GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2017

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771
email: garante@gpdp.it
www.garanteprivacy.it

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

13.1. *Protezione dei dati personali e rapporto di lavoro*

Una volta completata ed applicata a pieno regime la riforma del mercato del lavoro (cd. *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 dei dati personali (d.lgs. nn. 150/2015 e 151/2015), anche nel 2017 sono stati portati all'attenzione dell'Autorità diversi casi di trattamenti di dati effettuati nell'ambito del rapporto di lavoro rispetto ai quali ha trovato applicazione la nuova disciplina dei controlli a distanza della prestazione lavorativa (art. 4, l. n. 300/1970, come modificato dall'art. 23, d.lgs. n. 151 cit.).

In tali occasioni il Garante ha avuto modo di affrontare alcuni aspetti meritevoli di attenzione sul piano interpretativo ed applicativo, approfondendo l'impatto della predetta disciplina lavoristica sulle garanzie e sui diritti previsti dalla normativa in materia di protezione dei dati personali, al fine di individuare il corretto bilanciamento fra i diversi interessi in campo.

Già nel 2016 l'Autorità, in un provvedimento adottato nei confronti di un ateneo, aveva espresso il proprio orientamento sull'ambito di applicazione del comma 2 del predetto art. 4 dello Statuto dei lavoratori 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 (provv. 13 luglio 2016, n. 303, doc. web n. 5408460; cfr. Relazione 2016, p. 100). In questo ambito – e, più in generale, sul rapporto fra disciplina lavoristica in materia di controlli a distanza e garanzie poste a protezione dei dati personali dei lavoratori – il Garante è intervenuto anche nel periodo di riferimento, tenendo conto della specificità dei trattamenti e degli strumenti utilizzati in concreto dal datore di lavoro dai quali è risultato "indirettamente" il controllo dell'attività lavorativa.

Ciò è avvenuto prevalentemente rispetto a trattamenti di dati personali effettuati attraverso sistemi che consentono la localizzazione geografica dei dipendenti; l'installazione di dispositivi tecnologici dotati di tale funzionalità (ormai agevolmente reperibili sul mercato, a costi contenuti, pure attraverso la fornitura dei relativi servizi da parte di società specializzate) ha costituito infatti l'oggetto di una quota significativa dell'attività dell'Autorità in materia di trattamenti in ambito lavorativo, sia in sede di decisione di istanze di verifica preliminare sia con riferimento alla definizione di casi oggetto di reclami e/o segnalazioni nonché all'esito di accertamenti ispettivi disposti anche d'ufficio.

Il Garante è altresì intervenuto in merito al trattamento di dati biometrici dei lavoratori (cfr. par. 13.5), come pure in tema di videosorveglianza (cfr. par. 13.4).

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. 13.6) o di dati sanitari (cfr. par. 13.7).

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

Nel corso dell'anno di riferimento il Garante ha valutato le finalità e le concrete modalità di funzionamento dei sistemi di geolocalizzazione portati alla sua attenzio-

13

ne alla luce dell'aggiornato quadro normativo in materia di controlli a distanza, la cui osservanza costituisce condizione di liceità del trattamento dei dati personali (art. 4, l. n. 300/1970; artt. 11, comma 1, lett. *a*), e 114 del Codice). In relazione alla peculiarità di ciascun sistema tecnologico l'Autorità si è pronunciata sulla configurazione dello stesso quale strumento "dal quale derivi anche la possibilità di controllo a distanza" oppure quale strumento "utilizzat[o] dal lavoratore per rendere la prestazione lavorativa", con conseguente applicazione, rispettivamente, del comma 1 o 2 del menzionato art. 4 e quindi dell'obbligo o meno di attivare la procedura di garanzia ivi prevista.

Sotto tale ultimo profilo, in alcune decisioni il Garante ha ritenuto determinati sistemi non "direttamente preordinati all'esecuzione della prestazione lavorativa", con conseguente applicazione dell'art. 4, comma 1.

Al riguardo anche l'Ispettorato nazionale del lavoro, con circolare n. 2/2016, 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 dell'Ispettorato nazionale del lavoro".

Localizzazione dei veicoli per finalità di gestione, coordinamento e rendicontazione

Venendo ora ai singoli casi decisi, il Garante, con provvedimento reso in sede di verifica preliminare richiesta da una società che eroga servizi di fornitura di acqua potabile nonché di raccolta e trattamento delle acque reflue, ha precisato le condizioni di liceità del trattamento di dati di localizzazione dei veicoli aziendali, già oggetto del provvedimento di carattere generale del 4 ottobre 2011, n. 370 (provv. 16 marzo 2017, n. 138, doc. web n. 6275314).

Le finalità perseguite dal sistema sono risultate preordinate ad una pluralità di scopi, in particolare alla ottimizzazione della gestione delle attività aziendali in occasione di richieste di intervento o emergenze (conformemente ai livelli di garanzia e qualità delle prestazioni indicati dalla Carta dei servizi); all'innalzamento delle condizioni di sicurezza sul lavoro nonché della protezione della flotta aziendale in caso di furto; alla più efficiente programmazione delle attività sul territorio e degli interventi di manutenzione dei veicoli; all'effettiva commisurazione del tempo di lavoro; alla gestione di eventuali sinistri; alla gestione delle contestazioni di violazione amministrativa di disposizioni del codice della strada. Alla luce di tali finalità nonché delle modalità di funzionamento dei dispositivi, l'Autorità ha innanzitutto ritenuto il sistema di localizzazione dei veicoli non "direttamente preordinato all'esecuzione della prestazione lavorativa", con conseguente applicazione dell'art. 4, comma 1, l. n. 300/1970 (richiamato dall'art. 114 del Codice); in questa prospettiva i trattamenti sono stati ritenuti leciti, considerato altresì che la società aveva provveduto a stipulare accordi con le rappresentanze sindacali conformemente alla menzionata disciplina di settore in materia di controlli a distanza. Tuttavia, come misure a tutela dei diritti e delle libertà degli interessati, è stato prescritto alla società di configurare il sistema in modo da rilevare la posizione geografica con una cadenza temporale strettamente proporzionata alle finalità perseguite e in modo da consentire la conservazione dei dati trattati esclusivamente nelle ipotesi e con le modalità indicate in concreto nel provvedimento, in applicazione dei principi di protezione dei dati, distintamente per ciascuna finalità. Inoltre è stato precisato che il sistema deve essere configurato in modo da consentire l'accesso ai dati trattati esclusivamente al personale incaricato, al quale devono essere assegnate credenziali di autenticazione differenziate, individuando profili autorizzativi personalizzati e limitando quanto più possibile l'assegnazione di profili con funzionalità di modifica ed estrazione dei dati.

