

Protezione dei dati personali

## Trattamento dei dati lavorativi e protezione dei dati personali nell'Ente locale

di Aldo Monea - Avvocato e Giurista delle Organizzazioni pubbliche e Profit

Il trattamento dei dati lavorativi rappresenta, per le Amministrazioni pubbliche, un "voluminoso" e variegato ambito di trattamento, che, dopo l'avvenuta operatività del Regolamento 2016/679 ed a seguito del D.Lgs. n. 101/2018 che "novella" il D.Lgs. n. 196/2003, continua a richiedere un'attenta cura giuridica da parte di Titolare di trattamento, Responsabile/i di trattamento e (più recentemente) nuovo DPO.

L'articolo intende dare una traccia ragionata dei principali profili della normativa" che si applica ai dati del lavoratore, alla luce del Regolamento europeo e della "novella" sul Codice Privacy.

Questo articolo è rivolto ad approfondire quanto presente, in via diretta, nel Regolamento europeo e nel "rivisitato" Codice nazionale sulla Privacy. Quindi, non si prenderà in esame, ad esempio, quanto disciplinato in altre fonti giuridiche (come ad esempio, i controlli lavorativi del datore che sono disciplinati, al fine di limitare le facoltà concesse, dallo Statuto dei Lavoratori, vale a dire la Legge n. 300/1970 e modifiche e integrazioni) che meritano un approfondimento ad hoc.

### Premessa

A seguito del Regolamento europeo e della novella del Codice, il trattamento dei dati personali del lavoratore attraversa un cambiamento giuridico simile a quello della maggior parte dei trattamenti di dati personali. Da un lato, come qualsiasi trattamento, richiede che il Titolare (e la sua struttura per la *privacy*) ponga in essere un approccio gestionale nuovo che sia conseguente alle mutate "logiche di fondo" introdotte dai recenti testi normativi. Dall'altro lato richiede l'attuazione di regole, sostanzialmente, reiterate e quindi già note, che è augurabile siano, finalmente, applicate.

### Le fonti giuridiche

Il trattamento dei dati del dipendente è regolato, fondamentalmente, da:

- il Regolamento europeo n. 2016/679;
- il D.Lgs. n. 196/2003 per come integrato e modificato, da ultimo, dal D.Lgs. 10 agosto 2018, n. 101;
- le Linee guida e le interpretazioni del Garante per la Protezione dei dati personali, che, pur dettate sotto la vigenza dei precedenti testi normativi, è da ritenere

perdurino nella loro efficacia giuridica, pur dovendo essere da reinterpretare in base al rinnovato quadro normativo.

### I dati personali lavorativi

Parafrasando l'art. 4 n. 1 del Regolamento europeo, è dato personale inerente al lavoratore/trice qualsiasi informazione che:

- riguardi la persona, indenticata o identificabile, del/la lavoratore/trice;
- concerna profili di rapporto tra lui/lei e il datore di lavoro (e la sua Organizzazione);
- sia oggetto di trattamento da parte di quest'ultimo o dei soggetti che operino per conto di lui.

Quanto detto implica, al contrario, che ogni qual volta si trattino dati del/la lavoratore/trice resi anonimi (per effetto della "pseudominizzazione" di cui all'art. 4, n. 5 del Regolamento europeo), gli stessi non sono da considerare più dati personali.

D'altra parte, le informazioni personali sono utilizzate in tutto il ciclo del rapporto del lavoro. Così, ad esempio, le informazioni del lavoratore sono impiegate a fini di c.d. Amministrazione del Personale, in talune attività di Organizzazione (compreso lo

Sviluppo Organizzativo), nella Gestione del rapporto di lavoro, nello Sviluppo delle Risorse umane, nella fase di Valutazione della sua *performance* e nella Sicurezza sul Lavoro (comprese i profili di suo benessere fisico, mentale e sociale sul lavoro).

Si tratta, a ben vedere, di un terreno in cui i rischi di invadenza nella sfera personale del lavoratore/trice sarebbero potenzialmente notevoli, se non intervenisse il Diritto a delimitare l'utilizzo datoriale di poteri, facoltà, sistemi e strumenti.

