GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2019

www.garanteprivacy.it

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

13.1. *La protezione dei dati nell'ambito del rapporto di lavoro privato tra vecchia e nuova disciplina*

Anche in relazione ai trattamenti di dati personali effettuati nell'ambito del rapporto di lavoro, l'Autorità ha continuato a dare corso agli adempimenti previsti dal RGPD e dalla disciplina di adeguamento del Codice (contenuta nel decreto legislativo n. 101/2018) nonché a fornire chiarimenti ai soggetti coinvolti dall'applicazione delle disposizioni in materia di protezione dei dati (titolari, interessati, associazioni di categoria e rappresentative di interessati) sulle novità normative, in particolare con riferimento al trattamento dei dati biometrici e dei dati giudiziari (v., relativamente a tale ultima tipologia di dati, Relazione 2018, p. 127).

Il trattamento dei dati biometrici è ora sottoposto a garanzie più rigorose rispetto al passato. Infatti l'art. 9, par. 1, del RGPD ha inserito i dati biometrici nel novero dei dati "particolari" per i quali vige un generale divieto di trattamento. Esso può essere superato solo qualora ricorrano alcune tassative condizioni di liceità che, ove il trattamento avvenga nell'ambito del rapporto di lavoro, consistono nella necessità di "assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. *b*), e cons. da 51 a 53, del RGPD).

Allo stato sono espressamente previste dal legislatore nazionale due ipotesi di trattamento di dati biometrici nel contesto del rapporto di lavoro. In primo luogo, l'art. 2-*septies*, comma 7, del Codice consente il trattamento dei dati biometrici nell'ambito dell'accesso fisico e logico ai dati da parte di soggetti autorizzati; merita evidenziare che non rientrano in tale ambito i trattamenti effettuati per finalità di controllo dell'autenticazione all'accesso ad aree particolari e riservate, così come quelli finalizzati alla rilevazione della presenza in servizio nell'ambito del lavoro privato.

La seconda ipotesi riguarda esclusivamente il lavoro pubblico. La legge 19 giugno 2019, n. 56, recante interventi per la concretezza delle azioni delle pp.aa. e la prevenzione dell'assenteismo (in relazione alla quale non è stata adottata la necessaria normativa secondaria di attuazione) ha infatti previsto l'utilizzo di sistemi biometrici per finalità di verifica dell'osservanza dell'orario di lavoro. Al riguardo, come già anticipato, il Garante ha manifestato riserve sulla compatibilità di tale disciplina rispetto ai principi e alle disposizioni in materia di tutela dei dati personali sia in sede di audizione del Presidente del Garante nel corso dell'*iter* legislativo – presso la Commissione Lavoro pubblico e privato, previdenza sociale del Senato, 27 novembre 2018 (doc. web n. 9064421) e presso le Commissioni riunite Affari costituzionali e Lavoro della Camera dei deputati, 6 febbraio 2019 (doc. web n. 9080870) –, sia nel parere reso sullo schema di d.P.C.M. concernente la disciplina di attuazione della disposizione di cui all'art. 2, l. 19 giugno 2019, n. 56 (provv. 19 settembre 2019, n. 167, doc. web n. 9147290; v. già il parere su uno schema di

disegno di legge recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", 11 ottobre 2018, n. 464, doc. web n. 9051774) (cfr. par. 2.2 n. 14).

In proposito l'Autorità ha avviato i lavori per la predisposizione del provvedimento che individua le misure di garanzia ex art. 2-*septies* del Codice relativamente al trattamento, nell'ambito lavorativo, di dati biometrici e di dati relativi allo stato di salute.

Il Garante ha poi continuato ad occuparsi dei trattamenti effettuati mediante la posta elettronica aziendale ed altri dispositivi tecnologici utilizzati nell'ambito del rapporto di lavoro, indicando le condizioni per conformare i trattamenti ai principi di protezione dei dati (cfr. *infra* par. 13.3).

13.2. *Il trattamento di categorie particolari di dati nell'ambito del rapporto di lavoro: dall'autorizzazione generale al provvedimento prescrittivo del Garante ex art. 21, d.lgs. n. 101/2018*

Nel quadro degli adempimenti attribuiti al Garante dalla disciplina di adeguamento del Codice al RGPD e, in particolare, in base a quanto stabilito dall'art. 21, d.lgs. n. 101/2018, con provvedimento di carattere generale, l'Autorità ha portato a termine (cfr. già Relazione 2018, p. 119 s.) il procedimento con il quale sono state individuate le prescrizioni contenute nelle autorizzazioni generali riferite ai trattamenti di categorie particolari di dati (ora elencati nell'art. 9, par. 1, del RGPD e nel sistema previgente definiti dati sensibili) effettuati nell'ambito del rapporto di lavoro, relative alle situazioni di trattamento di cui agli artt. 6, par. 1, lett. *c*) ed *e*), 9, par. 2, lett. *b*), e 4 nonché al Capo IX del RGPD, risultate compatibili con le disposizioni comunitarie e il decreto che ha novellato il Codice, provvedendo altresì al loro aggiornamento (provv. 13 dicembre 2018, n. 497, doc. web n. 9068972; v. anche Relazione 2018, pp. 119 e 120). Lo schema di provvedimento, sottoposto a consultazione pubblica, è stato definitivamente adottato con provvedimento 5 giugno 2019, n. 146 (doc. web n. 9124510).

Premesso che nel quadro normativo delineato dal RGPD i trattamenti dei dati personali nel contesto lavorativo sono disciplinati unitariamente, sia se effettuati da datori di lavoro pubblici che privati (cfr. artt. 88 e 9, par. 2, lett. *b*), del RGPD), il provvedimento prescrittivo definisce le "garanzie appropriate" richieste dall'art. 9, par. 2, lett. *b*), del RGPD per i trattamenti di categorie particolari di dati effettuati dai soggetti che a vario titolo trattano dati nell'ambito del rapporto di lavoro e nella fase pre-assuntiva.

Nell'ordinamento vigente il trattamento di categorie particolari di dati personali non fondato su uno dei presupposti indicati dall'art. 9, par. 2, del RGPD è vietato. I trattamenti per finalità di gestione del rapporto di lavoro (anche successivamente all'interruzione dello stesso) o in fase pre-assuntiva possono essere effettuati solo in quanto necessari per l'adempimento di obblighi previsti da leggi e regolamenti oppure da un contratto collettivo nei limiti previsti dall'ordinamento (v. art. 9, par. 2, lett. *b*), del RGPD). Allo stato, il trattamento di dati particolari contenuti nei *curricula* di candidati può essere quindi effettuato solo in presenza del consenso esplicito dell'interessato (v. art. 9, par. 2, lett. *a*), del RGPD).

