1997 2017

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Relazione2016

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Antonello Soro, *Presidente*
Augusta Iannini, *Vice Presidente*
Giovanna Bianchi Clerici, *Componente*
Licia Califano, *Componente*

Giuseppe Busia, *Segretario generale*

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
www.garanteprivacy.it

14 La protezione dei dati personali nell'ambito del rapporto di lavoro pubblico e privato

Com'è noto nel 2015 è stata completata la cd. riforma del lavoro (o *Jobs Act*) con i decreti legislativi di attuazione della legge-delega n. 183/2014 alcuni dei quali hanno avuto importanti riflessi sulla normativa in materia di protezione di dati personali, sia sotto il profilo del trattamento di informazioni in grandi banche dati nel settore lavoristico (anche di nuova istituzione e nell'ambito del sistema informativo unitario delle politiche del lavoro; d.lgs. nn. 150/2015 e 151/2015), sia per quanto riguarda la disciplina dei controlli a distanza dell'attività dei lavoratori (art 23, d.lgs. n. 151/2015 che ha modificato l'art. 4, l. n. 300/1970, recante lo Statuto dei lavoratori) (cfr. Relazione 2015, par. 2.1.2). Il Garante aveva seguìto l'*iter* di approvazione di tali atti normativi formulando anche osservazioni critiche nel corso dell'esame parlamentare degli schemi di decreto, in due audizioni presso le Commissioni lavoro della Camera e del Senato (tenute rispettivamente il 9 e il 14 luglio 2015, doc. web n. 4119045).

Nel 2016 sono stati portati all'attenzione dell'Autorità diversi trattamenti effettuati in tale ambito rispetto ai quali ha trovato applicazione la nuova disciplina dei controlli a distanza, nell'esame dei quali il Garante ha avuto modo di affrontare alcuni aspetti meritevoli di attenzione sul piano interpretativo ed applicativo. In particolare, come meglio si vedrà avanti (cfr. par. 14.2), un provvedimento del Garante ha rappresentato la prima occasione in cui l'Autorità ha espresso il proprio orientamento sull'ambito di applicazione del comma 2 del predetto art. 4 dello Statuto dei lavoratori come modificato dal citato art. 23, d.lgs. n.151/2015, mediante una possibile "perimetrazione" degli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", in presenza dei quali vengono meno talune garanzie per gli interessati.

Il Garante è altresì intervenuto in merito al trattamento di dati biometrici dei lavoratori per finalità di sicurezza o di rilevazione delle presenze nel quadro della più generale esigenza di assicurare il rispetto dell'obbligo di prestazione lavorativa a fronte di casi di assenteismo verificatisi in alcune amministrazioni pubbliche (cfr. par. 16.2).

Non sono mancate infine altre pronunce sul trattamento di dati personali nella gestione del rapporto di lavoro, con particolare riguardo al trattamento di dati giudiziari (cfr. par. 14.4), o in caso di pubblicazione dei dati dei lavoratori, anche in relazione alle possibili interferenze con la disciplina in materia di trasparenza (cfr. par. 14.3).

14.1. *Il trattamento di dati relativi ai dipendenti tramite sistemi di geolocalizzazione*

Con riferimento ai trattamenti di dati personali effettuati attraverso sistemi che consentono la localizzazione geografica dei dipendenti nell'ambito del rapporto di lavoro, anche nel 2016 si registra un incremento dei casi sottoposti all'attenzione dell'Autorità sia con segnalazioni, sia con istanze di verifica preliminare presentate dai titolari del trattamento, sia all'esito di attività di controllo effettuate anche con accertamenti *in loco*.

Tale incremento è indice dell'uso sempre più diffuso di dispositivi tecnologici completi di funzionalità di geolocalizzazione nel contesto dei processi produttivi, preordinati al raggiungimento di finalità eterogenee.

