La nuova frontiera del web *permette di far comunicare tra loro oggetti connessi in rete*

"Internet delle cose" e sicurezza ma attenzione alla privacy

di **Francesca Masso**, **Silvia Campigotto** e **Beatrice Toniolo,** *B&P Avvocati*

Le nuove opportunità che l'evoluzione tecnologica offre oggi in termini di efficienza produttiva possono essere spesso mutuate e utilizzate anche per una migliore e più efficace gestione della salute e sicurezza sul lavoro. É necessario, però, che la legislazione si adegui alle più moderne applicazioni, promuovendo il dialogo e il coordinamento tra le diverse discipline normative, tra le differenti sensibilità applicative della giurisprudenza giuslavoristica e antinfortunista, nonché tra le (spesso) contrapposte istanze delle parti sociali. In questa ottica, l'articolo propone una riflessione sulla applicabilità del cosiddetto "internet delle cose" nel campo della sicurezza sul lavoro e sulla compatibilità del suo utilizzo con la disciplina – recentemente modificata – del controllo a distanza dei lavoratori.

INTERNET DELLE COSE – SICUREZZA SUL LAVORO – PRIVACY – CONTROLLO A DISTANZA

Internet delle cose

L'*internet delle cose* (in inglese: *internet of things*; si veda il *Box 1*) è formato da una rete di oggetti (spesso chiamati *smart objects*) in grado di comunicare tra loro e di raccogliere dati dal mondo circostante, ma anche di reagire alle informazioni ricevute, "comportandosi" di conseguenza, senza che sia necessario alcun intervento da parte dell'uomo[1]. L'idea di sfruttare le potenzialità della connessione precede la nascita del concetto di *internet of things* e risale già agli anni '80. Tuttavia, il progresso tecnologico ha reso possibile sviluppare questa idea in modi prima difficilmente immaginabili; in particolare, la diffusione sempre più capillare della rete *web*, l'avvento del *cloud computing*, l'aumento delle capacità di calcolo e analisi, le sempre più ridotte dimensioni degli strumenti tecnologici e la diminuzione dei prezzi, sono solo alcuni di questi fattori[2].

Oggi sono connessi circa 9 miliardi di dispositivi e si stima che, entro il 2025, saranno tra i 25 e i 50 miliardi[3]. Secondo la commissione europea entro il 2020 il mercato dell'*internet delle cose* varrà, solo in Europa, più di mille miliardi di euro[4].

---

[1] *In questo senso si parla di* machine to machine *communication (M2M).*

[2] *The Internet Society,* The Internet of things: an Overview. Understanding the Issues and Challenges of a more Connected World*, p. 8; UK Government, Office for Science*, The Internet of Things: making the most of the Second Digital Revolution, A report by the UK Government Chief Scientific Adviser *pp. 15-16, European Commission,* Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination" *pp. 19-20.*

[3] *McKinsey Global Institute,* The Internet Of Things: Mapping The Value Beyond The Hype*, giugno 2015, p. 27. Il numero indicato non comprende computer, smartphone e tutti gli oggetti che sono pensati primariamente per ricevere* input *dall'uomo.*

[4] *Si veda:* https://ec.europa.eu/digital-single-market/internet-things

Box 1

Internet delle cose: cos'è e come funziona

L'espressione "internet delle cose" (*internet of things*, nella versione inglese, spesso abbreviato in IoT) fu usata per la prima volta nel 1999 da Kevin Ashton, per descrivere un sistema nel quale oggetti fisici sono connessi direttamente a internet tramite sensori. Ashton inventò il termine per illustrare le potenzialità delle "etichette intelligenti", ovvero delle etichette connesse tramite Rfid (*radio-frequency identification*) e utilizzate nelle catene di fornitura aziendale per contare e tenere traccia delle merci, senza la necessità di intervento umano. L'*internet delle cose* è formato da una rete di oggetti (spesso chiamati *smart objects*) in grado di comunicare tra loro e di raccogliere dati dal mondo circostante, ma anche di reagire alle informazioni ricevute, "comportandosi" di conseguenza. Le comunicazioni avvengono in genere - ma non necessariamente - tramite l'utilizzo degli strumenti di comunicazione Ip (*internet protocols*) e senza che sia necessario alcun intervento da parte dell'uomo. I dati raccolti sono trasmessi a una piattaforma dove vengono immagazzinati, elaborati ed analizzati, per poi essere messi a disposizione dell'utente tramite un interfaccia. L'*internet delle cose*, dunque, è composto:

- da *hardware* (gli oggetti fisici, quali *smartphone, wearable*, sensori, reti, eccetera)
- e da *software* (piattaforme per la conservazione dei dati, programmi, applicazioni, eccetera).

Per funzionare propriamente, l'IoT necessita di un determinato "ecosistema", in cui in ogni momento e in ogni luogo, chiunque e/o qualunque oggetto può accedere a qualunque servizio utilizzando qualunque rete (tipicamente, *"the internet of things ecosystem*" è descritto utilizzando le seguenti parole chiave: *anything, anyone, anywhere, anytime, any business/any service, any path/any network).*

I miglioramenti la sicurezza sul lavoro: esperienze in Italia e all'estero

I campi di applicazione dell'*internet delle cose* sono potenzialmente moltissimi, spaziando dal settore dei trasporti all'ambito energetico, dalle cosiddette *smart homes* e *smart cities* al settore medico, fino all'agricoltura, alle industrie, ecc. Non meno interessanti sono i possibili utilizzi all'interno dei luoghi di lavoro. Secondo un recente studio del *world economic forum*, infatti, gli operatori, tramite l'impiego di nuove tecnologie all'interno delle industrie, sperano non solo di ottimizzare l'utilizzo delle risorse disponibili e aumentare la produttività, ma anche di apportare miglioramenti alla sicurezza dei lavoratori[5]. In questo senso, sono già in atto interessanti sperimentazioni, soprattutto nei settori estrattivo, chimico, petrolifero, edile e delle costruzioni, nelle acciaierie e simili.

Si pensi a caschetti, scarpe antinfortunistiche, guanti e tute, dotati di sensori capaci di riconoscerne il corretto utilizzo e di inviare al lavoratore un segnale in caso di impiego inappropriato; un po' come avviene quando l'automobile emette un segnale acustico per indicare che le cinture di sicurezza non sono allacciate o non sono allacciate correttamente[6]. Oppure, per i soggetti che prestano la loro attività lavorativa in ambienti potenzialmente pericolosi, un oggetto capace di monitorare costantemente i dati biometrici e la posizione del lavoratore potrebbe inviare direttamente al responsabile un segnale in caso di anomalie nella posizione o nelle condizioni di salute del lavoratore, permettendo, così, di intervenire tempestivamente in caso di incidenti.

Sempre a riguardo di "ambienti critici", occhiali dotati di connessione *wireless* e sensori di geolocalizzazione potrebbero monitorare il livello di esposizione a gas dannosi durante il

[5] *World Economic Forum, Industrial Internet Survey, 2014, citato in: World Economic Forum, Industry agenda:* Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, *gennaio 2015, p. 9.*

[6] *Un esempio in tal senso sono i caschetti che segnalano quando la visiera integrata non è abbassata correttamente.*

Box 2

La realtà aumentata

L'espressione *augmented reality* è stata (abbreviata *Ar*) – coniata nel 1992 dal ricercatore Thomas Preston Caudell della Boeing – e indentifica la tecnologia, associata alla *computer graphic*, che – tramite l'utilizzo di dispositivi elettronici - è capace d'incrementare la percezione sensoriale dell'uomo, inserendo oggetti e informazioni virtuali all'interno del mondo reale. L'aggettivo "aumentata" sta a definire proprio l'aumento del livello di conoscenza offerto all'utente sulla realtà circostante. Le informazioni che aumentano la realtà percepita sono aggiunte su diversi dispositivi, quali *smartphone* e *computer*, che immediatamente sovrappongono sui loro schermi contenuti multimediali (video, audio, oggetti 3D e così via) alla realtà dell'ambiente circostante. In questo senso, la realtà aumentata comporta una combinazione tra ambiente fisico e virtualità, differenziandosi in questo dalla realtà virtuale (*virtual* reality), che, infatti, permette la ricostruzione di uno scenario del tutto separato dalla realtà, capace tuttavia di rendere la sensazione di essere presenti nell'ambiente ricostruito.