Il sistema prevede che, in ogni caso, restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa dell'UE che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali. Considerato che il datore di lavoro tratta i dati personali nel rispetto delle disposizioni nazionali "più specifi-

che per assicurare la protezione dei diritti e delle libertà" (art. 88 del RGPD), deve essere osservato quanto stabilito dall'art. 113 del Codice che fa salvo l'art. 8, l. 20 maggio 1970, n. 300 (in base al quale il datore di lavoro non può, ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore), e l'art. 10, d.lgs. 10 settembre 2003, n. 276 (che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, all'affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute e ad eventuali controversie con i precedenti datori di lavoro, nonché di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo). In proposito rileva altresì quanto previsto dall'art. 15, l. 20 maggio 1970, n. 300 (che dispone la nullità di patti o atti "diretti a fini di discriminazione politica, religiosa, razziale, di lingua o di sesso, di handicap, di età o basata sull'orientamento sessuale o sulle convinzioni personali") e dall'art. 6, l. 5 giugno 1990, n. 135 (che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività) nonché dalle altre norme in materia di pari opportunità o volte a prevenire discriminazioni.

Si segnala che in occasione della predisposizione del provvedimento di carattere generale, il Garante ha precisato la portata di alcune prescrizioni già contenute nella precedente autorizzazione n. 1/2016 e ne ha introdotte di nuove (alla luce del potere attribuitogli dal legislatore di disporre aggiornamenti), attingendo alla casistica dei provvedimenti adottati nel tempo in materia. In particolare, è stato chiarito che il trattamento di categorie particolari di dati effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, posto che una diversa interpretazione che consentisse di prendere in considerazione anche astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento (v. punto 1.3, lett. *d*), provv. 5 giugno 2019, n. 146, doc. web n. 9124510).

Con riferimento al trattamento di dati che rivelano le opinioni politiche, è stato stabilito che in caso di partecipazione di dipendenti ad operazioni elettorali in qualità di rappresentanti di lista, in applicazione del principio di necessità, il datore di lavoro non deve trattare, nell'ambito della documentazione da presentare al fine del riconoscimento di benefici di legge, dati che ne rivelino le opinioni politiche (ad es., non deve essere richiesto il documento che designa il rappresentate di lista essendo allo scopo sufficiente la certificazione del presidente di seggio; v. punto 1.4.2, lett. *c*), provv. 5 giugno 2019, n. 146).

Infine, sono state fornite prescrizioni specifiche relative alle modalità del trattamento di tale categoria di dati, precisando che in occasione dell'utilizzo di forme di comunicazione individualizzate nei confronti dell'interessato, anche avvalendosi di personale autorizzato, qualora si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità per il datore di lavoro di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto (v. punto 1.5, lett. *b*), provv. 5 giugno 2019, n. 146). In caso di trasmissione di documenti contenenti categorie particolari di dati ad altri uffici o funzioni interne che risultino in concreto legittimati a conoscerli in base

alle rispettive attribuzioni, è necessario verificare che la trasmissione riguardi esclusivamente le informazioni necessarie allo svolgimento della funzione, astenendosi dall'allegare, se non strettamente indispensabile, documentazione integrale o stralci di documentazione non pertinente e non necessaria (v. punto 1.5, lett. *c*), provv. 5 giugno 2019, n. 146).

Come già stabilito in alcuni provvedimenti dell'Autorità, è stato altresì espressamente prescritto che, qualora per concrete ragioni organizzative si proceda a mettere a disposizione i turni di servizio di una pluralità di colleghi interessati (ad es., mediante affissione in bacheca), il datore di lavoro non deve esplicitare, anche attraverso l'uso di acronimi o sigle, le causali dell'assenza dal servizio dalle quali sia possibile conoscere categorie particolari di dati riferiti a soggetti identificabili (es. permessi sindacali o dati relativi alla salute) (v. punto 1.5, lett. *d*), provv. 5 giugno 2019, n. 146).

La violazione delle prescrizioni contenute nel provvedimento generale è soggetta alla sanzione amministrativa di cui all'art. 83, par. 5, del RGPD (ex art. 21, comma 5, d.lgs. n. 101/2018).

13.3. *Controlli sulla posta elettronica aziendale successivamente alla cessazione del rapporto di lavoro*

Con un reclamo è stato lamentato il persistente funzionamento, cessato il rapporto di lavoro, di un *account* di posta elettronica aziendale di tipo individualizzato assegnato ad un lavoratore. Accertata la fondatezza del reclamo – posto che per circa un anno e sette mesi il titolare del trattamento ha avuto accesso alle comunicazioni pervenute, tramite reindirizzamento automatico delle stesse ad altro *account*, provvedendo a cancellarlo solo a seguito di diffida presentata dal reclamante –, il Garante ha ritenuto illecito il trattamento. Peraltro, è stato constatato che tale trattamento è avvenuto in assenza di alcuna informativa predisposta dal titolare del trattamento e, quindi, senza che gli interessati fossero stati informati in merito alle specifiche modalità dei trattamenti effettuati sugli *account* loro assegnati. Sia il trattamento effettuato nei confronti del reclamante sia la prassi aziendale della società non sono stati quindi ritenuti conformi ai principi di liceità, necessità e proporzionalità; in considerazione di tali violazioni il trattamento – non più in essere al momento dell'adozione del provvedimento – è stato dichiarato illecito e il titolare del trattamento è stato ammonito sulla necessità di conformare i trattamenti effettuati sugli *account* di posta elettronica aziendale dopo la cessazione del rapporto di lavoro alle disposizioni e ai principi in materia di protezione dei dati personali. Il Garante, richiamato quanto enunciato nelle linee guida per posta elettronica e internet (provv. 1° marzo 2007, n. 13, doc. web n. 1387522), ha affermato che "il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i *file* allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali" e che la trasposizione di tale principio in ambito lavorativo comporta la possibilità che il lavoratore – o terzi soggetti coinvolti – possano vantare una legittima aspettativa di confidenzialità rispetto ad alcune forme di comunicazione, anche nel caso in cui venga a cessare il rapporto di lavoro. Ha pertanto intimato al datore di lavoro di rimuovere gli *account* di posta elettronica aziendale riconducibili a persone identificate o identificabili dopo la cessazione del rapporto di lavoro, previa disattivazione degli stessi e contestuale adozione di sistemi

automatici volti ad informare i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento, provvedendo altresì ad adottare misure idonee ad impedire la visualizzazione di messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione (provv. 20 dicembre 2019, n. 216, doc. web n. 9215890).