In materia il Garante ha adottato un provvedimento di carattere generale relativo alla geolocalizzazione di veicoli (cfr. provv. 4 ottobre 2011, n. 370, doc. web n. 1850581), nonché due provvedimenti "pilota" relativi all'utilizzo di applicazioni informatiche che consentono di localizzare geograficamente dispositivi mobili (*smartphone*) forniti in dotazione ai dipendenti (cfr. provv.ti 11 settembre 2014, n. 401, doc. web n. 3474069 e 9 ottobre 2014, n. 448, doc. web n. 3505371). L'Autorità ha in particolare ritenuto che il trattamento di dati personali riferiti alla localizzazione di dispositivi – che, differentemente dai veicoli di servizio, da un lato "seguono" costantemente il dipendente, dall'altro si prestano comunemente ad utilizzi anche privati, spesso consentiti dal datore di lavoro – presenta rischi specifici per le libertà (es. di circolazione e di comunicazione), i diritti e la dignità dei lavoratori.

In relazione a tali trattamenti, inoltre, il Garante ha rammentato che la localizzazione dei dati relativi alla posizione geografica è soggetta all'obbligo di notificazione ai sensi dell'art. 37, comma 1, lett. *a*) del Codice.

Per quanto riguarda l'applicazione ai predetti sistemi della disciplina in materia di controlli a distanza dell'attività del lavoratore (art. 4, l. 20 maggio 1970, n. 300, recante lo Statuto dei lavoratori, richiamato dall'art. 114 del Codice), si segnala che a seguito delle recenti modifiche apportate al citato art. 4 dal d.lgs. 14 settembre 2015, n. 151 (art. 23), l'Ispettorato nazionale del lavoro, con circolare n. 2 del 2016, relativamente all'installazione di apparecchiature di localizzazione satellitare GPS su autovetture aziendali, ha chiarito che "in linea di massima e in termini generali […] i sistemi di geolocalizzazione rappresentano un elemento «aggiunto» agli strumenti di lavoro", e pertanto "le relative apparecchiature possono essere installate solo previo accordo con la rappresentanza sindacale ovvero, in assenza di tale accordo, previa autorizzazione da parte dell'Ispettorato nazionale del lavoro".

Uso delle tecnologie di geolocalizzazione per finalità di rilevazione delle presenze

Il Garante, nell'ambito di un procedimento di verifica preliminare, ha ammesso l'utilizzo di un sistema di rilevazione di inizio e fine dell'attività lavorativa (e della pausa pranzo, se prevista) prospettato da due società operanti nel settore dell'intermediazione in materia di lavoro. Il sistema prospettato – ferma restando l'alternatività con gli altri strumenti già in uso e rimasti comunque a disposizione – si basava sull'installazione sui dispositivi *smartphone* di proprietà dei lavoratori di un applicativo sviluppato da un soggetto terzo designato responsabile del trattamento.

Considerato che la gran parte dei dipendenti svolgeva la propria attività lavorativa al di fuori della sede aziendale, sia presso l'utilizzatore (in caso di somministrazione di lavoro) sia presso i clienti, il sistema sottoposto a verifica preliminare avrebbe consentito alle società richiedenti di realizzare risparmi di gestione nonché di semplificare e di incrementare l'efficienza e la certezza dell'attività di rilevazione delle presenze, anche a favore dell'effettiva certificazione delle ore lavorate presso l'utilizzatore.

L'Autorità, nella prospettiva della *privacy by design*, ha impartito alcune misure a tutela dei diritti degli interessati, in attuazione del principio di necessità (art. 3 del Codice). In particolare, considerata l'incidenza di errori nella rilevazione della posizione geografica (dovuti sia al sistema che ai GPS installati sui singoli dispositivi mobili) e rilevata la diversità dell'informazione raccolta rispetto ai sistemi ordinari di rilevazione delle presenze, il Garante ha stabilito che le società dovranno configurare il sistema in modo da cancellare le coordinate geografiche della posizione del lavoratore, dopo aver verificato preventivamente – al fine di scongiurare abusi – l'associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavo-

14

ratore, e conservando eventualmente il solo dato relativo alla sede di lavoro, oltre che la data e l'orario cui si riferisce la "timbratura". Il sistema inoltre dovrà rendere sempre visibile un'icona che indichi che la funzionalità di localizzazione è attiva. Deve altresì essere preventivamente impedito il trattamento anche accidentale di dati presenti sul dispositivo riferiti alla vita privata del lavoratore (dati relativi al traffico telefonico, agli sms, alla posta elettronica, alla navigazione in internet ed altro) (provv. 8 settembre 2016, n. 350, doc. web n. 5497522).

