gli estremi per dare attuazione al principio del bilanciamento degli interessi disciplinato dall'art. 24, comma 1, lett. *g*), del Codice e che potessero, quindi, formare oggetto di comunicazione, per le esclusive finalità di contrasto al riciclaggio, i dati personali concernenti le segnalazioni previste dalla disciplina in materia di riciclaggio tra gli intermediari finanziari appartenenti al medesimo gruppo, in presenza delle condizioni previste dall'art. 46, comma 4, d.lgs. n. 231/2007, senza che a tal fine fosse quindi necessario acquisire il consenso degli interessati.

Ciò in considerazione della ponderazione tra le diverse situazioni giuridiche soggettive effettuata nel menzionato decreto legislativo, nel quale si precisa che il divieto di comunicazione a terzi della circostanza dell'avvenuta segnalazione previsto dall'art. 46, comma 1, non impedisce che essa avvenga *"tra gli intermediari finanziari appartenenti al medesimo gruppo"* (art. 46, comma 4). Ponderazione che, nel facoltizzare tale comunicazione tra gli intermediari finanziari appartenenti al medesimo gruppo, consente di non ritenere prevalenti, entro tale circoscritto ambito, i diritti degli interessati rispetto al legittimo interesse del titolare del trattamento e del terzo destinatario dei dati (nel caso di specie, altro intermediario finanziario appartenente al medesimo gruppo) alla comunicazione e al conseguente trattamento dei dati personali oggetto della segnalazione.

Di tale comunicazione, che potrà essere effettuata da parte dei soli incaricati (operanti nell'ambito dei diversi intermediari finanziari) dell'adempimento delle misure poste a contrasto del riciclaggio di denaro, il titolare dovrà fornire adeguata informativa agli interessati, dando distinte e specifiche indicazioni anche riguardo alla possibilità che le informazioni relative alle operazioni poste in essere dagli stessi interessati, ove ritenute "sospette" ai sensi dell'art. 41, comma 1, del d.lgs. 21 novembre 2007, n. 231, siano comunicate ad altri intermediari finanziari appartenenti al medesimo gruppo.

In relazione poi al trasferimento dei dati relativi alla segnalazione verso intermediari finanziari appartenenti allo stesso gruppo stabiliti in Paesi terzi, il provvedimento ha stabilito che tale trasferimento potrà avvenire ove ricorra uno dei presupposti indicati dalla legge (art. 44 del Codice).

10.2. INFORMAZIONI COMMERCIALI

Nel 2009 l'Autorità, a seguito di un'intensa attività collaborativa con l'Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito (Ancic, che controllano l'80% del volume d'affari del mercato considerato) ha affrontato la tematica dell'esonero dall'obbligo di fornire l'informativa agli interessati nell'ambito delle attività di *cd. "informazione commerciale"*.

Con il *provvedimento* del 14 maggio 2009 [doc. *web* n. 1616828] le società associate ad Ancic che operano nel settore delle informazioni commerciali sono state esonerate dall'obbligo di rendere un'informativa individualizzata in relazione al trattamento di dati personali provenienti da fonti pubbliche (o informazioni comunque pubblicamente accessibili) ove effettuato nel rispetto dei princìpi posti in materia di protezione dei dati personali. Ancic aveva rappresentato che i costi per rendere un'informativa in forma "individualizzata", risultavano sproporzionati rispetto ai diritti tutelati, in quanto elevatissimi per gli operatori di settore tenuto conto del numero ingente di soggetti ai quali la stessa avrebbe dovuto essere resa (alcuni milioni di soggetti censiti da parte di ciascuna società).

Con il medesimo provvedimento - fatte comunque salve le disposizioni contenute negli artt. 115 e 134 del r.d. 18 giugno 1931, n. 773 (*Testo unico delle leggi di pubblica sicurezza*) e la vigente normativa in materia di segreto aziendale e industriale - sono state altresì individuate misure e accorgimenti a garanzia degli interessati per consentire una maggiore conoscibilità del fenomeno delle *cd. "informazioni commerciali"* non solo tra gli operatori economici ma, più in generale, tra tutti i possibili soggetti censiti (clienti, aziende, professionisti, imprenditori, persone fisiche) dalle banche dati utilizzate per la *cd. "business information"*.

Le operazioni di trattamento prese in considerazione dal provvedimento sopra citato consistono nella raccolta e nella comunicazione alla clientela (art. 4, comma 1, lett. *l*), del Codice), anche per via telematica, di rapporti e *dossier* informativi a carattere economico o commerciale contenenti dati estratti dalle fonti pubbliche (quali visure camerali, *cd. "pregiudizievoli di conservatoria"*, dati ipocatastali, bilanci, protesti e procedure concorsuali) nonché informazioni frutto di ulteriore analisi, raffronto

ed elaborazione effettuati dalle società che rendono, in qualità di autonomi titolari del trattamento, i servizi di informazione commerciale (art. 4, comma 1, lett. *a*), del Codice).