13.4. *Il trattamento di dati dei dipendenti effettuato mediante dispositivi tecnologici indossabili*

All'esito di un'attività di controllo avviata d'ufficio dall'Autorità a seguito della pubblicazione di notizie di stampa è emerso che, nell'ambito dello svolgimento del servizio di spazzamento su strada svolto per conto della concessionaria dei servizi ambientali di un comune, una società ha attivato un sistema basato sul trattamento dei dati dei lavoratori effettuato mediante dispositivi tecnologici indossabili (sul polso, tipo braccialetto), idonei ad effettuare la lettura di etichette elettroniche (*tag*) mediante tecnologia Rfid ed altresì dotati di funzionalità di localizzazione geografica mediante sistema Gps.

Diversamente da quanto rappresentato dalla società, nel corso del procedimento è stato verificato che i dati trattati dal sistema erano riferiti ad interessati identificabili, sussistendo la possibilità di individuare il dipendente grazie alla rilevazione dei *tag* e della relativa localizzazione geografica mediante Gps attraverso il raffronto con altri dati raccolti (es. turni di lavoro).

In occasione di diverse interlocuzioni con il titolare del trattamento, l'Autorità ha preso atto che, secondo quanto dichiarato, la società si era limitata ad avviare la sperimentazione del sistema senza raccogliere e memorizzare alcun dato. Inoltre si è preso atto che, successivamente all'avvio del procedimento, l'azienda aveva provveduto a sottoscrivere un accordo ai sensi dell'art. 4, comma 1, l. 20 maggio 1970, n. 300 (la cui osservanza costituisce condizione di liceità del trattamento ai sensi dell'art. 114 del Codice), in base al quale la funzionalità di localizzazione sarà attivata al massimo per un turno di lavoro a settimana. Tale previsione è stata ritenuta conforme ai principi di necessità e proporzionalità in relazione alle finalità perseguite (v. art. 5, par. 1, lett. *c*), del RGPD).

L'Autorità ha poi ritenuto necessaria l'individuazione da parte della società, di una tipologia di dispositivo, anche per le sue caratteristiche esteriori, non lesivo della dignità del dipendente e che comunque non risulti tale nella percezione degli interessati, conformemente peraltro a quanto stabilito nel predetto accordo stipulato in base alla disciplina giuslavoristica in materia di controlli a distanza.

In relazione alle caratteristiche del sistema che si intende adottare, è stata altresì rammentata al titolare del trattamento la necessità di individuare i tempi di conservazione dei registri contenenti i turni di lavoro, la zona di spazzamento e l'identità dei lavoratori entro i limiti strettamente necessari rispetto alla finalità perseguita (cd. consuntivazione dell'attività svolta), di indicare preventivamente e tassativamente i casi nei quali si renderà necessario interconnettere le informazioni al fine di ricostruire fatti oggetto di eventuale contestazione da parte della stazione appaltante nonché di adottare misure organizzative e tecnologiche per mantenere distinte le basi di dati qualora non sia più necessaria l'interconnessione per la ricostruzione di fatti oggetto di contestazione, ma sia comunque necessaria l'ulteriore conservazione dei registri dei turni per fini amministrativi. Si è altresì evidenziato che, ai sensi dell'art. 35 del RGPD, la società dovrà effettuare una valutazione di impatto sulla protezione dei dati alla luce delle concrete caratteristiche del sistema

tecnologico che intende adottare (nota Segretario generale 28 febbraio 2019, doc. web n. 9094427).

13.5. *Il trattamento di dati contenuti in una relazione investigativa relativi ad un terzo*

A seguito di reclamo, il Garante si è pronunciato in merito alla liceità del trattamento posto in essere da un datore di lavoro avente ad oggetto i dati (riferiti ad un soggetto diverso da quello sottoposto ad investigazione), tratti dai dispositivi informatici e mobili assegnati ad una propria dipendente, contenuti in una relazione investigativa commissionata al fine di acquisire elementi di prova dell'uso improprio dei dispositivi stessi da parte di quest'ultima. Premesso che l'accertamento dell'Autorità ha riguardato esclusivamente il trattamento dei dati riferiti al reclamante (soggetto terzo rispetto al rapporto di lavoro in questione), è risultato che tali dati, in particolare le immagini, ritraevano l'interessato in contesti di vita privata ed intima, e che la relazione investigativa era stata consegnata, in versione integrale, a diversi esponenti di vertice del soggetto datoriale.

L'Autorità ha ritenuto non conforme ai principi di liceità, proporzionalità e non eccedenza il trattamento effettuato (v., nel testo previgente, gli artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice) ed ha ammonito il datore di lavoro in ordine alla necessità di conformare i trattamenti di dati personali, anche per la finalità di tutela dei propri diritti in giudizio, ai principi ed alle disposizioni in materia di protezione dei dati personali. Il fine per il quale sono stati trattati i dati oggetto di reclamo poteva, infatti, essere utilmente perseguito provvedendo ad oscurare alcune immagini di natura privatissima o, quantomeno, a non rendere riconoscibili i terzi presenti nelle immagini riprodotte tratte dai dispositivi oggetto di relazione tecnica, considerata anche la necessità di tutelare la dignità del reclamante oltre che della dipendente. Si sarebbe dovuto, per tale motivo, fare in modo che la documentazione a supporto dell'avvio dell'azione disciplinare nei confronti della dipendente contenesse esclusivamente i dati a tal fine necessari. Il trattamento, inoltre, è stato effettuato nei confronti del reclamante in assenza di idonei criteri di legittimazione al trattamento: non era, infatti, "necessario" ai sensi del previgente art. 24, comma 1, lett. *f*), del Codice e non è stato rispettato quanto enunciato dall'art. 26, par. 4, lett. *c*), del Codice in base al quale, in relazione alla finalità di fare valere un diritto in giudizio, il titolare può trattare i dati sensibili solo se necessari al perseguimento della finalità nonché rispettando il cd. principio del pari rango ("Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile") (provv. 2 ottobre 2019, n. 182).

13.6. *Compiti e responsabilità dei professionisti che effettuano trattamenti di dati personali su incarico del datore di lavoro*

Con nota 22 gennaio 2019 indirizzata al Consiglio nazionale dei consulenti del lavoro, l'Autorità ha fornito alcuni chiarimenti, sollecitati dallo stesso organismo rappresentativo della categoria e da numerosi professionisti (commercialisti, avvocati, consulenti legali), in ordine ad alcuni aspetti affrontati dalla circolare 23 luglio 2018, n. 1150, adottata dal medesimo Consiglio nazionale, con particolare riferimento alla individuazione del ruolo di titolare, responsabile o contitolare relativamente alle attività svolte da tale categoria di professionisti.