**Tavola 1 - Esempi di dati del dipendente**

- **Dati anagrafici**
- **Dati retributivi**
- **Dati fiscali e sulle prestazioni sociali**
- **Informazioni relative alle ferie annuali, ai permessi, alle assenze straordinarie/non retribuite**
- **Note informative/di valutazione annuali**
- **Dati su promozioni**
- **Dati su trasferimenti**
- **Dati a fini disciplinari**
- **Dati sulla formazione svolta**
- **Dati a fini di sicurezza sul lavoro (compresi Infortuni sul lavoro)**
- **Posta elettronica o accessi a Internet**
- **Dati del curriculum (o altre informazioni personali professionali/lavorative), messi a disposizione dal futuro dipendente, in occasione del concorso, e che (una volta divenuto, egli, dipendente) formano parte del suo fascicolo personale**

## **I principi generali di trattamento. Profili**

Prima di evidenziare taluni obblighi è opportuno premettere che (anche) al trattamento dei dati lavorativi si applicano, con evidenti conseguenze sul piano operativo, principi generali, nuovi e vecchi, propri di ogni trattamento.

### **I nuovi principi ...**

- “*Accountability*” del Titolare, secondo cui a lui compete di decidere, autonomamente, su modalità, garanzie e, spesso, limiti del trattamento dei dati lavorativi. Inoltre, sempre per effetto di tale principio,

- il Titolare deve essere in grado di dimostrare di avere adottato misure adeguate e efficaci a proteggere i dati personali, elaborando uno specifico “modello organizzativo” (1);

- “*Privacy by default*”, secondo cui anche i dati lavorativi devono essere protetti per “impostazione predefinita”;

- “*Privacy by design*”, in base al quale il dato del dipendente va protetto sin dal momento della progettazione dei sistemi aziendali;

- “*Valutazione del rischio*”, per cui l'impatto negativo sulle libertà e i diritti degli interessati devono essere oggetto di una specifica valutazione (di cui agli artt.

(1) Su tale tema, per un primo orientamento, il mio “Regolamento n. 2016/679: la necessità di uno specifico ‘Modello

organizzativo’ per la protezione dei dati personali” in *Azienditalia*, n. 8-9/2018.

35-36) e, in conseguenza di essa il titolare occorre adottare le misure tecniche e organizzative di sicurezza che ritiene necessario adottare per mitigare tali rischi.

## ... e i vecchi principi

Inoltre, la struttura organizzativa per la *privacy* deve rispettare altresì principi generali, in larga parte presenti nella passata normativa sulla protezione dei dati ed ora espressi all'art. 5 par. 1 del Regolamento europeo. I più significativi ai nostri fini sono:

### - *Liceità e Pertinenza*

In tal senso un trattamento di dati lavorativi è consentito, al datore e ai suoi collaboratori interni e esterni, in quanto le informazioni trattate siano effettivamente legate a legittime facoltà datoriali di trattamento e siano pertinenti rispetto ad esse. Per fare un esempio paradossale ma che rende l'idea: un datore pubblico non potrà conoscere dati sulla famiglia del lavoratore per decidere se far fare una progressione economica o di carriera al dipendente.

### - *Minimizzazione dei dati*

Le informazioni che il datore pubblico tratta devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. In altre parole, egli può raccogliere solo i dati che strettamente servono ai suoi legittimi fini datoriali.

### - *Esattezza dei dati*

Le informazioni che il datore tratta devono essere esatte e, se necessario, aggiornate. Inoltre, secondo l'art. 5 del Regolamento, devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente quei dati che risultino inesatti rispetto alle finalità per le quali sono trattati.

Per fare un esempio concreto, una procedura di progressione orizzontale o verticale si deve basare, su dati esatti e, se necessario, aggiornati.

