Codice, sia tenuto a predisporre idonee misure organizzative che consentano l'esercizio stesso, attraverso modalità semplici e non onerose per l'interessato.

Spam proveniente dall'estero

L'attività di contrasto al fenomeno dello *spam* proveniente dall'estero incontra ancora ostacoli a causa di alcune differenze tra le legislazioni degli Stati europei, in termini sia di disciplina sostanziale, sia di tutele garantite dall'ordinamento giuridico, in relazione alla veste giuridica dei destinatari delle comunicazioni promozionali automatizzate indesiderate (per le disposizioni che hanno in buona misura escluso dall'ambito di applicazione del Codice le persone giuridiche v. d.l. n. 201/2011, convertito dalla l. n. 214/2011; v. par. 2.1.1.).

In tema di illecito trattamento dati mediante l'invio di fax, l'Autorità si è pronunciata nei confronti di una società che, sebbene conservasse all'estero i dati personali e li gestisse in modalità remota, utilizzava in modo prevalente e per le funzioni più importanti un apparato di rete (fax *gateway*) collocato sul territorio italiano. Per tale ragione, il Garante ha ritenuto la società tenuta al rispetto della normativa del Codice e quindi ha dichiarato illecito e inibito l'invio di fax promozionali mediante modalità automatizzate, senza aver fornito un'idonea informativa, senza aver acquisito il consenso dell'interessato, e in assenza di un idoneo recapito per l'esercizio dei diritti di cui all'art. 7 del Codice.

Inoltre, il Garante ha prescritto alla medesima società di predisporre, quale titolare del trattamento, per ogni messaggio in uscita, un riquadro (*template*) recante un'idonea informativa, e di verificare l'esistenza di un consenso preventivo, specifico e informato dei destinatari delle suddette comunicazioni promozionali.

L'Autorità ha inoltre ravvisato nel trattamento dati effettuato, la configurabilità –oltre che delle violazioni amministrative concernenti l'omesso rilascio dell'informativa e l'omessa acquisizione del consenso– anche della violazione penale relativa al trattamento illecito di dati (art. 167 del Codice), in ragione del nocumento conseguente all'invio massivo di fax. Il Garante si è altresì riservato di verificare, con autonomi procedimenti, la liceità del trattamento operato dalle singole società committenti individuate nel corso dell'ispezione e dei successivi accertamenti (provv. 7 aprile 2011 [doc. *web* n. 1810207]).

Più in generale, per i casi in cui l'invio di comunicazioni promozionali automatizzato è risultato episodico, l'Autorità ha inviato apposite note di richiamo al pieno rispetto della

disciplina in materia (note 30 novembre 2011 e 7 dicembre 2011) e talora avviato autonomi procedimenti sanzionatori per la contestazione delle sanzioni amministrative previste dagli artt. 161 e 162, comma 2-*bis*, del Codice.

9.10. DATI PERSONALI UTILIZZATI A FINI DI PROFILAZIONE E *MARKETING*

Nel 2011 il Garante ha proseguito l'attività ispettiva avviata nel 2010 per la verifica del corretto adempimento, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico, delle misure tecnico-giuridiche prescritte con i provvedimenti emanati a seguito delle istanze di *prior checking* da essi presentate all'Autorità, relative all'utilizzo dei dati personali aggregati di traffico telefonico e telematico dei clienti, per finalità di profilazione, senza l'acquisizione del relativo specifico consenso, così come stabilito nel provvedimento generale del 25 giugno 2009 [doc. *web* n. 1629107].

Nell'ambito di tale attività l'Autorità ha riscontrato una serie di irregolarità ed inadempimenti da cui sono scaturiti provvedimenti di blocco dei trattamenti di profilazione, sino alla verifica del puntuale e completo adempimento delle misure prescritte.

In alcuni casi, a fronte degli accertati inadempimenti, sono state anche comminate rilevanti sanzioni amministrative. In altri casi il Garante ha dettato ulteriori misure prescrittive volte a rafforzare la tutela dei soggetti interessati.

Presso gli stessi operatori coinvolti, l'Autorità ha poi dato avvio alla verifica dell'effettiva attuazione di tutte le prescrizioni impartite.

Con riguardo all'attività di profilazione, sono pervenute anche nuove istanze di verifica preliminare che hanno condotto all'emanazione di provvedimenti diretti a consentire tale attività con l'utilizzo di dati aggregati degli utenti, sulla base del previsto esonero dall'acquisizione del consenso, una volta adottate le specifiche misure tecnico-giuridiche dettate dal Garante.