In particolare, rispetto a tali trattamenti il Garante ha individuato, quale modalità appropriata al fine di assicurare comunque un'adeguata informativa (art. 13, comma 5, lett. *c*)) da parte delle società associate ad Ancic, la pubblicazione con cadenza annuale dell'informativa, contenente gli estremi identificativi di tutti i titolari del trattamento e gli altri elementi previsti dall'art. 13, commi 1 e 2, del Codice, sulle "Pagine Gialle" e sulle "Pagine Bianche" in versione cartacea e mediante un *banner* sui relativi siti *web*, nonché la permanente pubblicazione da parte di ciascuna delle associate ad Ancic dell'informativa prevista dall'art. 13 del Codice sul proprio sito *web*.

L'Autorità, ha inoltre stabilito, quale ulteriore misura opportuna ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, che Ancic tenga costantemente aggiornato sul proprio sito *web* l'elenco delle società di informazione commerciale alla medesima aderenti, al fine di agevolare gli interessati nell'acquisizione degli elementi dell'informativa.

10.3. SETTORE ASSICURATIVO

Si è riferito nella *Relazione 2008* (p. 133-134) sul *parere* (*Nota* del Presidente 12 febbraio 2009) relativo allo schema di regolamento sottoposto al Garante dall'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Isvap), concernente la disciplina della banca dati antifrode (art. 135 del codice delle assicurazioni private, art. 120 del Codice) disciplinata dal provvedimento Isvap n. 2179 del 10 marzo 2003 (Banca dati sinistri r.c. auto: modalità operative per l'accesso).

10.4. RAPPORTI DI LAVORO E PREVIDENZA

10.4.1. Rapporto di lavoro in ambito pubblico

I lavoratori, nel rapporto con il proprio datore di lavoro pubblico, hanno diritto di ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (artt. 2, comma 5, e 50 d.lgs. 7 marzo 2005, n. 82, come modificato

dal d.lgs. 4 aprile 2006, n. 159). Le amministrazioni locali, pertanto, fermi gli obblighi di legge sulla trasparenza delle deliberazioni dell'ente, devono selezionare con estrema attenzione i dati personali da diffondere, non solo alla luce dei princìpi di pertinenza, non eccedenza e indispensabilità rispetto alle finalità perseguite dai singoli provvedimenti, ma anche in relazione al divieto di diffusione dei dati idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice).

Diffusione dei dati di un dipendente sul sito internet di una provincia

Lo ha ribadito il Garante accogliendo la segnalazione di una dipendente provinciale che, attraverso un motore di ricerca, aveva rinvenuto *online* alcuni atti dell'ente locale in cui erano riportati i suoi dati anagrafici e delicate informazioni sul suo stato di salute, la cui diffusione è vietata dal Codice (*Provv.* 25 giugno 2009 [doc. *web* n. 1640102]).

Richiamando le indicazioni fornite in passato agli enti locali circa l'utilizzo delle tecnologie dell'informazione (*Provv.* 19 aprile 2007 [doc. *web* n. 1407101] punto 6 e *Provv.* 14 giugno 2007 [doc. *web* n. 1417809] punto 6), l'Autorità ha ritenuto il trattamento illecito e ha disposto il blocco dei dati idonei a rivelare lo stato di salute della dipendente, contenuti in due delibere pubblicate sul sito istituzionale della provincia che, a seguito degli accertamenti effettuati dall'Ufficio, risultavano integralmente e direttamente accessibili non solo dall'*home page* del predetto sito, ma anche liberamente reperibili in internet. Le delibere, adottate del responsabile delle risorse umane dell'ente locale, riguardavano una richiesta di riconoscimento di infermità per causa di servizio avanzata dall'interessata: uno dei documenti riportava, inoltre, accanto al nome e cognome della dipendente, la valutazione medico-legale relativa al tipo di infermità riscontrata (art. 2, comma 7, d.P.R. 29 ottobre 2001, n. 461 e tab. A allegata al d.P.R. 30 dicembre 1981, n. 834; art. 6 decreto 12 febbraio 2004).

Accertamenti di idoneità al servizio: anonimato per la diagnosi Hiv

In materia di accertamenti finalizzati a verificare l'idoneità al servizio dei pubblici dipendenti, l'Autorità ha affermato che le sole informazioni che possono comparire sui certificati medici che attestano l'idoneità al servizio di un lavoratore sono quelle relative alla valutazione medico-legale (idoneità, non idoneità parziale, temporanea o permanente, con prescrizioni o limitazioni), non essendo consentito alcun riferimento alle patologie sofferte. Ciò, in particolare, nel caso di lavoratori di cui sia accertata la