Una volta sottolineato che il RGPD non ha introdotto innovazioni sostanziali

rispetto alle disposizioni previgenti relativamente alle definizioni di titolare del trattamento e responsabile del trattamento (v. art. 4, nn. 7) e 8), RGPD), l'Autorità ha chiarito, che mentre in relazione alle attività di trattamento che riguardano dati dei propri dipendenti e dei propri clienti il consulente del lavoro (o altro professionista) determina puntualmente le finalità e i mezzi del trattamento sulla base dei criteri di legittimazione applicabili (contratto, discipline di settore applicabili), operando pertanto in qualità di titolare del trattamento, nel caso in cui effettui attività "esternalizzate" dal datore di lavoro per conto di quest'ultimo riveste necessariamente il ruolo di responsabile del trattamento. L'affidamento a professionisti qualificati dell'effettuazione di segmenti di attività relativi alla gestione del rapporto di lavoro (dall'elaborazione delle buste paga agli adempimenti previsti dalle discipline previdenziali e assistenziali, dalla gestione degli obblighi in fase di assunzione a quelli relativi al fine rapporto) comporta il conferimento al professionista di una pluralità di dati, anche afferenti a categorie particolari, che nell'ambito del rapporto di lavoro possono essere raccolti e successivamente trattati in base a quanto previsto dalle norme di legge e di regolamento applicabili e in base al contratto collettivo di lavoro (v. artt. 6, 9, par. 2, lett. *b*), e 88 del RGPD). Pertanto il professionista tratta le informazioni relative ai lavoratori (dipendenti dei propri clienti) utilizzando i dati raccolti dal datore di lavoro nel perseguimento di finalità legittime nonché in base ai criteri e alle direttive da questo impartite relativamente alla gestione del rapporto di lavoro sottostante. Tale ricostruzione è confermata anche dalla normativa di settore relativa all'attività del consulente del lavoro (l. 11 gennaio 1979, n. 12, norme per l'ordinamento della professione di consulente del lavoro) laddove prevede che il consulente iscritto all'Albo dei consulenti del lavoro può assumere "gli adempimenti in materia di lavoro, previdenza ed assistenza sociale dei lavoratori dipendenti, quando non sono curati dal datore di lavoro, direttamente od a mezzo di propri dipendenti". Peraltro in capo al datore di lavoro, anche a seguito del conferimento dell'incarico e dell'eventuale consegna della documentazione necessaria al suo svolgimento, permane la responsabilità prevista dall'ordinamento in caso di violazione degli obblighi posti in materia di lavoro, previdenza ed assistenza sociale (v. art. 7, l. n. 12/1979).

L'incarico al consulente è affidato mediante la sottoscrizione di un "contratto o altro atto giuridico" stipulato dalle parti tenendo conto dei compiti in concreto affidati, del contesto, delle finalità e modalità del trattamento e non in base a modelli imposti unilateralmente. A sua volta il consulente potrà avvalersi di collaboratori di fiducia, che operino sotto la sua autorità, inquadrabili nella figura prevista all'art. 2-*quaterdecies* del Codice. Il consulente potrà altresì avvalersi di sub-responsabili qualora sia loro demandata "l'esecuzione di specifiche attività di trattamento per conto del titolare" (v. art. 28, par. 4, del RGPD); in tal caso il relativo atto di incarico deve essere autorizzato, anche in via generale, dal titolare.

Considerato che, rispetto al quadro previgente, l'art. 28 del RGPD ha precisato i compiti che possono essere attribuiti dal titolare al responsabile, individuando l'ambito delle rispettive responsabilità e gli obblighi di cooperazione cui è tenuto il responsabile, l'Autorità ha sottolineato che anche sul responsabile grava l'adempimento delle disposizioni poste in materia di misure di sicurezza (ex art. 32 del RGPD), in particolare per quanto riguarda la gestione dell'archivio. Infine è stato chiarito che al termine del rapporto professionale i dati contenuti negli archivi dovranno essere cancellati (oppure anonimizzati) e/o consegnati al titolare conformemente alle condizioni individuate nel contratto di affidamento dell'incarico (nota 22 gennaio 2019, doc. web n. 9080970).

13

13.7. *La limitazione dell'esercizio dei diritti dopo le modifiche al Codice*

In sede di decisione di un reclamo avente ad oggetto l'esercizio del diritto di accesso del lavoratore ai dati contenuti in una relazione investigativa commissionata dal datore di lavoro ad un'agenzia privata nel periodo in cui il reclamante era in malattia (in relazione a fatti avvenuti prima dell'applicazione del RGPD), il Garante ha fornito alcuni chiarimenti sulle disposizioni che disciplinano la limitazione dei diritti degli interessati in applicazione di quanto previsto dall'art. 23 del RGPD. Tale disposizione individua alcuni specifici requisiti che la disciplina nazionale deve indefettibilmente contenere laddove ponga limitazioni alla "portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34", in vista della salvaguardia, tra l'altro, della tutela "dei diritti e delle libertà altrui", sempre che tali limitazioni rispettino l'essenza dei diritti e delle libertà fondamentali e siano una misura necessaria e proporzionata in una società democratica.

A tale disposizione ha dato attuazione l'art. 2-*undecies* del Codice, in base al quale i diritti di cui agli artt. da 15 a 22 del RGPD non possono essere esercitati con richiesta al titolare del trattamento o con reclamo nel caso in cui, tra le altre ipotesi, "dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto […] allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria". Anche relativamente a tale ipotesi il successivo comma 3 specifica che "i diritti […] sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'art. 23, par. 2, del RGPD. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato".

L'Autorità ha in proposito ritenuto che la disciplina in parola si pone in linea di continuità con quanto già stabilito dal previgente art. 8, comma 2, lett. *e*), del Codice in applicazione del quale il Garante ha ritenuto – avuto riguardo alle circostanze del caso concreto – di accogliere le istanze di limitazione dell'esercizio del diritto di accesso "limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per l'esercizio del diritto in sede giudiziaria" (provv. ti 21 gennaio 2016, n. 11, doc. web n. 4715667 e 13 dicembre 2012, n. 412, doc. web n. 2273474). Nel caso considerato, posto che l'istanza di accesso è stata presentata in data successiva alla conclusione del procedimento disciplinare, in fase precontenziosa, e che, dato il particolare regime probatorio del processo del lavoro – che prevede l'onere della prova a carico del datore di lavoro –, la comunicazione dei dati trattati nell'ambito dell'attività investigativa avrebbe comportato un "pregiudizio effettivo e concreto […] all'esercizio di un diritto in sede giudiziaria", è stata ritenuta applicabile la limitazione all'esercizio del diritto prevista dal richiamato art. 2-*undecies* del Codice. Il Garante ha comunque precisato che la limitazione è circoscritta al periodo strettamente necessario ad evitare un pregiudizio all'esercizio del diritto da parte del titolare. Pertanto, fermi restando i poteri del giudice del lavoro in ordine alla produzione ed esibizione di atti e documenti nel corso del procedimento giurisdizionale, una volta venute meno le ragioni del pregiudizio nessun ostacolo potrà essere frapposto all'esercizio del diritto previsto dall'art. 15 del RGPD (provv. 31 gennaio 2019, n. 20, doc. web n. 9086480).