Sistemi di localizzazione dei dispositivi affidati al personale in servizio all'esterno

In un altro caso l'Autorità ha ritenuto conforme ai princìpi di protezione dei dati l'adozione di un sistema basato sull'installazione di un'applicazione – contenente una funzionalità di localizzazione – sugli *smartphone* forniti in dotazione ai dipendenti impegnati all'esterno della sede aziendale. Il sistema era configurato per rilevare, a seguito dell'attivazione di apposito pulsante, l'orario e il luogo di "inizio e fine lavoro", "inizio pausa pranzo" e "inizio e fine di evento meteorologico di maltempo". Anche in questo caso l'applicazione era sviluppata da un soggetto terzo che però non aveva accesso ai dati raccolti.

Il Garante ha ritenuto lecito lo scopo prefisso, vale a dire la possibilità di effettuare con modalità automatiche (conformemente a quanto previsto dal contratto) il calcolo delle indennità di viaggio e trasferta o altri emolumenti, commisurato al luogo in cui l'attività lavorativa è stata effettuata oppure di acquisire elementi preordinati alla presentazione all'ente competente delle domande di cassa integrazione per impossibilità di svolgere la prestazione lavorativa in caso di particolari eventi meteorologici. Il trattamento è stato ritenuto lecito anche considerato che la società titolare del trattamento, in attuazione del cit. art. 4 dello Statuto dei lavoratori, ha stipulato un accordo con le rappresentanze sindacali. Sono state altresì ritenute conformi al principio di proporzionalità, pertinenza e non eccedenza la disattivazione del dispositivo al di fuori dell'orario di lavoro e nella pausa pranzo e la predisposizione del sistema in modo da non consentire la localizzazione geografica dei dispositivi al di fuori dei casi stabiliti.

Anche in questo caso sono state impartite misure ed accorgimenti a tutela degli interessati, come la necessità di configurare il sistema in modo da impedire il trattamento di dati ulteriori e non pertinenti rispetto alle finalità indicate (in particolare dei dati relativi al traffico telefonico, agli sms, alla posta elettronica, alla navigazione in internet). Il sistema deve altresì prevedere, anche quando l'applicazione lavora in *background*, la presenza di un'icona che indichi che la funzionalità di localizzazione è attiva (provv. 18 maggio 2016, n. 226, doc. web n. 5217175).

Uso di sistemi di localizzazione all'interno di una cd. scatola nera

Conformemente a quanto già deciso in casi analoghi (cfr. provv. 29 novembre 2012, n. 368, doc. web n. 2257616), il Garante in sede di verifica preliminare ha ammesso l'installazione di un dispositivo a bordo di veicoli che svolgono il servizio di trasporto pubblico locale, in grado di raccogliere una pluralità di dati quali la localizzazione geografica del veicolo, immagini mediante un sistema di videoregistrazione nonché alcuni altri dati quali la velocità, le accelerazioni e decelerazioni improvvise. I dati raccolti sono memorizzati per 72 ore (il tempo necessario ad effettuare le necessarie verifiche) ed eventualmente conservati solo in caso di eventi ritenuti rilevanti ossia i sinistri o l'attivazione del sistema di allarme da parte dell'autista, limitatamente ad un contenuto ambito temporale (20 secondi), immediatamente precedente e successivo al verificarsi dell'evento.

Nella descrizione della società richiedente le finalità del sistema consistevano nella ricostruzione della dinamica dei sinistri, nel rafforzamento della sicurezza di dipendenti, utenti e beni aziendali nonché nella razionalizzazione del servizio prestato, considerato che – sotto quest'ultimo profilo – il sistema avrebbe consentito di visualizzare gli itinerari percorsi dai mezzi.

Le finalità perseguite dal titolare con l'installazione del descritto sistema sono state ritenute dall'Autorità lecite, considerato anche che in applicazione dell'art. 4 dello Statuto, è stato raggiunto un accordo con le rappresentanze sindacali.

