornitori al 30 aprile 2009, ovvero per quanto riguarda la strong authentication riferita agli incaricati che accedono ai dati di traffico nell'ambito dell'attività di call center, al 30 giugno 2009. Entro tale termine, i fornitori dovranno dare conferma al Garante attestando formalmente l'integrale adempimento al presente provvedimento.

8. APPLICAZIONE DI ALCUNE MISURE A DATI TRATTATI PER ALTRE FINALITÀ

Le considerazioni svolte sulla natura particolarmente delicata dei dati di traffico, sulla necessità di garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone e di prescrivere una più incisiva messa in sicurezza di dati rilevano anche per ogni altro trattamento di dati di traffico telefonico e telematico effettuato dai fornitori di cui al paragrafo 3.

Ciò, comporta l'improrogabile esigenza di assicurare che almeno alcuni tra gli accorgimenti e le misure di cui al precedente punto 7, limitatamente a quelli adattabili al caso di specie, siano applicati comunque dai predetti fornitori nell'ambito di analoghi trattamenti di dati di traffico telefonico e telematico effettuati per finalità non di giustizia, ma di fatturazione, pagamento in caso di interconnessione e commercializzazione di servizi, nel più breve periodo temporale indicato nel menzionato art. 123.

Per tali ragioni il Garante, contestualmente e distintamente da quanto va disposto ai sensi dell'art. 132, comma 5, del Codice, prescrive ai fornitori di cui al paragrafo 3, ai sensi dell'art. 17 del medesimo Codice, di adottare nel termine e con la modalità di cui al paragrafo 7.10. le misure e gli accorgimenti indicati nella lettera c) del seguente dispositivo.

Copia del presente provvedimento verrà 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.

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi degli artt. 17, 123 e 132, comma 5, del Codice, prescrive ai fornitori di servizi di comunicazione elettronica individuati nel paragrafo 3 di adottare nel trattamento dei dati di traffico telefonico e telematico di cui al paragrafo 4 le misure e gli accorgimenti a garanzia degli interessati individuate nel presente provvedimento, provvedendo a (par. 7):

   1. adottare specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento, nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Per i dati di traffico trattati per esclusive finalità di accertamento e repressione dei reati, una di tali tec-

nologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, in modo tale da assicurare la presenza fisica di quest'ultimo presso la postazione di lavoro utilizzata per il trattamento. Tali modalità di autenticazione devono essere applicate anche a tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che possano accedere ai dati di traffico custoditi nelle banche dati del fornitore. Relativamente ai soli addetti tecnici indicati al presente punto 1, qualora circostanze legate a indifferibili interventi per malfunzionamenti, guasti, installazioni hardware e software, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso informatico a sistemi di elaborazione che trattano dati di traffico in assenza di strong authentication, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B. al Codice, deve essere tenuta traccia dell'evento in un apposito "registro degli accessi", nonché delle motivazioni che li hanno determinati, con una successiva descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore.

2. adottare specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati. Il fornitore deve definire e attribuire agli incaricati specifici profili di autorizzazione differenziando le funzioni di trattamento dei dati di traffico per finalità di ordinaria gestione da quelle per finalità di accertamento e repressione dei reati e, infine, dalle funzioni di trattamento dei dati in caso di esercizio dei diritti dell'interessato (art. 7 del Codice);
3. adottare, per la conservazione dei dati di traffico per esclusive finalità di accertamento e repressione di reati, sistemi informatici distinti fisicamente da quelli utiliz-

zati per gestire dati di traffico anche per altre finalità, sia nelle componenti di elaborazione, sia di immagazzinamento dei dati (storage). I dati di traffico conservati per un periodo non superiore ai sei mesi dalla loro generazione possono, invece, essere trattati per le finalità di giustizia sia prevedendone il trattamento con i medesimi sistemi di elaborazione e di immagazzinamento utilizzati per la generalità dei trattamenti, sia provvedendo alla loro duplicazione, con conservazione separata rispetto ai dati di traffico trattati per le ordinarie finalità. Le attrezzature informatiche utilizzate per i trattamenti di dati di traffico per le esclusive finalità di giustizia di cui sopra devono essere collocate all'interno di aree ad accesso selezionato (ovvero riservato ai soli soggetti legittimati ad accedervi per l'espletamento di specifiche mansioni) e munite di dispositivi elettronici di controllo o di procedure di vigilanza che comportino la registrazione dei dati identificativi delle persone ammesse, con indicazione dei relativi riferimenti temporali. Nel caso di trattamenti di dati di traffico telefonico per esclusive finalità di giustizia, il controllo degli accessi deve comprendere una procedura di riconoscimento biometrico. Infine, il fornitore deve adottare misure idonee a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici in tempi compatibili con i diritti degli interessati e comunque non superiori a sette giorni;

4. designare specificamente gli incaricati che possono accedere ai dati di traffico conservati per le finalità di cui all'art. 132 del Codice, anche per consentire l'esercizio dei diritti di cui all'art. 7 del Codice medesimo. Il processo di designazione deve prevedere la documentata frequenza di una periodica attività formativa concernente l'illustrazione delle istruzioni, il rispetto delle misure di sicurezza e le relative responsabilità. Per quanto riguarda le richieste per l'esercizio dei diritti di cui all'art. 7 del Codice che comportano l'estrazione dei dati di traffico, nei limiti in cui ciò è consentito ai sensi dell'art. 8, comma 2, lettera f) del Codice, il fornitore deve conservare in forma specifica la documentazione comprovante l'idonea verifica dell'identità del richiedente ai sensi dell'art. 9 del Codice stesso, e adottare opportune cautele per comunicare i dati al solo soggetto legittimato in base al medesimo articolo;

5. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti. Il fornitore deve cancellare o rendere anonimi senza ritardo tali dati, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di cui all'art. 132 del Codice;
6. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati. Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di audit log devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi il fornitore deve adottare, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;
7. svolgere, con cadenza almeno annuale, un'attività di controllo interno per verificare costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal prov-

vedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati. Tale attività di controllo deve essere demandata a un'unità organizzativa o, comunque, a personale diverso rispetto a quelli cui è affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di Alerting e di Anomaly Detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione. L'attività di controllo deve essere adeguatamente documentata in modo tale che sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito dell'attività di controllo deve essere: comunicato alle persone e agli organi legittimati ad adottare decisioni e ad esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della società; richiamato nell'ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza; messo, a richiesta, a disposizione del Garante o dell'autorità giudiziaria;

8. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e

messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

9. proteggere i dati di traffico trattati per esclusive finalità di giustizia con tecniche crittografiche, in particolare contro rischi di acquisizione fortuita o di alterazione accidentale derivanti da operazioni di manutenzione sugli apparati informatici o da ordinarie operazioni di amministrazione di sistema. Il fornitore deve adottare soluzioni che rendano le informazioni residenti nelle basi di dati a servizio delle applicazioni informatiche utilizzate per i trattamenti, non intelligibili a chi non disponga di diritti di accesso e profili di autorizzazione idonei, ricorrendo a forme di cifratura od offuscamento di porzioni dei data base o degli indici o ad altri accorgimenti tecnici basati su tecnologie crittografiche. Tale misura deve essere efficace per ridurre al minimo il rischio che incaricati di mansioni tecniche accessorie ai trattamenti (amministratori di sistema, data-base administrator e manutentori hardware e software) possano accedere indebitamente alle informazioni registrate, anche fortuitamente, acquisendone conoscenza nel corso di operazioni di accesso ai sistemi o di manutenzione di altro genere, oppure che possano intenzionalmente o fortuitamente alterare le informazioni registrate. Eventuali flussi di trasmissione dei dati di traffico tra sistemi informatici del fornitore devono aver luogo tramite protocolli di comunicazione sicuri, basati su tecniche crittografiche, o comunque evitando il ricorso alla trasmissione in chiaro dei dati. Protocolli di comunicazione sicuri devono essere adottati anche per garantire più in generale la sicurezza dei sistemi evitando di esporli a vulnerabilità e a rischio di intrusione;

b) ai sensi dei medesimi artt. 17, 123 e 132, comma 5 del Codice, nonché dell'art. 157 del Codice, prescrive ai predetti fornitori titolari del trattamento di effettuare tutti gli adempimenti di cui alla precedente lett. a) al più presto e, comunque, entro e non oltre il termine del 30 aprile 2009, dandone conferma al Garante attestando entro lo stesso termine l'integrale adempimento;

c) ai sensi dell'art. 17 del Codice prescrive ai medesimi fornitori titolari del trattamento di adottare, rispetto ai dati di traffico trattati per le finalità di cui all'art. 123 del Codice,

entro e non oltre il termine del 30 aprile 2009, ovvero per quanto riguarda la strong authentication riferita agli incaricati che accedono ai dati di traffico nell'ambito dell'attività di call center, 30 giugno 2009, dandone ai sensi dell'art. 157 del Codice conferma al Garante e attestando entro lo stesso termine l'integrale adempimento, i seguenti accorgimenti e misure (par. 8):

1. adottare specifici sistemi di autenticazione informatica basati su tecniche di strong authentication, consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione, che si applichino agli accessi ai sistemi di elaborazione da parte di tutti gli incaricati di trattamento nonché di tutti gli addetti tecnici (amministratori di sistema, di rete, di data base) che abbiano la possibilità concreta di accedere ai dati di traffico custoditi nelle banche dati del fornitore, qualunque sia la modalità, locale o remota, con cui si realizzi l'accesso al sistema di elaborazione utilizzato per il trattamento, evitando che questo possa aver luogo senza che l'incaricato abbia comunque superato una fase di autenticazione informatica nei termini anzidetti. Qualora circostanze eccezionali, legate a indifferibili interventi per malfunzionamenti, guasti, installazione hardware e software, aggiornamento e riconfigurazione dei sistemi, determinino la necessità di accesso a sistemi di elaborazione che trattano dati di traffico da parte di addetti tecnici in assenza di strong authentication, fermo restando l'obbligo di assicurare le misure minime in tema di credenziali di autenticazione previste dall'Allegato B. al Codice in materia di protezione dei dati personali, deve essere tenuta traccia in un apposito "registro degli accessi" dell'eventuale accesso fisico ai locali in cui sono installati i sistemi di elaborazione oggetto di intervento e dell'accesso logico ai sistemi, nonché delle motivazioni che li hanno determinati, con una descrizione sintetica delle operazioni svolte, anche mediante l'utilizzo di sistemi elettronici. Tale registro deve essere custodito dal fornitore presso le sedi di elaborazione e messo a disposizione del Garante nel caso di ispezioni o controlli, unitamente a un elenco nominativo dei soggetti abilitati all'accesso ai diversi sistemi di elaborazione con funzioni di amministratore di sistema, che deve essere formato e aggiornato costantemente dal fornitore;

2. adottare procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati;
3. rendere i dati di traffico immediatamente non disponibili per le elaborazioni dei sistemi informativi allo scadere dei termini previsti dalle disposizioni vigenti, provvedendo alla loro cancellazione o trasformazione in forma anonima, in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery) effettuate dal titolare anche in applicazione di misure previste dalla normativa vigente e, al più tardi, documentando tale operazione entro i trenta giorni successivi alla scadenza dei termini di conservazione (art. 123 del Codice);
4. adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi database utilizzati. Tali soluzioni comprendono la registrazione, in un apposito audit log, delle operazioni compiute, direttamente o indirettamente, sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici. I sistemi di audit log devono garantire la completezza, l'immodificabilità, l'autenticità delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing. A tali scopi il fornitore deve adottare, per la registrazione dei dati di auditing, anche in forma centralizzata per ogni impianto di elaborazione o per datacenter, sistemi di memorizzazione su dispositivi non alterabili. Prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche;

5. documentare i sistemi informativi utilizzati per il trattamento dei dati di traffico in modo idoneo secondo i princìpi dell'ingegneria del software, evitando soluzioni documentali non corrispondenti a metodi descrittivi standard o di ampia accettazione. La descrizione deve comprendere, per ciascun sistema applicativo, l'architettura logico-funzionale, l'architettura complessiva e la struttura dei sistemi utilizzati per il trattamento, i flussi di input/output dei dati di traffico da e verso altri sistemi, l'architettura della rete di comunicazione, l'indicazione dei soggetti o classi di soggetti aventi legittimo accesso al sistema. La documentazione va corredata con diagrammi di dislocazione delle applicazioni e dei sistemi, da cui deve risultare anche l'esatta ubicazione dei sistemi nei quali vengono trattati i dati per le finalità di accertamento e repressione di reati. La documentazione tecnica deve essere aggiornata e messa a disposizione dell'Autorità su sua eventuale richiesta, unitamente a informazioni di dettaglio sui soggetti aventi legittimo accesso ai sistemi per il trattamento dei dati di traffico;

d) dispone 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, 17 gennaio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

28. Anagrafe tributaria: sicurezza e accessi (*)

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);

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 prof. Francesco Pizzetti;

PREMESSO

Sulla base di un'analisi preliminare del sistema informativo della fiscalità, il 14 dicembre 2007 il Garante ha deliberato l'avvio di accertamenti volti a verificare, in più fasi, i trattamenti di dati personali effettuati presso l'anagrafe tributaria, rilevando che elementi di maggior criticità e urgenza erano da ravvisarsi nelle misure di sicurezza adottate per gli accessi da parte di enti esterni, pubblici e privati, all'amministrazione finanziaria.

La prima fase di accertamenti attinente a tali accessi è stata completata. Il Garante svolgerà nel prosieguo le altre verifiche programmate sul trattamento dei dati effettuato dalle articolazioni dell'amministrazione finanziaria, con particolare riguardo alla struttura degli archivi, alle modalità di accesso, alle applicazioni utilizzate, alle tipologie di informazioni, alle misure di sicurezza, alle abilitazioni e alle autorizzazioni degli utenti.

Le attività ispettive completate hanno invece riguardato, in particolare:

1) il controllo degli applicativi che consentono l'accesso all'anagrafe tributaria a soggetti esterni all'amministrazione finanziaria (loro funzionalità; tipologie di dati visualizzabili con i differenti profili di autorizzazione previsti);
2) la designazione di responsabili e di incaricati, i sistemi di autenticazione (ad es., modalità di formazione e gestione delle password; controlli degli accessi ai sistemi applicativi)

(*) [doc. *web* n. 1549548]

e i sistemi di autorizzazione;

3) le procedure di audit interno ed esterno sull'accesso alle informazioni contenute nell'anagrafe tributaria (ad es., controlli sulle abilitazioni e sulle autorizzazioni degli utenti abilitati all'utilizzo degli applicativi, modalità di raccolta dei log file e loro analisi automatizzata).

Gli accertamenti ispettivi hanno avuto luogo presso l'Agenzia delle entrate, Sogei S.p.A. (Società generale d'informatica, responsabile del trattamento dei dati contenuti nell'anagrafe tributaria), regioni, province, comuni e altri enti che accedono a tale anagrafe, con la piena collaborazione degli enti coinvolti. Le verifiche hanno consentito di evidenziare criticità, in ambito sia informatico, sia organizzativo, documentate nei verbali in atti.

Dalle risultanze emerge che i sistemi di collegamento all'anagrafe tributaria utilizzati dai soggetti esterni all'amministrazione finanziaria sono i seguenti:

- "Siatel", applicazione web utilizzata principalmente da comuni, province, regioni, università, asl e consorzi di bonifica, per un totale di circa 9.400 enti e 60.000 utenze, che consente di visualizzare dati anagrafici completi, dati fiscali e atti del registro relativi alla totalità dei contribuenti;
- "Puntofisco", applicazione web di recente realizzazione e attualmente in dotazione a enti previdenziali, tribunali, camere di commercio e società varie, per un totale di circa 180 enti e 18.000 utenze. Puntofisco consente di visualizzare dati anagrafici, fiscali e atti del registro relativi alla totalità dei contribuenti, più aggiornati e con maggiore segmentazione delle informazioni rispetto a Siatel (ad es., differenziando tra dati anagrafici attuali o completi dello storico), ma permette anche di accedere a dati sensibili (presenti nel dettaglio degli oneri deducibili);
- "3270 enti esterni", collegamento diretto, tramite terminali fisici o emulatori di terminale, ai sistemi centrali dell'anagrafe tributaria, in corso di dismissione per esigenze di aggiornamento tecnologico, che tuttora consente a soggetti anche privati (Telecom Italia S.p.A., Enel, Inail, Inps, camere di commercio, Ministero delle politiche agricole, "inter forze") di collegarsi a informazioni anagrafiche e fiscali relative alla totalità dei contribuenti; la struttura dell'applicativo non consente all'Agenzia delle entrate di conoscere il numero di utenti;
- "Entratel", applicativo utilizzato dagli enti principalmente ai fini della trasmissione delle

dichiarazioni, con flussi di dati solo in entrata verso l'Agenzia delle entrate; le credenziali di autenticazione fornite dall'Agenzia permettono altresì all'operatore di visualizzare la posizione fiscale dell'ente attraverso l'apposita web application ("Fisconline"/"Cassetto fiscale");

- "web services", strumenti realizzati sulla base di specifiche tecniche definite caso per caso dall'Agenzia delle entrate, che consentono di accedere a dati anagrafici anche completi relativi alla totalità dei contribuenti. Tali collegamenti sono utilizzati da 21 enti, ma la configurazione del collegamento non consente all'Agenzia di conoscere il numero di utenti;
- "file transfer", collegamenti per la gestione di flussi di dati per la gran parte in entrata (principalmente provenienti da banche), ma alcuni anche in uscita (ad es., verso concessionari della riscossione), utilizzati da circa 200 enti.

OSSERVA

Nel corso dei menzionati accertamenti ispettivi, sulla base della documentazione in atti, sono state riscontrate alcune criticità di seguito descritte, già in parte riconosciute dall'Agenzia, relative agli accessi all'anagrafe tributaria da parte degli enti esterni all'amministrazione finanziaria, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati. Accanto a diverse problematiche attinenti alla sicurezza, sono emersi e vengono affrontati connessi profili concernenti aspetti sostanziali del trattamento.

Il Garante, ai sensi dell'art. 154, comma 1, lett. c) del Codice, ritiene necessario prescrivere una serie di misure e accorgimenti che devono essere adottati dall'Agenzia delle entrate, anche in riferimento ai soggetti esterni che accedono all'anagrafe tributaria, di seguito indicati. Tali misure e accorgimenti, principalmente di carattere tecnico e organizzativo, sono necessari al fine di porre rimedio alle carenze riscontrate e a incrementare, in particolare, i livelli di sicurezza degli accessi all'anagrafe tributaria, rendendo il trattamento conforme alle disposizioni vigenti.

1. ACCESSI ALL'ANAGRAFE TRIBUTARIA DA PARTE DI SOGGETTI ESTERNI ALL'AMMINISTRAZIONE FINANZIARIA: PROFILI GENERALI

Criticità

Alcuni accertamenti in proposito sono risultati meno agevoli in considerazione del fatto che l'Agenzia non aveva immediatamente disponibile, come richiesto dall'Autorità, una completa documentazione relativa sia ai soggetti esterni collegati, sia ai sistemi di accesso utilizzati da questi ultimi (numero e categorie di soggetti, finalità degli accessi e tipologie di collegamenti e di dati comunicati).

Dagli atti emerge ora che l'Agenzia autorizza gli accessi all'anagrafe tributaria solo in seguito alla stipula di apposite convenzioni, anche standard, a livello centrale e regionale. Tuttavia, l'assenza di una documentazione di insieme sui collegamenti in essere non agevola un monitoraggio costante sulla sussistenza dei presupposti che hanno consentito l'attivazione del canale informativo, nonché i dovuti controlli sulla correttezza della gestione degli accessi e della consultazione delle informazioni. La periodica ricognizione degli enti che accedono all'anagrafe tributaria, e dei rispettivi utenti, costituisce infatti la premessa per prevenire usi impropri e illeciti delle informazioni in essa contenute.

È stato inoltre riscontrato in atti che in alcune convenzioni stipulate per l'accesso all'anagrafe tributaria non risultano delimitate chiaramente le finalità per cui gli accessi vengono autorizzati; sotto tale aspetto, è stato rilevato che alcuni enti, attraverso gli amministratori locali (soggetti deputati all'abilitazione degli utenti), hanno abilitato di propria iniziativa alcuni utenti al fine di attivare nuovi flussi di dati per finalità ulteriori rispetto a quelle consentite.

Non risulta altresì dagli atti che gli operatori che effettuano gli accessi abbiano l'onere (o la possibilità) di registrare, anche al fine di successivi controlli, le ragioni a supporto delle interrogazioni eseguite.

È stato inoltre verificato che i dati visualizzabili attraverso gli applicativi non sono segmentabili in relazione al bacino di utenza dell'ente che chiede il collegamento (ad es., territorio comunale), e sono relativi a tutto il territorio nazionale.

Infine, le informazioni consultabili non risultano, talvolta, sufficientemente aggiornate per lo svolgimento delle funzioni istituzionali cui gli accessi sono finalizzati (ad es., in Siatel, ai fini

della verifica dell'Isee non sono visualizzabili i dati dell'ultima dichiarazione presentata e vengono invece visualizzati dati reddituali riferiti ad annualità pregresse, eccedenti e non pertinenti rispetto alle finalità perseguite, che non consentono di effettuare i puntuali controlli sulle autocertificazioni reddituali ai sensi del d.P.R. n. 445/2000).

Da ultimo, sulla base delle risultanze in atti, è stato rilevato che gli accessi all'anagrafe tributaria vengono effettuati talvolta per conoscere informazioni (ad es., la residenza) che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti (ad es., amministrazioni certificanti ai sensi dell'art. 71 del d.P.R. n. 445/2000).

Prescrizioni

L'Agenzia deve disporre di informazioni complete e strutturate sulla molteplicità di soggetti che, a vario titolo, accedono alla banca dati dell'anagrafe tributaria. Occorre pertanto che la stessa rediga un documento, con formalità descrittive standard, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, batch o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa (anche ai sensi dell'art. 19, comma 2 del Codice, previa comunicazione al Garante), la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento dovrà essere mantenuto costantemente aggiornato, nonché reso disponibile nel caso di controlli.

L'Agenzia deve altresì verificare, con cadenza periodica annuale, l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice (norme di legge o regolamento, nonché eventuali comunicazioni al Garante ai sensi dell'art. 19 del Codice) e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti.

Per vincolare effettivamente gli accessi alle finalità consentite, l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati un campo per l'indicazione obbliga-

toria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

L'Agenzia deve poi far sì che gli applicativi consentano, per quanto più possibile, la segmentazione dei dati visualizzabili -in particolare in modo cronologico (attuale o storico, per periodi di imposta), geografico (comune, provincia, regione) e per tipologia di dati (ad es. di sintesi)- al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza dell'ente che chiede il collegamento, esclusivamente i dati necessari rispetto alle finalità perseguite (ad es. l'ultimo domicilio fiscale o l'ultimo periodo di imposta).

2. I SISTEMI UTILIZZATI PER IL COLLEGAMENTO ALL'ANAGRAFE TRIBUTARIA

2.1. *Profili comuni*

Le principali criticità di carattere generale relative all'utilizzo degli applicativi riscontrate nel corso degli accertamenti ispettivi sugli accessi da parte dei soggetti esterni sono di seguito individuate.

2.1.1. Sicurezza dei sistemi di autenticazione

Criticità

Per le web application è stato utilizzato un certificato Ssl di tipo self signed (non firmato da una Ca, Certification authority, ufficiale) non attendibile che, in mancanza di una Ca affidabile, non offre le garanzie di certezza dell'identità dell'erogatore del servizio tipiche della certificazione digitale tramite Pki (public key infrastrucure): risultano pertanto facilitate azioni di phishing in danno di utenti del sistema e la possibile acquisizione indebita di credenziali di autenticazione, idonea a consentire utilizzi impropri dell'applicazione.

Dalle risultanze agli atti emerge inoltre che, rispetto a taluni collegamenti, l'identificazione dell'utente finale dell'applicazione è in molti casi in capo all'ente esterno. L'Agenzia non ha pertanto alcuna conoscenza dell'effettiva identità e del numero degli utenti che accedono, con tali modalità di connessione, da sistemi informativi esterni collegati direttamente all'anagrafe tributaria (ad es., 3270 enti esterni e web services).

È risultato, poi, possibile accedere alle web application Siatel e Puntofisco attraverso l'utilizzo delle medesime credenziali contemporaneamente da postazioni diverse, anche con indirizzo Ip

diverso (perfino da rete esterna all'ente), nonostante, per quanto riguarda il Siatel, all'atto dell'accesso tale possibilità venga esclusa da un apposito avviso.

Prescrizioni

L'Agenzia deve prevedere che tutte le applicazioni accessibili da rete pubblica in forma di web application siano implementate con protocolli https/ssl provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale, evitando il ricorso a certificati di tipo self-signed.

Allo scopo di identificare le postazioni da cui vengono effettuati gli accessi, occorre inoltre che l'Agenzia implementi un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che, basandosi sul mutuo riconoscimento tra i server che erogano il servizio e le postazioni che accedono a esso, consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

A fronte dell'accertata possibilità per taluni applicativi di effettuare più accessi contemporanei con le medesime credenziali, al fine di consentire a ciascun utente di controllare l'utilizzo del proprio account, l'Agenzia deve poi prevedere -in considerazione della specificità dell'anagrafe tributaria- la visualizzazione, nella prima schermata successiva al collegamento, di informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Per accrescere la consapevolezza del controllo, le stesse informazioni devono essere riportate anche relativamente alla sessione corrente.

Infine, l'Agenzia deve disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali (sessioni multiple), limitandone l'utilizzo ai soli casi necessari per esigenze di servizio (ad es., per le connessioni originate da una stessa postazione di lavoro). In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti, come sopra descritto. Nel caso in cui non sia possibile individuare la postazione di lavoro, nelle more dell'attuazione delle prescrizioni sopra individuate, deve essere inibita la possibilità di accessi contemporanei.

2.1.2. Amministratori locali, abilitazioni e autorizzazioni

Criticità

È stato verificato negli accertamenti ispettivi che gli enti esterni hanno spesso affidato il compito di amministratore locale (il soggetto deputato alla gestione delle utenze) a personale non in grado né di valutare la pertinenza delle richieste di abilitazione delle utenze, né di monitorarne gli eventuali utilizzi impropri. In taluni enti è stata riscontrata la presenza di più amministratori locali con funzionalità che non consentivano di gestire gli utenti in modo tra loro coordinato.

Dalle risultanze agli atti è emerso, inoltre, che non è stato predeterminato un adeguato flusso informativo tra l'amministratore locale e l'unità organizzativa deputata alla gestione del personale al fine di consentire l'immediata disabilitazione o revisione del profilo di autorizzazione dei soggetti indirizzati ad altre mansioni o il cui rapporto con l'ente sia cessato.

Sono stati riscontrati poi casi di cessioni e condivisioni di credenziali di accesso, profili di autorizzazione inadeguati e/o eccessivi rispetto alle finalità perseguite, nonché mancate designazioni di incaricati al trattamento.

É stato verificato altresì che alcuni enti hanno utilizzato strumenti automatizzati di interrogazione che hanno consentito la duplicazione anche massiva di dati contenuti nell'anagrafe tributaria, con la creazione di autonome basi di dati, non conforme alle finalità per le quali è stato autorizzato l'accesso all'anagrafe tributaria.

Dalla documentazione in atti emerge che l'Agenzia, anche a seguito delle prime risultanze dell'attività ispettiva sopra illustrate, ha manifestato l'intenzione di voler gestire direttamente l'abilitazione di tutte le utenze, eliminando gli amministratori di sistema degli enti esterni.

Al riguardo, nonostante le predette criticità concernenti l'attività svolta dagli amministratori esterni, il modello decentrato di gestione delle utenze incentrato su tali figure, opportunamente integrato con le misure di seguito descritte, costituisce comunque il perno per un corretto sistema di accesso all'anagrafe tributaria. L'amministratore locale, infatti, è il soggetto più idoneo a controllare l'attività quotidiana dei propri utenti senza limitarne l'operatività, anche a fronte dell'ingente numero di enti, e quindi di utenti, abilitati ad accedere all'anagrafe tributaria, ognuno per il proprio specifico fabbisogno informativo.

Prescrizioni

L'Agenzia, nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria, deve prevedere che gli "amministratori locali" (soggetti deputati alla gestione delle utenze) scelti dagli enti esterni siano individuati sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze; deve essere altresì dotato degli adeguati strumenti di controllo sugli accessi (cfr. punto 3).

Nelle convenzioni deve essere poi previsto che gli enti esterni, anche per mezzo degli amministratori locali, debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei software. Le convenzioni, entro i medesimi termini, devono inoltre imporre periodici controlli sugli accessi agli enti esterni -anche attraverso gli appositi strumenti di monitoraggio e alert in dotazione all'amministratore locale che saranno attivati dall'Agenzia (cfr. punto 3)- i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni stesse.

Le convenzioni devono anche predefinire una procedura per le autenticazioni e le autorizzazioni che coinvolga attivamente le figure apicali degli uffici interessati e un unico supervisore (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'amministratore locale e l'articolazione che si occupa della gestione delle risorse umane, al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente (soprattutto con riguardo ad enti di rilevanti dimensioni), anche con apposite verifiche a cadenza almeno trimestrale.

Per quanto riguarda la possibilità di individuare più amministratori locali per ciascun ente, l'Agenzia deve valutare e coordinare attentamente i profili di autorizzazione da attribuire, garan-

tendo in capo a un'unica figura la possibilità, ove occorra, di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato (amministratore con ruolo di supervisore).

É necessario che l'Agenzia predefinisca anche soglie relative al numero di utenti abilitabili da ciascun ente in relazione alle sue dimensioni e alle finalità per le quale viene richiesto il collegamento. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia stessa.

Le web application predisposte dall'Agenzia per l'utilizzo da parte di enti esterni vanno integrate con procedure di "autenticazione forte" (strong authentication) per ridurre la possibilità di usi impropri delle credenziali, la loro cessione o la loro sottrazione ai legittimi assegnatari. Tali procedure devono essere prefigurate nei confronti delle classi di utenti cui corrispondono profili di autorizzazione più critici in relazione alle funzioni o ai dati accessibili e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale delle applicazioni. Tali procedure potranno essere basate sull'utilizzo di dispositivi standard quali smart card o token per la generazione di one-time-password.

L'Agenzia deve infine prevedere limitazioni orarie per gli accessi, mantenendo la possibilità di specifiche deroghe adeguatamente motivate.

Le convenzioni stipulate con ciascun ente devono prevedere espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e devono stabilire le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

2.2. *I singoli sistemi*

2.2.1. Siatel

Criticità

Con particolare riferimento all'applicativo Siatel, nel corso degli accertamenti sono state rilevate le seguenti criticità:

- l'area di gestione dei file da scaricare nella funzione "fornitura dati" disponibile per i comuni e le regioni riporta soltanto la data di primo download del file, che rimane da quel momento disponibile per ulteriori e illimitati download non censiti e, pertanto, non controllabili;

- le funzionalità di file transfer , predisposte per i comuni ai fini dell 'allineamento dell'anagrafe tributaria con le anagrafi della popolazione, sono state talvolta utilizzate per finalità diverse, potendo determinare l'introduzione di informazioni errate nei sistemi;
- i dati anagrafici visualizzabili sono completi (ad es., forniscono sempre lo "storico" delle residenze) e non è possibile limitare la consultazione alle sole informazioni anagrafiche attuali.

Prescrizioni

L'Agenzia deve introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo (ad es., rimuovendo il file messo a disposizione in rete dopo un certo tempo dalla richiesta, ovvero indicando il numero di operazioni di download già effettuate per ciascun file, l'utenza, la data e l'orario del download, nonché limitandoli alla sola utenza richiedente).

Con riferimento alle funzionalità di Siatel utilizzabili da parte degli operatori comunali a soli fini anagrafici, devono essere inserite nell'applicativo da parte dell'Agenzia specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune.

2.2.2. Puntofisco

Criticità

In relazione al sistema Puntofisco è stato verificato dalle risultanze in atti che l'applicativo permette di visualizzare i dati sensibili relativi agli oneri deducibili contenuti nelle dichiarazioni dei redditi.

L'amministratore locale ("gestore") non è in grado di visualizzare lo stato delle utenze (attiva/disattiva) e la lista utenti a lui disponibile comprende anche gli utenti già disabilitati. Il sistema di gestione delle utenze, inoltre, non permette regolarmente al gestore (amministratore), visualizzando il profilo dell'utente, di conoscere l'effettiva possibilità di accesso dello stesso al sistema.