È stato altresì prescritto di adottare misure preordinate alla cancellazione automatica dei dati dopo la decorrenza degli eventuali termini di conservazione nonché di predisporre misure organizzative e tecnologiche volte ad anonimizzare i dati raccolti qualora ulteriormente utilizzati per finalità statistiche e di programmazione.

Con riferimento alla conservazione dei dati trattati, ove prevista, limitata ai dati strettamente necessari al perseguimento delle finalità perseguite, l'Autorità ha chiarito che "è in particolare escluso il monitoraggio dei tracciati percorsi".

All'esito della valutazione circa la liceità del trattamento, la sussistenza delle garanzie previste della disciplina sui controlli a distanza e le complessive caratteristiche del sistema (come sopra sommariamente riportate), il Garante ha individuato con il menzionato provvedimento, alla luce della disciplina sul cd. bilanciamento di interessi, un legittimo interesse del titolare al trattamento ai sensi dell'art. 24, comma 1, lett. *g*), del Codice.

Nell'ambito di una verifica preliminare presentata dal servizio di polizia locale di un comune, relativa alla prospettata installazione di un sistema di localizzazione satellitare sui veicoli e sulle radio ricetrasmittenti affidate al personale che svolge attività di polizia municipale e amministrativa anche per conto di tre comuni limitrofi, il Garante ha ritenuto lecite e coerenti con lo svolgimento delle funzioni istituzionali attribuite dall'ordinamento all'ente locale, le finalità di coordinamento e gestione di eventuali emergenze perseguite dal sistema attraverso la consultazione delle informazioni sulla posizione geografica di veicoli e dispositivi da parte del personale autorizzato addetto alla centrale operativa (provv. 19 ottobre 2017, n. 432, doc. web n. 7321142).

Parimenti lecito è stato ritenuto lo scopo di consentire la raccolta dei dati necessari alla rendicontazione delle attività effettuate dalle pattuglie nelle diverse aree comunali in vista della ripartizione tra i comuni dei costi sostenuti. Sotto il profilo della liceità, poi, anche in questo caso è stata ritenuta conforme alla disciplina in materia di controlli a distanza la preannunciata attivazione da parte del comune della procedura di garanzia prevista dall'art. 4, comma 1, l. n. 300/1970.

Quanto alla valutazione circa la necessità e proporzionalità delle modalità del prospettato trattamento, l'Autorità ha ritenuto conforme ai suindicati principi la possibilità di visualizzare in tempo reale sui *monitor* della sala operativa – da parte del responsabile del servizio (o di un suo delegato) – i dati raccolti in modo da non consentire la diretta identificazione degli operatori. Solo in caso di necessità il personale autorizzato potrà identificare e contattare i singoli operatori attraverso il raffronto con il registro cartaceo dei turni di servizio. Tale registro viene distrutto prima dell'inizio del nuovo turno, posto che in relazione agli scopi dell'ulteriore conservazione (consuntivazione dei costi relativi alle attività effettuate) non è necessaria (né comunque utile) l'identificazione degli operatori. Da ultimo si rileva che il Garante, in considerazione della assoluta peculiarità dell'attività svolta dalla polizia locale, ha ritenuto la periodizzazione temporale della posizione geografica effettuata dal sistema (pari a due rilevamenti al minuto) non in contrasto con il principio di proporzionalità.

In un altro caso, a seguito di istanza di verifica preliminare presentata da un gestore per conto di vari committenti (comuni o consorzi di comuni) dei servizi di igiene urbana (raccolta differenziata e trasporto rifiuti solidi urbani), ha formato oggetto di esame un sistema radiomobile digitale (dispositivi portatili e veicolari installati sulla flotta impiegata nel servizio erogato dalla società) per le comunicazioni del personale operativo (provv. 24 maggio 2017, n. 247, doc. web n. 6495708). Il Garante ha ritenuto che le finalità perseguite con il menzionato sistema, tra le quali l'ottimizzazione della gestione, il coordinamento e la sicurezza delle risorse sul

territorio, nonché la razionalizzazione del servizio in termini di copertura delle aree oggetto di intervento, fossero riconducibili alle "esigenze organizzative e produttive, per la sicurezza del lavoro e per tutela del patrimonio aziendale" in presenza delle quali la disciplina di settore in materia di controlli a distanza consente l'installazione di siffatti sistemi (artt. 11, comma 1, lett. *a*), e 114 del Codice nonché art. 4, comma 1, l. n. 300/1970).