9.11. ISTRUTTORIE SU CASI DI MALFUNZIONAMENTO DI SISTEMI E DI DISPERSIONE DI DATI PERSONALI

Nell'aprile 2011 l'Autorità ha verificato la liceità del trattamento dati effettuato da un'importante società multinazionale mediante dispositivi smartphone/tablet computer, i

quali registrano e conservano nella loro memoria interna dati relativi alla posizione dell'utente nonché alle celle di rete mobile e degli access point Wi-Fi rilevati in prossimità (dato che può indirettamente identificare la posizione dell'utente).

Sul caso, rispondendo ad apposita richiesta di informazioni formulata dall'Autorità, la società ha comunicato di aver reso disponibile, un aggiornamento *software* gratuito che ha risolto diversi dei problemi evidenziati ed originati da un cd. "bug", ed ha aggiunto nuove funzioni correttive idonee a risolvere i problemi lamentati.

Tra il 17 ed il 19 aprile 2011 alcuni sistemi informatici di un grande gruppo societario operante nei settori dell'elettronica di consumo e della comunicazione, relativi ai servizi *online* per clienti, hanno subìto un attacco informatico, con sottrazione dei dati personali di circa 77 milioni di utenti. Il *data-center* ubicato negli USA conteneva parecchi dati della clientela: nome, cognome, indirizzo e-mail, indirizzo postale, data di nascita, sesso, lingua, *online id*, password, domande per il recupero della password nonché l'eventuale numero di carta di credito e la relativa data di scadenza, ma non il codice di sicurezza (CVV).

Nel corso dell'istruttoria, il Garante ha accertato che i clienti italiani coinvolti erano 1,47 milioni e di questi 217.128 avevano fornito il numero della carta di credito. La società non è stata in grado di confermare né escludere che tali dati relativi alle carte di credito fossero stati trafugati, ma ha confermato l'adozione di nuove misure di sicurezza, tecniche e organizzative: lo spostamento dei *server* ad altra sede; l'implementazione di sistemi di sicurezza aggiuntivi come firewall, alert e monitor di attività anomale e intrusioni; l'uso di protezioni crittografiche; l'istituzione della figura del *Chief Information Security Office*. Si è detta, inoltre, disponibile a valutare eventuali, comprovate richieste di risarcimento. Sul caso sono tuttora in corso indagini da parte dell'FBI.

Nell'aprile 2011, un corto circuito in uno dei gruppi di continuità elettrici (batterie dei gruppi UPS) ha causato un principio di incendio presso il *data-center* di un importante internet service *provider* italiano, con conseguente interruzione, per alcune ore, di tutti i servizi informatici erogati. Al riguardo l'Autorità ha condotto appositi accertamenti istruttori dai quali è emerso che non si è comunque verificata alcuna perdita, distruzione o violazione dei dati, come confermato anche dall'assenza di segnalazioni o lamentele degli utenti.

Sempre nel mese di aprile 2011 si è appreso dai mezzi di informazione che la polizia olandese aveva pianificato controlli periodici sui limiti di velocità, ricorrendo a un *database* contenente dati cinematici e di localizzazione di mezzi circolanti sulla rete stradale, fornito indirettamente da una società che produce sistemi di navigazione satellitare. Tale *database*, apparentemente alimentato da dati di geolocalizzazione aggregati trasmessi dai dispositivi di navigazione presenti a bordo di autoveicoli, in alcuni casi sarebbe stato infatti concesso in uso –dietro pagamento di una licenza– a una società intermediaria che, a sua volta, l'avrebbe concesso in licenza alla polizia olandese.

L'istruttoria condotta dal Garante ha evidenziato che i trattamenti dei dati in questione non riguardavano il territorio italiano e, comunque, avvenivano in forma anonima ed aggregata e che l'informativa resa e le formule utilizzate per l'acquisizione del consenso degli interessati erano conformi alle prescrizioni di legge.

10. PROTEZIONE DEI DATI PERSONALI E RAPPORTO DI LAVORO PUBBLICO E PRIVATO

Numerose ed eterogenee sono le segnalazioni indirizzate all'Autorità da parte di lavoratori o di rappresentanze sindacali, ovvero le richieste di datori di lavoro, concernenti il trattamento di dati personali nell'ambito del rapporto di lavoro pubblico e privato. Vi sono tuttavia nei diversi casi trattati profili comuni, che di seguito si evidenziano, segnalando altresì che a partire dall'aprile del 2011 la materia è stata affidata a un'unica unità organizzativa e che intensa è stata, in questo settore, l'attività di natura ispettiva effettuata dall'Ufficio, direttamente o avvalendosi della Guardia di finanza.

Il tema del controllo a distanza dei lavoratori mediante l'impiego di tecnologie (vecchie e nuove), già regolato dall'art. 4, l. n. 20 maggio 1970, n. 300 (nonché dall'art. 171 del Codice), rappresenta quello di più frequente oggetto delle segnalazioni che, non di rado, vengono indirizzate anche ai competenti uffici periferici del Ministero del lavoro (par. 10.1.).

