10.8. *Il* mobile payment

Come riferito nella Relazione 2012, il Garante ha avviato un'attività conoscitiva in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, noti come *mobile remote payment*, che vedono coinvolti, in particolare, operatori di telecomunicazioni, *hub* tecnologici e fornitori di beni e servizi digitali, che, tramite applicazioni che consentono l'accesso a un mercato virtuale, offrono agli utenti la possibilità di acquistare servizi e prodotti digitali fruibili tramite *smartphone*, PC e *tablet*, con addebito del relativo costo sul conto telefonico ovvero con decurtazione dell'importo dal credito telefonico (nel caso di *sim* ricaricabili).

All'esito di tale attività, con provvedimento del 12 dicembre 2013, n. 561, è stata avviata una pubblica consultazione su uno schema di provvedimento generale in materia (doc. web n. 2830145) volto a garantire, in un mercato sempre più dinamico, un uso sicuro e corretto delle informazioni che riguardano gli utenti alla luce dell'attuale assetto normativo del settore (cfr. in particolare la direttiva sui servizi di pagamento 2007/64/CE, cd. *Payment Service Directive*, il relativo decreto di recepimento, d.lgs. 27 gennaio 2010, n. 11, e il provvedimento della Banca d'Italia del 5 luglio 2011 "Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento").

L'attività conoscitiva si è estesa anche ai *server* di *mobile proximity payment* che riguardano le operazioni di pagamento di beni (digitali e non) eseguite dal cliente avvicinando il dispositivo mobile, dotato di tecnologia NFC (*Near Field Communication*) che fornisce connettività *wireless* (RF) bidirezionale a corto raggio, ad un apposito lettore pos (*point of sale*) posto presso il punto vendita dell'esercente da cui si acquista il bene. Tali servizi sono offerti da soggetti che operano in ambito bancario e nel circuito delle carte di credito.

In tale ambito, il Garante si è quindi riservato, all'esito di tale attività, di intervenire, nei limiti delle proprie competenze, con ulteriori provvedimenti che potranno investire anche il settore dell'offerta e dei pagamenti di titoli digitalizzati per l'accesso a servizi di utilità sociale o a servizi in mobilità (con riguardo, in particolare, alle operazioni di *mobile ticketing* e *mobile parking*).

10.9. *La disciplina dei* data breach

Gli obblighi per i fornitori di servizi di comunicazione elettronica accessibili al pubblico (quali telefonia, accesso a internet, *account* di posta elettronica, *etc.*) di comunicare le violazioni di dati personali ai sensi del nuovo testo degli artt. 32 e 32-*bis*, del Codice sono già stati ampiamente descritti nella Relazione 2012 (v. p. 171 e ss.) unitamente alle "Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" (provv. 26 luglio 2012, n. 183, doc. web n. 1915485), contenenti prescrizioni nei confronti dei fornitori; l'Autorità ha altresì predisposto un modello per la comunicazione dei *data breach* (reso disponibile *online* sul sito dell'Autorità: cfr. doc. web n. 1915835).

All'esito della consultazione pubblica avviata nel 2012, in merito ad alcune specifiche modalità applicative della nuova disciplina contenuta nell'art. 32-*bis* del Codice (e in considerazione dei primi casi di violazione di dati personali comunicati dai fornitori), il Garante ha adottato, ai sensi dell'art. 32-*bis*, comma 6, del Codice, un provvedimento generale – che ha sostituito le ricordate linee guida – per fornire indicazioni in relazione alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione e alle relative modalità di effettuazione (provv. 4 aprile 2013, n. 161, doc. web n. 2388260).

Nel redigere tale provvedimento, l'Autorità ha tenuto conto delle indicazioni della Commissione europea, formalizzate poi nel regolamento Ue n. 611/2013 del 24 giugno 2013, sulle misure applicabili alle comunicazioni dei *data breach* (in G.U.E.E. n. L 173 del 26 giugno 2013 ed entrato in vigore il 25 agosto 2013), sì da rendere sostanzialmente omogenei i due atti (che presentano lievi differenze, attinenti più a profili procedurali che di merito).

Nel 2013 sono pervenute all'Autorità circa venti comunicazioni di *data breach*, da parte dei più importanti fornitori di servizi di comunicazione elettronica operanti in Italia.

In alcuni casi, la violazione ha riguardato i servizi offerti *online* dai fornitori sui propri siti web, quali, ad esempio, quelli che consentono alla clientela di effettuare ricariche telefoniche o visualizzare il traffico telefonico effettuato a fini di controllo dell'esattezza degli addebiti; in tale ambito, gli incidenti verificatisi hanno determinato la visualizzazione, da parte di alcuni clienti, di dati relativi ad altri interessati (quali, ad es., i numeri dei clienti che hanno effettuato la ricarica, l'ammontare della stessa nonché i numeri in uscita dall'utenza coinvolta).

In un caso, che ha riguardato uno dei principali ISP italiani, un utente, accedendo alla propria *webmail*, ha visualizzato la *mailbox* di un altro utente (che a sua volta aveva perso alcuni messaggi di posta elettronica). Entrambi si erano prontamente rivolti al gestore che, oltre a recuperare quasi tutti i messaggi perduti, ha chiarito la natura dell'anomalia verificatasi.

In un altro caso, l'Autorità si è attivata sulla base delle notizie, apparse su diversi mezzi di informazione, relative ad un attacco informatico che aveva minato la sicurezza degli indirizzi *e-mail* e delle *password* di circa 250.000 utenti di un noto *social network*. È stata così inviata una dettagliata richiesta di informazioni alla società statunitense che lo gestisce, che ha fornito gli elementi richiesti assicurando, peraltro, di aver notificato l'accaduto alle competenti autorità federali e di avere in corso ulteriori accertamenti, con la collaborazione delle stesse, nonché di aver subito modificato le *password* degli utenti coinvolti mettendoli al corrente dell'accaduto tramite messaggi di posta elettronica.

Il pregiudizio per i dati personali degli utenti è derivato, in alcuni casi, dalle incaute operazioni svolte dagli stessi e non dalla negligenza dei fornitori. Il Garante, ad esempio, ha verificato, mediante accertamento ispettivo, il furto delle credenziali di autenticazione di clienti di una società di telecomunicazioni, effettuato attraverso l'installazione operata dagli stessi clienti sui propri terminali mobili, di un'*app* fraudolenta tramite la quale ignoti carpivano le suddette credenziali e le utilizzavano per attività di *spam*.

Nei casi sinora esaminati, l'Autorità, all'esito delle istruttorie svolte nei confronti dei fornitori, ha verificato che fossero state adottate misure idonee a porre rimedio alle violazioni subite e a prevenirne di analoghe. In nessuno dei casi trattati si è ritenuto necessario adottare uno specifico provvedimento. Tuttavia, nell'ambito dell'istruttoria relativa ad una specifica violazione comunicata all'Autorità, è stata rilevata l'inosservanza, da parte del fornitore, dei ristretti termini per la comunicazione al Garante (24 ore dall'avvenuta conoscenza della violazione per la prima sommaria comunicazione e 3 giorni da questa per la comunicazione dettagliata) ed è stato pertanto avviato un separato procedimento sanzionatorio.

Oltre alla gestione ordinaria delle comunicazioni di *data breach*, l'Autorità ha partecipato agli approfondimenti svolti sulla materia a livello europeo, anche al fine di assicurare l'uniformità delle misure in vigore nei diversi Paesi. I temi di maggiore rilievo affrontati in quest'ambito sono stati: il canale predisposto presso le diverse autorità competenti per le comunicazioni di *data breach*; la collaborazione tra le diverse

autorità nazionali competenti nei casi di violazioni che riguardino interessati situati in diversi Stati membri nonché la valutazione da parte delle autorità competenti delle misure tecnologiche adottate dai fornitori per far fronte alle singole violazioni, con particolare riferimento all'ininrelligibilità dei dati.