Anche in questo caso il Garante ha indicato al titolare la necessità di adottare misure ed accorgimenti a tutela dei diritti degli interessati ed, in particolare, misure tecniche idonee a non consentire l'identificazione di soggetti non coinvolti nei sinistri o negli altri eventi rilevanti in caso di comunicazione a terzi dei dati raccolti e ad anonimizzare – con contestuale adozione di modalità di utilizzo in forma aggregata – i dati relativi alla localizzazione geografica trattati allo scopo di razionalizzare il servizio di trasporto prestato (provv. 25 febbraio 2016, n. 78, doc. web n. 4807812).

14.2. *Il trattamento di dati personali dei dipendenti mediante dispositivi e posta elettronica*

Software di gestione dei servizi di rete e "strumenti di lavoro"

L'utilizzo dei servizi di comunicazione elettronica (internet, posta elettronica aziendale) – già oggetto, in termini generali, di specifiche linee guida del Garante (provv. 1° marzo 2007, linee guida per posta elettronica e internet, doc. web n. 1387522) – ha formato oggetto di verifica in relazione al trattamento posto in essere da un Ateneo italiano e avente ad oggetto *file* di *log*, MAC *Address (Media Access Control Address*), indirizzo IP nonché altre informazioni relative all'accesso ai servizi internet, alla posta elettronica e alle connessioni di rete, da parte di una pluralità di utenti (personale tecnico amministrativo, docenti, ricercatori e studenti). Tali informazioni, raccolte e conservate per un periodo di 5 anni, erano oggetto di ulteriori operazioni di trattamento per il tramite degli amministratori di sistema, quali, il monitoraggio e il filtraggio delle stesse. Contrariamente a quanto sostenuto dall'Ateneo, l'accertamento ha evidenziato che i dati raccolti erano chiaramente riconducibili ai singoli utenti, anche grazie al tracciamento puntuale degli indirizzi IP e dei MAC *Address* (identificativo *hardware*) dei computer assegnati ai dipendenti o in uso agli altri utenti abilitati, consentendo di risalire, anche indirettamente, alla postazione corrispondente e, quindi, all'utente che vi operava (cfr., Gruppo Art. 29, parere n. 4/2007 – WP 136 sul concetto di dato personale; sul carattere di dato personale del MAC *Address* stante la relativa univocità, cfr. Gruppo Art. 29, parere n. 13/2011 – WP 185 sui servizi di geolocalizzazione su dispositivi mobili intelligenti, spec. p. 11).

All'esito dell'accertamento l'Autorità ha dichiarato illecito il trattamento, con la conseguente inutilizzabilità dei dati trattati in violazione di legge (art. 11, comma 2 del Codice) e disposto il divieto dell'ulteriore trattamento su base individuale dei dati personali, salva la conservazione di quelli necessari ai fini della eventuale acquisizione da parte dell'autorità giudiziaria.

Il trattamento effettuato dall'Ateneo infatti è stato ritenuto in contrasto con i princìpi di necessità, pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. *a*) e *d*) del Codice) che non consentono controlli massivi, prolungati e indiscriminati, ma impongono di privilegiare soluzioni ispirate alla gradualità del monitoraggio e alla residualità di controlli. L'Ateneo non aveva poi reso la dovuta informativa in favore degli utilizzatori della rete, anche con riguardo alle effettive caratteristiche delle operazioni di trattamento effettuate (art. 13 del Codice), né a tal fine è risultato idoneo il regolamento interno sull'utilizzo degli strumenti elettronici.

Il descritto sistema era stato inoltre configurato con funzionalità tali da permettere operazioni di controllo dell'attività e dell'utilizzo dei servizi della rete effettuato da soggetti identificabili. Sotto questo profilo è stato accertato che il trattamento nei

14

confronti dei dipendenti dell'Ateneo era effettuato in violazione anche della disciplina sull'impiego di apparecchiature idonee al controllo a distanza dell'attività dei lavoratori (art. 4, l. n. 300/1970 e art. 114 del Codice).

