Ente Bilaterale Terziario

Ente Bilaterale Lavoro Turismo

CONTROLLI A DISTANZA E NUOVE TECNOLOGIE

Tra l'art. 4 dello Statuto dei Lavoratori e il Regolamento Europeo per la Protezione dei dati personali

a cura di Antonio Vargiu

CHI SIAMO

L'ENTE BILATERALE DEL TERZIARIO (E.B.T.)

è formato e gestito dall'associazione imprenditoriale ASCOM CONFCOMMERCIO e dalle Organizzazioni Sindacali delle lavoratrici e dei lavoratori – FILCAMS CGIL, FISASCAT CISL, UILTuCS UIL.

L'E.B.T. si rivolge, quale beneficiari dei propri servizi, alle aziende che applicano il CCNL terziario, distribuzione, servizio ed ai loro dipendenti, entrambi se in regola con la contribuzione contrattualmente prevista a favore dell'Ente stesso.

L'ENTE BILATERALE LAVORO DEL TURISMO (E.B.L.T.)

è formato e gestito dalle Associazioni imprenditoriali EPAT (Pubblici Esercizi), FEDERALBERGHI (agenzie alberghiere), FAITA (camping e villaggi turistici) e dalle Organizzazioni Sindacali delle lavoratrici e dei lavoratori – FILCAMS CGIL, FISASCAT CISL, UILTuCS UIL.

L'E.B.L.T. si rivolge quali beneficiari dei propri servizi, alle aziende che applicano i CCNL delle aziende alberghiere e della ristorazione, dei pubblici servizi e ai loro dipendenti, ma devono essere in regola con la contribuzione prevista contrattualmente a favore dell'Ente stesso.

SCOPI DEGLI ENTI

Gli Enti Bilaterali operano come strumento di servizio per la realizzazione di politiche, progetti e servizi di favore nei confronti sia delle imprese sia delle lavoratrici e lavoratori dei settori del terziario e del turismo ricompresi dai Contratti Nazionali di Lavoro sottoscritti dalle Pari Sociali socie degli Enti stessi.

CONTATTI

Sede: Via Massena 20, 10128 – Torino

Sito: www.ebtorino.it

mail E.B.T.: segreteriaterziario@ebtorino.it

mail E.B.L.T.: segreteriaturismo@ebtorino.it

INDICE

INTRODUZIONE

Il controllo a distanza: una definizione

Nell'ambito dei rapporti di lavoro subordinato il datore di lavoro è titolare di una serie di poteri nei confronti del lavoratore. È lui che organizza il lavoro, definisce gli orari e la loro articolazione, vigila sul rispetto delle direttive impartite, esercita il relativo potere disciplinare.

Ovviamente tutto questo deve avvenire nel rispetto delle norme di legge e di quanto stabilito contrattualmente tra le parti, associazioni imprenditoriali, aziende ed organizzazioni sindacali.

Fatta questa premessa, ***il controllo a distanza è quella particolare forma di controllo che viene esercitato sui punti nevralgici dell'azienda, ma anche sui lavoratori e sul loro operato, con l'utilizzazione degli strumenti messi oggi a disposizione dalle nuove tecnologie.***

Le nuove tecnologie dell'informazione e della comunicazione

I profondi cambiamenti dell'attuale contesto socio-economico, dovuti al proliferare delle reti digitali e delle tecnologie dell'informazione (IT, *Information Technology*) e della comunicazione (ICT, *Information and Communication Technology*), ma anche all'incremento del numero dei mercati e alla loro crescente liberalizzazione, stanno modificando le basi dell'organizzazione della società: educazione, sanità, trasporti, turismo, mobilità, business, modi di concepire le relazioni e i gruppi sociali. Questa nuova situazione viene a caratterizzarsi per la rilevanza primaria della conoscenza.

Infatti, oltre a essere fonte di rinnovamento, riconfigurazione e coordinamento di ogni altro processo fondante la società moderna, la conoscenza presenta caratteristiche sostanzialmente diverse da quelle delle altre risorse: l'immaterialità e la difficile quantificabilità, la conoscenza, cioè, non può essere misurata, la soggezione alle leggi dell'abbondanza e dei rendimenti crescenti, la conoscenza quindi non si consuma, anzi, attraverso lo scambio e la condivisione cresce e si rinnova continuamente.

Negli ultimi decenni, l'interesse verso il 'bene' conoscenza è stato alimentato da alcune sue caratteristiche economiche, in particolare riguardo a determinati aspetti: la rilevanza assunta dalla conoscenza come fattore primario di produzione, la

focalizzazione sulle risorse intangibili piuttosto che su quelle tangibili, l'esplosione dell'interconnettività a opera della diffusione delle reti digitali e di standard universali di comunicazione, la virtualizzazione, l'aumento della velocità di diffusione dell'innovazione, la mobilità come elemento fondante dell'antropizzazione del territorio e dei processi dinamici della globalizzazione.

Questa visione del mondo configura una società nella quale la conoscenza assume il ruolo di risorsa primaria. Inoltre, benché si possano discutere le origini tecnologiche dei fenomeni di gestione della conoscenza, le tecnologie ne costituiscono di fatto una condizione necessaria, assumendo sempre più un ruolo di integrazione e supporto.

Un modello descrittivo per il mondo dell'informazione

Un modello, molto semplice, che tenti di rappresentare il ruolo che le tecnologie ICT svolgono a supporto della gestione dell'informazione, considerato come processo di trasformazione dei dati in conoscenza, è fondato su tre elementi basilari: le reti di comunicazione; i dati che attraverso le reti possono essere raccolti e trasmessi, e rappresentati ed elaborati per divenire informazioni; le applicazioni o servizi per i quali l'informazione, divenuta conoscenza, può essere utilizzata come asset, risorsa suscettibile di valutazione economica**.**

Come sempre le nuove tecnologie hanno, però, un valore "ambiguo", accanto alle grandi potenzialità positive per la crescita economica e sociale, non possiamo non considerare anche i rischi di forme di controllo sempre più capillari ed invasive della sfera privata di ciascuno di noi e che mettono in discussione consolidati diritti e libertà fondamentali.

In conclusione dobbiamo assolutamente evitare il conflitto tra "tecnologia della libertà" e "tecnologia del controllo"

La trasformazione dell'ambiente di lavoro

Anche nelle aziende le nuove tecnologie hanno prodotto profondi cambiamenti: in questi ultimi decenni, infatti, i dipendenti si sono trovati, sempre più spesso, a prestare la propria opera in realtà sempre più informatizzate.

Si è passati, cioè, dall'essere solamente sotto l'occhio vigile di una telecamera, all'essere controllati in modi molto capillari e a rischio di stress: infatti si entra in azienda usando ad esempio un badge, che segnala i movimenti del suo possessore quando passa davanti a postazioni di rilevamento in radiofrequenza. Oppure la propria attività lavorativa può essere monitorata da remoto tutte le volte che viene usato un computer o uno smartphone aziendale. Senza parlare poi del diffondersi, nei magazzini, di braccialetti od altri analoghi strumenti elettronici con cui si opera nella logistica più moderna (Amazon, ma non solo).

In sostanza le nuove tecnologie sono fortemente pervasive.

Tra il potere dispositivo e la tutela della dignità del lavoratore

Non c'è dubbio che siamo oggi lontani mille anni luce dal tipico controllo ottocentesco sul lavoro operaio nelle fabbriche: quello ravvicinato, esercitato dai "capetti" con angherie anche fisiche.

Gli strumenti di controllo, come s'è visto, sono molto più raffinati. Questo ci porta ad una prima conclusione: se da un lato l'esperienza ci fa escludere che si possa fermare l'evoluzione tecnica degli strumenti usati dall'uomo, dentro o fuori i luoghi di lavoro, dall'altra è chiaro che un'accettazione acritica di questa evoluzione può portare a pesanti conseguenze nei rapporti sociali.

Siamo di fronte, quindi, a due esigenze che devono essere contemperate: quelle del datore di lavoro, volte ad organizzare al meglio e nella maniera più efficiente il lavoro nella propria azienda, e quelle dei lavoratori a vedere rispettata la propria persona, pur nell'impegno e nell'esercizio di una attività subordinata.

Le normative di riferimento

Ne facciamo adesso una semplice elencazione, in quanto un'analisi più approfondita sarà oggetto del secondo capitolo di questo libro.

La fonte primaria è costituita **dall'art.4 della legge 300/70, lo Statuto dei lavoratori.**

Si tratta di un corpo normativo fondamentale del diritto del lavoro italiano che, parzialmente modificato e integrato nel corso di questi decenni, ancora oggi costituisce la disciplina di riferimento per i rapporti tra lavoratore e impresa e i diritti sindacali.

È stato approvato a seguito delle tensioni sociali e delle lotte sindacali della fine degli anni sessanta, conosciute come la stagione dell'autunno caldo, e preceduto dall'introduzione nell'ordinamento di alcune significative norme di tutela e garanzia per i lavoratori…lo Statuto rappresentò una svolta dal punto di vista sia politico che giuridico, nel sancire positivamente alcuni dei diritti fondamentali del lavoratore e delle sue rappresentanze sindacali.

In particolare l'art.4, inserito nel Titolo III, Della libertà e dignità del lavoratore, ha per titolo "Impianti audiovisivi", anche se il testo non parla solo di "… *impianti audiovisivi", ma anche "(de)gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori…*".

L'art.4 è stato poi notevolmente modificato dal c.d. "Jobs Act" (precisamente dall'art. 23 del decreto legislativo n. 151/2015, in vigore dal 24 settembre 2015). Più avanti ne vedremo anche, in maniera più analitica, l'impatto sulla contrattazione.

Parallelamente, a livello della Comunità Europea, in consonanza con l'evoluzione delle nuove tecnologie informatiche si è andato sviluppando il dibattito sulla necessità di proteggere i dati personali, non più legati solamente ad archivi "fisici" e quindi ora più facilmente acquisibili ed utilizzabili.

Da qui ne è scaturita una normativa, che è andata ad integrarsi, pur partendo da un altro punto di vista, con la stessa tematica affrontata in Italia dallo Statuto dei lavoratori.
Parliamo in particolare della **Direttiva (UE) 46 del 1995**, attuata in Italia con la creazione del ***"Codice in materia di protezione dei dati personali***" (decreto legislativo 30 giugno 2003, n.196, entrato in vigore il 1° gennaio 2004).

Un'ulteriore evoluzione della materia la abbiamo avuta, infine, con il **Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio Europeo o GDPR** (General Data Protection Regulation). Il Regolamento è entrato in vigore in Italia il 25 maggio 2018.

Capitolo 1
LE FONTI NORMATIVE

1.1 L'articolo 4 dello Statuto dei lavoratori

Questo articolo è uno dei fondamenti dello Statuto dei lavoratori e, non a caso, è inserito nel Titolo I della legge 300/70, che tratta "della libertà e dignità del lavoratore" (artt. 1-13).

La norma ha subìto, successivamente, alcune modifiche con il decreto legislativo 151 del 2015 (jobs act). Per una migliore comprensione quindi della portata dell'articolo e della sua attualità, nonostante i "rimaneggiamenti", passiamo ad una analisi delle sue norme così come modificate nel tempo.

1.2 Il testo originario (4)

Nella sua formulazione originaria l'art.4 dello Statuto stabiliva un divieto assoluto dell'uso *"di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori".*

Questo divieto veniva però attenuato nel caso in cui la necessità del controllo venisse richiesta "*da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro*".

In questo caso scattava, però, l'obbligo di un tentativo di accordo "*con le rappresentanze sindacali aziendali*".
In sintesi possiamo dire, che all'introduzione di una casistica, che rendeva possibile il controllo a distanza, veniva fatto seguire un meccanismo di limitazione e di contenimento delle decisioni datoriali, consistente nell'obbligo di contrattazione con le organizzazioni sindacali presenti in azienda.