10.10. *Il contrasto allo* spam

L'Autorità ha proseguito l'arrività di contrasto al fenomeno dello *spam* (v. *infra* più nel derraglio, le linee guida del 4 luglio 2013, n. 330, doc. web n. 2542248).

Turtavia, anche nel 2013 numerose sono state le segnalazioni telarive a sms, fax e ancor più *e-mail* indesiderati, per le quali talvolta è risultato difficile individuare i titolari del trarramento, sia per la modalirà con cui si può operare in tete, sia perché talora i siti "mittenti" risultano inrestati a soggetti fantasiosi o comunque privi di recapiti utilmente contattabili (non di rado in Paesi extraeuropei). Quando, invece, l'invio di fax e, ancor più di *e-mail*, promozionali indesiderati è risultato effettuato da società localizzate in Paesi membri dell'Ue (in particolare, Francia, Inghilterra e Germania), il Garante ha richiesto la collaborazione delle competenti Autorità per far cessare gli invii, nei limiti consentiti dalle (diverse) legislazioni esistenti. In proposito, merita segnalare anche che l'Autorirà è designata quale autorità nazionale competente per l'applicazione dell'art. 13 della direttiva 2002/58/CE (relativo alle comunicazioni indesiderate) nell'ambito del Sistema di cooperazione per la tutela dei consumatori (CPCS), creato dal regolamento (CE) n. 2006/2004 al fine di agevolare lo scambio di informazioni e la cooperazione tra le autorità europee competenti in materia di tutela dei consumatori.

Nella maggior parte dei casi, in cui il titolare del trattamento è stato individuato, l'Autorità ha avviato apposite istruttorie preliminari anche in relazione alla singola segnalazione. Talora sono stati ravvisati i presupposti per l'avvio di un autonomo procedimento sanzionatorio nei confronti del medesimo titolare ai fini dell'eventuale applicazione delle sanzioni previste dal Codice, con particolare riferimento alla violazione dell'obbligo dell'informativa ai sensi dell'art. 13 del Codice e dell'obbligo di previa acquisizione del consenso del destinatario delle comunicazioni automatizzate ai sensi degli artt. 23 e 130 del Codice (note 21 maggio e 13 novembre 2013). Più spesso, quando l'invio di comunicazioni promozionali automatizzate è risultato occasionale, oppure frutto di un mero errore, l'Ufficio ha invece inviato ai titolari del trattamento apposite note di richiamo al pieno rispetto della disciplina in materia (note 30 settembre e 28 ottobre 2013).

L'Autorità inoltre è intervenuta per fornire una serie di indicazioni anche agli organismi che si occupano di formazione in materia di mediazione civile e commerciale. In particolare, è stato evidenziato che, in assenza del preventivo consenso dell'interessato, non è possibile inviare comunicazioni tramite modalità automatizzate, neanche nel caso in cui i dati personali siano tratti da registri pubblici, elenchi, siti web, atti o documenti conosciuti o conoscibili da chiunque e i destinatari delle predette comunicazioni siano soggetti che svolgono un'attività economica. Un ulteriore consenso dell'interessato è poi necessario laddove il trattamento implichi la comunicazione di dati a terzi: non è infatti possibile utilizzare sistemi automatizzati di invio di messaggi promozionali, come le *mailing list*, che rendano visibili a tutti i destinatari gli indirizzi di posta elettronica utilizzati, senza rilasciare l'informativa ed acquisire il consenso degli interessati (nota 16 maggio 2013).

Con riferimento alle nuove forme di *spam*, ed in particolare all'attività di *social marketing* (effettuata, nei confronti degli utenti di *Facebook*, *Twitter* e di altri *social network* o mediante servizi di messaggistica e *Voip* sempre più diffusi), è stato ribadito,

da un lato, che l'agevole reperibilità dei dati personali in rete non significa che gli stessi possano essere liberamente usati per inviare comunicazioni promozionali agli interessati; dall'altro, che a questi tipi di trattamento non può essere applicato rigidamente il Codice, soprattutto tenendo conto della peculiare funzione dei *social network*, che comportano la condivisione volontaria e la circolazione di idee e dati personali, nelle forme di conoscenze, foto, contatti, gusti ed *hobby*.

Riguardo a siffatta attività, l'Autorità ha individuato, fra quelle più ricorrenti, due ipotesi. Una prima ipotesi è quella in cui l'utente riceve in bacheca o al proprio indirizzo di posta elettronica (collegato al profilo *social*) un messaggio promozionale (relativo a uno specifico prodotto o servizio) da parte di chi abbia ricavato i menzionati dati di contatto dal profilo del *social network* al quale l'utente è iscritto. Una seconda fattispecie ricorre quando l'utente sia diventato *fan* della pagina di una determinata impresa o società oppure si sia iscritto a un gruppo di *follower* di un determinato marchio, personaggio, prodotto e, in tale veste, riceva quindi messaggi a contenuto promozionale.

Nel primo caso, il trattamento viene considerato illecito, a meno che il mittente non dimostri di aver acquisito dall'interessato un consenso preventivo ai sensi dell'art. 130, commi 1 e 2, del Codice. Nel secondo caso, invece, l'invio di comunicazioni promozionali riguardanti un determinato marchio, prodotto o servizio, effettuato dall'impresa a cui fa riferimento la relativa pagina, può considerarsi lecito se dal contesto o dalle modalità di funzionamento del *social network*, anche sulla base delle informazioni rese, possa desumersi che l'interessato abbia in tal modo voluto fornire il proprio consenso alla ricezione di messaggi promozionali. Venuta meno la qualità di *follower* (o comunque in caso di opposizione al ricevimento di eventuali ulteriori comunicazioni promozionali), il successivo invio di messaggi promozionali sarà illecito, con le relative conseguenze sanzionatorie.

L'Autorità, inoltre, con le linee guida del 4 luglio 2013, ha stabilito che il *marketing* "virale" può rientrare nello *spam* se non rispetta principi e norme, con particolare riferimento agli artt. 3, 11, 13, 23 e 130 del Codice. Non è comunque soggetto al Codice il trattamento dei dati effettuato da chi, ricevendo una proposta promozionale, la inoltri a sua volta a titolo personale, consigliando il prodotto o il servizio ai propri amici, pur utilizzando strumenti automatizzati, come sms o *e-mail* (cd. passaparola); il Codice si applica invece al trattamento effettuato da chi inoltri, o comunque comunichi il messaggio promozionale ricevuto a una molteplicità di destinatari i cui dati personali (numeri di telefono o indirizzi *e-mail*) siano stati reperiti su elenchi pubblici o sul web.

L'Autorità ha infine ricordato che le persone giuridiche (come anche enti e associazioni), sottratte dal campo applicativo del concetto di "interessato", pur non potendo più chiedere l'intervento dell'Autorità nelle forme previste dal Codice (segnalazione, reclamo, ricorso), possono comunque essere indirettamente tutelate dal Garante che, messo a conoscenza, per il tramite di tali soggetti, di possibili violazioni della normativa sulle comunicazioni promozionali automatizzate, può intervenire nell'esercizio dei suoi poteri *ex officio*, inclusi quelli sanzionatori.