Sotto quest'ultimo profilo, il provvedimento del Garante ha rappresentato la prima occasione in cui l'Autorità ha espresso il proprio orientamento sull'ambito di applicazione del comma 2 del citato art. 4 della l. n. 300/1970 quale risultante dalle modifiche intervenute per effetto dell'art. 23, d.lgs. n. 151/2015 (riforma del lavoro o *Jobs act*), mediante una possibile "perimetrazione" degli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", in presenza dei quali vengono meno talune garanzie per gli interessati sul piano lavoristico (la procedura di "concertazione" sindacale o l'equivalente autorizzazione dell'organo pubblico di controllo).

Il Garante, infatti (con ciò muovendosi nel solco di quanto già tracciato, seppure in termini più generali, dal Ministero del lavoro delle politiche sociali, con nota 18 giugno 2015), ha precisato che – con riferimento agli strumenti oggetto del provvedimento, vale a dire servizio di posta elettronica e navigazione web – possono ritenersi ricompresi nella predetta nozione solo "servizi, *software* o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza". A titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un *account* personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad es., sistemi di *logging* per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cd. *envelope* del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti-*virus* che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui *server* per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso).

Viceversa – ha concluso coerentemente il Garante- non possono considerarsi "strumenti di lavoro" nei termini anzidetti *software* che consentano, con modalità indipendenti e non percepibili dall'utente (cd. in *background*) e senza alcun impatto o interferenza sulla normale attività dell'utilizzatore, costanti operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" degli accessi a internet o al servizio di posta elettronica (provv. 13 luglio 2016, n. 303, doc. web n. 5408460).

Controlli sulla posta elettronica aziendale e su dispositivi *Blackberry* affidati ai dipendenti

All'esito di un procedimento seguito alla proposizione di un reclamo, il Garante ha disposto il divieto dei trattamenti di dati personali dei dipendenti effettuato da una società attraverso il servizio di posta elettronica aziendale (sia in costanza del rapporto di lavoro che successivamente alla sua interruzione) e tramite l'utilizzo dei dispositivi *Blackberry* affidati in dotazione ai dipendenti.

In particolare, l'Autorità ha ritenuto illecita la sistematica conservazione sul *server* aziendale dei dati esterni e dei contenuti delle comunicazioni elettroniche effettuate attraverso gli *account* di posta elettronica aziendali, peraltro per un periodo di tempo – dieci anni – ritenuto non conforme ai princìpi di necessità, pertinenza e non eccedenza in quanto non commisurato alle ordinarie necessità di gestione dei servizi di posta elettronica ivi comprese quelle di sicurezza dei sistemi. Tali dati, gestiti anche da un soggetto terzo in assenza di idoneo criterio di legittimazione, erano accessibili alla società nell'ambito di una procedura di *security investigation request*. È emerso che tale complessiva attività non era stata in alcun modo resa nota ai dipendenti, né attraverso informative individualizzate né tramite i documenti

relativi alle politiche aziendali in materia di utilizzo degli strumenti informatici, in contrasto con l'obbligo per il datore di lavoro di fornire una previa informativa ai dipendenti su tutti i trattamenti effettuati, anche in base al principio di correttezza. Inoltre tale trattamento consentiva alla società di effettuare il controllo dell'attività dei dipendenti in violazione della disciplina di settore (cfr. artt. 11, comma 1, lett. *a*) e 114 del Codice nonché art. 4, l. n. 300/1970). Tale disciplina, pure a seguito delle modifiche introdotte con il già citato articolo 23 del d.lgs. n. 151/2015, non consente l'effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore (v. linee guida per posta elettronica e internet, provv. 1° marzo 2007, n. 13, doc. web n. 1387522, spec. par. 4, 5.2. lett. *b*) e 6; si veda anche Consiglio di Europa, raccomandazione del 1° aprile 2015, CM/Rec(2015)5, spec. princ. 14). Inoltre, posto che la società permetteva – ragionevolmente – l'uso di *e-mail* a scopo privato, tali operazioni avrebbero consentito l'eventuale trattamento di dati "non rilevanti ai fini della valutazione dell'attitudine professionale" del dipendente nonché di dati sensibili, in violazione dell'art. 8 dello Statuto dei lavoratori e 10 del d.lgs. n. 276/2003.