In tale quadro è stata ritenuta correttamente attivata la procedura per l'acquisizione della specifica autorizzazione da parte della Direzione territoriale del lavoro competente (sul punto v. pure Ispettorato nazionale del lavoro, circolare n. 2/2016, ma già, seppur con riguardo al quadro normativo previgente, provv. 4 ottobre 2011, cit., punti 2.2. e 2.3). Sebbene infatti i dati di localizzazione del veicolo non fossero associati immediatamente ai lavoratori interessati, il datore di lavoro era in condizione di risalire alla loro identità (essendo ciascuno di essi, di volta in volta, assegnatario dei dispositivi e del veicolo nel quale gli stessi erano installati), ricostruendone così, anche indirettamente, l'attività (art. 4, comma 1, lett. *b*), del Codice; cfr., in proposito, provv. 4 ottobre 2011, cit., punto 1; parere n. 5/2005 del 5 novembre 2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto del Gruppo Art. 29, WP 115, p. 10; v. altresì parere n. 4/2007 sul concetto di dati personali, WP 136, p. 11).

Accanto al predetto sistema di geolocalizzazione la società intendeva inoltre implementare un "sistema di predisposizione turni" – configurato in modo da consentire, per ogni specifico servizio, l'assegnazione dei dispositivi (veicolari o mobili) ai dipendenti identificati nominativamente. Sebbene il sistema di geolocalizzazione non fosse idoneo a consentire un'associazione diretta tra le coordinate geografiche e i singoli operatori, la società poteva comunque associare i dipendenti ad un particolare dispositivo veicolare, per il tramite delle direzioni competenti, confrontando manualmente i *report* prodotti dai rispettivi sistemi, pur logicamente separati. La società aveva inoltre rappresentato l'intenzione di utilizzare tutti i dati, già raccolti ai sensi dell'art. 4, comma 1, l. n. 300/1970, e contenuti nei due distinti sistemi (rispettivamente quello di geolocalizzazione e quello di predisposizione dei turni), al fine di analizzarli per la risoluzione di eventuali "anomalie" nell'ambito della copertura del servizio e "a tutti i fini connessi al rapporto di lavoro".

Il Garante, nel rendere una prima applicazione della disposizione normativa di cui all'art. 4, comma 3, l. n. 300/1970, ha chiarito che anche tali ulteriori operazioni di trattamento devono essere effettuate nel rigoroso rispetto, sia della disciplina di protezione dei dati che di quella in materia di controlli a distanza. Sotto questo profilo, pertanto, è stato precisato che l'identificazione degli interessati può avvenire "solo in caso di necessità", "per scopi determinati, espliciti e legittimi" e a condizione che i dati siano utilizzabili "in altre operazioni di trattamento in termini compatibili con tali scopi", il trattamento ulteriore avvenga solo a fronte della concreta ricorrenza delle "anomalie", siano state predeterminate e rese note ai lavoratori unitamente alle modalità con le quali la società si riserva di trattare i dati e venga fornito agli interessati ogni informazione necessaria ad assicurare la piena consapevolezza dei trattamenti ulteriori che il datore di lavoro si riserva di effettuare e degli strumenti utilizzati (artt. 13 del Codice e 4, comma 3, l. n. 300/1970). Tali trattamenti potranno essere effettuati nei limiti della disponibilità dei dati personali trattati dal sistema di geolocalizzazione (in particolare, le coordinate geografiche ed il codice del dispositivo) in base a tempi di conservazione commisurati per il periodo strettamente necessario alla specifica finalità di consuntivazione del servizio.

Nel richiamare i propri consolidati orientamenti, il Garante ha ribadito che ogni operazione di trattamento ulteriore, ancorché effettuata nell'ambito della gestione

del rapporto contrattuale con il lavoratore e nell'esercizio del potere di verifica dell'effettivo adempimento della prestazione (artt. 2086, 2087 e 2104 c.c.), deve essere ispirata alla liceità, proporzionalità e gradualità nel trattamento dei dati evitando interferenze ingiustificate nella sfera privata dei lavoratori, pena l'inutilizzabilità dei dati stessi (art. 11, comma 2, del Codice; cfr. punto 5, provv. 13 luglio 2016, n. 303, doc. web n. 5408460; ancorché con riferimento al quadro normativo previgente, con riguardo alla non utilizzabilità del dato sulla geolocalizzazione acquisito in violazione di legge, v. Cass. civ., sez. lav., n. 19922/2016).

Il Garante ha prescritto alcune misure a tutela dei diritti e delle libertà degli interessati: in particolare che le interrogazioni di ambedue i sistemi siano consentite solo a un numero ridotto di incaricati operanti presso le competenti unità organizzative, i quali devono essere identificati mediante specifiche credenziali di autenticazione; che le interrogazioni dei due sistemi siano registrate, tramite un apposito *file* di *log* (riportante la data e l'ora dell'operazione, l'operazione effettuata, i codici dei dispositivi/veicoli visualizzati, l'identificativo dell'incaricato) nel rispetto del provvedimento del Garante del 27 novembre 2008 sugli amministratori di sistema; che il sistema venga configurato in modo da consentire la conservazione dei dati trattati in applicazione dei principi di protezione dei dati, distintamente per ciascuna finalità. In particolare, è stato prescritto di anonimizzare i *report* destinati ad essere messi nella disponibilità rispettivamente dell'ufficio turni (per la finalità di pianificazione dei turni e l'assegnazione delle priorità del servizio da parte del personale) e dell'ente affidatario del servizio (per la finalità di consuntivazione del servizio) in modo che in essi non ricorrano dati che siano, anche indirettamente, riconducibili agli interessati (ad es., codice veicolo, sul punto, provv. 2 ottobre 2014, n. 434, doc. web n. 3534543). I dati dei percorsi storicizzati potranno essere conservati, come richiesto nei capitolati tecnici per l'affidamento del servizio, solo se le informazioni relative alla localizzazione per l'intera flotta utilizzata siano state opportunamente anonimizzate (artt. 3 e 11, comma 1, lett. *e*), del Codice; e punto 3, provv. 4 ottobre 2011, cit.). Con riferimento alla frequenza della rilevazione dei dati di geolocalizzazione, il Garante ha prescritto, in sostituzione delle due rilevazioni al minuto prospettate dalla società, che il sistema sia configurato in modo che la rilevazione del dato di geolocalizzazione avvenga nel momento in cui l'automezzo giunge in prossimità di punti di raccolta predeterminati e precedentemente georeferenziati (cd. rilevazione ad eventi) per scongiurare il monitoraggio continuo della posizione del veicolo (artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice; sul punto, raccomandazione del 1° aprile 2015, CM/Rec(2015)5, sul trattamento di dati personali nel contesto occupazionale, par. 16; ma v. già Gruppo Art. 29, parere n. 13, 16 maggio 2011, sui servizi di geolocalizzazione su dispositivi mobili intelligenti, WP 185, p. 15 e, in senso analogo, punto 3, provv. 4 ottobre 2011, cit.). È stato inoltre prescritto che solo in presenza di predeterminate anomalie nella gestione di un servizio la società potrà prevedere l'attivazione della rilevazione in tempo reale della posizione geografica del mezzo quando quest'ultimo dovesse effettuare una sosta superiore a un tempo massimo individuato dalla società e comunque non inferiore a cinque minuti.