sieropositività, ai quali deve essere assicurata la garanzia assoluta dell'anonimato. Questi princìpi sono stati ribaditi dal Garante con il *provvedimento* del 2 ottobre 2009 [doc. *web* n. 1658119] in cui è stato ritenuto fondato il reclamo di un dipendente del Ministero della difesa che aveva contestato la modalità con cui i suoi dati erano circolati all'interno del Ministero. Nel verbale della visita collegiale trasmesso dalla commissione medica all'Ispettorato di sanità della marina erano infatti riportati i dati nominativi dell'interessato e la diagnosi accertata. Nella copia del verbale inviata all'ufficio del personale del Ministero e al comando di appartenenza dell'interessato la diagnosi risultava invece *"sbarrata e omessa"*, consentendo così, seppure indirettamente, di risalire all'infezione da Hiv, in quanto la prassi di oscurare la diagnosi sui verbali di accertamento medico era stata adottata dall'amministrazione unicamente per la sieropositività.

Il Garante ha pertanto vietato al Ministero di utilizzare ulteriormente le informazioni sulla salute del lavoratore, specie quelle riguardanti l'Hiv, riportate nella documentazione medica. Ha inoltre prescritto di utilizzare un attestato che riporti il solo giudizio medico-legale senza diagnosi, anziché il verbale integrale della visita collegiale, in tutti i casi di accertamento sanitario di idoneità al servizio o di altre forme di inabilità. L'Autorità ha infine sollecitato l'amministrazione a modificare anche il modello di informativa utilizzato, al fine di informare in modo chiaro i lavoratori interessati sull'obbligatorietà o meno di fornire i dati sulla propria salute e sulle relative conseguenze nell'ambito degli accertamenti medico legali ai fini dell'idoneità al servizio.

In un altro caso, un'insegnante aveva contestato dinanzi all'Autorità che il circolo didattico, presso cui prestava servizio, era in possesso di copia integrale del verbale di visita medica effettuata a seguito della sua richiesta di pensione di inabilità, sul quale erano riportati informazioni riferite alla diagnosi accertata, agli esami obiettivi e agli accertamenti clinici e strumentali compiuti, nonché dati anamnestici, tra cui quelli relativi all'infezione da Hiv contratta in precedenza dall'interessata.

Dagli accertamenti effettuati nel corso dell'istruttoria l'amministrazione scolastica, tuttavia, non risultava più in possesso della documentazione medico-legale riferita alla dipendente: dopo aver ricevuto la copia del verbale di visita dalla commissione medica di

verifica del Ministero dell'economia e delle finanze, la sede di servizio dell'interessata l'aveva infatti inviata, insieme al fascicolo personale della dipendente, al circolo didattico presso cui la docente figurava come titolare, in quanto competente ad adottare i provvedimenti conseguenti all'accertata inabilità al lavoro dell'interessata.

Con il *provvedimento* del 24 dicembre 2009 [doc. *web* n. 1658058] il Garante, ritenendo illecita l'avvenuta trasmissione di copia integrale del verbale di visita da parte dall'organo di accertamento sanitario, ha vietato alla commissione medica di effettuare ulteriori comunicazioni illecite dei dati sulla salute della dipendente contenuti nella predetta documentazione. Richiamando le particolari cautele previste dalla normativa sulla protezione dei dati, nonché dalla l. n. 135/1990, per il trattamento delle informazioni sanitarie e, in particolare per quelle riguardanti l'Hiv, l'Autorità ha altresì richiesto alla commissione medica di utilizzare, in luogo del verbale integrale di visita, un attestato riportante la sola valutazione medico-legale ai fini della comunicazione alle amministrazioni di appartenenza dei lavoratori interessati dell'esito degli accertamenti sanitari di inidoneità al servizio o altre forme di inabilità non dipendenti da causa di servizio.

Nel medesimo provvedimento, avverso il quale pende un'opposizione dinanzi all'autorità giudiziaria, il Garante ha infine ritenuto illecito il trattamento dei dati sanitari della docente posto in essere dall'amministrazione scolastica presso cui prestava servizio: questa infatti, in conformità a quanto indicato dall'Autorità nelle *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico"* (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]) circa l'inutilizzabilità delle informazioni trattate in violazione della disciplina rilevante sulla protezione dei dati, avrebbe dovuto astenersi da ogni ulteriore operazione di trattamento delle informazioni dell'interessata contenute nella documentazione medica pervenuta, ad eccezione di quelle relative alla valutazione medico-legale, adottando ogni misura idonea a limitarne rigorosamente la loro conoscibilità (linee-guida *cit.*, punti 3.2 e 8.4). Ciò, senza pregiudicare la prosecuzione del procedimento avviato dall'interessata volto ad ottenere la pensione di inabilità.