### - *Liceità, correttezza e trasparenza*

I dati del lavoratore devono essere trattati in modo lecito, corretto e trasparente nei confronti dello stesso. In questo senso, ad esempio, non si potrebbe registrare un colloquio di lavoro tra dirigente e

dipendente, all'insaputa di quest'ultimo, senza averlo cioè informato che quanto sta dicendo viene registrato.

### - *Limitazione della conservazione*

Le informazioni personali sul lavoratore devono essere conservate, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Decorso tale termine, scatta il diritto all'oblio.

## Profili di liceità del trattamento

La condizione di liceità del trattamento di dati lavorativi (cioè che ne rende lecito il trattamento nell'ambito di un'Amministrazione pubblica) segue le regole generali del Regolamento; in particolare quella di cui all'art. 6, par. 1, lett. e) di quel testo, secondo cui il trattamento da parte di un soggetto pubblico è lecito in quanto necessario per l'esecuzione di un compito di interesse pubblico (2). Lo stesso Regolamento (art. 6, par. 3) rimanda poi al Diritto nazionale affinché stabilisca una serie di profili specifici. In questo senso il trattamento in esame segue, in via generale, le norme di settore, quale ad esempio il D.Lgs. n. 165/2001, i CCNL, il Codice di comportamento nazionale e quello locale del dipendente pubblico.

Rispetto a quanto detto occorre aggiungere due precisazioni:

a) un'attenzione giuridica particolare meritano, però, due particolari operazioni di trattamento dei dati personali "comuni" (che, usando la vecchia terminologia nata sotto il vecchio regime normativo, sono da considerare tutti i dati ordinari che non siano "sensibili", "ipersensibili" e "giudiziari"): la "comunicazione" (sulla cui nozione giuridica si veda l'art. 2-ter, comma 4, lett. a) del D.Lgs. n. 196/2003 novellato (3)) e la "diffusione" (su cui si consideri l'art. 2-ter, comma 4, lett. b) (4) di dati c.d. ordinari è possibile solo se le due operazioni di trattamento siano previste (come impone l'art. 2-ter comma 1 del *Codice Privacy*) da una norma di legge o di regolamento. In mancanza, come in passato, si può

(2) Questa sorta di "attrazione" del trattamento dei dati lavorativi dei dipendenti nell'ambito del regime normativo riguardanti i soggetti pubblici in generale è un principio interpretativo dominante, a parte nella primissima applicazione della normativa italiana sulla *privacy*, in cui qualche interprete (rimasto isolato su tale profilo) aveva sostenuto che al trattamento dei dati lavorativi si applicasse il regime proprio dei soggetti privati (con la conseguenza che fosse, ad esempio, necessario il consenso del dipendente per il trattamento datoriale dei suoi dati).

(3) In tal senso la norma considera "a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati

diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'art. 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;"

(4) È Invece, secondo la norma, "b) 'diffusione', il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

trattarli (art. 2-ter comma 2, secondo periodo) in quanto le predette operazioni siano necessarie per lo svolgimento di “compiti di interesse pubblico” e sia decorso il termine consentito al Garante per negare la liceità delle specifiche operazioni di trattamento;

b) il trattamento dei dati particolari di cui all'art. 9, par. 1 (ad esempio, l'appartenenza sindacale), vale a dire gli *ex* “dati sensibili” della vecchia normativa, sarebbero, in linea di massima, vietati.

Tuttavia, secondo quanto previsto dal par. 2 lett. b) della disposizione citata, tale trattamento di dati lavorativi “particolari” è lecito ove sia necessario per assolvere obblighi ed esercitare diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, sicurezza sociale e protezione sociale (5).

## Il quadro organizzativo intorno al trattamento dei dati lavorativi

In un precedente articolo (quello citato in nota 1) si è già avuto modo di approfondire, specificatamente, del cambiamento organizzativo imposto, in via generale, dal Regolamento europeo. Qui si possono aggiungere alcune rapide considerazioni specifiche al tema qui in esame.