Ricorrenti sono le richieste di utilizzare dati biometrici –anche al fine di commisurare il tempo di lavoro– che l'Autorità continua a ritenere, di regola, eccedenti, come già risulta dalle indicazioni di ordine generale fornite in passato (cfr., in particolare, il punto 4 del provv. 23 novembre 2006, linee-guida per il trattamento di dati dei dipendenti privati [doc. *web* n. 1364099]) nonché il punto 7 del provv. 14 giugno 2007, linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico [doc. *web* n. 1417809] (par. 10.2.).

Ulteriori e delicati ambiti di intervento hanno riguardato l'utilizzo di questionari di personalità –mediante i quali sono trattati anche dati sensibili, inerenti a sfere intime del lavoratore– in sede di assunzione, come pure in pendenza del rapporto di lavoro, al fine di dare attuazione alla disciplina sulla sicurezza sul lavoro, con particolare riferimento all'identificazione del fenomeno dello stress lavoro-correlato (questi ultimi all'esame dell'Autorità) (par. 10.3.).

Oggetto di lamentela è costituito talvolta anche dalle più varie operazioni di trattamento di dati personali riferibili a lavoratori nell'ambito dell'esecuzione del rapporto di lavoro: i

profili presi in esame riguardano l'utilizzo di informazioni personali per finalità diverse rispetto a quelle che ne avevano in origine giustificato la raccolta, le modalità di consegna della documentazione indirizzata al singolo lavoratore (contenenti, ad esempio, contestazioni disciplinari, notizie di carattere valutativo o sanitario) o (più in generale) l'accessibilità ad informazioni inerenti il singolo lavoratore da parte di altri colleghi (ad esempio, in ragione della configurazione data al protocollo informatico interno, ovvero a causa delle modalità di comunicazione prescelte dal datore di lavoro) (par. 10.4.).

Diverse questioni, spesso connesse alla trasparenza dell'attività amministrativa, riguardano l'applicazione delle 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], nonché delle linee-guida del Garante in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul *web* del 2 marzo 2011 (pubblicate in G.U. 19 marzo 2011, n. 64 [doc. *web* n. 1793203]), delle quali si è riferito nella Relazione 2010, p. 54 e ss.) con riferimento al regime di conoscibilità di dati riferiti a pubblici dipendenti (par. 10.5.).

Viene talora riproposta la questione inerente le condizioni di liceità del trattamento in relazione all'istituzione di procedure di segnalazione interna (cd. *"whistleblowing"*), tematica già oggetto di segnalazione al Parlamento e al Governo ai sensi dell'art. 154, comma 1, lett. *f*), del Codice da parte dell'Autorità (cfr. segnalazione 10 dicembre 2009 [doc. *web* n. 1693019]), ed almeno in parte oggetto di considerazione nell'ambito del più ampio processo legislativo che interessa la materia della corruzione (A.C. 4434 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione").

Tra i profili all'attenzione dell'Autorità va infine annoverata la corretta individuazione, nel rispetto del principio di pertinenza e non eccedenza (e spesso di indispensabilità, venendo in gioco dati sensibili), delle informazioni suscettibili di formare oggetto di trattamento in vista del riconoscimento delle agevolazioni previste dalla l. n. 5 febbraio 1992, n. 104 (legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate).

10.1. CONTROLLI A DISTANZA

Passando ad un esame più ravvicinato dei provvedimenti del Garante, merita sottolineare che tra le tecniche di controllo a distanza di più frequente oggetto di segnalazione e verifica da parte dell'Autorità, la videosorveglianza –più volte contemplata, anche in relazione al rapporto di lavoro, nei provvedimenti generali in materia adottati dall'Autorità (cfr. punti 4.1. del provv. 8 aprile 2010 [doc. *web* n. 1712680], e del precedente provv. 29 aprile 2004 [doc. *web* n. 1003482])– rimane ancora la più ricorrente (verosimilmente, trattandosi di quella di più agevole riconoscibilità da parte dei lavoratori, salvi i casi di controlli effettuati clandestinamente, talvolta rilevati in sede di verifica).