13.8. *Il trattamento di dati di dipendenti pubblici e di utenti mediante il sistema di prenotazione e gestione dei servizi*

Nell'ambito di verifiche compiute in relazione sull'uso delle *app* nel settore pubblico, il Garante ha adottato un provvedimento nei confronti di Roma Capitale in relazione ai trattamenti di dati personali dei dipendenti e degli utenti posti in essere mediante il sistema denominato "TuPassi", fornito da una società terza, per la gestione delle prenotazioni dei servizi erogati al pubblico e delle code allo sportello (cfr. par. 4.6). Il sistema utilizzato dall'Ente costituisce, nella ricostruzione effettuata dal Garante, uno strumento per perseguire il miglioramento dell'efficienza ed economicità dell'attività amministrativa attraverso la gestione delle prenotazioni degli appuntamenti dei servizi erogati allo sportello e delle attese; di conseguenza, i trattamenti di dati personali effettuati possono essere considerati necessari per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. *e*), del RGPD) contemplato dall'ordinamento (art. 97 Cost.; art. 1, l. n. 241/1990; artt. 1, 10 e 11, d.lgs. n. 165/2001). Tuttavia, dalle risultanze istruttorie è emerso che il titolare del trattamento effettuava, mediante detto sistema, operazioni di trattamento di dati personali riferiti ad utenti e dipendenti non conformi alla disciplina in materia di protezione dei dati personali, con riguardo sia al quadro normativo vigente al momento della messa in funzione del sistema (risalente al 2015), sia a quello delineato dal RGPD e dal decreto legislativo n. 101/2018. In particolare, è stato accertato che in nessuna delle fasi di prenotazione/erogazione del servizio gli utenti ricevevano informazioni circa i trattamenti dei dati personali loro riferiti effettuati dall'Ente. Analogamente, non è risultato essere stata resa ai dipendenti la dovuta informativa circa le modalità e le finalità delle operazioni di trattamento rese possibili dal sistema, né in forma individualizzata, a ciascun lavoratore, né con documenti informativi resi noti alla generalità dei dipendenti (artt. 5, par. 1, lett. *a*) nonché 13 e 14 del RGPD e, non diversamente, il previgente art. 13 del Codice; cfr. quanto stabilito in Corte EDU, Grande Camera, case of Bărbulescu v. Romania, ricorso n. 61496/08, 5 settembre 2017).

Peraltro, con riguardo alla funzione di estrazione di *report* e statistiche sull'erogazione dei servizi, il Garante ha precisato che tale trattamento avrebbe potuto integrare un controllo a distanza sui lavoratori da parte dell'Amministrazione ed ha al riguardo dichiarato che, nel perseguimento delle specifiche finalità, il trattamento debba avvenire nell'osservanza delle condizioni di garanzia prescritte dall'art. 4, comma 1, l. n. 300/1970 (accordo sindacale o autorizzazione pubblica), anche per effetto del rinvio operato dall'art. 114 del Codice, che costituisce condizione di liceità del trattamento dei dati personali (artt. 5 e 6 par. 1, lett. *c*), e 88, par. 2, del RGPD e 114 del Codice).

Inoltre la società fornitrice del sistema, che assicura anche il servizio di assistenza e manutenzione non aveva stipulato con l'Ente un accordo per la protezione dei dati personali. Il Garante sul punto ha chiarito che, ai fini del rispetto della normativa in materia di protezione dei dati personali, assume rilievo identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, in particolare quella di titolare e di responsabile del trattamento (art. 4, par. 1, punto 7, del RGPD e, con riferimento ai trattamenti effettuati sino al 24 maggio 2018, artt. 28 e 29 del Codice). Atteso che le funzioni svolte dall'Ente per assicurare l'assistenza e la manutenzione del sistema comportano anche un trattamento di dati personali di cui lo stesso è titolare (dati personali dei dipendenti ed eventualmente degli utenti che non abbiano effettuato la prenotazione direttamente tramite i servizi della società fornitrice del sistema), il Garante

ha concluso che, anche sotto questo profilo, il trattamento dei dati personali non risulta conforme alla disciplina di riferimento (art. 29 del Codice in relazione ai trattamenti effettuati fino al 24 maggio 2018 e, successivamente, art. 28 del RGPD), dando luogo a una comunicazione illecita di dati personali (cfr. la nozione di "terzo" di cui all'art. 4, par. 1, punto 10, del RGPD; art. 2-*ter* del Codice).

Il Garante ha inoltre ritenuto che le misure tecniche e organizzative adottate dall'Ente non fossero adeguate agli specifici rischi connessi al trattamento; per tali ragioni, ha ingiunto al titolare di conformare il trattamento alle disposizioni menzionate del RGPD e del Codice e di adottare adeguate azioni correttive volte ad eliminare le criticità tecniche e organizzative (provv. 7 marzo 2019, n. 81, doc. web n. 9121890).

13.9. *Comunicazione di dati dei dipendenti a un ordine professionale*

È stato affrontato anche il tema della comunicazione, da parte del datore di lavoro, dei dati personali dei dipendenti per consentire agli ordini professionali l'esercizio delle funzioni disciplinari nei confronti di figure professionali per le quali sia richiesta l'iscrizione ad uno specifico albo.

Nel definire il procedimento – avviato ai sensi dell'art. 2-*ter*, comma 2, del Codice da un'azienda ospedaliera che aveva ricevuto da parte di un ordine interprovinciale delle professioni infermieristiche una richiesta di comunicazione di dati personali dei propri dipendenti in servizio con la qualifica di infermieri (nominativi e residenza) al fine di poter effettuare i controlli previsti dalla vigente normativa (cfr. d.lgs. del Capo provvisorio dello Stato 13 settembre 1946, n. 233, come modificato dalla l. 11 gennaio 2018, n. 3, ricostituzione degli ordini delle professioni sanitarie e per la disciplina dell'esercizio delle professioni stesse) – l'Ufficio ha ribadito che il Codice, come modificato dal decreto legislativo 10 agosto 2018, n. 101, prevede che la comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli di cui agli artt. 9 e 10 del RGPD, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, è ammessa se prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e di funzioni istituzionali e ad essa può darsi corso spirato il termine di quarantacinque giorni dalla comunicazione al Garante senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati (art. 2-*ter*, comma 2, del Codice).

Nel merito della questione sollevata, nel prendere atto che, in base alla disciplina di settore, l'onere di iscrizione all'albo incombe sul singolo professionista (cfr. art. 5, comma 2, d.lgs. CpS n. 233/1946, come modificato nel 2018) e che il quadro normativo applicabile prevede che gli ordini delle professioni sanitarie esercitino istituzionalmente poteri di vigilanza e disciplinari nei confronti di "tutti gli iscritti all'albo", ha concluso che, in tale quadro, non risultano attribuite agli ordini specifiche competenze per il compimento di generalizzate attività di ricerca e raccolta di informazioni personali riferite a soggetti diversi da coloro che abbiano già richiesto l'iscrizione all'albo.

