Infine, è stato rivolto un invito affinché i soggetti che fossero risultati privi di reale e autonoma capacità decisionale in ordine alle finalità e modalità del trattamento fossero designati quali responsabili ai sensi dell'art. 29 del Codice.

L'Autorità, che si è riservata ulteriori iniziative e determinazioni (anche alla luce di eventuali revisioni apportate al programma dall'Osservatorio), ha conclusivamente prescritto alle società sportive di disporre la pubblicazione del *provvedimento* sui propri siti *web* (ove esistenti) al fine di favorirne una immediata consultazione da parte degli utenti.

12. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

La materia dei trasferimenti transfrontalieri di dati personali è stata oggetto di costante attenzione nel corso del 2010 con riferimento sia alla attiva partecipazione del Garante ai lavori del Gruppo Art. 29, sia al rilascio di autorizzazioni al trasferimento dei dati verso Paesi terzi, in particolare tramite "*Binding Corporate Rules*" (*BCR*) ("*Norme vincolanti d'impresa*").

In merito, diversi contributi sono stati apportati nell'ambito del sottogruppo *BCR*, per promuovere una maggiore trasparenza verso l'esterno (attraverso la proposta di pubblicare sul sito della Commissione europea, una pagina *web* contenente le principali informazioni relative alla fase europea di approvazione delle *BCR* e alle modalità e ai tempi per ottenere le relative autorizzazioni nazionali) ed estendere progressivamente la platea delle Autorità aderenti al meccanismo di *cd.* "*mutuo riconoscimento*", giunte attualmente a quota 19. Tale sistema, volto ad accelerare i tempi della procedura europea di cooperazione, ha comportato nell'ultimo anno considerevoli vantaggi, attraverso la definizione in tempi rapidi di diverse procedure europee di approvazione delle *BCR*.

Il lavoro del sottogruppo si è inoltre rivolto alla definizione di un documento ad uso interno delle Autorità per fornire una comune interpretazione degli aspetti maggiormente problematici collegati alla valutazione di adeguatezza delle norme vincolanti d'impresa, e semplificare l'analisi delle bozze di *BCR* da parte della *lead Authority*, costituendo un valido ausilio nell'ambito della procedura di mutuo riconoscimento.

Nel documento relativo alle "*standard contractual clauses*" (clausole contrattuali tipo) (WP 176 del 12 luglio 2010), redatto con l'attiva partecipazione di questa Autorità, sono stati forniti chiarimenti sui principali dubbi interpretativi espressi dagli operatori del settore nella fase di prima applicazione della Decisione della Commissione n. 2010/87/EU del 5 Febbraio 2010 (v. *infra* par. 20.2.).

L'attività del Garante è stata intensa anche a livello nazionale. La citata Decisione n. 2010/87/EU in materia di clausole contrattuali tipo è stata oggetto nel maggio 2010 di attuazione nell'ordinamento italiano, mediante specifica autorizzazione (*Provv.* 27 maggio 2010 [doc. *web* n. 1728496]). Il documento autorizza, con effetto dal 15 maggio 2010,

i trasferimenti di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea (da titolare a responsabile) effettuati in conformità ad un nuovo schema di clausole contrattuali tipo, recante al proprio interno una clausola di "*subcontratto*" (v. *Relazione* 2009, p. 189). Al contempo, con tale autorizzazione il Garante ha raccolto l'invito della Commissione ad estendere l'applicazione del nuovo *set* di clausole contrattuali tipo anche a responsabili stabiliti in UE, che affidino il trattamento a subincaricati stabiliti in un Paese terzo, prevedendo, in capo al titolare del trattamento, l'obbligo di comunicare al Garante l'avvenuta designazione in successione di più di un subincaricato del trattamento (v. Decisione della Commissione n. 2010/87/UE, considerando 23).

Con riferimento al settore delle *BCR* l'Autorità, con i provvedimenti dell'8 aprile 2010 [doc. *web* n. 1717863] e del 7 ottobre 2010 [doc. *web* n. 1763052], si è pronunciata per la prima volta in ordine ad alcuni progetti di norme vincolanti d'impresa elaborati da importanti gruppi societari di carattere multinazionale.