In linea di massima, il datore di lavoro e le figure impegnate nel trattamento dei dati lavorativi devono trovare “spazio” nella struttura organizzativa per la *privacy*, incardinandosi nella compagine organizzativa prescelta del Titolare del trattamento. In particolare:

a) Datore di lavoro e dirigenti (ove questi ultimi siano soggetti distinti dal primo), in quanto trattino dati personali di dipendenti, devono, prevedibilmente, “inglobarsi” (6) nella figura di:

- un (eventuale) responsabile interno (di cui all'art. 28 del Regolamento) o

- un (eventuale) *sub*-responsabile di trattamento (di cui all'art. 28 par. 4) o

- un (eventuale) delegato di trattamento del Titolare o del Responsabile di trattamento (di cui all'art. 29).

b) In ogni caso, le altre figure di impiegati pubblici che, come tali, trattano informazioni personali di dipendenti devono essere “ufficializzati”, ai fini della protezione *privacy*, come delegati di trattamento ed essere istruiti allo scopo.

c) Il Responsabile della protezione dei dati (RPD o, acronimo inglese, DPO) deve tenere presente che il suo ambito di “consulenza” riguarda pure il

trattamento dei dati lavorativi. E ciò sia per la consulenza che deve offrire al titolare del trattamento e ai responsabili di trattamento sia per il rapporto che deve gestire con i dipendenti degli Enti locali in quanto soggetti “interessati” che possono rivolgersi a lui per informazioni.

d) Un altro profilo da tenere presente è che eventuali figure esterne all'ente, che per conto di esso trattano dati lavorativi di dipendenti, dovranno essere ufficializzate, anch'esse, come responsabili trattamenti o come delegati di trattamento. In questo caso, esempi di soggetti sono quegli esperti che fanno parte del Nucleo di valutazione o, ad esempio, eventuali consulenti amministrativi del lavoro, psicologi del lavoro, consulenti di organizzazione, talora anche formatori (in quanto siano messi a conoscenza di specifici dati di singoli dipendenti) e ogni figura simile che si trovi a dover trattare informazioni personali dei dipendenti.

e) Un elemento da evidenziare (analogo a quanto previsto in precedenza in merito alla figura dell'incaricato di trattamento) è che (come si ricava implicitamente dall'art. 2-*quaterdecies* del Codice Privacy) eventuali Società o soggetti diversi dall'individuo che trattino dati personali lavorativi per conto dell'ente devono essere individuate come Responsabili di trattamento e non come semplici delegati di trattamento.

f) Stesso discorso rispetto a quanto detto in questo paragrafo vale per coloro che facciano parte, internamente o esternamente, della struttura organizzativa per la Sicurezza sul Lavoro (datore, dirigente e preposto per la sicurezza). Si tenga presente, a questo proposito, che il “datore di lavoro per la sicurezza” potrebbe essere (e molto spesso è) soggetto diverso dal datore di lavoro inteso in senso strettamente lavoristico, quindi da scindere anche a fini *privacy*. Sempre in ordine alla compagine organizzativa di prevenzione infortuni si ricordi di far emergere, nell'ufficialità della struttura per la *privacy*, anche le ulteriori figure che collaborano a fini di prevenzione degli infortuni, quali, ad esempio, medico competente e chi fa parte del Servizio di Prevenzione e Protezione (responsabile/addetti).

## Due adempimenti da curare

Il trattamento dei dati lavorativi deve essere svolto nel rispetto degli obblighi propri di ogni normale trattamento. Essendo superfluo ripetere profili che saranno sicuramente già noti al lettore, in questa sede si evidenzieranno solo due profili di obbligo che

(5) Il tema non è approfondibile in questa sede, ma richiederebbe ulteriori considerazioni in ordine al raccordo tra le norme di cui alla predetta disposizione con l'art. 2-*sexies* del Codice.

(6) Considerando la struttura descritta a pag. 1118 di “Regolamento n. 2016/679: la necessità di uno specifico ‘Modello organizzativo’ per la protezione dei dati personali”, op. cit.

assumono, nel trattamento qui in esame, una particolare specificità.

