CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

CONTROLLI, RISERVATEZZA E DATI PERSONALI NELL´IMPRESA DIGITALE

Il contributo analizza il rapporto tra controllo datoriale e tutela dei dati personali alla luce del coordinamento tra l'art. 4 dello Statuto dei Lavoratori e il Regolamento UE 2016/679. L'indagine evidenzia come l'evoluzione tecnologica e la diffusione degli strumenti digitali abbiano ampliato le prerogative del controllo a distanza, imponendo una rilettura delle garanzie poste a tutela della dignità e della riservatezza del lavoratore.

di **Giacomo Farinella**
IUS/07 - DIRITTO DEL LAVORO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Martedì 26 Maggio 2026

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

This article analyzes the relationship between employer control and personal data protection in light of the coordination between Article 4 of the Workers´ Statute and EU Regulation 2016/679. The study highlights how technological evolution and the spread of digital tools have expanded the scope of remote monitoring, requiring a reinterpretation of the guarantees established to protect workers´ dignity and privacy.

Sommario: 1. Premessa; 2. Statuto dei Lavoratori e Regolamento UE 2016/679 tra coordinamento e integrazione; 3. Il trattamento dei dati personali nell'impianto regolamentare europeo: principi e condizioni di legittimità del controllo a distanza; 4. Nuovi obblighi datoriali: dall'«accountability» alla Data Protection Impact Assessment (DPIA); 5. L'adeguata informativa quale presupposto per l'utilizzo degli strumenti di controllo; 6. Conclusioni.

1. Premessa

All'interno di una realtà sempre più permeata dal digitale e dall'innovazione tecnologica sorge spontaneo domandarsi se sia ancora possibile parlare di limiti ai controlli datoriali. Nell'attuale contesto lavorativo moderno, infatti, il confine tra l'esercizio del potere di controllo dell'imprenditore e la tutela della privacy[1] del lavoratore è diventato sempre più labile. L'introduzione di strumenti tecnologici sempre più sofisticati ha reso possibile una sorveglianza capillare e costante delle attività dei dipendenti, sia in presenza che da remoto, sollevando rilevanti interrogativi sul rispetto dei diritti fondamentali della persona nel rapporto di lavoro[2].

Con sfumature del tutto inedite rispetto alla disciplina previgente, il jobs act ha introdotto una gestione maggiormente flessibile del rapporto di lavoro subordinato[3], con innovativi risvolti sull'art. 4 St. lav., novellato alla luce di una tutela più incisiva nei confronti del lavoratore, almeno nell'intenzione del legislatore. Pertanto, in questo scenario, il citato art. 4, nella sua corrente formulazione, assume un ruolo centrale nel tentativo di bilanciare le esigenze organizzative e produttive dell'impresa con la salvaguardia della dignità e della riservatezza dei lavoratori. Tale equilibrio deve essere oggi reinterpretato anche alla luce dei principi sanciti dal Regolamento UE 2016/679 (GDPR), che impone regole precise in materia di trattamento dei dati personali.

L'analisi composita delle norme in tema di controlli datoriali e tutela della privacy si rivela essenziale per comprendere le sfide giuridiche e operative poste dall'evoluzione

CamminoDiritto.it
ISSN 2421-7123

digitale del mondo del lavoro. Parlare di una necessaria armonizzazione[4] dei due testi precettivi conferma la necessità di un coordinamento contenutistico e normativo, essendo l'interprete obbligato ad applicare direttamente la fonte regolamentare europea.

La «lettura unitaria»[5] è, altresì, avallata dall'espresso richiamo al Codice della privacy contenuto nel co. 3 dell'art. 4 St. lav. in merito all'informativa obbligatoria che deve essere fornita dal datore di lavoro ai singoli lavoratori in tutti quei casi in cui lo stesso acquisisca dati personali dei suoi subordinati[6]. In quest'ottica, perciò, è essenziale svolgere un'attenta disamina circa l'informazione che deve essere fornita dall'imprenditore, affinché il trattamento – spesso automatizzato – effettuato dallo stesso sia conforme al GDPR ed a tutti i precetti in esso contenuti.

È dato rilevare come l'avvento dell'innovazione tecnologica, anche negli ambienti di lavoro, ha portato a una maggiore facilitazione dello scambio di informazioni e dati personali[7], rendendo l'individuo in ogni momento tracciabile – attraverso, ad esempio, i geolocalizzatori che permettono di individuare fisicamente una persona – ed esposto ad eventuali violazioni della sua riservatezza. Ad oggi, con una massiccia circolazione dei dati non si deve tenere in considerazione solo la circolazione in uscita – in riferimento ai dati personali di cui altri soggetti possano impossessarsi o venirne a conoscenza – ma anche di quella in entrata – in riferimento a quei dati personali che possono casualmente entrare nel possesso di un soggetto invadendo la sfera privata di un altro[8].

Tale ricostruzione ci permette di condividere l'affermazione di chi, in dottrina, sostiene come sia necessario predisporre una disciplina che tiene conto non solo di una piena tutela a livello costituzionale e ordinamentale, ma anche di strumenti tutelativi predisposti dall'Autorità garante per la protezione dei dati personali, dalla contrattazione collettiva o, ancora, dai codici di autoregolamentazione aziendale[9], che dispongano una efficacie ed efficiente tutela del dipendente in merito alla sua sfera privata e personale.

2. Statuto dei Lavoratori e Regolamento UE 2016/679 tra coordinamento e integrazione

Per comprendere quale sia la tutela prestata al lavoratore dalla normativa vigente è necessario fornire, come già anticipato, una lettura integrata tra lo Statuto dei Lavoratori e il Regolamento UE 2016/679. Il datore di lavoro, nell'esercizio delle sue prerogative, quale l'utilizzo dei dati raccolti dei suoi dipendenti, deve conformarsi, perciò, non solo alle disposizioni contenute nella disciplina statuaria, ma anche alle disposizioni contenute nel testo regolamentare, tenendo conto dei principi applicabili al trattamento e dell'adozione di misure idonee volte ad eliminare il rischio di una eventuale lesione dei diritti fondamentali[10]. Invero, la disciplina regolamentare europea lascia liberi gli stati

CamminoDiritto.it
ISSN 2421-7123

membri di prevedere delle norme di dettaglio, ove lo si ritenga opportuno, potendo fissare delle condizioni maggiormente precise e garantistiche circa il «trattamento di categorie particolari di dati personali»[11]; seppur il Regolamento, infatti, non fissa norme dirette a tutelare la figura del lavoratore, lascia comunque spazio al diritto statale e alla contrattazione collettiva, solo per le materie indicate nel medesimo, per disporre «norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro»[12]. Tutto ciò viene enfatizzato dall'art. 88 del Regolamento[13], il quale dispone, altresì, come dette disposizioni debbano essere «appropriate e specifiche a salvaguardia della dignità umana» per garantire la «trasparenza del trattamento»: questo dimostra come, in realtà, coloro che vogliono predisporre una normativa settoriale non possono derogare ai principi del Regolamento, ma possono solamente integrarlo e armonizzarlo attraverso gli accordi di prossimità[14] o la legge nazionale[15]. A ben vedere, la necessità di un'armonizzazione dei due testi normativi era sentita ancor prima dell'emanazione del GDPR e aprioristicamente dell'espresso richiamo al Codice della privacy nel co. 3 dell'art. 4 St. lav.[16].