In ragione dell'estrema delicatezza delle informazioni sanitarie dell'interessata riportate

nella copia integrale del verbale di visita, è stato invece vietato all'amministrazione scolastica - che ne è risultata effettivamente in possesso - di utilizzare ulteriormente tali informazioni, con conseguente obbligo di adottare ogni misura di ulteriore conservazione del documento che li contiene idonea a limitarne rigorosamente la conoscibilità, stante l'inutilizzabilità dei medesimi dati (*cfr.* artt. 11 e 22, commi 1, 3 e 5, del Codice; art. 5, l. n. 135/1990; artt. 4, 5 e 6, comma 8, del d.P.R. n. 461/2001).

Trattamenti di dati sanitari del personale del Ministero della difesa

Il soggetto pubblico datore di lavoro, nell'utilizzare per una finalità lecita i dati sensibili relativi allo stato di salute dei propri dipendenti deve, in particolare, eliminare ogni occasione di superflua conoscibilità di dati sulla salute anche da parte degli stessi soggetti incaricati o responsabili del trattamento (artt. 11, 22, commi 1, 5 e 9 e 112 del Codice) (*Provvedimenti* 23 luglio 2004 [doc. *web* n. 1099216] e 2 ottobre 2009 [doc. *web* n. 1658119] *cit.*).

Tali princìpi sono stati ribaditi dal Garante nel *provvedimento* del 21 ottobre 2009, con cui ha ritenuto fondata la segnalazione di un militare cessato dal servizio per permanente inidoneità, il quale aveva contestato la liceità del trattamento dei suoi dati personali contenuti in alcuni documenti sanitari detenuti dall'ufficio del personale del Ministero della difesa, ritenendo che tale ufficio, avente competenze non sanitarie in materia di stato giuridico, avanzamento e contenzioso del personale militare, avesse indebitamente raccolto informazioni relative al suo stato di salute attraverso l'acquisizione delle certificazioni e dei verbali di visita medica formati dagli organismi sanitari militari.

Nella specie, la documentazione trasmessa dalle commissioni mediche militari all'ufficio del personale era risultata contenere informazioni non necessarie per l'adozione dei provvedimenti di competenza in materia di stato giuridico e di avanzamento dei militari. Nel corso dell'istruttoria della segnalazione tali informazioni riguardanti, in particolare, l'anamnesi, le patologie accertate, gli esami clinici e gli altri accertamenti sanitari effettuati erano state, d'altra parte, espunte dalla documentazione posseduta a cura dello stesso ufficio del personale, in quanto ritenute eccedenti, non pertinenti e non indispensabili (artt. 11, comma 1, lett. *d*), 22, commi 3 e 5, e 112 del Codice; l. 10 aprile 1954, n. 113, sullo stato degli ufficiali dell'Esercito, della Marina e dell'Aeronautica).

Richiamando le indicazioni fornite nelle linee-guida in materia di trattamento di dati personali dei dipendenti pubblici [doc. *web* n. 1417809] citate e ferme restando le prescrizioni impartite al Ministero della difesa nel citato *provvedimento* del 2 ottobre 2009, il Garante ha pertanto richiesto all'amministrazione di rendere conformi alla normativa sulla riservatezza le modalità di circolazione interna dei dati sulla salute del personale (*Provv.* 21 ottobre 2009 [doc. *web* n. 1689440]).

Pubblicazione *online* di elenchi del collocamento obbligatorio

In materia di trattamenti di dati effettuati nell'ambito delle attività di avviamento al lavoro, il Garante, sulla base di un autonomo accertamento avviato dall'Ufficio, ha disposto il blocco della diffusione in internet dei dati sanitari di migliaia di persone iscritte nelle graduatorie, provvisorie e definitive, negli elenchi del collocamento obbligatorio dei disabili, delle categorie protette e dei centralinisti telefonici non vedenti. All'amministrazione provinciale che aveva pubblicato tali informazioni sul proprio sito istituzionale è stata contestata anche una sanzione pecuniaria per illecito trattamento dei dati sulla base dei nuovi poteri sanzionatori attribuiti al Garante dalla l. 27 febbraio 2009, n. 14, di conversione, con modificazioni, del d.l. 30 dicembre 2008 n. 207 (art. 162, comma 2-*bis*, del Codice).

Dall'accertamento svolto è emerso che nelle graduatorie - liberamente accessibili dall'*home page* del sito della Provincia - erano menzionati integralmente e senza alcuna limitazione, accanto al nominativo degli interessati, anche il codice fiscale, il comune di residenza, il reddito, nonché lo specifico stato di disabilità o di appartenenza alle altre categorie previste dalla normativa sul collocamento obbligatorio (invalido civile, invalido del lavoro, invalido di servizio, profugo, eventi terroristici, cieco assoluto, *ecc.*).

Nel provvedimento di blocco il Garante ha rilevato che l'amministrazione provinciale, nella predisposizione degli elenchi formati in attuazione della normativa sul collocamento obbligatorio, può effettuare le sole operazioni indispensabili per garantire la trasparenza delle graduatorie e il corretto svolgimento delle attività di avviamento al lavoro, astenendosi da ogni forma di diffusione di informazioni idonee a rivelare lo stato di salute (*Provv.* 21 aprile 2009 [doc. *web* n. 1616870]). Tali informazioni vanno rese conoscibili ai soggetti legittimati anche attraverso l'utilizzo di tecnologie telematiche, rispettando

il divieto di diffusione dei dati sulla salute.