Nel primo caso, l'istanza di autorizzazione è stata presentata da un gruppo multinazionale statunitense operante nel settore della ristorazione alberghiera, a seguito della conclusione, da parte della *lead Authority* (Autorità di protezione dei dati personali del Regno Unito di Gran Bretagna e Irlanda del Nord-*Information Commissioner's Office*), del procedimento di cooperazione europea instauratosi secondo il sistema di mutuo riconoscimento. La richiesta riguardava i trasferimenti intragruppo dei dati personali relativi ai dipendenti e alla clientela dal territorio dello Stato italiano, verso le filiali con sede in Paesi non appartenenti all'Unione europea.

Il Garante, a seguito di una complessa istruttoria, nel corso della quale ha preso atto delle dichiarazioni integrative rese dalla richiedente alla stessa Autorità (relative in particolare al contenuto e all'efficacia vincolante della clausola di responsabilità e del terzo beneficiario, nonché all'esatta portata dell'obbligo di adempimento delle misure di sicurezza prescritte dalla legge), ha autorizzato il trasferimento summenzionato secondo le modalità fissate nelle *BCR*, per il perseguimento delle sole finalità ivi dichiarate.

Il Garante ha comunque ribadito il proprio potere di svolgere in qualsiasi momento i necessari controlli sulla liceità e correttezza del trasferimento dei dati e, comunque, su

ogni operazione di trattamento ad essi inerente, nonché di adottare, se necessario, eventuali provvedimenti di blocco o di divieto. Infine, ha precisato che le operazioni di trattamento dei dati personali, anche se poste in essere a seguito del rilascio dell'autorizzazione, saranno lecite solo ove conformi alla normativa nazionale vigente e alle sue successive modificazioni, anche in materia di protezione dei dati personali, con particolare riferimento alle specifiche disposizioni sui presupposti di legittimità delle attività di raccolta dei dati oggetto del trasferimento e sulla sussistenza dei presupposti di legittimità per la comunicazione dei dati medesimi.

Di analogo tenore l'autorizzazione nazionale adottata dal Garante il 7 ottobre 2010, a seguito della definizione di una procedura di cooperazione europea attivata secondo le forme previste dal WP 107, nei confronti di un importante gruppo statunitense operante nel settore bancario e finanziario.

L'istanza aveva ad oggetto il trasferimento infragruppo, verso Paesi terzi, dei dati personali relativi al personale, anche interinale, ai fornitori, ai clienti, anche potenziali, ai referenti presso clienti aziendali, alle controparti, ai consorziati e altri operatori del mercato, nonché ai subappaltatori, per le finalità connesse alla gestione del rapporto di lavoro e alle operazioni svolte dalle società nell'esercizio della propria attività.

Anche in questo caso il Garante ha effettuato una complessa istruttoria, chiedendo opportuni chiarimenti in merito all'individuazione dei soggetti coinvolti nel trasferimento intragruppo dei dati verso Paesi terzi, all'ambito di applicazione delle clausole di responsabilità e del terzo beneficiario, alle definizioni contenute nel testo, ai diritti dell'interessato e all'esatta indicazione della tipologia dei dati personali oggetto delle *BCR*. L'autorizzazione è stata rilasciata nei limiti delle modalità di trasferimento indicate nelle *BCR* e per il perseguimento delle sole finalità ivi dichiarate.

Privacy e agenzie di *rating*: maggiori controlli sui conflitti di interesse

Con riguardo al delicato tema del conflitto di interesse e del connesso trattamento di dati personali, il Garante è intervenuto con una importante decisione nel corso del 2010, che ha tratto origine dalla richiesta della filiale italiana di un'agenzia di *rating* statunitense di poter consultare, sulla base di una specifica *policy* interna aziendale, le informazioni relative alle operazioni su strumenti finanziari eseguite dai propri dipendenti e dai soggetti

facenti parte del loro nucleo familiare ristretto. Senza tali controlli, infatti, la società capogruppo, che opera in tutto il mondo, non avrebbe potuto ottemperare alla normativa vigente negli Stati Uniti, che richiede di certificare che l'attività di *rating* venga svolta in modo indipendente e senza essere influenzata da alcun conflitto di interessi anche dalle relative società controllate e/o collegate.