Prescrizioni

Occorre aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa che consenta la comunicazione di tale categoria di dati.

L'Agenzia deve inserire all'interno della procedura informatica di gestione degli utenti in uso

all'amministratore locale indicazioni che gli consentano di visualizzare lo status di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Deve essere corretta altresì l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema.

2.2.3. 3270 enti esterni, web services e file transfer

Criticità

Con riferimento alle risultanze ispettive, è stato rilevato che il collegamento denominato 3270 enti esterni, l'accesso tramite web service e lo scambio dati mediante file transfer non consentono attualmente di limitare e controllare gli accessi in relazione alla loro provenienza, e non garantiscono misure idonee a verificare il rispetto delle regole di sicurezza di cui all'Allegato B del Codice. In particolare, è risultato che:

- l'Agenzia non è in grado di quantificare i soggetti che accedono ai dati, di attribuire agli stessi le operazioni tracciate dal sistema e di verificare il rispetto delle misure di sicurezza poiché l'identificazione degli end-user degli applicativi è affidata all'ente esterno che chiede il collegamento, come anche l'attribuzione certa a ogni incaricato di una o più credenziali per l'autenticazione, nonché la periodica scadenza della parola chiave;
- è impossibile per l'Agenzia individuare la postazione che effettua gli accessi, risultando assenti idonei sistemi che la consentirebbero quali, ad esempio, la certificazione digitale sulle postazioni e sugli emulatori di terminale utilizzati.

Prescrizioni

Devono essere garantite condizioni adeguate di protezione dei dati personali, di controllo e di verifica delle attività compiute (funzioni di audit) sugli applicativi utilizzati per accedere all'anagrafe tributaria, nonché strumenti che permettano all'Agenzia di verificare il rispetto delle misure di sicurezza.

Per quanto riguarda gli accessi all'anagrafe tributaria effettuati mediante l'applicativo 3270 enti esterni gli enti ad oggi abilitati devono migrare verso applicativi che offrono maggiori garanzie (ad es., Puntofisco o Siatel).

Con riferimento ai web service, l'Agenzia deve effettuare una ricognizione dei servizi al

momento esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le adeguate misure e gli accorgimenti di seguito descritti.

Laddove, infatti, l'Agenzia intenda impiegare web service esposti anche in una rete pubblica per l'utilizzo da parte di enti esterni, questi, in considerazione della delicatezza delle informazioni contenute nell'anagrafe tributaria, anche al fine di evitare duplicazioni delle banche dati e rischi di disallineamento, devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web service che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un determinato codice fiscale). Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei web service devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati personali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il timestamp, l'indirizzo Ip di provenienza dell'utente e del server interconnesso, l'operazione effettuata e i dati trattati.

I collegamenti per la gestione di flussi di dati mediante file transfer devono essere realizzati su canali di connessione sicuri e l'Agenzia deve garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

2.2.4. Entratel

Criticità

Dagli accertamenti ispettivi è emerso che le caratteristiche tecniche di Entratel, in uso dal 1998, sono state realizzate al fine di consentire al tempo la massima fruibilità dell'applicativo anche a soggetti con limitate risorse tecnologiche. Allo stato degli atti, le credenziali attribuite

dall'Agenzia (anche le chiavi asimmetriche) identificano però solo l 'ente richiedente, anziché l'operatore finale. Per quanto riguarda l'accesso all'applicativo Fisconline/Cassetto fiscale, le password non sono soggette a scadenza periodica.

Prescrizioni

L'Agenzia deve configurare Entratel e Fisconline/Cassetto fiscale in modo da poter v erificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, in particolare, al sistema di scadenza delle passwor d e all 'attribuzione di cr edenziali idonee ad identificar e dir ettamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l 'accesso, autentica e trasmette i file.

3. LE PROCEDURE DI *AUDIT* SULL'ACCESSO ALLE INFORMAZIONI CONTENUTE NELL'ANAGRAFE TRIBUTARIA DA PARTE DI SOGGETTI ESTERNI

Criticità

Gli accertamenti hanno permesso di verificare che tutti i file di log relativi alle transazioni effettuate nell'anagrafe tributaria sono conservati a tempo indeterminato da Sogei S.p.a., quelli relativi agli ultimi sette giorni sono mantenuti in linea, mentre quelli precedenti sono conservati su nastri magnetici. Talvolta Sogei S.p.a., di pr opria iniziativa, al fine di monitorar e anomalie e funzionalità del sistema, ha eseguito alcuni rilievi quantitativi sulle transazioni effettuate pr ovvedendo a segnalare all'Agenzia le attività difformi riscontrate.

Secondo quanto si evince dalla documentazione in atti, l 'Agenzia dispone di uno str umento di business intelligence denominato Vermont che, per quanto riguarda gli enti esterni, consente di controllare gli accessi effettuati dagli utenti con S iatel (e non quindi, in par ticolare, con Puntofisco e w eb ser vices) dal 1° gennaio 2005 alle informazioni lor o disponibili. Tale str umento permette poi monitoraggi statistici degli accessi e la pr edisposizione di sistemi di aler t. Vermont utilizza database multidimensionali e consente di visualizzar e i log r elativi a un'interrogazione delle cd. "informazioni generalizzate at" (principalmente, dati anagrafici e fiscali contenuti in anagrafe tributaria), mentr e quelli r elativi alle v ariazioni delle utenz e o agli accessi a dati diversi, pur essendo registrati, non vengono rilevati da tale sistema. Analogo strumento è in dotazione anche a Sogei S.p.a.

Sulla base delle risultanze ispettive, è possibile rilevare tuttavia che l'Agenzia delle entrate non ha predisposto idonee procedure di audit anche periodiche sugli enti esterni.

Con particolare riferimento alle web application (Siatel e Puntofisco), non risultano monitorati l'attività degli amministratori locali, il numero di utenze abilitate da questi ultimi, i profili di autorizzazione e gli accessi; ciò, sebbene, per quanto riguarda Siatel, siano disponibili gli strumenti applicativi di gestione delle utenze (in uso alla Direzione centrale e alle direzioni regionali competenti) e il predetto sistema Vermont.

L'applicativo di business intelligence Vermont utilizzato dall'Agenzia non registra, in particolare, le interrogazioni effettuate dagli utenti attraverso Puntofisco e i web service.

Non risultano allo stato strumenti di controllo idonei a monitorare gli accessi effettuati attraverso l'applicativo 3270 enti esterni, web service e file transfer.

Dagli atti emerge che gli amministratori locali degli enti esterni che accedono all'anagrafe tributaria non hanno effettuato i necessari controlli, anche periodici, sugli accessi e sulla sussistenza dei requisiti per le abilitazioni e le autorizzazioni degli utenti, anche per l'assenza di idonei strumenti a ciò finalizzati; tali soggetti, oltre alle anomalie relative alla gestione degli utenti riscontrate nei punti precedenti, non sono dotati di un sistema di alert o di un "cruscotto" che consenta loro di monitorare a livello statistico gli accessi all'anagrafe tributaria da parte degli utenti dell'ente. Peraltro, in taluni enti sono presenti più amministratori la cui attività non è risultata essere coordinata.

Prescrizioni

L'Agenzia deve predisporre idonee e concrete procedure di audit anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. in qualità di responsabile del trattamento. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di audit basate sul monitoraggio delle transazioni e su sistemi di alert, tali procedure devono prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso.

Negli strumenti di business intelligence (applicativo Vermont o altri analoghi) utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria dovranno confluire i log relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni.

Deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici alert che individuino com-

portamenti anomali o a rischio, anche attrav erso il monitoraggio e l ’analisi periodica, a liv ello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni.

Gli amministratori locali pr esso gli enti esterni dev ono essere dotati di str umenti di gestione delle utenze più efficaci e intuitivi che pr evedano anche la possibilità di monitoraggi statistici degli accessi con l’attivazione di sistemi di alert. Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l’accesso all’anagrafe tributaria. Tali controlli devono riguardare in particolare, anche a campione, la rispondenza delle interr ogazioni a una precisa finalità amministrativa (cfr. l’inserimento del numero di pratica nell’applicativo), e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l ’Agenzia.

***

Le prescrizioni sopra illustrate devono essere predisposte al più presto. Anche sulla base del confronto con l’Agenzia -curato da ultimo dall ’Ufficio- rispetto all’impiego delle risorse necessarie per la lor o idonea attuazione e tenuto conto del rispetto dei diritti degli inter essati, si ritiene necessario che le misure e gli accorgimenti sopra indicati, valutati singolarmente e nel loro complesso, siano accorpati in due distinti gruppi di adempimenti che dovranno essere posti in essere dall’Agenzia entro i termini, rispettivamente, di tre e di sei mesi. Limitatamente a taluni specifici e limitati pr ofili, considerata la par ticolare complessità organizzativa richiesta, alcune delle misure e degli accorgimenti indicati dev ono essere invece completati entr o il temine di dodici mesi. L’adempimento di tutte le prescrizioni del Garante dovrà essere, di volta in volta, puntualmente documentato a questa Autorità nei termini indicati decorrenti dalla data di ricezione del presente provvedimento.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell’art. 154, comma 1, lett. c) del Codice pr escrive all’Agenzia delle entrate, con particolare riferimento alle attività dei soggetti esterni che accedono all ’anagrafe tributaria, di adottare al più presto le misure e gli accorgimenti seguenti al fine di porr e rimedio alle carenze indicate in motivazione, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell’Agenzia e alle estese possibilità di accesso alle banche dati, r endendo il trattamento conforme alle disposizioni vigenti e pr ovve-

dendo comunque entr o, e non oltr e, i distinti termini di v olta in v olta indicati. L'adempimento delle pr escrizioni dovrà essere, di v olta in v olta, documentato puntualmente a questa A utorità nei medesimi termini indicati decorr enti dalla data di rice zione del presente provvedimento.

a) Con riferimento ai profili generali relativi agli accessi all'anagrafe tributaria da parte di soggetti esterni all'amministrazione finanziaria:

I) entro 6 mesi:

- l'Agenzia dev e r edigere con formalità descrittiv e standar d un documento, costantemente aggiornato, che ripor ti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattiv o, batch o di altro genere, specificando per ciascun flusso o accesso l 'identità dei soggetti legittimati a r ealizzarlo, la base normativ a, la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la fr equenza e il volume dei trasferimenti o degli accessi e il numer o di soggetti che utilizzano la pr ocedura. Tale documento dev e esser e mantenuto costantemente aggiornato, e reso disponibile nel caso di contr olli;
- con cadenza periodica annuale, l 'Agenzia deve verificare l'attualità delle finalità per cui ha concesso l 'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi effettuati al di fuori dei pr esupposti riconducibili all'art. 19 del Codice e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscer e informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti;

II) entro 12 mesi:

- l'Agenzia deve introdurre nelle applicazioni v olte all'uso interattivo da par te di incaricati un campo per l 'indicazione obbligatoria del numer o di riferimento della pratica nell'ambito della quale viene effettuata la consultazione;
- devono essere segmentati per quanto più possibile i dati visualizzabili attraverso gli applicativi (in modo cr onologico, geografico e per tipologia di dati).

b) In relazione alla sicurezza dei sistemi di autenticazione degli applicativi utilizzati, l'Agenzia delle entrate deve:

I) entro 3 mesi:

- prevedere che tutte le applicazioni accessibili da rete pubblica in forma di web application siano implementate con protocolli https/ssl provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale;
- permettere la visualizzazione, nella prima schermata successiva al collegamento, di informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Le stesse informazioni devono essere riportate anche relativamente alla sessione corrente;
- disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali, limitandone l'utilizzo ai soli casi necessari per esigenze di servizio. In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti. Nel caso in cui non sia possibile individuare la postazione di lavoro, la possibilità di accessi contemporanei deve essere inibita;

II) entro 6 mesi:

- provvedere all'implementazione di un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

c) Per quanto riguarda gli amministratori locali, le abilitazioni e le autorizzazioni degli utenti occorre che:

I) entro 3 mesi:

- nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria sia previsto che gli enti esterni individuino gli " amministratori locali" sulla base di ele-

vati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze;

- l'Agenzia stabilisca nelle convenzioni che gli enti esterni debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei software. Le convenzioni, entro i medesimi termini, devono imporre agli enti, anche attraverso gli strumenti di audit in uso all'amministratore locale, controlli periodici i cui esiti devono essere documentati secondo le modalità definite nella stessa convenzione;
- le convenzioni stipulate dall'Agenzia predefiniscano una procedura per le autenticazioni e le autorizzazioni che coinvolga attivamente le figure apicali degli uffici interessati e un supervisore unico (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'amministratore locale e l'articolazione che si occupa della gestione delle risorse umane al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente, anche con apposite verifiche a cadenza almeno trimestrale;
- in presenza di più amministratori locali per ciascun ente, l'Agenzia valuti e coordini i profili di autorizzazione da attribuire, garantendo in capo a un'unica figura la possibilità di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato;

- l'Agenzia predefinisca, soglie relative al numero di utenti abilitabili da ciascun ente. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia;
- siano previste limitazioni orarie per gli accessi, mantenendo comunque la possibilità di specifiche deroghe adeguatamente motivate;

II) entro 6 mesi:

- le web application predisposte dall'Agenzia per l'utilizzo da parte di enti esterni siano integrate, con procedure di "autenticazione forte" per ridurre la possibilità di usi impropri delle credenziali. Tali procedure devono essere prefigurate nei confronti di quelle classi di utenti cui corrispondano profili di autorizzazione che risultano più critici e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale;
- le convenzioni stipulate con ciascun ente prevedano espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e stabiliscano anche le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

d) Con riguardo ai singoli sistemi l'Agenzia deve:

I) entro 3 mesi:

- rispetto all'applicativo Siatel, introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo e, con riferimento alle funzionalità utilizzabili da parte degli operatori comunali a soli fini anagrafici, inserire nell'applicativo medesimo specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune;
- per quanto riguarda l'applicativo Puntofisco, aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa. All'interno della procedura informatica di gestione degli utenti in uso all'amministratore locale devono essere inserite indicazioni che consentano

all'Agenzia di visualizzare lo status di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Entro il medesimo termine, deve essere corretta l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema;

- per quanto riguarda gli applicativi Entratel e Fisconline/Cassetto fiscale, configurare i sistemi in modo da poter verificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, con particolare riferimento al sistema di scadenza delle password e all'attribuzione di credenziali idonee a identificare direttamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l'accesso, autentica e trasmette i file;

II) entro 6 mesi:

- realizzare la migrazione degli enti a oggi abilitati ad accedere all'anagrafe tributaria mediante 3270 enti esterni verso applicativi che offrono maggiori garanzie;
- con riferimento ai web service, effettuare una ricognizione dei servizi attualmente esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le misure e gli accorgimenti di seguito descritti. Laddove l'Agenzia intenda impiegare web service esposti anche in rete pubblica per l'utilizzo da parte di enti esterni, questi devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo booleano. Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei web service devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati per-

sonali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il timestamp, l'indirizzo Ip di provenienza dell'utente e del server interconnesso, l'operazione effettuata e i dati trattati;

III) entro 12 mesi:

- realizzare i collegamenti per la gestione di flussi di dati mediante file transfer su canali di connessione sicuri e garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

e) In relazione alle procedure di audit sull'accesso alle informazioni contenute nell'anagrafe tributaria da parte di soggetti esterni:

I) entro 3 mesi:

- l'Agenzia deve predisporre idonee e concrete procedure di audit anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di audit basate sul monitoraggio delle transazioni e su sistemi di alert, tali procedure devono prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso;

II) entro 6 mesi:

- negli strumenti di business intelligence utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria devono confluire i log relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni;
- deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici alert che individuino comportamenti anomali o a rischio, anche attraverso il monitoraggio e l'analisi periodica, a livello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni;

- gli amministratori locali presso gli enti esterni devono essere dotati di strumenti di gestione delle utenze più efficaci e intuitivi che prevedano anche la possibilità di monitoraggi statistici degli accessi con l'attivazione di sistemi di alert. Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l'accesso all'anagrafe tributaria. Tali controlli devono riguardare, in particolare, anche a campione la rispondenza delle interrogazioni ad una precisa finalità amministrativa e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l'Agenzia.

Roma, 18 settembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

29. Archivi storici *on-line* dei quotidiani: accoglimento dell'opposizione dell'interessato alla reperibilità delle proprie generalità attraverso i motori di ricerca (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

Visti gli interpelli preventivi ex artt. 7 e 8 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, 196) inviati a Google Inc. e Rcs Quotidiani S.p.A. con i quali XY, in relazione alla pubblicazione nella sezione del sito Internet dedicata all'archivio storico del quotidiano "Il Corriere della Sera" di un articolo del KW dal titolo "WZ", che contiene dati personali che lo riguardano e che è attualmente reperibile anche mediante il motore di ricerca "www.google.it", ha chiesto "di mettere in atto ogni più opportuno accorgimento (cancellazione della notizia oppure trasformazione della stessa in forma anonima oppure blocco elettronico della stessa) affinché chiunque, via internet, faccia una ricerca nominativa" relativa alla sua persona, attraverso il motore di ricerca, non acceda direttamente ai dati personali che lo riguardano contenuti nel citato articolo;

Visto il ricorso presentato il 21 luglio 2008 nei confronti di Google Inc. e di Rcs Quotidiani S.p.A., in qualità di editore del sito Internet "www.corriere.it", con il quale XY, non avendo ricevuto un idoneo riscontro, ha ribadito le precedenti richieste rilevando che, a suo avviso, la riproposizione on-line, a QJ anni di distanza, dell'articolo in questione –nel quale si narra del suo arresto nell'ambito di un'ampia inchiesta giudiziaria relativa a episodi di concussione e corruzione in ambito militare– sarebbe illecita, non rispondendo più "ai requisiti di attualità, essenzialità ed interesse pubblico" e sarebbe "in contrasto con il cd. diritto all'oblìo"; tale riproposizione sarebbe inoltre lesiva della sua reputazione e dignità, non tenendosi conto del fatto che "dalla vicenda de qua ad oggi sono trascorsi ben QJ anni durante i quali il ricorrente si è ricostruito una nuova vita" e che l'articolo "riflette un'immagine del ricorrente non più corrispon-

(*) [doc. *web* n. 1583162]

dente con il suo attuale modo di esser e e ne mette a rischio la pr esente e rinnovata dimensione sociale"; rilevato che, con il ricorso, il ricorrente ha chiesto anche di porre a carico delle controparti le spese sostenute per il pr ocedimento;

Visti gli ulteriori atti d 'ufficio e, in par ticolare, la nota del 28 luglio 2008 con la quale questa Autorità, ai sensi dell'art. 149 del Codice, ha invitato il titolare del trattamento a fornire riscontro alle richieste dell 'interessato, nonché la nota del 3 no vembre 2008 con la quale questa Autorità ha disposto la pr oroga del termine per la decisione sul ricorso ai sensi dell 'art. 149, comma 7, del Codice;

Vista la memoria datata 16 settembr e 2008 con la quale G oogle Inc. (rappr esentata e difesa dagli avv.ti Marco Berliri e Massimiliano Masnada), nel richiamare un riscontro fornito al ricorrente prima della pr esentazione del ricorso e dopo av er eccepito la sua inammissibilità poiché "al trattamento di dati personali per me zzo di copie cache con cui G oogle mette a disposizione degli utenti le pagine w eb indicizzate contenenti par ole chiav e utilizzate nella ricer ca, non si applica la legge italiana", avendo il titolar e del trattamento sede negli U sa, ha comunque illustrato le modalità di funzionamento del sistema di scansione utilizzato da G oogle; rilevato che la società ha precisato che è possibile escludere pagine web di siti sorgente ancora disponibili in rete dall'indicizzazione automaticamente operata dai propri crawler esclusivamente con la collaborazione dei w ebmaster dei medesimi siti sorgente e che, quindi, " nel caso specifico, solo rimuovendo dall'archivio storico del sito www.corriere.it la pagina web cui" il ricorrente "fa riferimento o inser endo un codice (r obot.txt) che impedisca al crawler di G oogle di sele zionare automaticamente la pagina, potrà esser e definitivamente impedita l'indicizzazione della stessa da parte di Google";

Viste le memorie del 17 e del 22 settembr e 2008 con le quali Rcs Quotidiani S.p.A. ha negato di poter dar corso alle richieste del ricorr ente, sostenendo che il trattamento effettuato è lecito; secondo la r esistente, la richiesta di cancellazione dei dati non può esser e accolta facendo riferimento a un articolo (che peraltro "riferiva di fatti veri") contenuto nell'archivio storico del quotidiano che, " per assolv ere alla sua funzione, dev e contener e tutti gli ar ticoli pubblicati su tutte le edizioni" e non potrebbe subire alcuna "amputazione" a pena di perdere tale carattere di storicità e di complete zza; il trattamento sarebbe lecito anche per ché è effet-

tuato, allo stato, non per finalità giornalistiche (come all'atto della sua pubblicazione o nel caso di una "nuova pubblicazione" nell'ambito di una "nuova iniziativa giornalistica"), ma "a fini documentaristici, nell'ambito di un archivio reso liberamente consultabile con lo strumento più rapido ed agevole, la rete internet, e attraverso i meccanismi di recupero del dato più diffusi, i motori di ricerca" e nel rispetto peraltro delle specifiche disposizioni poste con riferimento al trattamento di dati effettuato per scopi storici; sempre ad avviso della resistente, il trattamento non sarebbe altresì lesivo tenuto conto che "la particolarità della fonte, cioè la collezione dei numeri del periodico già pubblicati, rende immediatamente evidente a chiunque giunga alla notizia, la data della sua pubblicazione sul quotidiano, fugando ogni dubbio sul fatto che si tratta di vicenda passata, più o meno remota. L'utente, inoltre, può autonomamente comprenderne la eventuale inattualità, apprezzandone invece il valore di documento storico, con le sue potenzialità, ma anche i suoi limiti, in termini di informazione"; rilevato che, con riferimento al caso di specie, la resistente ha altresì considerato che l'articolo oggetto del ricorso fa riferimento a un fatto "dotato di rilevante interesse pubblico; interesse che non è affatto detto che sia oggi del tutto scemato" e contiene comunque dati che non "appartengono esclusivamente alla vita privata dell'interessato", quale la circostanza del suo arresto;

Vista la nota datata 17 settembre 2008 con la quale il ricorrente ha ribadito le proprie richieste rilevando che se è vero che "l'archivio storico della R.c.s. deve conservare memoria delle notizie accadute nel tempo", sarebbe altresì necessario che "dopo un congruo periodo di tempo (…) la pagina, al limite" possa essere "accessibile solo dall'indirizzo principale (appunto www.corriere.it) e non dai singoli motori di ricerca";

Vista la nota fatta pervenire via fax il 17 novembre 2008 con la quale R.c.s. Quotidiani S.p.A. ha richiamato le precedenti argomentazioni e, in ordine alle considerazioni del ricorrente relative all'accessibilità dell'articolo per il tramite del motore di ricerca, ha rilevato che "la legittimità della conservazione del dato e della sua libera fruizione (…) non può che implicare necessariamente la possibilità di porre al servizio della ricerca tutti i mezzi che la tecnica informatica permette di utilizzare"; ciò, a maggior ragione quando il dato in questione è contenuto nell'"archivio storico documentaristico del Corriere della Sera";

Vista la memoria del 17 novembre 2008 con la quale Google Inc. ha ribadito di ritenere inammissibile il ricorso proposto nei propri confronti, precisando che l'attività di trattamento posta in essere dalla società è "interamente gestita attraverso i suoi server che (…) sono localizzati presso la sede del titolare in Usa", e ha ulteriormente illustrato le modalità di funzionamento del proprio motore di ricerca;

Ritenuta di dover dichiarare inammissibile il ricorso proposto nei confronti di Google Inc. dal momento che la società resistente non risulta stabilita nel territorio di un paese appartenente all'Unione europea e che la stessa ha dichiarato di effettuare il trattamento dei dati esclusivamente attraverso i server localizzati in tale paese terzo (cfr. art. 5, commi 1 e 2, del Codice);

Rilevato, in ordine al merito del ricorso proposto nei confronti di Rcs Quotidiani S.p.A., che, al fine di contemperare i diritti della persona (in particolare il diritto alla riservatezza) con la libertà di manifestazione del pensiero –e con essa anche l'esercizio della libera ricerca storica e del diritto allo studio e all'informazione–, la disciplina in materia di protezione dei dati personali prevede specifiche garanzie e cautele nel caso di trattamenti effettuati per tali finalità, confermando la loro liceità, anche laddove si svolgano senza il consenso degli interessati, purché avvengano nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati (cfr. artt. 136 e s. e art. 102, comma 2, lett. a), del Codice, nonché artt. 1, comma 1, e 3, comma 1, codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, pubblicato in G. U. 5 aprile 2001, n. 80);

Rilevato che il trattamento dei dati personali del ricorrente cui fa riferimento l'odierno ricorso, a suo tempo effettuato in modo lecito per finalità giornalistiche nel rispetto del principio dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico, rientra ora, attraverso la riproposizione dei medesimi dati nell'articolo pubblicato quale parte integrante dell'archivio storico del quotidiano reso disponibile on-line sul sito Internet dell'editore resistente, tra i trattamenti effettuati al fine di concretizzare e favorire la libera manifestazione del pensiero e, in particolare, la libertà di ricerca, cronaca e critica storica; rilevato che, alla luce di ciò, l'attuale trattamento può essere effettuato senza il consenso degli interessati (cfr. art. 136 e s. del Codice), è compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati e può essere effettuato in termini generali anche oltre il periodo di tempo necessario per conse-

guire tali diversi scopi (cfr. art. 99 del Codice);

Rilevato che, ai sensi dell'art. 7, comma 3, lett. b), del Codice, ogni interessato ha diritto di chiedere la cancellazione o la trasformazione in forma anonima o il blocco dei dati personali che lo riguardano qualora gli stessi siano trattati in violazione di legge, ovvero nel caso in cui la loro conservazione non sia necessaria in relazione agli scopi per i quali sono stati raccolti o successivamente trattati;

Rilevato che, nel caso in esame, alla luce delle citate disposizioni normative, il trattamento di dati personali relativi all'interessato effettuato mediante la riproposizione on-line, sul sito Internet dell'editore resistente, dell'articolo che li contiene quale parte integrante dell'archivio storico del quotidiano non risulta in termini generali illecito, essendo riferito ad una notizia relativa a un fatto vero, non contestato dalle parti e di interesse pubblico e ciò, tanto al tempo della sua iniziale pubblicazione sull'edizione cartacea del quotidiano, quanto attualmente, soprattuto per chi opera una ricerca relativa alle vicende giudiziarie in questione; ritenuto pertanto di dover dichiarare, nel caso di specie, stante anche la liceità dell'originaria pubblicazione, infondata la richiesta del ricorrente volta a ottenere la cancellazione o la trasformazione in forma anonima o il blocco dei dati personali che lo riguardano contenuti nel citato articolo;

Rilevato tuttavia che vanno separatamente considerati i motivi legittimi di opposizione sostanzialmente argomentati dall'interessato, il quale ha rappresentato legittimamente la propria aspirazione affinché sulla rete Internet, per mezzo delle "scansioni" operate automaticamente dai motori di ricerca esterni al sito dell'editore resistente, non resti associata perennemente al proprio nominativo la notizia oggetto dell'articolo pubblicato sul Corriere della sera nel KW; ciò pur nell'ipotesi che la stessa permanga nell'archivio storico conservato e diffuso dall'editore resistente mediante il proprio sito Internet e quindi possa essere rinvenuta da coloro che la cerchino direttamente nell'archivio del giornale mediante il motore di ricerca interno a tale sito, avendone magari una pur vaga conoscenza;

Ritenuto che tali motivi di opposizione appaiono meritevoli di tutela, tenuto conto delle peculiarità del funzionamento della rete Internet che può comportare la diffusione di un gran numero di dati personali riferiti a un medesimo interessato e relativi a vicende anche risalenti

nel tempo –e dalle quali gli interessati stessi hanno cercato di allontanarsi, intraprendendo nuovi percorsi di vita personale e sociale– che però, per mezzo della rappresentazione istantanea e comulativa derivante dai risultati delle ricerche operate mediante i motori di ricerca, rischiano di riverberare comunque per un tempo indeterminato i propri effetti sugli interessati come se tali vicende fossero sempre attuali; ciò, tanto più considerando che il successivo utilizzo degli esiti delle ricerche effettuate sulla rete Internet mediante i motori di ricerca può avvenire per le finalità più diverse e non sempre per finalità di ricerca storica in senso proprio;

Ritenuto che, tenuto anche conto del tempo trascorso dalla vicenda oggetto dell'articolo cui si riferisce l'odierno ricorso, una per enne associazione al ricorrente della stessa, nei termini predetti, comporta un sacrificio sproporzionato dei suoi diritti (cfr. art. 2, comma 1, del Codice); ritenuto pertanto di dover dichiarare, nel caso di specie, parzialmente fondato il ricorso e di dover indicare, quale misura a tutela dei diritti dell'interessato, che la pagina web che contiene i dati personali del ricorrente oggetto del ricorso sia tecnicamente sottratta, all'atto della ricerca del nominativo del ricorrente, alla diretta individuabilità tramite i più diffusi motori di ricerca esterni, pur restando inalterata nel contesto dell'archivio consultabile telematicamente accedendo all'indirizzo web dell'editore resistente;

Rilevato che, alla luce dell'attuale meccanismo di funzionamento dei motori di ricerca standard, intendendo con ciò quelli a maggiore diffusione, la raccolta delle informazioni sulle pagine disponibili nel world wide web (fase di grabbing) è influenzabile dal solo amministratore di un sito web sorgente per il tramite della compilazione del file robots.txt, previsto dal "Robots Exclusion Protocol", o tramite l'uso dei "Robots Meta tag", secondo convenzioni concordate nella comunità Internet (avendo presente comunque come tali accorgimenti non siano immediatamente efficaci rispetto a contenuti già indicizzati da parte dei motori di ricerca Internet, la cui rimozione potrà avvenire secondo le modalità da ciascuno di questi previste);

Rilevato comunque che l'Autorità si riserva di avviare sul tema un eventuale autonomo procedimento nell'ambito del quale, anche attraverso il coinvolgimento delle istituzioni e dei soggetti allo stesso interessati (ordine dei giornalisti, associazioni rappresentative degli editori, gestori di motori di ricerca, ecc.), potranno essere valutate le molteplici implicazioni che la diffusione mediante la rete Internet di vasti archivi contenenti dati personali, seppur lecita e

di indiscusso interesse e valore, comporta per i soggetti cui gli stessi si riferiscono e per i loro diritti;

Ritenuto allo stato di dover ordinare, ai sensi dell'art. 150, comma 2, del Codice, a R.c.s. quotidiani S.p.A. di adottare, entro il termine di sessanta giorni dalla data di ricezione del presente provvedimento, ogni misura tecnicamente idonea ad evitare che le generalità del ricorrente contenute nell'articolo oggetto del ricorso siano rinvenibili direttamente attraverso l'utilizzo dei comuni motori di ricerca esterni al proprio sito Internet (anche, ad esempio, mediante predisposizione di distinte versioni o di differenti modalità di presentazione delle pagine web interessate a seconda dello strumento di ricerca utilizzato dagli utenti –motori di ricerca Internet o funzioni di ricerca interne al sito– o con modalità che l'Autorità si riserva, ove del caso, di valutare ai sensi dell'art. 150, comma 5, del Codice) e di dare conferma dell'avvenuto adempimento al ricorrente e a questa Autorità entro il medesimo termine;

Ritenuto che sussistono giusti motivi per compensare le spese tra le parti;

Visti gli artt. 145 e s. del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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

Relatore il dott. Giuseppe Chiaravalloti;

TUTTO CIÒ PREMESSO IL GARANTE

a) dichiara inammissibile il ricorso proposto nei confronti di Google Inc.;

b) dichiara infondate le richieste del ricorrente volte a ottenere la cancellazione o la trasformazione in forma anonima o il blocco dei dati personali che lo riguardano contenuti nell'articolo oggetto del ricorso;

c) dichiara parzialmente fondato il ricorso in ordine all'opposizione manifestata dal ricorrente e ordina, quale misura a tutela dell'interessato ai sensi dell'art. 150, comma 2, del Codice, a R.c.s. quotidiani S.p.A. di adottare, entro il termine di sessanta giorni dalla data di ricezione del presente provvedimento, ogni misura tecnicamente idonea ad evitare che i dati personali del ricorrente contenuti nell'articolo oggetto del ricorso siano rinvenibili direttamente attraverso l'utilizzo dei comuni motori di ricerca esterni al proprio sito

Internet e di dare conferma dell'avvenuto adempimento al ricorrente e a questa Autorità entro il medesimo termine;

d) dichiara compensate le spese tra le parti.