Copia del provvedimento è stata inviata anche al Ministero del lavoro, della salute e delle politiche sociali e alla Conferenza Stato-Regioni affinché, nella predisposizione delle graduatorie dei disabili vengano individuate, in conformità alla legge, forme proporzionate di accessibilità ai dati in grado di contemperare il diritto alla riservatezza e la trasparenza amministrativa.

Pubblicazione *online* di dati relativi a consorzi e società di cui fanno parte le amministrazioni pubbliche

Con riferimento all'*"operazione trasparenza"* avviata dal Ministro per la pubblica amministrazione e l'innovazione, il Dipartimento per la funzione pubblica ha chiesto all'Autorità una valutazione sulla pubblicazione *online* di dati personali relativi ad incarichi ricoperti in consorzi e società di cui fanno parte le amministrazioni pubbliche. In particolare, è stato evidenziato che, tra i dati che le amministrazioni pubbliche sono tenute a comunicare al Dipartimento, ai sensi del comma 587 della legge finanziaria per il 2007 - definiti "pubblici" dal comma 591 della medesima legge - vi sono anche i nominativi e il trattamento economico lordo annuo degli incarichi ricoperti dai rappresentanti delle amministrazioni in consorzi e società. Al riguardo, l'Autorità ha condiviso la scelta del Dipartimento di non pubblicare sul proprio sito internet anche i codici fiscali di tali rappresentanti in quanto non pertinenti ed eccedenti rispetto alle finalità che si intendono perseguire con la predetta pubblicazione (*Nota* 20 aprile 2009).

Utilizzo di *test* psicoattitudinali nell'ambito di procedure concorsuali e pubblicazione su internet della relativa graduatoria

Un reclamo aveva lamentato la pubblicazione in internet della graduatoria di un concorso bandito da un comune, con le generalità dei candidati ed i risultati dei *test* psicoattitudinali utilizzati per descrivere e valutare alcuni tratti della personalità degli interessati nell'ambito della prova preselettiva. L'Ufficio, nel rilevare che l'utilizzo di strumenti telematici per finalità di trasparenza era previsto dal regolamento dell'ente locale e che la graduatoria, a seguito di un accertamento svolto, non risultava essere ancora disponibile sul *web*, ha osservato che, sebbene i risultati anche parziali, conseguiti dai candidati nei *test* espletati fossero riportati nella graduatoria preselettiva tramite formule numeriche, non poteva escludersi che le predette indicazioni consentissero - seppure in via mediata - di risalire al profilo psicologico degli interessati indicati nominativamente.

Al riguardo, è stato richiamato quanto indicato dal Garante nelle linee-guida sulla

pubblicazione di atti e documenti di enti locali in merito all'opportunità di dare attuazione al principio di pubblicità delle procedure concorsuali, nei casi in cui questa riguardi prevalentemente solo una o alcune categorie di persone, tramite forme di accesso in rete selezionato, attribuendo agli interessati una chiave personale (*username* e *password*; numero di protocollo o altri estremi identificativi della pratica forniti dall'ente agli aventi diritto), in modo da limitare la conoscibilità di taluni dettagli soltanto agli interessati e ai controinteressati (*Provv.* 19 aprile 2007 [doc. *web* n. 1407101] punto 5) (*Nota* 21 aprile 2009).

10.4.2. Rapporto di lavoro in ambito privato

Nel corso dell'anno l'Autorità ha avuto modo di pronunciarsi ripetutamente in ordine a distinti profili relativi ai trattamenti di dati personali nella gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati.

Un caso (*Provv.* 2 aprile 2009 [doc. *web* n. 1606053]) ha riguardato il monitoraggio costante e reiterato, effettuato da una società relativamente alla navigazione internet di un proprio dipendente; monitoraggio che avrebbe comportato la contestazione di una sanzione disciplinare, contribuendo così al successivo licenziamento dell'interessato.

Le risultanze ispettive hanno evidenziato che era stato installato un *software* che registrava sistematicamente gli accessi ai siti *web* visitati dal lavoratore, senza che tuttavia ricorressero i presupposti previsti dalla disciplina di settore in tema di controlli a distanza dell'attività lavorativa (art. 4, l. 20 maggio 1970, n. 300). Benché il dipendente, al pari del restante personale, fosse stato reso edotto del divieto di navigazione in internet per motivi diversi da quelli legati all'attività lavorativa e della possibilità di controlli sulla sua postazione individuale, il trattamento effettuato dalla società è risultato illecito sia per violazione degli artt. 11, comma 1, lett. *a*) e 114, del Codice, sia perché sproporzionato rispetto alla finalità perseguita (anche tenuto conto della forma reiterata e costante con cui il monitoraggio era stato effettuato).