Localizzazione di *smartphone* o *tablet* in uso ai dipendenti

Il Garante ha autorizzato, nell'ambito di un procedimento di verifica preliminare avviato da una società, l'installazione di un sistema tecnologico completo di funzionalità di localizzazione geografica di dispositivi *smartphone* e *tablet* preordinato al miglioramento dell'efficacia della certificazione ai clienti dei risultati di un servizio di controllo sulla qualità della distribuzione di materiale pubblicitario all'interno delle cassette postali (es. volantini, *depliant* commerciali, etc.) (provv. 30 novembre 2017, n. 505, doc. web n. 7522639).

Anche in questo caso, alla luce delle finalità perseguite dalla società e delle concrete modalità del trattamento prospettato, l'Autorità ha ritenuto che il sistema deve ritenersi "non direttamente preordinato all'esecuzione della prestazione lavorativa", con conseguente applicazione dell'art. 4, comma 1, l. n. 300/1970. Sotto tale profilo il complessivo trattamento è stato ritenuto lecito considerato che la società aveva dichiarato di voler attivare la procedura di garanzia prevista dalla menzionata disciplina di settore in materia di controlli a distanza.

L'Autorità ha in particolare valutato positivamente le concrete caratteristiche del sistema alla luce dei principi di necessità e proporzionalità. Si segnala in particolare la prevista pseudonimizzazione dei dati del dipendente addetto al controllo di qualità e la scelta di configurare la rilevazione della posizione geografica del dispositivo non in base ad un intervallo temporale predeterminato bensì all'esito del comportamento attivo del dipendente/*controller* e solo nell'ambito temporale di riferimento della specifica attività programmata nel turno di lavoro. Inoltre ciascun supervisore potrà accedere al sistema esclusivamente per finalità di gestione, coordinamento e migliore organizzazione dell'attività e i rapporti consegnati ai clienti circa i risultati dell'attività svolta non potranno contenere dati identificativi dei dipendenti/*controller*, conformemente a quanto già affermato dall'Autorità (v. provv. 2 ottobre 2014, n. 434). I tempi di conservazione dei dati raccolti, individuati alla luce dei tempi medi di gestione di eventuali contestazioni da parte dei clienti (in dieci giorni), sono stati ritenuti conformi ai principi di necessità e proporzionalità.

All'esito della valutazione circa la liceità del trattamento, la sussistenza delle garanzie previste della disciplina sui controlli a distanza, le complessive caratteristiche del sistema (come in sintesi riportate), il Garante ha individuato, alla luce della disciplina sul cd. bilanciamento di interessi (ai sensi dell'art. 24, comma 1, lett. *g*), del Codice), un legittimo interesse del titolare al trattamento dei dati.

L'Autorità ha tuttavia prescritto l'adozione di specifiche misure volte ad impedire l'eventuale trattamento di dati presenti sui dispositivi non afferenti all'attività lavorativa e comunque privati, quali quelli tratti dalla posta elettronica o dalla navigazione in internet o relativi al traffico telefonico, considerato anche che la società intende consentire ai dipendenti l'uso dei dispositivi aziendali anche per fini personali. Sui dispositivi, infine, dovrà essere visualizzata un'icona per tutto il tempo in cui la funzionalità di localizzazione è attiva.

13.3. *Il trattamento dei dati personali mediante "altri strumenti": un sistema di gestione delle attese allo sportello*

Il Garante ha assunto un'altra importante decisione all'esito dell'esame di numerose segnalazioni e reclami da parte di organizzazioni sindacali e dipendenti nei confronti di un gestore del servizio postale con riguardo ad un sistema utilizzato per la gestione delle attese allo sportello (provv. 16 novembre 2017, n. 479, doc. web n. 7355533).

Il sistema consentiva al datore di lavoro, in qualità di titolare del trattamento per il tramite del personale abilitato e incaricato con diversi profili di accesso al sistema, operazioni di trattamento di dati, anche su base individuale, riferiti ai lavoratori addetti allo sportello. Il sistema consentiva la visualizzazione di dati identificativi dell'operatore, sia sui *display* collocati su ogni singola postazione di sportello dell'ufficio postale, sia su una *console* di monitoraggio, che rendeva possibile una consultazione in tempo reale (e in alcuni casi continuativa) anche di altre informazioni di dettaglio (ad es., disponibilità dello sportello e tempo medio di evasione dei *ticket*

serviti associati in via diretta al nominativo dell'operatore). Era inoltre effettuata la memorizzazione dei dati anche identificativi dell'operatore (nominativo) con possibilità di estrazione di reportistica.