10.1.1. La videosorveglianza

In quest'ambito, i provvedimenti di divieto del trattamento dell'Autorità, fondati sull'inosservanza dell'art. 4, l. n. 300/1970 (o delle garanzie dallo stesso previste, vale a dire, il preventivo accordo con le rappresentanze sindacali dei lavoratori rispetto all'installazione delle apparecchiature di controllo o l'autorizzazione del competente ufficio periferico del Ministero del lavoro) –con la conseguente trasmissione degli atti all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali eventualmente configurabili– hanno riguardato una casa di cura, nella quale anche l'area occupata dal sistema di rilevazione delle presenze formava oggetto di ripresa (provv. 10 novembre 2011 [doc. *web* n. 1859539]; così pure nel caso deciso con provv. 16 febbraio 2012 [doc. *web* n. 1892377]), un centro di riabilitazione, nel quale formavano oggetto di ripresa gli accessi e i corridoi al piano (provv. 17 novembre 2011 [doc. *web* n. 1859546]), una società, nella quale le riprese interessavano gli ingressi principali e di emergenza, i corridoi ai diversi piani, nonché le aree di accesso a talune zone degli uffici (provv. 17 novembre 2011 [doc. *web* n. 1859558]), un hotel (provv. 14 aprile 2011 [doc. *web* n. 1810223]) e alcuni enti pubblici (provv. 10 novembre 2011 [doc. *web* n. 1859569]; provv. 2 febbraio 2012 [doc. *web* n. 1884167]; provv. 9 febbraio 2012 [doc. *web* n. 1886999]; provv. 16 febbraio 2012 [doc. *web* n. 1892377]). Talvolta si è reso necessario prescrivere la designazione quale "incaricato del trattamento" del personale preposto all'utilizzo del sistema di videosorveglianza ovvero disporre la riduzione dei tempi di

conservazione delle immagini registrate (provv. 17 novembre 2011 [doc. *web* n. 1859558) o, ancora, l'integrazione dell'informativa fornita agli interessati (provv. 10 novembre 2011 [doc. *web* n. 1859539]).

10.1.2. La geolocalizzazione

Di crescente rilevanza è il fenomeno della geolocalizzazione, in particolare di veicoli, che (di regola) consente anche l'individuazione degli spostamenti dei lavoratori che ne fanno uso (e princìpi non diversi possono trovare applicazione in relazione ad altre strumentazioni che determinano il medesimo effetto).

La tematica, già in passato oggetto di interventi dell'Autorità (cfr. provv. 7 ottobre 2010 [doc. *web* n. 1763071]), è stata riproposta con alcune verifiche preliminari presentate ai sensi dell'art. 17 del Codice (provv.ti 7 luglio 2011 [doc. *web* nn. 1828354 e 1828371]), nelle quali particolare attenzione è stata riservata all'individuazione dei dati suscettibili di trattamento, conformemente al principio di pertinenza e non eccedenza, considerate le finalità in concreto perseguite. Sono state ritenute lecite finalità riconducibili ad esigenze organizzative e produttive dell'azienda: in tali ipotesi, possono essere trattati solo i dati idonei a rilevare, quando necessario, la posizione dei veicoli nonché le sole informazioni indispensabili alla compilazione del rapporto di guida e per la commisurazione dei costi da imputare alla clientela (quali la distanza percorsa e il relativo consumo di carburante). Date le finalità in concreto perseguite dal titolare del trattamento, non si è invece ritenuto pertinente il trattamento di informazioni suscettibili di determinare un controllo sulla condotta di guida del conducente (dati tecnici relativi ai giri del motore ed alla frenata). In caso di esternalizzazione delle attività finalizzate alla localizzazione dei veicoli, il Garante ha evidenziato che il fornitore del servizio deve assumere il ruolo di responsabile del trattamento. I dati utilizzati per la regolare tenuta del libro unico del lavoro (disciplinata dall'art. 6, d.m. 9 luglio 2008), tra i quali quelli relativi alle presenze, alle ferie, ai tempi di lavoro, ed altri previsti dalle vigenti disposizioni, possono essere conservati per cinque anni.

Data la diffusione del fenomeno, la materia ha formato oggetto di un provvedimento generale di bilanciamento di interessi, con il quale sono state altresì impartite alcune

prescrizioni ai titolari del trattamento consentendo di avvalersi con maggiore speditezza di sistemi di geolocalizzazione, nel rispetto delle garanzie previste dalla disciplina di settore (prima fra tutte, quelle dettate dallo Statuto dei lavoratori) (provv. 4 ottobre 2011 [doc. *web* n. 1850581]). In base al provvedimento, quindi, i datori di lavoro pubblici e privati possono trattare (senza che sia necessario il consenso dei singoli lavoratori) dati personali ricavati da sistemi di localizzazione per soddisfare esigenze organizzative e produttive, ovvero per la sicurezza sul lavoro nell'ambito della fornitura di servizi di trasporto a condizione che, oltre la normativa sulla protezione dei dati personali, sia rispettata la disciplina dettata dall'art. 4, l. n. 300/1970. Ai lavoratori sottoposti a localizzazione devono essere forniti, oltre che gli elementi informativi prescritti dall'art. 13 del Codice, ulteriori ragguagli circa la natura dei dati trattati e le caratteristiche del sistema, da cui risulti con inequivocabile chiarezza che il veicolo è sottoposto a localizzazione (anche secondo il modello semplificato allegato al cit. provvedimento).