10.11. *La profilazione della clientela e i beni di lusso*

Nel 2013 sono stati adottati dal Garante tre provvedimenti prescrittivi, sulla base di altrettante istanze di verifica preliminare presentate all'Autorità da società di alta moda e che offrono beni di lusso finalizzate ad effettuare operazioni di trattamento per profilare la propria clientela ed offrirle servizi personalizzati (cd. *marketing* profilato).

Le richieste sono state presentate dalle società ai sensi dell'art. 17 del Codice, sulla base del provvedimento generale del 24 febbraio 2005 relativo alle carte di fidelizzazione (doc. web n. 1103045), nel quale è previsto che chiunque voglia conservare i dati della propria clientela per finalità di profilazione e *marketing*, per un periodo superiore a dodici mesi, deve presentare al Garante un'istanza di verifica preliminare.

Nelle richieste le società prospettavano un tempo di conservazione pari a dieci anni dei dati personali della clientela, comprensivi del dettaglio degli acquisti effettuati.

Il Garante, ricordando che tali attività necessitano comunque, *in primis*, del consenso (pienamente informato) degli interessati, ha ritenuto congruo un periodo di conservazione pari a sette anni (cfr. provv. 30 maggio 2013, n. 263, doc. web n. 2547834; provv. 7 novembre 2013, n. 500, doc. web n. 2920245) e a dieci anni (in provv. 24 aprile 2013, n. 219, doc. web n. 2499354) – con successiva cancellazione o trasformazione in forma anonima – considerando tra l'altro che i beni acquistati riguardano un genere particolare, di cd. fascia alta, con acquisti effettuati una o due volte l'anno, sicché un periodo inferiore di conservazione avrebbe potuto determinare, nella sostanza, l'impossibilità di profilare la clientela.

Il Garante, in occasione di tali verifiche, ha precisato che ciascun punto vendita deve essere designato come responsabile del trattamento ed ha altresì evidenziato l'esigenza di acquisire apposite procedure di autenticazione ed autorizzazione nonché il tracciamento dei *log* di accesso a ciascun sistema informatico, in modo da realizzare un controllo analitico *ex post* delle attività svolte dai singoli incaricati (provv.ti 24 aprile, 30 maggio e 7 novembre 2013, citati).

11 La protezione dei dati personali nel rapporto di lavoro pubblico e privato

La materia del trattamento dei dati personali nel settore del lavoro (pubblico e privato) ha registrato, nel periodo considerato, un ulteriore incremento del numero di segnalazioni e reclami pervenuti da parte di singoli o di rappresentanze sindacali per i quali, tenuto conto della necessità dell'accertamento delle circostanze di fatto, non di rado l'Ufficio ha dovuto ricorrere ad attività di natura ispettiva, sovente avvalendosi della Guardia di finanza (cfr. par. 18.2).

Una ricognizione, pur sommaria, delle istanze rivolte all'Autorità – ancorché le annotazioni svolte di seguito si incentrino prevalentemente sui provvedimenti adottati dal Garante – consente di rilevare che, dal punto di vista contenutistico, continuano a pervenire numerose segnalazioni concernenti l'utilizzo dei sistemi più vari che consentono il controllo a distanza dei lavoratori come pure la circolazione dei dati nel contesto lavorativo (tra colleghi come pure verso terzi); un significativo aumento contrassegna le segnalazioni e i quesiti conseguenti alla disciplina di trasparenza in ambito pubblico contenuta nel d.lgs. n. 33/2013, anche in considerazione delle valutazioni critiche espresse dal Garante nel parere rispetto allo schema di decreto trasmesso all'Autorità (provv. 7 febbraio 2013, n. 49: cfr. par. 3.2.2.A), che è altresì tornata a pronunciarsi sull'utilizzo dei dati biometrici al fine di commisurare il tempo di lavoro. Contesto (nuovo rispetto al passato) sul quale l'Autorità è stata chiamata a pronunciarsi (mettendo a parte, per le valutazioni di competenza, il Ministero del lavoro e delle politiche sociali – Direzione generale per le politiche dei servizi per il lavoro della decisione adottata) è quello del trattamento di dati personali di persone che, alla ricerca di un posto di lavoro, ricorrono ai più vari canali di intermediazione e, tra questi, a soggetti che, gestendo siti internet, trattano – specie in considerazione della profonda crisi occupazionale che attraversa il Paese – quantità rilevantissime di dati personali.

Un cenno merita la riproposizione, specie da parte di società multinazionali, della questione inerente le condizioni di liceità del trattamento di dati personali delle persone coinvolte nel funzionamento di procedure di segnalazione interna (cd. *whistleblowing*), tematica che, benché oggetto di segnalazione a Parlamento e Governo da parte dell'Autorità (cfr. provv. 10 dicembre 2009, doc. web n. 1693019), sia in relazione al settore pubblico che a quello privato, ha formato oggetto di intervento regolatorio – con disposizione, contenuta nell'art. 54-*bis*, d.lgs. 30 marzo 2001, n. 165, come novellato dall'art. 1, comma 51, l. 6 novembre 2012, n. 190, che trova espressa applicazione al solo ambito pubblico (lasciando peraltro irrisolti nodi di non poco momento, pur evidenziati nella menzionata segnalazione) –, con conseguente (persistente) incertezza giuridica per gli operatori.

Si segnala inoltre che, a fine 2013, l'autorizzazione generale al trattamento dei dati sensibili nei rapporti di lavoro è stata rinnovata per un altro anno, in termini sostanzialmente analoghi alla precedente (provv. 12 dicembre 2013, n. 564, doc. web n. 2818993).

11.1. *Il trattamento di dati personali e i controlli a distanza*

Videosorveglianza

Una ricognizione più puntuale dei provvedimenti del Garante consente di evidenziare tra le aree di più frequente intervento dell'Autorità – nonostante precedenti ormai copiosi (della giurisprudenza, anzitutto, e quindi del Garante) – quella del trattamento di dati personali mediante strumenti di controllo a distanza, per lo più mediante sistemi di videosorveglianza. In quest'ambito, i provvedimenti che hanno rilevato l'illiceità del trattamento ai sensi dell'art. 11, comma 1, lett. *a*), del Codice, sovente si radicano nell'inosservanza delle garanzie previste dalla disciplina di settore (segnatamente l'art. 4, comma 2, l. 20 maggio 1970, n. 300, richiamato dall'art. 114 del Codice) che, come noto, consistono nel preventivo accordo con le rappresentanze sindacali dei lavoratori rispetto all'installazione delle apparecchiature di controllo o nell'autorizzazione del competente ufficio periferico del Ministero del lavoro (il cui procedimento di rilascio è stato peraltro semplificato con la circolare del 16 aprile 2012, prot. n. 7162 del Ministero del lavoro e delle politiche sociali).

Le fattispecie prese in considerazione hanno riguardato una casistica assai varia, nella quale spiccano (per la gravità delle condotte tenute) alcune vicende nelle quali è stato accertato che la ripresa delle immagini è stata effettuata in modo occulto (violando così anche il principio di correttezza nei trattamenti) e quindi all'insaputa dei lavoratori (cfr. provv. 4 aprile 2013, n. 164, doc. web n. 2439178, nel quale le telecamere sono risultate celate all'interno di rilevatori di fumo e dei segnali luminosi delle uscite di emergenza in una società editoriale) nonché, talvolta, anche della clientela (cfr. provv. 4 aprile 2013, n. 163, doc. web n. 2464167, concernente microcamere occultate nei *privées* di un locale notturno nonché mimetizzate all'interno dei camerini delle dipendenti del locale; provv. 30 ottobre 2013, n. 483, doc. web n. 2851973, relativo ad un impianto di videosorveglianza occultato, ed accessibile da remoto, presso un supermercato).