Questa norma può essere definita, quindi, come ***norma di sostegno alla contrattazione***.

Se l'accordo non veniva raggiunto, il datore di lavoro poteva comunque ricorrere all'Ispettorato del lavoro, che eventualmente stabiliva anche le modalità di uso degli impianti audiovisivi. In ogni caso le organizzazioni sindacali potevano anche ricorrere, in ultima istanza, al Ministro del Lavoro.
Non era comunque possibile, da parte dei datori di lavoro, utilizzare le telecamere per assumere provvedimenti di carattere disciplinare.

1.3 I controlli "difensivi" prima del jobs act

La copiosa giurisprudenza in materia è il segno più evidente della delicatezza della questione e del prudente avanzamento nel campo minato del bilanciamento tra le esigenze di protezione del patrimonio aziendale, inteso in senso ampio e correlato alla libertà di iniziativa economica costituzionalmente garantita e la tutela della dignità e riservatezza dei lavoratori.

Negli anni successivi all'entrata in vigore dello Statuto dei lavoratori, sul tema dei "controlli a distanza" si è aperto un contenzioso tra aziende e lavoratori, assistiti dalle organizzazioni sindacali, sulla portata delle "*esigenze organizzative e produttive ovvero della sicurezza del lavoro*".

Si è ricorsi quindi alla magistratura per la delimitazione del confine tra tutela del patrimonio aziendale, umano e materiale e rispetto della dignità del lavoratore.

Il presupposto della norma, che si inserisce nel solco tracciato dal legislatore e ripreso dalla giurisprudenza e dalla dottrina, è quello di non spingere l'attività di vigilanza, ancorché necessaria nell'organizzazione produttiva, oltre limiti tali da escludere qualsiasi spazio di autonomia e di riservatezza per il lavoratore, c.d. dimensione umana della vigilanza.

Si tratterebbe, così, di contenere in vario modo le manifestazioni del potere direttivo e organizzativo del datore di lavoro, che, per le modalità di attuazione incidenti nella sfera

della persona, si ritengono lesive della dignità e riservatezza del lavoratore. (Cass. n. 8250/00).

Pertanto, l'attenzione si sofferma sulla modalità e sullo strumento tecnologico utilizzato per il controllo, che non deve determinare un monitoraggio continuativo, rigido, esasperato ed asfissiante.

Il filone maggioritario della giurisprudenza si è orientato a consentire solo i controlli difensivi c.d. preventivi, quando si tratti di reprimere e far cessare condotte illecite già prodottesi e non sottoposte a vigilanza, con la finalità di impedire ed evitare il compimento di ulteriori future condotte di tal genere, pur sempre lesive del patrimonio o dell'immagine aziendale.

1.4 Un problema di organizzazione della rappresentanza

Al di là della buona volontà del legislatore il comma 2 dell'art.4, nella versione originale, presentava un problema per le organizzazioni sindacali.

Infatti gli accordi sull'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dei lavoratori, potevano essere sottoscritti solo dalle rappresentanze aziendali oppure, in mancanza di queste, dalle

commissioni interne, queste ultime in realtà non più rinnovate dalla fine degli anni ‘60.

È questo uno schema tipicamente industriale, che fa riferimento a unità produttive medio-grandi, con un numero consistente di dipendenti.

L’art.35 dello Statuto dei lavoratori chiarisce come si possano costituire le rappresentanze sindacali aziendali. Ebbene questo articolo ne prevede la costituzione in due casi:

A. in ciascuna sede, stabilimento, filiale, ufficio o reparto autonomo che occupa più di quindici dipendenti;
B. in imprese industriali e commerciali che nell'ambito dello stesso comune occupano più di quindici dipendenti.

Mentre queste disposizioni erano ben calibrate per le attività industriali, la normativa si è mostrata di più difficile gestione per le aziende commerciali e più in generale, del terziario, che spesso operavano in unità produttive, che da sole o all’interno di un comune, non raggiungevano i numeri previsti per la costituzione delle rappresentanze sindacali aziendali.
Questo per molto tempo ha rappresentato un forte limite alla definizione di accordi sindacali sulla videosorveglianza.

1.5 Il testo come modificato dal jobs act

Il nuovo testo è profondamento cambiato rispetto alla versione originaria.

Qui di seguito elenchiamo i punti principali delle modifiche:

a) è stato tolto il divieto assoluto del controllo a distanza dell'attività dei lavoratori;
b) sono state ampliate le motivazioni per le quali è possibile l'utilizzo degli impianti audiovisivi e degli altri strumenti; infatti alle "esigenze organizzative e produttive ovvero alla sicurezza del lavoro", adesso si aggiunge "la tutela del patrimonio aziendale";
c) la titolarità ad intervenire per definire un eventuale accordo è stata parzialmente modificata, in modo da consentire un maggior spazio di intervento per le organizzazioni sindacali; adesso infatti si prevede che: "…previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale";
d) le informazioni ottenute con i predetti strumenti sono "*utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione…";*

A controbilanciare questa ultima affermazione, nel nuovo testo dell'art.4 compare anche un riferimento normativo importante, che, come vedremo più avanti, parlando delle esperienze contrattuali, porta a conseguenze pratiche di grande rilievo.

Ci riferiamo in particolare al comma 3 nel punto nel quale si parla di obbligo di informazione preventiva "nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196, che è il cosiddetto Codice della privacy (Codice in materia di protezione dei dati personali).

A questo punto il legislatore opera una specifica saldatura tra la normativa dello Statuto e quella che deve garantire la riservatezza dei dati personali dei lavoratori.

1.6 Dal Codice per la protezione dei dati personali del 2004 al Regolamento generale sulla protezione dei dati (GDPR del 2018)

Come abbiamo indicato, su impulso di dibattiti e di orientamenti che man mano si sono andati consolidando a livello europeo, altre fonti normative si affiancano all'art. 4 dello Statuto dei lavoratori con lo scopo di garantire la

riservatezza dei dati personali sia negli ambiti lavorativi sia negli altri ambiti della vita sociale.

La definizione di "dati personali" data dal Garante

"Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica.

Particolarmente importanti sono:

• i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

• i dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

• i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale… o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti".

L'entrata in vigore delle nuove norme

Il **Codice per la protezione dei dati personali** entra in vigore in Italia il 1° gennaio 2004, con il Decreto legislativo 30 giugno 2003, n. 196.

Ci sembra utile operare qui un primo chiarimento sulle finalità delle nuove norme.
Il diritto alla riservatezza è diverso rispetto al diritto sui propri dati perché non riguarda solamente informazioni circa la propria vita privata, ma più in generale ingloba ogni informazione relativa ad una persona, pure se non coperta da

riserbo, sono dati personali ad esempio il nome o l'indirizzo della propria abitazione.

Lo scopo della normativa è quello di evitare che il trattamento dei dati avvenga senza il consenso dell'avente diritto, ovvero in modo da recargli pregiudizio.

Al Codice si aggiunge, più recentemente, il Regolamento generale per la protezione dei dati personali 2016/679 (**General Data Protection Regulation** o **GDPR**), che è la principale normativa europea in materia di protezione dei dati personali e che è entrato in vigore il 25 maggio 2018.

Qual è il rapporto tra le norme del Codice e quelle del Regolamento generale?

Il Regolamento non interviene proprio su tutto. Alcune cose le lascia ai legislatori nazionali.

Infatti, il Codice Privacy, che in Italia abbiamo adottato per recepire la Direttiva 45/1996, non è sparito, ma è stato rivisto. Si dice novellato. In parole povere è stato modificato su singoli punti e con riforme parziali.

A cosa serve e come metterlo insieme alle disposizioni del GDPR?

Il Codice novellato interviene in quegli spazi che il legislatore europeo ha voluto rimandare ai singoli Stati. Quindi l'UE stabilisce la cornice, ma spetta poi al legislatore nazionale adottare le norme.

Questi spazi sono:

- il **trattamento di dati sensibili**: dati genetici, dati sulla salute, l'orientamento sessuale, le convinzioni religiose, le opinioni politiche eccetera.
- la **disciplina dell'Autorità**: ogni Stato ha un'autorità – un organo nazionale - che garantisce la tutela dei dati personali, ma l'UE non può imporre un modello unico uguale per tutti i Paesi. Ogni Stato alle sue regole costituzionali. Per esempio, in Italia l'Autorità Garante viene nominata dal Parlamento. Quindi questo aspetto resta in capo ai singoli Stati.
- parte della **disciplina delle sanzioni**. L'UE non ha competenze penali che spettano ai singoli Stati quindi può comminare solo sanzioni amministrative. Una sorta di multa. Però nei casi più gravi ha dato la possibilità ai singoli Stati di prevedere una sanzione penale che viene data dal giudice, non dall'Autorità Garante, che resta un organo amministrativo e che quindi non si occupa di reati penali".

1.7 Il Regolamento generale sulla protezione dei dati (GDPR): i principi generali

Il Regolamento ha la caratteristica di non partire dai divieti, ma attribuisce al **titolare del trattamento dei dati personali** precise responsabilità, in inglese **accountability**, che si basano sull'osservanza dei seguenti principi, che vedremo quindi ricorrere spesso anche negli accordi sindacali:

- *liceità, correttezza e trasparenza del trattamento*, nei confronti dell'interessato, escludendo ad esempio i controlli vietati e le indagini sulle opinioni personali dei lavoratori ecc.; quanto alla trasparenza questa si concretizza nella assoluta necessità di una puntuale informazione al lavoratore di tutti i trattamenti riguardanti i suoi dati personali;
- *limitazione della finalità del trattamento* - obbligo di assicurare che i dati personali devono essere raccolti per finalità determinate, esplicite e legittime; inoltre eventuali trattamenti successivi non devono essere incompatibili con le finalità della raccolta dei dati;
- *minimizzazione dei dati*, i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- *esattezza e aggiornamento dei dati* - comprende il loro continuo aggiornamento e la tempestiva cancellazione di quei dati che risultino inesatti rispetto alle finalità del trattamento;
- *limitazione della conservazione* - è necessario provvedere alla conservazione dei dati per il tempo strettamente necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- *il principio di responsabilizzazione* - il datore di lavoro non solo è responsabile del come siano utilizzati i dati personali dei lavoratori, ma ha anche l'onere di provare di aver preso tutte le misure necessarie per impedirne la sottrazione o l'impossessamento da parte di terzi non autorizzati; il titolare, quindi, deve mettere in atto misure tecniche e

organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento Europeo (articolo 24, paragrafo 1);

- *integrità e riservatezza* - occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento; questo significa che il titolare deve adottare misure di sicurezza tecniche ed organizzative atte a proteggere i dati stessi da atti illeciti, dalla loro perdita o distruzione e dal danno accidentale; queste misure devono riguardare tutto il ciclo del trattamento.

1.8 Il Regolamento generale sulla protezione dei dati (GDPR): il trattamento dei dati, il titolare, il responsabile e l'incaricato

Possiamo affermare che tutta l'impostazione delle normative europee sulla protezione dei dati personali si basa non tanto sull'elencazione di divieti quanto sulla *distribuzione di responsabilità tra soggetti diversi.*

Un chiaro esempio di questa impostazione è dato dalla distinzione tra *titolare* e *responsabile* del trattamento dei dati.

Il *titolare* del trattamento è la persona fisica o giuridica a cui spettano, singolarmente o insieme ad altri titolari, tutte le decisioni in merito alle finalità e modalità del trattamento,

compresi i profili inerenti alla sicurezza. Sostanzialmente coincide con l'azienda o l'organizzazione. Facciamo un esempio: un'azienda ha necessità di utilizzare i dati dei dipendenti per fare le buste-paga. Se fa il tutto in casa, abbiamo la *coincidenza tra titolare e responsabile*.