La materia, anche alla luce delle segnalazioni pervenute, ha formato altresì oggetto di attività ispettive, parte delle quali hanno interessato il settore del trasporto pubblico locale, i cui esiti sono, allo stato, in fase di valutazione.

10.1.3. Internet e data elettronica

Il trattamento di dati personali nell'utilizzo dei servizi di comunicazione elettronica (internet, posta elettronica aziendale nonché sistemi di telefonia su protocollo IP) –già oggetto, in termini generali, del provv. 1° marzo 2007 "Linee-guida per posta elettronica e internet" [doc. *web* n. 1387522]– nonché l'applicazione dei provvedimenti concernenti il ruolo e le funzioni degli amministratori di sistema nella sicurezza dei trattamenti (provv.ti 27 novembre 2008 [doc. *web* n. 1577499] e 25 giugno 2009 [doc. *web* n. 1626595]), hanno formato oggetto di verifica presso una società di primaria rilevanza. All'esito degli accertamenti, l'Autorità ha (tra l'altro) vietato la conservazione e la categorizzazione, anche su base individuale, dei dati riferiti alla navigazione in internet dei dipendenti (tra i quali i tentativi di accesso di ogni singolo dipendente ai domini selezionati, con registrazione dei log indicanti tra l'altro la macchina utilizzata per l'accesso ad internet, indirizzo (*URL*) di

destinazione e utente richiedente), ritenendola in violazione degli artt. 11, comma 1, lett. *a*), c) e d), 113 e 114 del Codice nonché 4 e 8, l. n. 300/1970. Il *software* a tal fine utilizzato categorizzava le pagine filtrate ricorrendo ad una molteplicità di classi di siti visitati nonché la navigazione di ciascun utente secondo categorie predefinite dal sistema medesimo (quali, ad esempio, quelle denominate *adult material, advocacy groups, business and economy, entertainment, abortion, drugs, militancy and extremist*). La società disponeva di dati relativi alla navigazione internet riconducibili ad ogni singolo utente, conservati per un minimo di sei mesi, sino ad un anno, essendo vincolata alla disponibilità di spazio per l'archiviazione.

Inoltre, con riguardo al trattamento di dati personali effettuato dagli amministratori di sistema, è stato prescritto alla società di dare integrale attuazione alla prescrizione di cui alle lett. *c)* ed *f)* del citato provvedimento del 27 novembre 2008, assicurando in particolare che sia resa nota o conoscibile l'identità degli amministratori di sistema nell'ambito della società, nonché la completezza del tracciamento delle attività effettuate dagli amministratori di sistema. Il provvedimento adottato dal Garante nei confronti della società è stato impugnato davanti al Tribunale di Roma, che né ha sospeso gli effetti nelle more dello svolgimento del giudizio (provv. 21 luglio 2011 [doc. *web* n. 1829641]).

L'Autorità si è poi occupata di un reclamo che lamentava presunti illeciti controlli sul computer aziendale in uso all'interessata (provv. 7 aprile 2011 [doc. *web* n. 1812154]).

Dall'istruttoria è emerso che la società aveva illecitamente trattato i dati personali dell'interessata, ricavati da file di *backup* nell'ambito delle ordinarie operazioni di gestione del *server* aziendale. In particolare, non è risultato provato che la società avesse fornito all'istante un'idonea informativa preventiva relativamente ai trattamenti connessi all'utilizzo degli strumenti elettronici e ai correlati eventuali controlli, né che il trattamento fosse proporzionato rispetto alla finalità perseguita. L'Autorità ha quindi vietato alla società l'ulteriore trattamento dei dati personali dell'interessata ritratti dai file e documenti acquisiti in occasione delle operazioni di *backup*, invitando altresì il titolare a disciplinare le modalità di utilizzo degli strumenti elettronici conformemente alle istruzioni dell'Autorità, in particolare alle linee-guida su posta elettronica e internet del 1° marzo 2007 [doc. *web* n. 1387522].

10.1.4. Monitoraggio delle conversazioni di un call center

Ha altresì formato oggetto di esame il controllo a distanza degli operatori di un *call center* appartenenti ad una compagnia telefonica, in relazione ad operazioni di monitoraggio –realizzato previa registrazione delle conversazioni effettuate dagli operatori con gli utenti– dei processi aziendali di gestione del customer care. Trattandosi di vicenda relativa a dati, oltre che dei lavoratori, degli utenti se ne riferisce con maggiore dettaglio in altra parte (par. 11.3.), richiamando qui solo l'esito favorevole della valutazione del Garante, in ragione, tra l'altro, degli accordi sindacali conclusi con le rsa/rsu e degli accorgimenti tecnici e procedurali adottati dal titolare del trattamento (provv. 9 febbraio 2011 [doc. *web* n. 1797032]).