In molti altri casi, pur essendo riconoscibile agli interessati la presenza di un impianto di videosorveglianza, il trattamento è tuttavia risultato effettuato in violazione della disciplina di settore sui controlli a distanza (richiamata dall'art. 114 del Codice): ciò è accaduto in presenza di telecamere che riprendevano gli ambiti spaziali più vari nei quali l'attività dei lavoratori (oltre che di utenti e clienti) poteva svolgersi: in luoghi di cura (provv. 18 aprile 2013, n. 199, doc. web n. 2476068, con riguardo a riprese effettuate nella sala d'attesa e in corrispondenza degli ingressi a strutture sanitarie), nell'area di vendita di un esercizio commerciale e nell'annesso deposito, ove pure erano presenti postazioni di lavoro (provv. 12 settembre 2013, n. 398, doc. web n. 2705679), o, ancora, all'interno di una sala giochi (provv. 8 maggio 2013, n. 231, doc. web n. 2499485); in corrispondenza degli accessi ad un Archivio di Stato e nei suoi corridoi, nelle sale convegno e studio nonché in alcuni ambienti aperti all'utenza per la consultazione di documenti e la visione dei beni archivistici (provv. 18 aprile 2013, n. 200, doc. web n. 2483269); in tal caso, come in altri (cfr. la decisione relativa all'installazione di sistemi di videosorveglianza in sale giochi richiesta in provvedimenti autorizzatori emessi dalla competente autorità di pubblica sicurezza: cfr. provv. 18 dicembre 2013, n. 587, doc. web n. 2914191), il Garante, pur riconoscendo l'ammissibilità dell'installazione dei predetti sistemi di videosorveglianza, ha comunque ritenuto che le operazioni di trattamento delle immagini raccolte dovessero comunque essere effettuate nel rispetto della disciplina sul controllo a distanza dei lavoratori.

Anche alla luce di accertamenti pregressi, l'Autorità ha poi effettuato controlli a campione nell'ambito della grande distribuzione (cfr. par. 18.4), inserendo tale attività ispettiva tra le proprie priorità. Le verifiche hanno evidenziato ampie aree di inosservanza della disciplina applicabile anzitutto in relazione alla normativa in materia di

controlli a distanza dei lavoratori, con riguardo a telecamere installate, all'esterno e all'interno del punto vendita, in modo da poter riprendere anche l'attività del personale addetto alle casse (provv. 18 luglio 2013, n. 361, doc. web n. 2605290) nonché gli ingressi carrai e pedonali (provv. 4 luglio 2013, n. 334, doc. web n. 2577203) o in ambiti ulteriori nei quali poteva comunque essere rilevata l'attività dei lavoratori (ad es., in un deposito seminterrato: cfr. provv. 4 luglio 2013, n. 335, doc. web n. 2577227; v. pure provv. 30 ottobre 2013, n. 484, doc. web n. 2908871). In qualche occasione sono stati altresì accertati tempi di conservazione delle immagini diversi da quelli previsti dal provvedimento autorizzatorio della competente Direzione provinciale del lavoro e quindi in violazione dei principi di liceità del trattamento (cfr. provv. 5 settembre 2013, n. 385, doc. web n. 2683203).

La mancata designazione di incaricati o responsabili del trattamento come pure l'assenza o l'inidoneità dell'informativa resa agli interessati (finanche secondo le modalità semplificate da tempo fissate dal Garante, da ultimo nel provvedimento generale dell'8 aprile 2010, doc. web n. 1712680) rappresentano due "classici" ulteriori esempi di violazioni riscontrate. Per evitare di incorrere in tali violazioni sarebbe stato sufficiente rendere chiaramente visibili agli interessati appositi avvisi sintetici in grado di rendere gli stessi chiaramente edotti del fatto di accedere all'interno di aree videosorvegliate (provv. 21 novembre 2013, n. 521, doc. web n. 2898732); opportunamente, in particolare in relazione ad esercizi commerciali di ampia estensione (o strutturati su più piani), la collocazione di tali avvisi potrebbe estendersi ad aree ulteriori rispetto al solo accesso agli esercizi commerciali (cfr. provv. 12 settembre 2013, n. 397, doc. web n. 2691507).

In mancanza delle garanzie previste dalla disciplina di settore, il Garante ha ritenuto illecito il trattamento effettuato anche nei casi di produzione da parte del titolare del trattamento (per lo più in tempi successivi all'effettuazione delle verifiche *in loco*) di documentazione volta ad attestare, oltre all'informativa resa ai dipendenti, anche una loro manifestazione di consenso al trattamento posto in essere mediante il sistema di videosorveglianza (provv.ti 4 luglio 2013, n. 336, doc. web n. 2578071; 18 luglio 2013, n. 361, doc. web n. 2605290).

Merita infine richiamare, ancorché già menzionato nella Relazione 2012 (p. 195), il provvedimento con il quale il Garante ha dichiarato illecito un trattamento effettuato tramite un sistema di videosorveglianza (che, tra l'altro, riprendeva anche l'area nella quale era posto l'apparecchio per la rilevazione delle presenze dei lavoratori) installato per finalità antitaccheggio presso un esercizio commerciale di una nota catena distributiva, disponendo (in questo caso) il blocco del trattamento dei dati. Al di là di alcuni (più ricorrenti) profili di illiceità del trattamento rilevati nel caso di specie (da un lato l'inidoneità dell'informativa fornita agli interessati nonché la riscontrata possibilità, dal punto di vista tecnico, di accedere alle immagini registrate con modalità diverse da quelle stabilite nell'accordo con le rappresentanze sindacali, in violazione quindi dei princìpi di liceità e correttezza nel trattamento), il Garante ha ravvisato (anche considerato il consolidato indirizzo interpretativo della giurisprudenza di legittimità: cfr. Cass. pen., sez. III, 3 dicembre 2010, n. 1821) quale ulteriore profilo di illiceità del trattamento la circostanza che il personale incaricato di visionare le immagini per le menzionate finalità antitaccheggio, appartenente a società diversa da quella titolare del trattamento, fosse privo della licenza prefettizia richiesta dalla normativa di settore (art. 134, r.d. 18 giugno 1931, n. 773, Tulps) (provv. 17 gennaio 2013, n. 16, doc. web n. 2291893).

Geolocalizzazione

Con riguardo al fenomeno della geolocalizzazione (in particolare di veicoli) – già oggetto di un provvedimento generale dell'Autorità (provv. 4 ottobre 2011, n. 370, doc. web n. 1850581) – sono stati effettuati approfonditi accertamenti ispettivi a

seguito di una segnalazione nella quale si lamentava, presso un compartimento del gestore della rete stradale nazionale, l'uso improprio (e senza l'adozione delle misure previste in materia di controllo a distanza dei lavoratori) di un sistema informativo denominato *road management tool*, comprendente telecamere e un dispositivo di geolocalizzazione installati su veicoli aziendali. Alla luce delle risultanze emerse, il Garante, pur considerando gli strumenti in questione idonei a concorrere ad una più efficiente gestione del servizio reso (specie in casi di criticità sulla rete stradale), come pure incrementare la sicurezza per i lavoratori (in particolare nel caso in cui gli stessi siano chiamati ad operare in luoghi impervi o in presenza di condizioni ambientali avverse), ha ritenuto che il loro impiego dovesse comunque avvenire nel rispetto dei principi in materia di protezione dei dati personali e della disciplina di settore nonché con modalità concretamente idonee a garantire, in particolare, l'osservanza dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (provv. 7 marzo 2013, n. 103, doc. web n. 2471134). Non è stato invece possibile accertare il lamentato uso improprio di detto sistema a causa di alcune operazioni di modifica dei tempi di conservazione dei dati, effettuate nel corso degli accertamenti ispettivi (e oggetto ora di valutazione da parte della competente autorità giudiziaria), che hanno comportato la cancellazione di tutte le immagini in precedenza registrate nel sistema (il cui termine di conservazione era originariamente decennale).