## **a) L'informativa**

L'obbligo di dare un'informativa è divenuto, sotto il regime del nuovo Regolamento europeo, un adempimento di primissimo piano perché cardine della Trasparenza, a sua volta caratteristica della nuova disciplina sulla protezione dei dati personali. Approfondendo la cosa, nell'ambito del rapporto di lavoro, dare l'informativa al lavoratore/trice-interessato/a significa mettere quella persona a conoscenza di una serie di profili del trattamento che il datore di lavoro sta svolgendo sui suoi dati personali (senza che, sostanzialmente, egli/ella si possa sottrarre ove voglia continuare ad essere parte di un rapporto di lavoro pubblico).

In questo senso, secondo le regole generali, va dunque applicato l'art. 13 del Regolamento riguardante l'informativa di dati personali raccolti presso l'interessato-lavoratore. In special modo, secondo chi qui scrive, va assicurata l'informazione su:

- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali (inserendo eventuali soggetti esterni, quali ad esempio gli Istituti previdenziali);
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza di una serie di diritti a suo favore.

## **b) Il rispetto dei diritti del lavoratore (art. 12 e segg. del Regolamento)**

A favore del/la lavoratore/trice originano tutti i diritti propri dell'"interessato" precisati nel Regolamento. In questa sede si ricordano, come più significativi ai nostri fini, i seguenti:

### **• Diritto di accesso dell'interessato (art. 15 del Regolamento europeo).**

Tale basilare diritto consiste, essenzialmente, nel consentire al lavoratore pubblico di poter sapere dal datore di lavoro (non tanto, come dicono le regole generali, l'esistenza di un trattamento, ma più concretamente) cosa viene trattato su di lui/lei ed ulteriori informazioni di corredo (quali, ad esempio, i destinatari, il periodo di conservazione dei dati e così via).

### **• Diritto di rettifica (art. 16 del Regolamento europeo)**

Il dipendente ha il diritto di ottenere, senza ingiustificato ritardo, dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano. Inoltre, tenuto conto delle finalità del trattamento, l'interessato ha il

diritto di ottenere l'integrazione dei dati personali incompleti, fornendo una dichiarazione integrativa.

È da segnalare, invece, che è venuto meno il vecchio limite alla rettifica (di cui all'art. 8 del vecchio testo del Codice) da parte dell'interessato in ordine ai propri dati valutativi soggettivi. Questo significa che, nel nuovo regime normativo, pure tali dati sono integrabili da parte del lavoratore. Ciò è da ritenere sia da intendere nel senso che per effetto di tale diritto il lavoratore non possa sostituirsi al valutatore (ad esempio, un Nucleo di valutazione), ma bensì avanzare pretese di rettificazione, che dovranno essere vagliate da chi di dovere.

### **• Diritto cancellazione (art. 17 del Regolamento europeo)**

Il lavoratore ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza (ingiustificato) ritardo. Nel caso dei dati di lavoro ciò significa che il titolare del trattamento ha l'obbligo di portare nell'oblio quei dati che non più necessari rispetto alle finalità di raccolta (lett. a) o che sono trattati illecitamente (lett. d).

### **• Diritto di limitazione di trattamento (art. 18 del Regolamento europeo)**

Un breve accenno merita tale diritto che consente al lavoratore di ottenere che sia limitato il trattamento dei propri dati (art. 16 del Regolamento europeo), qualora ricorrano le situazioni descritte ai numeri da a) a d) della disposizione citata. Le più significative previste dalla norma sono che:

- il lavoratore-interessato contesti l'esattezza dei dati personali. In tal caso il datore non può trattarli per il periodo necessario per verificare l'esattezza di tali dati personali;

- il trattamento sia illecito (ad esempio, si pensi a dati non lecitamente trattabili da parte del datore) e l'interessato chieda che ne sia limitato l'utilizzo.

- l'interessato si sia opposto ai sensi dell'art. 21. Secondo le regole generali, l'interessato si può opporre al trattamento adducendo (art. 21, paragrafo 1) motivi connessi alla sua situazione particolare. In tal caso egli ha diritto alla limitazione del trattamento durante la fase di verifica.