Questa operazione può invece essere affidata ad un *soggetto esterno*, che in questo caso assume il ruolo di *responsabile* (Data Processor) del trattamento.

Il responsabile deve essere selezionato tra soggetti altamente qualificati, ovvero tra coloro che per esperienza, capacità o particolari doti di affidabilità siano in grado di garantire il rispetto degli obblighi di legge. Il responsabile del trattamento, inoltre, deve essere designato con un contratto o altro atto giuridicamente valido, individuando in modo tassativo, e per iscritto, i compiti, le responsabilità e lo specifico ambito di operatività.

Gli *incaricati,* infine, sono *"*le persone fisiche autorizzate a compiere operazioni di trattamento dal responsabile, previa autorizzazione scritta da parte del titolare"*.*

1.9 Il Regolamento generale sulla protezione dei dati (GDPR): il Data Protection Officer (DPO)

Per non fare confusione tra tutti questi termini in inglese, la sigla DPO si può tradurre in italiano con Responsabile Protezione Dati (RPD). Qualcuno lo ha anche ribattezzato come il "facilitatore", in quanto esperto del Regolamento e delle norme relative pronto a consigliare aziende ed amministrazioni.

Difatti così ne definisce i compiti il cosiddetto "*gruppo di lavoro articolo 29",* che ha formulato i contenuti del Regolamento comunitario.

Nelle Linee guida, infatti, sottolineava l'utilità di designare un RPD "… per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche, ovvero trattino su larga scala categorie particolari di dati personali".

Questo al fine della responsabilizzazione e dell'osservanza della normativa e per aumentare il margine competitivo delle imprese, oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo controlli interni in materia di protezione dei dati), i Responsabili della Protezione dei dati fungono da interfaccia fra i soggetti coinvolti: autorità di controllo,

interessati, divisioni operative all'interno di un'azienda o di un ente...".

1.10 Il Regolamento generale sulla protezione dei dati (GDPR): con le sanzioni non si scherza!

Lo spiega chiaramente Il Garante nella nota con cui annuncia l'applicazione anche in Italia del Regolamento europeo.

La nota riassume brevemente i principi che informano il nuovo Regolamento che entra in vigore, sottolineando in particolare il diritto dell'utente "di ricevere informazioni chiare sull'uso che viene fatto dei suoi dati personali, potrà trasferirli da un titolare del trattamento ad un altro, compresi i social network (diritto alla portabilità dei dati), e vedrà rafforzato il suo diritto di far cancellare, anche on line, le informazioni non più necessarie rispetto alle finalità per le quali sono state raccolte (diritto all'oblio).

Per le aziende cambia radicalmente l'approccio alla protezione dei dati: "imprese ed enti dovranno operare seguendo il principio di responsabilizzazione, considerare la protezione dei dati non come obbligo formale, ma come una parte integrante e permanente delle loro attività e promuovere consapevolezza negli utenti sui loro diritti e le loro libertà".

Ma una particolare sottolineatura viene fatta a proposito delle sanzioni previste per le aziende che non rispettano le nuove norme europee.

Sanzioni di carattere economico di un livello mai visto prima. Difatti le aziende che non rispettino le nuove regole non vanno incontro a semplici multe, ma possono essere condannate a pagare il *4% del proprio fatturato* globale annuo!

Note Capitolo 1

Il *testo originario dell'art.4 dello Statuto:* art. 4 - Impianti audiovisivi

È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

l'art.4 dello Statuto così come modificato dallo jobs act: art. 4 - Impianti audiovisivi.

1. *Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale*

unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

2. *La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*
3. *Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.*

Capitolo 2
LA CONTRATTAZIONE NEL TERZIARIO

In questa sezione faremo una esposizione ragionata delle esperienze di contrattazione relative alle diverse *"apparecchiature e sistemi informatici"* attraverso le quali i datori di lavoro possono entrare in possesso dei dati personali dei lavoratori. In particolare esamineremo i risultati della contrattazione nei diversi settori del Terziario.

A) La videosorveglianza

Si tratta della forma più tradizionale del controllo a distanza nelle aziende, ben conosciuto già negli anni '60 e '70. Questa forma di "sorveglianza" non solo non ha conosciuto un declino, ma ha avuto, negli ultimi anni, un rinnovato sviluppo.
Passiamo a scorrerne rapidamente le ragioni.

2.1 Una nuova edizione del "grande fratello"?

Nell'introdurre - una decina di anni fa - uno studio finanziato dalla Commissione Europea avente per oggetto il tema del rapporto tra "cittadini e videosorveglianza" Michel Markus tra i motivi principali dell'aumentata presenza delle telecamere sottolineava la sempre maggiore complessità delle città: "Le città si densificano e si espandono, moltiplicando le offerte di mobilità, di cultura, di educazione, con conseguente richiesta di impianti sempre più complessi, con costi di funzionamento elevati. Diversi flussi di traffico si incrociano, le offerte commerciali più invitanti sono in bella mostra sotto gli occhi dei passanti e ne stuzzicano gli appetiti. La sorveglianza umana 24 ore su 24 diventa impossibile per ragioni economiche, ma le possibilità offerte dall'espansione dell'elettronica, che permette di raccogliere, immagazzinare e incrociare dati e informazioni ai fini del controllo o di disporre di strumenti a fini preventivi o dissuasivi, incitano a moltiplicare le telecamere di sorveglianza".

Naturalmente questa espansione dell'utilizzo della videosorveglianza mette a forte rischio la tutela della sfera privata delle persone e sembra dar ragione alle visioni di Orwell descritte nel romanzo 1984 (scritto nel 1949), quello di un mondo super controllato e manipolato da poche persone. È quindi assolutamente necessario far seguire all'aumento dei controlli un aumento delle garanzie per i cittadini.

2.2 Il Comitato Europeo per la Protezione dei Dati (European Data Protection Board - EDPB).
Le linee guida sul trattamento dei dati personali attraverso dispositivi video

Il Comitato europeo, oltre ad interpretare il Regolamento Generale per la protezione dei dati, ha il compito di "fornire consulenza alla Commissione europea su ogni questione connessa con la protezione dei dati nell'UE, compresa ogni proposta di modifica del RGPD e ogni proposta legislativa dell'UE".

È opportuno citare questo organismo per una sua pubblicazione, abbastanza recente, di linee guida in materia di videosorveglianza.

Esso risulta molto utile, per "inquadrare" la problematica che ci accingiamo ad affrontare, riportare ampi stralci della sua introduzione.

1. "L'uso intensivo di dispositivi video influisce sul comportamento dei cittadini. Un ricorso significativo a tali strumenti in numerosi ambiti della vita delle persone eserciterà su queste ultime un'ulteriore pressione per impedire il rilevamento di quelle che potrebbero essere percepite come anomalie. Di fatto, queste tecnologie possono limitare le possibilità di muoversi e di utilizzare servizi in maniera anonima

nonché, in linea generale, la possibilità di passare inosservati. Le conseguenze per la protezione dei dati sono enormi".

2. "Mentre le persone potrebbero essere a proprio agio con la videosorveglianza installata, ad esempio, per una determinata finalità di sicurezza, occorre assicurare che non ne venga fatto un uso improprio per scopi totalmente diversi e inaspettati per l'interessato (ad esempio, per scopi di marketing, controllo delle prestazioni dei dipendenti, ecc.). Inoltre, attualmente si utilizzano molti strumenti per sfruttare le immagini acquisite e trasformare le telecamere tradizionali in telecamere intelligenti. La quantità di dati generati da video, unitamente a questi strumenti e tecniche, aumenta i rischi di un uso secondario (correlato o meno allo scopo al quale viene inizialmente destinato il sistema) o persino improprio. Nel gestire la videosorveglianza sarebbe opportuno considerare sempre attentamente i principi generali del GDPR (articolo 5").

3. "I sistemi di videosorveglianza incidono in svariati modi sulle interazioni messe in atto dai professionisti del settore privato e pubblico in luoghi pubblici o privati allo scopo di migliorare la sicurezza, analizzare le risposte del pubblico, fornire pubblicità personalizzata, ecc. La videosorveglianza è diventata un sistema ad alte prestazioni grazie alla crescente applicazione di analisi video intelligenti. Queste tecniche possono essere più intrusive (tecnologie biometriche complesse) o meno intrusive (semplici algoritmi di conteggio)".

4. "Oltre alle questioni di privacy, sussistono anche i rischi legati a possibili malfunzionamenti di questi dispositivi e alle distorsioni che possono indurre. I ricercatori riferiscono che il software utilizzato per l'identificazione, il riconoscimento o l'analisi facciale funziona in modo diverso in base all'età, al genere e all'etnia della persona che sta identificando. Le prestazioni degli algoritmi sembrano variare in rapporto ai dati demografici, per cui una distorsione nel riconoscimento facciale minaccia di rafforzare il pregiudizio sociale. Per questo motivo, i titolari del trattamento devono anche assicurare che il trattamento dei dati biometrici derivanti dalla videosorveglianza sia soggetto a una valutazione periodica della sua pertinenza e dell'adeguatezza delle garanzie fornite".

5. "La videosorveglianza non è di per sé indispensabile se esistono altri mezzi per raggiungere lo scopo che ci si prefigge. Altrimenti si rischia di modificare le norme culturali con la conseguenza di ammettere come regola l'assenza di privacy".

2.3 La necessità di nuove tutele sui luoghi di lavoro

L'attività lavorativa è oggi immersa in un ambiente sempre più controllato, in varie forme, da sistemi informatici e visivi.

Nei settori del commercio e del Terziario, più in generale, i luoghi sono caratterizzati da telecamere onnipresenti e sempre accese.

Questo ha come effetto immediato l'innalzamento del livello di stress per chi vi opera. Per questo vari enti raccomandano di verificare sempre la possibilità di ridurre al minimo il numero delle telecamere, installando solo quelle più necessarie.

Per quanto riguarda gli ambienti di lavoro, si è visto come in Italia operino delle precise normative, che intrecciano quanto disposto dallo Statuto dei lavoratori con quanto prescritto dalle norme sulla protezione dei dati personali.

Il tutto va fatto contemperando le esigenze di operatività e produttività aziendale con quelle di salvaguardia e tutela dei lavoratori.

2.3.1 Il tentativo di accordo sindacale è il primo passo obbligatorio per l'installazione delle telecamere

Quando si è osservato che l'art. 4 dello Statuto è una norma di sostegno alla contrattazione si è fatto a ragion veduta. La cogenza di questa norma, infatti, è attestata dalle sanzioni penali previste in caso di una sua violazione.

Il datore di lavoro ha un divieto assoluto di installare *in maniera unilaterale* telecamere, anche se spente e non funzionanti, se prima non ha raggiunto un accordo.

A questo proposito, e a solo titolo esemplificativo, si cita una *sentenza della Cassazione penale* del 2016, che afferma che configura un reato "... la predisposizione, da parte del datore di lavoro, di apparecchiature idonee, nella specie telecamere, a controllare a distanza l'attività dei lavoratori e per la sua punibilità non è richiesta la messa in funzione o il concreto utilizzo delle attrezzature essendo sufficiente l'idoneità al controllo a distanza dei lavoratori e la sola installazione dell'impianto.

Infatti, sempre per la Cassazione penale, il confronto con le organizzazioni sindacali è **ineludibile e non aggirabile** neppure con la sottoscrizione di un consenso da parte di tutti i lavoratori occupati nell'azienda!

In questo senso una recente sentenza riafferma che "la fattispecie incriminatrice di cui all'art. 4 in esame sia integrata

anche quando, in mancanza di accordo con le rappresentanze sindacali aziendali e di provvedimento autorizzativo dell'autorità amministrativa, la stessa sia stata preventivamente autorizzata per iscritto da tutti i dipendenti".

La Corte ha quindi puntualizzato che l'installazione di impianti debba sempre essere preceduta da una *forma di codeterminazione tra il datore di lavoro e le rappresentanze sindacali dei lavoratori* o, se l'accordo non è raggiunto, da una autorizzazione della Direzione Territoriale del Lavoro (oggi ITL) competente.