Il legislatore italiano è intervenuto solo nel 2018, con il D.lgs. n. 101, integrando il GDPR e abrogando, in parte, le norme contenute all'interno del Codice della privacy (D.lgs. n. 196/2003), il quale, ad oggi, prevede solamente un lapidario richiamo all'art. 4 St. lav.

Particolare rilevanza, in tale disamina, assume l'art. 111 del Titolo VIII, dedicato al «Trattamento nell'ambito del rapporto di lavoro», il quale conferisce al Garante privacy la facoltà di adottare «regole deontologiche (…) per le finalità di cui all'art. 88 del Regolamento», ribadendo la necessità di adottare misure idonee per rendere un'adeguata informazione all'interessato. La scelta del legislatore italiano risulta una scelta lungimirante nella misura in cui non solo il Garante privacy ha le competenze tecniche per fissare delle regole settoriali idonee, ma specialmente perché lo stesso è in grado di supportare le necessarie modifiche della disciplina applicativa di fronte al cambiamento della compagine sociale e lavorativa dovuto all'evoluzione tecnologica, rispetto, ad esempio, a una legge nazionale, che ha delle tempistiche tutt'altro che brevi[17].

In tale ricostruzione ha, altresì, valenza significativa il co. 3 dell'art. 4 St. lav., che fa un rinvio esplicito al D.lgs. n. 196/2003, occupandosi, in prima battuta, della raccolta delle informazioni operata dal datore di lavoro e, in secondo luogo, quale condizione necessaria per la raccolta delle stesse, dell'«adeguata informazione» che deve essere data al lavoratore per esercitare il potere di controllo. Il richiamo al Codice della privacy, introdotto dalla riforma del jobs act, conferma la volontà del legislatore nazionale di armonizzare lo Statuto dei Lavoratori con la disciplina sulla protezione dei dati personali, tenuto conto delle modifiche introdotte dal Regolamento[18] e della maggiore considerazione della dignità e riservatezza del lavoratore.

CamminoDiritto.it
ISSN 2421-7123

La riforma del 2015 ha permesso un utilizzo «più agevole» dei dispositivi digitali «nella strumentazione di lavoro» grazie all'eliminazione «dell'autorizzazione sindacale o amministrativa» per l'impiego degli strumenti professionali dati in dotazione dell'azienda [19], attribuendo un nuovo diritto al lavoratore - diritto a un'«adeguata informativa» – affinché possa essere reso edotto in merito alle modalità di utilizzo di detti strumenti e alle procedure di monitoraggio. Ne discende che l'imprenditore, essendo il «titolare del trattamento», deve osservare tutti gli obblighi che il GDPR prescrive, affinché il lavoratore – c.d. interessato – venga messo a conoscenza dell'utilizzo e della raccolta dei propri dati.

3. Il trattamento dei dati personali nell'impianto regolamentare europeo: principi e condizioni di legittimità del controllo a distanza.

Il Regolamento UE 2016/679 ha dato un importante contributo garantistico al diritto alla protezione dei dati personali dell'individuo, indicando una serie di regole e principi imprescindibili nel trattamento degli stessi, ancor più negli ambienti di lavoro.

In considerazione dell'impostazione precauzionale sottesa al GDPR, la legittimità del controllo a distanza deve valutarsi alla luce di un «giudizio bifasico»[20]: in primo luogo, è necessario considerare le condizioni di liceità del trattamento sancite dall'art. 6 del Reg. UE 2016/679 (cd. base giuridica); in secondo luogo, le modalità di attuazione del controllo devono risultare conformi ai principi generali in materia di trattamento dei dati personali, di cui all'art. 5 del medesimo Regolamento.

La base giuridica del trattamento deve soddisfare sei condizioni: il consenso dell'interessato (lett. a))[21] , la necessarietà del trattamento dovuta «all'esecuzione di un contratto di cui l'interessato è parte» (lett. b))[22], all'adempimento di un obbligo legale (lett. c)), alla salvaguardia di interessi vitali (lett. d)), all'«esecuzione di un compito di interesse pubblico» (lett. e)) o al «perseguimento di un legittimo interesse» (lett. f)).

Particolare rilevanza, nel rapporto lavorativo, assume la prima condizione: gli interpreti, infatti, si sono spesso interrogati sulla eventuale necessarietà della manifestazione del consenso da parte del dipendente affinché l'imprenditore possa esercitare il potere di controllo[23]. Tra le tante opinioni nella letteratura giuslavoristica, v'è chi ha dato una risposta negativa, sostenendo che la normativa sulla privacy non possa interferire nella normativa giuslavoristica per due aspetti fondamentali: le finalità del controllo, in quanto già esplicitate dall'art. 4 St. lav., e l'obbligo di informazione, in quanto la normativa lo configura come una comunicazione unilaterale del datore di lavoro verso il lavoratore[24].

CamminoDiritto.it
ISSN 2421-7123

Tuttavia, è doveroso sottolineare come, di fatto, la disciplina statuaria non apporta alcuna deroga al Codice della privacy, anzi, presuppone una implicita e necessaria armonizzazione tra le due normative di riferimento. Si potrebbe ritenere, infatti, che il consenso del lavoratore si possa configurare come una manifestazione di volontà «viziata»[25], dovuta alla posizione di subordinazione dello stesso nel contratto, costretto ad esprimere tale approvazione per ottenere l'instaurazione del rapporto di lavoro, o mantenerlo. Tra l'altro, in dottrina[26], si è sostenuto come l'eventuale dissenso potrebbe determinare un'interruzione del rapporto contrattuale da parte del datore di lavoro[27].

Affinché il consenso possa essere qualificato come "libero", è indispensabile che il lavoratore sia nella condizione di poterlo manifestare o revocare, senza che su di esso possano confluire eventuali effetti giuridici negativi, che incidano sulla «sfera personale o economica dell'interessato»[28]. A parere di chi scrive, perciò, il consenso risulta essere un mero e vano adempimento che non garantirebbe una maggiore conoscibilità del contenuto dell'obbligo informativo del datore di lavoro, tanto più ove lo stesso si avvalesse di formulari o prestampati, che vanificherebbe l'obiettivo a proprio vantaggio. Invero, il consenso potrebbe essere prestato solo in quelle ipotesi che esulano dai controlli datoriali e da cui non discendono conseguenze negative per il lavoratore: si pensi al caso in cui l'imprenditore voglia utilizzare l'immagine dello stesso a fini pubblicitari aziendali[29]. Seppur lapalissiano, è fuori dubbio che il consenso non possa in alcun modo sostituirsi alla procedura autorizzativa sindacale o amministrativa per l'installazione di impianti tecnologici all'interno dei locali aziendali[30].