### **• Diritto di opposizione dell'interessato (art. 21 del Regolamento europeo).**

In questo caso all'opposizione del lavoratore- "interessato" ai propri dati, il titolare di trattamento risponde solo cercando di dimostrare l'esistenza cogente del primo a procedere al trattamento. Il caso potrebbe essere, ad esempio, che il lavoratore (ad es., un dirigente) contesti che un certo trattamento di dati personali del lavoratore avvenga su

propri dati di natura psicologica (con la consulenza di psicologi) e si opponga, mentre il titolare adduca, a motivo legittimo, il mantenimento del benessere psicologico del dipendente e dei suoi collaboratori.

## I precedenti "input" del Garante

Pure non essendo regole rintracciabili né nel Regolamento nel Codice si ritiene di fare cosa utile ricordando ai lettori alcuni degli specifici testi emanati dal Garante negli anni passati e che possono essere considerati ancor oggi vigenti, pur sottolineando che sarebbe opportuna una qualche rivisitazione da parte del Garante.

### Linee Guida sui lavoratori pubblici

Il principale documento sono le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (Deliberazione 14 giugno 2007, n. 23)

Tale documento fornisce sotto forma di "indicazioni e raccomandazioni" una serie di prescrizioni sul trattamento di dati personali di lavoratori.

In questo senso l'Autorità considera, in modo particolare:

- l'applicazione dei principi di liceità, pertinenza, trasparenza;
- la corretta individuazione delle figure che presiedono o che realizzano operativamente le operazioni di comunicazione e diffusione di dati;
- le particolari cautele sul trattamento di quelli che oggi sono i "dati particolari" di cui all'art. 9 (e che prima erano denominati "dati sensibili");
- l'utilizzo dell'operazione di "comunicazione" di dati lavorativi, ivi compreso nel rapporto con le organizzazioni sindacali;
- la "diffusione" di dati personali di lavoratori. In questo senso vengono introdotte raccomandazioni in ordine ai dati relativi a concorsi e selezioni, a dati su retribuzione o a titolarità di cariche incarichi pubblici, andati in materia di organizzazione degli uffici contenenti informazioni personali di lavoratori;
- dati idonei a rivelare lo stato di salute, ivi compresi i profili di denuncia all'Inail e le visite medico legali.

Un profilo di particolare attenzione merita il paragrafo "7. *Impronte digitali accesso luogo di lavoro*" a questo proposito è da dire che il garante si è già espresso in ordine ad un tema che, recentemente, è ritornato nel dibattito pubblico, quale quello del controllo delle presenze dei dipendenti mediante la raccolta di dati biometrici, quali ad esempio impronte digitali o similare. È da ricordare questo proposito che

il garante in quell'occasione si è espresso in maniera estremamente negativa sostenendo l'interpretazione secondo cui è "privo di giuridico fondamento l'utilizzo di sistemi di rilevazione delle impronte digitali per verificare l'esatto adempimento di prestazioni lavorative, ove siano attivabili misure convenzionali non lesive dei diritti della persona quali, ad esempio, la posizione di firme anche in presenza di eventuale personale incaricato, fogli di presenza o sistemi di timbratura mediante badge magnetico". Questo significa che ogni eventuale tentativo di installare sistemi tecnologicamente avanzati ma anche, potenzialmente, invasivi della *privacy* del dipendente è giuridicamente lecito (secondo il Garante) solo qualora nell'ente non siano concretamente efficaci altre modalità di controllo.

Il testo in esame, quindi, pur essendo bisognoso di aggiornamento (se non altro per la mutata terminologia presente nel Regolamento europeo e nel Codice e nella numerazione dei riferimenti legislativi oltre che del nuovo testo della Legge n. 300/1970) è da ritenere possa essere tuttora considerato un testo interpretativo alquanto utile al datore di lavoro.

### Linee Guida internet e posta elettronica

Altro fondamentale testo da segnalare è quello avente come titolo "*Lavoro: le linee guida del Garante per posta elettronica e Internet*" (deliberazione 1° marzo 2007, n. 13). Esso tende a inquadrare, come si evince dal titolo, l'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro, fornendo numerose chiavi di interpretazione.