turno di lavoro e, in futuro, essere in grado di utilizzare la realtà aumentata (si veda il *box 2*) per permettere agli operatori che lavorano a stretto contatto con macchinari complessi di leggere o ricevere istruzioni senza dover mai staccare lo sguardo dai controlli.

Internet delle cose e Dpi: una forma consentita di controllo a distanza?

L'applicazione di queste tecnologie ai dispositivi di sicurezza può, dunque, aumentare il livello di sicurezza dei lavoratori in modo esponenziale. Tuttavia, allo stesso tempo, ciò comporta - inevitabilmente - che siano raccolti e analizzati ingenti quantità di dati, più o meno sensibili, riguardanti il lavoratore. Si potrebbero, quindi, porre questioni di tutela della *privacy* del lavoratore e di sicurezza - anche con riferimento ai rischi posti da eventuali usi inappropriati - dei dati raccolti[7]. Logico chiedersi, quindi, quali siano le possibili interazioni tra l'applicazione ai dispositivi di protezione individuale di nuove tecnologie potenzialmente, però, lesive della *privacy* e la disciplina dei controlli a distanza, come recentemente modificata dal D.Lgs. n. 151/2015 e se sia possibile (oltre che, come si vedrà più avanti, quanto mai auspicata) una loro coesistenza.

In questa ottica si può tentare di fornire una possibile chiave di lettura della nuova normativa in tema di controlli a distanza per capire se (e in che misura) tecnologie cui si farà (o si potrà fare) largo ricorso nei prossimi decenni possano trovare spazio nel tessuto normativo vigente. È opportuno, dunque, richiamare preliminarmente la nozione, natura e importanza dei dispositivi di protezione nei luoghi di lavoro.

I dispositivi di protezione individuale (Dpi) sono definiti all'art. 74, comma 1, D.Lgs. 81/2008 come «*qualsiasi attrezzatura destinata ad essere indossata e tenuta dal lavoratore allo scopo di proteggerlo contro uno o più rischi suscettibili di minacciarne la sicurezza o la salute durante il lavoro, nonché ogni complemento o accessorio destinato a tale scopo*». Tra i dispositivi di protezione più comunemente utilizzati si possono citare, a titolo meramente esplicativo, caschetto, guanti e scarpe.

---

[7] *Diversi studi indicano* privacy *e* cibersecurity *quali maggiori ostacoli allo sviluppo dell'IoT, unitamente a problemi di ordine diverso quali la interoperabilità, la necessità di infrastrutture adeguate, l'incerto quadro regolamentare. Si vedano: World Economic Forum, Industry agenda,* Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, *gennaio 2015 pp. 10-11; McKinsey Global Institute,* The Internet Of Things: Mapping The Value Beyond The Hype*, giugno 2015, pp. 21-22; UK Government, Office for Science*, The Internet of Things: making the most of the Second Digital Revolution, A report by the UK Government Chief Scientific Adviser*, pp. 16-17; The Internet Society,* The Internet of things: an Overview. Understanding the Issues and Challenges of a more Connected World*, pp. 20 e segg. ; C. Perera, R. Ranjan, L. Wang, S.U. Khan, A.Y. Zomaya,* Privacy of Big Data in the Internet of Things Era.