10.2. DATI BIOMETRICI

Coerentemente ad un orientamento consolidato (e sintetizzato nelle linee-guida sopra menzionate in materia di lavoro pubblico e privato), nell'ambito di una verifica preliminare presentata ai sensi dell'art. 17 del Codice, il Garante ha ritenuto lecito il trattamento di dati biometrici ricavati dalla lettura delle impronte digitali effettuato da una società che opera nel settore della sicurezza privata, finalizzato unicamente a consentire l'accesso di un numero ristretto di dipendenti –mediante il confronto tra il *template* rilevato dal lettore e quello sullo stesso memorizzato in fase di *enrollment* (cd. *"matching on device"*) e senza memorizzazione di alcun dato ulteriore (in linea con l'art. 3 del Codice)– a determinate aree dello stabile aziendale destinate alla conta di denaro e alla custodia di beni di rilevante valore (provv. 10 giugno 2011 [doc. *web* n. 1835792]).

In una diversa ipotesi, segnalata dal dipendente di una società operante nel campo delle traduzioni e di servizi di interpretariato, il sistema biometrico utilizzato, centralizzando in una banca dati i *template* ricavati dalle impronte dei dipendenti, non è stato ritenuto lecito, non essendo stata dimostrata l'esistenza di "aree sensibili" che potessero giustificarne l'utilizzo in ragione della natura delle attività svolte, né essendo stato provato che il trattamento fosse conforme ai princìpi di necessità e proporzionalità, atteso che la società risultava essersi già dotata di un sistema di allarme e non risultava l'effettiva inefficacia delle ulteriori misure di protezione prospettate dalla società stessa (quali il servizio di portineria o l'utilizzo di *badge*)

(provv. 10 marzo 2011 [doc. *web* n. 1807683]). Nello stesso ordine di idee, un comune che aveva comunicato l'intenzione di istituire un sistema di rilevazione di impronte digitali per verificare la presenza dei dipendenti sul luogo di lavoro è stato invitato a verificare anche sulla base di quanto previsto al riguardo nelle citate linee-guida sul trattamento dei dati dei lavoratori in ambito pubblico (provv. 14 giugno 2007 [doc. *web* n. 1417809]) l'effettiva sussistenza delle particolari esigenze di controllo che consentono l'installazione di tali sistemi (nota 5 luglio 2011).

La tematica del trattamento di dati biometrici nel rapporto di lavoro è stata esaminata anche in sede di interpello preventivo (art. 17 del Codice). Con un primo provvedimento, adottato a seguito di un accertamento ispettivo espletato dal Ministero del lavoro, della salute e delle politiche sociali presso una società operante nel campo dell'edilizia per conto terzi, il Garante ha vietato l'ulteriore trattamento dei dati biometrici dei dipendenti effettuato allo scopo di rilevare la loro presenza sul posto di lavoro (provv. 20 ottobre 2011 [doc. *web* n. 1851657]). Ciò in quanto la società non aveva dimostrato l'effettiva sussistenza di eventuali aree "sensibili" (peraltro "esclusa" già in sede di accertamento ispettivo), né comprovato l'effettiva indispensabilità del trattamento alla luce delle finalità perseguite. Inoltre, non è risultato acquisito il libero consenso degli interessati, né che la società avesse fornito un'idonea informativa preventiva ai dipendenti relativamente al trattamento in esame.

L'Autorità si è inoltre riservata di valutare l'applicabilità di sanzioni.

Sempre in sede di interpello preventivo il Garante ha invece autorizzato, ritenendolo proporzionato alle finalità perseguite, il trattamento dei dati biometrici di alcuni dipendenti da parte di una società di ricerca, sviluppo e produzione di sistemi elettronici, anche per scopi militari (provv. 26 maggio 2011 [doc. *web* n. 1832558]).

Infatti il trattamento risultava preordinato a garantire l'accesso da parte del solo personale debitamente autorizzato a due sale *server* ubicate presso uno stabilimento adibito alla progettazione e alla realizzazione di sistemi di navigazione utilizzati a bordo di aerei militari e "contenenti apparati con applicazioni critiche e/o informazioni riservate" (astrattamente riconducibili a quelle "classificate" di cui alla l. n. 3 agosto 2007, n. 124 e al d.P.C.m. 3 febbraio 2006). L'adozione di adeguate misure di sicurezza "materiale" rispondeva a

specifiche esigenze previste a livello normativo e risultava funzionale a garantire l'osservanza degli stringenti requisiti di affidabilità richiesti dalle disposizioni ISO. Risultava conforme alla disciplina del Codice la prevista acquisizione del consenso libero ed espresso degli interessati (artt. 13 e 23 del Codice), come pure la predisposizione di adeguate misure di sicurezza (art. 31 e ss. e Allegato B. del Codice) relative anche alle modalità di accesso ai dati da parte degli amministratori di sistema e alla "tracciabilità" dei loro interventi.