Sotto diverso profilo – impregiudicate le specifiche responsabilità, anche sotto il profilo penale, che incombono su coloro che esercitino le professioni sanitarie in assenza di iscrizione all'albo, il cui accertamento è rimesso ordinariamente in capo ad altri organi pubblici – il datore di lavoro deve svolgere le necessarie verifiche sul possesso dei particolari requisiti previsti per l'accesso a specifici impieghi per finalità

di assunzione e nel corso dell'esecuzione del contratto di lavoro (cfr. art. 88, par. 1, del RGPD), nei limiti previsti dalle norme vigenti (ad es., artt. 43, 46 e 71, d.P.R. n. 445/2000) nonché consultando gli albi professionali che sono pubblici e reperibili anche *online*.

Per le citate ragioni, l'Ufficio ha concluso che non sussistono le condizioni necessarie a legittimare la preventiva e massiva comunicazione all'ordine professionale, da parte dell'azienda sanitaria datore di lavoro, dei dati personali relativi a tutto il personale infermieristico impiegato (cfr. nota 16 gennaio 2019, doc. web n. 9084551).

13.10. *Inconfigurabilità del silenzio-assenso nel procedimento di autorizzazione amministrativa all'installazione ed utilizzo di impianti audiovisivi dai quali possa derivare la possibilità di controllo a distanza dei lavoratori*

L'Ufficio ha fornito riscontro ad un quesito, formulato dal Ministero del lavoro e delle politiche sociali, in relazione ad un'istanza di interpello presentata dal Consiglio nazionale dei consulenti del lavoro, in merito alla formazione del silenzio assenso in caso di mancato riscontro, da parte dell'Ispettorato nazionale del lavoro, ad una richiesta di autorizzazione amministrativa all'installazione ed utilizzo di impianti audiovisivi o altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori.

L'Autorità, nel rilevare che l'art. 4 dello Statuto dei lavoratori considera esplicitamente illecita (e penalmente sanzionabile) l'installazione di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di un controllo a distanza dei lavoratori in assenza delle previste procedure di garanzia, ha rilevato che, in relazione al procedimento di autorizzazione, la cui conclusione è fissata in 60 giorni (d.P.C.M. 22 dicembre 2010, n. 275, tabella B), non è prevista la formazione del silenzio assenso.

Peraltro, l'Ufficio ha chiarito che la procedura autorizzativa pubblica – che deve essere esperita dal datore di lavoro quando sia risultata infruttuosa quella condeterminata con le rappresentanze sindacali – costituisce (anche alla luce dei consolidati orientamenti della giurisprudenza) uno strumento di tutela sostanziale, attraverso il quale l'Ispettorato nazionale del lavoro, contemperando la richiesta del datore di lavoro con la necessità di preservare le libertà fondamentali e la dignità dei dipendenti, valuta, in concreto, la liceità di quanto richiesto, fornendo al datore di lavoro indicazioni e limitazioni circa le modalità e le condizioni di utilizzo di tali sistemi potenzialmente idonei ad effettuare un controllo a distanza dei lavoratori (nota 8 aprile 2019).

13.11. *I trattamenti di dati nell'ambito dell'acquisizione e gestione delle segnalazioni in materia di* whistleblowing

Il Garante ha adottato il parere sullo schema di linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro dell'Anac, ai sensi dell'art. 54-*bis*, comma 5, d.lgs. 30 marzo 2001, n. 165 (Tutela del dipendente pubblico che segnala illeciti), come modificato dall'art. 1, comma 2, l. n. 179/2017.

Il testo, già sottoposto a consultazione pubblica sul sito web dell'Anac, ha recepito le principali indicazioni fornite dall'Autorità nel corso di alcuni incontri tenutisi con i rappresentanti di Anac al fine di garantire il necessario coordinamento tra la disciplina di settore e il quadro normativo in materia di protezione dei dati personali

nell'ambito dalle procedure di acquisizione e gestione delle segnalazioni di presunti illeciti. Ciò anche alla luce della particolare tutela accordata dalla disciplina in materia di *whistleblowing* all'identità del segnalante e, in generale, degli specifici rischi per i diritti e le libertà degli interessati nel contesto lavorativo (art. 88 del RGPD).

In tale prospettiva, le linee guida – rivolte ai datori di lavoro in ambito pubblico, ma contenenti anche indicazioni per l'inoltro di segnalazioni da parte di dipendenti di imprese fornitrici di beni o servizi per la pubblica amministrazione – sostituiranno le precedenti linee guida adottate con la determinazione Anac del 28 aprile 2015, n. 6. Nella prospettiva promossa dal Garante e accolta dall'Anac, le linee guida individueranno le misure tecniche e organizzative di base che i titolari del trattamento devono adottare nell'ambito delle procedure informatiche per l'acquisizione e gestione delle segnalazioni, lasciando comunque agli stessi la definizione del proprio specifico modello di gestione delle segnalazioni, in coerenza con il principio di responsabilizzazione e i principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (artt. 5, parr. 1, lett. *f*), e 2, 24, 25 e 32 del RGPD).

Al fine di rafforzare la tutela che deve caratterizzare il riserbo sull'identità del segnalante e sulle informazioni che facilitano l'individuazione di fenomeni corruttivi nella p.a., il Garante, nel prendere atto del recepimento dei principali suggerimenti formulati durante i lavori – frutto anche degli esiti di un ciclo di attività ispettive condotte nel corso dell'anno che ha consentito di esplorare, presso alcuni fornitori di servizi informatici e titolari del trattamento, le principali funzionalità di alcuni tra gli applicativi per l'acquisizione e gestione delle segnalazioni più diffusamente impiegati nel settore pubblico (cfr. provv. 12 settembre 2019, n. 166, doc. web n. 9147297) –, ha comunque evidenziato alcuni profili di criticità, rispetto ai quali ha segnalato la necessità di integrare e modificare lo schema di linee guida.

Al fine di incrementare l'utilizzo di tale istituto, il Garante ha evidenziato l'opportunità che nelle linee guida vengano meglio circoscritte e definite le condotte oggetto di segnalazione, così da prevenire trattamenti di dati personali non sorretti da un'idonea base giuridica in quanto riferiti a casi non previsti dalla normativa anticorruzione. Si è altresì ritenuto indispensabile provvedere a specificare le modalità per l'esercizio dei diritti degli interessati nella prospettiva della tutela dell'identità del segnalante nonché, allo stesso scopo, a rafforzare le misure tecniche e organizzative, utilizzando, ad esempio, protocolli sicuri per la trasmissione dei dati, abilitando accessi selettivi ai dati contenuti nelle segnalazioni ed evitando che la piattaforma invii al segnalante notifiche sullo stato della pratica, in quanto tali messaggi potrebbero pregiudicare la riservatezza della segnalazione (provv. 4 dicembre 2019, n. 215, doc. web n. 9215763).