Nell'istruttoria, l'Autorità ha tenuto conto della recente normativa europea sul tema (*Regolamento* (CE) n. 1060/2009 del Parlamento europeo e del Consiglio del 16 settembre 2009, relativo alle agenzie di *rating* del credito), volta a migliorare, in particolare, la trasparenza, la responsabilità e l'affidabilità delle attività di *rating* del credito nella Comunità, per garantire un buon funzionamento del mercato interno e, al contempo, raggiungere un elevato grado di protezione degli investitori. È risultato necessario bilanciare la tutela della *privacy* con altre finalità di rilevante interesse pubblico quali l'indipendenza, l'oggettività e la qualità dei *rating* utilizzati nella Comunità, nonché la prevenzione di situazioni di conflitto di interesse. Pertanto, il Garante ha stabilito che la società potrà raccogliere e utilizzare i dati relativi agli strumenti finanziari, e alle operazioni ad essi connesse, di cui risultino detentori i dipendenti purché le informazioni, oggetto di trattamento, attinenti alle circostanze economiche e personali relative a tali soggetti, siano limitate all'accertamento della sussistenza dell'ipotetico conflitto di interessi (art. 11, comma 1, lett. *a*) e *b*), del Codice). L'Autorità ha inoltre precisato che tali dati potranno essere trattati per il perseguimento della sola predetta finalità e, comunque, nel rispetto dei princìpi e dei limiti stabiliti dalla normativa comunitaria vigente, anche con riferimento all'individuazione dei soggetti appartenenti al *cd.* "nucleo familiare ristretto", i quali dovranno essere ricondotti alle figure indicate nell'art. 1, par. 2 della Direttiva n. 2004/72/CE del 29 aprile 2004. L'agenzia di *rating*, inoltre, dovrà fornire a tutti gli interessati un'adeguata e puntuale informativa separatamente dalla relativa *Policy* aziendale e in lingua italiana. Infine, l'Autorità ha sottolineato che qualunque dato trattato dalla società in violazione della disciplina sulla *privacy* non potrà essere utilizzato (*Provv.* 19 maggio 2010 [doc. *web* n. 1736161]).

13. LIBERE PROFESSIONI

13.1. ORDINI PROFESSIONALI

Nel corso del 2010 sono pervenuti al Garante diversi quesiti concernenti, in particolare, il regime di conoscibilità delle informazioni relative agli iscritti agli albi.

Al riguardo, in termini generali, è stato ribadito che la diffusione dei dati degli iscritti ad un ordine professionale deve essere valutata in concreto dal relativo consiglio, in considerazione delle specifiche forme di pubblicità previste dalla normativa di settore.

Più in dettaglio, un consiglio nazionale aveva chiesto se fosse possibile, per esigenze di trasparenza, pubblicare sul proprio sito *web* i nominativi degli iscritti all'ordine destinatari di una sanzione disciplinare definitiva.

In proposito è stato evidenziato che può essere "*menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio delle professione*", purché il trattamento riguardi informazioni corrette, complete ed aggiornate (art. 11, comma 1 e 61, comma 2, del Codice; *Provv.* 29 marzo 2001 [doc. *web* n. 39536]; *Relazione* 2003, p. 82) (*Nota* 18 gennaio 2010).

È stato evidenziato ad un ordine professionale, in merito alla possibilità di diffondere gli indirizzi di posta elettronica degli iscritti, che una specifica recente normativa di settore prevede che i professionisti iscritti in albi ed elenchi debbano comunicare ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica (*Nota* 30 luglio 2010).

In termini analoghi si è risposto ad un avvocato che lamentava la pubblicazione sull'albo, in particolare, del suo codice fiscale (prevista dall'art. 3-*bis* del d.l. 29 dicembre 2009, n. 193, convertito, con modificazioni, dalla l. 22 febbraio 2010, n. 24) (*Nota* 31 marzo 2010).