L'Autorità ha tuttavia prescritto alla società, in luogo delle prospettate modalità centralizzate di conservazione dei *template* (ossia delle mappe delle impronte, codificate per impedire di risalire da esse alle immagini da cui sono tratte), di memorizzare questi ultimi su dispositivi posti nella esclusiva disponibilità degli interessati, per prevenire il rischio di eventuali utilizzi impropri delle informazioni o di possibili abusi. Alla società, inoltre, è stato prescritto di: impartire adeguate istruzioni circa l'eventuale perdita e sottrazione dei dispositivi affidati ai lavoratori; provvedere alla formale designazione degli incaricati e degli eventuali responsabili del trattamento; notificare al Garante il trattamento medesimo; rendere agli interessati un'idonea informativa preventiva; farsi rilasciare dall'installatore del sistema il prescritto attestato di conformità (regola n. 25 dell'Allegato B. del Codice).

10.3. QUESTIONARI DI PERSONALITÀ

Con provvedimento del 21 luglio 2011 [doc. *web* n. 1825852], impugnato in sede giurisdizionale, il Garante si è espresso in relazione a una procedura di selezione di un dirigente tecnico da parte di un ente pubblico economico, nella quale ai candidati erano stati somministrati, a cura di una psicologa, *test* di personalità contenenti dettagliate domande relative, fra l'altro, alla sfera affettiva, alla vita sessuale, alle condizioni di salute psico-fisica (con richiesta di indicare la patologia e il medicinale assunto, nonché le visite di natura psicologica/psichiatrica eventualmente effettuate); venivano inoltre richieste informazioni concernenti i disturbi del sonno, abitudini personali relative al fumo, al consumo di alcolici o di droghe ovvero inerenti ad abitudini alimentari o a tentativi di suicidio (effettuati o presi in considerazione dal candidato) nonché informazioni concernenti eventuali provvedimenti giudiziari di condanna, nonché, per le donne, eventuali interruzioni di gravidanza. Ritenuta

la co-titolarità del trattamento dei dati personali connesso alla somministrazione dei *test* di personalità in capo all'ente pubblico che aveva commissionato la selezione, alla società incaricata della sua esecuzione nonché alla psicologa che aveva somministrato i *test*, l'Autorità ha dichiarato l'illiceità del trattamento effettuato, ritenuto in violazione del principio di liceità (data la raccolta di informazioni vietate ai sensi dell'art. 8, l. n. 300/1970) nonché di pertinenza e non eccedenza, con la conseguente inutilizzabilità dei dati trattati in violazione di legge ai sensi dell'art. 11, comma 2, del Codice.

Come anticipato, l'utilizzo di questionari di personalità caratterizzantisi per l'elevato dettaglio e la natura sensibile dei dati rilevati, ha formato oggetto di accertamento da parte dell'Ufficio (e gli esiti sono allo stato in corso di valutazione) non solo in fase assuntiva, ma anche al fine di individuare, in talune categorie di dipendenti, condizioni di stress lavoro correlato: gli esiti di tali accertamenti sono in corso di valutazione.

10.4. TRATTAMENTI IMPROPRI DI DATI PERSONALI

Tra le decisioni relative all'utilizzo di dati personali nell'ambito della gestione del rapporto di lavoro, merita evidenziare la riconosciuta illiceità, per violazione dei princìpi di necessità, finalità e liceità, del trattamento effettuato da una Direzione didattica di dati sensibili concernenti le condizioni di salute della sorella della segnalante (nonché la loro successiva comunicazione). Tali informazioni, infatti, contenute in documentazione originariamente prodotta dalla segnalante nell'ambito di un procedimento mirante al riconoscimento alla stessa dei benefici previsti dalla l. n. 104/1992, erano state successivamente utilizzate dal titolare del trattamento nell'ambito del diverso procedimento volto al riconoscimento, sempre in capo alla segnalante, di un'infermità per causa di servizio (provv. 12 gennaio 2012 [doc. *web* n. 1872998]).

In un altro caso un dipendente lamentava di aver ricevuto, da parte di personale non incaricato del trattamento dei dati, una missiva, recante gli indirizzi di altri (numerosi) destinatari, con la quale veniva comunicata, in forma cumulativa, l'entità delle ferie non fruite da ciascun lavoratore negli anni precedenti, nonché le ore di permesso non godute e quelle da recuperare. Il Garante, oltre a ritenere illecita tale modalità comunicativa poiché

non rispettosa dei princìpi di necessità e di non eccedenza, nel richiamare le puntuali indicazioni già fornite in ordine al corretto trattamento dei dati dei lavoratori nell'ambito delle attività di gestione del rapporto di lavoro privato, ha ritenuto illecito il trattamento evidenziando altresì la necessità di preporre alla custodia dei dati medesimi personale specificamente incaricato del trattamento (provv. 2 marzo 2011 [doc. *web* n. 1802433]).