L'Autorità ha attivato una complessa attività istruttoria che ha messo in evidenza alcuni profili di violazione della disciplina di protezione dei dati personali. In particolare è stato rilevato che la società non aveva reso ai dipendenti la dovuta informativa circa modalità e finalità delle operazioni di trattamento rese possibili dal sistema né all'interno delle informative individualizzate né con documenti informativi resi noti alla generalità dei dipendenti. La società si era limitata, infatti, a trasmettere una "documentazione descrittiva" alle sole organizzazioni sindacali che non recava gli elementi essenziali richiesti dalla legge (art. 13 del Codice).

Con il provvedimento che ha definito il procedimento il Garante ha ribadito che l'informativa ai sensi dell'art. 13 è dovuta indipendentemente dalla eventuale determinazione del titolare del trattamento di voler riservarsi di utilizzare le informazioni raccolte "a tutti i fini connessi al rapporto di lavoro" e che inoltre tali eventuali e successive operazioni di trattamento presuppongono il rigoroso rispetto della disciplina di protezione dei dati e di quella di settore in materia di controlli a distanza (provv. 24 maggio 2017, n. 247, doc. web n. 6495708, punto 5.3). Alla luce delle accertate caratteristiche, il Garante ha ritenuto il sistema non indispensabile all'operatore per rendere la prestazione lavorativa, "collocandolo" così fra quegli strumenti, anche organizzativi, dai quali può indirettamente derivare il controllo a distanza dell'attività dei lavoratori, con conseguente necessità di attivare le procedure concertativo/amministrative previste dalla legge (art. 4, comma 1, l. n. 300/1970 rispetto al comma 2; cfr. sul punto anche provv. 13 luglio 2016, n. 303, punto 4.3, doc. web n. 5408460).

Tali condizioni di garanzia, che costituiscono il presupposto di liceità del trattamento, non possono essere soddisfatte, come avvenuto nel caso di specie, con l'invio alle organizzazioni sindacali di un mero documento informativo o dall'eventuale acquiescenza dei lavoratori (cfr. Cass., III sez. pen., n. 22148/2017; sul punto, tra i tanti, provv. 8 maggio 2014, n. 230, doc. web n. 3250490). Pertanto, il trattamento che sarebbe derivato dal sistema in parola è stato ritenuto, anche sotto tale profilo, in contrasto con la disciplina in materia di protezione dei dati personali e con la rilevante disciplina di settore. Inoltre, alcune funzionalità del sistema, in particolare la possibilità in capo a specifiche funzioni aziendali, anche a livello centrale, di accedere in tempo reale e in via continuativa ai dati su base individuale relativi a tutte le postazioni e a tutti gli operatori in servizio in un dato momento presso un determinato ufficio, seppur nell'ambito di un'area territoriale definita, sono state ritenute non conformi ai principi di necessità, pertinenza e non eccedenza rispetto alle finalità "organizzative e produttive", "di sicurezza del lavoro" e "di tutela del patrimonio aziendale" consentite dalla richiamata disciplina di settore. Sotto questo profilo, il monitoraggio costante dell'attività e della produttività del lavoratore reso possibile dal sistema è stato ritenuto illecito (artt. 3, 11, comma 1, lett. *d*), del Codice e art. 4, l. n. 300/1970; raccomandazione Consiglio di Europa 1° aprile 2015, CM/Rec(2015)5, princ. 15; provv.ti 22 dicembre 2016, n. 547, par. 3.5, doc. web n. 5958296 e 13 luglio 2016, n. 303, par. 5, cit.).

Per tali ragioni il Garante ha disposto il divieto del trattamento con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2 del Codice.

Con riguardo, invece, alla visualizzazione del nome di battesimo o dello pseudonimo del lavoratore sul *display*, quale diversa ed ulteriore misura rispetto a quella, peraltro già in uso per il personale operante a contatto con il pubblico, consistente

nell'apposizione del cartellino identificativo, il Garante ha ritenuto che la possibilità di raggiungere gli stessi legittimi obiettivi nei rapporti con i clienti con modalità diverse da quelle in uso potrà essere valutata, anche in alternativa al cartellino, previa idonea informativa ai lavoratori interessati, avuto riguardo, nel rispetto del principio di proporzionalità, alle dimensioni della struttura, al numero degli operatori che vi prestano servizio, alle mansioni svolte da ciascuno, al bacino di utenza del singolo ufficio postale, valutando l'opportunità di una rideterminazione dell'arco temporale di esposizione del nominativo dell'operatore.

13.4. *Il trattamento di dati personali mediante sistemi di videosorveglianza all'interno di aree particolari con rilevazione dell'audio*

Il Garante ha effettuato la valutazione di un sistema composto da apparecchiature preordinate alla registrazione di immagini e suoni all'interno di particolari aree tecniche delle navi da crociera gestite dalla società che ha presentato l'istanza di verifica preliminare (cd. *Engine control room*, sala di controllo dell'intero apparato motore della nave) (provv. 16 febbraio 2017, n. 62, doc. web n. 6164054).

In base alla vigente disciplina di rango nazionale, europeo e internazionale posta a protezione della sicurezza delle persone e dell'ambiente marino a fronte dei rischi connessi alle attività di trasporto marittimo, tutte le navi che fanno scalo nei porti nazionali devono essere dotate di un registratore dei dati di viaggio contenente, tra l'altro, la registrazione dell'audio delle conversazioni ed ogni altro suono captato da microfoni collocati sul ponte di comando.

A fronte della rappresentata necessità di innalzare i livelli di sicurezza, di consentire la ricostruzione di eventuali incidenti o anomalie nel funzionamento dei sistemi e l'individuazione di possibili fattori di rischio nelle procedure adottate, l'Autorità ha ritenuto di autorizzare un (analogo) sistema di raccolta dei dati anche all'interno della *Engine control room*, posto che l'attività che ivi si svolge è strettamente collegata a quella effettuata sul ponte di comando, anche alla luce delle caratteristiche tecnologiche della strumentazione di bordo.