14. Trattamento dei dati personali in ambito condominiale

In questa materia, nella quale la casistica è di significativa rilevanza, si menziona un ricorso nel quale si lamentava l'affissione in spazi condominiali accessibili a terzi, di documenti contenenti dati personali riferiti all'istante (e, segnatamente, di una comunicazione avente ad oggetto la convocazione di un'assemblea straordinaria e di una copia del ricorso introduttivo che la ricorrente aveva proposto nei confronti di una delibera condominiale), in seguito rimossi. Si lamentavano, altresì, nuove affissioni nella bacheca, recanti la ripartizione delle spese sostenute dai singoli partecipanti (nominativamente identificati) in ambito condominiale.

L'Autorità ha ritenuto fondate le doglianze, per violazione, oltre che del principio di necessità (art. 3, del Codice), delle disposizioni in tema di pertinenza e non eccedenza dei dati trattati (artt. 3, 11, comma 1, lett. *d*), del Codice), evidenziando che le finalità perseguite avrebbero potuto essere ugualmente perseguite omettendo i riferimenti all'interessata e, comunque, ricorrendo a modalità alternative di comunicazione con gli altri partecipanti al condomino (cfr. *Provv.* 19 febbraio 2009 [doc. *web* n. 1601674]). In mancanza del consenso dell'interessata alla divulgazione dei suoi dati personali, il trattamento è stato ritenuto illecito, con prescrizione al condominio di adottare opportune misure volte a conformarlo alla disciplina di protezione dei dati personali (*Provv.* 8 luglio 2010 [doc. *web* n. 1741950]).

Il Garante si è poi pronunciato in ordine alla liceità del trattamento operato da una società a responsabilità limitata (nella sua qualità di amministratore di un condominio) conseguente all'avvenuta partecipazione di alcuni suoi soci alle assemblee condominiali.

Al riguardo, l'Autorità ha precisato che il trattamento svolto nel caso di specie non poteva considerarsi lecito, posto che tra i poteri dei soci legislativamente (art. 2479 c.c.) e statutariamente (art. 11 dei patti sociali) previsti non figurava il diretto e personale espletamento di attività attuative dell'oggetto sociale (l'amministrazione dei condomini e la gestione dei servizi comuni relativi agli immobili); al contrario, dal materiale documentale acquisito agli atti è emerso che l'unico soggetto concretamente legittimato ad amministrare

e rappresentare il condominio (perseguendo, così, l'oggetto sociale della società) risultava, in base alla legge, all'atto costitutivo e ai patti sociali, l'amministratore unico della società. Inoltre, non è risultato provato che la partecipazione in assemblea dei predetti soci fosse stata ritenuta necessaria dagli stessi partecipanti all'assemblea condominiale.

Il Garante ha dunque prescritto alla società, nella sua dichiarata veste di titolare del trattamento, di adottare idonee misure organizzative tese a prevenire la partecipazione alle assemblee del condominio di soggetti non effettivamente legittimati (*Provv.* 9 settembre 2010 [doc. *web* n. 1758751]).

15. La videosorveglianza e la biometria

15.1. Videosorveglianza in ambito pubblico

Nel 2010 il Garante è stato più volte chiamato a fornire chiarimenti sul nuovo *provvedimento* generale adottato in materia di videosorveglianza (*Provv.* 8 aprile 2010 [doc. *web* n. 1712680], in *G.U.* 29 aprile 2010, n. 99; *Relazione* 2009, p. 25 ss.).

Conformemente a quanto già registrato in questa sede da alcuni anni, anche quest'anno molti comuni, dopo aver adottato uno specifico *provvedimento* per disciplinare le modalità d'installazione di un sistema di videosorveglianza sul proprio territorio, lo avevano trasmesso al Garante per ottenerne l'approvazione ovvero solo per darne conoscenza. Al riguardo, è stato ribadito che l'installazione di tali sistemi non deve essere sottoposta all'esame preventivo del Garante, fatte salve le specifiche ipotesi per le quali è necessario richiedere una verifica preliminare, e che non può desumersi alcuna approvazione implicita dal silenzio del Garante dopo la ricezione di documenti relativi a progetti di videosorveglianza (punti 3.2.1. e 3.2.2. del cit. *provvedimento* generale; art. 17 del Codice) (*Note* 9 giugno; 18 giugno; 9 luglio; 23 agosto; 25 ottobre; 4 novembre; 15 novembre; 22 novembre e 24 novembre 2010).