Questo perché ed è bene sottolinearlo ancora una volta, nel rapporto con l'impresa i lavoratori costituiscono la parte più debole e come scrivono i giudici nella sentenza, "*basterebbe al datore di lavoro fare firmare a costoro, all'atto dell'assunzione, una dichiarazione con cui accettano l'introduzione di qualsiasi tecnologia di controllo per ottenere un consenso viziato, perché ritenuto dal lavoratore stesso, a torto o a ragione, in qualche modo condizionante l'assunzione*".

2.3.2 Solo se l'accordo sindacale non viene raggiunto è possibile, per le aziende, il ricorso all'Ispettorato nazionale del lavoro

Evidentemente un accordo, visto che deve vedere la convergenza tra parte datoriale ed organizzazioni sindacali, non può essere dato per scontato.

Come scritto nel primo capitolo, in caso di mancato accordo, l'art. 4 dello Statuto dei lavoratori prevede per l'azienda interessata la possibilità di ricorrere, per l'autorizzazione, alla sede territoriale dell'Ispettorato Nazionale del Lavoro o in alternativa, nel caso di imprese con unità produttive dislocate in più sedi territoriali, alla sede centrale dello stesso Ispettorato.

2.4 Gli accordi nazionali

La prevenzione dei furti e la tutela del patrimonio sono tra le motivazioni principali per l'installazione delle telecamere. Da questo punto di vista l'attività commerciale è tra le più coinvolte.

Sono numerosi gli accordi sull'installazione delle telecamere e sulla gestione dei dati da esse ricavabili. La maggior parte

riguardano catene di vendite al dettaglio, ma ci sono anche magazzini di distribuzione all'ingrosso e realtà produttive di altri settori del terziario.

Due condizioni indispensabili

Tra le varie condizioni necessarie per raggiungere un accordo, le Federazioni nazionali di Filcams Cgil, Fisascat Cisl, Uiltucs Uil, ne hanno posto due assolutamente ineludibili:

1) che le immagini ottenute tramite le telecamere non siano usate per assumere provvedimenti disciplinari; questo si traduce, quindi, nella rinuncia da parte delle imprese ad utilizzare il comma 3 del nuovo art.4 dello Statuto;

2) che si sottoscriva un accordo quadro nazionale e un accordo territoriale, quest'ultimo finalizzato alla definizione del numero e del posizionamento delle telecamere e le modalità di verifica da parte delle Rappresentanze sindacali aziendali del corretto uso dell'impianto.

L'articolazione degli accordi

A livello nazionale sono definiti i principi da rispettare e i criteri di riferimento per l'istallazione delle "apparecchiature" e per la gestione dei dati ricavati dal loro uso.

A livello locale va sottoscritto l'accordo "applicativo", non essendo l'accordo quadro nazionale esaustivo per l'installazione del sistema di controllo, ma solo riportante criteri di riferimento. Oggetto dell'accordo locale: "gli aspetti tecnici, il numero e il collocamento delle telecamere di videosorveglianza, unitamente al cono di inquadramento e le modalità di verifica del corretto uso dell'impianto".

L'accordo deve essere esposto dall'azienda società in tutte le sue sedi nelle quali è stato istallato il sistema di controllo, in un luogo visibile ed accessibile a tutti i soggetti coinvolti, nonché portato a conoscenza dei dipendenti in fase di assunzione, con comunicazione scritta e sottoscritta dall'interessato".

Le finalità dell'installazione

Due sono le finalità principali perseguite dalle aziende: la tutela del patrimonio aziendale (furti, rapine ecc.) e la sicurezza di chi opera nella struttura videosorvegliata.

Nel caso di strutture commerciali la prevenzione coinvolge ovviamente anche la clientela.

Pertanto il controllo video ha il duplice scopo di aumentare la sicurezza del patrimonio aziendale per prevenire, impedire e comunque ostacolare atti criminosi nell'ambito delle strutture di propria pertinenza e dall'altra, di aumentare la sicurezza dei lavoratori impiegati all'interno e/o all'esterno delle suddette

unità produttive, con particolare riguardo all'incolumità e all'integrità psicofisica degli stessi e comunque non con finalità di controllo dei lavoratori ivi occupati.

Questi concetti li ritroviamo espressi in tutti gli accordi sindacali sottoscritti.

Esclusione di finalità disciplinari

In coerenza con le condizioni precedentemente indicate, gli accordi escludono che le immagini prese dalle telecamere possano essere utilizzate per l'accertamento dell'obbligo di diligenza del lavoratore né per assumere provvedimenti disciplinari.

Dove possono essere installate le telecamere

L'esigenza delle aziende di installare le videocamere deve ovviamente essere contemperata dal diritto dei lavoratori a non vedere violata la loro giusta "riservatezza (privacy)".

Il posizionamento delle telecamere quindi sarà funzionale alla sorveglianza dei varchi di accesso da/verso l'esterno, delle corsie, dei registratori di cassa e le inquadrature saranno tali da cogliere un'immagine il più pertinente possibile.

L'eventuale ripresa di lavoratori potrà avvenire esclusivamente in via incidentale e con carattere di occasionalità, fermo

restando gli obblighi di informativa sulle modalità d'uso degli strumenti ed effettuazione dei controlli e non per finalità connesse all'adozione di provvedimenti disciplinari".

In conformità al principio di necessità e di non eccedenza, secondo correttezza e per scopi determinati, espliciti e legittimi, la raccolta dei dati è quella strettamente necessaria al raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo delle riprese, evitando immagini dettagliate, ingrandite o dettagli non rilevanti e stabilendo in modo conseguente la focalizzazione delle telecamere.

Dove* non *possono essere installate le telecamere

Sono esclusi dall'installazione i luoghi destinati esclusivamente al personale dipendente, quali ad esempio spogliatoi, sale ristoro, sale riunioni e servizi igienici, oltre che i corridoi contigui.

La gestione delle immagini

È questo un aspetto molto delicato, motivo per cui gli accordi vi dedicano una particolare attenzione.

L'impianto di videosorveglianza in funzione 24 ore su 24 per 365 giorni all'anno, non potrà prevedere né l'accesso da remoto in tempo reale né postazioni fisse di monitoraggio.

La visualizzazione delle immagini in presa diretta è consentita al "personale di regia" del punto vendita all'esclusivo scopo di tutela del patrimonio ed il corretto uso della visualizzazione è rimesso alla verifica delle RSA/RSU, anche con visite non preannunciate nei locali con i monitor.

Le immagini sono conservate per un breve periodo di tempo per poi essere definitivamente cancellate mediante sovrascrittura. La conservazione per un periodo superiore è prevista solo per indagini su fatti denunciati svolte dall'autorità giudiziaria".

L'"architettura" delle responsabilità aziendali e il suo rilievo negli accordi

Si illustrerà ora come le modalità di gestione dei dati delle lavoratrici e dei lavoratori, previste dal Regolamento generale europeo, si calino concretamente all'interno degli accordi sulla videosorveglianza.

Il *Titolare* del trattamento dati è ovviamente è l'azienda, tramite un suo *Responsabile* del Trattamento appositamente nominato e/o degli *incaricati* addetti alla sorveglianza e alla sicurezza, che hanno ricevuto apposite istruzioni in merito.
Il *Responsabile* gestirà i dati con strumenti automatizzati e con modalità tali da garantirne la sicurezza e la riservatezza.
Al dipendente viene anche ricordato che può rivolgersi al Responsabile della protezione dei dati, che può essere

contattato per tutte le questioni relative al trattamento dei suoi dati personali e all'esercizio dei diritti derivanti dal GDPR".

L'informazione sull'impianto di videosorveglianza: diritto per i lavoratori, dovere per le aziende

L'informativa sulla privacy è un elemento assolutamente da non trascurare e viene esplicitamente richiesta dall'art.13 del Regolamento europeo.

Si può definire come una comunicazione che ha lo scopo di informare il lavoratore**,** prima che diventi interessato, cioè prima che inizi il trattamento dei dati, sulle finalità e le modalità operate dal titolare del trattamento.

Essa è una condizione essenziale non solo del rispetto del diritto del singolo lavoratore ad essere informato, quanto soprattutto del dovere del titolare del trattamento di assicurare la trasparenza e correttezza fin dalla fase di progettazione dei trattamenti stessi, e di essere in grado di dimostrarlo in qualunque momento (principio di responsabilità).

Da qui la necessità, nel caso della videosorveglianza, di avvertire in maniera chiara delle possibilità di essere ripresi sia i lavoratori, che nel caso di un luogo aperto al pubblico, gli utenti, ecc.

L'accordo locale

All'accordo locale spetta, come detto, soprattutto il compito di definire il numero delle telecamere, il loro posizionamento, il loro funzionamento ecc. È molto importante sottolineare, che l'eventuale accordo quadro nazionale o comunque riferito a perimetri aziendali oltre l'unità produttiva, non ha valore applicativo, questo è riservato all'accordo relativo all'unità produttiva.

Di norma si prevede la *designazione nominativa* degli incaricati della raccolta e del trattamento dei dati, affiancati da uno o più RSA/RSU (in caso di assenza si designerà l'RSA/RSU del punto vendita più vicino) anche questi con nome e cognome.

Viene confermato che la visione in presa diretta delle immagini avverrà solo all'esclusivo scopo della tutela del patrimonio, viene ribadito inoltre che la visualizzazione delle immagini non potrà costituire in nessun modo supporto all'accertamento dell'obbligo di diligenza del lavoratore, anche incidentalmente ripreso dagli impianti audiovisivi, e per l'avvio dl procedimenti disciplinari.

Sono poi indicate le caratteristiche degli impianti con *il numero delle telecamere* interne fisse, con planimetria e documentazione allegata.

Inoltre non sono previste postazioni fisse di monitoraggio in tempo reale, fermo restando la presenza di monitor a presa diretta senza presenza fissa dell'operatore. Le immagini

registrate verranno convogliate in una DVR (sistema di registrazione) istallato in ambiente (armadio) sigillato dotato di serratura la cui chiave è conservata in busta sigillata all'interno del punto vendita, custodita all'interno della cassaforte del punto vendita.

L'uso corretto della presa diretta è verificato dall'RSA/RSU anche con sopralluoghi improvvisi nei locali con i monitor e le immagini registrate potranno essere viste solo in presenza dell'RSA/RSU per motivazioni da questi accettate o per decisione dell'autorità giudiziaria.

B) La geolocalizzazione

In tema di videosorveglianza si è sottolineato la tendenziale invasività, anche sociale, degli strumenti utilizzati per realizzarla.

Ma che dire allora della geolocalizzazione?

Per geolocalizzazione si intende l'identificazione della posizione geografica nel mondo reale di un qualsiasi oggetto come device mobile, computer, e altri dispositivi che siano connessi o meno alla Rete.

Le tecnologie attraverso le quali è possibile detta identificazione si basano sui segnali radio, sistemi cablati o, ancora, ibridi. I sistemi di geolocalizzazione maggiormente in uso sono il GPS, l'uso delle celle della rete telefonica e la rete internet attraverso connessioni WiFi o WLAN.

2.5 Come funziona il gps

Il gps funziona attraverso una rete di satelliti artificiali i quali dialogano con un dispositivo mobile e gli forniscono, attraverso la trasmissione di un segnale radio, informazioni sulle sue coordinate geografiche e l'orario.

Il global position system è attivo in qualsiasi condizione meteorologica e segnala la posizione dei vari dispositivi mobili in qualsiasi punto della Terra, purché il contatto non abbia ostacoli e possa appoggiarsi ad almeno 4 satelliti.

Il sistema di posizionamento si compone di tre segmenti: il segmento spaziale, il segmento di controllo e il segmento utente.