Nella disciplina previgente del Codice della privacy, invero, veniva previsto un ulteriore presupposto di liceità eccezionale, che sostituiva la manifestazione del consenso: il perseguimento di un interesse legittimo[31], che, ad oggi, trova il suo fondamento anche nell'art. 6 del GDPR. Tale ipotesi eccezionale costituiva un presupposto di liceità del trattamento solo in tutti quei casi in cui individuati dal Garante per la protezione dei dati personali, sempreché venisse rispettata la normativa vigente in materia (D.lgs. n. 196/2003 e Direttiva 95/46/CE).

Il quadro d'insieme cambia in toto con la modifica dell'art. 4 St. lav., che non richiede più il filtro autorizzativo – sindacale o amministrativo – per gli «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa» e «strumenti di registrazione degli accessi e delle presenze», determinando una sottrazione di una quota rilevante dei dati personali dei lavoratori dal previo «vaglio di legittimità», un tempo applicabile alla scelta datoriale di ricorrere a controlli a distanza per necessità organizzative specifiche e finalità determinate[32]. Anche nella disciplina odierna, in materia di trattamento dei dati personali, si richiama il perseguimento di un «legittimo interesse del titolare del trattamento o di terzi»[33], ammesso che «non prevalgano interessi o i diritti e le libertà fondamentali dell'interessato», dovendo garantire, quindi, un bilanciamento tra i poteri datoriali e i

CamminoDiritto.it
ISSN 2421-7123

diritti dell'interessato e una piena conformità ai principi di proporzionalità e sussidiarietà [34].

Si potrebbe pensare che nel co. 2 dell'art. 4 St. lav. si rinunci alla condizione circa il perseguimento di un legittimo interesse, ma così non è, poiché, nella prima ipotesi, gli strumenti sono funzionali allo svolgimento della prestazione lavorativa, nella seconda ipotesi, invece, si suole rilevare la presenza dei lavoratori all'interno dei locali aziendali. Questo permette di rilevare come il fondamento giuridico sia rinvenibile in esigenze «presuntive», imputabili non alla necessità di effettuare controlli sul lavoratore, ma a ragioni di natura organizzativa e produttiva[35].

Il «giudizio bifasico» è caratterizzato, altresì, dai principi individuati dall'art. 5 del GDPR, che devono osservarsi in merito al trattamento dei dati personali raccolti, in conseguenza dell'esplicazione dei controlli datoriali. La lett. a), par. 1, individua, tra i primi, i principi di «liceità, correttezza e trasparenza»: col primo, si richiede che i dati siano acquisiti in conformità a ciò che stabilisce la legge; il secondo e il terzo, invece, fanno riferimento ai principi del diritto contrattuale privato, in merito alla buona fede oggettiva (art. 1375 c.c. unitamente all'art. 2 Cost.), la quale prescrive, infatti, un «obbligo di trasparenza»[36] in capo al datore di lavoro nel rapporto lavorativo. La «trasparenza» trova la sua più significativa esplicazione nel diritto di accesso ai dati raccolti[37], presupposto per esercitare altri diritti, tra i quali quello di rettifica o di opposizione al trattamento.

La lett. b), invece, prescrive l'osservanza del principio di «limitazione della finalità», inteso come obbligo per l'imprenditore di raccogliere i dati per scopi determinati, espliciti e legittimi, che trova la sua esplicazione all'interno dell'adeguata informativa fornita dal datore di lavoro nei confronti del dipendente (co. 3, art. 4 St. lav.), il quale dovrà trattarli «in modo che non sia incompatibile con tali finalità». Giova rammentare, che le informazioni raccolte possono essere trattate anche per finalità diverse, purché siano compatibili con quelle annunciate ab initio[38]. Tuttavia, si potrebbe ritenere che il "test di compatibilità" sembrerebbe essere lasciato alla piena discrezionalità dell'imprenditore; infatti, il Gruppo di lavoro ex art. 29 ha elaborato un criterio valutativo in base alla quale lo stesso si intende superato ove si sia tenuto conto della natura dei dati, della necessità di garantire la correttezza del trattamento, del contesto, della legittima aspettativa degli interessati e del «rapporto tra le finalità per cui i dati sono stati raccolti e le finalità di un ulteriore trattamento»[39]. A parere di chi scrive, dovrebbe configurarsi un'interpretazione restrittiva dei criteri valutativi, dovuta all'invasività e insidiosità dei controlli datoriali informatici, che potrebbero determinare una lesione della sfera privata e intima del lavoratore e, conseguentemente, un trattamento illecito dei suoi dati personali.

CamminoDiritto.it
ISSN 2421-7123

Ulteriormente, tra gli altri principi, spicca, di certo, quello di «minimizzazione dei dati», il quale sancisce che gli stessi debbano essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono stati trattati». Tale disposizione deve essere letta in combinato disposto con il principio di finalità del trattamento, in quanto si richiede che il sistema di controllo datoriale sia «indispensabile e proporzionato» rispetto ai fini perseguiti: l'imprenditore, infatti, deve privilegiare «misure organizzative e tecnologiche» idonee a scongiurare una scorretta utilizzazione dei dispositivi dati in dotazione[40]. In conclusione, dall'art. 5 del GDPR discendono i principi di «esattezza» – per il quale è necessario che i dati siano esatti ed aggiornati –, «limitazione della conservazione» – per il quale i dati non possono essere conservati per un tempo maggiore rispetto a quello necessario per raggiungere le finalità – e «integrità e riservatezza» – per i quali bisogna garantire un'adeguata sicurezza agli stessi.

4. Nuovi obblighi datoriali: dall'«accountability» alla Data Protection Impact Assessment (DPIA)

Una delle novità più significative della disciplina regolamentare europea è rappresentata dalla previsione di una responsabilità del titolare del trattamento/datore di lavoro, il quale dovrà adottare «misure adeguate ed efficaci» per garantire un adeguato trattamento rispondente alle regole sancite e all'efficacia della misura[41].

È l'art. 24 del GDPR che individua gli adempimenti che devono essere eseguiti dal titolare del trattamento, tra cui spicca, infatti, la realizzazione di «politiche adeguate» per garantire la protezione dei dati personali del lavoratore, ove, principalmente, si utilizzino strumenti informatici che siano caratterizzati da un potenziale rischio alla dignità e alla riservatezza[42].

Di non facile comprensione, vista la mancata puntualizzazione del Regolamento, sono di certo le nozioni di «adeguatezza» ed «efficacia»: riguardo alla prima, possono considerarsi adeguate le misure poste in essere dal datore di lavoro ove si tenga conto del contesto lavorativo e circostanze individuali del trattamento; con la seconda, invece, si potrebbe alludere a una necessaria valutazione ex post circa il raggiungimento della tutela del lavoratore[43]. Tutto questo ha come obiettivo non l'inibizione del trattamento dei dati da parte del datore, ma, al contrario, quello di segnare un confine delineato e l'area di liceità del trattamento, affinché si tuteli la posizione del dipendente[44] che, altrimenti, assisterebbe a una gravissima e sproporzionata lesione del diritto alla protezione dei dati personali.