Roma, 11 dicembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

30. Prescrizioni ai titolari di banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 a seguito della deroga introdotta dall'art. 44 d.l. n. 207/2008 (*)

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 cons. Filippo Patroni Griffi, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

Visto l'art. 129, comma 2, del Codice che, in attuazione della disciplina comunitaria e, in particolare, della direttiva 2002/58/Ce, ha individuato nella " mera ricerca dell'abbonato per comunicazioni interpersonali" la finalità primaria degli elenchi telefonici realizzati in qualunque forma;

Considerato che tale disposizione ribadisce che il trattamento dei dati inseriti negli elenchi, se realizzato per fini ulteriori tra cui rientrano quelli pubblicitari, promozionali o commerciali, è lecito solo se è effettuato con il consenso espresso liberamente e specificamente dagli interessati, documentato per iscritto e previa informativa;

Visto il provvedimento del 15 luglio 2004 (in www.garanteprivacy.it, doc. web n. 1032381) con il quale l'Autorità ha individuato le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati e agli acquirenti del traffico prepagato negli elenchi telefonici "alfabetici" del servizio universale, realizzati in qualsiasi forma, in rapporto alle diverse finalità sopraindicate, anche in rapporto all'informativa;

Visto il provvedimento del 14 luglio 2005 (in www.garanteprivacy.it, doc. web n. 1151640) con il quale l'Autorità ha individuato procedure semplificate per la redazione e l'utilizzo degli elenchi organizzati per categorie merceologiche/professionali (cd. elenchi "categorici");

Rilevato che la disciplina in materia di protezione dei dati personali prevede la possibilità di utilizzare, per attività di carattere promozionale, pubblicitario o commerciale, alcune categorie di dati e, in particolare: a) quelli presenti negli elenchi cd. " alfabetici" per i quali l'interessato ha

(*) Gazzetta Ufficiale 20 marzo 2009, n. 66 [doc. *web* n. 1598808], in inglese [doc. *web* n. 1613568]

manifestato il proprio consenso (Provv. 15 luglio 2004 cit.); b) quelli presenti negli elenchi cd. "categorici" (Provv. 14 luglio 2005 cit.); c) quelli presenti nelle banche dati costituite utilizzando anche dati estratti da elenchi telefonici formati precedentemente al 1° agosto 2005, sempre che il titolare del trattamento sia in grado di dimostrare di aver fornito effettivamente, prima di tale data, l'informativa agli interessati ai sensi dell'art. 13 del Codice;

Rilevato che resta impregiudicato quanto previsto dall'art. 130 del Codice riguardo alle attività promozionali effettuate attraverso sistemi automatizzati di chiamata senza l'intervento di un operatore, per le quali è sempre necessario il consenso espresso dell'interessato;

Visto l'art. 44, comma 1-*bis* del decreto legge 30 dicembre 2008, n. 207, convertito, con modificazioni, nella legge 27 febbraio 2009, n. 14 (in G.U. n. 28L del 28 febbraio 2009), che ha stabilito che i dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del Codice, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005;

Considerato che la predetta previsione ha introdotto una deroga temporanea ai principi generali della vigente disciplina sopra richiamata che, in quanto tale, cessa alla scadenza del 31 dicembre 2009 e non istituisce, invece, un regime speciale applicabile anche successivamente a tale data;

Considerato che la deroga in questione è subordinata al contemporaneo verificarsi di due condizioni, ossia che le banche dati siano state costituite prima del 1° agosto 2005 e che i dati in esse presenti vengano utilizzati per finalità promozionali esclusivamente dagli stessi titolari che le hanno a suo tempo costituite;

Considerato che la stessa deroga ha posto quindi un vincolo di finalità e un vincolo di carattere temporale nell'utilizzo delle predette banche dati, rappresentato dallo svolgimento di attività di carattere promozionale sino al 31 dicembre 2009 e che, quindi, i dati personali presenti nelle predette banche dati non possono essere utilizzati, in vigenza del regime derogatorio, per finalità ulteriori e al di fuori dell'ambito temporale di operatività della deroga;

Ritenuto, pertanto, che rendere una informativa e acquisire un consenso, nel predetto periodo, finalizzati alla costituzione di una banca dati da utilizzare per attività promozionali anche in data

successiva al 31 dicembre 2009, costituisce una attività ulteriore rispetto ai vincoli di finalità e di ordine temporale indicati nella norma derogatoria e transitoria;

Considerato, inoltre, che l'informativa, ove resa agli interessati nel corso del predetto periodo, non renderebbe lecita la costituzione di una banca dati utilizzabile per attività di carattere promozionale, come avveniva anteriormente al 1° agosto 2005;

Considerato, poi, in ragione del predetto vincolo di finalità introdotto per il periodo transitorio, che il consenso, anche laddove fosse acquisito in vigenza della deroga, non rileverebbe in alcun modo per lo svolgimento di attività promozionali o per lo svolgimento di altre attività per le quali è necessario acquisirlo, anche in data successiva al 31 dicembre 2009;

Considerato, dunque, che una banca dati potrebbe essere utilizzata per attività promozionali, successivamente al 31 dicembre 2009, solo se formata nel rispetto della disciplina ordinaria, atteso che la disciplina derogatoria e transitoria cessa alla predetta data e, come già rilevato, costituisce una deroga di carattere temporaneo alla disciplina generale e non istituisce un regime speciale applicabile anche successivamente alla scadenza indicata;

Considerato inoltre che, in ragione di quanto detto, i dati personali presenti nelle banche dati considerate dalla norma derogatoria e transitoria, non possono essere ceduti, a qualunque titolo, a terzi;

Considerato che, in relazione all'attuale utilizzo delle predette banche dati per finalità promozionali, resta comunque impregiudicata la disciplina generale prevista dal Codice e, in particolare, quella relativa ai diritti degli interessati; e che, pertanto, le predette banche dati non possono contenere i dati degli interessati che, nel corso del tempo, abbiano esercitato il diritto di opposizione ai sensi dell'art. 7 del Codice;

Ritenuta la necessità di prescrivere ai titolari del trattamento, ai sensi dell'art. 143, comma 1, lett. b) e art. 154, comma 1, lett. c) del Codice, le misure necessarie per rendere il trattamento conforme alle disposizioni vigenti, anche in considerazione delle recenti modifiche normative;

Tenuto conto che, ai sensi dell'art. 162, comma 2-*ter* del Codice, in caso di inosservanza del presente provvedimento prescrittivo, è applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro;

Tenuto conto, inoltre, che, ai sensi dell'art. 164-bis, comma 2, del Codice, in caso di più viola-

zioni di un'unica o di più disposizioni relative a violazioni amministrative, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da cinquantamila euro a trecentomila euro;

Tenuto conto, infine, che ai sensi dell'art. 168 del Codice, chiunque, in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni;

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 del 28 giugno 2000;

Relatore il prof. Francesco Pizzetti;

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, prescrive a tutti i titolari del trattamento che siano in possesso di banche dati costituite sulla base di elenchi telefonici pubblici formati prima del 1° agosto 2005 e che intendano utilizzarle per fini promozionali avvalendosi della deroga introdotta dalla legge 27 febbraio 2009, n. 14, le seguenti misure necessarie per rendere il trattamento conforme alle disposizioni vigenti:

a) documentare in modo adeguato l'avvenuta costituzione della banca dati prima del 1° agosto 2005 e conservare la relativa documentazione presso la sede legale del titolare;

b) trattare direttamente i dati personali presenti nelle banche dati oggetto del presente provvedimento, senza possibilità di cederli, a qualunque titolo, a terzi;

c) specificare, in occasione di ogni contatto con gli interessati, chi rivesta la qualifica di titolare del trattamento dei dati, anche nel caso in cui questi operi per conto di terzi e fare presente agli interessati stessi che hanno il diritto di opporsi ai sensi dell'art. 7 del Codice;

d) registrare in via immediata l'eventuale opposizione dell'interessato al trattamento dei suoi dati personali effettuato dal titolare (art. 7, comma 4, del Codice), con effetto anche nei confronti dei terzi per conto dei quali questo operi, anche qualora ciò

avvenga telefonicamente, e fornire altresì all'interessato l'identificativo dell'operatore o dell'operazione compiuta;

e) utilizzare i dati personali presenti nelle banche dati di cui alla lett. a) esclusivamente per finalità promozionali e sino al 31 dicembre 2009, non potendo i titolari rendere un'informativa agli interessati e richiedere agli stessi un consenso per l'uso dei loro dati per attività di carattere promozionale da effettuare in data successiva al 31 dicembre 2009;

f) comunicare al Garante, entro quindici giorni dalla pubblicazione in Gazzetta Ufficiale del presente provvedimento, di essere in possesso di banche dati costituite anteriormente al 1° agosto 2005 che si intendono utilizzare per attività promozionali fino al 31 dicembre 2009, chiarendo se il trattamento dei dati personali venga effettuato anche per conto di terzi.

Si dispone la trasmissione di copia del presente provvedimento al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 12 marzo 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Patroni Griffi

31. Trasporto pubblico: geolocalizzazione e sicurezza dei passeggeri (*)

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;

Esaminata la richiesta di verifica preliminare presentata da Air Pullman S.p.A. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visti gli atti d'ufficio;

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

Relatore il dott. Mauro Paissan;

PREMESSO

1. TRATTAMENTO DI DATI MEDIANTE SISTEMI DI LOCALIZZAZIONE SATELLITARE E DI SISTEMI DI REGISTRAZIONE DI EVENTI DI GUIDA

1.1. Air Pullman S.p.A., società che gestisce linee di trasporto pubblico, ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati personali dei conducenti dei veicoli in dotazione –nonché di quelli a disposizione delle società controllate "Air Pullman Noleggi s.r.l." e "Saco s.r.l."– conseguente all'utilizzo di un sistema satellitare di localizzazione basato su tecnologia Gps (Global Positioning System). Tale sistema, comprensivo della gestione di una banca dati e del portale messi a disposizione della società di trasporto, verrebbe fornito da Digigroup s.r.l. (di seguito, denominata "fornitore del servizio").

Unitamente ai trattamenti effettuati mediante il sistema, la cui installazione è presupposto per partecipare a gare relative all'affidamento di servizi di trasporto pubblico locale, verrebbero trattate, con l'ausilio del fornitore del servizio, ulteriori informazioni relative allo "stile di guida" del conducente e ad alcuni parametri (quali la pressione nei serbatoi freni a inizio e fine frenata e la velocità del veicolo, anche durante la frenata) rilevati in occasione di eventuali sinistri mediante

(*) [doc. *web* n. 1531604]

un dispositivo di registrazione e trasmissione dei dati ("event data recorder", denominato dalla società "black box").

Nel complesso, la società sarebbe in grado di:

a) localizzare geograficamente i propri veicoli su una mappa cartografica e di conoscerne velocità e direzione;

b) verificare l'osservanza, da parte dei conducenti, della normativa in tema di circolazione stradale e delle prescrizioni aziendali;

c) valutare la sicurezza e il "comfort" della condotta di guida degli autisti;

d) analizzare il consumo di carburante (e l'efficienza energetica) nella fase di marcia;

e) ricostruire la dinamica di eventuali sinistri;

f) riscontrare anomalie tecnico-meccaniche dei veicoli.

1.2. Secondo quanto prospettato dalla società, il trattamento di dati personali riferiti ai conducenti per mezzo di un codice identificativo appositamente cifrato, associati a quelli necessari per la localizzazione del veicolo (posizione in tempo reale del veicolo, data e ora di transito, velocità sostenuta e direzione percorsa), servirebbe a "garantire la sicurezza dei passeggeri e del mezzo rintracciandone sul percorso la posizione, per ogni necessità di intervento che assicuri l'espletamento del servizio a favore dei passeggeri e la possibilità di assistenza ai medesimi" (cfr. richiesta di verifica preliminare, p. 4).

Le predette informazioni, acquisite automaticamente dal sistema di bordo secondo criteri concordati previamente con il fornitore del servizio (all'accensione e allo spegnimento del veicolo; ogni cinque minuti con veicolo fermo o in movimento; ogni cinque km con veicolo in movimento; all'inizio e al termine di ogni fermata: cfr. allegato A alla menzionata richiesta), confluirebbero in una banca dati gestita dal fornitore medesimo.

Gli stessi dati, unitamente al servizio per la loro elaborazione (come, ad esempio, il tracciato del percorso effettuato), sarebbero resi fruibili all'azienda dal fornitore attraverso un portale ad accesso riservato, denominato "i-Nets" (cfr. richiesta di verifica preliminare, cit., p. 6); non verrebbero trattati, comunque, dati personali relativi ai passeggeri trasportati (cfr. richiesta di verifica preliminare, cit., p. 3).

1.3. Con riferimento alle funzionalità correlate alla sicurezza stradale e al consumo energetico,

la società intende acquisire i dati identificativi dei conducenti associati a informazioni relative alle loro "condotte di guida". Le informazioni (riferite, in particolare, ai tempi di permanenza oltre il numero massimo di giri motore consentito, al superamento delle velocità massime, al "comfort di guida" durante la marcia e in sede di frenata e al consumo energetico connesso all'utilizzo dell'acceleratore) sarebbero trattate solo in forma di indici medi e non sulla base di dati analitici.

Le medesime informazioni sarebbero utilizzate esclusivamente per finalità connesse al "rispetto delle prescrizioni normative di marcia su strada pubblica" (cfr. richiesta di verifica preliminare cit., p. 4) e alla corresponsione di trattamenti economici premianti a beneficio dei lavoratori che conformino il proprio stile di guida agli standard della società (in coerenza con la politica di incentivazione da essa portata avanti, che "formerebbe oggetto di negoziazione a livello aziendale": cfr. verbale di incontro del 31 marzo 2008). Anche le informazioni in questione confluirebbero all'interno di una banca dati fruibile dall'azienda per mezzo del portale "i-Nets".

1.4. La sicurezza dei dati personali sarebbe monitorata e implementata costantemente mediante accorgimenti tecnici atti a garantire la loro protezione (cfr. richiesta di verifica preliminare, cit., p. 9). In particolare, l'accesso al portale "i-Nets" –e, conseguentemente, a tutte le informazioni ivi contenute– verrebbe consentito esclusivamente previo inserimento di una password associata a un identificativo utente ("UserId"), in funzione del profilo di autorizzazione predefinito con il fornitore.

2. PROTEZIONE DEI DATI PERSONALI, LOCALIZZAZIONE E REGISTRAZIONE DELLA CONDOTTA DI GUIDA

Con esclusione delle funzionalità del sistema utilizzato dalla società per la telediagnostica del veicolo (punto 1.1. lett. f), in relazione al quale la società ha dichiarato che verranno trattate informazioni riconducibili non agli autisti, ma al solo veicolo: cfr. verbale di riunione, cit.), il caso sottoposto a verifica preliminare riguarda un trattamento di dati personali riferiti ai conducenti, con particolare riferimento alla localizzazione.

I dati relativi all'ubicazione dei veicoli, infatti, se associati a codici identificativi dei conducenti, costituiscono anche informazioni personali riconducibili agli interessati (art. 4, comma 1,

lett. b), del Codice). Ciò, anche nel caso in cui i dati di localizzazione del veicolo non siano associati immediatamente dal sistema informativo al nominativo dei conducenti (o a codici ad essi attribuiti), atteso che la società sarebbe comunque in condizione di risalire in ogni momento al conducente assegnatario di ciascun veicolo (cfr., in proposito, Parere n. 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto del Gruppo di lavoro ex art. 29, direttiva n. 95/46/Ce, WP115, p. 10; v. altresì Parere n. 4/2007 sul concetto di dati personali del Gruppo di lavoro ex art. 29, direttiva n. 95/46/Ce, WP136, p. 11).

Anche gli ulteriori dati trattati per il tramite del fornitore del servizio, quali quelli relativi allo "stile di guida" o registrati mediante la "black box", devono ritenersi dati personali, essendo riconducibili (anche in un secondo momento, ad esempio in occasione di sinistro) ad azioni poste in essere dai conducenti.

A tali trattamenti trova pertanto applicazione la disciplina contenuta nel Codice.

Per tutte le finalità indicate nel presente provvedimento, il trattamento dovrà quindi avvenire con modalità comunque rispettose, in concreto, dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 2, primo comma, del Codice) e dovrà essere svolto, in ogni caso, in conformità all'art. 11, comma 1, lett. a) del medesimo Codice, con le garanzie e procedure espressamente previste a tutela dei lavoratori dall'art. 4 della legge n. 300/1970.

3. RAPPORTO TRA SOCIETÀ DI TRASPORTO PUBBLICO LOCALE (TITOLARE DEL TRATTAMENTO) E FORNITORE DEL SERVIZIO

L'esternalizzazione delle attività finalizzate all'esecuzione del servizio sopra descritto, grazie a un apposito contratto di collaborazione, asseconda legittime esigenze organizzative in base alle quali la società di trasporto, "titolare del trattamento", si avvale del fornitore del servizio che viene a rivestire, ai sensi dell'art. 29 del Codice, il ruolo di "responsabile del trattamento" (in tal senso cfr. i pareri resi il 19 dicembre 1998, in www.garanteprivacy.it, doc. web n. 41941 e l'8 giugno 1999, doc. web n. 1092666).

Il fornitore del servizio, chiamato a operare in base a un apposito incarico, non gode di spazi di autonomia in ordine alle finalità perseguibili (salva la necessaria autonomia dal punto di vista tecnico per fornire il servizio richiesto), atteso che il potere decisionale in relazione alle mede-

sime finalità rimane in capo alla società di trasporto (cfr. in tal senso già il parere del 9 dicembre 1997, doc. web n. 30915; Provv. 16 febbraio 2006, doc. web n. 1242592).

Pertanto, l'accordo con la società di trasporto deve permettere di delimitare gli obiettivi da raggiungere, di orientare al loro esclusivo perseguimento le operazioni di trattamento dei dati effettuate dal fornitore del servizio e di individuare analiticamente i dati pertinenti e non eccedenti da trattare (artt. 4, comma 1, lett. g) e 29 del Codice). L'attività del fornitore del servizio deve essere vincolata dalle istruzioni impartite dal titolare, che devono a loro volta tener conto delle prescrizioni stabilite dal Garante con il presente provvedimento.

4. LICEITÀ, FINALITÀ E PERTINENZA DEL TRATTAMENTO RISPETTO ALLA LOCALIZZAZIONE

La finalità del trattamento dichiarata dalla società in relazione al funzionamento del sistema Gps risulta lecita. Il sistema di localizzazione del veicolo (e indirettamente del conducente) è preordinato a rendere più efficiente il servizio di trasporto pubblico locale (con una migliore allocazione dei mezzi in dotazione, specie in caso di sopravvenienze), consentendo di fornire un'informazione tempestiva a vantaggio della società che gestisce il servizio di trasporto (oltre che, eventualmente, dell'utenza), anche per l'eventuale attività di reportistica nei confronti dell'ente pubblico affidante e per il monitoraggio del servizio (cfr. artt. 14, comma 3, lett. f), 18, comma 3-quater, lett. a) e 19, comma 3, lett. c) d.lg. 19 novembre 1997, n. 422, Conferimento alle regioni ed agli enti locali di funzioni e compiti in materia di trasporto pubblico locale). Le informazioni verranno utilizzate anche per incrementare le condizioni di sicurezza del conducente e delle persone trasportate (cfr. nota della società del 12 marzo 2008).

Per tali finalità verranno trattati i dati relativi alla localizzazione dei veicoli, ivi compresa la loro direzione e velocità media tenuta negli intervalli spazio-temporali sopra indicati (punto 1.2.).

Risulta conforme al principio di necessità (art. 3 del Codice) l'adozione di opportuni accorgimenti al fine di non rendere conoscibile al fornitore del servizio i dati identificativi dei conducenti, attribuendo a questi ultimi, come dichiarato dalla società, codici cifrati (v. punto 1.2.).

Per quanto riguarda le predette finalità, funzionali al perseguimento di esigenze organizzative e produttive e a un incremento della sicurezza del lavoro, la società, assolti gli obblighi previsti dall'art. 4 della legge 20 maggio 1970, n. 300, potrà avvalersi del sistema di localizzazione e trat-

tare i dati personali necessari al suo funzionamento (nello stesso senso v. il decreto del Ministero del lavoro e delle politiche sociali, Direzione generale della tutela delle condizioni di lavoro, Divisione IV, 24 giugno 2004, in tema di installazione di impianti di controllo satellitare su autovetture di pronto intervento di un'impresa erogatrice di gas, nonché la risposta a una istanza di interpello del medesimo Ministero, Direzione generale per l'attività ispettiva, prot. n. 25/I/0006585 del 28 novembre 2006, in materia di localizzazione mediante computer palmari assegnati in dotazione a informatori scientifici del farmaco).

5. Liceità e finalità rispetto all'osservanza delle prescrizioni normative in materia di circolazione e alla definizione dello "stile di guida"

5.1. In termini generali, del pari lecito risulta il trattamento di dati personali riferiti agli autisti in relazione alla "condotta di guida" osservata (sintetizzata in forma di indici medi) per finalità connesse al "rispetto delle prescrizioni normative di marcia su strada pubblica" (cfr. richiesta di verifica preliminare cit., p. 4). Al riguardo, deve infatti rilevarsi che la sicurezza stradale, specie nell'ambito del trasporto professionale, costituisce per l'ordinamento un obiettivo di primaria rilevanza, come confermato dalla stessa disciplina comunitaria (ad esempio, in tema di cronotachigrafo digitale: cfr. regg. Ce nn. 3821/85, 2135/98 e 561/2006) e nazionale (si pensi alla "Carta di qualificazione del conducente", che obbliga gli esercenti a conseguire una qualificazione iniziale e a sottostare a periodici corsi di formazione: cfr. artt. 14 ss. e 20 d.lg. 21 novembre 2005, n. 286, recante Disposizioni per il riassetto normativo in materia di liberalizzazione regolata dell'esercizio dell'attività di autotrasportatore).

Nel rispetto delle specifiche disposizioni di legge in materia (in particolare, il d.lg. n. 285/1992 "Nuovo codice della strada" e successive modifiche e integrazioni), la società potrà quindi trattare le informazioni relative alle "condotte di guida" dei conducenti.

5.2. Con riguardo al trattamento delle informazioni relative alla "condotta di guida" al fine di riconoscere trattamenti economici premiali "ai lavoratori che conformino il proprio stile di guida agli standard fissati dalla società" (cfr. verbale di riunione cit.), sebbene tali dati siano ricavati mediante l'impiego di "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", non può escludersi che il controllo posto in essere sia giustificato da esigenze orga-

nizzative e produttive della società di trasporto (art. 4, secondo comma, legge n. 300/1970). Tali sono da ritenersi il risparmio derivante dal monitoraggio delle "condotte di guida" e l'eventuale utilizzo degli indici medi per riconoscere premi ai dipendenti, eventualmente in aggiunta agli elementi attualmente in uso; alla luce dell'accordo aziendale in atti, infatti, il premio di risultato è correlato alla "diminuzione di danni per sinistri interni e passivi" e "all'andamento del parametro fatturato dell'attività di linea su dipendenti medi".

La società dovrà selezionare attentamente i dati pertinenti e non eccedenti ai fini del calcolo degli indici medi che intende utilizzare per riconoscere trattamenti economici premiali ai dipendenti (v. sopra punto 1.3.), tenendo presenti nel trattamento dei dati i limiti di legge in materia (in particolare, per quanto riguarda il divieto operante per le imprese di trasporto di "retribuire i conducenti salariati o conceder e loro premi o maggiorazioni di salario in base alle distanze percorse [...], se queste retribuzioni siano di natura tale da mettere in pericolo la sicurezza stradale": art. 10 reg. Ce n. 561/2006 del 15 marzo 2006).

Il trattamento, previo espletamento, da parte della società di trasporto, degli adempimenti richiesti dal menzionato art. 4, dovrà essere altresì svolto nel rispetto degli ulteriori adempimenti formulati al successivo punto 7.

6. LICEITÀ DEL TRATTAMENTO RISPETTO ALLA TRACCIABILITÀ DEI SINISTRI MEDIANTE LA *CD. BLACK BOX*

Ancorché la società non abbia chiarito del tutto in atti la finalità che intende perseguire mediante la cd. black box (e debba meglio esplicitarla negli atti attuativi del presente provvedimento), con riguardo ai dati dei conducenti dai quali sia possibile ritrarne la condotta in occasione di un sinistro, il trattamento che si intende porre in essere risulta anch'esso, allo stato degli atti, lecito.

Infatti, l'acquisizione di elementi volti alla ricostruzione di un sinistro, oltre che a incrementare, in prospettiva, gli standard di sicurezza dei soggetti trasportati (e, in primo luogo, dello stesso conducente), può rivelarsi utile ai fini dell'accertamento di condotte non conformi alla disciplina in materia di sicurezza stradale e per l'accertamento di eventuali responsabilità in capo ai conducenti medesimi.

La società, anche alla luce delle specifiche previsioni contrattuali in materia (cfr., in particolare,

artt. 73 e 74 del vigente Ccnl degli autoferrotranvieri, che pongono in capo all'autista specifiche responsabilità in ordine al rispetto della circolazione stradale e l'eventuale risarcimento dei danni imputabili), potrà trattare le informazioni relative ai conducenti inerenti alla tracciabilità degli eventuali sinistri; la stessa società, al fine di garantire la liceità e correttezza del trattamento (art. 11, comma 1, lett. a), del Codice), dovrà tuttavia provvedere al preventivo espletamento delle procedure richieste dall'art. 4, secondo comma, della legge n. 300/1970; dovrà essere inoltre garantito il rispetto degli ulteriori adempimenti formulati al successivo punto 7.

7. ADEMPIMENTI ULTERIORI

Resta fermo che per tutte le finalità indicate nel presente provvedimento (punti 4-6):

a) ai lavoratori dovranno essere forniti gli elementi prescritti dall'art. 13 del Codice unitamente a compiuti ragguagli sulla natura dei dati trattati e sulle caratteristiche del sistema, tenuto conto delle diverse finalità perseguite (in proposito, cfr. già Provv. 1° marzo 2007, Linee-guida del Garante per posta elettronica e internet, doc. web n. 1387522);

b) l'accesso ai dati riferiti ai conducenti, concernenti la localizzazione o inerenti alle "condotte di guida", dovrà essere consentito ai soli incaricati della società che possono prenderne legittimamente conoscenza in ragione delle mansioni svolte (ad esempio, in relazione alla circolazione dei veicoli, il personale incaricato di coordinare il servizio di trasporto pubblico nei diversi turni di lavoro; nel caso degli indici medi utili a misurare la "condotta di guida", agli incaricati operanti nella gestione delle risorse umane);

c) i dati personali non potranno essere conservati per un tempo superiore a quello necessario al conseguimento delle finalità indicate (art. 11, comma 1. lett. e), del Codice). In particolare, le informazioni relative alla localizzazione, opportunamente anonimizzate, potranno essere trattate per le attività di monitoraggio e pianificazione del servizio di trasporto pubblico solo se in forma aggregata (artt. 3 e 11, comma 1, lett. e), del Codice);

d) la società dovrà designare il fornitore del servizio oggetto della verifica preliminare quale responsabile del trattamento ai sensi dell'art. 29 del Codice (v. sopra, punto 3);

e) infine, con specifico riferimento ai dati relativi alla localizzazione, la società dovrà notificare il trattamento nel rispetto di quanto previsto dagli artt. 37 e ss. del Codice.

TUTTO CIÒ PREMESSO IL GARANTE

a conclusione della verifica preliminare relativa all'utilizzo di un sistema di localizzazione satellitare che Air P ullman S.p.A. e le società contr ollate "Air Pullman Noleggi s.r.l." e "Saco s.r.l." intendono installar e per finalità connesse alla gestione di linee di traspor to, prende atto del trattamento di dati personali oggetto di dichiarazioni della società che potrà essere svolto, fermo restando che:

1. agli interessati, unitamente agli elementi da fornir e ai sensi dell'art. 13 del Codice, dovranno essere forniti compiuti ragguagli sulla natura dei dati trattati e sulle caratteristiche del sistema, tenuto conto delle div erse finalità perseguite (punto 7);
2. l'accesso ai dati trattati do vrà esser e consentito ai soli incaricati della società che, in ragione delle mansioni svolte, possono prenderne legittimamente conoscenza (punto 7);
3. i dati dovranno essere conservati per il tempo necessario al conseguimento delle finalità perseguite. In particolare, le informazioni relative alla localizzazione, opportunamente anonimizzate, dovranno essere trattate per le attività di monitoraggio e pianificazione del servizio di trasporto pubblico solo in forma aggr egata (punto 7);
4. per la finalità richiamata al punto 5.2, il trattamento dei dati do vrà avvenire tenuto conto dei limiti di legge in materia, in par ticolare dell'art. 10 reg. Ce n. 561/2006 del 15 marzo 2006;
5. siano previamente espletate le pr ocedure previste dall'art. 4, secondo comma, della legge n. 300/1970;
6. la società dovrà notificare al Garante il trattamento, con specifico riferimento ai dati relativi alla localizzazione, e designar e il fornitor e del servizio quale responsabile del trattamento ai sensi dell'art. 29 del Codice.

Roma, 5 giugno 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

32. Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili (*)

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) e ritenuta l'opportunità di promuovere alcune misure di semplificazione per l'intero settore pubblico e privato in relazione alle correnti attività amministrative e contabili, in particolare nei riguardi di piccole e medie imprese, liberi professionisti e artigiani;

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

Relatore il prof. Francesco Pizzetti;

PREMESSO

1. Esigenze alla base di nuove misure di semplificazione

Presso vari operatori si avverte l'esigenza di alcune semplificazioni nell'applicazione della disciplina sulla protezione dei dati personali.

La riflessione in ambito pubblico e privato è avvertita in modo particolare presso piccole e medie imprese, liberi professionisti e artigiani, per quanto riguarda la gestione di informazioni attinenti ad altre imprese, amministrazioni, clienti, fornitori e dipendenti utilizzate, anche in relazione a obblighi contrattuali e normativi, per correnti finalità amministrative e contabili.

(*) Gazzetta Ufficiale 1° luglio 2008, n. 152 [doc. *web* n. 1526724]
Congiuntamente al presente provvedimento sulla semplificazione, in fase di pubblicazione sulla Gazzetta ufficiale, il Garante ha segnalato alle competenti autorità di Governo l'opportunità di apportare una modifica al Codice con riferimento alla disciplina delle misure minime di sicurezza e al documento programmatico, per contemperare meglio l'applicazione delle necessarie cautele di sicurezza dei dati e dei sistemi con l'esigenza di adattarle alle attività che, specie presso piccole e medie imprese, liberi professionisti e artigiani, vengono svolte in relazione ad attività di corrente gestione amministrativa e contabile.
In tale prospettiva, il Garante ha ipotizzato una modifica normativa dell'art. 33 del Codice, del seguente tenore:

"Art.
All'articolo 33 del decreto legislativo 30 giugno 2003 n. 196, dopo il comma 1, è aggiunto il seguente:
"1-bis. Il Garante può individuare con proprio provvedimento modalità semplificate in ordine all'adozione delle misure minime di cui al comma 1, con riferimento ai trattamenti effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani"."

Sulla base dell'esperienza acquisita in materia vengono prospettate alcune criticità rispetto a determinate modalità per adempiere a obblighi di legge o derivanti da un contratto, avvertite come troppo onerose in rapporto alle garanzie per gli interessati.

Il Garante ha completato un'analisi approfondita della problematica. In aggiunta alle misure di semplificazione disposte con decisioni per casi specifici, l'Autorità ha intrapreso varie iniziative, anche sulla base di un dialogo con le categorie interessate, che ha già comportato l'approvazione di un provvedimento di carattere generale ("Guida pratica e misure di semplificazione per le piccole e medie imprese", Provv. 24 maggio 2007, n. 21, in G.U. 21 giugno 2007, n. 142 e doc. web n. 1412271).