L'aspetto certamente di maggiore importanza è rappresentato dall'"obbligo" posto dal Garante di adottare un disciplinare interno, che sostanzialmente un codice interno proveniente dal datore di lavoro in materia di corretto utilizzo, da parte del lavoratore, di posta elettronica di Internet. In questo senso il datore deve chiarire, preliminarmente rispetto ai controlli sulla strumentazione elettronica, numerosi profili di tale attività.

In particolare, secondo il documento, il datore deve, ad esempio, esplicitare:

- quali e quanti comportamenti di navigazione sono tollerati;
- la misura dell'utilizzo, consentito al lavoratore, per ragioni personali di servizi di posta elettronica di Internet;
- se, in quale misura e quali siano le specifiche ragioni per cui il datore potrebbe effettuare controlli datoriali;
- le conseguenze, anche di tipo disciplinare, che il datore di lavoro si riserva di trarre qualora constati

che la posta elettronica e la rete Internet siano utilizzate indebitamente;

- le soluzioni per assicurare, con la cooperazione del lavoratore la continuità dell'attività, qualora il lavoratore sia assente.

Sono, poi, espressi dal Garante una serie di profili relativi all'organizzazione al fine di prevenire l'accesso a dati personali gli spazi di memoria segnati dipendenti nel corso di interventi di manutenzione del sistema elettronico.

Sono poi segnalati prescrizioni in ordine alle misure tecnologiche da adottare a carico del datore di lavoro in ordine alla navigazione in Internet e all'utilizzo, in specifico della posta elettronica (distinguendo tra un ambito pubblico lavorativo è quello privato del dipendente) da parte del lavoratore.

Il testo in esame richiederebbe, tuttavia, un aggiornamento specie alla luce della modifica normativa introdotta in materia di controlli datoriali

## **Profili ulteriori**

Infine, si segnalano, in modo rapido, alcune norme da tenere, comunque, presenti.

### **Non utilità giuridica del consenso del lavoratore**

Riconfermando un'interpretazione, assolutamente maggioritaria, nata sotto il vecchio regime, è da ritenere che il trattamento di dati lavorativi dei dipendenti pubblici da parte del datore di lavoro pubblico, non sia soggetta a consenso. In passato ciò reggeva sul vecchio testo dell'art. 18 comma 4 del Codice (che esplicitamente non richiedeva il consenso per trattamenti da parte di soggetti pubblici, con eccezione di quelli sanitari), ora essendo stato abrogato tale norma è da ritenere che valga la regola generale secondo anche il trattamento dei dati lavorativi da parte del titolare pubblico rientri nella previsione di cui all'art. 6 par. 1, lett. c) (7). In ogni caso potrebbe valere, a non comportare il consenso del lavoratore, anche quanto previsto dall'art. 6 par. 1, lett. b) (8)

### **Un futuro codice deontologico**

L'art. 111 (*Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro*) del Codice prefigura (ma visto che la norma era già presente nel precedente testo, si potrebbe dire auspica) che il Garante promuova, ai

sensi dell'art. 2-*quater*, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'art. 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.

### **Informativa in caso di ricezione di curriculum spontaneo (art. 111-bis del Codice)**

È stata reiterata, anche nel nuovo regime normativo, la disposizione di cui all'art. 111-bis del Codice (*Informazioni in caso di ricezione di curriculum*) la quale prevede che, nei casi di *curricula* inviati spontaneamente dagli interessati al fine di un futuro rapporto di lavoro, l'informativa di cui all'art. 13 del regolamento sia necessaria solo al momento del primo contatto utile con l'interessato, così sgravando i datori pubblici (come quelli privati) di un onere eccessivo.

### **Cautela nel telelavoro (art. 115 del Codice)**

Si segnala che l'art. 115 (*Telelavoro, lavoro agile e lavoro domestico*), come già faceva il precedente Codice, sottolinea l'obbligo del datore di lavoro pubblico di garantire il rispetto della sua personalità e della sua libertà morale.