Alla società è stato dunque vietato l'ulteriore trattamento di dati personali relativi agli accessi a internet effettuati dal lavoratore.

In un altro caso (*Provv.* 2 ottobre 2009 [doc. *web* n. 1665170]) la dipendente di una società ha chiesto l'intervento del Garante in relazione all'asserito accesso da parte della società stessa, durante un periodo trascorso in cassa integrazione guadagni, ai dati personali memorizzati nel computer aziendale in uso all'interessata. Era stato in particolare lamentato il mancato rilascio dell'informativa da parte della società (sia in ordine alle procedure aziendali volte a garantire l'accesso ai dati dei dipendenti assenti o sospesi dal servizio, sia al correlato trattamento), sottolineando inoltre l'eccedenza del trattamento medesimo in relazione al preteso accesso a *file* di natura personale (ritenuti estranei all'attività lavorativa e, in quanto tali, non accessibili dalla società).

A seguito di una complessa istruttoria non è risultato provato che la società avesse avuto concreto accesso (per il tramite di propri incaricati) ai dati personali in parola. Peraltro, le risultanze documentali hanno evidenziato che la stessa società aveva predisposto i necessari controlli di accesso e di autenticazione e che le cartelle erano configurate per assicurare la disponibilità dei dati in caso di emergenza. Inoltre, a tutto il personale dipendente era stata rilasciata apposita informativa con indicazione, tra l'altro, della possibilità di accesso al computer per ragioni organizzative dell'attività lavorativa.

Tuttavia, dagli atti non sono risultate chiare le condizioni di accesso da parte della società ai *file* contenuti nei computer assegnati in dotazione ai dipendenti; il Garante ha pertanto prescritto alla società di fornire agli interessati una puntuale informativa al riguardo.

In una segnalazione un dipendente di una cooperativa sociale aveva lamentato, anche in ragione della possibile circolazione del documento al di fuori del contesto lavorativo, l'esplicita indicazione nel prospetto di paga di informazioni relative alla propria appartenenza alla categoria delle *"persone svantaggiate"* (di cui all'art. 4, l. 8 novembre 1991, n. 381). Le risultanze istruttorie hanno evidenziato sia che il quadro normativo non autorizzava l'indicazione dello *status*, sia l'eccedenza dei dati trattati, attesa la possibilità di raggiungere la medesima finalità di trasparenza degli elementi della retribuzione con modalità alternative, quali l'adozione di codici sostitutivi, come peraltro già indicato in precedenti pronunce dell'Autorità (*cfr. Provv.* 19 febbraio 2002 [doc. *web* n. 1063659]

e *Provv.* 31 ottobre 2007 [doc. *web* n. 1459297]). Inoltre, il *software* utilizzato - in conformità al principio di necessità di cui all'art. 3 del Codice - avrebbe dovuto essere configurato già in partenza in modo da ridurre al minimo l'utilizzo di dati personali non necessari (nel caso di specie, peraltro, particolarmente delicati).

L'Autorità (*Provv.* 18 giugno 2009 [doc. *web* n. 1640331]) ha dunque prescritto alla cooperativa l'adozione di diciture sostitutive rispetto a quella di *"lavoratore svantaggiato"*.

Il Garante si è poi occupato (*Provv.* 2 ottobre 2009 [doc. *web* n. 1666101]) di alcune segnalazioni relative ad un patronato che (per il tramite di alcune sedi locali) aveva acquisito, in assenza di uno specifico mandato, dati personali riferiti ai segnalanti stessi (prevalentemente alle anagrafiche e alla loro situazione contributiva) che sarebbero stati successivamente utilizzati nell'ambito di una procedura di mobilità che aveva interessato la società di appartenenza.

Le risultanze istruttorie (anche ispettive) hanno evidenziato che il patronato, tramite appositi collegamenti telematici con i sistemi informativi dell'Inps, aveva effettivamente acquisito detti dati (in adempimento a specifiche richieste di un rappresentante sindacale allo stesso collegato e coinvolto nella gestione delle menzionate procedure di mobilità) per finalità di individuazione dei lavoratori "licenziabili" (anche in un'ottica di tutela degli stessi). Tale acquisizione è risultata tuttavia illecita perché effettuata (ancorché da un singolo incaricato presso la sede locale del patronato) in assenza di uno specifico mandato scritto da parte degli interessati (come previsto dalla pertinente disciplina di settore, dall'art. 116 del Codice e dalle stesse disposizioni impartite dal patronato a livello centrale); inoltre, non è risultata altrimenti provata l'acquisizione del consenso degli interessati, ovvero la ricorrenza di altro presupposto di liceità del trattamento (artt. 23, 24 e 26 del Codice).