All'esito della valutazione circa la liceità del trattamento, la sussistenza delle garanzie previste della disciplina sui controlli a distanza (anche in questo caso la società ha dichiarato di voler attivare la procedura prevista dall'art. 4, comma 1, l. n. 300/1970) e le complessive caratteristiche del sistema, il Garante ha riconosciuto con il provvedimento, alla luce della disciplina sul cd. bilanciamento di interessi (ai sensi dell'art. 24, comma 1, lett. *g*), del Codice), un legittimo interesse del titolare del trattamento dei dati.

Considerati i rischi specifici per i diritti e la libertà degli interessati connessi in special modo alla raccolta dei dati relativi all'audio, il Garante ha prescritto l'adozione di specifiche misure relative all'autenticazione dei soggetti autorizzati ad accedere al sistema (attribuzione di specifiche credenziali o dispositivi di autenticazione forte); al tracciamento degli accessi effettuati, che deve anche indicare i riferimenti temporali ed avere caratteristiche di completezza, integrità, inalterabilità e durata della conservazione analoghe a quelle richieste per i *log* degli accessi degli amministratori di sistema. È stata inoltre prescritta la cifratura delle registrazioni audio e video e la cancellazione irreversibile delle stesse decorsi i tempi di conservazione dei dati (individuati in 70 ore), tranne che in caso di verificazione degli eventi previsti (sinistri ed eventi anomali).

Visto, infine, che la società intende utilizzare alcune registrazioni per finalità didattico-formative, l'Autorità ha precisato che la necessaria previa anonimizzazione

dei dati dovrà riguardare anche le voci (provvedendo alla loro alterazione) e che si dovrà altresì eliminare qualunque elemento che possa ricondurre all'identità delle persone coinvolte (es: nomi, appellativi, riferimenti temporali espliciti).

13.5. *Il trattamento di dati biometrici*

A seguito di una segnalazione presentata al Garante da un dipendente civile del Ministero della difesa è emerso che per un lungo periodo di tempo l'amministrazione ha trattato dati biometrici (mediante estrazione del *template* dell'impronta digitale) di tutti i dipendenti – civili e militari, indipendentemente dalla mansione svolta – che hanno chiesto il rilascio o il rinnovo della Carta multiservizi della difesa (tessera di identificazione dei dipendenti anche per finalità di autenticazione all'accesso ai servizi forniti in rete con funzioni di carta nazionale dei servizi). Tale trattamento, secondo quanto dichiarato dall'amministrazione, era preordinato all'autenticazione dei soggetti specificamente autorizzati ad accedere alle aree della *Certification Authority*. Il Garante, all'esito di una complessa istruttoria, ha ritenuto illecito il trattamento sotto diversi profili (provv. 24 maggio 2017, n. 249, doc. web n. 6531525).

La disciplina sulla tessera di riconoscimento elettronica rilasciata dalle amministrazioni dello Stato prevede l'inserimento di dati personali, anche biometrici, previa attivazione di un procedimento di verifica preliminare dinnanzi al Garante ai sensi dell'art. 17 del Codice (art. 6, d.P.C.M. 24 maggio 2010, Regole tecniche delle tessere di riconoscimento (mod. AT) di cui al d.P.R. n. 851 del 1967 rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'art. 66, comma 8, d.lgs. n. 82/2005, modificato con d.P.C.M. 18 gennaio 2016). Inoltre, in base a tale disciplina, nell'ambito delle finalità proprie delle tessere di riconoscimento, l'amministrazione può utilizzare "per particolari esigenze di sicurezza fisica o logica […] informazioni biometriche come le impronte digitali […] del titolare dell'ATe. L'utilizzo di tali informazioni avviene nel rispetto della normativa in materia di protezione dei dati personali". È inoltre specificato che i dati biometrici possono essere inseriti nella tessera "per specifici scopi di sicurezza dell'amministrazione stessa" (all. B, d.P.C.M. cit., punti 3.1 e 6.2).

In materia di trattamento dei dati biometrici l'Autorità, in un'ottica di semplificazione, con il provvedimento generale prescrittivo in materia di biometria (12 novembre 2014, n. 513, doc. web n. 3556992) ha, tra l'altro, individuato alcune ipotesi per le quali – in presenza dei requisiti di legittimità previsti dal Codice nonché nel rispetto di determinate prescrizioni tecniche – il titolare del trattamento è esonerato dall'attivare l'istanza di verifica preliminare dinnanzi all'Autorità (v. in particolare punto 4.2, relativo al controllo dell'accesso fisico ad aree sensibili e all'utilizzo di apparati e macchinari pericolosi). Resta ferma la possibilità di trattare dati, anche biometrici, per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge (v. art. 58 del Codice).

Il trattamento effettuato dal Ministero della difesa non si inseriva entro tale cornice, sia perché i dati biometrici (nell'arco temporale sopra indicato) venivano raccolti e successivamente trattati nei confronti di tutti i dipendenti, senza alcuna selezione di coloro che avrebbero avuto accesso alle particolari aree destinate ad ospitare la *Certification Authority*, sia perché ai dipendenti non era stata fornita un'idonea informativa sulle caratteristiche fondamentali del trattamento; né, infine, l'amministrazione aveva provveduto ad effettuare la notificazione al Garante.

Il Garante, ritenuto illecito il trattamento, ha prescritto all'amministrazione di effettuare un programma di aggiornamento delle Carte multiservizi contenenti i

dati biometrici volto ad inibire il trattamento dei dati memorizzati in violazione delle disposizioni vigenti.