Chiarimenti circa l'applicazione del nuovo *provvedimento* del Garante in materia di videosorveglianza sono stati, altresì, richiesti da numerosi comuni all'Associazione nazionale comuni italiani (ANCI), che ha ritenuto opportuno predisporre delle apposite linee-guida, invitando l'Autorità a collaborare al fine di fornire adeguate indicazioni per l'installazione e la gestione di telecamere e sistemi di controllo video anche a fini di sicurezza urbana.

Un'università, un'azienda sanitaria locale, un comune e una regione avevano chiesto al Garante la possibilità di conservare le immagini registrate tramite un sistema di videosorveglianza per un tempo superiore alle 24 ore ma non eccedente la settimana. Al riguardo, il Garante ha evidenziato che –fatte salve le speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi o richieste investigative dell'autorità giudiziaria o di polizia giudiziaria– la conservazione deve essere limitata alle 24 ore successive alla rilevazione e solo in alcuni casi, per peculiari esigenze tecniche o per la

particolare rischiosità dell'attività svolta dal titolare del trattamento, può ritenersi ammesso un tempo più ampio, che non superi comunque la settimana.

In tale quadro, spetta al titolare del trattamento valutare la sussistenza in concreto dei presupposti che giustificano la conservazione delle immagini raccolte, per un periodo di tempo inferiore alla settimana; la conservazione delle immagini per un periodo superiore necessita invece della verifica preliminare dell'Autorità (punti 3.2.1. e 3.4. del cit. *provvedimento* generale; art. 17 del Codice) (*Note* 28 luglio; 7 dicembre; 13 dicembre e 20 dicembre 2010).

A seguito di segnalazioni e di quesiti, sono stati forniti chiarimenti anche sull'istallazione di sistemi di videosorveglianza presso istituti scolastici ribadendo, in particolare, la necessità di garantire "*il diritto dello studente alla riservatezza*" (art. 2, comma 2, d.P.R. 24 giugno 1998, n. 249) e prevedendo opportune cautele al fine di assicurare l'armonico sviluppo della personalità dei minori. L'utilizzo di sistemi di videosorveglianza è ammissibile solo se indispensabile per tutelare l'edificio ed i beni scolastici da atti vandalici, riprendendo solo le aree interessate, attivando gli impianti negli orari di chiusura degli istituti e vietando la messa in funzione delle telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche all'interno della scuola (punto 4.3.1.).

Inoltre, laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo le aree non strettamente pertinenti l'edificio (punto 4.3.2.); infine è stato ricordato che il mancato rispetto di quanto prescritto al riguardo comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (*Note* 28 luglio e 28 dicembre 2010).

Sempre in ambito scolastico, talune rappresentanze sindacali avevano lamentato la collocazione delle telecamere in prossimità dell'apparecchiatura marcatempo utilizzata per rilevare le presenze del personale ATA o del registro utilizzato dai docenti per documentare le loro presenze, in modo da rendere possibile un controllo dell'attività dei lavoratori.

Al riguardo, è stato fatto presente che nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, e quindi di installazione di apparecchiature specificatamente preordinate alla predetta finalità; non devono perciò essere

effettuate riprese al fine di verificare la correttezza nell'esecuzione della prestazione lavorativa (ad es., orientando la telecamera sul *badge*). Inoltre, quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive ovvero è richiesta per la sicurezza del lavoro, devono essere osservate le garanzie previste in materia: in tali casi gli impianti "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti*" (artt. 4 e 8, l. 20 maggio 1970, n. 300; artt. 113 e 114 del Codice; art. 2 d.lgs. 30 marzo 2001, n. 165) (*Note* 7 e 15 dicembre 2010).