Il segmento spaziale comprende da 24 a 32 satelliti. Il segmento di controllo si compone di una stazione di controllo principale, una stazione di controllo alternativa, varie antenne dedicate e condivise e stazioni di monitoraggio. Il segmento utente infine è composto dai ricevitori GPS.

Una tecnologia onnipresente

È bene sapere che è molto facile collegare la persona ad un luogo fisico.

Un esempio molto facile da comprendere: tutti hanno in tasca un telefonino e magari si è fatta poca attenzione quando, per "scaricare" alcune app, è stato chiesto di consentire la localizzazione. Naturalmente, in maniera quasi automatica, è stato dato il proprio consenso.

Questo fatto, se è importante nella vita privata, lo è ancora di più nella vita lavorativa, dove, se dipendenti, occorre proteggersi sia da uno stress da iper-sorveglianza che da un utilizzo anomalo dei dati personali.

A sollevare l'attenzione dell'opinione pubblica su questo argomento intervengono, ogni tanto, fatti clamorosi.

I "braccialetti" di Amazon (futuribili) e quelli di Livorno

I primi di febbraio del 2018 e in America Amazon ottiene l'approvazione di un brevetto, che ha una sua particolarità.

Lo spiega Giuditta Mosca**:**
"Amazon potrebbe dotare i propri addetti alla logistica di un braccialetto elettronico con il quale trasmettere ordini e velocizzare le operazioni di consegna. Il computer da polso, brevettato dalla multinazionale dell'e-commerce, guiderà i

dipendenti verso i prodotti che dovranno impacchettare e rendere disponibili per la consegna.
Il sito *Geek Wire* ha ricostruito il funzionamento del braccialetto. Una volta indossato, sfrutta una rete di trasduttori a ultrasuoni posizionati nei magazzini e permette di tracciare i movimenti di chi lo indossa.
Amazon ha depositato il brevetto nel 2016, ma solo lo scorso 30 gennaio è stato approvato. Anche se per il momento ci si muove nel campo delle ipotesi, la multinazionale potrebbe adottarlo nei propri centri logistici.

In futuro, sostiene *Gizmodo*, il bracciale consentirà al gigante di Jeff Bezos di puntare alla completa automazione del processo che va dall'acquisto alla spedizione dei prodotti, riducendo però i dipendenti a propaggini di una procedura gestita da algoritmi e sensori. A destare dubbi c'è anche la questione relativa alla privacy, perché i movimenti di chi indossa il dispositivo sono mappati senza sosta.
L'intento rimane quello di accelerare i tempi di evasione degli ordini, una pista che Amazon percorre in continuazione cercando un costante miglioramento delle performance. Non senza incorrere in problemi, come nel caso della videocamera che apre le porte ai fattorini.
Geek Wire, commentando questa novità, ha rilanciato una tesi diffusa negli Stati Uniti, secondo la quale Amazon tenderebbe a cancellare le differenze tra dipendenti umani e robot. La polemica torna con ciclicità agli onori delle cronache. In Italia il

malcontento dei dipendenti è legato ai contratti e ha portato a uno sciopero in occasione del Black Friday".

A questa descrizione c'è poco da aggiungere: si è in presenza di una vera e propria "fabbrica dei pacchi" con ritmi di lavoro, oggi dettati dalla cosiddetta "intelligenza artificiale", ma che poco hanno da invidiare a quelli delle vecchie fabbriche.

La cosa inusuale è stata la reazione violenta (verbalmente) del mondo politico: una "levata di scudi" da parte di tutti i partiti, dalla sinistra all'estrema destra, con l'ultima parola lasciata all'allora ministro dello sviluppo economico, Calenda, che convocò i rappresentanti di Amazon dichiarando, a conclusione dell'incontro, che "abbiamo chiarito ad Amazon che braccialetti non si usano e non si useranno in Italia. Bene investimenti ma con qualità del lavoro".

In realtà nella logistica e nella grande distribuzione commerciale sono già presenti e non hanno sollevato un analogo scandalo o discussione.

Ma nell'aprile si apre un'altra polemica sui braccialetti. Questa volta c'è una localizzazione precisa: si tratta di Livorno.

Lo spiega un articolo dell'Ansa di quei giorni, che titola "A Livorno scoppia il caso braccialetti elettronici. Il Comune si "ispira" ad Amazon?".

L'articolo spiega poi, in materia sintetica, la questione: "Gli operatori ecologici dotati dei "wearable" device (i famosi

braccialetti) per tenere traccia dei cestini svuotati. Insorgono i sindacati", L'amministrazione replica: "Non c'è Gps, non monitora la produttività".

Un nuovo "caso braccialetto elettronico", ma questa volta su scala molto ridotta. Se il colosso dell'e-commerce stava studiando un sistema per dotare i propri dipendenti addetti alla logistica nei centri di stoccaggio di wearable per individuare con più facilità i pacchi sugli scaffali, e per questo si era meritata l'accusa di essere un "grande fratello" che voleva controllare in tempo reale i movimenti dei propri dipendenti nei magazzini, una circostanza simile sta succedendo proprio in queste ore nella città di Livorno. La protagonista è l'amministrazione comunale della città toscana, che ha dotato i propri operatori ecologici di un braccialetto elettronico in grado di connettersi con i 2.500 nuovi cestini della spazzatura installate sul territorio per "certificarne" lo svuotamento.

A stretto giro la replica dell'amministrazione comunale, che respinge le accuse: "non c'è nessun controllo dei dipendenti", ma semplicemente una tecnologia Rfid "priva di Gps che non monitora gli spostamenti o la produttività dei lavoratori".

Di cosa si tratta allora? Il device wearable, utilizzato da Avr, società che ha in appalto la pulizia stradale per conto della municipalizzata Aamps, serve soltanto per tenere sotto controllo lo svuotamento dei cestini.

“Il braccialetto è un semplice lettore, come quelli usati quando si fa la spesa al supermercato, sottolinea l’amministrazione comunale, che certifica solo lo svuotamento di un cestino. Un servizio simile è già in uso a Lucca per la raccolta porta a porta dei rifiuti. È una tecnologia al servizio del cittadino per gestire meglio il servizio per il quale viene pagata la Tari, e non ha nulla a che fare con il modello Amazon”.

Nuove tecnologie, nuove tutele

Come si spiega questa rinnovata attenzione a tematiche molto importanti, come la tutela dei lavoratori rispetto a controlli a distanza sempre più intrusivi? Non è solo questione di nuove tecnologie, anche se l’introduzione di alcune di esse, come ad esempio i “braccialetti” hanno impressionato la pubblica opinione.

C’è da dire che sta crescendo non solo la sensibilità dei cittadini rispetto alla tutela dei propri dati personali e all’eccessiva invadenza di strumenti di controllo all’interno dei luoghi di lavoro, ma si sta rafforzando anche il complesso delle normative tese a far rispettare questi diritti.

2.6 Cosa succede in Italia

Si parte dal 2014. È questo infatti l'anno in cui viene approvata la legge delega in materia di lavoro, che porterà l'anno successivo all'emanazione di numerose leggi delegate che prenderanno il nome di jobs act.

Non è questo il luogo per analizzare e valutare i contenuti dei singoli provvedimenti, che peraltro hanno dato vita a forti polemiche e ad accese discussioni.

Per quanto riguarda, invece, i temi che qui si affrontano, si sottolinea che uno dei provvedimenti che modifica in maniera significativa l'art. 4 dello Statuto dei lavoratori ribadisce però lo stretto legame tra lo stesso Statuto e il Codice per la protezione dei dati personali, rafforzandone l'efficacia.

Il 2016 è l'anno in cui, sulla scorta di quelle norme, si registrano importanti pronunce ed interpretazioni delle norme sui controlli a distanza, destinate ad incidere sui casi concreti e ad ampliare gli spazi lasciati alla contrattazione e, quindi, a quella che si potrebbe definire "co-determinazione" tra le parti.

Naturalmente all'inizio non si è in presenza di pareri convergenti, nell'analisi che faremo partiremo da alcuni organi periferici del Ministero del lavoro per andare alle sempre più autorevoli indicazioni del Garante della protezione dei dati personali e per finire a quella decisiva dell'Ispettorato nazionale del lavoro.

Il Ministero del Lavoro: la Direzione interregionale di Milano

Un primo intervento interpretativo viene dalla Direzione Interregionale di Milano. La circolare del 10 maggio 2016, molto cauta e conservatrice, precisa in premessa che le sue affermazioni sono subordinate e quindi valide solo se non "smentite" dalle due Direzioni generali del Ministero del lavoro, alle quali sono inviate per conoscenza, cioè la Direzione Generale per l'Attività Ispettiva (ancora attiva) e quella della Direzione Generale della Tutela delle condizioni di lavoro e delle relazioni industriali.

Non staremo ad analizzare punto per punto questa prima interpretazione (ne vedremo altre più interessanti e decisive) che, a nostro parere si caratterizza in senso conservatore e limitativo dello spazio concesso dal legislatore alla contrattazione tra le parti.

Sull'argomento si precisa che sia l'autorizzazione amministrativa rilasciata dalla DTL sia l'accordo sindacale devono avere ad oggetto esclusivamente la verifica della sussistenza di una delle tre esigenze tassativamente indicate dal legislatore (produttive ed organizzative, sicurezza del lavoro, tutela del patrimonio) quali legittimanti l'installazione.

Così vengono sottolineate tutte le situazioni da cui vengono esclusi gli accordi o le autorizzazioni ministeriali.

La grande novità è invece rappresentata dal 2 comma: l'accordo sindacale *ovvero l'autorizzazione amministrativa non sono*

necessari per gli strumenti di lavoro e per gli strumenti di registrazione delle presenze e degli accessi in azienda.

In tal senso, il Ministero del lavoro ha così precisato sul proprio sito istituzionale «la modifica all'articolo 4 dello Statuto chiarisce, poi, che non possono essere considerati strumenti di controllo a distanza gli strumenti che vengono assegnati al lavoratore per rendere la prestazione lavorativa, una volta si sarebbero chiamati gli "attrezzi di lavoro", come pc, tablet e cellulari. In tal modo, viene fugato ogni dubbio per quanto teorico, circa la necessità del previo accordo sindacale anche per la consegna di tali strumenti ai dipendenti.

Cassazione e la migliore dottrina confermano la nozione di strumento di lavoro quale "strumento idoneo ad assolvere complessivamente una funzione di mezzo necessario normalmente (secondo le regole dell'arte) per rendere la prestazione lavorativa".

Si arriva quindi, per quanto riguarda i gps, ad affermare come non necessario l'accordo sindacale, soprattutto nel caso di un veicolo acquistato con il gps incorporato.

Ma, come vedremo, non è questa la giusta interpretazione.

La stessa cosa possiamo dire per gli altri esempi citati, come i "controlli in cuffia" di un operatore di call center e le app inserite negli smartphone.

Questa circolare sposta tutte le tutele per i lavoratori nel solo spazio della “privacy”.

Oggi infatti le informazioni raccolte dal datore di lavoro (sia con gli strumenti di controllo a distanza autorizzati sia con gli strumenti di lavoro dati semplicemente in uso al lavoratore) sono utilizzabili a tutti i fini connessi al rapporto di lavoro solo nel pieno rispetto di due obblighi di legge:

“che sia stata fornita adeguata informazione ai lavoratori circa l’uso degli strumenti e le modalità di effettuazione dei controlli; che le informazioni siano utilizzate nel pieno rispetto delle previsioni contenute nel D”.

Lgs n. 196/2003 e dei provvedimenti del Garante per la privacy (principio dl liceità, principio di pertinenza, principio di correttezza, principio di necessità, principio di non eccedenza).

Quindi, oggi la tutela dei lavoratori nei confronti dei controlli datoriali trova adeguata ed appropriata tutela nell’impianto sanzionatorio predisposto dalle norme sulla privacy poste a presidio della dignità dei lavoratori.