È stata invece accolta la richiesta di verifica preliminare finalizzata, nel rispetto delle procedure previste dallo Statuto dei lavoratori, alla conservazione fino a trenta giorni delle immagini registrate dal sistema di videosorveglianza e dei dati rilevati dal sistema di controllo accessi biometrico, basata su oggettive esigenze di sicurezza, da parte di una società proprietaria di un complesso immobiliare adibito a centro orafo in cui sono ubicati immobili di proprietà delle imprese socie e spazi ad uso comune di proprietà esclusiva della società consortile che provvede inoltre alla gestione di tutte le attività di servizi e di impresa necessarie (vigilanza, custodia, sicurezza, tutela, pulizia, manutenzione, ristorazione) (provv. 20 aprile 2017, n. 198, doc. web n. 6393088).

13.6. *Il trattamento di dati giudiziari*

Nel 2017 il Garante si è pronunciato rispetto ad alcune richieste di autorizzazione al trattamento di dati giudiziari in ambito di lavoro (artt. 27 e 41 del Codice).

Fra i casi esaminati, si menziona una richiesta di una società che gestisce in appalto servizi di pulizie nel settore dei trasporti ferroviari rispetto ai dati giudiziari dei propri dipendenti con funzioni di "manovale e pulitore di impianti fissi" a bordo dei treni (provv. 15 giugno 2017, n. 267, doc. web n. 6558837).

In particolare la società ha chiesto di poter acquisire il certificato del casellario giudiziale consegnato dai medesimi dipendenti e di fornirne copia alla società appaltante. La società ha infatti motivato la richiesta con la necessità di conformarsi a quanto previsto da uno schema di contratto di appalto, non ancora stipulato, il quale prevedrebbe per l'appunto l'impegno dell'appaltatore a raccogliere il certificato generale del casellario nonché a "segnalare tempestivamente al committente il nominativo di coloro a carico dei quali risultano sentenze di condanna passate in giudicato nonché i reati ascritti e la pena comminata".

Con l'autorizzazione generale n. 7 del 2016 il Garante, conformemente a quanto previsto dall'art. 27 del Codice, ha autorizzato i datori di lavoro al trattamento dei dati giudiziari qualora ciò sia "indispensabile per […] adempiere o esigere l'adempimento di specifici obblighi o eseguire specifici compiti previsti da leggi, dalla normativa dell'Unione europea, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro".

Il Garante ha ritenuto insussistente nel caso concreto un'idonea base giuridica – legislativa, regolamentare o contrattuale – per il trattamento nell'ambito del rapporto di lavoro da parte della società richiedente di informazioni così delicate (considerato che il certificato generale del casellario contiene il riferimento ai provvedimenti di condanna definitivi, in relazione a qualsiasi tipologia di fattispecie di reato, nonché la menzione di alcuni provvedimenti definitivi in materia civile ed amministrativa), né in relazione alla prospettata comunicazione dei dati alla società appaltante. L'Autorità, per tali motivi, ha rigettato la richiesta di autorizzazione.

Un'altra richiesta ai sensi dell'art. 41 del Codice – pervenuta da una società, a tutela propria e delle numerose amministrazioni per conto delle quali opera in settori altamente strategici per il Paese – ha riguardato la possibilità di richiedere, direttamente e a campione, il certificato penale del casellario giudiziale di un centinaio di dipendenti, posti in posizione apicale e in ruoli chiave all'interno dell'azienda. Nell'accoglierla, l'Autorità ha ritenuto che il trattamento dei dati giudiziari fosse necessario per lo svolgimento delle funzioni e degli specifici servizi erogati in

ambito pubblico dalla società, che tratta volumi rilevanti di dati personali rivestendo un ruolo centrale nel processo di digitalizzazione e di interoperabilità tra le pp.aa. (anche mediante servizi integrati). In particolare, il trattamento è stato autorizzato per le rilevanti finalità di interesse pubblico perseguite, tra le quali rientra la necessità di assicurare elevati livelli di sicurezza, tenuto conto della delicatezza nonché del volume dei dati trattati, anche mediante l'accertamento dei requisiti di affidabilità e onorabilità del personale cui sono assegnati incarichi o funzioni di particolare rilevanza e "sensibilità" all'interno della società. Il Garante ha prescritto alla società di informare il personale della possibilità della verifica e di definire l'ambito oggettivo del trattamento, individuando tassativamente il novero delle fattispecie di reato oggetto di verifica rispetto alle finalità perseguite (ed esplicitate), con riguardo a reati di particolare gravità, tali da incidere sui profili di onestà e di correttezza del dipendente in relazione alle specifiche funzioni o mansioni a questi assegnate; in tale prospettiva la valutazione deve incentrarsi sui delitti contro il patrimonio e la personalità interna dello Stato (provv. 19 gennaio 2017, n. 10, doc. web n. 5953097).

13.7. *Il trattamento di dati sanitari di familiari e congiunti del dipendente a fini di fruizione di permessi e congedi*