Tra le altre misure, rilevano quelle sancite dall'art. 25, il quale prevede, nei primi due paragrafi, obblighi di privacy by design e privacy by default[45]. Le procedure in esame

CamminoDiritto.it
ISSN 2421-7123

costituiscono il precipitato logico e concettuale dei principi di minimizzazione dei dati e di limitazione della finalità: esse impongono al datore di lavoro, con il supporto indispensabile di un gruppo di tecnici e con l'obiettivo di «progettare e designare un'organizzazione» che garantisca i diritti e le libertà di chi lavora, l'obbligo di programmare e mantenere una strumentazione aziendale che tenga conto dei principi contenuti nel Regolamento[46].

Il par. 1 dell'art. 25, che si occupa della privacy by design, impone al titolare del trattamento di adottare «misure tecniche e organizzative adeguate» per tutelare i diritti dei lavoratori, tra i quali la «pseudonimizzazione» e «minimizzazione». Tali misure possono essere applicate tenuto conto di una serie di criteri, tra i quali lo «stato dell'arte» e i «costi di attuazione», ma anche tenendo conto «della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche». Tali parametri non sono altresì previsti per le misure di privacy by default, che impongono al titolare del trattamento di raccogliere, conservare, trattare e rendere accessibili «solo i dati personali necessari per ogni specifica finalità del trattamento» - obbligo sancito per tutelare il lavoratore da eventuali accessi da parte di soggetti terzi senza il suo consenso.

In conformità al principio di accountability il datore di lavoro, prima di esercitare il potere di controllo a distanza, deve, inoltre, attuare la valutazione d'impatto sulla protezione dei dati (c.d. DPIA, Data Protection Impact Assessment) in tutti quei casi in cui gli strumenti utilizzati possano determinare un rischio per i diritti e le libertà fondamentali del dipendente. Tale istituto, sancito dall'art. 35 del GDPR, prescrive l'obbligo per il titolare del trattamento di confrontarsi con il responsabile per la protezione dei dati[47], affinché, prima dell'installazione dei dispositivi elettronici, si possa realizzare una «mappatura» del modello organizzativo aziendale strumentale, per valutare, ex ante, se gli strumenti informatici possano avere ripercussioni negative sulla dignità e riservatezza del lavoratore [48].

La valutazione d'impatto può risultare indispensabile in tutti quei casi in cui «il trattamento può presentare un rischio elevato» tenuto conto dell'utilizzo di nuove tecnologie, della natura, dell'oggetto e del contesto, nonché delle finalità del trattamento.

Ove il titolare del trattamento sia insoddisfatto dell'esito della valutazione d'impatto privacy, in quanto ritenga che il trattamento non sia conforme ai principi cardini del Regolamento, potrà rivolgersi al Garante per la protezione dei dati personali – ai sensi dell'art. 36 del GDPR – affinché possa esprimere un parere sulla valutazione d'impatto redatta o, comunque, esercitare il suo potere di controllo[49].

CamminoDiritto.it
ISSN 2421-7123

Tale valutazione, inoltre, deve indicare in modo dettagliato i soggetti autorizzati dal titolare del trattamento a prendere visione e trattare i dati personali dei lavoratori, al fine di garantire il pieno rispetto dei principi di trasparenza e accountability, nonché assicurare agli interessati, o ai loro rappresentanti, l'effettivo esercizio dei diritti previsti dagli artt. 15 ss., incluso il diritto di accesso e il diritto di opposizione[50]. In conclusione, si può desumere che il trattamento dei dati effettuato per finalità di controllo ex art. 4 St. lav. sarà strettamente collegato alla condizione di adempimento della valutazione d'impatto privacy dal datore di lavoro, salvo tutti quei casi in cui il trattamento sia «privo di sistematicità, non organizzato, né predeterminato e metodico»[51].

5. L'adeguata informativa quale presupposto per l'utilizzo degli strumenti di controllo.

Il legislatore del jobs act ha novellato l'art. 4 St. lav., introducendo come condizione dell'utilizzo degli strumenti di controllo l'obbligo di dare un'«adeguata informazione» circa le modalità di uso degli stessi da parte del datore di lavoro. Tale condizione, indispensabile per il datore di lavoro, permette l'utilizzo dei dispositivi di controllo «a tutti i fini connessi al rapporto di lavoro», da intendersi, perciò, non solo la vigilanza del lavoratore, ma anche l'esercizio di tutti i poteri datoriali, tra i quali il potere disciplinare[52] . Tale obbligo è strettamente collegato a quello dell'art. 13 del GDPR, il quale indica quali sono tutte le informazioni che devono essere fornite dal titolare del trattamento, ogni qualvolta si proceda a raccogliere i dati personali di un individuo, c.d. interessato[53].

L'informativa risponde a una serie di principi enunciati all'interno della disciplina regolamentare europea, quali, tra i più importanti, la liceità, la correttezza e la trasparenza [54], che impongono l'utilizzo di un «linguaggio semplice e chiaro»[55]. Inoltre, il datore di lavoro deve chiarire quali saranno le finalità del trattamento, che dovranno essere inevitabilmente attinenti alle esigenze organizzative e produttive, alla sicurezza sul lavoro o alla tutela del patrimonio aziendale, per tutti quei dispostivi ex art. 4 co. 1; altresì, dovrà adempiere all'obbligo informativo anche per tutti quei dispositivi utilizzati «per rendere la prestazione lavorativa» o per rilevare gli accessi e le presenze[56].

Se da un lato, la normativa statuaria odierna rafforza certamente i «diritti conoscitivi» del dipendente sottoposto a controllo tecnologico, dall'altro, esclude la necessità di un consenso che deve essere fornito dallo stesso, valorizzando sproporzionalmente l'«autodeterminazione informativa»[57].

Le finalità dell'informativa prevista dallo Statuto dei lavoratori sono diverse da quelle dell'art. 13 del GDPR[58]: nel primo caso, infatti, l'informazione riguarda le «modalità d'uso» dei dispositivi di controllo utilizzati dal datore di lavoro per raccogliere dati sui

CamminoDiritto.it
ISSN 2421-7123

propri lavoratori, utilizzabili anche a fini disciplinari, la cui funzione è insita nel rapporto di lavoro; mentre nel secondo caso, l'informazione ha l'obiettivo di rendere l'interessato (lavoratore) cosciente delle diverse ed eventuali operazioni di trattamento[59]. Da questo non discende un doppio obbligo informativo, altrimenti, da un lato, si andrebbe ad onorare il datore di lavoro in modo sproporzionato e, dall'altro, si contrasterebbero i principi portanti del nostro ordinamento, che dispongono una piena armonizzazione della legislazione nazionale con la normativa comunitaria[60].

L'adeguata informazione al lavoratore garantisce una «verificabilità del corretto procedimento di trattamento dei dati», consentendo allo stesso di individuare errori o manomissioni nell'iter procedimentale e di esercitare pienamente il diritto di difesa contro eventuali illiceità poste in essere dal datore di lavoro[61]. Naturalmente, l'obbligo informativo è un'operazione prodromica rispetto ai provvedimenti disciplinari (o altri tipi di provvedimenti) che il datore di lavoro voglia adottare in merito all'operato del dipendente, ovvero, rispetto alla «raccolta e memorizzazione dei dati»[62].