Dall'istruttoria sono emerse tre valutazioni di fondo:

a) alcune modalità applicative, seguite soprattutto presso piccole imprese, liberi professionisti e artigiani, sono ancora basate su approcci prettamente burocratici e di ordine puramente formale. Istituti posti a garanzia degli interessati vengono banalizzati in contrasto con lo spirito del Codice che intende assicurare una protezione elevata dei diritti e delle libertà fondamentali "nel rispetto dei princìpi di semplificazione, armonizzazione ed efficacia" (art. 2, comma 2). Da tali prassi conseguono adempimenti superflui o ripetuti inutilmente, talvolta anche per effetto di erronee valutazioni fornite in sede di consulenza, con oneri organizzativi da cui non deriva un reale valore aggiunto ai fini della correttezza e della trasparenza del trattamento e che gli interessati avvertono con disinteresse o fastidio;

b) è possibile apportare ulteriori semplificazioni (in particolare per agevolare la corrente attività gestionale di organismi pubblici e privati di ridotte dimensioni), in aggiunta a quelle già introdotte per legge o da questa Autorità e in armonia con la disciplina complessiva, anche comunitaria, della materia, salvaguardando i diritti e le libertà fondamentali dei cittadini;

c) la protezione dei dati personali può rappresentare una risorsa, anche per piccole e medie imprese, rendere più efficiente l'attività gestionale e incrementare la fiducia degli interessati.

L'Autorità intende fornire un suo nuovo contributo in materia esercitando le attribuzioni che le sono conferite per legge.

Con il presente provvedimento sono pertanto individuate soluzioni concrete volte ad agevolare

ulteriormente l'ordinaria attività di gestione amministrativa e contabile, in modo particolare rispetto ai casi in cui non sono trattati dati di carattere sensibile o giudiziario. Di seguito, vengono quindi enunciate nuove linee guida-interpretative della normativa vigente e sono individuate alcune modalità innovative per semplificare taluni adempimenti, in modo particolare per l'informativa agli interessati e il consenso.

2. L'INFORMATIVA AGLI INTERESSATI

Diverse realtà, specie imprenditoriali di piccole e medie dimensioni, trattano dati, anche in relazione a obblighi contrattuali, precontrattuali o di legge, esclusivamente per finalità di ordine amministrativo e contabile (gestione di ordinativi, buste paga e di ordinaria corrispondenza con clienti, fornitori, realtà esterne di supporto anche in outsourcing, dipendenti); spesso, ciò accade in relazione a informazioni che non hanno carattere sensibile o giudiziario.

Alcune tra le criticità menzionate riguardano le modalità con cui l'informativa è fornita per iscritto, anziché oralmente (art. 13). Sono stati formati spesso moduli lunghi e burocratici, privi di comunicatività e basati sull'eccessivo uso di espressioni prettamente giuridiche, inidonee a far comprendere le caratteristiche principali del trattamento. Alla mancanza di chiarezza si è sommata l'inutile ripetizione dell'informativa in occasione di ciascun contatto con gli interessati, frazionando le spiegazioni che andrebbero invece fornite in modo organico e possibilmente unitario.

Il Garante intende prescrivere a tutti i titolari in ambito privato e pubblico alcune misure opportune e formulare indicazioni per semplificare l'informativa nei termini di cui al seguente dispositivo (artt. 2, comma 2, 13, commi 3 e 5 e 154, comma 1, lett. c)).

3. IL CONSENSO

Il Garante, con riferimento al consenso (art. 23), considerati i princìpi di efficacia e proporzionalità e in relazione agli artt. 2, 18, 24 comma 1 e 154, comma 1, lett. c), del Codice, intende anche prescrivere a tutti i titolari del trattamento pubblici e privati alcune misure opportune affinché non richiedano il consenso nei vari casi in cui esso non deve essere richiesto (dai soggetti pubblici) o è superfluo (per i soggetti privati). Ciò, in particolare, quando:

a) il trattamento dei dati in ambito privato è svolto per adempiere a obblighi contrattuali o

normativi o, comunque, per ordinarie finalità amministrative e contabili;

b) i dati trattati provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque o sono relativi allo svolgimento di attività economiche dell'interessato (v., per i presupposti relativi a ciascuno dei predetti casi, l'art. 24, comma 1; v. anche l'art. 18, comma 4).

Il Garante, in applicazione dell'istituto del bilanciamento degli interessi (art. 24, comma 1, lett. g)) intende anche individuare un'ulteriore ipotesi nella quale il consenso non va richiesto.

Il titolare del trattamento che abbia già venduto un prodotto o prestato un servizio a un interessato, nel quadro dello svolgimento di ordinarie finalità amministrative e contabili, potrà utilizzare nei termini di cui al seguente dispositivo i recapiti (oltre che di posta elettronica, come già previsto per legge: art. 130, comma 4) di posta cartacea forniti dall'interessato medesimo, per inviare ulteriore suo materiale pubblicitario o promuovere una sua vendita diretta o per compiere sue ricerche di mercato o di comunicazione commerciale.

Tale bilanciamento degli interessi considera le difficoltà rappresentate da alcuni operatori economici nel conservare un proprio diretto "canale comunicativo" con i soggetti con i quali abbiano già instaurato un rapporto contrattuale; tiene al tempo stesso conto del diritto dell'interessato a non essere disturbato mediante comunicazioni promozionali, in base a garanzie analoghe a quelle previste, per la situazione appena indicata, per l'uso della posta elettronica (art. 130, comma 4; v. anche, con riguardo alle comunicazioni postali, l'art. 58, comma 2, d.lg. n. 206/2005).

Non è necessario rivolgere un'istanza al Garante per avvalersi delle opportunità previste dal presente punto 3.

Viene infine dato atto nel seguente dispositivo di alcune altre risultanze dell'istruttoria relative alla designazione degli incaricati del trattamento e alla notificazione dei trattamenti.

TUTTO CIÒ PREMESSO IL GARANTE

1) ai sensi degli artt. 2, comma 2, 13, commi 3 e 5 e 154, comma 1, lett. c), del Codice formula a tutti i titolari del trattamento in ambito privato e pubblico, in particolare a piccole e medie imprese, liberi professionisti, artigiani, le seguenti indicazioni per semplificare l'informativa rispetto allo svolgimento di correnti finalità amministrative e contabili, anche in relazione all'adempimento di obblighi contrattuali, precontrattuali o normativi.

Detti soggetti possono:

a) fornire un'unica informativa per il complesso dei trattamenti, anziché per singoli aspetti del rapporto con gli interessati;

b) fornire a questi ultimi una ricostruzione organica dei trattamenti e con linguaggio semplice, senza frammentarla o reiterarla inutilmente;

c) indicare le informazioni essenziali in un quadro adeguato di lealtà e correttezza;

d) redigere, per quanto possibile, una prima informativa breve. All'interessato, anche oralmente, andrebbero indicate sinteticamente alcune prime notizie chiarendo subito, con immediatezza, le principali caratteristiche del trattamento. In linea di massima l'informativa breve, quando è scritta, può avere la seguente formulazione:

"I SUOI DATI PERSONALI

Utilizziamo –anche tramite collaboratori esterni– i dati che la riguardano esclusivamente per nostre finalità amministrative e contabili, anche quando li comunichiamo a terzi. Informazioni dettagliate, anche in ordine al suo diritto di accesso e agli altri suoi diritti, sono riportate su ...";

e) per l'informativa, specie per quella breve, si possono utilizzare gli spazi utili nel materiale cartaceo e nella corrispondenza che si impiegano già, ordinariamente, per finalità amministrative e contabili;

f) l'informativa breve può rinviare a un testo più articolato, disponibile agevolmente senza oneri per gli interessati, in luoghi e con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per la clientela, messaggi preregistrati disponibili digitando un numero telefonico gratuito).
Anche questa più ampia informativa deve essere improntata a correttezza, tenendo conto di possibili modifiche del trattamento, ed essere basata su espressioni sintetiche, chiare e comprensibili. Le notizie da indicare per legge (art. 13, comma 1) devono essere aggiornate, specificando la data dell'ultimo aggiornamento;

g) è possibile non inserire nell'informativa più articolata gli elementi noti all'interessato (art. 13, commi 2 e 4). È opportuno omettere riferimenti meramente burocratici o

circostanze ovvie, per esempio quando alcune informazioni, compresi gli estremi identificativi del titolare, risultano da altre parti del documento in cui è presente l'informativa. Vanno utilizzate espressioni efficaci, anche se sintetiche, anche per quanto riguarda i diritti degli interessati e l'organismo o soggetto al quale rivolgersi per esercitarli. Se è prevista la raccolta di dati presso terzi è possibile formulare una sola informativa per i dati forniti direttamente dall'interessato e per quelli che saranno acquisiti presso terzi. Per questi ultimi dati, l'informativa può non essere fornita quando vi è un obbligo normativo di trattarli (art. 13, comma 5);

h) è opportuno che l'informativa più articolata sia basata su uno schema tendenzialmente uniforme per il settore di attività del titolare del trattamento;

i) è invece necessario fornire un'informativa specifica o ad hoc quando il trattamento ha caratteristiche del tutto particolari perché coinvolge, ad esempio, peculiari informazioni (es. dati genetici) o prevede forme inusuali di utilizzazione di dati, specie sensibili, rispetto alle ordinarie esigenze amministrative e contabili, o può comportare rischi specifici per gli interessati (ad esempio, rispetto a determinate forme di uso di dati biometrici o di controllo delle attività dei lavoratori). Se il titolare del trattamento è un soggetto pubblico devono essere inserite le indicazioni che la legge prevede per i dati sensibili e giudiziari;

2) invita le associazioni di categoria a predisporre informative-tipo per determinati settori o categorie di trattamento, anche in collaborazione con questa Autorità. Il Garante si riserva in questo quadro di porre a disposizione gratuita (chiedendo anche la collaborazione delle camere di commercio), un kit contenente concrete istruzioni e fac-simile per semplificare tutti gli adempimenti in materia;

3) richiama l'attenzione dei titolari del trattamento sulla circostanza che la designazione degli incaricati del trattamento può avvenire in modo semplificato evitando singoli atti circostanziati relativi distintamente a ciascun incaricato, individuando i trattamenti di dati e le relative modalità che sono consentiti all'unità cui sono addetti gli incaricati stessi (art. 30);

4) richiama l'attenzione dei titolari del trattamento sulla circostanza che, per effetto delle previsioni del Codice e delle determinazioni già adottate da questa Autorità, la notifica-

zione telematica al Garante non è necessaria per perseguire finalità amministrative e contabili, salvo che per eventuali casi eccezionali indicati per legge (art. 37);

5) ai sensi degli artt. 2, comma 2, 24 e 154, comma 1, lett. c), del Codice invita tutti i titolari del trattamento pubblici e privati a non chiedere il consenso degli interessati quando il trattamento dei dati è svolto, anche in relazione all'adempimento di obblighi contrattuali, precontrattuali o normativi, esclusivamente per correnti finalità amministrative e contabili, nonché quando i dati provengono da pubblici registri ed elenchi pubblici conoscibili da chiunque, o sono relativi allo svolgimento di attività economiche o sono trattati da un soggetto pubblico;

6) in applicazione del principio del bilanciamento degli interessi (art. 24, comma 1, lett. g)), dispone che i titolari del trattamento in ambito privato che hanno venduto un prodotto o prestato un servizio, nel quadro del perseguimento di ordinarie finalità amministrative e contabili, possono utilizzare senza il consenso i recapiti (oltre che di posta elettronica come già previsto per legge) di posta cartacea forniti dall'interessato, ai fini dell'invio diretto di proprio materiale pubblicitario o di propria vendita diretta o per il compimento di proprie ricerche di mercato o di comunicazione commerciale. Ciò, rispettando anche le garanzie previste per le attività di profilazione degli interessati (Provv. 24 febbraio 2005, doc. web n. 1103045), a condizione che:

   a) tale attività promozionale riguardi beni e servizi del medesimo titolare e analoghi a quelli oggetto della vendita;

   b) l'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le menzionate finalità, sia informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente, anche mediante l'utilizzo della posta elettronica o del fax o del telefono e di ottenere un immediato riscontro che confermi l'interruzione di tale trattamento (art. 7, comma 4);

   c) l'interessato medesimo, così adeguatamente informato già prima dell'instaurazione del rapporto, non si opponga a tale uso, inizialmente o in occasione di successive comunicazioni;

7) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-

Ufficio pubblicazione leggi e decr eti, per la sua pubblicazione sulla G azzetta U fficiale della Repubblica italiana, nonché alle associazioni di categoria, ai ministeri inter essati e alle camere di commercio.

Roma, 19 giugno 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

33. Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B. al Codice in materia di protezione dei dati personali (*)

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) e, in particolare gli articoli 33 ss., nonché il relativo Allegato B. contenente il disciplinare tecnico in materia di misure minime di sicurezza;

Visto l'art. 29 del decreto-legge 25 giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133, con il quale è stato, fra l'altro, modificato l'art. 34 del Codice;

Ritenuta l'esigenza di individuare alcune modalità semplificate di applicazione del predetto disciplinare tecnico da parte dei "soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale", nonché rispetto a " trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani", nel rispetto dei diritti degli interessati (comma 1-*bis* art. 34 cit.);

Rilevata l'ulteriore esigenza che di tali modalità semplificate, da aggiornare periodicamente, sia data la più ampia pubblicità anche attraverso il sito Internet dell'Autorità (www.garanteprivacy.it);

Visto il parere del Ministro per la semplificazione normativa formulato con nota del 21 novembre 2008, sullo schema preliminare del presente provvedimento trasmesso con nota del 3 novembre 2008;

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

Relatore il prof. Francesco Pizzetti;

(*) Gazzetta Ufficiale 9 dicembre 2008, n. 287 [doc. *web* n. 1571218], in inglese [doc. *web* n. 1619241]

PREMESSO

Il presente provvedimento individua modalità semplificate di applicazione delle misure minime di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B. al Codice in materia di protezione dei dati personali, di seguito indicato come Allegato B.

LA DISCIPLINA SULLE MISURE MINIME DI SICUREZZA

I soggetti che trattano dati personali sono tenuti a proteggerli attraverso adeguate misure di sicurezza.

Alcune di esse sono individuate puntualmente dal Codice e delineano il livello minimo di protezione dei dati: si tratta delle misure indicate dagli articoli 33 ss. del Codice, da adottare nei modi previsti dall'Allegato B.

Di recente sono state introdotte con disposizione di legge alcune semplificazioni relative ai trattamenti effettuati con strumenti elettronici da parte dei soggetti che utilizzano soltanto dati personali non sensibili e che trattano, come unici dati sensibili, quelli inerenti allo stato di salute o alla malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero all'adesione a organizzazioni sindacali o a carattere sindacale.

Per questi casi, la tenuta di un aggiornato documento programmatico sulla sicurezza (art. 34, comma 1, lett. g) del Codice) è stata sostituita da un obbligo di autocertificazione (resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445) di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte (art. 29 d.l. 25 giugno 2008, n. 112, come modificato dalla legge di conversione 6 agosto 2008, n. 133).

In relazione ai trattamenti sopra menzionati, nonché a quelli effettuati da chiunque per correnti finalità amministrative e contabili in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante deve individuare modalità semplificate di applicazione dell'Allegato B) sentito il Ministro per la semplificazione normativa.

Tale individuazione avviene mediante il presente provvedimento, che sarà aggiornato con cadenza periodica.

SEMPLIFICAZIONE PER TALUNI TRATTAMENTI

Come il Garante ha già evidenziato nel provvedimento del 19 giugno 2008 (in Gazzetta Ufficiale 1° luglio 2008, n. 152 e in www.garanteprivacy.it, doc. web n. 1526724), nonché mediante la segnalazione al Parlamento e al Governo in materia di misure minime di sicurezza del 19 giugno 2008, da parte di taluni titolari del trattamento le medesime misure di sicurezza possono essere attuate in modo semplificato, alla luce dell'esperienza applicativa e senza diminuire dal punto di vista sostanziale le cautele volte a prevenire determinati rischi (art. 34, comma 1 bis, del Codice, come introdotto dall'art. 29 cit.).

Sono state pertanto individuate alcune nuove modalità volte a semplificare incisivamente l'applicazione di varie regole contenute nell'Allegato B.

L'obiettivo è garantire egualmente un idoneo livello di sicurezza tenendo conto delle ridotte dimensioni di alcune realtà organizzative, nonché della particolare natura di alcuni trattamenti a fini esclusivamente amministrativo-contabili. Ciò, sulla base di una dettagliata ricognizione delle singole questioni e di approfondimenti svolti in ordine alle questioni applicative che sono state poste a vario titolo all'attenzione di questa Autorità, in particolare attraverso quesiti e segnalazioni.

Le modalità semplificate elencate nell'unito prospetto potranno essere applicate immediatamente dai soggetti interessati.

TUTTO CIÒ PREMESSO IL GARANTE

a) ai sensi dell'art. 34, comma 1-bis, del Codice individua nell'unito prospetto che costituisce parte integrante del presente provvedimento le modalità semplificate per applicare le misure minime di sicurezza per il trattamento dei dati personali;

b) dispone 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.

Roma, 27 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

Misure semplificate per applicare le misure minime di sicurezza nel trattamento dei dati personali

1. Soggetti che possono avvalersi della semplificazione

Le seguenti modalità semplificate sono applicabili dai soggetti pubblici o priv ati che:

a) utilizzano dati personali non sensibili o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori anche a pr ogetto quelli costituiti dallo stato di salute o malattia senza indicazione della r elativa diagnosi, o vvero dall'adesione a organizzazioni sindacali o a carattere sindacale;

b) trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (cfr. art. 2083 cod. civ. e d.m. 18 aprile 2005, r ecante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese, pubblicato nella Gazzetta Ufficiale 12 ottobre 2005, n. 238).

2. Trattamenti effettuati con strumenti elettronici

I soggetti di cui al paragrafo 1 possono applicar e le misure minime di sicurezza prescritte dalla disciplina in materia di trattamenti r ealizzati con l'ausilio di str umenti elettronici (art. 34 del Codice e regole da 1 a 26 dell'Allegato B.) osservando le modalità semplificate di seguito indi - viduate.

2.1. *Istruzioni agli incaricati del trattamento (modalità applicative delle regole di cui ai punti 4, 9, 18 e 21 dell'Allegato B.)*

Le istruzioni in materia di misur e minime di sicur ezza previste dall'Allegato B. possono esser e impartite agli incaricati del trattamento anche oralmente, con indicazioni di semplice e chiara formulazione.

2.2. *Sistema di autenticazione infor matica (modalità applicativ e delle regole di cui ai punti 1, 2, 3, 5, 6, 7, 8, 10 e 11 dell 'Allegato B.)*

Per l'accesso ai sistemi informatici si può utilizzar e un qualsiasi sistema di autenticazione basato su un codice per identificar e chi accede ai dati (di seguito, " username"), associato

a una parola chiave (di seguito: "password"), in modo che:

a) l'username individui in modo univoco una sola persona, evitando che soggetti diversi utilizzino codici identici;

b) la password sia conosciuta solo dalla persona che accede ai dati.

L'username deve essere disattivato quando l'incaricato non ha più la qualità che rende legittimo l'utilizzo dei dati (ad esempio, in quanto non opera più all'interno dell'organizzazione).

Può essere adottata, quale procedura di autenticazione anche la procedura di login disponibile sul sistema operativo delle postazioni di lavoro connesse a una rete.

In caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, se l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della password, il titolare può assicurare la disponibilità di dati o strumenti elettronici con procedure o modalità predefinite. Riguardo a tali modalità, sono fornite preventive istruzioni agli incaricati e gli stessi sono informati degli interventi effettuati (ad esempio, prescrivendo ai lavoratori che si assentino dall'ufficio per ferie l'attivazione di modalità che consentano di inviare automaticamente messaggi di posta elettronica ad un altro recapito accessibile: si vedano le Linee-guida in materia di lavoro per posta elettronica e Internet approvate dal Garante e pubblicate nella Gazzetta ufficiale 10 marzo 2007, n. 58 [doc. web n. 1387522]).

2.3. *Sistema di autorizzazione (modalità applicative delle regole di cui ai punti 12, 13 e 14 dell'Allegato B.)*

Qualora sia necessario diversificare l'ambito del trattamento consentito, possono essere assegnati agli incaricati –singolarmente o per categorie omogenee corrispondenti profili di autorizzazione, tramite un sistema di autorizzazione o funzioni di autorizzazione incorporate nelle applicazioni software o nei sistemi operativi, così da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

2.4. *Altre misure di sicurezza (modalità applicative delle regole di cui ai punti 15, 16, 17 e 18 dell'Allegato B.)*

I soggetti di cui al paragrafo 1 assicurano che l'ambito di trattamento assegnato ai singoli incaricati, nonché agli addetti alla gestione o alla manutenzione degli strumenti elettronici, sia coe-

rente con i princìpi di adeguatezza, proporzionalità e necessità, anche attraverso verifiche periodiche, provvedendo, quando è necessario, ad aggiornare i profili di autorizzazione eventualmente accordati.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici (ad esempio, antivirus), anche con riferimento ai programmi di cui all'art. 615-quinquies del codice penale, nonché a correggerne difetti, sono effettuati almeno annualmente. Se il computer non è connesso a reti di comunicazione elettronica accessibili al pubblico (linee ADSL, accesso a Internet tramite rete aziendale, posta elettronica), l'aggiornamento deve essere almeno biennale.

I dati possono essere salvaguardati anche attraverso il loro salvataggio con frequenza almeno mensile. Il salvataggio periodico può non riguardare i dati non modificati dal momento dell'ultimo salvataggio effettuato (dati statici), purché ne esista una copia di sicurezza da cui effettuare eventualmente il ripristino.

2.5. *Documento programmatico sulla sicurezza (modalità applicative delle regole di cui ai punti da 19.1 a 19.8 dell'Allegato B.)*

2.5.1. Fermo restando che per alcuni casi è già previsto per disposizione di legge che si possa redigere un'autocertificazione in luogo del documento programmatico sulla sicurezza (vedi il precedente par. 1, lett. a); art. 29 d.l. n. 112/2008 cit.), i soggetti pubblici e privati che trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese, possono redigere un documento programmatico sulla sicurezza semplificato sulla base delle indicazioni di seguito riportate.

Il documento deve essere redatto prima dell'inizio del trattamento e deve essere aggiornato entro il 31 marzo di ogni anno nel caso in cui, nel corso dell'anno solare precedente, siano intervenute modifiche rispetto a quanto dichiarato nel precedente documento.

Il documento deve avere i seguenti contenuti:

a) le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento;

b) una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

c) l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità;

d) una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

3. MODALITÀ APPLICATIVE PER I TRATTAMENTI REALIZZATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (MODALITÀ APPLICATIVE DELLE REGOLE DI CUI AI PUNTI 27, 28 E 29 DELL'ALLEGATO B.)

I soggetti di cui al paragrafo 1 possono adempiere all'obbligo di adottare le misure minime di sicurezza di cui all'art. 35 del Codice applicando le misure contenute nell'Allegato B. relativamente ai trattamenti realizzati senza l'ausilio di strumenti elettronici (regole da 27 a 29 dello stesso Allegato B.), con le modalità semplificate di seguito individuate.

3.1. Agli incaricati sono impartite, anche oralmente, istruzioni finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

3.2. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dai medesimi incaricati fino alla restituzione in modo che a essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

34. Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale reggente;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) e, in particolare, gli artt. 31 ss. e 154, comma 1, lett. c) e h), nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del medesimo Codice;

Visto il provvedimento del Garante del 27 novembre 2008 relativo a "misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008;

Visto il punto 3 del dispositivo del predetto provvedimento, il quale prescrive che le misure e gli accorgimenti di cui al punto 2 del medesimo dispositivo siano introdotti, per i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del provvedimento stesso, al più presto e comunque entro e non oltre il termine di centoventi giorni dalla medesima data, mentre, per i trattamenti che avranno inizio dopo il termine di trenta giorni dalla pubblicazione, tali accorgimenti e misure siano introdotti anteriormente all'inizio del trattamento dei dati;

Tenuto conto dei quesiti pervenuti sia da singoli titolari del trattamento sia da alcune associazioni rappresentative di categoria, relativi all'esatta interpretazione degli adempimenti prescritti dal citato provvedimento del 27 novembre 2008;

Considerata l'ampia platea di soggetti interessati all'adempimento del suddetto provvedimento e la conseguente necessità di assicurare la massima diffusione e la più completa e precisa conoscenza delle prescrizioni in esso contenute;

Riservata la possibilità, all'esito di un attento esame dei quesiti già pervenuti e di quelli che

(*) Gazzetta Ufficiale 24 febbraio 2009, n. 45 [doc. *web* n. 1591970]

potranno essere sottoposti all'attenzione del Garante, anche a seguito dell'attività di consultazione attualmente in corso all'interno di alcune associazioni professionali e di categoria, di fornire chiarimenti in merito attraverso risposte ai quesiti più frequenti da diffondere anche tramite il sito Internet dell'Autorità;

Ritenuta l'opportunità di unificare i termini previsti per l'adempimento delle prescrizioni di cui al citato provvedimento del 27 novembre 2008 e ravvisata altresì la necessità di prorogare tali termini, disponendo che tutti i titolari del trattamento (qualunque sia la data di inizio dei trattamenti che li riguardano) adottino le misure e gli accorgimenti di cui al punto 2 del dispositivo di tale provvedimento entro il 30 giugno 2009;

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

Relatore il prof. Francesco Pizzetti;

DISPONE:

a) di unificare e contestualmente prorogare i termini per l'adempimento delle prescrizioni di cui al citato provvedimento del 27 novembre 2008, prescrivendo che tutti i titolari del trattamento interessati (qualunque sia la data di inizio dei trattamenti che li riguardano) adottino le misure e gli accorgimenti di cui al punto 2 del dispositivo del provvedimento medesimo entro il 30 giugno 2009;

b) di trasmettere copia del presente provvedimento al Ministero della giustizia-Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 12 febbraio 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE REGGENTE
De Paoli

35. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (*)

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) e, in particolare, gli artt. 31 ss. e 154, comma 1, lett. c) e h), nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B al medesimo Codice;

Visti gli atti d'ufficio relativi alla protezione dei dati trattati con sistemi informatici e alla sicurezza dei medesimi dati e sistemi;

Rilevata l'esigenza di intraprendere una specifica attività rispetto ai soggetti preposti ad attività riconducibili alle mansioni tipiche dei cd. " amministratori di sistema ", nonché di coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati, evidenziandone la rilevanza rispetto ai trattamenti di dati personali anche allo scopo di promuovere presso i relativi titolari e nel pubblico la consapevolezza della delicatezza di tali peculiari mansioni nella "Società dell'informazione" e dei rischi a esse associati;

Considerata l'esigenza di consentire più agevolmente, nei dovuti casi, la conoscibilità dell'esistenza di tali figure o di ruoli analoghi svolti in relazione a talune fasi del trattamento all'interno di enti e organizzazioni;

Ritenuta la necessità di promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare (due diligence);

Constatato che lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di

(*) Gazzetta Ufficiale 24 dicembre 2008, n. 300 [doc. *web* n. 1577499], in inglese [doc. *web* n. 1583535]

regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti;

Rilevata la necessità di richiamare l'attenzione su tale rischio del pubblico, nonché di persone giuridiche, pubbliche amministrazioni e di altri enti (di seguito sinteticamente individuati con l'espressione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice) che impiegano, in riferimento alla gestione di banche dati o reti informatiche, sistemi di elaborazione utilizzati da una molteplicità di incaricati con diverse funzioni, applicative o sistemistiche;

Rilevato che i titolari sono tenuti, ai sensi dell'art. 31 del Codice, ad adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (artt. 15 e 169 del Codice);

Constatato che l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti;

Considerato inoltre che, qualora ritenga facoltativamente di designare uno o più responsabili del trattamento, il titolare è tenuto a individuare solo soggetti che "per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza" (art. 29, comma 2, del Codice);

Ritenuto che i titolari di alcuni trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati e sono stati pertanto oggetto di recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008), debbano essere allo stato esclusi dall'ambito applicativo del presente provvedimento;

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

Relatore il prof. Francesco Pizzetti;

PREMESSO:

1. CONSIDERAZIONI PRELIMINARI

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615-*ter*) e di frode informatica (art. 640-*ter*), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635-*bis* e *ter*) e di danneggiamento di sistemi informatici e telematici (artt. 635-*quater* e *quinques*) di recente modifica (1).

La disciplina di protezione dei dati previgente al Codice del 2003 definiva l'amministratore di

(1) V., ad es., l'art. 5 l. 18 marzo 2008, n. 48 che prevede, oltre a una maggiore pena, la procedibilità d'ufficio nel caso in cui il reato sia commesso con "abuso della qualità di operatore del sistema"

sistema, individuandolo quale " soggetto al quale è conferito il compito di so vrintendere alle risorse del sistema operativ o di un elaborator e o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Il Codice non ha inv ece incluso questa figura tra le pr oprie definizioni normativ e. Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e r ecovery dei dati) alla custodia delle cr edenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

Nel loro complesso, le norme pr edette mettono in rilievo la par ticolare capacità di azione pr opria degli amministratori di sistema e la natura fiduciaria delle r elative mansioni, analoga a quella che, in un contesto del tutto differ ente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di par ticolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo sv olgimento di uno dei ruoli più delicati della "Società dell'informazione" (2).

Nel corso delle attività ispettiv e disposte negli ultimi anni dal G arante è stato possibile rilev are quale importanza annettano ai ruoli di system administrator (e di network administrator o database administrator) la gran parte di aziende e di grandi organizzazioni pubbliche e private, al di là delle definizioni giuridiche, individuando tali figur e nell'ambito di piani di sicur ezza o di documenti programmatici e designandoli a volte quali responsabili.

In altri casi, non soltanto in organizzazioni di piccole dimensioni, si è inv ece riscontrata, anche a elev ati liv elli di r esponsabilità, una car ente consapev olezza delle criticità insite nello sv olgimento delle pr edette mansioni, con pr eoccupante sotto valutazione dei rischi deriv anti dall'azione incontrollata di chi do vrebbe essere preposto anche a compiti di vigilanza e contr ollo del corretto utilizzo di un sistema informatico.

(2) Per altro verso il legislator e, nell'intervenire in tema di "S ocietà dell'informazione", ha pr evisto che i certificatori di firma elettr onica, i quali sono pr eposti al trattamento dei dati connessi al rilascio del cer tificato di firma, debbano posseder e i r equisiti di onorabilità richiesti ai soggetti che sv olgono funzioni di amministrazione, direzione e controllo presso banche, oltre ai requisiti tecnici necessari per lo svolgimento della loro attività (artt. 26, 27 e 29 del d.lg. 7 mar zo 2005 n. 82)

Con il presente provvedimento il Garante intende pertanto richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema. L'Autorità ravvisa inoltre l'esigenza di individuare in questa sede alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito di organizzazioni ed enti pubblici e privati, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

2. QUADRO DI RIFERIMENTO NORMATIVO

Nell'ambito del Codice il presente provvedimento si richiama, in particolare, all'art. 154, comma 1, lett. h), rientrando tra i compiti dell'Autorità quello di promuovere la "conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati".

La lett. c) del medesimo comma 1 prevede poi la possibilità, da parte del Garante, di prescrivere misure e accorgimenti, specifici o di carattere generale, che i titolari di trattamento sono tenuti ad adottare.

3. SEGNALAZIONE AI TITOLARI DI TRATTAMENTI RELATIVA ALLE FUNZIONI DI AMMINISTRATORE DI SISTEMA

Ai sensi del menzionato art. 154, comma 1, lett. h) il Garante, nel segnalare a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sulla necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema; richiama inoltre l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione

l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione.

4. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

Di seguito sono indicati gli accorgimenti e le misure che vengono prescritti ai sensi dell'art. 154, comma 1, lett. c) del Codice, a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008).

I seguenti accorgimenti e misure lasciano impregiudicata l'adozione di altre specifiche cautele imposte da discipline di settore e per particolari trattamenti o che verranno eventualmente prescritte dal Garante ai sensi dell'art. 17 del Codice.

Per effetto del presente provvedimento:

4.1. *Valutazione delle caratteristiche soggettive*

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

4.2. *Designazioni individuali*

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

4.3. *Elenco degli amministratori di sistema*

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, dev ono essere riportati nel documento pr ogrammatico sulla sicurezza, oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantener e aggiornato e disponibile in caso di accer tamenti anche da par te del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di caratter e personale di lav oratori, i titolari pubblici e priv ati nella qualità di datori di lav oro sono tenuti a r endere nota o conoscibile l'identità degli amministratori di sistema nell 'ambito delle pr oprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono pr eposti. Ciò, avv alendosi dell'informativa resa agli inter essati ai sensi dell 'art. 13 del Codice nell'ambito del rappor to di lav oro che li lega al titolar e, oppure tramite il discipli - nare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 mar zo 2007, n. 58); in alternativ a si possono anche utilizzar e strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in for za di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settor e.