Box 3

I dispositivi di protezione individuale (Dpi)

I dispositivi di protezione individuale (Dpi) sono definiti all'art. 74, comma 1, D.Lgs. n. 81/2008 come «*qualsiasi attrezzatura destinata ad essere indossata e tenuta dal lavoratore allo scopo di proteggerlo contro uno o più rischi suscettibili di minacciarne la sicurezza o la salute durante il lavoro, nonché ogni complemento o accessorio destinato a tale scopo*». Il loro utilizzo è obbligatorio qualora il rischio non possa essere altrimenti evitato o sufficientemente ridotto ricorrendo a misure di riduzione del rischio "alla fonte" o di riorganizzazione della prestazione lavorativa (art. 75, D.Lgs. n. 81/2008). I dispositivi devono essere adeguati al rischio che intendono prevenire o ridurre, alle condizioni del luogo di lavoro, allo stato di salute e alle condizioni del lavoratore (art. 77, D.Lgs. n. 81/2008).
Il datore di lavoro, previa identificazione e valutazione dei rischi, deve fornire gli appropriati dispositivi di protezione individuale ed esigere che i lavoratori rispettino gli obblighi loro imposti dalla normativa, nonché le direttive aziendali, le istruzioni operative e le misure di prevenzione e protezione (tra cui, appunto, l'uso dei dispositivi di protezione individuale) previsti dal documento di valutazione dei rischi e messi a loro disposizione. D'altro canto, però, al lavoratore è fatto obbligo di osservare le istruzioni impartite dal datore di lavoro in materia di sicurezza, di utilizzare in modo appropriato i dispositivi di protezione individuale forniti e di partecipare ai programmi di formazione e addestramento organizzati dal datore di lavoro (artt. 20 e 78, D.Lgs. 81/2008).

Alcune statistiche condotte a livello europeo[8] riportano come nel 2012 si siano verificati circa 2,5 milioni di incidenti non mortali e 3.515 incidenti mortali sui luoghi di lavoro; molti di questi sono legati al mancato e/o scorretto utilizzo dei dispositivi di protezione individuale (Dpi), nonché all'insufficiente informazione, formazione e addestramento dei lavoratori.
È chiaro, quindi, come l'applicazione dell'*internet of things* ai dispositivi di protezione individuale potrebbe favorire non solo una riduzione degli incidenti o delle conseguenze dannose degli stessi, ma anche una maggiore diffusione della cultura della sicurezza in azienda, sensibilizzando gli operatori al loro corretto utilizzo, abituandoli a "prassi virtuose" (un po', appunto, come è successo agli automobilisti con le cinture di sicurezza). È altrettanto evidente, però, come queste tecnologie, consentendo di raccogliere e trasmettere numerose informazioni sul lavoratore in tempo reale, possano interferire con la normativa sui "controlli a distanza".
La disciplina dei controlli a distanza, contenuta nell'art. 4 dello statuto dei lavoratori, è stata recentemente riformata dal D.Lgs. 151/2015, recante «*Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità*», in attuazione all'art. 1, comma 7, lettera *f)*[9] della legge "delega" 10 dicembre 2014, n. 183. La riforma, sempre tutelando la dignità e la riservatezza dei lavoratori, ambisce, però, ad adeguare il dettato normativo all'evoluzione tecnologica. Quando negli anni '70, infatti, fu introdotto lo statuto dei lavoratori, molte delle innovazioni tecnologiche oggi d'uso comune e necessario (*internet, tablet, smartphone* e pc) non esistevano, né si immaginava che in futuro gli stessi strumenti di lavoro avrebbero assunto una capacità intrusiva nella sfera di riservatezza del lavoratore al pari di impianti e apparecchi, che, proprio perché

[8] *Si vedano sul punto le più recenti statistiche Eurostat, consultabili al link* http://ec.europa.eu/eurostat/statistics-explained/index.php/Accidents_at_work_statistics.
[9] *L'art. 1, comma 7, lettera* f*), legge n. 183/2014 conferiva delega al Governo per la* «revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore».

in grado di determinare un controllo a distanza dei lavoratori, divennero oggetto di specifica regolamentazione[10]. Un aggiornamento della norma si rendeva, dunque, quanto mai opportuno; altrettanto utile sarebbe, quindi, non limitarne la portata, ove non necessario, allo scopo di tutelare valori più elevati.