Le garanzie in materia di controlli a distanza dell'attività lavorativa sono state richiamate anche nei confronti di una Regione e di una sede territoriale della motorizzazione civile che avevano installato gli impianti di videosorveglianza presso i propri uffici (*Note* 6 settembre e 29 luglio 2010).

Infine, ad una azienda sanitaria dell'Emilia-Romagna è stato ricordato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti (quali le unità di rianimazione e reparti di isolamento) è limitato ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati e richiede tutti gli accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche nel rispetto del *provvedimento* generale del 9 novembre 2005 [doc. *web* n. 1191411] sul rispetto della dignità delle persone nelle strutture sanitarie.

Inoltre, il titolare del trattamento deve garantire che alle immagini rilevate per le predette finalità possano accedere solo i soggetti specificamente autorizzati; particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti di ricoverati) in reparti dove non sia consentito agli stessi di recarsi personalmente (quale quello di rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.

In ogni caso, in applicazione del divieto di diffusione di immagini idonee a rivelare lo stato di salute di cui all'art. 22, comma 8, del Codice, non possono essere diffuse su *monitor* collocati in locali liberamente accessibili al pubblico immagini di persone malate.

Il mancato rispetto di quanto sopra oltre a rendere applicabili le sanzioni amministrative stabilite dall'art. 162, comma 2-*bis* e 2-*ter*, del Codice, può integrare la fattispecie di reato stabilita dall'art. 167, comma 2, del Codice. (cfr. punto 4.2. del cit. *Provv.* 8 aprile 2010) (*Nota* 15 dicembre 2010).

15.2. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Da accertamenti ispettivi svolti in seguito ad una segnalazione è risultato che, per finalità di sicurezza, presso un centro commerciale era stata installata una *webcam* in assenza della prescritta informativa e in violazione della pertinente disciplina di settore in tema di controlli a distanza dell'attività dei lavoratori (art. 4, comma 2, l. n. 300/1970), con conseguente illiceità del trattamento svolto (artt. 11, comma 1, lett. *a*) e 114, del Codice).

Il Garante ha quindi disposto il blocco del trattamento effettuato a mezzo della *webcam* installata, in attesa dell'eventuale espletamento delle procedure previste dal richiamato art. 4, comma 2, l. n. 300/1970 (*Provv.* 10 giugno 2010 [doc. *web* n. 1736167]).

L'Autorità si è poi pronunciata in relazione ad una istanza di verifica preliminare presentata da una società operante nel settore della progettazione e produzione di *smart card* principalmente per il mercato *GSM* e bancario e volta ad ampliare, quale misura di protezione ulteriore a garanzia dei clienti, i tempi di conservazione delle immagini registrate a mezzo dell'impianto di videosorveglianza installato presso la sede operativa della società; ciò, muovendo dall'assunto che l'attività svolta, assimilabile a quella della Zecca di Stato, sarebbe stata potenzialmente soggetta ad un alto rischio di illecito.

Il periodo di conservazione suggerito dalla società (90 giorni), "imposto" dagli enti certificatori (tra i più noti, VISA, MASTERCARD, *GSM Association*) anche ai fini di un eventuale rinnovo delle stesse certificazioni, avrebbe inoltre risposto all'esigenza di rafforzare le misure di prevenzione e contrasto contro possibili comportamenti fraudolenti da parte di terzi (in particolare, i lavoratori della società), consentendo l'accertamento a posteriori

di possibili illeciti di natura penale suscettibili di verifica solo a distanza di tempo dalla loro commissione (anche in ragione delle complesse procedure organizzative e produttive in essere presso la società).