Solo dopo gli accertamenti, la società ha provveduto, da un lato, a designare incaricati del trattamento soggetti che potevano avere accesso ai dati di localizzazione solo in ragione delle mansioni concretamente svolte e, dall'altro, a concludere, a livello nazionale, un accordo con le rappresentanze sindacali (poi inoltrato ai capi compartimento della società al fine di attivare il confronto con le organizzazioni sindacali locali e condividerne i contenuti tra il personale).

11.2. *Il trattamento di dati biometrici e la rilevazione delle presenze*

Sono continuate a pervenire al Garante segnalazioni (talvolta da parte di direzioni territoriali del lavoro) riferite all'utilizzo di sistemi biometrici (cfr. par. 12.1) finalizzati alla rilevazione delle presenze dei dipendenti. In proposito l'Autorità ha ribadito il proprio consolidato orientamento in base al quale il trattamento di dati biometrici dei lavoratori per finalità di ordinaria gestione del rapporto di lavoro e, in particolare, di commisurazione dell'orario di servizio prestato, non è di regola conforme ai principi di necessità, pertinenza e non eccedenza (cfr. già punto 4 del provv. 23 novembre 2006, linee guida per il trattamento di dati dei dipendenti privati, doc. web n. 1364099 e 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). Indirizzo – condiviso dalla giurisprudenza di merito (Trib. Prato, 19 settembre 2011) e coerente con quanto affermato nel parere 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012, dal Gruppo Art. 29 – secondo cui "il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico" – che ammette il trattamento dei dati biometrici solo in casi particolari, di regola per presidiare l'accesso ad "aree sensibili", tenendo conto delle attività che si svolgono nei luoghi presidiati o dei beni nelle stesse custoditi.

Il Garante ha altresì chiarito che si ha trattamento di dati biometrici (diversamente da quanto sovente rappresentato nella documentazione predisposta da società che producono e/o installano sistemi biometrici) – con conseguente applicazione della disciplina in materia di trattamento dei dati personali – anche nel caso in cui il rilievo dat-

tiloscopico, temporaneamente raccolto ai soli fini del completamento della fase di *enrollment*, venga successivamente utilizzato (sotto forma di codice numerico) per le operazioni di verifica e raffronto nell'ambito di procedure di autenticazione.

In termini generali è altresì ricorrente l'inadempimento dell'obbligo di notificare i trattamenti effettuati mediante l'impiego di dispositivi biometrici (cfr. artt. 37 e 163 del Codice) nonché quello di fornire preventivamente ai lavoratori interessati idonei elementi informativi circa le caratteristiche dei trattamenti da effettuarsi (cfr. artt. 13 e 161 del Codice).

Per quanto riguarda la casistica considerata, si segnala l'istanza nella quale un Comune, presso il quale si erano verificati fenomeni di abusi derivanti da un uso improprio del *badge* attribuito ai dipendenti per la rilevazione delle rispettive presenze – peraltro stigmatizzati dall'intervento della magistratura con provvedimenti a carico degli interessati – manifestava l'intenzione di avvalersi per detta finalità di un sistema biometrico. L'Autorità ha in proposito rilevato l'assenza di circostanziati elementi, strettamente rapportati alla specifica realtà lavorativa (quali, ad es., la dislocazione decentrata degli uffici tale da ostacolare un'agevole verifica della corretta esecuzione delle prestazioni lavorative), da cui si potesse effettivamente arguire l'insufficienza di ordinarie misure di controllo (e, correlativamente, la reale indispensabilità del trattamento dei dati biometrici dei lavoratori per la finalità suindicata). Né è risultata comprovata l'adozione da parte dell'amministrazione di sistemi fisici volti ad assicurare la presenza effettiva dei lavoratori durante l'orario di lavoro (ad es., l'installazione dei cc.dd. tornelli) o di ulteriori misure, meno invasive, volte comunque a prevenire il ripetersi di abusi (quali l'associazione di un codice individuale ai *badge* già attribuiti ai dipendenti) o, ancora, l'inefficacia dei controlli ordinari circa la presenza dei lavoratori presso l'amministrazione istante per il tramite dei dirigenti (sui quali anzitutto incombe la verifica quotidiana, peraltro di immediata evidenza, della presenza del personale agli stessi assegnato, il quale, a domanda, può assentarsi dal lavoro solo a seguito di valutazione del superiore gerarchico preposto all'unità organizzativa presso cui presta servizio) ovvero di controlli a campione da parte delle competenti strutture dell'amministrazione comunale non risultando dalle dichiarazioni rese né la frequenza, né le modalità in concreto osservate di utilizzo, in sede di verifica, dei fogli-presenza. Verifiche, queste, di agevole realizzazione, anche considerato il numero contenuto di dipendenti comunali (numero ancor più ridotto ove il fenomeno dell'assenteismo fosse risultato consolidato), delle quali nel caso di specie non è stata dimostrata l'inefficacia e che potrebbero comunque contenere significativamente il rischio di pratiche abusive ove efficacemente contrastate, porendo le stesse configurarsi quali violazioni di carattere penale, oltre che disciplinare e contabile. Peraltro, ad avviso del Garante, il trattamento dei dati biometrici per la finalità considerata, oltre ad essere in linea di principio sproporzionato (come detto), potrebbe in concreto rivelarsi comunque di scarsa utilità nel contrasto dell'assenteismo; tale modalità di rilevazione delle presenze, infatti, non è di per sé in grado di assicurare l'effettiva presenza sul luogo di lavoro dei dipendenti infedeli ove manchino, in pari tempo, efficaci sistemi di controllo e vigilanza sull'effettiva (operosa) presenza dei lavoratori durante l'arco dell'intera giornata lavorativa (specie ove il fenomeno assuma le proporzioni segnalate nel caso in esame) (provv. 31 gennaio 2013, n. 38, doc. web n. 2304669).

L'Autorità ha altresì adottato tre provvedimenti in materia nei confronti di altrettanti istituti scolastici. Nel primo dei casi considerati è risultato essere stato installato (anche a seguito di ispezione effettuata dalla competente Direzione territoriale del lavoro), presso un Liceo scientifico statale, un sistema biometrico (basato sulla rilevazione delle impronte digitali) finalizzato alla rilevazione delle presenze del personale docente. Tale trattamento è stato ritenuto illecito alla luce dei principi di necessità,

pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice) posto che il titolare del trattamento non aveva dato prova dell'esistenza di elementi obiettivi dai quali desumere, rispetto alla legittima finalità di controllo delle presenze, l'inidoneità delle ordinarie misure di controllo. Peraltro l'utilizzo del sistema biometrico è stato ritenuto non conforme alla specifica disciplina dettata per il settore scolastico, in base alla quale l'accertamento delle presenze del personale docente è effettuata mediante la compilazione di apposito foglio firme ovvero del registro di classe (provv. 30 maggio 2013, n. 261, doc. web n. 2502951).

Anche presso un Istituto tecnico industriale è stato installato un sistema biometrico (anch'esso relativo a impronte digitali) allo scopo di controllare le presenze del personale amministrativo, tecnico e ausiliario, stante la dichiarata necessità di prevenire condotte abusive. Anche in questo caso non sono stati rappresentati al Garante elementi concreti riferiti alla specifica realtà lavorativa dell'istituto dai quali poter dedurre l'inefficacia degli ordinari strumenti di controllo della presenza in servizio. Pertanto, pur ribadendo che l'utilizzo dei sistemi biometrici avrebbe potuto risultare legittimo in relazione alla diversa finalità di controllare l'accesso del personale ad aree ove venissero custoditi documenti riservati o attrezzature di valore, l'Autorità ha dichiarato illecito il trattamento dei dati biometrici riferiti ai lavoratori (provv. 30 maggio 2013, n. 262, doc. web n. 2503101).