Anche il testo riformato prevede che l'installazione di strumenti da cui possa derivare anche il controllo a distanza dei lavoratori sia ammessa solo per determinati fini[11] (esigenze organizzative e aziendali, tutela della sicurezza del lavoro e tutela del patrimonio aziendale[12]) e previa concertazione con le rappresentanze sindacali (art. 4, comma 1).

Il comma 2, però, esclude espressamente da questa disciplina gli «*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*" e "*gli strumenti di registrazione degli accessi e delle presenze*». Per questi strumenti, il dato letterale pare escludere tanto l'applicabilità della procedura concertativa, quanto il vincolo dell'impiego dei mezzi, per le sole finalità tassativamente elencate. Il primo ed evidente obiettivo del legislatore è quello di non dover necessariamente ricorrere, in contesti aziendali ove sempre più di frequente la prestazione lavorativa viene svolta su *tablet*, pc e *smartphone*, a un preventivo accordo sindacale per la consegna ai lavoratori di questi strumenti[13].

Occorre fare riferimento alla nozione di "strumenti" di lavoro per verificare l'ambito innovativo, più o meno ristretto, della riforma. Lo strumento di lavoro si pone in una correlazione finalistica rispetto alla prestazione lavorativa; in altri termini, è il mezzo tramite il quale il lavoratore presta la sua attività lavorativa. In accoglimento di questa impostazione, il ministero, nella nota 18 giugno 2015, ha precisato che «*nel momento in cui tale strumento viene modificato (ad esempio con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore di lavoro per controllarne la prestazione. Con la conseguenza che queste "modifiche" possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione*». Il ministero pare, dunque, supportare una nozione di "strumento di lavoro" rigorosa e oltremodo restrittiva che, però, non sembra cogliere nel segno. Come correttamente argomentato «*Il senso della deroga in esame è che, quando ci troviamo di fronte a una funzionalità mista (cioè strumento di lavoro che può consentire il controllo), se lo strumento viene effettivamente utilizzato per lavorare, quest'ultima funzionalità deve caratterizzare lo strumento in via prevalente e determinare l'operatività della deroga*»[14]. Pertanto, l'in-

---

[10] *Sul punto si vedano i contributi di Lorenzo Cairo "*Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con le norme di oggi*", Labour and Law Issues (LLI), Vol. 2, No. 1, 2016, p. 71 e di Ilario 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*", Labour and Law Issues (LLI), Vol. 2, No. 1, 2016, p. 4.*

[11] *L'eliminazione del comma 1 del previgente articolo non ha liberalizzato i controlli a distanza sui lavoratori; oggi, come allora, non è ammessa l'installazione di impianti audiovisivi o altri strumenti con il fine principale di controllare a distanza l'attività dei lavoratori. Il divieto risulta, tutt'oggi, implicitamente ribadito.*

[12] *Tra i fini che, a seguito della riforma, legittimano l'installazione di strumenti dai quali possa anche derivare il controllo a distanza dei lavoratori, si annovera la "*tutela del patrimonio aziendale*". La modifica recepisce la più recente giurisprudenza sui cosiddetti "controlli difensivi". In estrema sintesi, la giurisprudenza era arrivata ad ammettere che controlli effettuati dal datore di lavoro per accertare possibili condotte illecite del lavoratore non fossero soggetti all'art. 4 dello statuto dei lavoratori (si veda la sentenza della Cassazione civile, sez. lav., 3 aprile 2002, n. 4746). Questi controlli, in quanto non contemplati dalla norma, dovevano ritenersi sempre ammessi. La giurisprudenza più recente ha, invece, cercato di giungere a un più equo contemperamento tra le legittime esigenze del datore di lavoro e la tutela della dignità e della riservatezza del lavoratore (si vedano la sentenza della Cassazione civile, sez. lav., 23 febbraio 2010, n. 4375; Cassazione civile, sez. lav., 23 febbraio 2012, n. 2722; Cassazione civile, sez. lav., 1° ottobre 2012, n. 16622; Cassazione civile, sez. lav., 27 maggio 2015, n. 10955). A questo più recente approdo pare ispirata la novella sul punto.*

[13] *Comunicato stampa Ministero del Lavoro 18 giugno 2015 "*Controlli a distanza: Ministero del Lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy".