È stata altresì ritenuta non conforme alle disposizioni in materia di protezione dei dati personali la procedura adottata dalla società consistente nel mantenere attive fino a sei mesi le caselle di posta elettronica aziendale dopo la cessazione del rapporto di lavoro. In base all'orientamento consolidato dell'Autorità, dopo la cessazione del rapporto gli *account* riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di meccanismi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del datore di lavoro (v. da ultimo provv. 30 luglio 2015, n. 456, doc. web n. 4298277).

Per quanto riguarda l'utilizzo dei dispositivi *Blackberry* è stata ritenuta illecita la possibilità per la società di accedere da remoto ai contenuti (anche di natura privata) presenti nel dispositivo nonché di raccogliere, conservare, comunicare a terzi e cancellare i dati. Ciò pur in presenza di un'informativa (che peraltro non menzionava la presenza di un'applicazione in grado di rilevare le soglie di consumo di ciascun utente), in quanto le descritte attività sono state ritenute non conformi ai princìpi di liceità (anche con riferimento ai già menzionati artt. 4 e 8, l. n. 300/1970 richiamati dagli artt. 113 e 114 del Codice), necessità, pertinenza e non eccedenza.

Il Garante ha infine invitato la società ad adottare di regola – a seguito dell'interruzione del rapporto di lavoro o di trasferimento del dipendente – procedure che consentano a quest'ultimo di partecipare alla ricognizione e, se del caso, alla consegna di documenti o di oggetti collocati all'interno degli uffici, soprattutto in caso di assegnazione individuale di spazi e postazioni (provv. 22 dicembre 2016, n. 547, doc. web n. 5958296).

14.3. *Pubblicità e trasparenza dei dati dei lavoratori*

Pubblicazione *online* di dati idonei a rivelare la condizione di disabilità

Nonostante la pregressa attività di sensibilizzazione del Garante, continuano a pervenire segnalazioni e notizie in tema di pubblicazione *online* sui siti istituzionali degli enti pubblici di dati, atti o provvedimenti contenenti dati personali riferiti a lavoratori. Il tema già oggetto di precedenti pronunce è stato nuovamente affrontato nel 2016 con specifico riguardo alla diffusione dei dati idonei a rivelare la condizione di disabilità o comunque idonee a rivelare lo stato di salute di lavoratori o partecipanti alle prove concorsuali, a volte nell'ambito di procedure selettive "riservate" ai sensi della l. n. 68/1999. Nella maggior parte dei casi, i dati erano conte-

nuti in graduatorie o altri atti, reperibili in rete tramite motori di ricerca generalisti, che recavano in chiaro i dati identificativi delle persone. In applicazione dell'art. 22, comma 8, del Codice, a seguito delle necessarie verifiche, è stata dichiarata l'illiceità della diffusione di dati sulla salute dei soggetti interessati analogamente a qualsiasi riferimento alla condizioni di invalidità, disabilità o handicap fisici e/o psichici – in qualche caso anche altre informazioni eccedenti (ad es., il codice fiscale) – disponendo il divieto dell'ulteriore diffusione in internet e prescrivendo ai titolari del trattamento (in prevalenza province e comuni) l'adozione di idonei accorgimenti nelle operazioni di trattamento funzionali alla pubblicazione di tali atti e attivando i conseguenti procedimenti sanzionatori sul piano amministrativo (cfr., anche, linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, adottate con provv. 15 maggio 2014, n. 243, doc. web n. 3134436, parte II, punti 1 e 3.b.) (provv. ti 4 febbraio 2016, nn. 35 e 36, doc. web nn. 4727305 e 4912481; provv. 1° giugno 2016, n. 244, doc. web n. 5260571).