Alle medesime conclusioni il Garante è pervenuto nel caso di un sistema biometrico di rilevazione delle presenze del personale amministrativo, tecnico e ausiliario installato (come verificato a seguito di accertamenti ispettivi disposti dall'Autorità) presso un Liceo scientifico statale. La scelta di adottare dispositivi basati sulla tecnologia biometrica è stata effettuata in base all'astratta possibilità di utilizzo abusivo degli strumenti tradizionali di controllo delle presenze (ad es., i *badge*), senza peraltro rappresentare l'eventuale effettuazione di controlli circa la presenza in servizio dei lavoratori secondo modalità meno invasive: il trattamento è stato quindi ritenuto illecito alla luce dei già richiamati principi di necessità, pertinenza e non eccedenza (provv. 1° agosto 2013, n. 384, doc. web n. 2578547).

11.3. *L'intermediazione di lavoro e la ricerca e selezione del personale*

Il Garante ha altresì affrontato alcuni aspetti relativi al trattamento di dati personali riferiti a candidati al lavoro. A seguito di una complessa attività istruttoria, nel corso della quale è stato effettuato un accertamento ispettivo, l'Autorità ha verificato che attraverso un sito internet erano stati trattati con modalità ritenute illecite centinaia di migliaia di dati personali (contenuti all'interno di *curricula vitae* e profili) di candidati a posizioni lavorative. Il titolare del trattamento, infatti, è risultato effettuare trattamenti di dati personali dei candidati per finalità di intermediazione tra domanda ed offerta di lavoro, come definita dall'art. 2, comma 1, lett. *b*), d.lgs. 10 settembre 2003, n. 276 (Attuazione delle deleghe in materia di occupazione e mercato del lavoro, di cui alla legge 14 febbraio 2003, n. 30) – in particolare le attività di "raccolta dei *curricula* dei potenziali lavoratori", la "costituzione di relativa banca dati" nonché la "promozione e gestione dell'incontro tra domanda e offerta di lavoro" – senza soddisfare i requisiti previsti dalla legge per lo svolgimento di tale attività soggetta ad autorizzazione (e, tra questi, il conferimento dei dati relativi ai candidati a Cliclavoro, portale del Ministero del lavoro e delle politiche sociali che costituisce la Borsa continua nazionale del lavoro), con conseguente violazione del principio di liceità del trattamento. Sotto diverso profilo, le informazioni conferite dai candidati sono risultate trattate per finalità ulteriori (veicolazione di promozioni per conto del medesimo tito-

lare o di terzi) in assenza di un'informativa chiara e trasparente e senza aver previamente raccolto il libero consenso degli interessati in relazione alle distinte operazioni di trattamento (che dovevano invece formare oggetto di accettazione "in blocco" da parte degli interessati affinché gli stessi potessero utilmente conferire il proprio *curriculum*). Per questi motivi i descritti trattamenti sono stati vietati dal Garante (provv. 5 dicembre 2013, n. 547, doc. web n. 2865637) e copia del provvedimento è stata trasmessa al Ministero del lavoro e delle politiche sociali per i profili di competenza.

In una diversa fattispecie, un'agenzia per il lavoro (regolarmente autorizzata) in occasione dello svolgimento di "colloqui conoscitivi" di candidati a determinate posizioni lavorative acquisiva la copia del documento di identità al dichiarato scopo di riservarsi "un più accurato controllo, in un secondo momento, dell'esattezza dei dati trascritti". Tale attività di acquisizione e conservazione di copia di documenti identificativi già in fase di selezione dei candidati è stata ritenuta dal Garante eccedente (ai sensi dell'art. 11, comma 1, lett. *d*), del Codice) rispetto alla legittima finalità di identificazione dei candidati stessi. Allo scopo deve infatti ritenersi sufficiente l'adozione di misure organizzative volte ad assicurare la corretta identificazione degli interessati – anche previa esibizione di un documento personale – limitando la raccolta delle informazioni a quelle pertinenti e non eccedenti (rilevato che, ad esempio, la carta di identità contiene anche informazioni non rilevanti per il conseguimento delle finalità di preliminare selezione di personale). Pertanto, anche nella prospettiva del contrasto del cd. furto di identità, l'acquisizione di copie di documenti di identità deve limitarsi ai casi previsti da puntuali previsioni normative ovvero qualora ne risulti provata l'indispensabilità (provv. 4 aprile 2013, n. 162, doc. web n. 2484965; v. già provv. 27 ottobre 2005, doc. web n. 1189435).

11.4. *Il trattamento di dati personali nella gestione del rapporto di lavoro*

Sempre più frequentemente vengono lamentate forme di accesso ad informazioni personali o di circolazione improprie di dati personali all'interno della realtà lavorativa. In taluni casi, l'accertamento dei trattamenti oggetto di segnalazione è risultato non agevole o impossibile (v., ad es., provv. 1° agosto 2013, n. 383, doc. web n. 2604028, nel quale il Garante, a seguito di una pur articolata istruttoria, in presenza di dichiarazioni non concordanti rese dalle parti del procedimento, ha potuto accertare il solo mancato aggiornamento di dati personali riferiti al segnalante alla luce delle risultanze del libro dei soci; analogamente, nel caso deciso con provv. 8 maggio 2013, n. 232, doc. web n. 2501216, pur non risultando comprovato che note aventi ad oggetto un procedimento disciplinare fossero state trasmesse all'interessato da personale non autorizzato in base alle mansioni attribuite all'interno di un'amministrazione regionale, sulla base degli elementi emersi, il Garante ha comunque prescritto all'ente, quale misura opportuna, di rivalutare le soluzioni organizzative adottate al fine di assicurare maggiore effettività nell'attuazione della disciplina di protezione dei dati personali, con particolare riguardo alla designazione degli incaricati e al coordinamento tra le molteplici unità organizzative presenti all'interno dell'amministrazione).

In molti altri casi sono invece emerse diverse violazioni: così, in una vicenda peculiare, è stata ritenuta illecita la comunicazione effettuata ad una compagnia di assicurazione di dati personali di una lavoratrice al fine di attivare una polizza collettiva da parte del datore di lavoro contraente, in assenza del consenso informato della lavoratrice/assicurata necessario ai sensi degli artt. 13 e 23 del Codice (oltre che in base all'art. 1919 c.c. per i diversi profili contrattuali). Si è ritenuto pertanto (in un contesto di dichiarazioni peraltro discordanti circa l'origine e le modalità di acquisizione dei

dati personali riferiti alla segnalante) di muovere dal contenuto del contratto di assicurazione stipulato dal datore di lavoro che poneva in capo a quest'ultimo (contraente e beneficiario della polizza) l'obbligo di trasmettere all'assicuratore i dati personali riferiti ai propri dipendenti (allo stesso noti) necessari alla predisposizione e alla successiva gestione della polizza collettiva. Nell'ambito del medesimo provvedimento è stata altresì dichiarata l'illiceità del trattamento dei dati riferiti alla segnalante effettuato dalla compagnia di assicurazione in difetto della prescritta informativa (provv. 11 aprile 2013, n. 179, doc. web n. 2492743).