[14] *Sul punto si veda il contributo di Lorenzo Cairo "*Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con le norme di oggi*", Labour and Law Issues (LLI), Vol. 2, No. 1, 2016, p. 75.*

Box 4

Glossario

- **Cloud computing:** letteralmente "nuvola informatica". Identifica la messa a disposizione di dati informatici per utilizzo, condivisione e archiviazione attraverso una piattaforma internet, con possibilità di accesso in remoto.
- **Hardware**: indica la parte fisica, i componenti tangibili, di un apparecchio o sistema, come ad esempio, lo schermo, la tastiera, il *mouse* di un computer.
- **IP (internet protocol)**: protocollo di comunicazione usato dalla rete internet.
- **Smart objects**: letteralmente, oggetti intelligenti. Sono oggetti di uso quotidiano che, dotati di microprocessori, capacità di memoria, capacità di archiviazione e di comunicazione diventano una sorta di "mini-computer" in grado di interagire con gli esseri umani e l'ambiente circostante. Questi oggetti intelligenti possono essere utilizzati in diversi contesti, come ad esempio laddove si parla di *smart homes* e *smart cities* (rispettivamente, case intelligenti e città intelligenti), con riferimento all'impiego di questo tipo di tecnologia all'interno di case e città. In particolare il concetto di *smart city* è spesso usato in relazione a tutti quegli strumenti di pianificazione urbanistica che utilizzano l'innovazione tecnologica per diminuire gli impatti ambientali delle città e migliorare la qualità di vita di chi vi abita.
- **Software**: contrapposto ad *hardware*, è l'insieme dei programmi utilizzati in un sistema di elaborazione, come, ad esempio, il sistema operativo di un computer.

stallazione di un *software* sullo strumento di lavoro non dovrebbe far venire meno l'operatività della deroga di cui all'art. 4, comma 2, dello statuto dei lavoratori.

Rispetto ai Dpi è necessario, innanzitutto, rilevare come, nei casi in cui il loro utilizzo sia previsto come obbligatorio dal **documento di valutazione dei rischi**, non si possa mettere in dubbio, richiamando proprio il dettato normativo e l'interpretazione finalistica confermata dal ministero, che gli stessi costituiscano "strumenti di lavoro". Sono, infatti, indispensabili per poter rendere la prestazione lavorativa in sicurezza e, posto che la prestazione di lavoro non può essere svolta in condizioni di pericolo, ne consegue che, in loro assenza, la prestazione non può essere resa. Logico chiedersi, a questo punto, quali conseguenze si avrebbero qualora ai Dpi venisse applicato un *software* che consentisse di verificarne l'utilizzo o addirittura il "corretto" utilizzo e se, per casi come questi, sia necessario ottenere l'accordo sindacale di cui al comma 1 o possa valere la deroga di cui al comma 2.

Se il *software* installato azionasse semplicemente un segnalatore acustico su un dispositivo dello stesso lavoratore (ad esempio *smartphone*) fino a quando non venissero ripristinate le condizioni di sicurezza (esempio tipico del più comune segnalatore acustico di mancato inserimento delle cinture di sicurezza sull'automobile) si potrebbe pacificamente applicare la deroga di cui all'art. 4, comma 2.

Diverso sarebbe se il *software* inviasse il segnale di mancato o non corretto utilizzo a un sistema centrale di controllo (che, per esempio, non consentisse all'operatore sfornito del Dpi previsto di accedere ad aree delimitate da sistemi di interblocco). Secondo la teoria della funzionalità prevalente sopra esposta dovrebbe, comunque, trovare applicazione il regime derogatorio di cui al comma 2 dell'art. 4 (il lavoratore non può rendere la prestazione di lavoro senza il Dpi, che diventa, quindi, strumento di lavoro).