Tanto premesso, a parere di questa Direzione lnterregionale l’auto fornita in uso ai dipendenti per eseguire la propria prestazione lavorativa è sicuramente strumento di lavoro e lo è nella sua unicità: quindi il sistema GPS (pur se montato successivamente alla originaria consegna del veicolo) non è da considerare separatamente dall’auto cui accede e per la sua

installazione non è necessario il preventivo accordo sindacale o la preventiva autorizzazione ministeriale.

Molto diversa l'interpretazione del Garante per la protezione dei dati personali

Anche il Garante ha l'occasione di pronunciarsi nel corso del 2016, incominciando a dare indirizzi interpretativi al complesso delle norme relative ai gps.

Possiamo citare ad esempio il caso di una richiesta di parere preventivo al Garante avanzato da una S.P.A. in relazione al trattamento dei dati personali connesso all'attivazione di una funzionalità di localizzazione geografica mediante l'installazione di una specifica applicazione sugli smartphone aziendali forniti in dotazione ai dipendenti che svolgono l'attività lavorativa all'esterno delle sedi aziendali. Il dispositivo consentirebbe di raccogliere, al momento dell'attivazione dell'applicazione da parte del lavoratore, l'orario di "inizio e fine lavoro, […] inizio e fine pausa pranzo, […] inizio e fine di un evento meteorologico di maltempo" associato alla rilevazione della posizione geografica effettuata mediante il sistema GPS - Global Positioning System.

Gli scopi perseguiti con l´adozione del sistema sono indicati nella possibilità di effettuare il "calcolo della presenza dei dipendenti, orario di lavoro – ordinario, straordinario, notturno – per l´elaborazione della busta paga; il calcolo della

sospensione momentanea o definitiva del lavoro e conseguentemente l´orario di lavoro effettivo svolto; nonché il calcolo delle indennità di viaggio e di trasferta spettanti al dipendente e per conoscere la località ove si verifica l´evento meteorologico del maltempo che l´Azienda deve indicare nella richiesta di Cassa integrazione ordinaria.

In risposta il Garante sottolinea la necessità che l'azienda si attenga alle seguenti indicazioni:

a. adottare specifiche misure idonee a garantire che le informazioni presenti sul dispositivo mobile visibili o utilizzabili dall'applicazione installata siano riferibili esclusivamente a dati di geolocalizzazione nonché ad impedire l'eventuale trattamento di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta
elettronica o alla navigazione in internet o altro);

b. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva; l'icona dovrà essere sempre chiaramente visibile sullo schermo del dispositivo, anche quando l'applicazione lavora in background;

c. consentire l'accesso ai dati trattati ai soli incaricati della società che, in ragione delle mansioni svolte o degli incarichi affidati, possono prenderne legittimamente conoscenza;

d. in relazione all'accesso ai dati di localizzazione nel sistema aziendale di gestione del personale, assegnare credenziali di autenticazione differenziate per ogni incaricato, individuando profili autorizzativi personalizzati e limitando quanto più

possibile l'assegnazione di profili con funzionalità di modifica ed estrazione dei dati; con riferimento a tali ultimi profili autorizzativi, registrare gli accessi ai dati di rilevazione
tramite un apposito file di log riportante la data e l'ora dell'operazione, il tipo di operazione effettuata, i dipendenti visualizzati e l'identificativo dell'incaricato;

e. individuare tempi certi per la cancellazione dei dati conservati temporaneamente sul dispositivo, che deve essere effettuata dal dipendente salvaguardando eventuali esigenze di ulteriore conservazione da parte dello stesso;

f. rammenta la necessità di effettuare la notificazione al Garante ai sensi dell'articolo 37, comma 1, lett. a), del Codice, di fornire ai dipendenti un'informativa completa di tutti gli elementi previsti dall'articolo 13 del Codice, di predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 7 e seguenti del Codice;

g. rammenta la necessità di attenersi, in quanto applicabili, alle prescrizioni ed alle raccomandazioni contenute nel provvedimento del Garante del 1° marzo 2007, n. 13 ("Linee guida per posta elettronica e internet"), in caso di trattamenti effettuati in occasione della predisposizione di idonee misure di sicurezza per assicurare la disponibilità e l´integrità di sistemi informativi e di dati e a seguito della riconsegna del dispositivo per interventi di manutenzione o a seguito della cessazione del rapporto di lavoro".

Ancora più decisiva l'interpretazione dell'Ispettorato nazionale del Lavoro

Il 2016 è l'anno in cui si realizza una importante novità dal punto di vista istituzionale: la creazione dell'*Ispettorato Nazionale del Lavoro*, che assume il ruolo di agenzia unica per il controllo dell'osservanza delle norme sul lavoro.

Da subito questa agenzia si assume il ruolo di interpretare in profondità le disposizioni relative ai controlli a distanza dei lavoratori, determinando con il suo intervento precise conseguenze pratiche.

La distinzione tra "strumenti per rendere la prestazione" e "strumenti per migliorare la prestazione"

L'occasione per l'intervento dell'Ispettorato nazionale del lavoro è data da alcune questioni sollevate a proposito dell'installazione dei gps.

Cosa viene affermato di tanto innovativo a proposito delle apparecchiature Gps? Semplicemente che, in linea di massima, i sistemi di geolocalizzazione rappresentano "un elemento aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro.

Fini nobili, ma che non esimono dall'applicazione di quanto stabilito dall'art. 4 dello Statuto, anzi a maggior ragione ne va applicata la parte che prevede la necessità di un previo confronto con le organizzazioni sindacali al fine di trovare un accordo.

È questa la regola generale. L'eccezione è invece quella che si realizza solo in casi del tutto particolari, qualora i sistemi di localizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa e cioè la stessa non possa essere resa senza ricorrere all'uso di tali strumenti, ovvero l'installazione sia richiesta da specifiche normative di carattere legislativo o regolamentare (es. uso dei sistemi GPS per il trasporto di portavalori superiore a euro 1.500.000,00, ecc.), si può ritenere che gli stessi finiscano per trasformarsi in veri e propri strumenti di lavoro e pertanto si possa prescindere, ai sensi di cui al comma 2 dell'art. 4 della L. n. 300/1970, sia dall'intervento della contrattazione collettiva che dal procedimento amministrativo di carattere autorizzativo previsti dalla legge.

Quello che va da subito sottolineato è che, sulla base di questa interpretazione, si è aperta la strada all'applicazione della procedura prevista dall'art.4 dello statuto dei lavoratori anche per quanto riguarda l'installazione di numerose altre applicazioni, capaci di "vedere" e registrare molteplici dati personali dei dipendenti.

2.7 Gli accordi sulla geolocalizzazione

A questo punto possiamo riprendere il nostro discorso sui gps e sugli accordi sottoscritti da Filcams Cgil, Fisascat Cisl, Uiltucs Uil riguardanti la loro installazione.

Un esempio

Un'azienda che progetta, realizza e installa montascale manifestava l'intenzione di dotare i propri camioncini, utilizzati dai tecnici per le consegne e il montaggio dei montascale a casa dei clienti, di un sistema gps.

Lo scopo dichiarato era quello di un utilizzo del sistema non solo a protezione del patrimonio aziendale, ma anche a fini pratici, come, ad esempio, indicare agli autisti la più via breve o migliore (a giudizio di un operatore centrale) per raggiungere il cliente. Il che avrebbe implicato anche un monitoraggio continuo del veicolo.

Queste indicazioni, come abbiamo visto, erano in contrasto con quanto indicato dal Garante della protezione dei dati personali, che aveva prescritto la necessità di dare non solo una adeguata informazione ai lavoratori, ma anche di predisporre le necessarie limitazioni all'uso delle geolocalizzazioni.

Inoltre, in alcune sue pronunce, il Garante aveva già stigmatizzato i comportamenti dei titolari che non avevano provveduto "a configurare il sistema tecnologico mediante

misure adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (cfr. in proposito, oltre ai citati articoli del Codice, l'art. 25 del Regolamento (UE) 2016/679, in attuazione del principio di c.d. privacy by default; si veda anche il Provvedimento di carattere generale in materia di localizzazione dei veicoli nell'ambito del rapporto di lavoro, 4 ottobre 2011, n. 370, in www.garanteprivacy.it, doc. web n. 1850581, laddove il Garante ha stabilito che "nel rispetto del principio di necessità (artt. 3 e 11, comma 1, lett. d), del Codice), la posizione del veicolo di regola non dovrebbe essere monitorata continuativamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite").

Le soluzioni adottate nell'accordo

L'accordo è stato quindi raggiunto seguendo le indicazioni del Garante ed inserendo precisi limiti all'utilizzo del gps.

Tra questi i più importanti sono quelli relativi al *non monitoraggio continuo* degli autoveicoli e alla *cancellazione dei dati* dopo un periodo prefissato.

Dopo aver ripetuto che le motivazioni sottostanti all'accordo sono di carattere organizzativo, di sicurezza dei lavoratori e di tutela del patrimonio aziendale, si precisa in particolare che si vuole consentire:

a. una rapida localizzazione dei mezzi in caso di furto o l'invio di tempestivi soccorsi;
b. un incremento della sicurezza dei dipendenti, specie quando si trovano a lavorare in luoghi impervi o in condizioni ambientali avverse, consentendone un'immediata localizzazione attivabile anche dall'operatore in caso di bisogno;
c. l'assicurazione di una più efficiente gestione e manutenzione del parco veicoli con effetti vantaggiosi sulla sicurezza dei lavoratori e collettiva.

A fronte di queste finalità vengono, però, anche indicati alcuni limiti nell'utilizzo dei gps, che possiamo così sintetizzare:

1) la geolocalizzazione non sarà continua;
2) verranno rispettati, rispetto ai dati potenzialmente acquisibili, i criteri di pertinenza e di non eccedenza;
3) i dati raccolti non potranno essere utilizzati per eventuali accertamenti sull'obbligo di diligenza dei lavoratori e, quindi, non potranno essere usati per l'adozione di provvedimenti disciplinari;
4) in caso di infrazioni amministrative i dati non potranno essere conservati oltre i 90 giorni;
5) ai lavoratori sarà data adeguata informazione sulle modalità di trattamento dei propri dati personali;
6) i dati saranno gestiti direttamente dall'azienda e sarà reso noto il responsabile del trattamento dei dati designato.

Altro esempio

In questo caso siamo in presenza di un'azienda che, opera nella distribuzione automatica di prodotti alimentari; le motivazioni che la spingevano ad installare su tutti i propri autoveicoli un segnalatore gps erano:

a) ottenere una maggiore sicurezza sul lavoro, che nello specifico si potevano realizzare promuovendo comportamenti di guida virtuosi, finalizzati a prevenire incidenti;
b) tutelare il patrimonio aziendale, evitando il danneggiamento e il deterioramento dei veicoli e il rischio di rapine.

I dati ricavati dai gps sarebbero confluiti in una ricerca attivata dalla "casa-madre", ricerca che avrebbe coinvolto tutte le sue filiali.

L'azienda, affidandosi ad una ditta specializzata, si proponeva, infatti, di analizzare i dati relativi alle distanze percorse, alla durata media nella guida e al comportamento degli autisti nella guida stessa (rispetto dei codici della strada, dai limiti di velocità in poi, durata del motore acceso a veicolo fermo ecc.).

Naturalmente le organizzazioni sindacali italiane, prima di dare l'assenso a questa operazione, hanno richiesto tutta una serie di garanzie.

In primo luogo l'azienda doveva procedere, in via preliminare, ad una "valutazione d'impatto sulla protezione dei dati (DPIA)", prevista dal comma 1, art.35 del Regolamento europeo sulla protezione dei dati.

Oggetto di questa valutazione: il trattamento dei dati dal punto di vista della necessità e proporzionalità e della gestione dei rischi per i diritti e le libertà delle persone.