In altra vicenda, il Garante ha ritenuto infondato un reclamo presentato a seguito della comunicazione di informazioni sul reddito di un dipendente (emolumenti percepiti e somme che avrebbero dovuto essere corrisposte all'esito di una transazione in corso) effettuata dal datore di lavoro su richiesta di un legale nell'ambito di un giudizio di separazione personale. Posto che non è necessario acquisire il consenso dell'interessato per effettuare una comunicazione di dati personali quando ciò sia necessario per far valere o difendere un diritto in giudizio (cfr. art. 24, comma 1, lett. *f*), del Codice), le informazioni comunicate sono state ritenute pertinenti e non eccedenti rispetto alla trattazione nel corso della pendente causa di separazione (provv. 11 aprile 2013, n. 180, doc. web n. 2475832).

Anche nel settore del pubblico impiego la materia dell'indebita circolazione di informazioni personali non solo verso l'esterno ma anche all'interno dei contesti lavorativi (verso soggetti non autorizzati), rimane d'attualità. Ciò è confermato dai numerosi casi segnalati, alcuni dei quali aventi ad oggetto dati sensibili dei lavoratori, che evidenziano talora la mancata adozione di idonee procedure interne volte a consentire il corretto trattamento di dati personali (o comunque la loro inosservanza ove previste). Nella maggior parte dei casi, l'Autorità ha accertato l'illiceità delle comunicazioni di dati personali dei lavoratori a soggetti terzi riservandosi di valutare, con separato procedimento, gli estremi per la contestazione delle violazioni amministrative previste dalla disciplina del Codice.

A tale proposito, è stato ribadito che, anche in ambito lavorativo, il trattamento di dati sensibili da parte di soggetti pubblici può essere effettuato in modo lecito solo se previsto da specifica norma di legge ed in relazione ad informazioni ritenute indispensabili per lo svolgimento delle attività istituzionali da parte dell'amministrazione (cfr. artt. 20, comma 1 e 22, comma 3 del Codice). Ciò tanto più se trattasi, come in un caso oggetto di segnalazione, della comunicazione di informazioni su specifiche patologie (nonché sul grado di disabilità conseguito) sofferte dal dipendente di un'azienda sanitaria provinciale avvenuta in occasione della richiesta, avanzata da quest'ultimo, di permanenza in servizio fino al compimento del 67° anno di età. La normativa di settore prevede che, in tale ipotesi, l'amministrazione debba valutare la richiesta in base alle proprie "esigenze organizzative e funzionali", senza riferimento alcuno alla necessità di trattare dati sanitari. Nella vicenda considerata, invece, il dato riferito ad una grave patologia (puntualmente indicata) occorsa al lavoratore ha formato oggetto di menzione nell'ambito di uno scambio di corrispondenza tra diverse articolazioni dell'azienda: ritenuta tale circolazione di informazioni sensibili non indispensabile né pertinente rispetto alla finalità perseguita dall'amministrazione, oltre che lesiva della dignità dell'interessato, il trattamento è stato ritenuto dal Garante illecito; considerato inoltre il contenuto (talvolta anche divergente) delle comunicazioni inviate all'Autorità nel corso dell'istruttoria, il Garante ha altresì prescritto al titolare di rivalutare le soluzioni organizzative esistenti allo scopo di assicurare effettività nell'attuazione della disciplina di protezione dei dati personali, identificando, vista la presenza della figura del "referente aziendale *privacy*", le funzioni competenti ad interloquire con l'autorità di controllo (provv. 18 dicembre 2013, n. 589, doc. web n. 2909040).

Tra le segnalazioni e i reclami pervenuti vale la pena evidenziare quelli relativi alle modalità di notifica di comunicazioni concernenti procedimenti disciplinari ovvero documenti contenenti valutazioni riferite a singoli lavoratori. In particolare, in occasione della consegna al personale di un'autorità portuale delle buste paga nelle quali venivano altresì liquidati gli importi legati al riconoscimento di premi di produttività, era stata consegnata al personale della struttura anche copia di un processo verbale concernente il raggiungimento degli obiettivi oggetto di contrattazione collettiva, contenente altresì le note valutative e la menzione dell'irrogazione di sanzioni disciplinari a carico di una dipendente. Nella vicenda considerata, il Garante ha ritenuto integrata una comunicazione di dati personali in violazione di legge (cfr. artt. 11, comma 1, lett. *a*) e 19, comma 3, del Codice), peraltro avvenuta secondo modalità non conformi al principio di pertinenza e non eccedenza nel trattamento dei dati (art. 11, comma 1, lett. *d*), del Codice). Nel ribadire che il datore di lavoro pubblico, nel legittimo perseguimento della propria attività istituzionale, deve poter tener conto delle eventuali sanzioni disciplinari comminate al personale in sede di commisurazione del premio di risultato (attività che rientra nel novero delle finalità di gestione del rapporto di lavoro), tuttavia, l'Autorità ha precisato che le misure disciplinari adottate non possono essere oggetto di comunicazione a soggetti diversi dall'interessato in assenza di una specifica norma di legge o di regolamento (provv. 3 ottobre 2013, n. 431, doc. web n. 2747867).

Tra le decisioni di analogo contenuto, merita evidenziare due casi concernenti la riconosciuta illiceità, per assenza del presupposto normativo, della trasmissione, da parte di un Tribunale, delle schede valutative relative a due dipendenti ai due diversi enti presso i quali le stesse prestavano temporaneamente la propria attività lavorativa (in un caso per distacco *ex* art. 30, comma 1, d.lgs. 10 settembre 2003, n. 276, in altro per assegnazione temporanea *ex* art. 23-*bis*, comma 7, d.lgs. n. 165/2001).

In entrambe le fattispecie la documentazione contenente dati personali (le menzionate schede di valutazione) era stata trasmessa (in un caso via fax e in un altro mediante casella di posta elettronica certificata) dal personale amministrativo operante presso il Tribunale, indirizzandola, non già alle dirette interessate (come peraltro stabilito dall'accordo sindacale al precipuo fine di consentire alle stesse di formulare le proprie osservazioni), ma ai diversi Uffici presso i quali le due lavoratrici risultavano temporaneamente in servizio, consentendo, per l'effetto, al personale ivi operante di prenderne conoscenza, in carenza di idoneo presupposto normativo (provv.ti 5 dicembre 2013, n. 545, doc. web n. 2894559 e n. 546, doc. web n. 2896275).

La condotta tenuta si è distaccata dalle indicazioni formulate da tempo dal Garante (cfr. le linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007 e già il punto 5.5 della deliberazione n. 53 del 23 novembre 2006, doc. web n. 1364939, linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati) con le quali si è precisato che "fuori dei casi in cui forme e modalità di divulgazione di dati personali siano regolate specificamente da puntuali previsioni [...], l'amministrazione deve utilizzare forme di comunicazione individualizzate con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali [...] da parte di soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali)" (punto 5.3). Né la circostanza che possa sussistere in capo al mittente, come nei casi considerati, un legittimo interesse ad acquisire prova dell'avvenuta ricezione

della documentazione inviata, può esonerarlo dall'adottare opportune cautele volte ad evitare che soggetti diversi dal destinatario possano apprenderne il contenuto senza essere a ciò legittimati, prevenendo così lesioni del diritto alla riservatezza e alla protezione dei dati dell'interessato.