L'Autorità ha rigettato l'istanza ritenendo sproporzionati i tempi di conservazione proposti in relazione alle esigenze prospettate, peraltro non sufficientemente documentate (*Provv.* 4 novembre 2010 [doc. *web* n. 1767759]). Da un lato, infatti, le "prescrizioni" impartite dagli enti certificatori sono risultate "derogabili" in presenza di "restrizioni legali" all'utilizzo di sistemi di videosorveglianza; dall'altro, non sono stati addotti elementi rigorosi tali da giustificare il segnalato allungamento dei tempi di conservazione delle immagini in rapporto alle (ipotetiche) condotte criminose descritte dalla società, peraltro mai verificatesi in concreto (verosimilmente anche in ragione delle altre numerose misure di sicurezza già approntate: accessi controllati; sensori di allarme e di movimento; sistemi di criptazione dei dati; divieto di utilizzo di strumenti di archiviazione, ecc.).

L'Autorità ha peraltro ricordato il consolidato orientamento giurisprudenziale che riconosce al datore di lavoro la possibilità, nel rispetto delle garanzie previste dall'ordinamento (in particolare, gli artt. 2, 3 e 6 della l. n. 300/1970), di adibire a mansioni di vigilanza e tutela del patrimonio aziendale anche propri dipendenti, a mezzo dei quali poter controllare l'attività di altri lavoratori per accertare eventuali comportamenti fraudolenti estranei alla prestazione lavorativa e incidenti sull'integrità del patrimonio aziendale.

15.3. BIOMETRIA

Biometria e luoghi di lavoro

Nel corso dell'anno il Garante è stato nuovamente interpellato in ordine all'utilizzabilità, da parte di soggetti pubblici, di sistemi di rilevazione automatica per il controllo degli accessi al luogo di lavoro mediante il riconoscimento dei dati biometrici dei dipendenti. Si è reso, quindi, necessario ribadire le indicazioni contenute nel *provvedimento* generale recante le linee-guida in materia (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]).

In particolare, il Garante ha ricordato ad una amministrazione comunale, a seguito di una specifica segnalazione di un sindacato che, di regola, i sistemi di rilevazione di impronte digitali possono essere attivati soltanto per l'accesso a speciali aree dei luoghi di

lavoro in cui si debbano assicurare elevati e specifici livelli di sicurezza, in relazione a particolari necessità e nel rispetto di specifiche condizioni indicate nel cit. *provvedimento* generale (cfr. punto 7.2.). Il Comune è stato quindi invitato a verificare l'eventuale sussistenza di tali condizioni e ad informare l'Ufficio in ordine alle misure volte ad assicurare il rispetto di quanto indicato (*Nota* 20 dicembre 2010; v., *infra*, *Nota* 31 dicembre 2010).

In un'altra occasione, in risposta alle preoccupazioni manifestate da un Prefetto, circa istanze sindacali relative al trattamento di dati biometrici dei lavoratori italiani presso una base militare degli Stati Uniti, il Garante, con disponibilità ad esaminare eventuali profili critici, ha ricordato che, nel corso di una fruttuosa attività di collaborazione con l'Ambasciata americana, sono state fornite puntuali indicazioni anche sugli adempimenti procedurali necessari per rendere il trattamento conforme alla disciplina sulla protezione dei dati. Da ultimo l'Ambasciata si era riservata di valutare la possibilità di formulare all'Autorità una richiesta di interpello per l'implementazione di una carta elettronica che consenta l'accesso ai sistemi informatici delle basi militari (*Nota* 9 luglio 2010).

Nel fornire indicazioni ad alcuni dipendenti italiani di un'altra base militare americana, l'Ufficio ha precisato che il trattamento dei dati biometrici effettuato per le sole finalità di autenticazione informatica non richiede la valutazione preventiva del Garante. L'adozione di un sistema di autenticazione informatica (conforme ai requisiti tecnici indicati dalle regole 1-11 dell'Allegato B. al Codice) costituisce infatti una misura minima di sicurezza, che deve essere adottata ai sensi dell'art. 34, comma 1, lett. *a*), del Codice. Tali credenziali di autenticazione possono consistere anche in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o a una parola chiave (*Nota* 31 dicembre 2010).

Con riferimento all'uso delle impronte digitali dei lavoratori per l'accesso a particolari aree riservate sono state richiamate le regole restrittive di cui sopra si è fatto cenno, indicate nel *provvedimento* 14 giugno 2007 [doc. *web* n. 1417809], in particolare al punto 7.2. (*Nota* 31 dicembre 2010; v., *supra*, *Nota* 20 dicembre 2010).