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

Trattamento di dati giudiziari di personale operante nei contesti educativi

Nel corso dell'anno il Garante si è pronunciato su trattamenti di dati personali nella gestione del rapporto di lavoro, affrontando in particolare il tema del trattamento di dati giudiziari del personale da parte del datore di lavoro al fine di accertare il possesso di requisiti dei dipendenti per l'accesso a particolari impieghi o mansioni; ciò con riguardo ad una società di gestione di asili nido che aveva chiesto, anche in vista di future assunzioni, di poter essere autorizzata ad acquisire in via periodica (con cadenza biennale) il certificato penale del casellario ed il certificato dei carichi pendenti degli interessati. Nel caso esaminato il Garante non ha ritenuto sussistenti i presupposti per autorizzare, ai sensi dell'art. 41 del Codice, il trattamento dei dati giudiziari dei dipendenti a contatto con i minori (educatori, coordinatori, cuochi ed ausiliari) presso gli asili nido gestiti dalla società istante.

Premesso che in base alla disciplina in materia di protezione dei dati personali, i soggetti privati possono trattare i dati giudiziari soltanto se autorizzati da espressa disposizione di legge o da provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 27 del Codice), il Garante non ha ritenuto sussistenti i presupposti per emanare un'autorizzazione specifica nei confronti della società richiedente. La materia è infatti disciplinata dall'art. 25-*bis*, d.P.R. 14 novembre 2002, n. 313 (disposizione introdotta dall'art. 2, d.lgs. 4 marzo 2014, n. 39, in attuazione della direttiva 2011/93/UE, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, ma v. già, decisione quadro 2004/68/GAI) che ha stabilito presupposti, limiti e condizioni, sul piano oggettivo e soggettivo, per l'acquisizione del pertinente certificato del casellario giudiziale da parte di chi intenda impiegare una persona per lo svolgimento di attività professionali che comportino contatti diretti e regolari con minori, al fine di verificare l'esistenza di condanne per fattispecie di reati indicate tassativamente dalla legge (sul punto, Ministero della giustizia, circolari 3 aprile 2014 e 24 luglio 2014 e note di chiarimento disponibili su www.giustizia.it; Ministero del lavoro e delle politiche sociali, circolare n. 9 dell'11 aprile 2014 e interpelli n. 25 del 15 settembre 2014 e n. 22 del 24 settembre 2015 nonché nota del 13 gennaio 2016, prot. 29/0000115/P).

Nel corso dell'istruttoria non sono state peraltro rappresentate, né sono emerse, circostanze particolari o situazioni eccezionali tali da consentire un trattamento difforme o ulteriore rispetto a quanto previsto dalla normativa di settore e da quanto già consentito dall'autorizzazione generale del Garante n. 7 (con riguardo al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici), né è stato ritenuto ammissibile individuare, in contrasto con la normativa vigente, ipotesi di accesso diretto ai predetti dati giudiziari non previste dalla citata disciplina in materia di casellario giudiziale (d.P.R. n. 313/2002) (provv. 15 dicembre 2016, n. 533, doc. web n. 5971199).

14.5. *Il trattamento di dati sulla salute del personale navigante da parte del "medico competente" del vettore aereo*

Nel corso dell'anno di riferimento il Garante, nell'esprimere il proprio avviso su un quesito del Ministero della salute, ha approfondito, per i profili di più diretto impatto sulla disciplina di protezione dei dati, la materia dei livelli di sicurezza del traffico aereo, anche alla luce del quadro normativo sovranazionale. Il Garante ha espresso il proprio avviso sul tema della comunicazione al medico competente di un vettore aereo nell'ambito dello svolgimento dei propri compiti in materia di igiene e sicurezza del lavoro (cd. sorveglianza sanitaria, art. 41, d.lgs. n. 81/2008), di dati relativi alla salute del personale navigante legittimamente trattati nell'ambito del procedimento per il rilascio delle licenze aeronautiche per l'aviazione civile dai soggetti pubblici istituzionalmente preposti alla verifica dei requisiti psico-fisici (AeMC, *aeronautical medical centre* che in Italia sono svolte dai competenti uffici dell'Aeronautica militare -IMAS e del Ministero della salute - SASN). Il Dicastero aveva formulato una richiesta circa la liceità della messa a disposizione in favore del medico competente operante presso un vettore aereo di documentazione sanitaria contenente informazioni relative alle limitazioni della licenza di volo dei piloti (segnatamente "il giudizio di non idoneità o di limitazione dell'idoneità al volo e ai privilegi della licenza"). Lo studio è stato condotto anche alla luce dei riscontri fatti pervenire dagli altri Stati membri interpellati sul tema e dei contributi tecnici di organismi che operano nel settore dell'aviazione civile a livello europeo (EASA, *Task force on measures following the accident of German Wings flight 9525- Final repor*t; EASA, *Action plan for the implementation of the Germanwings Task Force recommendations*. *Version 1 – 7 October* 2015; BEA, *Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, Rapport Final, Accident survenu le 24 mars 2015à Prads-Haute-Bléone (04) à l'Airbus A320-211, immatriculé D-AIPXexploité par Germanwings*- 13 marzo 2016).