Né viene meno l'illiceità della comunicazione per il fatto che il Tribunale, in una delle fattispecie considerate (provv. n. 545/2013, cit.) abbia inviato la documentazione in questione indirizzandola (anziché all'interessata) alla casella di posta elettronica certificata della società presso la quale la medesima prestava servizio. A giudizio del Garante, infatti, il richiamo operato dal titolare del trattamento all'art. 16-*bis*, comma 6, d.l. 29 novembre 2008, n. 185 (convertito con modificazioni, dall'art. 1, l. 28 gennaio 2009, n. 2) non era pertinente, atteso che detta disposizione, nel consentire alle pp.aa. di avvalersi della posta elettronica certificata quale canale comunicativo con i dipendenti della medesima (e di diversa) amministrazione, fa riferimento all'indirizzo di posta elettronica eventualmente ai medesimi assegnato (*uti singuli*) e non, invece, a quello dell'amministrazione presso la quale gli stessi prestano servizio. Ciò si desume dall'art. 47, comma 3, d.lgs. 7 marzo 2005, n. 82 (Cad) che consente alle pp.aa. di utilizzare "per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati", informativa che, peraltro, nel caso di specie, non è risultato sia stata fornita all'interessata. Peraltro, accedendo all'interpretazione fornita dal titolare del trattamento – al di là della circostanza che un novero assai ampio di comunicazioni di natura personale e talora sensibile riferite ai singoli interessati potrebbe essere soggetto ad ampia circolazione nell'ambito delle pp.aa. –, si perverrebbe all'esito opposto voluto dalla norma che mira, come esplicitato dalla rubrica dell'art. 16-*bis*, ad introdurre "misure di semplificazione": semplificazioni che si ottengono consentendo l'invio delle comunicazioni all'indirizzo di posta elettronica assegnato ai dipendenti destinatari delle stesse (non diversamente dai cittadini menzionati all'art. 16-*bis*, comma 5) e non invece obbligando (invero irrazionalmente) le amministrazioni ad utilizzare i propri indirizzi istituzionali di posta elettronica certificata per (poi) far pervenire – secondo canali tradizionali – le comunicazioni ai diretti interessati.

Analogamente, a fronte di un reclamo concernente la comunicazione di dati personali (sensibili) via posta elettronica indirizzata ad una pluralità di destinatari, il Garante ha ritenuto illecita l'operazione di trattamento in ragione delle modalità utilizzate dal datore di lavoro. Nel caso di specie era stata diramata ad alcune stazioni di un corpo forestale e di vigilanza ambientale, all'indirizzo *e-mail* personale di diversi dipendenti e ai superiori gerarchici degli interessati, una comunicazione riguardante 32 dipendenti, cui era allegata una tabella recante i nominativi dei lavoratori che, su richiesta del medico competente, a seguito della visita medica periodica effettuata ai fini dell'accertamento dello stato di salute ed idoneità alle mansioni (ai sensi dell'art. 41, comma 2, lett. *b*), d.lgs. n. 81/2008), avrebbero dovuto sottoporsi ad ulteriori accertamenti sanitari. La tabella riportava altresì per ciascuno il numero di matricola, la data di nascita, il Servizio di appartenenza, nonché l'indicazione delle ulteriori visite ed esami richiesti (provv. 10 ottobre 2013, n. 443, doc. web n. 2774063). La tipologia degli accertamenti medici richiesti per i reclamanti (e per ciascuno degli altri interessati) nell'ambito del procedimento per il rilascio del giudizio di idoneità alla mansione specifica non può, a giudizio del Garante, in assenza di specifica base normativa, essere resa nota a terzi (artt. 11, comma 1, lett. *a*), e 20 comma 1 e 2, del Codice). Sotto diverso profilo, inoltre, gli stessi lavoratori destinatari della comunicazione e convocati per gli accertamenti – rispetto ai

quali, come detto, sarebbe stato opportuno provvedere a comunicazioni individualizzate - non avevano titolo alcuno per venire a conoscenza degli accertamenti clinici disposti in capo ai colleghi, né sussistevano ragioni per mettere i lavoratori reciprocamente a conoscenza anche della specifica natura degli accertamenti prescritti. Con riguardo infine alla comunicazione nei confronti dei superiori gerarchici e delle strutture territoriali del Corpo forestale, l'Autorità ha chiarito che, salve le esigenze di servizio e di gestione dei turni di lavoro, l'avvenuta trasmissione della tabella nominativa è stata effettuata in violazione del principio di indispensabilità, poiché sarebbe stato sufficiente mettere a parte questi ultimi del solo termine fissato per lo svolgimento degli accertamenti del personale di diretta collaborazione al fine di consentire il tempestivo approntamento delle sostituzioni tra il personale, senza indicare la tipologia degli accertamenti sanitari.

Tale orientamento è stato confermato in successive decisioni, tra le quali merita evidenziare la riconosciuta illiceità, per violazione dei principi di necessità, finalità e liceità, del trattamento di dati sensibili concernenti le condizioni di salute di propri dipendenti effettuato da un'azienda sanitaria provinciale. Nel caso considerato, l'azienda aveva inviato nota di solleciro al Comitato di verifica per le cause di servizio relative a dieci dipendenti (e, tra questi, al segnalante), inviando a tutti per conoscenza la medesima nota. Per effetto delle modalità comunicative prescelte, il trattamento dei dati dei dipendenti – legittimamente effettuato dall'Asp limitatamente all'istruttoria del procedimento regolato dal d.P.R. n. 461/2001, con l'adozione delle garanzie ivi previste – è risultato effettuato in violazione degli artt. 11, comma 1, lett. *a*) e 20, commi 1 e 2, del Codice: ciascuno dei dieci interessati, infatti, è stato indebitamente reso edotto dell'esistenza di procedimenti amministrativi riguardanti, oltre che la propria persona, gli altri nove lavoratori e, al contempo, messo a conoscenza di dati concernenti le condizioni di salute di ciascuno di questi (provv. 10 ottobre 2013, n. 442, doc. web n. 2753605). La menzione di procedimenti per il riconoscimento della dipendenza di infermità da causa di servizio facenti capo ai lavoratori contenuta nel sollecito oggetto di segnalazione comporta invero, pur non essendo stata esplicitata nel medesimo la specifica patologia relativa a ciascuno, una comunicazione di dati comunque suscettibile di "rivelare lo stato di salute" degli interessati ai sensi dell'art. 4, comma 1, lett. *d*), del Codice (in merito alla nozione di dato relativo alle condizioni di salute cfr. linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, punto 6.3; provv.ti 27 giugno 2013, n. 315, doc. web n. 2576686; 3 febbraio 2009, doc. web 1597590; 7 luglio 2004, doc. web n. 1068839 e 1068917; v. anche Cass., 1° agosto 2013, n. 18980).

In altra decisione, il Garante ha dichiarato l'illiceità della circolazione avvenuta nell'ambito di un ateneo di documentazione contenente dati relativi alla salute dell'interessata (segnatamente le informazioni relative all'"interdizione dal lavoro" di una docente per le ragioni previste dall'art. 17 comma 2, lett. *a*), d.lgs. n. 151/2001 in presenza di "gravi complicanze della gravidanza o [a] persistenti forme morbose che si presume possano essere aggravate dallo stato di gravidanza"). L'Autorità ha precisato che i dati sensibili in questione, che legittimamente possono essere trattati dalle competenti funzioni e dal personale amministrativo dell'Università a tal fine incaricato del trattamento per la dichiarata finalità di "gestione del rapporto di lavoro" (cfr. artt. 11, comma 1, lett. *a*), 20, comma 1 e 112, comma 1, del Codice), non potevano invece formare legittimamente oggetto di comunicazione a terzi (nel caso di specie ad altro docente nonché ai componenti del Consiglio di Facoltà) non avendo questi titolo alcuno a trattarli per la menzionata finalità di gestione del rapporto di lavoro (provv. 27 giugno 2013, n. 315, doc. web n. 2576686).