Nel caso di ser vizi di amministrazione di sistema affidati in outsour cing il titolare deve conservare direttamente e specificamente, per ogni ev entuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

4.4. *Verifica delle attività*

L'operato degli amministratori di sistema dev e essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicur ezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

4.5. *Registrazione degli accessi*

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli ar chivi elettr onici da par te degli amministratori di

sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di v erifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell 'evento che le ha generate e devono essere conservate per un congr uo periodo, non inferiore a sei mesi.

5. TEMPI DI ADOZIONE DELLE MISURE E DEGLI ACCORGIMENTI

Per tutti i titolari dei trattamenti già iniziati o che avranno inizio entr o trenta giorni dalla data di pubblicazione nella G azzetta Ufficiale del pr esente provvedimento, le misur e e gli accorgimenti di cui al punto 4 dovranno essere introdotti al più presto e comunque entro, e non oltre, il termine che è congr uo stabilire, in centoventi giorni dalla medesima data.

Per tutti gli altri trattamenti che avranno inizio dopo il pr edetto termine di tr enta giorni dalla pubblicazione, gli accorgimenti e le misur e dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

TUTTO CIÒ PREMESSO IL GARANTE:

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, nel segnalar e a tutti i titolari di trattamenti di dati personali soggetti all 'ambito applicativo del Codice ed effettuati con str umenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sull 'esigenza di valutare con par ticolare attenzione l'attribuzione di funzioni tecniche pr opriamente corrispondenti o assimilabili a quelle di amministratore di sistema (system administrator), amministrator e di base di dati (database administrator) o amministrator e di r ete (network administrator), laddo ve tali funzioni siano eser citate in un contesto che r enda ad essi tecnicamente possibile l 'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l 'opportunità o meno di tale attribuzione e le concr ete modalità sulla base delle quali si sv olge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato;
2. ai sensi dell 'art. 154, comma 1, lett. c) del Codice pr escrive l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all 'ambito applicativ o del Codice ed effettuati con str umenti elettronici, anche in ambito giudiziario e di for ze di

polizia (artt. 46 e 53 del Codice), salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008):

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

b. Designazioni individuali

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

c. Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie orga-

nizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

d. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

e. Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

3. dispone che le misure e gli accorgimenti di cui al punto 2 del presente dispositivo siano introdotti, per tutti i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, al più presto e

comunque entro, e non oltre, il termine che è congruo stabilire in centoventi giorni dalla medesima data; per tutti gli altri trattamenti che avranno inizio dopo il pr edetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misur e dovranno essere introdotti anteriormente all'inizio del trattamento dei dati;

4. dispone che copia del pr esente pr ovvedimento sia trasmesso al M inistero della giustizia–Ufficio pubblicazione leggi e decr eti per la sua pubblicazione sulla G azzetta Ufficiale della Repubblica Italiana.

Roma, 27 novembre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Buttarelli

Provvedimento "Amministratori di sistema" del 27 novembre 2008 (*)

Risposte alle domande più frequenti (FAQ) (1)

1) Cosa deve intendersi per "amministratore di sistema"?

In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

Il Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi.

Anche il riferimento al d.P.R. 318/1999 nella premessa del provvedimento è puramente descrittivo poiché la figura definita in quell'atto normativo (ormai abrogato) è di minore portata rispetto a quella cui si fa riferimento nel provvedimento.

Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

2) Cosa vuol dire la locuzione "Qualora l'attività degli ADS riguardi anche indirettamente servizi o sistemi che …"

I titolari sono tenuti a instaurare un regime di conoscibilità dell'identità degli amministratori di sistema, quale forma di trasparenza interna all'organizzazione a tutela dei lavoratori, nel caso in cui un amministratore di sistema, oltre a intervenire sotto il profilo tecnico in generici trattamenti di dati personali in un'organizzazione, tratti anche dati personali riferiti ai lavoratori operanti nell'am-

(*) Gazzetta Ufficiale del 24 dicembre 2008, n. 300
(1) Così richiamate dal provvedimento "Amministratori di sistema: avvio di una consultazione pubblica" del 21 aprile 2009 [doc. *web* n. 1611986]

bito dell'organizzazione medesima o sia nelle condizioni di acquisire conoscenza di dati a essi riferiti (in questo senso il riferimento nel testo del pr ovvedimento all'"anche indirettamente …").

3) Il caso di uso esclusiv o di un personal computer da par te di un solo amministrator e di sistema rientra nell'ambito applicativo del provvedimento?

Non è possibile rispondere in generale. In diversi casi, anche con un personal computer possono essere effettuati delicati trattamenti rispetto ai quali il titolar e ha il do vere di pr evedere e mettere in atto anche le misure e gli accorgimenti previsti nel provvedimento. Nel caso-limite di un titolare che svolga funzioni di unico amministrator e di sistema, come può accader e in piccolissime realtà d'impresa, non si applicheranno le pr evisioni relative alla v erifica delle attività dell'amministratore né la tenuta del log degli accessi informatici.

4) Relativamente all'obbligo di r egistrazione degli accessi logici degli A dS, sono compr esi anche i sistemi client oltr e che quelli ser ver?

Si, anche i client, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi degli AdS.

Nei casi più semplici tale requisito può essere soddisfatto tramite funzionalità già disponibili nei più diffusi sistemi operativi, senza richiedere necessariamente l'uso di strumenti software o hardware aggiuntivi. P er esempio, la r egistrazione locale dei dati di accesso su una postazione, in determinati contesti, può essere ritenuta idonea al corretto adempimento qualora goda di sufficienti garanzie di integrità.

Sarà comunque con v alutazione del titolar e che do vrà esser e considerata l'idoneità degli str umenti disponibili oppure l'adozione di strumenti più sofisticati, quali la raccolta dei log centralizzata e l'utilizzo di dispositivi non riscrivibili o di tecniche crittografiche per la verifica dell'integrità delle registrazioni.

5) Cosa si intende per operato dell 'amministratore di sistema soggetto a contr ollo almeno annuale?

È da sottoporr e a v erifica l'attività svolta dall'amministratore di sistema nell 'esercizio delle sue

funzioni. Va verificato che le attività svolte dall'amministratore di sistema siano conformi alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.

6) Chiarire i casi di esclusione dall'obbligo di adempiere al provvedimento.

Sono esclusi i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle misure di semplificazione introdotte nel corso del 2008 per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 27 novembre 2008).

7) Cosa si intende per descrizione analitica degli ambiti di operatività consentiti all'ADS? [Rif. comma 2, lettera d]

Il provvedimento prevede che all'atto della designazione di un amministratore di sistema, venga fatta "elencazione analitica" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ovvero la descrizione puntuale degli stessi, evitando l'attribuzione di ambiti insufficientemente definiti, analogamente a quanto previsto al comma 4 dell'art. 29 del Codice riguardante i responsabili del trattamento.

8) Oltre alla job description si deve andare più in dettaglio? Si devono indicare i singoli sistemi e le singole operazioni affidate?

No, è sufficiente specificare l'ambito di operatività in termini più generali, per settori o per aree applicative, senza obbligo di specificarlo rispetto a singoli sistemi, a meno che non sia ritenuto necessario in casi specifici.

9) Cosa si intende per access log (log-in, log-out, tentativi falliti di accesso, altro?...) [Rif. comma 2, lettera f]

Per access log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software.

Gli event records generati dai sistemi di autenticazione contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (timestamp), una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out, o di una condizione di errore, quale linea di comunicazione o dispositivo o terminale sia stato utilizzato …).

10) Laddove il file di log contenga informazioni più ampie, va preso tutto il log o solo la riga relativa all'access log? [Rif. comma 2, lettera f]

Qualora il sistema di log adottato generi una raccolta dati più ampia, comunque non in contrasto con le disposizioni del Codice e con i principi della protezione dei dati personali, il requisito del provvedimento è certamente soddisfatto. Comunque è sempre possibile effettuare un'estrazione o un filtraggio dei log files al fine di selezionare i soli dati pertinenti agli AdS.

11) Come va interpretata la caratteristica di completezza del log? Si intende che ci devono essere tutte le righe? L'adeguatezza rispetto allo scopo della verifica deve prevedere un'analisi dei rischi?

La caratteristica di completezza è riferita all'insieme degli eventi censiti nel sistema di log, che deve comprendere tutti gli eventi di accesso interattivo che interessino gli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali. L'analisi dei rischi aiuta a valutare l'adeguatezza delle misure di sicurezza in genere, e anche delle misure tecniche per garantire attendibilità ai log qui richiesti.

12) Come va interpretata la caratteristica di inalterabilità dei log?

Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software. Il requisito può essere ragionevolmente soddisfatto con la strumentazione software in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di

adottare sistemi più sofisticati, quali i log server centralizzati e "certificati".

È ben noto che il problema dell'attendibilità dei dati di audit, in generale, riguarda in primo luogo la effettiva generazione degli auditable events e, successivamente, la loro corretta registrazione e manutenzione. Tuttavia il provvedimento del Garante non affronta questi aspetti, prevedendo soltanto, come forma minima di documentazione dell'uso di un sistema informativo, la generazione del log degli "accessi" (login) e la loro archiviazione per almeno sei mesi in condizioni di ragionevole sicurezza e con strumenti adatti, in base al contesto in cui avviene il trattamento, senza alcuna pretesa di instaurare in modo generalizzato, e solo con le prescrizioni del provvedimento, un regime rigoroso di registrazione degli usage data dei sistemi informativi.

13) Si individuano livelli di robustezza specifici per la garanzia della integrità?

No. La valutazione è lasciata al titolare, in base al contesto operativo (cfr. faq n. 14).

14) Quali potrebbero essere gli scopi di verifica rispetto ai quali valutare l'adeguatezza?

Quelli descritti al paragrafo 4.4 del provvedimento e ribaditi al punto 2, lettera e), del dispositivo. L'adeguatezza è da valutare in rapporto alle condizioni organizzative e operative dell'organizzazione.

15) Cosa dobbiamo intendere per evento che deve essere registrato nel log? Solo l'accesso o anche le attività eseguite?

Il provvedimento non chiede in alcun modo che vengano registrati dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema. Si veda la risposta alla faq n. 11.

16) Quali sono le finalità di audit che ci dobbiamo porre con la registrazione e raccolta di questi log?

La raccolta dei log serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso…). L'analisi dei log può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.

17) Cosa si intende per "consultazione in chiaro"?

Il riferimento in premessa (par. 1 "Considerazioni preliminari") è alla criticità di mansioni che comportino la potenzialità di violazione del dato personale anche in condizioni in cui ne sia esclusa la conoscibilità, come può avvenire, per esempio, nel caso della cifratura dei dati.

18) Il regime di conoscibilità degli amministratori di sistema è da intendersi per i soli trattamenti inerenti i dati del personale e dei lavoratori?

Si.

19) La registrazione degli accessi è relativa al sistema operativo o anche ai DBMS?

Tra gli accessi logici a sistemi e archivi elettronici sono comprese le autenticazioni nei confronti dei data base management systems (DBMS), che vanno registrate.

20) Nella designazione degli amministratori di sistema occorre valutare i requisiti morali? [Rif. comma 2, lettera a]

No. Il riferimento alle caratteristiche da prendere in considerazione, al comma 2, lettera a), del dispositivo, è all'esperienza, alla capacità e all'affidabilità del soggetto designato. Si tratta quindi di qualità tecniche, professionali e di condotta, non di requisiti morali.

21) Cosa si intende per "estremi identificativi" degli amministratori di sistema?

Si tratta del minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza.

22) È corretto affermare che l'accesso a livello applicativo non rientri nel perimetro degli adeguamenti, in quanto l'accesso a una applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati?

Si. L'accesso applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema e quindi non è necessario, in forza del provvedimento del Garante, sottoporlo a registrazione.

23) Si chiede se sia necessario conformarsi al provvedimento nel caso della fornitura di servizi di gestione sistemistica a clienti esteri (housing, hosting, gestione applicativa, archiviazione remota...) da parte di una società italiana non titolare dei dati gestiti.

Il provvedimento si rivolge solo ai titolari di trattamento. I casi esemplificati prefigurano al più una responsabilità di trattamento (secondo il Codice italiano), e sono quindi esclusi dall'ambito applicativo del provvedimento.

24) Si possono ritenere esclusi i trattamenti relativi all'ordinaria attività di supporto delle aziende, che non riguardino dati sensibili, giudiziari o di traffico telefonico/telematico? Ci si riferisce ai trattamenti con strumenti elettronici finalizzati, ad esempio, alla gestione dell'autoparco, alle procedure di acquisto dei materiali di consumo, alla manutenzione degli immobili sociali ecc. ...).

Tali trattamenti possono considerarsi compresi tra quelli svolti per ordinarie finalità amministrativo-contabili e, come tali, esclusi dall'ambito applicativo del provvedimento.

36. Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali (*)

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;

Visti gli atti d'ufficio relativi alla problematica del rinvenimento di dati personali all'interno di apparecchiature elettriche ed elettroniche cedute a un rivenditore per la dismissione o la vendita o a seguito di riparazioni e sostituzioni; viste, altresì, le recenti notizie di stampa in ordine al rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;

Visto il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), con particolare riferimento agli artt. 31 e ss. e 154, comma 1, lett. h), nonché alle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza allegato "B" al Codice;

Visto il d.lg. 25 luglio 2005, n. 151 (Attuazione delle direttive 2002/95/Ce, 2002/96/Ce e 2003/108/Ce, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti), che prevede misure e procedure finalizzate a prevenire la produzione di rifiuti di apparecchiature elettriche e elettroniche, nonché a promuovere il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurne la quantità da avviare allo smaltimento (cfr. art. 1, comma 1, lett. a) e b));

Considerato che l'applicazione della disciplina contenuta nel menzionato d.lg. n. 151/2005, mirando (tra l'altro) a privilegiare il recupero di componenti provenienti da rifiuti di apparecchiature elettriche ed elettroniche (Raee), anche nella forma del loro reimpiego o del riciclaggio in beni oggetto di (nuova) commercializzazione (cfr. in particolare artt. 1 e 3, comma 1, lett. e) ed f), d.lg. n. 151/2005), comporta un rischio elevato di "circolazione" di componenti elettroniche "usate" contenenti dati personali, anche sensibili, che non siano stati cancellati in modo idoneo, e di conseguente accesso ad essi da parte di terzi non autorizzati (quali, ad esempio,

(*) Gazzetta Ufficiale 9 dicembre 2008, n. 287 [doc. *web* n. 1571514], in inglese [doc. *web* n. 1583482]

coloro che provvedono alle predette operazioni propedeutiche al riutilizzo o che acquistano le apparecchiature sopra indicate);

Considerato che il "reimpiego" consiste nelle operazioni che consentono lutilizzo dei rifiuti elettrici ed elettronici o di loro componenti "allo stesso scopo per il quale le apparecchiature erano state originariamente concepite, compresa l'utilizzazione di dette apparecchiature o di loro componenti successivamente alla loro consegna presso i centri di raccolta, ai distributori, ai riciclatori o ai fabbricanti" (art. 3, comma 1, lett. e), d.lg. n. 151/2005) e il " riciclaggio" consiste nel "ritrattamento in un processo produttivo dei materiali di rifiuto per la loro funzione originaria o per altri fini" (art. 3, comma 1, lett. e), d.lg. n. 151/2005);

Considerato che rischi di accessi non autorizzati ai dati memorizzati sussistono anche in relazione a rifiuti di apparecchiature elettriche ed elettroniche avviati allo smaltimento (art. 3, comma 1, lett. i), d.lg. n. 151/2005);

Rilevata la necessità di richiamare l'attenzione su tali rischi di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali (di seguito sinteticamente individuati con la locuzione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice), dismettono sistemi informatici o, più in generale, apparecchiature elettriche ed elettroniche contenenti dati personali (come pure dei soggetti che, su base individuale o collettiva, provvedono al reimpiego, al riciclaggio o allo smaltimento dei rifiuti di dette apparecchiature);

Rilevato che la disciplina di cui al citato d.lg. n. 151/2005 e alla normativa secondaria che ne è derivata (allo stato contenuta nel d.m. 25 settembre 2007, n. 185, recante "Istituzione e modalità di funzionamento del registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei rifiuti di apparecchiature elettriche ed elettroniche (Raee)", nell'ulteriore d.m. del 25 settembre 2007, recante "Istituzione del Comitato di vigilanza e di controllo sulla gestione dei Raee", nonché nel d.m. 8 aprile 2008, recante "Disciplina dei centri di raccolta dei rifiuti urbani raccolti in modo differenziato come previsto dall'art. 183, comma 1, lettera cc) del decreto legislativo 3 aprile 2006, n. 152 e successive modifiche") lascia impregiudicati gli obblighi che gravano sui titolari del trattamento relativamente alle misure di sicurezza nel trattamento dei dati personali (e la conseguente responsabilità);

Rilevato che ogni titolare del trattamento deve quindi adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della dismissione dei menzionati apparati elettrici ed elettronici (artt. 31 ss. del Codice); ciò, considerato anche che, impregiudicati eventuali accordi che prevedano diversamente, produttori, distributori e centri di assistenza di apparecchiature elettriche ed elettroniche non risultano essere soggetti, in base alla particolare disciplina di settore, a specifici obblighi di distruzione dei dati personali eventualmente memorizzati nelle apparecchiature elettriche ed elettroniche a essi consegnate;

Rilevato che dall'inosservanza delle misure di sicurezza può derivare in capo al titolare del trattamento una responsabilità penale (art. 169 del Codice) e, in caso di danni cagionati a terzi, civile (artt. 15 del Codice e 2050 cod. civ.);

Rilevato che analoghi obblighi relativi alla destinazione dei dati gravano sul titolare del trattamento nel caso in cui la dismissione delle apparecchiature coincida con la cessazione del trattamento (art. 16 del Codice);

Rilevato che le misure da adottare in occasione della dismissione di componenti elettrici ed elettronici suscettibili di memorizzare dati personali devono consistere nell'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, sì da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venirne a conoscenza non avendone diritto (si pensi, ad esempio, ai dati personali memorizzati sul disco rigido dei personal computer o nelle cartelle di posta elettronica, oppure custoditi nelle rubriche dei terminali di comunicazione elettronica);

Considerato che tali misure risultano allo stato già previste quali misure minime di sicurezza per i trattamenti di dati sensibili o giudiziari, sulla base delle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza che disciplinano la custodia e l'uso dei supporti rimovibili sui quali sono memorizzati i dati, che vincolano il riutilizzo dei supporti alla cancellazione effettiva dei dati o alla loro trasformazione in forma non intelligibile;

Ritenuto che i titolari del trattamento, in occasione della dismissione delle menzionate apparecchiature elettriche ed elettroniche, qualora siano sprovvisti delle necessarie competenze e strumentazioni tecniche per la cancellazione dei dati personali, possono ricorrere all'ausilio o con-

ferendo incarico a soggetti tecnicamente qualificati in grado di porre in essere le misure idonee a cancellare effettivamente o rendere non intelligibili i dati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione di tali operazioni o si impegnino ad effettuarle;

Ritenuto che chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti debba comunque assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

Considerato che, ferma restando l'adozione di ulteriori opportune cautele volte a prevenire l'indebita acquisizione di informazioni personali, anche fortuita, da parte di terzi, le predette misure, suscettibili di aggiornamento alla luce dell'evoluzione tecnologica, possono in particolare consistere, a seconda dei casi, anche nelle procedure di cui agli allegati documenti, che costituiscono parte integrante del presente provvedimento;

Ritenuta la necessità di curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati (art. 154, comma 1, lett. h), del Codice), con riferimento alla dismissione di apparecchiature elettriche ed elettroniche, anche attraverso la pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana;

Visteleosservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

TUTTO CIÒ PREMESSO IL GARANTE:

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, richiama l'attenzione di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, non distruggono, ma dismettono supporti che contengono dati personali, sulla necessità di adottare idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:

a. reimpiegate o riciclate, anche seguendo le procedure di cui all'allegato A);

b. smaltite, anche seguendo le procedure di cui all'allegato B).

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

2. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 13 ottobre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche

In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l'applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file), e comporta la necessità per l'utente di tenere traccia separatamente delle parole-chiave utilizzate.
2. Memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un cd. file-system crittografico (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo personal computer, e dispositivi elettronici) in grado di proteggere, con un'unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L'unica parola-chiave di volume verrà automaticamente utilizzata per le operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l'uso dei programmi software con cui i dati vengono trattati.

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.

Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.

4. Formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting - LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

ALLEGATO B) AL PROVVEDIMENTO DEL GARANTE DEL 13 OTTOBRE 2008

Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettr onici, l'effettiva cancellazione dei dati personali dai suppor ti contenuti nelle appar ecchiature elettriche ed elettr oniche può anche risultar e da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i suppor ti ottici come i cd-r om e i dvd);
- demagnetizzazione ad alta intensità.

37. Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali (*)

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. Giuseppe Fortunato, componente, e del dott. Giovanni Buttarelli, segretario generale;

Vista la deliberazione 29 novembre 2007, n. 62, con la quale l'Autorità ha avviato una procedura di consultazione pubblica su un documento, adottato in pari data, contenente "Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali" e pubblicato, unitamente alla medesima deliberazione, sul sito web dell'Autorità;

Visti i commenti e le osservazioni pervenuti a questa Autorità a seguito della consultazione pubblica per la quale era stato fissato il termine del 15 febbraio 2008;

Considerate le risultanze degli incontri intercorsi con i rappresentanti di categoria e con altri enti e organismi che hanno partecipato alla consultazione pubblica;

Ritenuto, in base agli approfondimenti svolti, di individuare un quadro unitario di misure e accorgimenti necessari e opportuni volti a fornire orientamenti utili per i promotori e gli altri operatori che, a vario titolo, intervengono nelle sperimentazioni cliniche riguardo al trattamento dei dati delle persone coinvolte;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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. Giuseppe Chiaravalloti;

DELIBERA:

a) di adottare in via definitiva le "Linee-guida per i trattamenti di dati personali nell'ambito

(*) Deliberazione n. 52 del 24 luglio 2008, Gazzetta Ufficiale 14 agosto 2008, n. 190 [doc. *web* n. 1533155], in inglese [doc. *web* n. 1544272]

delle sperimentazioni cliniche di medicinali" unitamente ad un modello di riferimento per l'informativa e la manifestazione del consenso al trattamento dei dati personali, contenuti nei documenti allegati quali parti integranti della presente deliberazione (Allegati A e n. 1);

b) che copia della presente deliberazione, unitamente ai menzionati allegati, 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;

c) che copia dei predetti documenti sia, altresì, trasmessa per opportuna conoscenza, al Ministero della salute, all'Istituto superiore di sanità, all'Agenzia italiana del farmaco e alla Conferenza Stato-Regioni.

Roma, 24 luglio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE
Buttarelli

ALLEGATO A. LINEE-GUIDA PER I TRATTAMENTI DI DATI PERSONALI NELL'AMBITO DELLE SPERIMENTAZIONI CLINICHE DI MEDICINALI

1. CONSIDERAZIONI PRELIMINARI

Gli studi condotti su esseri umani nell'ambito della sperimentazione clinica mirano a scoprire o verificare gli effetti di medicinali sperimentali, compresa qualsiasi reazione avversa, al fine di accertarne la sicurezza e l'efficacia. Tali studi vengono generalmente promossi da una società farmaceutica (committente o sponsor, di seguito individuata come "promotore") a livello nazionale e (specie a cura di società facenti parte di gruppi multinazionali) internazionale.

A tal fine detto soggetto, dopo aver predisposto un protocollo che descrive la progettazione, gli obiettivi e la metodologia della sperimentazione, cura la presentazione alle autorità competenti e ai comitati etici interessati della documentazione necessaria all'attivazione della sperimentazione.

Le attività collegate allo studio vengono eseguite presso una o più strutture ospedaliere o universitarie o istituti di ricerca pubblici o privati autorizzati in base alla legge (centri di sperimentazione) e appositamente individuati dalle società committenti. Vengono raccolti, in conformità al protocollo e a più riprese nel corso dello studio, varie informazioni di carattere medico/clinico e i campioni biologici delle persone che accettano di far parte dello studio tramite visite mediche e accertamenti diagnostici effettuati da medici sperimentatori.

A queste informazioni non ha accesso soltanto il personale sanitario operante presso i centri. Il promotore supervisiona, infatti, l'andamento dello studio, per garantire che esso venga effettuato in osservanza del protocollo. Ciò, avvalendosi di propri collaboratori (clinical study monitor) i quali, nell'ambito della loro attività di monitoraggio, visitano i centri di sperimentazione e, se necessario, esaminano la documentazione medica originale degli individui partecipanti allo studio messa a loro disposizione dai medici (ad es. cartelle ospedaliere, registri clinici, note di laboratorio, referti ecc.).

Le informazioni medico/cliniche raccolte da medici sperimentatori presso ciascun centro vengono trasmesse al promotore a più riprese nel corso dello studio, ovvero al termine della sperimentazione presso il centro. Conclusa la fase della sperimentazione presso il centro, le medesime informazioni sono normalmente inserite dal promotore, direttamente o tramite soggetti

esterni di cui si avvale, su un data-base unico attraverso il quale viene effettuato il controllo e la validazione dei dati e, successivamente, l'elaborazione statistica, con l'obiettivo di conseguire i risultati dello studio da documentare poi in un rapporto.

Negli studi promossi da promotori che operano nell'ambito di gruppi multinazionali, il destinatario dei dati medico/clinici raccolti dai medici sperimentatori è solitamente la società capogruppo che può avere sede al di fuori del territorio nazionale. Inoltre, i promotori si avvalgono sovente di soggetti esterni (clinical study monitor, organizzazioni di ricerca a contratto, laboratori di analisi, ecc.) che possono risiedere in Paesi anche al di fuori dell'Unione europea, per svolgere uno o più compiti relativi all'esecuzione della sperimentazione (ad es., il monitoraggio dello studio, l'inserimento, la validazione e l'analisi statistica dei dati, la farmacovigilanza, l'esecuzione degli esami clinici e di laboratorio previsti dal protocollo). Ciò, comporta che numerose informazioni o campioni biologici vengano condivisi tra diverse categorie di soggetti che possono accedervi o averne la disponibilità e che possono essere situati anche in Paesi terzi che non offrono un livello di protezione adeguato dei dati personali (il promotore; gli addetti al monitoraggio dello studio; i soggetti esterni che collaborano con il promotore per l'inserimento dei dati e il loro trattamento statistico; il laboratorio di analisi, ecc.).

Al fine di confermare la validità della conduzione dello studio e l'integrità dei dati raccolti anche in occasione di eventuali verifiche da parte delle autorità dotate di poteri ispettivi, le informazioni ottenute nel corso dello studio sono oggetto di conservazione per un periodo di tempo considerevole dopo il completamento della sperimentazione.

In base agli approfondimenti svolti, la raccolta, la circolazione e la conservazione massiva, anche in Paesi terzi, di molteplici informazioni attinenti alla salute e, in alcuni casi, alla vita sessuale, delle persone coinvolte in sperimentazioni cliniche presentano vari aspetti di criticità con riferimento alla protezione dei dati personali e necessitano, pertanto, dell'adozione di elevate cautele volte a prevenire rischi specifici per gli interessati.

Al fine di individuare tali cautele, l'Autorità ha svolto preliminarmente alcuni accertamenti ispettivi presso talune società farmaceutiche; ha indetto una specifica consultazione pubblica su un documento articolato indicante le misure e gli accorgimenti ritenuti allo stato idonei per il trattamento dei dati nell'ambito delle sperimentazioni cliniche di medicinali; ha, infine, effet -

tuato diversi altri approfondimenti, anche di carattere tecnico, con i principali organismi interessati alla consultazione, volti a verificare i profili critici evidenziati nelle osservazioni pervenute all'Autorità.

Le cautele ipotizzate in sede di consultazione pubblica hanno trovato conforto all'esito della stessa e degli specifici approfondimenti tecnici svolti successivamente.

Tutte le riflessioni e i commenti pervenuti sono stati comunque oggetto di specifica analisi e considerazione nell'elaborazione delle presenti "Linee-guida" che recano alcune circoscritte modifiche rispetto al precedente documento, giustificate dall'idoneità delle osservazioni formulate.

Le presenti "Linee-guida" sono pertanto rivolte a individuare gli accorgimenti e le misure necessari e opportuni riguardo al trattamento dei dati personali dei partecipanti a sperimentazioni cliniche da parte dei promotori degli studi. Gli accorgimenti e le misure indicati vanno, altresì, prese in considerazione da tutti gli altri titolari di trattamenti di dati personali effettuati a fini di sperimentazione clinica, quali promotori diversi dalle società farmaceutiche, organizzazioni di ricerca a contratto e centri di sperimentazione.

Prima di indicare quali cautele risultano idonee a seguito del complesso procedimento curato dal Garante, sono necessarie alcune premesse sulla natura dei dati trattati, sul ruolo dei promotori e degli altri soggetti coinvolti nelle sperimentazioni cliniche di medicinali rispetto al trattamento dei medesimi dati, nonché sul quadro normativo di base al quale occorre fare riferimento per un trattamento lecito e corretto dei dati.

2. NORMATIVA APPLICABILE

Gli studi condotti nell'ambito della sperimentazione clinica devono essere gestiti nel rispetto dei princìpi etici i quali traggono origine dalla Dichiarazione di Helsinki (fatta nel giugno 1964 e successive modificazioni), dei requisiti previsti dagli standard internazionali di buona pratica clinica (Gcp) adottati anche dall'Unione europea (e recepiti nell'ordinamento italiano, v. d.lg. 6 novembre 2007, n. 200; d.lg. 24 giugno 2003, n. 211; d.m. 15 luglio 1997 e, da ultimo, d.m. 21 dicembre 2007) e delle procedure operative standard delle società promotrici (Sop). Il centro di sperimentazione deve condurre lo studio in conformità al protocollo e alle procedure operative standard del promotore e non può discostarsi in alcun modo da essi, né apportarvi modifiche, senza

accordo con il promotore stesso. Ciò, eccetto casi eccezionali correlati al sorgere di rischi immediati per gli individui inclusi nella sperimentazione o a cambiamenti implicanti solo aspetti marginali dello studio (art. 10, comma 1, lettera a), d.lg. n. 211/2003; d.m. 15 luglio 1997, all. 1/1B punto 1.38, all. 1/4A punto 4.5.1. e 4.5.2, all. 1/5A punto 5.1 e all. 1/5B punto 5.20).

La normativa applicabile prevede diverse ipotesi in cui le informazioni medico/cliniche raccolte dal centro devono essere comunicate al promotore dello studio. Si tratta in primo luogo dei dati medico/clinici riferiti a ciascun partecipante allo studio i quali devono essere registrati dal medico su schede raccolta dati (Crf) trasmesse al promotore della sperimentazione (d.m. 15 luglio 1997, all. 1/1A punto 1.11). I centri sono tenuti, inoltre, a notificare al promotore le reazioni e gli eventi avversi (Ae e Adr), correlabili alla somministrazione del medicinale in sperimentazione o comunque al suo svolgimento, insieme a ogni altra informazione pertinente di follow-up (artt. 16, 17 e 18 d.lg. 24 giugno 2003, n. 211).

Al fine di tutelare l'identità delle persone coinvolte nello studio la medesima normativa prevede che il centro partecipante alla sperimentazione debba assegnare un codice di identificazione a ciascun interessato, al momento del suo coinvolgimento, e utilizzarlo al posto del relativo nominativo in ciascuna comunicazione al promotore di dati collegati allo studio (d.m. 15 luglio 1997, all. 1/1B punto 1.58 e all. 1/4B punto 4.11.1, v. anche art. 16, comma 5, d.lg. n. 211/2003). Una lista, che consente di associare ai codici i dati nominativi dei pazienti, è detenuta esclusivamente da ciascun centro di sperimentazione che la custodisce come documento riservato essenziale alla conduzione dello studio clinico (d.m. 15 luglio 1997, all. 1/1A punti 1.21 e 1.23, all. 1/2 punto 2.11, all. 1/4B punto 4.9.4 e 4.9.5, all. 1/5A punto 5.5.12, all. 1/8 punto 8.1 e 8.4.3).