### **Resta il divieto di indagini illecite**

L'art. 113 (*Raccolta di dati e pertinenza*) del Codice, come in passato, si limita a riconfermare, rinviando a quanto già disposto, all'articolo 8 della Legge 20 maggio 1970, n. 300 (*Divieto di indagine sulle opinioni*).

### **Reiterata la norma sul controllo a distanza**

L'art. 114 (*Raccolta di dati e pertinenza*) codicistico (come già in precedenza) rimanda all'art. 4 della Legge 20 maggio 1970, n. 300 (*Divieto di indagine sulle opinioni*).

## **Considerazioni conclusive**

Il trattamento dei dati lavorativi da parte del datore di lavoro pubblico è un ambito di particolare rilevanza ai fini della *privacy* del lavoratore. Questo perché, stante le crescenti esigenze di organizzazione/gestione/sviluppo delle risorse umane, il datore di lavoro tende, potenzialmente, ad utilizzare quanto più possibile (con rischi di invasività) i dati personali del lavoratore.

(7) La disposizione prevede che: "c) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare di trattamento".

(8) Tale seconda disposizione prevede che: "c) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte (...)".

Il recente cambiamento normativo non ha dedicato significative norme specifiche sul tema, rendendo particolarmente complesso il compito dell'interprete, che deve applicare, ad una tematica molto specifica, norme di carattere generale. Non riscontrandosi neppure novità "rivoluzionarie" in merito, questo tempo *post-* Regolamento europeo può essere utile utilizzare per sanare

molte delle carenze applicative che perdurano sul rapporto tra trattamento dei dati del lavoratore e *privacy*.

Il quadro esposto questo articolo rappresenta solo una sorta di promemoria (ci si augura utile agli Enti) per un approfondimento giuridico che gli attuali e futuri DPO devono fare accanto ai Titolari ed ai Responsabili di trattamento.

E-BOOK

**COLLANA:** Pubblica amministrazione ed Enti locali

## Protezione dei dati personali e GDPR: dai precetti giuridici ai processi organizzativi

**DPO e altri profili professionali - Processi e prassi - Modello operativo efficace e compliant rispetto al General Data Protection Regulation**

di Giuseppe Nucci



L'entrata in vigore, il 25 maggio scorso, del **regolamento europeo 2016/679/UE**, Regolamento generale sulla **protezione dei dati personali (RGDP o GRDP** -secondo l'acronimo inglese-) segna una pietra miliare nello sviluppo di un quadro regolatore armonizzato a livello europeo, in uno dei settori più sensibili della **tutela dei diritti** umani, quello dei **dati personali**. Il pregio dell'e-book è quello di offrire una **guida pratica** per integrare i precetti del regolamento nei processi organizzativi in modo da fare di un obbligo di **compliance** un'occasione di rinnovo e **modernizzazione delle strutture organizzative**. L'Autore dettaglia, dapprima, con linguaggio preciso e concreto e con numerosi esempi pratici, **i principi giuridici fondamentali in materia di tutela dei dati personali** contenuti nel nuovo regolamento; analizza, poi, passo per passo, il **ruolo dei vari attori**, fa una **map-**

**patura dei processi**, si sofferma sui vari registri e sviluppa un **modello di integrazione** della protezione dei dati con gli altri controlli, mirato alla prevenzione e gestione dei rischi, attività che costituisce un elemento essenziale *della corporate governance*. Ciò forte della propria esperienza in materia di *audit* interno, preziosa anche nel rilevare gli stretti legami che esistono tra precetti del regolamento in materia di **responsabilizzazione delle figure apicali (accountability del titolare e del responsabile del trattamento)** e gestione del rischio.

Wolters Kluwer, luglio 2018  
pagg. 162, € 24,00  
Codice e-book: 00230554  
ISBN (ebook): 978-88-217-6666-4

**Per informazioni e acquisti**  
• On line [www.shopwki.it](http://www.shopwki.it)