Pur rientrando tra le legittime facoltà del datore di lavoro quella di sovrintendere all'esecuzione della prestazione lavorativa (art. 2094 c.c.), verificando le presenze dei

dipendenti e il rispetto dell'orario di lavoro, le imprese che intendono adottare sistemi di lettura delle impronte digitali per verificare la presenza in servizio dei dipendenti devono prima dimostrare che le finalità di controllo non possano essere realizzate con sistemi meno invasivi, nel rispetto dei princìpi di necessità e di proporzionalità.

Con questa motivazione l'Autorità ha respinto le richieste di verifica preliminare, ai sensi dell'art. 17 del Codice, con le quali due società di trasporti chiedevano di poter usare, presso le proprie aziende, un meccanismo di autenticazione biometrico (*provvedimenti* 17 novembre 2010 [doc. *web* nn. 1779745 e 1779758]).

Secondo le società, il rilevamento delle impronte avrebbe potuto evitare eventuali condotte irregolari, come lo scambio di *badge* attestanti la presenza in servizio, con conseguenti maggiori garanzie per l'incolumità degli utenti e del personale viaggiante. Nel corso dell'istruttoria, tuttavia, è emerso che i tradizionali metodi di controllo si erano dimostrati più che sufficienti a garantire la verifica della presenza in servizio dei dipendenti.

L'uso dei sistemi biometrici era stato richiesto dalle due società anche per accedere ai locali nei quali venivano custodite le banche dati cartacee e informatiche contenenti i dati personali dei dipendenti. Dagli accertamenti effettuati dal Garante è invece emerso che tali dati, lungi dall'essere caratterizzati da specifiche peculiarità, non richiedevano particolari sistemi di controllo, trattandosi di informazioni solitamente elaborate dagli uffici amministrativi di qualsiasi azienda.

16. Il Registro dei trattamenti

In attuazione della direttiva europea relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Direttiva n. 95/46/CE), in riferimento alla quale la Commissione europea ha pubblicato il 4 novembre 2010 una Comunicazione che fissa le linee generali per la revisione di tale direttiva aprendo una consultazione pubblica conclusasi il 15 gennaio 2011, il Codice prevede che l'Autorità abbia il compito di tenere il Registro dei trattamenti, formato sulla base delle notificazioni ricevute (così l'art. 154, comma 1, lett. *l*), del Codice).

Tale Registro, secondo quanto disposto dall'art. 37, comma 4, del Codice deve essere accessibile a chiunque e consultabile gratuitamente per via telematica.

Tali condizioni di accessibilità sono state garantite fin dal 2004, con la realizzazione di una procedura di notificazione telematica ed un'apposita sezione del sito Internet dell'Autorità, dedicata alla consultazione *online* del Registro.

La notificazione consiste in una dichiarazione formale compilata direttamente sul *computer* dell'utente, con la quale vengono comunicati al Garante i trattamenti di dati suscettibili di recare particolare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali. (cfr. artt. 37 e 38 del Codice; *Provv.* 31 marzo 2004 [doc. *web* n. 852561]; *Relazione* 2004, p. 109 ss.).

Con riguardo, in particolare, alle modalità di compilazione del modello informatico e ai suoi contenuti, il Garante, che sin dal 2004 ha introdotto profondi cambiamenti in relazione ai profili procedurali della notificazione, ha operato una ulteriore semplificazione con il *provvedimento* a carattere generale del 22 ottobre 2008 [doc. *web* n. 1571196] nel contesto di modifiche normative volte alla semplificazione ed all'accelerazione delle procedure amministrative.

Tale *provvedimento*, in particolare, ha individuato il nuovo modello di notificazione e, tra l'altro, ha limitato i casi in cui si deve indicare il luogo principale di custodia dei dati ed ha sottratto al pagamento dei diritti di segreteria la modifica di elementi quali il numero telefonico, di fax e l'indirizzo di posta elettronica del titolare.