Anche le schede raccolta dati, le segnalazioni e i rapporti relativi agli eventi e alle reazioni avversi, in quanto documenti essenziali alla conduzione dello studio, devono essere conservati, in base alla citata normativa, sia presso il promotore, sia presso i singoli centri, per un periodo di tempo non inferiore a sette anni dal completamento della sperimentazione, ovvero per un periodo più lungo richiesto da altre disposizioni applicabili o da un accordo tra il promotore e detti centri (art. 18 d.lg. n. 200/2007; d.lg. n. 219/2006, all. 1, punto 5.2, lett. c); d.m. 15 luglio 1997, all. 1/4B, punto 4.9.4, 4.9.5, 5.5.11 e 5.5.12).

3. NATURA DEI DATI TRATTATI

I promotori hanno sviluppato in gener e specifiche pr ocedure interne per consentir e ai medici sperimentatori di codificar e i dati medico/clinici delle persone coinv olte nello studio: solitamente, si utilizzano codici numerici che consentono di identificare univocamente i singoli interessati all'interno dello stesso studio, senza utilizzare il nominativo, l'indirizzo o numeri di identificazione personale.

Tuttavia, alcuni promotori stabiliscono nel pr otocollo dello studio che i medici sperimentatori debbano registrare sulle schede raccolta dati e sulle segnalazioni di r eazioni e eventi avversi -da trasmettere ai primi- le iniziali del nome e cognome dei singoli individui par tecipanti, oltre ai rispettivi codici identificativi. Inoltre, in base alle finalità della ricerca e alle caratteristiche dello studio, il protocollo può prevedere che i medici raccolgano informazioni ulteriori rispetto ai dati medico/clinici riferiti agli interessati, quali dati di carattere demografico (data di nascita e/o età, sesso, origine etnica, peso e statura) o r elativi alla storia medica dei soggetti, agli stili di vita o alla vita sessuale. Queste informazioni, riportate sui documenti essenziali alla conduzione dello studio, sono conservate dai centri partecipanti e dal promotore per un periodo di tempo che, a seconda della disciplina applicabile, può esser e collegato all 'intera durata dell 'autorizzazione all'impiego del medicinale nei diversi Paesi.

Sebbene sia previsto che soltanto ciascun centro abbia la disponibilità della lista che consente di associare il nominativ o della persona al r elativo codice identificativ o e che il pr omotore non debba venire a conoscenza della sua identità, quest 'ultimo, tramite propri collaboratori addetti al monitoraggio, nell 'ambito delle visite effettuate pr esso il centr o di sperimentazione v olte a controllare che lo studio è effettuato in osservanza del protocollo, ha tuttavia accesso sotto il controllo dei medici alla documentazione sanitaria originale delle persone coinvolte nello studio (per verificare l'accuratezza e la completezza dei dati), nonché alla lista contenente i dati nominativi degli interessati (per controllare le procedure riguardanti l'acquisizione del consenso informato).

Va, inoltre, rilevato che tra le informazioni raccolte nel corso degli studi in esame compaiono, in gener e, uno o più elementi specifici caratteristici dell 'identità delle persone coinv olte (ivi compresa la statura o par ticolari patologie). Come confermato dalle indicazioni formulate dal Gruppo dei garanti europei nel Parere n. 4/2007 (Wp 136) sulla definizione di dato personale,

la combinazione di tali elementi è suscettibile di consentire il riconoscimento dell'interessato (ad esempio, mediante combinazione delle iniziali del nome e del cognome della persona con la data di nascita o con la sua collocazione geografica desumibile dai dati identificativi del centro di sperimentazione e del medico sperimentatore).

Le modalità di codifica previste dai promotori rappresentano una specifica cautela adottata in applicazione delle disposizioni normative vigenti a tutela della riservatezza degli individui partecipanti a uno studio clinico che però non è, di per sé, tale da rendere anonimi i dati oggetto di trattamento nell'ambito della sperimentazione (artt. 16, comma 5, d.lg. n. 211/2003; d.m. 15 luglio 1997, all. 1/1B punto 1.58 e all. 1/4B punto 4.11.1; v. anche autorizzazione del Garante n. 2/2008 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, specie punto 1.2, lett. a), disponibile sul sito Internet dell'Autorità, doc. web n. 1529389). Le predette modalità di utilizzo del codice identificativo mirano, del resto, a consentire, in base alla specifica disciplina applicabile, l'identificazione della singola persona in casi determinati; ad esempio, per consentire al medico sperimentatore, che è il solo ad avere un contatto diretto con il paziente, di modificare o interrompere la terapia farmacologica somministrata in caso di eventi o reazioni avversi; oppure, per permettere agli addetti al monitoraggio di controllare, per conto del promotore, l'accuratezza e la completezza delle informazioni raccolte verificandone la corrispondenza con quelle contenute nella documentazione medica originale degli individui partecipanti; o, ancora, per consentire al promotore di utilizzare le informazioni raccolte per difendere i propri diritti nell'ambito di eventuali azioni legali. Analogamente, ai fini delle valutazioni da operare sull'identificabilità, vanno tenuti in considerazione il tempo di conservazione della lista di identificazione, gli eventuali rischi di disfunzione o malfunzionamento delle misure tecnico-organizzative eventualmente adottate per la custodia e la sicurezza dei dati e quelli di violazione delle regole di riservatezza e confidenzialità previste dalle disposizioni normative applicabili (artt. 3, comma 1, lett. c) e 11, comma 3, d.lg. n. 211/2003), nonché le precauzioni che gli addetti al monitoraggio sono tenuti a utilizzare per mantenere riservata l'identità delle persone che si sottopongono alla sperimentazione (d.m. 15 luglio 1997, all. 1/1A punto 1.21 e all. 1/2, punto 2.11).

La quantità e la tipologia di informazioni fornite al promotore, le modalità di trattamento previste e le diverse categorie di soggetti che possono accedere ai dati della sperimentazione com-

portano, quindi, la possibilità di identificare gli interessati, sia pure indirettamente, mediante il riferimento ad altre informazioni detenute dal promotore medesimo o a qualsiasi altra informazione non necessariamente nella disponibilità di quest'ultimo, ma detenuta da terzi. Ciò, considerando, in conformità alla disciplina comunitaria, l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal promotore, come pure da soggetti terzi, per identificare gli interessati (considerando 26 della direttiva 95/46/Ce).

Pertanto, le informazioni collegate al codice identificativo di ciascun paziente sono da ritenere dati personali idonei a rivelare lo stato salute e, in qualche caso, la vita sessuale del singolo interessato (artt. 2, al. 1, lett. a) e 8 direttiva 95/46/Ce; art. 4, comma 1, lett. b) e d), del Codice). La loro acquisizione da parte del promotore nell'ambito delle sperimentazioni cliniche e le successive attività svolte su questi ultimi configurano un trattamento di dati al quale è applicabile la disciplina del Codice sulle informazioni sensibili (art. 26), nonché le ulteriori cautele poste a tutela dei diritti e della riservatezza degli interessati dall'autorizzazione del Garante n. 2/2008 al trattamento dei dati sulla salute e sulla vita sessuale (Provv. 19 giugno 2008, n. 33, doc. web n. 1529389) e, ove applicabile, dall'autorizzazione del Garante al trattamento dei dati genetici (Provv. 22 febbraio 2007, doc. web n. 1389918).

4. NOTIFICAZIONE

Alcuni trattamenti effettuati nell'ambito delle sperimentazioni cliniche di medicinali sono soggetti all'obbligo di notificazione al Garante. Si tratta, in particolare, dei trattamenti di dati che ricadono nelle ipotesi considerate dall'art. 37, comma 1, del Codice, vale a dire quelli relativi a dati genetici, oppure effettuati a fini di indagine epidemiologica (art. 37, comma 1, lett. a) e b)). Il Garante ha sottratto dall'obbligo di notificazione alcuni tra i trattamenti che rientrano in tali ipotesi, individuando i presupposti in base ai quali non devono essere notificati i trattamenti riguardanti dati genetici o finalizzati a indagini epidemiologiche effettuati da esercenti le professioni sanitarie anche in forma associata (Provv. 31 marzo 2004, doc. web n. 852561). A proposito di tali categorie di trattamenti, va nuovamente rilevato che l'esonero disposto da questa Autorità opera soltanto nei riguardi di quelli eventualmente effettuati da medici sperimentatori per attività di cura della salute associate alle sperimentazioni cliniche, sempre che si tratti di trat-

tamenti non sistematici e non organizzati in banche dati accessibili a terzi per via telematica. Si pensi, ad esempio, al caso del medico che, nell'ambito delle visite o degli accertamenti diagnostici previsti in uno studio clinico, venga a conoscenza e tratti saltuariamente, senza trasmetterle al committente dello studio, informazioni di tipo genetico riguardanti le malattie ereditarie dei pazienti coinvolti, a fini di cura della salute o di tutela dell'incolumità fisica degli interessati (cfr. Nota 26 aprile 2004, doc. web n. 996680).

5. TITOLARITÀ DEI TRATTAMENTI FINALIZZATI ALLA SPERIMENTAZIONE

Risulta essenziale verificare quale rapporto intercorre tra i promotori di sperimentazioni cliniche e i centri di sperimentazione, per ciò che riguarda il trattamento dei dati personali. In questo quadro, occorre approfondire il ruolo effettivamente svolto da tali società per quanto concerne l'individuazione delle finalità e delle modalità del trattamento, anche alla luce delle delucidazioni fornite dal Garante a proposito della figura del "titolare" e del "responsabile del trattamento" (cfr. Parere 18 maggio 2000, doc. web n. 30935).

Al riguardo, va evidenziato che il promotore, prima dell'avvio della sperimentazione, identifica i possibili centri partecipanti verificandone l'idoneità e il relativo interesse; predispone il protocollo da osservare nel corso dello studio; quindi, impartisce ai centri le necessarie direttive sul trattamento dei dati, ivi compresi i profili relativi alla loro custodia e sicurezza, nonché le istruzioni relative alle modalità di utilizzo dei sistemi informativi eventualmente previsti, e, se necessario, forniti al centro; verifica poi, a mezzo di propri collaboratori, l'osservanza del protocollo e delle proprie procedure interne da parte del centro; predispone i documenti da impiegare per informare le persone partecipanti e per ottenerne il consenso anche per ciò che riguarda il trattamento dei dati che li riguardano; infine, avverte i centri quando non è più necessario conservare la documentazione relativa allo studio.

Il promotore non effettua, quindi, alcuna attività di raccolta diretta dei dati, né può interloquire con gli individui inclusi nella sperimentazione; compiti, questi, spettanti ai medici sperimentatori. Tuttavia, il promotore acquisisce, come detto, in diverse ipotesi i dati dei pazienti raccolti dai centri e sugli stessi effettua diverse operazioni di trattamento; tramite i propri collaboratori addetti al monitoraggio esamina, infatti, presso i centri le informazioni contenute nella docu-

mentazione medica originale e nella lista di identificazione delle persone coinvolte nello studio; è destinatario dei dati registrati da ciascun centro sulle schede raccolta dati e sulle segnalazioni di reazioni e eventi avversi; ne cura direttamente, ovvero tramite soggetti esterni ai quali può demandare alcuni o tutti i compiti in materia di sperimentazione, il loro inserimento sul database, nonché il controllo, la validazione e la successiva elaborazione statistica dei dati al fine di conseguire i risultati dello studio.

D'altra parte, va rilevato che il centro non è assoggettato a vincoli di subordinazione nei confronti del promotore: accetta il protocollo concordandone con il promotore alcuni aspetti, compresi quelli relativi alla formulazione del consenso informato delle persone partecipanti in ottemperanza al parere del comitato etico di riferimento; esegue la sperimentazione con propria autonomia organizzativa, sebbene nel rispetto del protocollo, delle procedure operative standard e delle direttive del promotore; per l'esecuzione della sperimentazione si avvale di collaboratori che ritiene idonei ed è responsabile del loro operato; fornisce l'informativa alle persone coinvolte nello studio e acquisisce il loro consenso anche per ciò che attiene al trattamento dei dati che le riguardano; permette che i collaboratori del promotore accedano alla documentazione medica originale dei soggetti coinvolti per svolgere le attività di monitoraggio; gestisce e custodisce sotto la propria responsabilità tale documentazione.

Dalla ricostruzione delle attività svolte anche nell'ambito degli accertamenti ispettivi effettuati, i singoli centri di sperimentazione e i promotori hanno in genere responsabilità distinte nell'ambito degli studi clinici e si configurano, quindi, quali autonomi titolari o, a seconda dei casi, contitolari del trattamento (art. 28 del Codice). Per poter effettuare lecitamente il trattamento dei dati relativi alle sperimentazioni, tali soggetti sono per tanto tenuti al rispetto delle disposizioni del Codice e delle prescrizioni della citata autorizzazione generale del Garante con particolare riferimento ai profili relativi alle modalità di trattamento e ai requisiti dei dati, alla notificazione all'Autorità, alla designazione degli incaricati e di eventuali responsabili, nonché alla custodia e sicurezza delle medesime informazioni (artt. 11, 29, 30, 31-35, 37 e 38 del Codice; v. anche autorizzazione n. 2/2008 cit., specie punto 1.2). La trasmissione dei dati dello studio da parte dei centri di sperimentazione ai promotori configura una vera e propria "comunicazione" di dati e un trattamento di dati da parte di terzi, i quali vanno indicati nominativamente

e distintamente nell'informativa agli interessati e nel modello di consenso, anche per ciò che riguarda l'esercizio del diritto di accesso e degli altri diritti previsti dagli artt. 7 e 8 del Codice (artt. 13, 23 e 26 del Codice).

6. ALTRI SOGGETTI CHE INTERVENGONO NELLA SPERIMENTAZIONE DEI FARMACI

Il promotore può stipulare un contratto con soggetti esterni (organizzazioni di ricerca a contratto, laboratori di analisi, ecc.) per demandare loro alcuni, o tutti i compiti e le funzioni di sua competenza inerenti alle sperimentazioni di farmaci, specificandoli per iscritto (d.m. 15 luglio 1997, all. 1/5A, punto 5.2). In tal caso questi soggetti, i quali possono essere singole persone fisiche ovvero società, istituzioni e altri organismi, possono svolgere nell'ambito degli studi clinici attività che, a seconda delle mansioni di volta in volta affidate, comportano il trattamento di dati personali riferiti ai singoli individui inclusi nelle sperimentazioni, come accade nelle ipotesi in cui essi vengano incaricati del monitoraggio degli studi, dell'inserimento, della validazione o dell'analisi statistica dei dati, ovvero della farmacovigilanza.

In tutte queste ipotesi è necessario che il promotore definisca chiaramente, nei contratti di affidamento o in altri atti idonei, il ruolo svolto nel trattamento dei dati personali da eventuali collaboratori esterni ai quali demanda attività o parti di attività inerenti agli studi clinici (artt. 28, 29 e 30 del Codice).

Nell'ambito delle sperimentazioni questi soggetti eseguono generalmente attività per conto e, in alcuni casi, in nome del promotore, nel rispetto delle modalità operative standard di quest'ultimo, o di proprie procedure visionate e approvate dal promotore stesso, o vvero di puntuali direttive di volta in volta impartite per iscritto da quest'ultimo. A tal fine, il promotore espleta spesso un'attività di formazione specifica nei confronti di tali collaboratori e, talvolta, si riserva il diritto di esprimere il proprio gradimento sui singoli. I medesimi soggetti possono inoltre utilizzare le informazioni e i documenti eventualmente ottenuti dai centri di sperimentazione nell'ambito dello studio soltanto in funzione dell'espletamento delle mansioni loro delegate; a conclusione della collaborazione, consegnano di regola al promotore tutte le informazioni e la documentazione che ne è conseguita.

Con specifico riferimento alle attività di monitoraggio, i promotori di studi clinici possono

avvalersi, come detto, non solo di personale interno all'azienda, ma anche di collaboratori esterni. In entrambi i casi, gli addetti al monitoraggio (clinical study monitor) vengono selezionati, nominati e addestrati in modo specifico dal promotore che stabilisce l'estensione e il tipo di monitoraggio da effettuare; nello svolgimento della loro attività sono tenuti a osservare le procedure del promotore e le sue specifiche istruzioni; sono inoltre soggetti al controllo del promotore medesimo al quale devono sottoporre un rapporto scritto dopo ogni visita ai centri di sperimentazione o dopo ogni comunicazione riguardante la sperimentazione stessa (d.m. 15 luglio 1997, all. 1/5 punto 5.18).

La relazione fra i promotori, da un lato e, dall'altro, i soggetti esterni ai quali vengono affidate alcune, o tutte le mansioni riguardanti gli studi clinici (ivi compresi gli addetti al monitoraggio) vanno utilmente inquadrate nell'ambito di un rapporto fra "titolare" e "incaricati" (unicamente persone fisiche) o, eventualmente, in base al grado di autonomia da osservare nel trattamento dei dati, "responsabili del trattamento" (persone fisiche o giuridiche). Tali soggetti devono quindi essere designati, in conformità alle disposizioni del Codice sugli incaricati e sui responsabili, e ricevere idonee istruzioni alle quali attenersi nel trattamento dei dati della sperimentazione (artt. 29 e 30).

I soggetti che, in quanto collaboratori dei promotori, accedono ai dati personali delle persone incluse nello studio per le finalità della sperimentazione devono essere inoltre menzionati, anche per categorie, nell'informativa da fornire agli interessati; qualora vengano designati più responsabili, occorre indicare anche gli estremi identificativi di almeno uno di essi, nonché le modalità per reperire, anche on-line, il loro elenco aggiornato (art. 13 del Codice).

Diversamente, qualora i promotori ritengano, in base alla legge, di non poter designare i soggetti esterni di cui si avvalgono quali "incaricati" o "responsabili", in quanto i ruoli svolti da questi non possono essere ricondotti alle predette figure previste dal Codice, il flusso delle informazioni riferite agli individui partecipanti di cui siano eventualmente destinatari tali collaboratori costituirebbe una comunicazione di dati personali che potrebbe essere effettuata lecitamente in presenza del consenso specifico e informato degli interessati o di altro presupposto equipollente (artt. 11, comma 1, lett. a), 13, 23 e 26 del Codice).

Analoghe cautele devono essere adottate dai centri di sperimentazione nel caso in cui essi deman-

dino attività o parti di attività inerenti agli studi clinici a soggetti esterni quali, ad esempio, laboratori di analisi (artt. 13, 29 e 30 del Codice, autorizzazione del Garante al trattamento dei dati genetici del 22 febbraio 2007, doc. web n. 1389918, in particolare punti 4.3, 8 e 9).

I promotori devono prestare, comunque, particolare attenzione nella scelta dei soggetti, responsabili e incaricati, ai quali affidare, ai sensi degli artt. 29 e 30 del Codice, alcune o tutte le mansioni inerenti alle sperimentazioni di farmaci, specie con riferimento al monitoraggio dello studio, assicurandosi che essi possiedano requisiti di esperienza, capacità e affidabilità tali da fornire idonee garanzie del pieno rispetto delle istruzioni da impartire e delle regole di riservatezza e confidenzialità previste dalla disciplina in materia di protezione di dati personali e dalle disposizioni di settore. Gli addetti al monitoraggio devono essere sottoposti a regole di condotta analoghe al segreto professionale. Il loro processo di designazione deve prevedere la frequenza di una specifica attività formativa concernente l'illustrazione dei rischi e delle responsabilità derivanti dal trattamento di queste informazioni, le istruzioni da rispettare per la loro custodia e sicurezza, nonché le regole di riservatezza e confidenzialità previste dalle disposizioni normative applicabili (artt. 3, comma 1, lett. c) e 11, comma 3, d.lg. n. 211/2003; artt. 11, 29, 30, 31 e ss. d.lg. n. 196/2003) e le specifiche precauzioni da utilizzare per tutelare l'identità degli interessati anche nei riguardi dello stesso promotore (d.m. 15 luglio 1997, all. 1/1A punto 1.21 e all. 1/2, punto 2.11).

7. INFORMATIVA AI PAZIENTI

I promotori, di regola, individuano le informazioni da comunicare alle persone coinvolte nello studio e la procedura da seguire per raccogliere il loro consenso tramite i centri di sperimentazione, anche per ciò che riguarda il trattamento dei dati che li riguardano, per consentirne l'esame da parte dei comitati etici interessati (artt. 6, 7, 8 e 11 d.lg. n. 211/2003).

Tuttavia, ritenendo erroneamente di non dover applicare la disciplina di protezione dei dati alle informazioni riconducibili agli individui inclusi nella sperimentazione, alcuni promotori invitano i centri a informare i pazienti interessati che i dati che li riguardano saranno trasmessi dal medico dello studio a chi lo ha commissionato esclusivamente in forma anonima. Questa indicazione, oltre a essere erronea, non consente alle persone interessate di comprendere quali siano

i ruoli effettivamente svolti dal promotore e dagli altri soggetti, della cui collaborazione questo eventualmente si avvalga, riguardo al trattamento dei dati.

Così formulata, l'informativa agli individui partecipanti in sperimentazioni cliniche è, quindi, inidonea ai sensi del Codice (art. 13); non permette altresì agli interessati di esprimere una volontà consapevole riguardo al fatto che i trattamenti effettuati presso il promotore o i soggetti che con esso eventualmente collaborano (anche al di fuori del territorio nazionale) concernono informazioni che, seppure codificate, come sopra evidenziato, sono riconducibili ai medesimi interessati.

L'informativa da fornire agli interessati tramite i centri di sperimentazione deve invece comprendere, anche con formule sintetiche, ma pur sempre agevolmente comprensibili, indicazioni specifiche relative a:

a. la natura dei dati trattati dal promotore e la circostanza che tali dati vengono trasmessi all'estero;
b. il ruolo effettivamente svolto dal promotore riguardo al trattamento dei dati e le finalità e modalità di quest'ultimo;
c. i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di incaricati o di responsabili;
d. l'esercizio del diritto d'accesso e gli altri diritti in materia di dati personali nei confronti del promotore e degli altri soggetti eventualmente destinatari dei dati (artt. 7 e 8 del Codice).

Al fine di agevolare l'individuazione degli elementi essenziali da precisare nell'informativa, il Garante individua nel prospetto allegato (all. n. 1) un modello di riferimento che potrà essere utilizzato facoltativamente dai promotori per adempiere, tramite i centri di sperimentazione, all'obbligo dell'informativa, in armonia con i princìpi di semplificazione, armonizzazione ed efficacia previsti dal Codice nel quadro di un elevato livello di tutela dei diritti degli interessati (art. 2 del Codice). Nelle ipotesi in cui lo studio preveda il trattamento di informazioni genetiche (ad esempio, nelle indagini farmacogenetiche o farmacogenomiche) tali elementi devono essere integrati da indicazioni chiare in ordine a profili specifici dell'utilizzo di dati genetici e di campioni biologici individuati nella citata autorizzazione del Garante (punto 5 aut. 22 febbraio 2007, doc. web n. 1389918; cfr. anche d.m. 21 dicembre 2007, appendice 14).

Inoltre, deve essere cura dei centri di sperimentazione garantire che il personale coinvolto nelle sperimentazioni cliniche e, in particolare, nei colloqui preliminari volti all'acquisizione del consenso informato, sia formato adeguatamente anche sugli aspetti rilevanti della disciplina sulla protezione dei dati personali, in modo da essere in grado di spiegare accuratamente e con completezza agli interessati gli elementi essenziali riguardanti il trattamento dei dati. I promotori, nell'individuare i centri presso i quali condurre sperimentazioni cliniche, devono verificare l'adeguatezza del personale del centro a gestire tale procedura predisponendo, ove necessario, appositi interventi formativi. Il profilo della formazione andrebbe considerato anche dai comitati etici nelle valutazioni relative all'idoneità del medico sperimentatore e dei suoi collaboratori.

8. CONSENSO AL TRATTAMENTO DEI DATI

Anche il modello che i centri di sperimentazione devono sottoporre agli interessati per acquisire le dichiarazioni di consenso al trattamento dei dati che li riguardano viene di regola predisposto dai promotori e sottoposto all'esame dei comitati etici interessati (artt. 6, 7, 8 e 11 d.lg. n. 211/2003).

Le formule solitamente utilizzate per la manifestazione del consenso si limitano ad autorizzare il medico a far esaminare la documentazione medica originale delle persone che si sottopongono alla sperimentazione da parte del personale del promotore addetto al monitoraggio (o da personale esterno da questi delegato), dei componenti del comitato etico e delle autorità sanitarie competenti, al fine di verificare le procedure dello studio e/o l'accuratezza dei dati raccolti (d.m. 15 luglio 1997, all. 1/4B punto 4.8.10). Tali formule non consentono, invece, agli interessati di esprimere la propria volontà circa gli ulteriori trattamenti di dati effettuati presso lo sponsor e/o i soggetti che, anche all'estero, collaborano eventualmente con esso nell'ambito della sperimentazione.

Il promotore e i suoi eventuali collaboratori non possono utilizzare lecitamente i dati personali degli individui partecipanti allo studio clinico se non provvedono ad acquisire previamente dagli interessati, tramite i centri di sperimentazione, idonee e specifiche manifestazioni di consenso riguardo ai trattamenti di dati da essi effettuati (artt. 23 e 26 del Codice). Per facilitare anche tale adempimento da parte dei promotori, in armonia con i citati princìpi di semplificazione, armonizzazione ed efficacia, è individuata nell'allegato n. 1 anche una formula di riferimento

per l'acquisizione del consenso, da sottoporre agli interessati, unitamente al modello d'informativa, tramite i centri di sperimentazione.

Particolare attenzione deve essere prestata anche alle modalità con cui il consenso degli interessati viene acquisto, specie quando si tratta di persone che, per il loro particolare stato di vulnerabilità, sono suscettibili di essere sottoposti a forme di coercizione o influenza tali da ostacolare la libera espressione del loro consenso. Si pensi a pazienti affetti da malattie incurabili o in situazioni di emergenza, a persone indigenti o ospitate nelle case di riposo o, ancora, ad appartenenti a gruppi "strutturati gerarchicamente", come gli studenti di medicina, il personale subordinato di un ospedale o di un laboratorio, i dipendenti di una società farmaceutica, ecc. In tali casi, oltre ad adottare le specifiche cautele richieste dalla normativa di settore (d.m. 15 luglio 1997, all. 1/1B punto 1.61 e all. 1/4B punto 4.8), è opportuno utilizzare procedure per acquisire il consenso informato degli interessati che non si limitino ad approcci meramente formali e individualizzati con i singoli individui, organizzando, ad esempio, momenti di confronto con la generalità o con gruppi di partecipanti, o coinvolgendo le associazioni, anche locali, di pazienti interessati.

9. ESERCIZIO DEI DIRITTI DI CUI ALL'ART. 7 DEL CODICE

Le persone partecipanti a sperimentazioni cliniche di medicinali possono esercitare in ogni momento i diritti di cui all'art. 7 del Codice, tra i quali quello di accedere ai dati che li riguardano e di ottenerne la comunicazione in forma intelligibile, ovvero l'integrazione, l'aggiornamento o la rettifica, rivolgendosi direttamente al centro di sperimentazione o, per il tramite del medico sperimentatore (che è a conoscenza della loro identità e, mediante l'accesso alla lista di identificazione, può individuare il codice identificativo di ciascun interessato), al promotore.

Quest'ultimo, come pure il centro di sperimentazione, anche per il tramite dei rispettivi responsabili, eventualmente designati, qualora siano destinatari di simili istanze (per la presentazione delle quali non sono, peraltro, richieste particolari formalità) devono fornire senza ritardo all'interessato un riscontro compiuto e analitico (artt. 7, 8, 9, 10 e 146 del Codice). In particolare, va fornito riscontro alle richieste di accesso ai dati personali estrapolando dagli archivi le informazioni detenute e comunicandole all'interessato con modalità tali da renderne agevole la comprensione, nonché, se richiesto, trasponendole su supporto cartaceo o informatico, non potendo opporre rifiuto

se non nei casi espressamente previsti dal Codice (art. 8). In tema di ricerche in ambito medico, biomedico ed epidemiologico il principio alla base della disciplina in materia è che il riscontro a istanze di integrazione, aggiornamento e rettificazione dei dati può essere fornito annotando le modifiche richieste dall'interessato senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca (art. 110, comma 2, del Codice; art. 16, comma 2, codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, allegato A.4. al Codice, doc. web n. 1038384)).

Dal momento che la partecipazione allo studio clinico è su base volontaria, gli interessati possono interrompere in ogni momento e senza fornire alcuna giustificazione la loro partecipazione allo studio (art. 3, comma 1, lett. b) e c) d.lg. n. 211/2003; d.m. 15 luglio 1997, all. 1/1B punto 1.28 e all. 1/4B punto 4.8; d.m. 21 dicembre 2007, all. 1 punto 6.1.2.5; art. 7, comma 4, lett. a), del Codice). In questo caso, non è più possibile raccogliere ulteriori dati che riguardano gli interessati e i campioni biologici eventualmente prelevati e conservati in una forma che consente di identificarli vanno distrutti (punto 6, aut. al trattamento dei dati genetici del 22 febbraio 2007, doc. web n. 1389918; v. anche d.m. 21 dicembre 2007, all. 2 punto 6.1.2.5). Resta impregiudicata la possibilità di utilizzare i dati eventualmente già raccolti per determinare, senza alterarli, i risultati della ricerca (v. al riguardo, par. 3.3 Raccomandazione del Consiglio d'Europa R(83)10 del 23 settembre del 1983 relativa alla protezione dei dati a carattere personale utilizzati a fini di ricerca scientifica e di statistiche; par. 6.1 Raccomandazione del Consiglio d'Europa (97)18 del 30 settembre 1997 relativa alla protezione dei dati personali raccolti e trattati per scopi statistici).

10. TRASFERIMENTO DI DATI ALL'ESTERO

Nelle sperimentazioni cliniche dei medicinali accade, frequentemente, che le informazioni e i campioni biologici degli individui partecipanti, raccolti dai medici sperimentatori in un Paese, vengano trasferiti a soggetti ubicati in altri Paesi, anche al di fuori dell'Unione europea, o siano resi accessibili a diverse categorie di soggetti aventi sede in tali Paesi. Ciò, avviene specialmente negli studi promossi da promotori che operano nell'ambito di gruppi multinazionali nei quali gli stessi promotori, gli addetti al monitoraggio dello studio, il laboratorio di analisi e gli altri soggetti esterni che collaborano con il promotore, possono avere sede in Paesi terzi.

Tali informazioni, in quanto riconducibili alle singole persone coinvolte nello studio, possono essere trasferite lecitamente in Paesi extra-Ue che non garantiscono un livello adeguato di protezione dei dati personali a condizione che i pazienti interessati ne siano stati previamente informati e abbiano manifestato per iscritto un consenso specifico (art. 43, comma 1, lettera a) del Codice), ovvero vengano adottate garanzie equipollenti e adeguate per i diritti degli interessati (art. 44, comma 1, lett. b) del Codice). In particolare, costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti degli interessati le clausole contrattuali standard per il trasferimento di dati personali a "responsabili del trattamento" residenti in Paesi terzi (cfr. decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/Ce e Provv. del Garante 10 aprile 2002 n. 3, doc. web n. 1065361), nonché quelle previste per il trasferimento di dati effettuati da un "titolare del trattamento" avente sede nell'Unione europea a un diverso "titolare" residente al di fuori del territorio europeo (cfr. decisione della Commissione europea del 15 giugno 2001, n. 2001/497/Ce e Provv. del Garante del 10 ottobre 2001, doc. web n. 42156; decisione del 27 dicembre 2004, n. 2004/915/Ce e Provv. del Garante del 9 giugno 2005, doc. web n. 1151949). Ai fini dell'utilizzazione delle citate clausole è necessario definire preventivamente, con chiarezza e precisione, i ruoli svolti dai soggetti nell'ambito del trasferimento dei dati e delle operazioni di trattamento effettuate in conformità ai parametri indicati (l'esportatore deve risultare effettivamente "titolare" del trattamento e, l'importatore, deve essere l'effettivo "responsabile" o "titolare" autonomo del trattamento), nonché specificare le attività principali di trattamento cui sottoporre le informazioni personali oggetto di trasferimento.

Per ciò che concerne il trasferimento di dati verso organizzazioni stabilite negli Stati Uniti d'America fornisce, parimenti, adeguate garanzie per l'interessato l'idonea adesione ai princìpi in materia di riservatezza contenuti nel cd. accordo del "Safe Harbor" (cfr. decisione della Commissione europea del 26 luglio 2000 n. 2000/520/Ce e Provv. del Garante del 10 ottobre 2001, doc. web n. 30939).