Nulla si evince, invece, dalla normativa giuslavoristica, sulla modalità e sulla forma in cui l'informazione deve essere fornita, parte della dottrina ritiene che sia sicuramente conveniente un'«informativa a carattere individuale che dia conto in modo mirato delle attività di controllo»[63], cioè ad personam, garantendo che tale obbligo non si riduca a un mero adempimento formale[64] e, in ultimo, spiegando come l'uso del dispositivo sia funzionale al controllo dell'operato lavorativo senza sovrabbondare lo stesso di informazioni inutili o poco sintetiche[65]. In proposito, risulta preferibile – e ampiamente condivisibile – l'adozione della forma scritta, sia per «consentire al lavoratore di poter prendere pienamente atto di quanto in essa contenuto»[66], sia per esigenze probatorie, in particolare, ove nasca un contenzioso giudiziario a causa di un provvedimento disciplinare (che si concluda con un licenziamento), fondato sull'utilizzo dei dati raccolti mediante strumenti di controllo.

Tali premesse non escludono che il datore di lavoro possa scegliere comunque la modalità che più ritiene corrette per adempire al suo obbligo comunicativo, sempreché si osservino i «requisiti essenziali di leggibilità e agevole comprensione da parte del lavoratore»[67]. L'informativa, inoltre, deve contenere gli estremi identificativi del «titolare del trattamento» e del «responsabile per la protezione dei dati»[68], il trattamento giuridico, le finalità, l'arco di tempo in cui gli stessi saranno conservati e l'eventuale diffusione[69].

L'adeguata informativa – al fine di risultare conforme ai requisiti imposti dalla normativa vigente – deve necessariamente riferirsi a tutti gli strumenti attraverso i quali può essere esercitata un'attività di controllo, ivi inclusi quelli destinati allo svolgimento dell'attività lavorativa; essa, infatti, deve contenere una descrizione puntuale delle funzionalità

CamminoDiritto.it
ISSN 2421-7123

essenziali di ciascun dispositivo[70]. Sarebbe sicuramente conveniente per il datore di lavoro inserire nell'informativa quelle condotte che possono determinare un'inadempienza nel rapporto di lavoro e che, conseguentemente, possono costituire oggetto di un provvedimento disciplinare, coordinandole con quelle inserite nel codice di condotta aziendale, la cui mancanza all'interno dello stesso non giustificherebbe l'applicazione della sanzione.

Da ultimo, è opportuno evidenziare che il testo normativo in esame stabilisce espressamente che l'informativa debba essere «data al lavoratore»: questo implica che non è sufficiente una mera divulgazione tramite mezzi indiretti, come la pubblicazione sulla pagina aziendale o l'affissione in bacheca, anche se integrata nel codice disciplinare [71]. Al contrario, il datore di lavoro è tenuto a fornire prova dell'avvenuta conoscenza diretta da parte di ciascun lavoratore, utilizzando modalità idonee a documentare l'effettiva ricezione individuale dell'informativa[72].

6. Conclusioni.

Il diritto alla riservatezza, in quanto diritto non assoluto, rimane esposto ad eventuali «ingerenze» da parte di terzi solo se ricorrono tre requisiti: che sia la legge a concederle, che si persegua almeno una «finalità legittima» e l'ingerenza deve risultare indispensabile all'interno di una «società democratica»[73]. Tale diritto ha assunto una fisionomia inevitabilmente differente nella società digitale, dovuto, principalmente, al costante monitoraggio e profilazione del lavoratore, con la conseguenza di rideterminare una nuova disciplina garantistica della persona[74], che ha dato vita al diritto alla protezione dei dati personali, il quale, tuttavia, non può intendersi come una «prerogativa assoluta», ma deve necessariamente rapportarsi con la sua funzione sociale e con altre libertà fondamentali, rispettando il principio di proporzionalità[75].

Il giudizio di bilanciamento, infatti, trova il suo fondamento nella proporzionalità, che impone un adeguato equilibrio tra ogni eventuale restrizione imposta al diritto al rispetto della vita privata e familiare e il fine che si intende perseguire attraverso tale limitazione [76]. Tale finalità, naturalmente, deve essere non solo concretamente identificabile, ma anche legittima secondo i parametri stabiliti dall'ordinamento: questo presuppone che ogni intervento limitativo su un diritto fondamentale deve essere giustificato da un obiettivo sufficientemente rilevante e giuridicamente valido, e la misura adottata non può eccedere quanto strettamente necessario per il raggiungimento di tale scopo.

Tale giudizio è affidato, nella fase patologica del rapporto di lavoro, al giudice di merito, il quale deve necessariamente apportare un'interpretazione estensiva dell'art. 4 St. lav., tenendo conto delle norme sovranazionali (come già previsto dal co. 3), nonché delle

CamminoDiritto.it
ISSN 2421-7123

decisioni giurisprudenziali della Corte europea dei diritti dell'uomo. L'obbligo di conformarsi alle norme comunitarie garantisce una piena applicazione del diritto europeo su tutto il territorio, imponendo al giudice, altresì, di adottare una decisione che assicuri un'effettiva uniformazione allo stesso[77].

Nelle more del giudizio di bilanciamento gioca un ruolo del tutto marginale la contrattazione collettiva, attraverso cui le parti sociali potrebbero garantire una maggiore tutela al lavoratore sul piano della privacy, impedendo illecite interferenze da parte del datore di lavoro nella vita privata dei suoi sottoposti, dovute, principalmente, alla digitalizzazione del mondo lavorativo ed al conseguente potenziamento del potere di controllo. Alcune associazioni di categoria hanno dibattuto sulla possibilità di introdurre una nuova figura, il c.d. rappresentante dei lavoratori per la privacy, che, in mancanza di una disposizione di legge, troverebbe la sua ratio giustificatrice nella contrattazione collettiva[78]. Il rappresentante privacy, de facto, potrebbe intervenire in una fase antecedente alla consegna dei dispositivi elettronici di lavoro, affinché possa vagliare gli eventuali rischi per la riservatezza del lavoratore dovuti all'utilizzo degli stessi. La prevenzione del rischio derivante da trattamenti illeciti costituisce un obbligo giuridico riconducibile al principio di responsabilizzazione del titolare del trattamento, quindi, anche del datore di lavoro[79]. Tale figura potrebbe agevolare l'adozione di misure volte a garantire un utilizzo della tecnologia rispettoso dei diritti fondamentali e improntato a criteri di umanizzazione dei processi.

Invero, il legislatore comunitario ha cercato, attraverso l'espresso richiamo nell'art. 88 del GDPR, di far assumere un ruolo centrale, e non periferico, alle parti sociali, affinché possano contribuire a garantire una maggiore tutela al lavoratore; tuttavia, si tratta solo di un auspicio, in quanto, alla contrattazione collettiva non viene attribuita la stessa efficacia che è riconosciuta ai codici di condotta[80]. Ne discende, che una piena partecipazione delle organizzazioni sindacali aziendali alla «co-regolazione della materia» risulta sempre più necessaria, nell'obiettivo di uniformare il contenuto degli accordi alla disciplina regolamentare[81].