13.12. *Il trattamento di dati biometrici dei dipendenti pubblici per finalità di rilevazione delle presenze*

A seguito di numerosi quesiti pervenuti, anche in relazione all'*iter* normativo della legge 19 giugno 2019, n. 56 (recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo), il Garante ha fornito chiarimenti in merito al trattamento dei dati biometrici dei dipendenti per finalità di rilevazione delle presenze, muovendo dal particolare rilievo attribuito dal RGPD ai dati biometrici, ricompresi ora nel novero delle categorie particolari di dati (cfr. art. 9, par. 1, del RGPD).

Entro tale cornice, il trattamento di dati biometrici (di regola vietato) è consen-

tito in ambito lavorativo (sia pubblico che privato) solo quando sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro […], nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. *b*), del RGPD; v. pure, art. 88, par. 1, e cons. 51-53, del RGPD). Il quadro normativo vigente prevede altresì che il trattamento, per poter essere lecitamente posto in essere, debba avvenire nel rispetto delle "ulteriori condizioni, comprese limitazioni" (cfr. art. 9, par. 2, lett. *b*), e par. 4, del RGPD) che, nell'ordinamento nazionale, consistono anche nella "conformità alle misure di garanzia disposte dal Garante", ai sensi dell'art. 2-*septies* del Codice.

Con specifico riguardo al settore del pubblico impiego, è stato precisato che è tuttora in corso l'*iter* di approvazione dello schema di d.P.C.M. recante le modalità attuative della legge 19 giugno 2019, n. 56, in relazione all'utilizzo di sistemi di rilevazione di dati biometrici per finalità di rilevazione delle presenze.

Su tale schema di regolamento e, prima ancora, sullo schema di disegno di legge, il Garante ha reso il proprio parere, ai sensi degli artt. 36, par. 4 e 57, par. 1, lett. *c*), del RGPD, evidenziando criticità con riguardo alla proporzionalità delle misure introdotte con il menzionato intervento normativo. In generale, è stato rilevato che le disposizioni risultano incompatibili con il canone di proporzionalità di cui all'art. 52 della CDFUE in quanto prospettano l'introduzione sistematica, generalizzata e indifferenziata per tutte le pp.aa. di sistemi di rilevazione biometrica delle presenze, in ragione dei vincoli posti dall'ordinamento europeo sul punto, a motivo dell'invasività di tali forme di verifica e delle implicazioni derivanti dalla particolare natura del dato (cfr. provv. 19 settembre 2019, n. 167, doc. web n. 9147290; v. già, audizione del Presidente dell'Autorità nell'ambito dell'esame del disegno di legge C. 1433 recante interventi per la concretezza delle azioni delle pp.aa. e la prevenzione dell'assenteismo, doc. web n. 9080870 e provv. 11 ottobre 2018, n. 464, doc. web n. 9051774).

In merito all'intervento regolatorio in questione, i rilievi formulati dal Garante non possono essere superati neanche dall'eventuale consenso dei dipendenti che, peraltro, non costituisce un valido presupposto di liceità per il trattamento dei dati personali in ambito lavorativo, indipendentemente dalla natura pubblica o privata del datore di lavoro (cons. 43; art. 4, punto 11 e art. 7, parr. 3 e 4, del RGPD; v. l'orientamento consolidato in sede europea, Gruppo Art. 29, parere 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, p. 7 e 26, e le linee guida sul consenso ai sensi del Regolamento UE 2016/679, WP 259, adottate il 28 novembre 2017 e modificate il 10 aprile 2018).

Per tali ragioni è stato rappresentato che, allo stato, il quadro normativo non consente al datore di lavoro il trattamento dei dati biometrici dei dipendenti per la finalità di rilevazione delle presenze (artt. 5, par. 1, lett. *a*) e *c*), art. 6, lett. *c*), nonché art. 9, par. 2, lett. *b*), e par. 4, del RGPD) (nota 24 ottobre 2019) (parr. 2.2 e 3.1.4).

13.13. *Il trattamento di dati nell'ambito di procedimenti disciplinari e delle procedure di protocollazione degli atti*

L'Ufficio ha definito alcuni reclami concernenti il trattamento di dati personali dei dipendenti nell'ambito di procedimenti disciplinari oggetto di non corrette procedure di protocollazione dei relativi atti.

In particolare, in un caso un dipendente di un ente locale aveva lamentato che una nota contenente una segnalazione, da cui avrebbe avuto origine il procedimento disciplinare nei propri confronti, sarebbe stata protocollata "senza gli attributi di riservatezza, così da essere disponibile ad una pluralità di soggetti" e che, in ragione dell'ampia circolazione che il documento avrebbe avuto all'interno dell'amministrazione, la stessa sarebbe stata, successivamente, oggetto di scambio tra il personale dell'ente attraverso messaggi di posta elettronica e *social network*.

All'esito dell'attività istruttoria, il Garante ha ribadito che l'amministrazione, in qualità di datore di lavoro, può trattare i dati personali dei dipendenti che siano necessari per dare esecuzione al rapporto di lavoro o per attuare previsioni di legge e adempiere obblighi correlati alla gestione del rapporto di lavoro mediante il personale incaricato o comunque autorizzato e debitamente istruito in merito all'accesso ai dati (art. 30 del Codice, vedi anche, artt. 4, par. 10, 29, 32, par. 4, del RGPD). Il Garante ha inoltre chiarito, anche con provvedimenti di carattere generale i cui principi si confermano tuttora validi, che devono essere prescelte soluzioni che permettano di svolgere le funzioni di gestione dei dati dei lavoratori in modo da eliminare ogni occasione di non necessaria conoscibilità degli stessi, anche adottando cautele particolari per evitare l'indebita circolazione di informazioni personali in capo a soggetti non autorizzati, non solo verso l'esterno, ma anche all'interno dei contesti lavorativi (cfr. punti 2, 4, 5.1 e 5.3 delle 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, doc. web n. 1417809). In proposito è stato chiarito che il personale "incaricato alle operazioni di trattamento deve essere debitamente istruito in ordine all'accesso e all'utilizzo delle informazioni personali di cui può venire a conoscenza nello svolgimento della propria prestazione lavorativa" (cfr. punti 2, 4, 5.1 e 5.3, linee guida cit.).