10.5. DIFFUSIONE E COMUNICAZIONE DI DATI DI PUBBLICI DIPENDENTI

Le menzionate linee-guida del 14 giugno 2007, e quelle riguardanti il trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali (provv. 19 aprile 2007 [doc. *web* n. 1407101]) sono state richiamate in relazione ad una segnalazione relativa all'avvenuta pubblicazione, sul sito istituzionale di un comune, di una determina dirigenziale contenente dati relativi allo stato di salute di una dipendente. A seguito dell'intervento del Garante il comune ha prontamente rimosso dal sito *web* i dati oggetto della segnalazione (nota 12 luglio 2011).

Anche in un altro caso, nel quale un dirigente aveva lamentato la pubblicazione, sul sito istituzionale del comune dove prestava servizio, di taluni dati relativi a contestazioni disciplinari a suo carico contenuti in ordinanze del sindaco risalenti ad alcuni anni prima, a seguito dell'intervento del Garante il comune ha rimosso le ordinanze stesse dal sito *web* (nota 5 dicembre 2011).

Inoltre, in relazione a due analoghe vicende si lamentava rispettivamente l'affissione nell'albo pretorio comunale nonché nella bacheca di un'azienda ospedaliera di due determinazioni contenenti dati sulla salute degli interessati. In entrambe le occasioni l'Ufficio ha evidenziato che, in presenza di disposizioni che prevedono la pubblicazione obbligatoria delle deliberazioni adottate, nel rispetto dell'obbligo di adeguata motivazione degli atti amministrativi, occorre selezionare i dati da diffondere –in particolare se idonei a rivelare lo stato di salute, la cui diffusione è vietata– alla luce dei princìpi di pertinenza, non eccedenza ed indispensabilità dei dati trattati nonché delle indicazioni fornite con le citate linee-guida del 14 giugno 2007, del 19 aprile 2007 e del 2 marzo 2011 [doc. *web* n. 1793203] (note 27 dicembre 2011 e 23 gennaio 2012).

In un altro caso, alcuni dipendenti avevano lamentato la pubblicazione, sul sito istituzionale del Ministero della giustizia, di provvedimenti relativi al loro inquadramento, comprensivi di allegati contenenti il nominativo, il luogo e la data di nascita e il codice fiscale, dati che risultavano rinvenibili anche tramite i comuni motori di ricerca.

Il Garante ha premesso che occorre verificare, rispetto alle finalità della pubblicazione, se le informazioni contenute nei documenti debbano essere rese conoscibili a tutti e quindi liberamente reperibili sul sito istituzionale, ovvero ai soli interessati o ai contro interessati in un procedimento amministrativo (v. linee-guida 14 giugno 2007 e 2 marzo 2011, già citate). Ha inoltre rilevato che il Ministero, negli stessi provvedimenti oggetto di riproduzione sul sito *web*, aveva correttamente individuato, quale modalità adeguata per rendere conoscibile agli interessati la specifica documentazione, la pubblicazione di tali atti nella sezione intranet del sito *web* dell'Amministrazione, accessibile soltanto al personale, preceduta da un apposito avviso. Visto che la pubblicazione nella parte liberamente accessibile del sito istituzionale aveva comportato una diffusione non necessaria e sproporzionata in rapporto alla finalità perseguita anche in base alla disciplina di settore, il Garante ha ritenuto illecito il trattamento dei dati, ne ha quindi vietato l'ulteriore diffusione. È stato inoltre prescritto al Ministero di utilizzare in futuro modalità appropriate e proporzionate alle specifiche esigenze perseguite con la pubblicazione sul sito istituzionale di dati personali dei dipendenti, nel rispetto delle indicazioni fornite dal Garante con le citate linee-guida del 2 marzo 2011 (provv. 27 aprile 2011 [doc. *web* n. 1832775]).

In una diversa vicenda, il dipendente di un'azienda ospedaliera aveva segnalato che la copia della cartella sanitaria e di rischio rilasciatagli, su sua richiesta, dall'ospedale, recava la sigla del dirigente medico della struttura presso la quale prestava servizio in luogo di quella del medico competente. A tal proposito l'Autorità ha evidenziato, richiamando anche le citate linee-guida del 14 giugno 2007, che il datore di lavoro non può accedere alle informazioni contenute nella cartella sanitaria e di rischio del lavoratore essendo tenuto alla salvaguardia del segreto professionale. Alle medesime cautele, confermate dalla nuova normativa in materia di salute e sicurezza nei luoghi di lavoro, è tenuto il medico competente che ha il dovere di gestire la documentazione sanitaria curando le opportune misure di