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] Inteso come «diritto a decidere se rendere pubblici o meno, ed entro quali limiti, propri pensieri, emozioni, comportamenti privati», sul tema, A. Pizzoferrato, I limiti al potere di controllo datoriale nell'era digitale, in Lavoro Diritti Europa, 1, 2023, 2.

[2] Sul punto, tra gli altri, v. A. Trojsi, Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo, inDirittifondamentali.it, 2, 2020, 1414 ss.

[3] M. Ricci, Il ruolo del sindacato tra controllo del datore di lavoro e riservatezza dei lavoratori, in Lavoro Diritti Europa, 1, 2023, 12, precisa, inoltre, che «A differenza del passato, il fulcro del Jobs Act è stato rappresentato da una flessibilità maggiore nella gestione del rapporto di lavoro individuale (ius variandi, i controlli sul lavoratore), ma soprattutto rilevante in uscita, compensata da un favor nell'incentivare i rapporti di lavoro a tempo indeterminato a tutele crescenti rispetto a forme di lavoro temporaneo/precario».

[4] G. Proia, Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione), in C. Pisani, G. Proia, A. Topo (a cura di), Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro, Giuffrè, Milano, 2022, 353, il quale ribadisce che «L'ultimo, e forse più importante, "tassello" della nuova disciplina dei controlli a distanza è rappresentato dall'esplicito rinvio alla disciplina della privacy, il cui rispetto costituisce ulteriore e autonoma condizione per l'utilizzabilità dei dati raccolti mediante il legittimo impiego degli strumenti previsti dai primi due commi dell'art. 4. Il rinvio esplicito mira, anzitutto, a sottolineare la necessità dell'integrazione tra i due apparati normativi. La necessità di tale integrazione era agevolmente ricavabile in via interpretativa già nel quadro normativo preesistente, e lo sarebbe stato anche nella disciplina vigente pure in mancanza di un espresso richiamo».

[5] Si veda ampiamente sul punto A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, Carucci Editore, Bari, 2018, 153 ss.

[6] L. D'Arcangelo, L'obbligo di protezione dei dati del lavoratore: adempimento e sanzioni, in Diritti Lavori Mercati, 1, 2020, 79, sottolinea che «il richiamo alla disciplina del Codice privacy investe il datore di lavoro di un preciso obbligo di tutela ex ante nei confronti della persona del lavoratore e di tutto ciò che lo riguarda, intendendo qualunque informazione personale che sia allo stesso riconducibile o che comunque ne consenta l'identificazione».

[7] Cfr. S. Rodotà, Il mondo nella reta. Quali diritti, quali i vincoli, Laterza, Roma, 2014, 18.

[8] Ibidem.

[9] Cfr. F. Perrone, La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei Dritti dell'uomo e giurisdizione nazionale dopo la sentenza Bărbulescu 2, in Labor, 3, 2018, 290.

[10] Tra gli altri, V. Nuzzo, La protezione del lavoratore dai controlli impersonali, Editoriale scientifico, Napoli, 2018, 105; A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 79.

[11] Sul punto si veda il considerando n. 10 del Reg. UE 2016/679, in cui si precisa come «Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito».

[12] Nel considerando n. 155 del Reg. UE 2016/679 viene esplicitato come «Il diritto degli Stati membri o i contratti collettivi, ivi compresi gli «accordi aziendali», possono prevedere norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per quanto riguarda le condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente, per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei

CamminoDiritto.it
ISSN 2421-7123

vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro».

[13] Il testo dell'art. 88 del Reg. UE 2016/679 riporta in toto il contenuto del considerando 155, indicando, in più, gli obiettivi perseguiti da un eventuale normativa di dettaglio.

[14] Tale possibilità è ancor più marcata dal considerando n. 98 del Reg. UE 2016/679, il quale sottolinea che «Le associazioni o altre organizzazioni rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero essere incoraggiate a elaborare codici di condotta, nei limiti del presente regolamento, in modo da facilitarne l'effettiva applicazione, tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese. In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche».

[15] A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 80.

[16] Invero, il richiamo inserito all'interno dell'articolo è strettamente connesso alla legge delega 183/2014, che trova il suo fondamento nella necessità di «contemperare le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del legislatore», quindi, anche la disciplina in materia di protezione dei dati personali concorre a raggiungere il fine appena citato. Sul punto, G. Proia, Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione), in C. Pisani, G. Proia, A. Topo (a cura di), Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 353/354.

[17] In tal senso A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 82.

[18] Cfr. G. Proia, Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione), in C. Pisani, G. Proia, A. Topo (a cura di), Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 335.

[19] Ivi, 354.

[20] A. Ingrao, Il controllo a distanza realizzato mediante social network, in Labour & Law Iusses, vol. 2, 1, 2016, 108.

[21] Inoltre, il considerando n. 42 precisa che il titolare del trattamento «dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito il trattamento».

[22] Il considerando n. 44 esplica meglio tale condizione, precisando come «Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto».

[23] Per un'attenta analisi v. A. Sitzia, Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore), in Labour & Law Iusses, vol. 2, 1, 2016, 91 ss., il quale sostiene come il consenso presuppone un controllo lecito dell'imprenditore.

[24] Cfr. sul punto A. Maresca, Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore, Ipsoa Quotidiano, 22 febbraio 2016, in dottrinalovoro.it.

[25] A. Topo, D. Tardivo, Hard law e soft law nel diritto dell'Unione Europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore, in C. Pisani, G. Proia, A. Topo, Privacy e lavoro. la circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 98 ss., nel quale si evidenzia che «il lavoratore si troverebbe ad esprimere un consenso non genuino, in ragione della posizione di strutturale inferiorità in cui versa».

[26] Cfr. A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, cit., p. 112.

[27] Conclusione che emerge anche dal Parere 2/2017 sul trattamento dei dati sul posto di lavoro, del Gruppo di lavoro ex art. 29, dell'8 giugno 2017, WP 249, nel quale si evidenzia come «è importante riconoscere che i dipendenti si trovano raramente nella posizione di concedere,rifiutare o revocare liberamente il consenso al trattamento dei dati, vista la dipendenza derivante dal rapporto datore di lavoro/dipendente. Salvo in situazioni eccezionali, i datori di lavoro dovranno basarsi su un fondamento giuridico diverso dal consenso, ad esempio la

CamminoDiritto.it
ISSN 2421-7123

necessità di trattare i dati per un loro legittimo interesse».

[28] A. Topo, D. Tardivo, Hard law e soft law nel diritto dell'Unione Europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore, in C. Pisani, G. Proia, A. Topo, Privacy e lavoro. la circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 99.