All'esito positivo di questa valutazione d'impatto (i cui risultati sono stati allegati) si è proceduto a stipulare l'accordo, che prevede una serie di limitazioni all'uso dei gps, anche una volta montati.

Qui di seguito elenchiamo i principali impegni inseriti nell'accordo:

1) la non identificazione del singolo veicolo e quindi del singolo lavoratore che vi opera;
2) il coinvolgimento dei soli veicoli utilizzati per ragioni di servizio, con la conseguente esclusione di quelli ad uso promiscuo (personale e di lavoro);
3) una capillare informazione ai singoli lavoratori sull'installazione dei gps e sulle modalità di raccolta dati;
4) la nomina di tre rappresentanti sindacali aziendali, uno per organizzazione firmataria dell'accordo, cui far giungere un report mensile sulla raccolta dati;
5) ampie garanzie di anonimato, per cui i dati dovranno essere raccolti ed aggregati per un minimo di 10 veicoli,

scelti in modo casuale per aree geografiche; i dati avranno anche una misura temporale non meno di 30 giorni;

6) la cancellazione, dopo un anno, di tutti i dati;
7) infine, elemento non certo ultimo per la sua importanza, il non utilizzo dei dati per fini disciplinari.

In conclusione, al fine di contemperare gli interessi delle parti, i gps non vengono disattivati per garantire una omogeneità dei dati rispetto ai rilevamenti effettuati in tutte le filiali dell'azienda.
Abbiamo visto, quindi, come le caratteristiche dell'accordo rispondano sia alle esigenze organizzative e di tutela del patrimonio aziendale sia alla protezione dei dati personali dei lavoratori, che potranno continuare a lavorare senza il timore di possibili provvedimenti disciplinari.

Va anche detto che le organizzazioni sindacali sono comunque consapevoli che questa acquisizione di dati sull'utilizzo dei veicoli, ottenuti attraverso l'uso della geolocalizzazione, sconterà una serie di imprecisioni.

Basti pensare alla difficoltà di registrare gli scostamenti tra velocità reale degli automezzi e quella consentita dai relativi codici della strada. Almeno in Italia questo rischia di essere abbastanza difficile: non ci sono infatti solo le velocità teoriche da rispettare; che succederà infatti in caso di lavori che impongano rallentamenti non previsti o, viceversa, in caso di ripristino di una viabilità ordinaria?

Da questo punto di vista non c'è google che tenga!

In ogni caso si determinerà una organizzazione del lavoro, per questa azienda di vending, molto più rigida di quella attuale e questo comporterà comunque la necessità di aprire un confronto sulle nuove modalità di lavoro (ad esempio: se si va più lenti, saranno necessari più veicoli e più lavoratori per effettuare le stesse consegne di prima).

C) Le tecnologie della comunicazione

Partiamo dando uno sguardo generale alla "società della comunicazione", aiutati in questo dalla panoramica tratteggiata da Antonello Soro, che è stato, qualche anno fa, il Garante per la protezione dei dati personali:

"Siamo partecipi di una proliferazione inarrestabile delle connessioni mobili, della progressiva integrazione dei diversi strumenti di comunicazione, dello sviluppo innovativo delle applicazioni tecnologiche, sempre più piccole e indossabili.

Siamo immersi – spesso inconsapevolmente – nella società digitale e sempre di più conosciamo noi stessi, il mondo e gli altri attraverso la tecnologia".

Tutto questo ovviamente ci riguarda sia come cittadini che come operatori economici e lavoratori.

2.8 Un cambiamento culturale per vivere da protagonisti

È necessario quindi partire dal concetto di riservatezza dei dati personali perché *"l'idea di privacy, nella sua corretta accezione, rappresenta un segnalatore importante della organizzazione sociale, giuridica, valoriale del nostro tempo: attraverso questo punto di osservazione è possibile cogliere tendenze e contraddizioni, intravvedere gli orizzonti, forse assumere decisioni più consapevoli.*

Il diritto alla riservatezza, tradizionalmente inteso come diritto ad essere lasciati soli e tutelare la vita intima da ingerenze varie, ha assunto nel tempo un profilo sempre più connesso alla tutela della dignità della persona.

Il diritto alla protezione dei dati personali riconosciuto come fondamentale nella Carta europea dei diritti dell'uomo e costituzionalizzato dal Trattato di Lisbona, deve fare oggi i conti con la sfida più difficile e complessa posta dalla rete e dalle nuove tecnologie della comunicazione".

Se, infatti, non ci rendiamo conto dell'importanza fondamentale dei dati che ci riguardano personalmente, siamo

quasi sempre disponibili a fornirli a chi “in cambio” ci offre servizi sulla “grande rete” i dati diventano merce di scambio sempre più esposti a forme –spesso occulte – di raccolta e di monitoraggio continuo: è oggi possibile, grazie alle tecnologie, superare i limiti di tempo e di spazio, aggregare, analizzare ed archiviare quantità enormi di informazioni a costi contenuti.

Il primo obbiettivo della profilazione di massa è certo quello di conoscere gli orientamenti dei consumatori: gli Over The Top, i grandi monopolisti di internet che hanno un dichiarato interesse commerciale, raccolgono e archiviano in giganteschi server i dati personali che sono stati forniti per le più diverse ragioni: dai motori di ricerca alla posta elettronica, dalle piattaforme di condivisione dei video ai servizi di commercio online, ai viaggi, agli affari, ma soprattutto dalle reti sociali così largamente partecipate dai ragazzi fin dalla prima adolescenza.

In questo modo realizzano le più sofisticate forme di pubblicità comportamentale, diventando intermediari sempre più esclusivi tra produttori e consumatori, orientano le nostre scelte e spesso le nostre conoscenze, accumulano ricchezze incredibili, trattano da pari con i governi.

Ma i dati raccolti e trattati possono essere usati per costruire profili minuziosi di cittadini da controllare, per legittime ragioni di sicurezza, con modalità sempre più invasive.

Che fare dunque di fronte a questa “invadenza digitale” che può avere risvolti assai pericolosi?

Ebbene bisogna fare in modo che l**e regole e le tutele** previste nello spazio fisico per prevenire situazioni di pericolo e rimuovere gli ostacoli al libero dispiegamento della propria personalità, trovino cittadinanza anche nello spazio digitale nel quale si svolge una parte così rilevante della nostra quotidianità.

Nello spazio digitale si possono violare le persone, si possono negare o esercitare i diritti, si possono manipolare o perfino rubare informazioni che riguardano strettamente parti fondamentali della nostra esistenza.

L'impatto nella vita aziendale

Non c'è dubbio che nella nuova era digitale la comunicazione aziendale, sia interna che esterna, abbia subito profonde trasformazioni.

Del resto nell'azienda accade quello che accade nella società: oramai tutti ci serviamo di strumenti di comunicazione veloci e facili da usare. Basti pensare ai pc o ai telefonini, che sono entrati oramai in possesso della stragrande maggioranza degli italiani. Tutti conoscono internet e i canali social, da WhatsApp a Twitter.

Evidentemente anche la comunicazione aziendale non può fare a meno di utilizzare questi strumenti.

Un primo problema si presenta nel momento in cui ci sono aziende che si trovano a gestire contemporaneamente i più diversi strumenti di comunicazione, da quelli più tradizionali come le newsletter e i magazine a quelli più digitali come l'intranet o le app di messagistica come appunto WhatsApp e altre analoghe.

C'è quindi la necessità di raccordare tra loro tutti questi strumenti in modo da non costringere i lavoratori a passare da logiche comunicative molto diverse tra loro e rallentarne quindi l'attività.

Inoltre non si può non convenire sul fatto che una comunicazione più semplice e lineare aiuta ad alimentare relazioni di fiducia tra dipendenti e collaboratori.

Tutto questo porta all'introduzione di sistemi in grado di offrire una "comunicazione unificata", una comunicazione che consente, con qualunque dispositivo collegato con internet, di effettuare telefonate e videoconferenze, di integrare tra loro tutti gli strumenti e di condividere ogni tipo di documenti.

2.9 Contrattare le regole e le tutele

A questo punto però non possiamo non preoccuparci del mantenimento degli equilibri tra i diversi interessi e preoccupazioni in gioco.

È questo l'argomento centrale di questa pubblicazione. Ma avendo a disposizione un buon apparato regolatorio che dà un forte impulso alla contrattazione, vediamo come le parti se ne sono servite.

Qui di seguito andremo ad illustrare alcuni accordi aziendali, recenti ed assai significativi, frutto di una contrattazione di merito favorita dalle norme più volte citate.

2.10 Le reti aziendali e le implementazioni dei programmi utilizzati

Faremo precedere l'esposizione dei contenuti degli accordi con spiegazioni, sia pure sintetiche, sul funzionamento dei nuovi sistemi introdotti.

Il sistema Siem (e analoghi)

Parliamo del SIEM (Secury Information and Event Management = Informazioni sulla sicurezza e gestione degli eventi) e spieghiamo brevemente cosa è e come funziona.

Con questa tecnologia si realizza una raccolta centralizzata dei log (registri) e degli eventi generati da applicazioni e sistemi in rete, per consentire agli analisti di ridurre i tempi necessari alla risoluzione dei problemi e alle indagini su allarmi e incidenti di sicurezza.

Il SIEM, quindi, raccoglie, analizza e mette in correlazione un elevato numero di dati provenienti da:

- strumenti di sicurezza come, ad esempio, sistemi antivirus e anti malware, VPN, filtri web o firewalls;
- dispositivi di rete, come routers, switch, DNS server, wireless access point, data transfer ecc.;
- dispositivi degli utenti, server di autenticazione, database;
- applicazioni intranet e applicazioni web.

Il principio chiave del SIEM è un monitoraggio evoluto, basato sulla capacità di aggregare dati significativi, stabilendo in tempo reale analisi e correlazioni finalizzate a individuare comportamenti anomali, segnali critici e a generare allarmi.

Cosa fa il SIEM e quali sono le sue principali funzioni.

- *Raccoglie dati*: i log sono la fonte principale di dati analizzati da un SIEM. Ogni apparato di sicurezza, software, database, presente nel sistema invia i dati contenuti all'interno dei file di log al server principale sul quale risiede il SIEM.

- *Normalizza i dati*: siccome ogni dispositivo gestisce e conserva i dati a modo suo, il SIEM provvede ad uniformarli, agevolandone l'interpretazione.
- *Mette in correlazione i dati*: sebbene il SIEM disponga di una serie di regole di correlazione già predefinite, mette a disposizione la possibilità di creare delle regole personalizzate al fine di soddisfare le esigenze degli amministratori.
- *Crea rapporti specifici*: l'archiviazione dei dati a lungo termine unita alla possibilità di sfruttare query personalizzate per l'estrazione dei dati, consentono la creazione di report.
- *Crea notifiche*: I segnali di notifica e avviso vengono generati al presentarsi di determinati eventi, informando gli utenti di una possibile minaccia.

Diciamo subito che il mercato di queste nuove tecnologie è in grande espansione a causa della crescente attività di "banditi informatici", che cercano immediati e facili profitti violando gli accessi alle reti, sia private che pubbliche, minacciando massicci furti di dati o criptandoli e quindi rendendoli inservibili.

Il tutto con gravi conseguenze sulla vita economica e civile: basti pensare agli attacchi, in parte riusciti, ai database di aziende, banche, amministrazioni pubbliche ed ospedali. Queste azioni di ricatto sono state denunciate in numero crescente negli ultimi mesi e non si sa più se siamo in presenza di solo banditismo economico o anche, cosa che sarebbe

ancora più pesante, di tipo politico (una vera e propria guerra informatica non dichiarata).

C'è quindi una forte rincorsa, da parte delle aziende, ad implementare le misure di sicurezza relative ai propri database ed alle proprie reti di comunicazione.
Il tema quindi è di grande attualità.