È ragionevole ritenere che la deroga trovi applicazione anche ove la si interpreti secondo "l'intenzione del legislatore" e ciò sia in relazione al momento storico in cui la norma è stata emanata sia in connessione e con riferimento alla sua collocazione all'interno dell'intero sistema normativo (cosiddetta "interpretazione sistematica").

Quanto al **momento storico**, come detto in precedenza, l'applicazione attuale delle potenzialità della rete e la diffusione di sistemi

(anche integrati) di raccolta dei dati e di connessione, è talmente diffusa che sarebbe impossibile eliminarne tutti gli effetti e irragionevole non sfruttarne le potenzialità.

Quanto alla **sistematica legislativa**, si deve tenere conto della profonda connessione tra la normativa giuslavoristica e quella in materia di sicurezza (non si dimentichi in questo contesto anche la rilevanza dell'art. 2087, codice civile, quale norma di chiusura del sistema prevenzionistico). La questione relativa ai controlli a distanza non può, pertanto, non tenere conto degli obblighi posti a carico del datore di lavoro che, oltre a dover adottare le misure di prevenzione deve «*richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione»* [art. 18, comma 1, lettera *f*), D.Lgs. n. 81/2008].

La giurisprudenza intervenuta in tema di obblighi di sicurezza ha, ormai da anni, affermato che «*in tema di sicurezza antinfortunistica, il compito del datore di lavoro comprende non solo la necessità di adottare le previste misure di sicurezza ma anche il controllo nel sorvegliare ed accertare che tali misure vengano, in concreto, osservate. In tale contesto deve controllare che gli strumenti adeguati vengano concretamente utilizzati e che le modalità del processo di lavorazione vengano rispettate*» (Cassazione n. 13251/2005).

In ordine all'ampiezza di quest'obbligo di controllo e alle relative modalità di attuazione è opportuno richiamare una storica sentenza della Corte di Cassazione che, interpretando il D.P.R. n. 547/1955, ha affermato che «*il compito del datore di lavoro, o del dirigente cui spetta "la sicurezza del lavoro" è un compito molteplice, articolato, che va dalla istruzione dei lavoratori sui rischi di determinati lavori e sulla necessità di adottare certe misure di sicurezza, alla* ***predisposizione di queste misure e, quindi, ove le stesse consistano in particolari cose o strumenti, al mettere queste cose, questi strumenti a portata di mano del lavoratore e, soprattutto, al controllo, continuo, pressante per imporre che i lavoratori rispettino quelle norme, si adeguino alle misure in esse previste e sfuggano alla superficiale tentazione di trascurarle»*** (Cassazione n. 6486/1995).

Se al datore di lavoro è imposto il rigoroso onere di controllo e se allo stesso (e secondo un analogo principio consolidato) è richiesta anche l'applicazione delle "migliori tecnologie disponibili", si ritiene che, secondo una interpretazione della norma che valorizzi le finalità della stessa, la volontà del legislatore e l'intero sistema normativo, non si possano non includere tra gli "strumenti di lavoro" sottoposti alla deroga dell'art. 4 comma 2 anche i Dpi o, comunque, qualsiasi ulteriore attrezzatura che consenta, non solo di eseguire la prestazione, ma anche di prestarla "in sicurezza".

Ad analoga conclusione, del resto, si dovrà pervenire confrontando i diversi diritti "in gioco" dove il diritto alla "privacy" dovrà necessariamente cedere il passo al diritto alla salute di cui all'art. 32 della Costituzione.

Non senza, ove possibile, tenere conto del fatto che il ricorso per così dire "libero" all'utilizzo dello strumento di lavoro non implica, del resto, che le informazioni così ottenute possano essere utilizzate senza vincoli.