In tale quadro, anche nell'ambito dei trattamenti di dati personali effettuati mediante i sistemi informatici di gestione dei documenti, è necessario adottare procedure differenziate e/o riservate con riguardo, ad esempio, a tutti i documenti attinenti ai procedimenti disciplinari dei dipendenti nonché agli atti prodromici all'attivazione degli stessi, in ragione di informazioni delicate che possono essere contenute in tali atti (sul punto, v. anche alcune decisioni con le quali il Garante ha dichiarato illecito il trattamento dei dati personali dei dipendenti da parte di colleghi in ragione della scorretta configurazione del protocollo informatico: provvedimenti 11 ottobre 2012, n. 280, doc. web n. 2097560 e 12 giugno 2014, n. 298, doc. web n. 3318492).

Nel caso di specie, l'ente aveva specificato che la segnalazione, in quanto atto prodromico all'avvio del procedimento disciplinare, e quindi formalmente estranea allo stesso, non dovesse essere soggetta alla protocollazione riservata. Tuttavia, proprio tale mancata valutazione dello specifico contenuto della segnalazione, successivamente utilizzata per dare avvio al procedimento disciplinare a carico del reclamante, e la sua conseguente protocollazione senza gli attributi di riservatezza, ha reso accessibile il documento, contenente informazioni particolarmente delicate riferite ad un collega, ad una pluralità di altri dipendenti non autorizzati allo specifico trattamento, dando luogo a un illecito trattamento di dati personali (nota 26 settembre 2019).

In un altro caso, il reclamante aveva lamentato che, a seguito di un proprio esposto alla Procura generale della Corte dei conti in merito a presunte condotte illecite del comune presso il quale prestava servizio nella gestione dell'affidamento di incarichi a consulenti esterni, sarebbe stato attivato nei suoi confronti un procedimento culminato con l'adozione di una sanzione disciplinare. Ritenendo tale sanzione un atto ritorsivo, in violazione dell'art. 54-*bis*, d.lgs. n. 165/2001, il reclamante aveva

denunciato i predetti fatti all'Anac e, conformemente alla normativa vigente, anche all'Ispettorato per la Funzione pubblica presso la Presidenza del Consiglio dei ministri. A seguito delle verifiche effettuate, l'Ispettorato aveva trasmesso la nota contenente gli esiti dell'istruttoria, indirizzandola all'interessato e al segretario comunale, all'epoca Responsabile della prevenzione della corruzione e della trasparenza.

È stato al riguardo rilevato che il mancato rispetto delle procedure in sede di protocollazione avesse determinato la trasmissione, in copia, della nota in questione a un ufficio cui la comunicazione non era diretta (Servizio gestione del personale), nonché la possibilità che tutti i dirigenti comunali potessero consultare il documento, cagionando un illecito trattamento di dati personali del reclamante. In tale contesto l'Ufficio ha dato rilievo anche alla circostanza che il procedimento, cui la nota dell'Ispettorato della Funzione pubblica faceva riferimento, è disciplinato dalla specifica normativa in materia di tutela del dipendente che segnala illeciti di cui all'art. 54-*bis*, d.lgs. n. 165/2001 (cfr. par. 13.11), che prevede (anche nella versione anteriore alle modifiche intervenute per effetto dell'art. 1, comma 2, l. n. 179/2017) misure volte a proteggere l'identità del segnalante, allo scopo di prevenire l'adozione di atti discriminatori nei confronti dello stesso (nota 13 maggio 2019).

13.14. *I trattamenti di dati da parte del medico competente*

In merito ad un quesito formulato dalla Società italiana di medicina del lavoro (Siml) in ordine al trattamento dei dati personali posto in essere da parte del medico competente ai sensi della disciplina in materia di igiene e sicurezza sul luogo di lavoro, l'Ufficio, richiamando i precedenti dell'Autorità, ha precisato che la disciplina di settore (d.lgs. 9 aprile 2008, n. 81) individua la funzione del medico competente come autonoma rispetto a quella che, pure in tale ambito, deve essere svolta dal datore di lavoro, assegnando specifici e distinti obblighi in capo all'una e all'altra figura, così delineando l'ambito del rispettivo trattamento consentito. In particolare, nello svolgimento dei compiti che la legge gli attribuisce in via esclusiva (attività di sorveglianza sanitaria e tenuta delle cartelle sanitarie e di rischio dei singoli lavoratori), il professionista è l'unico legittimato *ex lege* a trattare in piena autonomia e competenza tecnica i dati personali di natura sanitaria indispensabili per tale finalità, non potendo essere in alcun modo trattate dal datore di lavoro informazioni relative, ad esempio, alla diagnosi o all'anamnesi familiare del lavoratore, se non con riferimento al solo giudizio di idoneità alla mansione specifica ed alle eventuali prescrizioni che il professionista fissa come condizioni di lavoro. Anche sotto il profilo sanzionatorio, il quadro normativo nazionale distingue chiaramente le responsabilità che ricadono sul datore di lavoro da quelle che invece sono direttamente imputabili al medico competente, sia quando opera in qualità di libero professionista o per conto di strutture convenzionate, sia quando opera in qualità di dipendente del datore di lavoro. Sulla base di tali valutazioni, il Garante ha tradizionalmente considerato il medico competente un autonomo titolare e, nonostante gli accertamenti volti a verificare l'idoneità alla mansione specifica del dipendente siano obbligatori per legge e svolti a spese e a cura del datore di lavoro (artt. 39, comma 5 e 41, comma 4, d.lgs. n. 81/2008), essi devono essere effettuati esclusivamente tramite il professionista. Egli è, infatti, l'unico soggetto legittimato a trattare i dati sanitari dei lavoratori per le finalità indicate dalla disciplina di settore, come chiarito dal Garante in un provvedimento nel quale è stato precisato, tra gli altri profili, che il medico competente tratta dati personali di natura sanitaria indispensabili ai fini dell'applicazione della normativa in materia di igiene e di sicurezza

13

del lavoro in qualità di titolare del trattamento (provv. 27 aprile 2016, n. 194, doc. web n. 5149198; ma v. pure, con particolare riguardo alla tenuta delle cartelle sanitarie e di rischio da parte del medico competente e alla diversa attività di tenuta e aggiornamento dei fascicoli personali dei dipendenti da parte del datore di lavoro, le 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, in particolare ai punti 8.1 e 8.4, doc. web n. 1364939; da ultimo, provv. 5 giugno 2019, n. 146, doc. web n. 9124510). Tanto, anche in considerazione del fatto che lo stesso RGPD considera in via autonoma le funzioni del medico competente con riguardo ai trattamenti necessari per le finalità di medicina del lavoro (art. 9, lett. *h*), del RGPD), diversamente dai trattamenti del datore di lavoro necessari per adempiere i propri obblighi normativi in materia di salute e sicurezza sul lavoro (artt. 9, lett. *b*), e 88 del RGPD) (nota 19 marzo 2019).