Limitatamente a detto profilo, non sono state tuttavia formulate specifiche prescrizioni nei confronti del patronato (ferma restando l'illiceità del trattamento svolto e la risarcibilità del danno eventualmente arrecato in sede giudiziaria) atteso che il trattamento è risultato in contrasto con le apposite disposizioni da questo impartite e che erano stati comunque predisposti interventi formativi anche nei confronti dell'incaricato del

trattamento coinvolto nella vicenda. Inoltre, i modelli precedentemente utilizzati per la formale designazione degli incaricati del trattamento sono risultati successivamente integrati con le esplicite istruzioni in ordine alla necessaria acquisizione, al momento della raccolta dei dati riferiti agli utenti, del mandato di assistenza e rappresentanza.

In un'ottica di semplificazione degli obblighi derivanti dalla disciplina di protezione dei dati personali, l'Autorità ha invece prescritto al patronato (in ragione della complessiva articolazione strutturale dell'istituto) di designare quali responsabili del trattamento i soggetti operanti presso le relative strutture regionali.

Il Garante si è peraltro riservato di approfondire alcuni aspetti (pur emersi in sede istruttoria) relativi all'accesso telematico garantito ai patronati da alcuni istituti previdenziali in ordine alle proprie banche dati.

In un altro caso, l'ex dirigente di una società aveva contestato alla stessa di aver indebitamente pubblicato sul proprio sito internet un comunicato stampa che, nell'informare gli operatori del settore di alcune decisioni societarie (specie di carattere organizzativo), riportava tuttavia anche informazioni relative al suo stato di salute (provocandogli in tal modo anche difficoltà nel reinserimento professionale).

Nel ritenere fondate le doglianze del segnalante (*Provv.* 16 dicembre 2009 [doc. *web* n. 1689148]) l'Autorità ha ritenuto che, diversamente da quanto sostenuto dalla società, la locuzione *"stato morbile"* utilizzata nel caso di specie risultava idonea *"rivelare lo stato di salute"* dell'interessato in quanto per sé sola in grado di palesare informazioni attinenti alla sfera sanitaria del segnalante (a prescindere, cioè, dal puntuale riferimento a specifiche patologie dello stesso).

La pubblicazione del comunicato stampa contenente tali informazioni, pertanto, integrava un'ipotesi di diffusione di dati personali idonei a rivelare lo stato di salute, vietata dal Codice (art. 26, comma 5). Il trattamento è inoltre risultato in violazione del principio di pertinenza e non eccedenza stabilito dall'art. 11, comma 1, lett. *d*), del Codice, atteso che la società avrebbe comunque potuto assicurare la trasparenza richiesta dal mercato omettendo l'indicazione, nel comunicato stampa oggetto di pubblicazione, delle condizioni di salute riferite al segnalante.

L'Autorità ha pertanto vietato alla società l'ulteriore diffusione, per il tramite del proprio sito *web*, dei dati personali del segnalante idonei a rivelare il suo stato di salute.

A fronte delle molteplici istanze pervenute (quesiti, pareri, verifiche preliminari) da parte di numerosi operatori economici sovente appartenenti a gruppi multinazionali, l'Autorità è stata inoltre chiamata ad approfondire la tematica sul fenomeno del *cd. "whistleblowing"*.

Si tratta, in sostanza, di misure organizzative appositamente predisposte da detti operatori economici (in adempimento, talora, a specifiche indicazioni provenienti dalle società capogruppo) per rendere fruibili ai soggetti operanti a vario titolo al loro interno appositi canali comunicativi per segnalare presunti illeciti (riconducibili, in particolare, a fenomeni di corruzione o frode) ascrivibili a colleghi.

All'esito degli approfondimenti condotti, l'Autorità (stante la delicatezza del tema e la sua rilevanza sociale, anche in termini di impatto sui diritti e sulle libertà fondamentali degli interessati), ha presentato il 10 dicembre 2009 una segnalazione al Parlamento e al Governo [doc. *web* n. 1693019] indicando le ragioni che potrebbero giustificare un eventuale intervento normativo in materia.

Preliminarmente si è evidenziato che la tematica in esame è stata oggetto di attenzione da parte del Gruppo Art. 29 che, con parere del 1° febbraio 2006 (WP 117 [doc. *web* n. 1607645]), ha fornito alcune indicazioni per rendere i trattamenti di dati personali effettuati per il tramite dei menzionati sistemi di segnalazione conformi ai princìpi contenuti nella suddetta direttiva (con particolare riferimento al loro ambito di applicazione; ai presupposti di liceità del trattamento; all'esercizio del diritto di accesso da parte degli interessati; all'ammissibilità di denunce anonime).