A seguito di una valutazione del complessivo trattamento prospettato alla luce dell'articolata normativa che disciplina la materia sotto il profilo dell'accrescimento dei livelli di sicurezza del traffico aereo, è emerso che il quadro normativo di riferimento consentirebbe ai Servizi assistenza sanitaria ai naviganti (SANS) del Ministero della salute di comunicare gli esiti delle visite mediche - da loro effettuate in qualità di AeMC - all'Enac, in qualità di "autorità competente" e organo di controllo del settore aeronautico sotto la vigilanza dell'EASA (*European Aviation Safety Agency*), non invece ai datori di lavoro operanti nel settore della aeronavigazione (regolamento (UE) n. 290/2012, Allegato IV, ARA.MED.150 e regolamento Enac "Organizzazione sanitaria e certificazioni mediche d'idoneità per il conseguimento delle licenze e degli attestati aeronautici" Edizione 3-4 maggio 2015).

Al trattamento dei dati idonei a rivelare lo stato di salute delle persone (art. 4,

14

comma 1, lett. *d*), del Codice) trovano anzitutto applicazione gli artt. 3, 11, 20 e, con specifico riguardo al trattamento da parte di soggetti privati, l'art. 26 del Codice e dall'autorizzazione generale del Garante n. 1, con riguardo ai trattamenti strettamente correlati all'adempimento di specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria connessi alla gestione del rapporto di lavoro ivi compresi quelli in materia di igiene e sicurezza del lavoro (artt. 25 e 41 ss, d.lgs. n. 81/2008, cit.; autorizzazione generale n. 1 punto 1, lett. *c*), punto 3 e punto 4, lett. *c*).

In tale quadro il Garante ha ritenuto che le finalità di tutela della sicurezza dei voli e della salvaguardia della vita e dell'incolumità della collettività rispondano ad un interesse pubblico rilevante al quale concorrono sia gli accertamenti sanitari, a carico del Ssn, necessari per il rilascio delle licenze nell'ambito del sistema pubblicistico di verifica dell'idoneità al volo dei piloti o aspiranti tali, sia gli adempimenti di sorveglianza sanitaria, obbligatoriamente posti in essere dal datore di lavoro per il tramite del medico competente, volti a verificare l'idoneità del pilota alla "*mansione specifica*" (artt. 11, comma 1 lett. *a*) e *b*), 20, comma 1, e 85, comma 1, lett. *a*), *d*) ed *e*), del Codice; regolamento (UE) n. 1178/2011; d.lgs. 25 luglio 1997, n. 250, istitutivo dell'Enac). Tuttavia il Garante ha precisato che allo stato della normativa vigente, non risulta ammissibile un flusso di dati sanitari dei piloti dai competenti organismi pubblici in favore del medico operante presso i vettori aerei, né la consultazione da parte dello stesso delle medesime informazioni eventualmente disponibili in banche dati. Nel richiamare l'attenzione sull'opportunità di integrare il quadro normativo vigente, il Garante si è riservato la facoltà di esprimere le valutazioni di competenza sulle eventuali future disposizioni regolamentari (artt. 20, comma 2 e 154, commi 1, lett. *g*), e 4 del Codice) (provv. 27 aprile 2016, n. 194, doc. web n. 5149198).