[29] Invero, il Gruppo di lavoro ex art. 29 è di opinione differente, ritenendo come in ogni caso non possa essere prestato il consenso da parte del dipendente, anche ove il lavoratore non sia subordinato, ma autonomo. Si veda Parere 2/2017 sul trattamento dei dati sul posto di lavoro, del Gruppo di lavoro ex art. 29, dell'8 giugno 2017, WP 249, p. 4, in cui si sottolinea che «con il termine "dipendente", nel presente parere il Gruppo di lavoro non si riferisce esclusivamente alle persone soggette a un contratto di lavoro riconosciuto come tale ai sensi delle leggi vigenti in materia. Negli ultimi decenni sono diventati più comuni nuovi modelli aziendali serviti da tipi diversi di rapporto di lavoro, in particolare il ricorso a lavoratori freelance. Il presente parere intende trattare tutte le situazioni di rapporto di lavoro, indipendentemente dal fatto che tale rapporto si basi su un contratto di lavoro».

[30] Tale precisazione risulta interessante in merito a un'isolata pronuncia della S. C., Cass. Pen., 11 giugno 2012, n. 22611, che ha sancito una piena equipollenza tra il consenso e la procedura autorizzativa nella misura in cui lo stesso sia prestato dalla totalità dei dipendenti, cfr. sul punto L. Biarella, Videosorveglianza lecita se c'è il consenso dei lavoratori, 13 giugno 2012, in altalex.com. Giova rammentare che, in quanto unica e sola, tale pronuncia è stata dissentita da tutte quelle successive aventi lo stesso oggetto, tra le quali, Cass. Pen., 31 gennaio 2017, n. 22148, nella quale si ribadisce come «non abbia alcuna rilevanza il consenso scritto o orale concesso dai singoli lavoratori, in quanto la tutela penale è apprestata per la salvaguardia di interessi collettivi di cui (…) le rappresentanze sindacali, per espressa disposizione di legge, sono portatrici, in luogo dei lavoratori che, a causa della posizione di svantaggio nella quale versano rispetto al datore di lavoro, potrebbero rendere un consenso viziato».

[31] Previsto dall'art. 24, co. 1, lett. g) del Codice della privacy – articolo abrogato.

[32] A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 113.

[33] Oggi sancito dall'art. 6, par. 1, lett. f), ed inoltre supportato dal Considerando n. 47, il quale sottolinea come «i legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento».

[34] Cfr. Gruppo di lavoro ex art. 29, parere n. 2/2017, nel quale si precisa inoltre che «Prima di usare un qualsiasi strumento di monitoraggio è opportuno effettuare una prova della proporzionalità per valutare se tutti i dati sono necessari, se il trattamento viola i diritti generali alla vita privata di cui godono i dipendenti anche sul posto di lavoro, e le misure da adottare per garantire che le violazioni dei diritti alla vita privata e alla segretezza delle comunicazioni siano limitate al minimo necessario».

[35] Conclusione supportata dalla Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, al punto 15.1, nel quale si precisa che «non dovrebbe essere consentito introdurre e utilizzare sistemi informativi e tecnologie aventi per scopo diretto e primario la sorveglianza dell'attività e del comportamento dei dipendenti. Se l'introduzione e l´utilizzazione di tali sistemi e tecnologie per altri scopi legittimi, quali la tutela dell'attività produttiva, della salute e della sicurezza, o l´efficace gestione di un´azienda o di un ente, comportano indirettamente la possibilità di sorvegliare l'attività dei dipendenti, esse dovrebbero essere soggette alle ulteriori salvaguardie previste nel Principio 21, ed in particolare alla consultazione di rappresentanti dei dipendenti». In tal senso, A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 115.

[36] Per un maggiore approfondimento sul punto v. A. Ingrao, ivi, 122.

[37] A. Ingrao, Il controllo a distanza realizzato mediante social network, op. cit., 110.

[38] Cfr. Considerando n. 50, il quale prescrive, inoltre, che «in tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali».

[39] Parere n. 6/2013 sui dati aperti e sul riutilizzo delle informazioni del settore pubblico adottato il 5 giugno 2013, WP 207, 21/22.

[40] Cfr. A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 124.

CamminoDiritto.it
ISSN 2421-7123

[41] Considerando n. 74, il quale prescrive, inoltre, che «tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche».

[42] I rischi possono derivare da diverse ragioni, sul punto cfr. Considerando n. 75, il quale evidenzia come «I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati».

[43] Cfr. E. Faccioli, M. Cassaro, Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design, in Il diritto industriale, 6, 2018, 561.

[44] G. Franza, Il ruolo dei regolamenti aziendali e della responsabilità sociale dell'impresa: eteronomia e autonomia individuale nel diritto interno, in C. Pisani, G. Proia, A. Topo (a cura di), Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 648/649.

[45] Per un'attenta analisi sull'argomento v. R. D'Orazio, Protezione dei dati by default e by design, in S. Sica, V. D'Antonio, G. M. Riccio (a cura di), La nuova disciplina europea sulla privacy, Wolters Kluwer, Milano, 2016, 79 ss.

[46] A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 131.

[47] Il DPO, ai sensi dell'art. 37 del GDPR, è una figura designata dal titolare del trattamento e dal responsabile del trattamento ogni qualvolta «le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala», come accade nel rapporto di lavoro.

[48] A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 134.

[49] Cfr. sul punto il considerando n. 94, nel quale viene sottolineato, inoltre, come «la mancanza di reazione dell'autorità di controllo entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi compiti e poteri previsti dal presente regolamento, compreso il potere di vietare i trattamenti».

[50] A. Ingrao, La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritmi, in A. Bellavista, R. Santucci (a cura di), Tecnologie digitali, poteri datoriali e diritti dei lavoratori, Giappichelli, Torino, 2022, 133.

[51] R. Rizzi, A. Ventura, La tutela della privacy del lavoratore controllato a distanza, CNDCEC - FNC, Roma, 2019, 47.

[52] Cfr. A. Maresca, Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav., in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 20; P. Tullini, Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?, in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 114, secondo cui deve sussistere un «vincolo di stretta correlazione con lo svolgimento del rapporto di lavoro».

[53] In dottrina, infatti, si sottolinea come le dichiarazioni dell'imprenditore debbano essere necessariamente integrate dagli obblighi informativi regolamentari, che riguardano «le finalità del trattamento e la sua base giuridica, nonché il tempo di conservazione dei dati raccolti», sul punto v. A. Ingrao, Il controllo a distanza sui lavoratori e la

CamminoDiritto.it
ISSN 2421-7123

nuova disciplina privacy: una lettura integrata, op. cit., 118.