Con segnalazione presentata da un'organizzazione sindacale è stato lamentato che una società operante nel settore delle telecomunicazioni richiedesse ai propri dipendenti la produzione di certificazione sanitaria contenente anche "elementi costituenti la diagnosi clinica" riferiti a terzi rispetto al rapporto di lavoro in applicazione della normativa di settore secondo cui la documentazione medica che deve essere presentata dal dipendente al proprio datore di lavoro ai fini della fruizione dei permessi retribuiti per "grave infermità" del coniuge, parenti o conviventi e dei congedi non retribuiti "per gravi motivi familiari" (art. 4, commi 1 e 2, l. 8 marzo 2000, n. 53 e artt. 1 e 2, comma 1, lett. *d*), d.m. 21 luglio 2000, n. 278). In particolare, è stato accertato che la società chiedeva ai propri dipendenti, quale condizione per la fruizione del beneficio (consistente in permessi giornalieri o periodi di congedo), la produzione di certificazione sanitaria contenente sia l'attestazione della condizione di "grave infermità", espressamente richiesta dalla legge, sia la descrizione degli elementi costituenti la diagnosi clinica, peraltro riferita a soggetti terzi rispetto al rapporto di lavoro ("documentata grave infermità del coniuge o di un parente entro il secondo grado o del convivente, purché la stabile convivenza con il lavoratore o la lavoratrice risulti da certificazione anagrafica"; art. 4, comma 1, l. 8 marzo 2000, n. 53, cit.). A seguito di una complessa attività istruttoria, tenuto conto di una pluralità di segnalazioni, istanze e quesiti in merito al medesimo comportamento posto in essere in altri contesti lavorativi nonché del generale impatto nell'ambito della gestione del rapporto di lavoro, sia pubblico che privato, sono stati effettuati approfondimenti con il Ministero del lavoro e delle politiche sociali, il quale ha rappresentato il proprio orientamento e i necessari chiarimenti in merito alla portata applicativa di alcuni propri precedenti interpretativi.

Nel definire il procedimento con nota del 19 ottobre 2017, l'Autorità ha dichiarato che la condotta del datore di lavoro non risultava conforme alla disciplina di protezione dei dati personali (artt. 3, 11, comma 1, lett. *d*), e 26 del Codice e autorizzazioni generali nn. 1 e 2 cit.; cfr., tra i tanti, provv. 21 marzo 2007, doc. web n. 1395821 e, anche, provv.ti 21 aprile 2009, doc. web n. 1616870; 9 novembre 2005, doc. web n. 1191411).

13

L'Autorità ha in proposito ribadito che il trattamento dei dati da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati può essere effettuato dal datore di lavoro nell'ambito della finalità di gestione del rapporto di lavoro, nel rispetto della disciplina di protezione dei dati personali; e ciò, anche ove i dati siano riferiti a soggetti terzi individuati dalla legge (art. 433 c.c.), come ad esempio i congiunti o conviventi del lavoratore (artt. 3, 11 e 26, comma 4, lett. *d*), del Codice, e autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro – n. 1/2016, n. 523, doc. web n. 5800451, punto 3), lett. *a*) e *b*) nonché autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale – n. 2/2016, n. 424, doc. web n. 5803257, punto 1.3, lett. *b*); cfr. anche 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, n. 53 del 23 novembre 2006, doc. web n. 1364099, punto 6.4).

La disciplina di protezione dei dati personali richiede in ogni caso l'osservanza dei princìpi di necessità, proporzionalità e indispensabilità, che impongono al datore di lavoro di valutare specificamente il rapporto tra i dati oggetto di trattamento e gli adempimenti derivanti da compiti e obblighi di volta in volta previsti dalla normativa di settore, e di adottare soluzioni che, pur consentendo di svolgere gli adempimenti in modo efficace, eliminino ogni occasione di superflua conoscibilità dei medesimi da parte di soggetti non legittimati al trattamento (cfr. artt. 3 e 11, comma 1, lett. *d*), del Codice; aut. gen. n. 1/2016, punto 5 e n. 2/2016, punto 3). In attuazione dei richiamati princìpi, pertanto, il datore di lavoro non può venire a conoscenza di tutti i dati sanitari del congiunto del lavoratore (diagnosi o anamnesi).

Come già chiarito negli altri casi di fruizione di permessi riconosciuti dalla legge per causali connesse allo stato morboso o di disabilità di un familiare, il lavoratore deve presentare al datore di lavoro una certificazione dalla quale risulti esclusivamente l'accertata condizione di volta in volta richiesta dalla legge. In altre parole, il perseguimento dei compiti e delle attribuzioni degli uffici preposti alla gestione del personale, destinatari della predetta documentazione, può ugualmente essere conseguito mediante l'acquisizione di una certificazione medico-legale attestante la sola sussistenza delle "grave infermità" o la ricorrenza di uno dei "gravi motivi familiari"; ciò consentirebbe l'effettuazione delle dovute verifiche da parte degli uffici destinatari della predetta documentazione in merito alla ricorrenza dei presupposti per il riconoscimento del beneficio, evitando al contempo la conoscibilità di informazioni sanitarie non indispensabili (sul punto, v. raccomandazione CM/REc (2015)5 sul trattamento dei dati personali nel contesto occupazionale, punto 9.7; Cass. civ., sez. lav., n. 2803/2015).

In conclusione l'Autorità ha precisato che è onere del lavoratore consegnare l'"idonea documentazione" di cui all'art. 3, d.m. n. 278/2000 al datore di lavoro quale condizione indefettibile per comprovare il proprio diritto e ottenere i benefici in esame e che, nell'attestare la sola sussistenza della "grave infermità" o la ricorrenza di uno dei "gravi motivi familiari", potrà specificare, ad esempio, se la patologia sia "acuta o cronica" e se sia direttamente riconducibile ad una delle situazioni patologiche individuate tassativamente ai punti da 1 a 4 della lett. *d*) dell'art. 2 del citato decreto, ma dovrà comunque essere priva dell'indicazione della specifica patologia diagnosticata all'interessato, con l'omissione delle parti dedicate alla descrizione dei dati anamnestici, all'esame obiettivo e alla diagnosi della persona (analoga considerazione vale per la certificazione da esibire nei casi di "grave infermità", trattandosi, come chiarito in più occasioni dal Ministero del lavoro e delle politiche sociali, di una *species* rispetto al *genus* dei "gravi motivi", di cui le patologie enumerate dal regolamento costituiscono cd. figure sintomatiche; art. 4, comma 2, l. n. 53/2000 e art. 2, comma 1, lett. *d*), d.m. n. 278/2000).