11. PERIODO DI CONSERVAZIONE E TRATTAMENTO DI DATI PER ULTERIORI FINI DI RICERCA

I dati e i campioni biologici delle persone che si sottopongono alle sperimentazioni devono essere conservati per un arco di tempo non superiore a quello necessario per conseguire le fina-

lità per le quali sono stati raccolti e trattati (art. 11, comma 1, lett. e) del Codice, aut. cit. del 22 febbraio 2007, doc. web n. 1389918). Al riguardo, la normativa applicabile alle sperimentazioni cliniche prevede che i documenti essenziali relativi allo studio (compresa la documentazione medica riferita ai singoli individui) debbano essere conservati presso il promotore e i centri partecipanti per almeno sette anni dopo il completamento della sperimentazione, ovvero per un periodo di tempo considerevolmente più lungo in conformità alla disciplina applicabile o agli accordi intervenuti il promotore medesimo e centri partecipanti (art. 18 d.lg. n. 200/2007; d.lg. n. 219/2006, all. 1, punto 5.2, lett. c); d.m. 15 luglio 1997, all. 1/4B, punti 4.9.4 e 4.9.5 e all. 1/5A, punti 5.5.11 e 5.5.12).

In termini generali, in applicazione della disposizione del Codice sopra richiamata sulla durata di conservazione, i dati devono essere conservati presso i soggetti esterni che eventualmente collaborano con il promotore per la gestione e l'analisi statistica, per il solo periodo di tempo non superiore a quello necessario per definire il rapporto finale della sperimentazione o pubblicare i risultati dello studio.

La possibilità di fissare un periodo di tempo più lungo rispetto a quello previsto dalla normativa applicabile per la conservazione dei medesimi dati presso il promotore e i centri partecipanti può, invece, essere valutata anche alla luce della durata dell'autorizzazione d'immissione in commercio del medicinale in sperimentazione o di eventuali ulteriori esigenze di analisi dei dati, connesse ad esempio, a nuove domande d'immissione in commercio o di estensione dell'autorizzazione, ovvero al manifestarsi di evidenze significative per la sicurezza dei pazienti.

I promotori di uno studio clinico possono utilizzare lecitamente in future attività di studio e di ricerca i dati e i campioni biologici riconducibili a ciascuna delle persone coinvolte, anche avvalendosi dei soggetti esterni che hanno collaborato con essi per l'esecuzione della sperimentazione, a condizione che gli interessati ne siano stati previamente e adeguatamente informati e abbiano manifestato per iscritto un consenso specifico e distinto rispetto a quello manifestato per lo studio principale (artt. 11, comma 1, lett. e), 13, 23, 26 e 99 del Codice; aut. del 22 febbraio 2007, doc. web n. 1389918).

12. CUSTODIA E SICUREZZA DEI DATI

A seguito degli appr ofondimenti, anche tecnici, sv olti nell'ambito degli accer tamenti ispettivi effettuati pr esso alcuni pr omotori e altri soggetti coinv olti nelle sperimentazioni, nonché di quelli effettuati, nell'ambito della consultazione pubblica, con i principali organismi interessati, sono stati individuati idonei accorgimenti e misure da porre a garanzia degli interessati nei trattamenti di dati effettuati per l'esecuzione di tali studi. La particolare delicatezza dei dati trattati nella sperimentazione impone l 'adozione di specifici accorgimenti tecnici per incr ementare il livello di sicurezza dei dati (ar t. 31 del Codice), senza pr egiudizio di ogni altra misura minima che ciascun titolar e del trattamento dev e adottare ai sensi del Codice (ar t. 33 e ss.). Ciò, con particolare riferimento alle operazioni di r egistrazione con str umenti elettr onici dei dati delle persone coinv olte nello studio pr esso i centri di sperimentazione, al lor o trasferimento in via telematica v erso un unico database pr esso il pr omotore o gli altri soggetti che sv olgono, per conto di quest 'ultimo, la v alidazione e l 'elaborazione statistica dei dati, nonché alla gestione della medesima banca dati.

In relazione a tali operazioni di trattamento, i promotori di sperimentazioni cliniche di medicinali, le organizzazioni di ricer ca a contratto e i centri di sperimentazione, ciascuno per la par te di propria competenza in relazione al ruolo ricoperto nel trattamento dei dati e alle conseguenti responsabilità ai fini dell'adozione delle misure di sicurezza, devono adottare:

a. laddove siano utilizzati sistemi di memorizzazione o archiviazione dei dati, idonei accorgimenti per garantir e la pr otezione dei dati r egistrati dai rischi di accesso abusiv o, furto o smarrimento parziali o integrali dei suppor ti di memorizzazione o dei sistemi di elaborazione por tatili o fissi (ad esempio, attrav erso l'applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppur e tramite l 'adozione di alt re misur e informatiche di protezione che rendano inintelligibili i dati ai soggetti non legittimati);

b. protocolli di comunicazione sicuri basati sull 'utilizzo di standar d crittografici per la trasmissione elettronica dei dati raccolti dai centri di sperimentazione al database centralizzato presso il promotore o gli altri soggetti che effettuano la successiva validazione ed elaborazione statistica dei dati;

c. con specifico riferimento al menzionato database:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento;
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati del trattamento;
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Il Garante si riserva, in relazione alle sperimentazioni cliniche multinazionali, di promuovere a livello comunitario e internazionale standard di sicurezza per i trattamenti di dati personali che prevedano un livello di protezione ancora più elevato in un quadro di armonizzazione delle misure e degli accorgimenti da adottare in tali ambiti per la custodia e la sicurezza dei dati.

13. ALTRE TIPOLOGIE DI STUDI CLINICI

Le indicazioni fornite nelle presenti "Linee-guida" a garanzia dei soggetti interessati possono, in linea generale, essere prese in considerazione come quadro unitario di riferimento per un uso lecito e corretto dei dati personali anche nell'ambito di altre tipologie di sperimentazioni cliniche, vale a dire quelle riguardanti i dispositivi medici (art. 7 d.lg 14 dicembre 1992, n. 507; art. 14 d.lg 24 febbraio 1997, n. 46; d.m. 2 agosto 2005) e quelle non promosse da società farmaceutiche o da altre strutture private per lo sviluppo industriale di un farmaco (cd. sperimentazioni "non aventi fini di lucro", cfr. art. 1 d.lg. n. 200/2007 e d.m. 17 dicembre 2004). In queste ipotesi, occorre verificare, innanzitutto, il ruolo dei soggetti coinvolti nello studio rispetto al trattamento dei dati (promotore, centro di sperimentazione, centro coordinatore, organizzazione di ricerca a contratto, laboratorio di analisi, ecc.) in modo da poter individuare il soggetto o i soggetti, titolari del trattamento, tenuti agli adempimenti previsti dal Codice in materia di notificazione, designazione di incaricati e di eventuali responsabili, consenso informato al trattamento dei dati, predisposizione di adeguate misure per la custodia e sicurezza dei dati, esercizio dei diritti di accesso e degli altri diritti riguardanti i dati personali. Occorre, inoltre, accertare, in base alle previsioni dello studio, eventuali flussi di dati, anche attraverso la loro messa a disposizione o consultazione (ad esempio, a fini di monitoraggio), verso soggetti esterni situati anche al di fuori dell'Unione europea, in modo da verificare la necessità di acquisire il

consenso specifico e informato degli interessati e/o di adottare garanzie equipollenti e adeguate (artt. 11, comma 1, lett. a), 13, 23, 26, 43 e 44 del Codice).

Vanno poi formulate in questa sede alcune precisazioni con riferimento ad altri studi, nei quali i medicinali sono prescritti e somministrati ai soggetti che accettano di partecipare secondo la normale pratica clinica (sperimentazioni "non interventistiche", v. art. 1 d.lg. n. 200/2007). Questi studi, cd. "osservazionali", qualora non siano strettamente associati ad attività di tutela della salute svolte da medici o organismi sanitari, ovvero -a differenza delle sperimentazioni cliniche sui medicinali- non possano ritenersi comparabili a tali attività in termini di ricaduta personalizzata sull'interessato, rientrano nell'ambito di applicazione delle previsioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (Allegato A.4. al Codice, doc. web n. 1038384) la cui osservanza, oltre a rappresentare un obbligo deontologico, costituisce condizione essenziale per la liceità e la correttezza del trattamento medesimo (art. 12, comma 3, del Codice). Anche nell'ambito di questi studi, il trattamento di informazioni medico/cliniche può essere effettuato, in linea generale, per gli scopi della ricerca con riferimento ai soli dati personali degli individui che vi acconsentono specificatamente dopo aver ricevuto un'idonea informativa sul trattamento dei dati (artt. 106, 107 e 110 del Codice; punto 1.2, lett. a) aut. n. 2/2008 cit.). Ciò, indipendentemente dal fatto che lo studio preveda di raccogliere queste informazioni direttamente presso gli interessati o presso terzi. In presenza di particolari e comprovate circostanze (di carattere etico, metodologico o di impossibilità organizzativa), dalle quali derivi l'impossibilità di informare gli interessati, il trattamento può essere effettuato, anche in assenza del loro consenso, a condizione che il programma di ricerca sia stato oggetto di motivato parere favorevole del competente comitato etico e venga ottenuta l'autorizzazione del Garante, che può essere rilasciata anche con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (artt. 110 ult. parte e 40 del Codice). Si pensi, ad esempio, ad alcuni studi di tipo retrospettivo in cui il tempo trascorso dal momento in cui i dati da analizzare sono stati raccolti, l'entità del campione da selezionare e le caratteristiche sulla base delle quali viene effettuato il campionamento (ad esempio, un gruppo di persone affette da patologie ad alta incidenza di mortalità) possono rendere ragionevolmente impossibile raggiungere gli interessati e fornire loro un'adeguata informativa.

Il Garante si riserva di adottare provvedimenti più specifici di prescrizione e di divieto che potranno derivare dalle verifiche di eventuali violazioni riguardanti singoli soggetti promotori, nonché di apportare alle presenti "Linee-guida" eventuali integrazioni riguardanti le concrete modalità di trattamento dei dati, anche alla luce dell'esperienza maturata nell'applicazione delle stesse e delle nuove tecnologie eventualmente intervenute.

ALLEGATO N. 1. INFORMATIVA E MANIFESTAZIONE DEL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI (1)

Titolari del trattamento e relative finalità

Il Centro di sperimentazione (indicare il nome del centro) e l'Azienda farmaceutica (indicare il nome del promotore), che ha commissionato lo studio che Le è stato descritto, ciascuno per gli ambiti di propria competenza e in accordo alle responsabilità previste dalle norme della buona pratica clinica (d.l. 211/2003), tratteranno i Suoi dati personali, in particolare quelli sulla salute e, soltanto nella misura in cui sono indispensabili in relazione all'obiettivo dello studio, altri dati relativi alla Sua origine, ai Suoi stili di vita e alla Sua vita sessuale (ecc.) (variabili da specificare a seconda delle caratteristiche dello studio), esclusivamente in funzione della realizzazione dello studio e a fini di farmacovigilanza.

A tal fine i dati indicati saranno raccolti dal Centro di sperimentazione e trasmessi all'Azienda farmaceutica e alle persone o società esterne che agiscono per loro conto, tra le quali ... (inserire gli estremi identificativi di almeno uno dei terzi cui i dati saranno trasmessi) anche in Paesi non appartenenti all'Unione europea che non garantiscono un adeguato livello di protezione dei dati personali (da inserire nel caso si preveda di trasferire i dati al di fuori dell'Ue specificando gli estremi identificativi dei destinatari). (2)

(1) Da sottoporre agli interessati unitamente al modulo di consenso informato che descrive le caratteristiche scientifiche dello studio, anche mediante integrazione dello stesso

(2) Quando non è possibile conoscere al momento della redazione dell'informativa l'elenco completo dei soggetti terzi a cui i dati saranno trasmessi anche in paesi extra-UE occorre specificare come e quando l'elenco completo verrà reso disponibile

Il trattamento dei dati personali relativi a ... (variabili da specificare a seconda delle caratteristiche dello studio) è indispensabile allo svolgimento dello studio: il rifiuto di conferirli non Le consentirà di parteciparvi (Indicare inoltre gli eventuali dati che possono invece essere forniti facoltativamente).

Natura dei dati

Il medico che La seguirà nello studio La identificherà con un codice: i dati che La riguardano raccolti nel corso dello studio, ad eccezione del Suo nominativo, saranno trasmessi all'Azienda farmaceutica, registrati, elaborati e conservati unitamente a tale codice, alla Sua data di nascita, al sesso, al Suo peso e alla Sua statura (tutte le variabili di cui sopra da precisare secondo le specifiche dello studio). Soltanto il medico e i soggetti autorizzati potranno collegare questo codice al Suo nominativo.

Modalità del trattamento

I dati, trattati mediante strumenti anche elettronici, saranno diffusi solo in forma rigorosamente anonima, ad esempio attraverso pubblicazioni scientifiche, statistiche e convegni scientifici. La Sua partecipazione allo studio implica che, in conformità alla normativa sulle sperimentazioni cliniche dei medicinali, il personale dell'Azienda farmaceutica o delle società esterne che eseguono per conto della prima il monitoraggio e la verifica dello studio, il Comitato etico e le autorità sanitarie italiane e straniere potranno conoscere i dati che La riguardano, contenuti anche nella Sua documentazione clinica originale, con modalità tali da garantire la riservatezza della Sua identità.

Esercizio dei diritti

Potrà esercitare i diritti di cui all'art. 7 del Codice (es. accedere ai Suoi dati personali, integrarli, aggiornarli, rettificarli, opporsi al loro trattamento per motivi legittimi, ecc.) rivolgendosi direttamente al centro di sperimentazione (indicare il nome di una persona fisica o di un ufficio responsabile e un recapito) o, per il suo tramite, all'azienda farmaceutica.

Potrà interrompere in ogni momento e senza fornire alcuna giustificazione la Sua partecipazione allo studio: in tal caso, i campioni biologici a Lei correlati verranno distrutti. Non saranno inoltre raccolti ulteriori dati che La riguardano, fermo restando l'utilizzazione di quelli eventualmente già raccolti per determinare, senza alterarli, i risultati della ricerca.

Consenso

Sottoscrivendo tale modulo acconsento al trattamento dei miei dati personali e al lor o trasferimento al di fuori dell'Unione europea (da inserire se effettuato specificando gli estr emi identificativi dei destinatari) per gli scopi della ricer ca nei limiti e con le modalità indicate nell'informativa fornitami con il pr esente documento.

Nome e Cognome dell'interessato (in stampatello): _____

Firma dell'interessato: _____

Data: _____

38. Linee-guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario (*)

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. Daniele De Paoli, segretario generale reggente;

Considerato che l'Autorità ha svolto alcuni approfondimenti istruttori su numerose iniziative –diversamente denominate– promosse da organismi sanitari pubblici e privati inerenti ai trattamenti di dati personali effettuati attraverso il Fascicolo sanitario elettronico (Fse);

Rilevata l'esigenza di individuare misure e accorgimenti necessari e opportuni da porre a garanzia dei cittadini interessati, in relazione ai trattamenti di dati che li riguardano;

Visto il provvedimento adottato dall'Autorità il 22 gennaio 2009 recante Linee-guida in tema di Fascicolo sanitario elettronico che è stato sottoposto alla preliminare consultazione del gruppo di lavoro, costituito presso il Ministero del lavoro, della salute e delle politiche sociali, per l'istituzione di un sistema nazionale di Fascicolo sanitario elettronico;

Viste le osservazioni formulate su tale provvedimento dal suddetto tavolo di lavoro con nota del 18 febbraio 2009 (prot. 0000603-P-18);

Rilevata l'opportunità che la prescrizione di tali misure e accorgimenti, allo stato individuati dal Garante nell'unito documento, sia preceduta da una consultazione pubblica dei soggetti e delle categorie interessate, in particolare degli organismi e professionisti sanitari pubblici e privati, dei medici di medicina generale e dei pediatri di libera scelta, degli organismi rappresentativi di operatori sanitari e delle associazioni di pazienti interessati, anche al fine di acquisire eventuali riscontri e osservazioni;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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

(*) Deliberazione n. 8 del 5 marzo 2009, Gazzetta Ufficiale 26 marzo 2009, n. 71 [doc. *web* n. 1598313], in inglese [doc. *web* n. 1608673]

Relatore il dott. Giuseppe Chiaravalloti;

DELIBERA:

a) di adottare l'unito documento che forma parte integrante della presente deliberazione ("Linee-guida in tema di Fascicolo sanitario elettronico e di dossier sanitario");

b) di avviare una consultazione pubblica sul documento di cui alla lettera a).

L'obiettivo della consultazione è acquisire osservazioni e commenti, in particolare da parte di organismi e professionisti sanitari pubblici e privati, dei medici di medicina generale e dei pediatri di libera scelta, di organismi rappresentativi di operatori sanitari e di associazioni di pazienti interessati.

Osservazioni e commenti potranno pervenire entro il 31 maggio 2009 all'indirizzo dell'Autorità di Piazza di Monte Citorio n. 121, 00186 Roma, ovvero all'indirizzo di posta elettronica:

fse@garanteprivacy.it

La presente deliberazione verrà pubblicata sul sito web del Garante www.garanteprivacy.it e verrà inviato un avviso all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia, affinché sia riportato sulla Gazzetta Ufficiale della Repubblica italiana.

Roma, 5 marzo 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Chiaravalloti

IL SEGRETARIO GENERALE REGGENTE
De Paoli

Linee-guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario

1. La sanità elettronica: profili generali

Nel quadro del processo di ammodernamento della sanità pubblica e privata sono in atto numerose iniziative volte a migliorare l'efficienza del servizio sanitario attraverso un ulteriore sviluppo delle reti e una più ampia gestione informatica e telematica di atti, documenti e procedure.

In tale contesto si collocano alcune iniziative volte ad archiviare, mediante nuove tecniche, la svariata documentazione di cui gli organismi sanitari si avvalgono a diverso titolo nei processi di cura dei pazienti come, ad esempio, le più recenti esperienze di informatizzazione della cartella clinica, documento sanitario che pure è regolato da specifiche disposizioni normative. Il trattamento dei dati utilizzati nell'ambito di tali iniziative è regolato già dal Codice sulla protezione dei dati personali (cfr., in particolare, artt. 75 e ss. e art. 20 del Codice).

Accanto a tali iniziative più generali emerge di recente un'attività più specifica che rientra anch'essa nel complesso delle azioni per modernizzare la realtà sanitaria, ma ha caratteristiche peculiari che ne rendono opportuna una considerazione in forma specifica.

La novità che si intende esaminare in questa sede in chiave autonoma riguarda la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica.

Questi dati e documenti possono presentare caratteristiche o sfumature diverse e sono da tempo oggetto di specifica attenzione nell'ambito della problematica del cosiddetto Fascicolo sanitario elettronico (di seguito Fse) e del cd. dossier sanitario (di seguito dossier). Nelle presenti Linee-guida per tali strumenti si ha riguardo all'insieme dei diversi eventi clinici occorsi ad un individuo, messo in condivisione logica dai professionisti o organismi sanitari che assistono l'interessato, al fine di offrirgli un miglior processo di cura.

La peculiarità della condivisione da parte di distinti soggetti delle delicate informazioni sanitarie che documentano un insieme di eventi di rilevanza medica occorsi a uno stesso individuo giustifica la formulazione di particolari considerazioni rispetto alla gestione cartacea di analoghi

documenti e alla più generale tematica dell'informatizzazione sanitaria.

Nelle more di un possibile intervento normativo che regoli alcuni aspetti di fondo, il Garante ritiene pertanto opportuno individuare un primo quadro di cautele, al fine di delineare per tempo specifiche garanzie e responsabilità, nonché alcuni diritti.

2. AMBITO DI APPLICAZIONE DELLE LINEE GUIDA

Il Fse e i dossier non risultano essere definiti a livello nazionale da norme di carattere primario o secondario. Ciò, comporta la necessità di utilizzare una definizione convenzionale del fenomeno che trae spunto anche da quanto emerso in sede europea nel Gruppo che riunisce le autorità garanti di protezione dei dati (cd. Gruppo Art. 29) (1).

Le considerazioni sviluppate nelle presenti linee guida sono applicabili al Fse e al dossier intesi, come detto, quali insieme di dati sanitari relativi di regola ad un medesimo soggetto e riportati in più documenti elettronici tra loro collegati, condivisibili da soggetti sanitari diversi, pubblici e privati.

Il Fse e il dossier contengono diverse informazioni inerenti allo stato di salute di un individuo relative ad eventi clinici presenti e trascorsi (es.: referti, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica. I dati personali sono collegati tra loro con modalità informatiche di vario tipo che ne rendono, comunque, possibile un'agevole consultazione unitaria da parte dei diversi professionisti o organismi sanitari che prendono nel tempo in cura l'interessato.

Alla luce di quanto emerso a livello nazionale ed, in particolare, dalle osservazioni del gruppo di lavoro costituito presso il Ministero del lavoro, della salute e delle politiche sociali, per l'istituzione di un sistema nazionale di Fascicolo sanitario elettronico, nelle presenti Linee-guida il suddetto insieme di dati sanitari risulta diversamente denominato in funzione del suo ambito di operatività. In particolare, si parla di dossier sanitario qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata) al cui interno operino più professionisti. Si intende invece per Fse il fascicolo formato

(1) Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (Cce) adottato il 15 febbraio 2007 consultabile sul sito: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_it.pdf

con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta). I dossier sanitari possono anche costituire, ad esempio, l'insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in una iniziativa di Fse regionale.

Il Fse dovrebbe essere costituito preferendo di regola soluzioni che non prevedano una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti o organismi sanitari che hanno preso in cura l'interessato.

In secondo luogo, provenendo i dati sanitari e i documenti riuniti nel Fse da più soggetti, dovrebbero essere adottate idonee cautele per ricostruire, anche in termini di responsabilità, chi ha raccolto e generato i dati e li ha resi disponibili nell'ambito del Fse.

Nel caso di Fse, venendo poi in considerazione documenti sanitari del tutto distinti tra loro, dovrebbe essere assicurato che ciascun soggetto che li ha prodotti autonomamente ne rimanga di regola l'unico titolare, anche se le informazioni sono -come detto- disponibili agli altri soggetti abilitati all'accesso (ad esempio -come spesso accade-, attraverso la condivisione, da parte di tutti i soggetti che prendono in cura l'interessato, dell'elenco degli eventi sanitari occorsi, elenco strutturato anche sotto forma di indici o di puntatori logici dei singoli episodi clinici).

In assenza di una previsione legislativa che preveda l'istituzione di tali strumenti per il perseguimento di finalità amministrative proprie delle regioni o di organi centrali dello Stato, le finalità che possono essere perseguite attraverso la costituzione del Fse o del dossier possono essere ricondotte esclusivamente a finalità di cura dell'interessato, ovvero ad assicurare un miglior processo di cura dello stesso attraverso la ricostruzione di un insieme -di regola su base logica- il più possibile completo della cronistoria degli eventi di rilievo clinico occorsi a un interessato relativi a distinti interventi medici.

A garanzia dell'interessato, le finalità perseguite dovrebbero essere ricondotte quindi solo alla prevenzione, diagnosi, cura e riabilitazione dell'interessato medesimo, con esclusione di ogni altra finalità (in particolare, per le attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, che possono essere, peraltro, espletate in vari casi anche senza la disponibilità di dati personali), ferme restando eventuali esigenze in ambito penale.

Qualora attraverso il Fse o il dossier si intendano perseguire anche talune finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria richiesta dall'interessato (es. prenotazione e pagamento di una prestazione), tali strumenti dovrebbero essere strutturati in modo tale che i dati amministrativi siano separati dalle informazioni sanitarie (2), prevedendo profili diversi di abilitazione degli aventi accesso agli stessi in funzione della differente tipologia di operazioni ad essi consentite.

Eventuali, future utilizzazioni anche parziali del Fse o del dossier per ulteriori fini di ricerca scientifica, epidemiologica o statistica dovrebbero avvenire in conformità alla normativa di settore ed essere oggetto di preventiva e specifica attenzione, anche nei casi in cui -come accade per taluni progetti di Fse esaminati- la tenuta dell'elenco degli eventi sanitari riguardante un determinato interessato sia demandata a un'infrastruttura regionale.

3. DIRITTO ALLA COSTITUZIONE DI UN FASCICOLO SANITARIO ELETTRONICO O DI UN DOSSIER SANITARIO

In base alle disposizioni contenute nel Codice dell'amministrazione digitale, deve essere assicurata la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando le tecnologie dell'informazione e della comunicazione nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82).

A ciò deve aggiungersi che allo stato delle notizie al momento acquisite dall'Autorità, non consta l'esistenza di una norma che obblighi gli organismi sanitari a costituire un Fse o un dossier, la cui introduzione deve ritenersi, pertanto, facoltativa.

Le finalità perseguite attraverso il Fse o il dossier, come sopra ricordato, sono generalmente riconducibili alla documentazione di una "memoria storica" degli eventi di rilievo sanitario relativi a un medesimo individuo consultabile dal medico curante.

Il trattamento dei dati personali effettuato mediante il Fse o il dossier, perseguendo le menzionate finalità di prevenzione, diagnosi, cura e riabilitazione, deve uniformarsi al principio di auto-

(2) Cfr. art. 22, comma 6, del Codice; regola 24 del Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B. al Codice

determinazione (artt. 75 e ss. del Codice). All'interessato dovrebbe essere consentito di scegliere, in piena libertà, se far costituire o meno un Fse/dossier con le informazioni sanitarie che lo riguardano, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista o organismo sanitario che li ha redatti, senza la loro necessaria inclusione in tali strumenti.

Il diritto alla costituzione o meno del Fse/dossier si dovrebbe quindi tradurre nella garanzia di decidere liberamente, sulla base del consenso, se acconsentire o meno alla costituzione di un documento che, come si è detto, raccoglie un'ampia storia sanitaria.

Affinché tale scelta sia effettivamente libera, l'interessato che non desideri che sia costituito un Fse/dossier dovrebbe poter accedere comunque alle prestazioni del Servizio sanitario nazionale e non avere conseguenze negative sulla possibilità di usufruire di prestazioni mediche.

Il consenso, anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura (cfr. art. 81 del Codice), deve essere autonomo e specifico.

In ragione delle finalità perseguite attraverso il Fse/dossier, dovrebbe essere illustrata all'interessato l'utilità di costituire e disporre di un quadro il più possibile completo delle informazioni sanitarie che lo riguardano, in modo da poter offrire un migliore supporto all'organismo sanitario, al medico e all'interessato stesso. Una conoscenza approfondita dei dati clinici, relativi anche al passato, può infatti contribuire ad una più efficace ricognizione degli elementi utili alle valutazioni del caso.

Tuttavia, dovrebbero essere previsti momenti distinti in cui l'interessato possa esprimere la propria volontà, attraverso un consenso di carattere generale per la costituzione del Fse e di consensi specifici ai fini della sua consultazione o meno da parte dei singoli titolari del trattamento (es. medico di medicina generale, pediatra di libera scelta, farmacista, medico ospedaliero).

Ferma restando l'indubbia utilità di un Fse/dossier completo, dovrebbe essere garantita la possibilità di non far confluire in esso alcune informazioni sanitarie relative a singoli eventi clinici (ad es., con riferimento a una specifica visita specialistica o alla prescrizione di un farmaco). Ciò, analogamente a quanto avviene nel rapporto paziente-medico curante, nel quale il primo può addivenire a una determinazione consapevole di non informare il secondo di certi eventi.

L'"oscuramento" dell'evento clinico (revocabile nel tempo) dovrebbe peraltro avvenire con modalità tali da garantire che, almeno in prima battuta, tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto

che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").

In tale quadro, alcuni progetti di Fse esaminati garantiscono l'esercizio della "facoltà di oscuramento" mediante una "busta elettronica sigillata" non visibile, apribile di volta in volta solo con la collaborazione dell'interessato, ovvero utilizzando codici casuali relativi a singoli eventi che non consentono di collegare tra loro alcune informazioni contrassegnate.

Il titolare del trattamento che intenda istituire il Fse/dossier anche con informazioni sanitarie relative a eventi clinici precedenti alla sua costituzione (es. referti relativi a prestazioni mediche pregresse) dovrebbe essere autorizzato preventivamente dall'interessato, lasciando libero quest'ultimo di esercitare la facoltà di "oscuramento".

In caso di incapacità di agire deve essere acquisito il consenso di chi esercita la potestà. Raggiunta la maggiore età, deve essere acquisito nuovamente il consenso informato dell'interessato divenuto maggiorenne (artt. 13 e 82, comma 4, del Codice).

In caso di revoca (liberamente manifestabile) del consenso, il Fse/dossier non dovrebbe essere ulteriormente implementato. I documenti sanitari presenti dovrebbero restare disponibili per l'organismo che li ha redatti (es. informazioni relative a un ricovero utilizzabili dalla struttura di degenza) e per eventuali conservazioni per obbligo di legge, ma non dovrebbero essere più condivisi da parte degli altri organismi o professionisti che curino l'interessato (art. 22, comma 5, del Codice).

Il trattamento di dati genetici eventualmente effettuato in relazione al Fse/dossier deve avvenire nel rispetto dell'apposita autorizzazione generale al trattamento dei dati genetici rilasciata dal Garante.

4. I SOGGETTI CHE TRATTANO I DATI

Il trattamento di dati personali effettuato attraverso il Fse/dossier, perseguendo esclusivamente fini di prevenzione, diagnosi e cura dell'interessato, dovrebbe essere posto in essere esclusivamente da parte di soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico nell'esercizio di attività medico-legale (es. visite per l'accertamento dell'idoneità lavorativa o alla guida).

La titolarità del trattamento dei dati personali effettuato tramite il Fse/dossier dovrebbe essere di regola riconosciuta alla struttura o organismo sanitario inteso nel suo complesso e presso cui

sono state redatte le informazioni sanitarie (es. azienda sanitaria o ospedale) (art. 4, comma 1, lett. f) del Codice).

I titolari hanno la facoltà di designare gli eventuali soggetti responsabili del trattamento, mentre devono preporre in ogni caso le persone fisiche eventualmente incaricate, le quali possono venire lecitamente a conoscenza dei dati personali trattati attraverso tali strumenti attenendosi alle funzioni svolte e sulla base di idonee istruzioni scritte (artt. 4, comma 1, lett. g) e h), 29 e 30 del Codice).

Le persone fisiche legittimate a consultare il Fse/dossier dovrebbero essere adeguatamente edotte delle particolari modalità di creazione e utilizzazione di tali strumenti.

Nell'individuare gli incaricati il titolare o il responsabile dovrebbero indicare con chiarezza l'ambito delle operazioni consentite (operando, in particolare, le opportune distinzioni tra il personale con compiti amministrativi e quello con funzioni sanitarie), avendo cura di specificare se gli stessi abbiano solo la possibilità di consultare il Fascicolo/dossier o anche di integrarlo o modificarlo (cfr. punto 5 del presente provvedimento).

5. DATI CHE POSSONO ESSERE TRATTATI E ACCESSO AL FASCICOLO SANITARIO ELETTRONICO E AL DOSSIER SANITARIO

Il titolare deve valutare attentamente quali dati pertinenti, non eccedenti e indispensabili inserire nel Fse/dossier in relazione alle necessità di prevenzione, diagnosi, cura e riabilitazione (artt. 11, comma 1, lett. d) e 22, comma 5 del Codice).

Dovrebbero essere pertanto preferite soluzioni che consentano un'organizzazione modulare di tali strumenti in modo da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al modulo di dati) indispensabili.

In alcuni progetti di Fse esaminati tale organizzazione modulare permette, ad esempio, di selezionare le informazioni sanitarie accessibili ai diversi titolari abilitati in funzione del loro settore di specializzazione (es. rete oncologica composta da unità operative specializzate nella lotta ai tumori), garantendo così l'accesso alle sole informazioni correlate con la patologia in cura.

Analogamente, alcune categorie di soggetti quali i farmacisti, che svolgono la propria attività in uno specifico segmento del percorso di cura, possono accedere ai soli dati (o moduli di dati)

indispensabili all'erogazione di farmaci (es. accesso limitato all'elenco dei farmaci già prescritti, al fine di valutare eventuali incompatibilità tra il farmaco vendibile senza obbligo di prescrizione medica (SOP) e altri farmaci precedentemente assunti).