[54] Principi sanciti all'interno dell'art. 5 del Reg. UE 2016/679, par. 1, lett. a). Cfr. inoltre A. Maresca, I controlli tecnologici a distanza, in Lavoro e previdenza oggi, 1-2/2021, 17; G. Bandelloni, Social network e protezione dei dati del lavoratore, in Labour & Law Iusses, vol. 9, 2/2023, 65, la quale sottolinea, inoltre, che «se si vuole continuare a leggere l'art. 4 St. lav. come norma a tutela della dignità dei lavoratori, occorre ammettere che tale dignità sia preservata oggi principalmente attraverso regole di trasparenza: ad essere vietato non è il controllo in sé, di regola, quanto il controllo di cui il lavoratore non sia consapevole e informato». Ancora per un'attenta analisi cfr. A. Maresca, Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav., in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 22 ss., nel quale si evidenzia come l'adeguata informativa non sia finalizzata a proteggere il lavoratore dai controlli, bensì, evitare che dall'utilizzo dei propri dati personali possano derivare «potenziali ripercussioni sulla posizione del prestatore nell'ambito del rapporto di lavoro».

[55] Cfr. Considerando n. 39, il quale precisa, inoltre, che «È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento».

[56] L'obbligo di informazione sulle finalità del trattamento trova il suo fondamento anche nell'art. 13, par. 1, lett. c), del Reg. UE 2016/679, che si esplica in modo diverso.

[57] R. Rizzi, A. Ventura, La tutela della privacy del lavoratore controllato a distanza, op. cit., 40.

[58] Cfr. sul punto M. Marazza, Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), in Argomenti di Diritto del Lavoro, 3/2016, 511; G. Proia, Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione), in C. Pisani, G. Proia, A. Topo (a cura di), Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 345; secondo A. Sitzia, Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore), op. cit., 83, tra le due informative c'è «una netta differenza metodologica e valoriale atteso che il primo (lo Statuto dei lavoratori) è portatore di una serie di divieti che inibiscono comportamenti dell'impresa ritenuti lesivi della dignità del lavoratore, mentre il secondo (il Codice privacy, come già la legge n. 675 del 1996) è caratterizzato da una impostazione generale onnicomprensiva, priva di una specifica considerazione per il lavoro».

[59] In quanto si vuole garantire una piena «consapevolezza di essere sottoposto, ancorché legittimamente, ad un controllo, realizzato tecnologicamente», sul punto cfr. A. Maresca, Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav., in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 22.

[60] Cfr. L. D'Arcangelo, L'obbligo di protezione dei dati del lavoratore: adempimento e sanzioni, op. cit., 99/100.

[61] A. Maresca, I controlli tecnologici a distanza, op. cit., 17/18.

[62] Cfr. A. Maresca, Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav., in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 21.

[63] Rispetto a un'informativa di tipo collettivo, che può sacrificare l'intento del legislatore, cfr. R. Rizzi, A. Ventura, La tutela della privacy del lavoratore controllato a distanza, op. cit., 86.

[64] In tal senso G. Cassano, I controlli ex art. 4, L. n. 300/1970, in Il Lavoro nella giurisprudenza, 7/2020, 782; cfr. inoltre A. Maresca,Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav., in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 1.

[65] A. Maresca, I controlli tecnologici a distanza, op. cit., 18; cfr. inoltre M. Marazza, Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), op. cit., 512, il quale sottolinea come la comunicazione sia «una manifestazione del potere direttivo del datore di lavoro»; P. Tullini, Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?, in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 116; A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 119, che evidenzia come la «concisione, intelligibilità e semplicità lessicale sono le caratteristiche che il documento informativo deve possedere».

[66] L. D'Arcangelo, L'obbligo di protezione dei dati del lavoratore: adempimento e sanzioni, op. cit., 100; cfr.

CamminoDiritto.it
ISSN 2421-7123

inoltre A. Ingrao, Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata, op. cit., 120.

[67] In tal senso P. Tullini, Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?, in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit.,117.

[68] Da intendersi, ai sensi dell'art. 4, n. 8, del Reg. UE 2016/679, come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

[69] L'elenco non è esaustivo, vi sono altre informazioni da fornire all'interessato ex art. 13 del Reg. UE 2016/679.

[70] L'obbligo può diversificarsi in base all'ipotesi in cui si prendano in considerazione strumenti di controllo o strumenti di lavoro: nel primo caso, sarà necessario illustrare al lavatore quale sia l'utilizzo del dispositivo effettuato dal datore di lavoro, mentre, nel secondo caso, lo stesso dovrà rappresentare al primo le prescrizioni a cui dovrà attenersi nello svolgimento della mansione. In tal senso, M. Marazza, Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), op. cit., 512 ss.

[71] Cfr. L. D'Arcangelo, L'obbligo di protezione dei dati del lavoratore: adempimento e sanzioni, op. cit., p. 100, il quale ritiene che sia «preferibile che venga portata a conoscenza di ogni singolo lavoratore attraverso l'invio ad personam con successiva sottoscrizione ai fini del suo perfezionamento ed efficacia»; I. Alvino, I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy, in Labour & Law Iusses, vol. 2, 1/2016, 35.

[72] Mentre l'art. 7 St. lav. sancisce la necessaria affissione del codice disciplinare «in un luogo accessibile a tutti», determinando una presunzione di conoscenza nei confronti di tutti i dipendenti, diretti destinatari del potere dell'imprenditore, la finalità nel co. 3, art. 4 St. lav. è differente, in quanto si vuole rendere «edotti» i lavoratori dei controlli datoriali disposti attraverso strumenti tecnologici. In tal senso, A. Maresca, Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav., in P. Tullini (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, op. cit., 25.

[73] A. Sitzia, Lavoro, controlli e privacy: un nouveau parcours per il test di bilanciamento nell'elaborazione della sezione lavoro (e del garante privacy), in Massimario di Giurisprudenza del Lavoro, 4, 2021, 697.

[74] Cfr. A. Topo, D. Tardivo, Hard law e soft law nel diritto dell'Unione Europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore, in C. Pisani, G. Proia, A. Topo, Privacy e lavoro. la circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 81.

[75] Cfr. Considerando n. 4, il quale dispone che «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

[76] Cfr. sul punto F. Perrone, Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Bărbulescu 2, in Labor, 23 febbraio 2018, 3; cfr. inoltre, per un'attenta analisi S. Bertocco, Il conflitto tra sfera privata del lavoratore e libertà di impresa: tutela del patrimonio e dell'organizzazione aziendale nella prospettiva del diritto europeo, in C. Pisani, G. Proia, A. Topo, Privacy e lavoro. la circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 132 ss.

[77] Cfr. F. Perrone, L'effetto conformativo del diritto dell'Unione europea sul diritto del lavoro tra tendenza espansiva e superamento della "grande dicotomia", in Lavori diritti Europa, 3, 2021, 8.

[78] Al pari di detta figura, troviamo il «Rappresentante dei lavoratori per la sicurezza da includere all'interno delle RSU», cfr. A. Ingrao, Controllo a distanza e privacy del lavoratore alla luce dei principi di finalità e proporzionalità della sorveglianza, op. cit., 118.

[79] Ivi, p. 119.

CamminoDiritto.it
ISSN 2421-7123

[80] A. Topo, D. Tardivo, Hard law e soft law nel diritto dell'Unione Europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore, in C. Pisani, G. Proia, A. Topo, Privacy e lavoro. la circolazione dei dati personali e i controlli nel rapporto di lavoro, op. cit., 107.

[81] Ivi, 108.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=11819