L'art. 4, comma 3 prevede già che le informazioni raccolte ai sensi dei commi 1 e 2 siano utilizzabili «*per tutti i fini connessi al rapporto di lavoro»* a condizione che il lavoratore ne venga debitamente informato e siano rispettate le previsioni del codice sul trattamento dei dati personali. Il garante della *privacy* aveva sollecitato un ripensamento della norma ritendendo che «*la possibilità del controllo dell'attività lavorativa e la conseguente utilizzabilità, anche a fini disciplinari, dei dati così acquisiti, diverrebbe in tal modo un "effetto naturale del contratto", in quanto finirebbe con il discendere naturalmente dalla costituzione del rapporto di lavoro*»[15]. Tuttavia, il richiamo alla normativa del codice della *privacy*

[15] *Il garante della* privacy *aveva espresso tale preoccupazione nel corso della audizione sugli schemi di decreti legislativi attuativi del cosiddetto "*jobs act*" presso la commissione lavoro della camera dei deputati (9 luglio 2015) e la commissione lavoro del senato (14 luglio 2015).*

e la necessaria previa informativa del lavoratore sembrano essere sufficienti a impedire forme indebite di sorveglianza dei lavoratori; ciò, in particolare, mediante l'applicazione dei principi di necessità, correttezza, determinatezza, legittimità ed esplicitazione del fine perseguito, pertinenza e non eccedenza dei dati trattati[16].

Dal coordinamento tra la disciplina tracciata dall'art. 4 dello statuto dei lavoratori e la normativa del codice della *privacy* discende che, comunque, qualora non sia fornita adeguata informativa al lavoratore sugli strumenti di controllo, ovvero qualora sia stata violata la normativa dettata dal codice della *privacy*, le informazioni così ottenute saranno inutilizzabili, sebbene apprese per mezzo di apparecchiature legittimamente installate ai sensi dell'art. 4 dello statuto dei lavoratori.

Peraltro, quale che sia l'impostazione preferita, ovvero che l'applicazione di *software* di geolocalizzazione o *similia* su dispositivi di protezione individuale comporti l'applicazione dell'art. 4,comma 1, ovvero della disciplina derogatoria del comma 2, è sempre possibile che la contrattazione collettiva deroghi in meglio o in peggio rispetto al dettato normativo[17].

Conclusioni

In conclusione si ritiene che, nell'applicazione e nell'interpretazione della riforma sui controlli a distanza, sia necessario tenere conto del momento storico, dell'evoluzione tecnologica, delle istanze di sicurezza e del necessario coordinamento sistematico della disciplina giuslavoristica con quella antinfortunistica. È in questa ottica, quindi, che è possibile ritenere come i DPI non possano non rientrare nella nozione di "strumenti di lavoro", anche qualora fossero dotati di software capaci di verificarne l'utilizzo e/o il corretto utilizzo; non a caso, l'applicazione di software ai DPI, non ne muta la natura di strumenti necessari al lavoratore per rendere la prestazione lavorativa, apparendo peraltro, l'applicazione anche in questo ambito del codice in materia di protezione dei dati personali, sufficiente presidio a tutela della riservatezza dei lavoratori. In ogni caso - e anche a prescindere dai limiti e dall'interpretazione che anche la giurisprudenza darà alla normativa - i vantaggi che le moderne tecnologie possono portare in tema di sicurezza, meriterebbe comunque la partecipazione delle parti sociali nel trovare soluzioni condivise che ne consentano la loro introduzione. ■

---

[16] *Per un approfondimento sui principi e le garanzie da osservare in materia di protezione dei dati personali si veda il paragrafo 2.3 delle linee guida del garante della* privacy *sull'utilizzo della posta elettronica e della rete internet nel rapporto di lavoro, registro delle deliberazioni, delibera del 1° marzo 2007, n. 13.*

[17] *La disciplina di "sostegno alla contrattazione collettiva di prossimità" (art. 8, D.L. n. 138/2011, convertito con la legge n. 148/2011) ha inserito la materia degli "impianti audiovisivi e della introduzione di nuove tecnologie" fra quelle derogabili dal contratto collettivo decentrato.*