In alcuni progetti di dossier sanitario è affidato alla direzione sanitaria il compito di valutare l'indispensabilità delle informazioni mediche generate dai diversi reparti/strutture ai fini della loro consultabilità, nonché quello di decidere se autorizzare o meno l'accesso alle informazioni relative agli eventi clinici anche pregressi da parte del reparto/struttura che ha in cura l'interessato sulla base del tipo di intervento medico e delle argomentazioni poste alla base della richiesta.

I titolari del trattamento, nel costituire il Fse/dossier e individuare la tipologia di informazioni che possono esservi anche successivamente riportate, dovrebbero rispettare le disposizioni normative a tutela dell'anonimato della persona tra cui quelle a tutela delle vittime di atti di violenza sessuale o di pedofilia (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269 e l. 6 febbraio 2006, n. 38), delle persone sieropositive (l. 5 giugno 1990, n. 135), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (d.P.R. 9 ottobre 1990, n. 309), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349), nonché con riferimento ai servizi offerti dai consultori familiari (l. 29 luglio 1975, n. 405).

Nella maggior parte dei progetti di Fse/dossier esaminati il rispetto delle garanzie di anonimato e riservatezza previste dalle sopra richiamate disposizioni di legge è stato ad esempio assicurato prevedendo che le informazioni relative ai suddetti eventi clinici non siano documentabili all'interno di tali strumenti.

In alcuni progetti esaminati all'interno del Fse/dossier è stata poi individuata una sintesi di rilevanti dati clinici sul paziente, ovvero un insieme di informazioni la cui conoscenza può rivelarsi indispensabile per salvaguardare la vita dell'interessato (es., malattie croniche, reazioni allergiche, uso di dispositivi o farmaci salvavita, informazioni relative all'impiego di protesi o a trapianti). Tali informazioni –raccolte di regola in un modulo distinto– sono conoscibili da parte di tutti i soggetti che prendono in cura l'interessato; circostanza di cui l'interessato dovrebbe essere edotto nell'informativa di cui all'art. 13 del Codice.

A garanzia del diritto all'autodeterminazione dovrebbero essere poi individuate modalità tali da

favorire un accesso modulare al Fse/dossier con riferimento ai dati personali e ai soggetti abilitati a consultarli.

L'identificazione dei soggetti abilitati a consultare il Fse/dossier dovrebbe essere effettuata con chiarezza. In relazione alle finalità perseguite con la costituzione del Fascicolo/dossier, l'accesso dovrebbe essere consentito solamente per fini di prevenzione, diagnosi e cura dell'interessato e unicamente da parte di soggetti operanti in ambito sanitario, con conseguente esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico che agisca nell'esercizio di attività medico-legali.

Il personale amministrativo operante all'interno della struttura sanitaria in cui venga utilizzato il Fse/dossier dovrebbe consultare solo le informazioni necessarie per assolvere alle funzioni amministrative cui è preposto e strettamente correlate all'erogazione della prestazione sanitaria (ad es., il personale addetto alla prenotazione di esami diagnostici o visite specialistiche dovrebbe consultare unicamente i soli dati indispensabili per la prenotazione stessa).

L'abilitazione all'accesso deve essere consentita all'interessato nel rispetto delle cautele previste dall'art. 84 del Codice, secondo cui gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni inerenti al suo stato di salute (es. referti, esiti di consulti medici) per il tramite di un medico –individuato dallo stesso interessato o dal titolare– o di un esercente le professioni sanitarie, che nello svolgimento dei propri compiti intrattiene rapporti diretti con il paziente (3). Tale garanzia dovrebbe essere osservata anche quando l'accesso al Fascicolo avviene mediante l'utilizzo di una smart card.

L'accesso al Fse/dossier dovrebbe essere consentito al soggetto che ha redatto il documento con riferimento allo stesso e agli altri soggetti che abbiano in cura l'interessato, sempre che quest'ultimo ne abbia consentito l'accesso nei termini sopra indicati. In alcuni progetti di Fse esaminati, l'accesso da parte di alcune categorie di soggetti (es. medici specialisti) è ad esempio autorizzato di volta in volta dallo stesso interessato attraverso la consegna di una smart card.

Il professionista o organismo sanitario che ha in cura l'interessato dovrebbe poter accedere a tali

(3) Cfr. Provvedimento del 9 novembre 2005 "Strutture sanitarie: rispetto della dignità" [doc. *web* n. 1191411]

strumenti consultando i documenti sanitari dallo stesso redatti e quelli relativi ad altri eventi clinici eventualmente formati da ulteriori reparti o strutture del medesimo titolare –nel caso di dossier- o da altri organismi o professionisti sanitari nel caso di Fse (es. ricovero pregresso, analisi cliniche antecedenti).

In ogni caso, l'accesso al Fse/dossier dovrebbe essere circoscritto al periodo di tempo indispensabile per espletare le operazioni di cura per le quali è abilitato il soggetto che accede. Ciò, comporta che i soggetti abilitati all'accesso dovrebbero poter consultare esclusivamente i fascicoli/dossier riferiti ai soggetti che assistono per il periodo di tempo in cui si articola il percorso di cura per il quale l'interessato si è rivolto ad essi.

L'elencazione della tipologia di informazioni da ricondurre ai cd. dati di emergenza dovrebbe essere effettuata in modo esaustivo dal titolare del trattamento, il quale procede anche ad aggiornare tale elenco.

Resta ovviamente ferma la normativa in materia di diritti di accesso ai documenti amministrativi (l. 7 agosto 1990, n. 241 e successive modificazioni e integrazioni).

6. INFORMATIVA

Per consentire all'interessato di esprimere scelte consapevoli, il titolare del trattamento deve fornire previamente un'idonea informativa (artt. 13, 79 e 80 del Codice).

L'informativa, da formulare con linguaggio chiaro, dovrebbe indicare tutti gli elementi richiesti dall'art. 13 del Codice. In particolare, dovrebbe essere evidenziata l'intenzione di costituire un Fascicolo/dossier il più possibile completo che documenti la storia sanitaria dell'interessato per migliorare il suo processo di cura e, quindi, per fini di prevenzione, diagnosi, cura e riabilitazione (cfr. art. 76, comma 1, lett. a) del Codice), spiegando in modo semplice le opportunità che offrono tali strumenti, ma, al tempo stesso, l'ampia sfera conoscitiva che essi possono avere.

A garanzia del diritto alla costituzione o meno del Fse/dossier, l'interessato dovrebbe essere - come detto- informato che il mancato consenso totale o parziale non incide sulla possibilità di accedere alle cure mediche richieste.

L'informativa, anche con formule sintetiche, ma agevolmente comprensibili, dovrebbe indicare in modo chiaro –nel caso di dossier– i soggetti (ad es., medici che operano in un reparto in cui

è ricoverato l'interessato o che operano in strutture di pronto soccorso) e –nel caso di Fse- le categorie di soggetti diversi dal titolare (es., medico di medicina generale, farmacista) che, nel prendere in cura l'interessato, possono accedere a tali strumenti, nonché la connessa possibilità di acconsentire che solo alcuni di questi soggetti possano consultarlo.

Nel caso di Fse, l'informativa e la connessa manifestazione del consenso potrebbero essere formulate distintamente per ciascuno dei titolari o, più opportunamente, in modo cumulativo, avendo comunque cura di indicare con chiarezza l'ambito entro il quale i singoli soggetti trattano i dati rispetto al Fse.

L'interessato dovrebbe essere informato anche della circostanza che il Fascicolo/dossier potrebbe essere consultato, anche senza il suo consenso, ma nel rispetto dell'autorizzazione generale del Garante, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività (art. 76 del Codice).

L'informativa dovrebbe anche mettere in luce la circostanza che il consenso alla consultazione del Fascicolo/dossier da parte di un determinato soggetto (ad es., del medico di medicina generale o del medico di reparto in cui è avvenuto il ricovero) potrebbe essere riferito anche al suo sostituto.

L'informativa dovrebbe rendere note all'interessato anche le modalità attraverso le quali rivolgersi al titolare per esercitare i diritti di cui agli artt. 7 e ss. del Codice (cfr. successivo punto 10), come pure per revocare il consenso all'implementazione del suo Fse/dossier o per esercitare la facoltà di oscurare alcuni eventi clinici (cfr. punto n. 3).

Al fine di assicurare una piena comprensione degli elementi indicati nell'informativa, il titolare dovrebbe formare adeguatamente il personale coinvolto sugli aspetti rilevanti della disciplina sulla protezione dei dati personali, anche ai fini di un più efficace rapporto con gli interessati.

7. MISURE DI SICUREZZA

La particolare delicatezza dei dati personali trattati mediante il Fse/dossier impone l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza (art. 31 del Codice), ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.).

Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati dovrebbero essere utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati).

Dovrebbero essere, inoltre, assicurati:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
- individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate;
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Nel caso di Fse, dovrebbero essere, poi, garantiti protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti.

8. NOTIFICAZIONE AL GARANTE

Il Fse, costituendo un insieme logico di informazioni e documenti sanitari volto a documentare la storia clinica di un individuo condiviso da più titolari del trattamento, dovrebbe essere improntato a criteri di massima trasparenza nella sua strutturazione e nel suo funzionamento. A garanzia di tale evidenza i trattamenti di dati personali effettuati attraverso il Fse dovrebbero essere resi noti al Garante mediante lo strumento della notificazione da parte degli organismi pubblici e privati coinvolti e non anche a cura di singoli medici di base o professionisti che consultano un Fse (art. 37 del Codice).

Il Codice ha, infatti, demandato all'Autorità il compito di individuare ulteriori trattamenti -in aggiunta a quelli elencati nell'art. 37- da notificare potendo recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle relative modalità o della natura dei dati personali (art. 37, comma 2, del Codice). La particolare delicatezza delle informazioni trattate attraverso il Fse, nonché la possibilità di utilizzazione delle stesse da parte di diversi titolari induce a considerare allo stato necessaria una notificazione preventiva al Garante di tali trattamenti. L'Autorità si riserva pertanto di disporre all'esito della consultazione pubblica che le attività di gestione del Fse siano oggetto di notificazione in tutto o in parte.

9. DIFFUSIONE E TRASFERIMENTO ALL'ESTERO DEI DATI

I dati sanitari documentati nel Fse/dossier non devono essere in alcun modo diffusi. La circolazione indiscriminata delle informazioni idonee a rivelare lo stato di salute è infatti vietata espressamente dal Codice (artt. 22, comma 8 e 23, comma 5, del Codice). La violazione di tale divieto configura un trattamento illecito di dati personali sanzionato penalmente (art. 167 del Codice).
Anche il trasferimento all'estero dei dati sanitari documentati nel Fse/dossier per finalità di prevenzione, diagnosi e cura dell'interessato può avvenire esclusivamente con il suo consenso, salvo il caso in cui sia necessario per la salvaguardia della vita o della incolumità di un terzo (art. 43 del Codice). Non a caso, nell'ambito dei progetti esaminati, la necessità di comunicare all'estero informazioni sanitarie dell'interessato contenute in tali strumenti si verifica prevalentemente per consentire all'interessato di usufruire di cure mediche all'estero o per consultare un esperto straniero.

10. DIRITTI DELL'INTERESSATO

Rispetto ai dati personali trattati mediante il Fse/dossier dovrebbe essere garantita la possibilità di esercitare in ogni momento i diritti di cui all'art. 7 del Codice. Tali diritti, tra i quali quello di accedere ai dati e di ottenerne la comunicazione in forma intelligibile, ovvero l'integrazione, l'aggiornamento o la rettifica, andrebbero esercitati direttamente nei confronti di ciascun organismo o professionista sanitario.
All'interessato dovrebbe essere fornito senza ritardo un riscontro compiuto e analitico in merito alle sue eventuali istanze (artt. 7, 8, 9, 10 e 146 del Codice). In particolare, dovrebbe essere for-

nito riscontro alle richieste di accesso ai dati personali estrapolando le informazioni oggetto dell'accesso e comunicandole all'interessato con modalità tali da renderne agevole la comprensione, se del caso trasponendole su supporto cartaceo o informatico; a tali istanze può essere opposto un rifiuto nei soli casi previsti dal Codice (artt. 8). Trattandosi di documentazione medica, in analogia a quanto disposto dall'Autorità in tema di ricerche in ambito medico, biomedico ed epidemiologico (4), il riscontro a istanze di integrazione, aggiornamento e rettificazione dei dati potrebbe essere fornito annotando le modifiche richieste senza alterare necessariamente la documentazione di riferimento.

(4) Provvedimento generale del 24 luglio 2008 "Linee-guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali" pubblicato in Gazzetta Ufficiale 14 agosto 2008, n. 190, [doc. *web* n. 1533155]

39. Segnalazione al Parlamento e al Governo sulla videosorveglianza nei condomini (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SEGNALAZIONE AL PARLAMENTO E AL GOVERNO SULLA VIDEOSORVEGLIANZA NEI CONDOMINI

(art. 154, comma 1, lett. f), d.lg. 30 giugno 2003, n. 196)

1. La presente segnalazione individua le ragioni per le quali il Garante ritiene opportuno un intervento normativo volto a disciplinare alcuni profili relativi alla videosorveglianza all'interno di edifici condominiali e nelle relative pertinenze, tematica che forma oggetto di recenti quesiti e segnalazioni indirizzate all'Autorità. Più specificamente, oggetto della presente segnalazione è il caso in cui non i singoli condomini, ma l'intera compagine condominiale intenda effettuare tali trattamenti (previa installazione di sistemi di videosorveglianza per il tramite della relativa amministrazione condominiale, anche presso amministrazioni di residence o di multiproprietà) in aree comuni (quali portoni d'ingresso, androni, cortili, scale, aree di accesso a parcheggi o dedicate a servizi comuni).

2. Da tempo, il tema più generale della videosorveglianza specie in luoghi pubblici o aperti al pubblico è all'attenzione del Garante e ha formato oggetto, oltre che di numerose decisioni in singoli casi, di due provvedimenti di carattere generale: il primo, del 29 novembre 2000 (in www.garanteprivacy.it, doc. web n. 31019, nel quale si impartivano prime prescrizioni "nell'attesa di una specifica legislazione"), il secondo, più dettagliato perché volto a tener conto di variegate sollecitazioni provenienti da prassi applicative, del 29 aprile 2004 (doc. web n. 1003482). Con tali interventi, il Garante non si è soffermato specificamente sulle condizioni di liceità per il trattamento di dati personali all'interno dei condomìni: non sono stati di conseguenza identificati né i soggetti la cui manifestazione di volontà è necessaria nel contesto condominiale per svolgere tali trattamenti (i proprietari e i titolari di diritti reali parziari o anche soggetti diversi, primi fra tutti i conduttori), né le eventuali maggioranze da rispettare.

(*) [doc. *web* n. 1523997]

3. In tempi più recenti, si sono moltiplicati i quesiti e le segnalazioni relativi allo specifico profilo delle condizioni di impiego della videosorveglianza da parte di compagini condominiali all'interno di aree comuni.

Dal loro esame emerge l'esistenza di due non convergenti approcci alla tematica, da parte dei contrapposti interessi potenzialmente coinvolti dal funzionamento di questi sistemi di videosorveglianza: da un lato, l'esigenza volta a preservare la sicurezza di persone e la tutela di beni comuni (ad esempio, rispettivamente, contro aggressioni e danneggiamenti o furti); dall'altro, la preoccupazione che i trattamenti effettuati, nel rendere più agevolmente conoscibili a terzi informazioni relative alla vita privata di chi vive in edifici condominiali, come pure abitudini e stili di vita individuali e familiari, siano idonei a incidere sulla libertà degli interessati di muoversi, non controllati, nel proprio domicilio e all'interno delle aree comuni.

4. Il profilo in esame non è regolato da una puntuale disciplina. Esso non trova (né avrebbe potuto trovare) espressa regolamentazione nel Codice civile del 1942; né, è chiaro, pur applicando i princìpi generali, se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei (com)proprietari (comunque, il quadro normativo esistente e l'interpretazione giurisprudenziale non consentono di comprendere con quale maggioranza) o se rilevi anche la volontà di coloro che rivestono la qualità di conduttori.

Deve essere anche tenuto in considerazione che l'art. 615 *bis* del codice penale sanziona "chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614", vale a dire nel domicilio (nozione che, secondo la giurisprudenza, è suscettibile di comprendere anche le aree comuni (1)): ciò comporterebbe, nel contesto condominiale, la necessaria acquisizione preventiva del consenso di un numero assai ampio di soggetti, non sempre peraltro di agevole identificazione, sì da rendere arduo il legittimo impiego dei sistemi di videosorveglianza nel peculiare contesto qui tenuto in considerazione.

Più in generale, gli orientamenti giurisprudenziali sull'uso delle aree comuni non appaiono utili a dissolvere i dubbi relativi ai profili in esame.

(1) Cfr. Cass. Pen., sez. V, 20 ottobre 1998, n. 12751; Cass., 15 maggio 1987; v pure Cass. pen., 27 marzo 2006, n. 10444

5. Per tali ragioni il Garante auspica che gli aspetti segnalati del tema qui rappresentato, suscettibile di interessare larga parte della popolazione, possano trovare una più specifica regolamentazione, con l'individuazione di una disciplina che assicuri un equo contemperamento tra i diritti fondamentali delle persone coinvolte e le legittime esigenze di difesa e protezione di persone e cose. Ciò, peraltro, potrebbe avvenire anche nell'ambito di più generali iniziative normative relative all'amministrazione dei condomini, già oggetto di diversi disegni di legge sottoposti all'esame di entrambi i rami del Parlamento. (2)

PER QUESTE RAGIONI

il Garante segnala al Parlamento e al Governo l'opportunità che sia valutata anche l'eventuale adozione di una possibile regolamentazione dell'utilizzo di sistemi di videosorveglianza delle aree comuni identificando le condizioni per assumere idonee determinazioni, con particolare riferimento all'individuazione:

- dei partecipanti al processo decisionale (i soli condomini, ovvero anche i conduttori);
- del numero di voti necessari per l'approvazione della deliberazione (l'unanimità o una determinata maggioranza).

Roma, 13 maggio 2008

(2) A questo proposito può evidenziarsi che nel corso della XV Legislatura (ripercorrendo testi ampiamente discussi e condivisi nel corso della XIV) sono stati presentati i seguenti disegni di legge: C. 1199 On. Cosimo Giuseppe Sgobio, Modifiche al codice civile in materia di condominio negli edifici, presentato il 26 giugno 2006; S. 647 Sen. Giovanni Legnini e altri, Modifiche alla disciplina del condominio negli edifici, presentato il 14 giugno 2006; S. 310 Sen. Franco Mugnai e altri, Modifiche alla disciplina del condominio negli edifici, presentato il 10 maggio 2006; S. 6 Sen. Andrea Pastore e altri, Modifiche alla normativa in materia di condominio negli edifici, presentato il 28 aprile 2006

40. Provvedimenti di particolare rilievo

Autorizzazione n. 1/2008 al trattamento dei dati sensibili nei rapporti di lavoro
19 giugno 2008 [doc. *web* n. 1529374]

Autorizzazione n. 2/2008 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale
19 giugno 2008 [doc. *web* n. 1529389]

Autorizzazione n. 3/2008 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni
19 giugno 2008 [doc. *web* n. 1529399]

Autorizzazione n. 4/2008 al trattamento dei dati sensibili da parte dei liberi professionisti
19 giugno 2008 [doc. *web* n. 1529408]

Autorizzazione n. 5/2008 al trattamento dei dati sensibili da parte di diverse categorie di titolari
19 giugno 2008 [doc. *web* n. 1529420]

Autorizzazione n. 6/2008 al trattamento dei dati sensibili da parte degli investigatori privati
19 giugno 2008 [doc. *web* n. 1529549]

Autorizzazione n. 7/2008 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici
19 giugno 2008 [doc. *web* n. 1529557]

Differimento dell'efficacia dell'autorizzazione al trattamento dei dati genetici rilasciata il 22 febbraio 2007
19 dicembre 2008 [doc. *web* n. 1582871]

Semplificazione al modello per la notificazione al Garante

22 ottobre 2008 [doc. *web* n. 1571196]

Misure in materia di propaganda elettorale - Esonero dall'informativa

2 aprile 2009 [doc. *web* n. 1603863]

Redditi *on-line*: illegittima la diffusione dei dati sul sito Internet dell'Agenzia delle entrate

6 maggio 2008 [doc. *web* n. 1512255]

Riconoscimento vocale e gestione di sistemi informatici

28 febbraio 2008 [doc. *web* n. 1501094]

Dati biometrici: vietati per la rilevazione dell'orario di lavoro

2 ottobre 2008 [doc. *web* n. 1571502]

Controlli *anti-doping* e trattamento dei dati personali dei ciclisti

13 ottobre 2008 [doc. *web* n. 1563970]

41. Ulteriori provvedimenti citati

Dichiarazione di appartenenza o aggregazione al gruppo linguistico in provincia di Bolzano

10 gennaio 2008 [doc. *web* n. 1484669]

Sicurezza dei dati di traffico telefonico e telematico

17 gennaio 2008 [doc. *web* n. 1482111]

Preiscrizioni universitarie per l'anno accademico 2008/2009

31 gennaio 2008 [doc. *web* n. 489926]

Trattamento di dati personali in albergo per finalità di *marketing*

31 gennaio 2008 [doc. *web* n. 1490553]

Marketing: possibile inviar e materiale pubblicitario e comunicazioni commer ciali solo con il consenso preventivo dell'interessato

31 gennaio 2008 [doc. *web* n. 1488781]

31 gennaio 2008 [doc. *web* n. 1489843]

13 maggio 2008 [doc. *web* n. 1520217]

13 maggio 2008 [doc. *web* n. 1520243]

13 maggio 2008 [doc. *web* n. 1520263]

19 dicembre 2008 [doc. *web* n. 1584213]

Consenso e trattamento dei dati personali a fini di *marketing*

31 gennaio 2008 [doc. *web* n. 1500829]

Trattamento di dati giudiziari del personale di società di *rating*

31 gennaio 2008 [doc. *web* n. 1488729]

Trattamento dei dati sensibili e giudiziari pr esso la Scuola superior e della pubblica amministrazione locale

7 febbraio 2008 [doc. *web* n. 1491594]

Banche: configurazione dei sistemi di aller ta rientranti nelle misur e pr eviste per il contrasto finanziario al terrorismo

7 febbraio 2008 [doc. *web* n. 1523046]

Pubblicità dei dati di debitori nelle esecuzioni immobiliari

7 febbraio 2008 [doc. *web* n. 1490838]

Movimenti politici: limiti e garanzie nel trattamento dei dati personali

15 febbraio 2008 [doc. *web* n. 1523069]

Trattamento dei dati biometrici di dipendenti per incr ementare la sicurezza della rete idrica

15 febbraio 2008 [doc. *web* n. 1497675]

Modalità di inserimento negli elenchi dei beneficiari del 5 per mille Irpef delle associazioni sportive

21 febbraio 2008 [doc. *web* n. 1497596]

Sportello unico doganale delle operazioni di impor tazione ed espor tazione

28 febbraio 2008 [doc. *web* n. 1523079]

Esonero dall'informativa per partiti e movimenti politici sino al 31 luglio 2008

28 febbraio 2008 [doc. *web* n. 1493909]

Diffusione di dati relativi a contributi per l'acquisto di testi scolastici

28 febbraio 2008 [doc. *web* n. 1501081]

Conservazione di dati relativi al traffico e all'ubicazione delle persone, nonché dei dati connessi necessari per identificare l'abbonato o l'utente

5 marzo 2008 [doc. *web* n. 1523089]

Modalità di richiesta di ammissione al beneficio del 5 per mille I rpef

13 marzo 2008 [doc. *web* n. 1500816]

Comunicazione unica per la nascita dell'impresa

13 marzo 2008 [doc. *web* n. 1500799]

Fondazioni bancarie: regolamento di bilancio

20 marzo 2008 [doc. *web* n.1502866]

Impresa: presentazione dei bilanci e altri atti al r egistro delle imprese

20 marzo 2008 [doc. *web* n. 1519563]

Tutela della salute e sicur ezza nei luoghi di lavoro

31 marzo 2008 [doc. *web* n. 1504941]

Documenti caratteristici del personale dell'Esercito, della Marina, dell'Aeronautica e dell'Arma dei carabinieri

2 aprile 2008 [doc. *web* n. 1519667]

Tecnologie per la formazione a distanza e contr ollo a distanza dei lavoratori

2 aprile 2008 [doc. *web* n. 1519695]

L'azienda non può comunicare a terzi i dati giudiziari riferiti ai collaboratori

2 aprile 2008 [doc. *web* n. 1519711]

Programmi di fidelizzazione: trattamento di dati personali riferiti al dipendente e loro utilizzo a fini disciplinari

2 aprile 2008 [doc. *web* n. 1519679]

Comunicazioni illecite di dati sulla salute dei dipendenti

2 aprile 2008 [doc. *web* n. 1519902]

Limiti al controllo sulla posta elettronica del dipendente

2 aprile 2008 [doc. *web* n. 1519703]

Prove di ammissione a corsi di laurea ad accesso programmato per l'anno accademico 2008/2009

10 aprile 2008 [doc. *web* n. 1519655]

Trattamento di dati sensibili e giudiziari da parte della Provincia di Roma. Nuova finalità di rilevante interesse pubblico

10 aprile 2008 [doc. *web* n. 1507195]

Regole tecniche per la firma digitale

15 aprile 2008 [doc. *web* n. 1519647]

Iscrizione al registro nazionale delle imprese operanti nel settore degli armamenti

24 aprile 2008 [doc. *web* n. 1514260]

Accesso agli atti delle imprese assicuratrici derivanti dalla circolazione dei veicoli a motore e natanti

30 aprile 2008 [doc. *web* n. 1514729]

Pubblicazione Internet degli elenchi dei contribuenti da parte dell'Agenzia delle entrate

30 aprile 2008 [doc. *web* n. 1510761]

Graduatorie di concorsi pubblici e dati sensibili

8 maggio 2008 [doc. *web* n. 1521716]

Marketing via *e-mail*: necessaria l'informativa per il trattamento di dati personali

13 maggio 2008 [doc. *web* n. 1521775]

Vendita a domicilio e trattamento di dati a fini di *marketing* in violazione di legge

19 maggio 2008 [doc. *web* n. 1526956]

Autonomia della comunicazione di dati rispetto alle altre operazioni di trattamento

19 maggio 2008 [doc. *web* n. 1523347]

Uso di strumenti informatici e telematici nel processo civile

19 maggio 2008 [doc. *web* n. 1521729]

Ministero della giustizia. Tenuta dei registri informatizzati negli uffici

19 maggio 2008 [doc. *web* n. 1521788]

Immigrazione, condizione dello straniero e ricongiungimento familiare

5 giugno 2008 [doc. *web* n. 1526943]

Esercizio di attività giornalistica e comunicazione all'interessato dei dati che lo riguardano

5 giugno 2008 [doc. *web* n. 1542403]

Trattamento dei dati completi e aggiornati tratti dai pubblici registri

5 giugno 2008 [doc. *web* n. 1535726]

Giornalismo: rispetto del principio di essenzialità dell'informazione nel caso di vittime di reato

5 giugno 2008 [doc. *web* n. 1527037]

Informazioni commerciali: qualità dei dati

12 giugno 2008 [doc. *web* n. 1537684]

Modifiche e integrazioni allo schema tipo di r egolamento per i trattamenti dei dati sensibili e giudiziari svolti presso le regioni e le province autonome

12 giugno 2008 [doc. *web* n. 1537639]

Uso di dati biometrici nelle operazioni di trasfusione

19 giugno 2008 [doc. *web* n. 1532480]

Telemarketing: banche dati precedenti al 1° agosto 2005 - Provvedimento inibitorio

26 giugno 2008 [doc. *web* n 1544326]

26 giugno 2008 [doc. *web* n.1544315]

26 giugno 2008 [doc. *web* n. 1544338]

25 settembre 2008 [doc. *web* n. 1562780]

25 settembre 2008 [doc. *web* n. 1562758]

Attività giornalistica: diffusione di dati su minori vittime di violenza sessuale

10 luglio 2008 [doc. *web* n. 1536583]

2 ottobre 2008 [doc. *web* n. 1557470]

16 febbraio 2009 [doc. *web* n. 1590076]

Schema di linee-guida in tema di insediamenti di comunità nomadi nelle r egioni Campania, Lazio e Lombardia

17 luglio 2008 [doc. *web* n. 1537659]

Individuazione dei soggetti certificatori della Cns

24 luglio 2008 [doc. *web* n. 1545983]

Trattamento dei dati sensibili nell'ambito di attività di informazione scientifica e di sperimentazione clinica di medicinali

24 luglio 2008 [doc. *web* n. 1544575]

Recepimento normativo in tema di dati di traffico telefonico e telematico

24 luglio 2008 [doc. *web* n. 1538224]

Social card: *privacy* garantita per i meno abbienti

18 settembre 2008 [doc. *web* n. 1553367]

Videosorveglianza: limiti e garanzie per il trattamento dei dati

2 ottobre 2008 [doc. *web* n. 1581352]

Identità personale e sistemi di informazione creditizia

13 ottobre 2008 [doc. *web* n. 1562822]

6 novembre 2008 [doc. *web* n. 1571531]

Società di informazioni commerciali: tutela dell'interessato nei casi di possibile omonimia

13 ottobre 2008 [doc. *web* n. 1571459]

Giornalismo: diffusione di dati su vittime di violenza sessuale

13 ottobre 2008 [doc. *web* n. 1563958]

Aggiornamento 2009/2010 del Programma statistico nazionale

22 ottobre 2008 [doc. *web* n. 1565063]

Informazioni commerciali: si possono trattare solo dati pertinenti

30 ottobre 2008 [doc. *web* n. 1570327]

Programmi di fidelizzazione: trattamento di dati personali riferiti al dipendente e loro utilizzo a fini disciplinari

6 novembre 2008 [doc. *web* n. 1573780]

Contratti di locazione: vietata la diffusione a terzi dei dati personali del conduttore

20 novembre 2008 [doc. *web* n. 1576139]

Dati genetici: limiti al trattamento a fini giudiziari

27 novembre 2008 [doc. *web* n. 1581365]

Attività giornalistica: dati relativi a minori

27 novembre 2008 [doc. *web* n. 1582436]

Esercizio dei diritti dell'interessato e difesa in giudizio

27 novembre 2008 [doc. *web* n. 1580262]

Videosorveglianza: vietata negli spogliatoi di poliambulatorio

4 dicembre 2008 [doc. *web* n. 1576125]

Archivi storici *on-line* dei quotidiani: accoglimento dell'opposizione dell'interessato alla reperibilità delle proprie generalità attraverso i motori di ricerca

11 dicembre 2008 [doc. *web* n. 1582866]

19 dicembre 2008 [doc. *web* n. 1583152]

Operazioni di scissione e fusione per incorporazione: prescrizioni in tema di aggiornamento dell'informativa a Banca Nazionale del Lavoro S.p.A. ed Artigiancassa

11 dicembre 2008 [doc. *web* n. 1584328]

Agenzia delle entrate: modalità e termini per la segnalazione da parte delle società di gestione del risparmio dei soggetti che hanno omesso la comunicazione necessaria ai fini dell'applicazione dell'imposta patrimoniale
19 dicembre 2008 [doc. *web* n. 1584260]

Frodi comunitarie: trattamento di dati sensibili e giudiziari da parte della Presidenza del Consiglio dei ministri
19 dicembre 2008 [doc. *web* n. 1584241]

Persone disperse in montagna: si può localizzare il cellulare per rintracciarle
19 dicembre 2008 [doc. *web* n. 1580543]

Accesso all'Indice dei nati in Trentino: intesa tra la Provincia autonoma di Trento e l'Arcidiocesi di Trento
19 dicembre 2008 [doc. *web* n. 1584224]

Operazione di fusione per incorporazione: prescrizioni in tema di aggiornamento dell'informativa a Banca Monte dei Paschi di Siena S.p.A.
19 dicembre 2008 [doc. *web* n. 1584272]

Operazione Cai/Alitalia: informativa semplificata per i clienti e trattamento dei dati personali
8 gennaio 2009 [doc. *web* n. 1580603]

Archivi storici *on-line* dei quotidiani: condizioni che rendono legittima la riproposizione di un articolo su Internet
12 febbraio 2009 [doc. *web* n. 1601624]

Conservazione dei dati di traffico: proroga dei termini
29 aprile 2009 [doc. *web* n. 1612508]