I riferimenti normativi rinvenibili nell'ordinamento italiano (d.lgs. n. 231/2001, artt. 2105, 1175 e 1275 c.c., art. 21 Cost.) non consentono di inquadrare sistematicamente il fenomeno; peraltro, un eventuale intervento del Garante in materia, oltre a comportare scelte di più opportuna pertinenza parlamentare, si sarebbe rivelato necessariamente parziale e limitato e non avrebbe risolto i profili di criticità che il fenomeno in questione comporta in rapporto alla vigente normativa sulla protezione dei dati personali. Ciò, con particolare riferimento a:

- i presupposti di liceità del trattamento (non potendo al riguardo ravvisarsi un trattamento di dati personali riconducibile ad un obbligo legale e tenuto conto che l'alternativa percorribile - il *cd.* "bilanciamento di interessi" - avrebbe comportato un'inevitabile perimetrazione dell'ambito di applicazione dei sistemi di segnalazione, con conseguente esclusione di talune tipologie di trattamento);
- l'estensione del diritto di accesso (con particolare riferimento al diritto, da parte del soggetto segnalato, di conoscere l'origine dei dati e, segnatamente, quelli identificativi dell'autore della segnalazione) il cui esercizio potrebbe infirmare l'efficacia di tali sistemi, dissuadendo i segnalanti dal proprio intento di riferire i presunti illeciti;
- l'ammissibilità di eventuali segnalazioni *"anonime"*, suscettibili di usi strumentali e inidonee, in taluni casi, a consentire la raccolta di informazioni ulteriori. Il Garante ha quindi auspicato un intervento legislativo volto ad assicurare un equo contemperamento tra i diritti fondamentali delle persone coinvolte e le legittime esigenze di trasparenza e di tutela delle aziende presso le quali queste operano, in particolare segnalando al Parlamento e al Governo, l'opportunità di:
  - individuare i presupposti di liceità del trattamento e l'ambito soggettivo di applicazione dell'eventuale disciplina;
  - individuare i soggetti che possono assumere la qualità di *"segnalati"*;
  - individuare le finalità perseguibili e le fattispecie oggetto di possibile *"denuncia"*;
  - definire la portata del diritto di accesso previsto dall'art. 7 del Codice;
  - stabilire l'eventuale ammissibilità dei trattamenti derivanti da segnalazioni anonime.

Un'altra pronuncia dell'Autorità ha riguardato il reclamo del dipendente di una società controllata dal Ministero per i beni e le attività culturali, relativo ad asserite violazioni del Codice da parte del datore di lavoro, in particolare con riguardo alle disposizioni in materia di misure (anche minime) di sicurezza. Più precisamente, il reclamante aveva lamentato la diffusione tra i dipendenti della società, anche a mezzo fax, del contenuto

di un verbale di conciliazione di una vertenza di lavoro sottoscritto dall'interessato in sede giudiziale. A sostegno della propria posizione, tra la documentazione allegata, il reclamante aveva prodotto la fotocopia di un fax inviato da un'utenza facente capo ad una delle sedi della società.

L'Autorità non ha ritenuto di dover adottare un provvedimento collegiale sul caso di specie, poiché dalla documentazione in atti e dalle dichiarazioni rese (anche in sede ispettiva) dalla società, era emerso che il fax, pur inviato da un'utenza della società, non conteneva informazioni che consentissero di risalire al destinatario; né è stato possibile comprovare che la trasmissione del fax fosse stata effettuata da un incaricato della società. Inoltre, i fatti riferiti al reclamante erano risultati già conoscibili da una precedente comunicazione sindacale relativa alla vicenda, pure inoltrata via fax.

Le risultanze istruttorie di accertamenti *in loco* avevano inoltre evidenziato che la società aveva adottato misure di sicurezza in conformità alle prescrizioni contenute negli artt. 31 *ss.* del Codice e nelle regole dell'Allegato B. al Codice medesimo (*Nota* 14 maggio 2009).

In un altro caso, una lavoratrice aveva lamentato l'illecita comunicazione, da parte del suo pregresso datore di lavoro, di dati personali relativi alle proprie condizioni di salute ad altra società, presso la quale la segnalante aveva pure prestato, in precedenza, la propria opera e nei confronti della quale pendeva un giudizio relativo al rapporto di lavoro cessato.

La documentazione trasmessa da una società all'altra (consistente nella richiesta di tentativo di conciliazione e nel ricorso promosso dalla segnalante ai sensi dell'art. 414 c.p.c., contenente anche dati riferiti alle condizioni di salute dell'interessata), in seguito alla comunicazione al precedente ex datore, era stata depositata da quest'ultimo anche in un diverso procedimento pendente tra il medesimo e l'interessata.

Il Garante ha rilevato che la comunicazione dei dati sensibili riferiti alla segnalante, finalizzata alla sola difesa giudiziaria della società destinataria dei dati (art. 24, comma 1, lett. *f*) e 26, comma 4, lett. *c*), del Codice) non era stata effettuata lecitamente (artt. 11 e 26, comma 4, lett. *c*), del Codice). Ciò in quanto le informazioni di natura sensibile,