Perché è necessario utilizzare la procedura prevista dal GDPR (Regolamento generale per la protezione dei dati personali) e dall'art.4 dello Statuto dei lavoratori

La risposta è abbastanza semplice.

Da un lato siamo in presenza di "dati relativi a comunicazioni elettroniche" (e-mail, comunicazioni telefoniche o messaggistica online e simili). In questo caso deve essere applicato il Regolamento generale per la protezione dei dati personali.

Dall'altro il SIEM attua un controllo sistematico e centralizzato delle interazioni computer/utente/applicazione, potendo quindi potenzialmente determinare un controllo a distanza dell'attività dei lavoratori, motivo per cui la sua installazione, in base all'art. 4 dello Statuto dei lavoratori, deve formare oggetto di preventivo accordo con i sindacati o, se non raggiunto, di autorizzazione da parte dell'Ispettorato del lavoro.

Primo esempio di accordo in:

una azienda che opera nel settore dei giochi, delle lotterie e delle sale da gioco.

Nella premessa dell'accordo l'azienda spiega le finalità che sono alla base dell'attivazione di un più efficiente sistema di protezione da "rischi cibernetici":

"i sistemi di sicurezza hanno la finalità di difesa da attacchi sulla struttura IT interna (hardware, applicazioni e dati); i sistemi in adozione hanno quindi l'unico scopo di riconoscere e analizzare comportamenti anomali o cambiamenti inaspettati dei sistemi IT. Non è obbiettivo dell'azienda quello di identificare il comportamento individuale o la condotta del dipendente né di effettuare controlli sulla perfomance, fintantoché il comportamento individuale non contribuisce a causare danneggiamenti dei sistemi tecnici di sicurezza e della protezione dei dati all'interno dell'infrastruttura IT e quindi a danneggiare la protezione aziendale; i server di conservazione dei dati sono su territorio italiano e rientrano quindi nel campo di applicazione della regolamentazione del nostro Paese; l'azienda, pertanto, nel rispetto di quanto previsto dall'art. 4 L. n. 300/1970, dal Regolamento UE 679/2016 e dal D.Lgs. n. 196/2003, intende far uso di sistemi di monitoraggio".

In particolare il monitoraggio viene effettuato:

- per la sicurezza della rete informatica oggetto della concessione dell'Agenzia delle Dogane e dei Monopoli,

per la realizzazione e conduzione della rete per la gestione telematica del gioco lecito mediante gli apparecchi da divertimento e intrattenimento previsti dall'articolo 110, comma 6, del Testo Unico delle Leggi di Pubblica Sicurezza (T.U.L.P.S.);

- per i requisiti della certificazione alla norma IS27001 al fine di assicurare la protezione del proprio sistema informatico da minacce e vulnerabilità e rispondere efficientemente a situazioni anomale garantendo una pronta reazione e la continuità dei servizi e la produttività aziendale;
- per la rilevazione di eventuali data breach **(*26)*** che si possano verificare all'interno delle infrastrutture informatiche aziendali ai sensi del Regolamento UE 679/2016".

Le garanzie per i lavoratori

Le garanzie, che l'azienda offre ai lavoratori per una gestione e un utilizzo corretto del suo rafforzato controllo sull'attività lavorativa, sono di due tipi, *uno di carattere generale e uno più specifico*, di carattere procedurale.

A livello generale si afferma, che "i sistemi di monitoraggio gestiti ed impiegati dalla Società possono essere utilizzati per fini probatori nonché in conformità con quanto previsto all'art. 4, L. n. 300/1970, e comunque senza alcuna finalità

persecutoria nei confronti dei dipendenti. Tali sistemi, su specifico impegno dell'azienda, rispettano il principio di proporzionalità tra i mezzi impegnati e i fini perseguiti, in applicazione delle regole imposte dal Garante della Privacy".

Si spiega poi che "i sistemi sopra citati sono gestiti in via centralizzata dall'azienda e sono amministrati esclusivamente dal personale di Sicurezza e Compliance IT, il quale è formalmente designato Amministratore di Sistema, secondo quanto previsto dal Provvedimento del Garante del 27 novembre 2008 in materia di "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".*

Il personale di Sicurezza e Compliance IT accede ai sistemi di monitoraggio esclusivamente attraverso l'utilizzo di credenziali nominali e vi opera in conformità con quanto previsto dallo standard ISO IEC 27001:2013, di cui l'azienda possiede regolare certificazione emessa da ente terzo certificatore. Gli accessi degli Amministratori di Sistema sono tracciati secondo quanto previsto dal Provvedimento del Garante del 27 novembre 2008, di cui sopra.

Sia le funzionalità di analisi automatica che quelle di conservazione sopra citate saranno attive H 24. I periodi di conservazione precedentemente illustrati sono individuati tenendo conto delle tempistiche necessarie per verificare e

analizzare eventuali anomalie nel traffico dati da parte degli Amministratori di Sistema".

Si avvicina molto di più alla realtà concreta vissuta dai lavoratori quanto indicato, in forma più specifica, successivamente, quando si indica il che fare in caso di anomalie riscontrate dal sistema.

In questi casi si mette in moto un meccanismo procedurale che prevede una gradualità di interventi finalizzati alla risoluzione delle anomalie stesse, senza addebiti, almeno in una prima fase, nei confronti dei lavoratori.

Al verificarsi di un evento, errore o problema tecnico per la sicurezza che abbia generato la segnalazione di un'anomalia, rilevata ad opera dei sistemi di monitoraggio implementati in azienda, i dati (a titolo esemplificativo e non esaustivo: dettaglio del dato di navigazione, numero seriale della macchina assegnata al dipendente, username, ecc.), saranno analizzati, da parte del personale di Sicurezza e Compliance IT, per le verifiche del caso, anche attraverso l'identificazione del dipendente associato all'indirizzo IP che abbia generato l'anomalia. In tali casi, i dati potranno essere estratti dai sistemi onde evitarne la cancellazione automatica e potranno essere utilizzati - in conformità con quanto previsto dal provvedimento del Garante, in materia di "Lavoro: le linee guida del Garante per posta elettronica e internet" (pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007) - secondo quanto

espressamente previsto dalle politiche aziendali vigenti nonché in conformità con quanto previsto dall'art. 4, L. n. 300/1970.

La funzione Sicurezza e Compliance IT, se ritenuto necessario per ragioni di sicurezza del sistema, potrà contattare - pure per le vie brevi - il dipendente associato all'indirizzo id anche al fine di richiedere la sua collaborazione per…riportare alla normalità il sistema; in ogni caso la funzione Servizio e Compliance IT potrà inviare un avviso generalizzato all'intera Direzione/Funzione, dove si è verificato l'evento anomalo.

In caso di singola anomalia ritenuta grave dalla funzione Sicurezza e Compliance IT o di anomalie reiterate generate dallo stesso utente, Sicurezza e Compliance IT potrà inviare al dipendente una comunicazione non avente finalità disciplinari, contenente l'indicazione dell'anomalia riscontrata e l'invito, ove ritenuto utile, a fornire eventuali considerazioni e/o suggerimenti al riguardo entro 5 giorni. Trascorso tale termine Sicurezza e Compliance IT ha facoltà di segnalare l'anomalia riscontrata all'Ufficio Risorse Umane che attuerà le procedure di sua competenza.

Secondo esempio di accordo in:

un gruppo turistico che controlla l'intera filiera dei servizi turistici. Al suo interno trovano spazio cinque diverse divisioni: Tour Operating, Aviation, Incoming, Hotel Management, Travel Agencies.

In questo caso siamo in presenza dell'installazione del "sistema" SIEM (*Security Information and Event Management*) vero e proprio, che è la piattaforma scelta dall'azienda "per la raccolta centralizzata dei log e degli eventi generati da applicazioni e sistemi in rete, per consentire agli analisti di sicurezza di ridurre i tempi necessari alla risoluzione e alle indagini su allarmi e incidenti di sicurezza".
Il principio-chiave, nell'utilizzo del sistema, "è un monitoraggio evoluto in grado di individuare situazioni anomale e segnali critici senza tuttavia l'obiettivo di monitorare l'attività dell'utente".

Le motivazioni che hanno portato l'azienda ad adottare questo nuovo sistema sono quelle comuni a tutte le aziende che stanno organizzando la propria difesa informatica: *"le esigenze organizzative e produttive, la sicurezza del lavoro e la tutela del patrimonio aziendale".*

Le garanzie per i lavoratori

Come vengono conciliate le esigenze di tutela dell'azienda e quelle di riservatezza dei dati personali e di tutela dal controllo a distanza dei lavoratori?

È chiaro che il monitoraggio costante, 24 ore su 24, di tutti i canali informatici su cui opera l'azienda avrà come effetto

quello di produrre un controllo indiretto e incidentale dell'attività lavorativa del personale dipendente; resta quindi inteso che i dati raccolti tramite gli impianti non saranno utilizzabili a fini disciplinari, in deroga a quanto previsto dall'art. 4, comma 3, dello Statuto dei Lavoratori, ad eccezione delle azioni compiute con dolo o colpa grave che emergano eventualmente dalla procedura di cui al successivo punto 7;

6. i dati raccolti saranno conservati, con adeguate misure di sicurezza, in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a 90 giorni dalla loro raccolta, salvi i casi in cui la legge ne preveda la conservazione obbligatoria per un periodo superiore.

L'utilizzo dei dati al fine di sanzionare disciplinarmente eventuali condotte dei lavoratori considerate inadeguate o peggio *è* quindi esplicitamente escluso.

Rispetto all'introduzione del nuovo sistema, l'azienda si impegna a dare ampia informazione ai lavoratori e, in particolare, *"nell'informativa privacy fornita ai lavoratori, in ossequio al disposto dell'art. 4, comma 3, dello Statuto dei Lavoratori, ed in applicazione dell'art. 13 del GDPR".*

Anche in questo accordo, come già visto in quello precedente, si predispongono ulteriori "procedure di garanzia", aggiuntive a quelle previste dallo Statuto.

Nel punto 7 sopra richiamato, si indica quale deve essere il compito delle parti nel caso di un rilevamento di anomalie e cioè:

“gli Amministratori di Sistema attiveranno delle funzioni di analisi più dettagliata dell’evento. Se, per esempio, si dovesse trattare di un sospetto accesso non autorizzato dall’esterno, quindi non riguardante l’utente interno, si procederà a verificare quali ambiti siano stati eventualmente violati, a valutarne gli effetti e ad attuare un piano di rimedio.

In caso di anomalia e/o di disservizio o di non corretto utilizzo delle risorse (dispositivi informatici, rete internet, posta elettronica, etc.) si provvederà – a cura degli Amministratori di Sistema dell’area Infrastructure & IT Security - inizialmente ad un controllo diretto su dati aggregati, riferiti all’intera struttura lavorativa.

Previa informazione alle Rsa/Rsu, con il persistere dell’anomalia, si invierà un avviso circoscritto ai gruppi di persone afferenti all’area/settore in cui è stata rilevata l’anomalia.

Solo nel caso della prosecuzione dell’anomalia il controllo potrà essere effettuato su base individuale. In tal caso il lavoratore potrà richiedere l’assistenza delle Rsa/Rsu aziendali”.

In buona sostanza la procedura vuole agire in positivo per risolvere i problemi e non aprire contenziosi tra azienda e lavoratori. Con ottime ragioni potremmo definire questa norma

contrattuale come un incentivo a relazioni sindacali sempre più partecipative.

I sistemi MDM (Mobile Device Management)

Mentre il Siem opera sulle postazioni fisse, questi altri sistemi operano sui dispositivi mobili (smartphone, mobile computer e tablet). Del resto è abbastanza comprensibile che, se un'azienda aumenta complessivamente la protezione sulla sua rete "fissa", non può lasciare aperti dei buchi per la sua sicurezza sui device utilizzati esclusivamente a fini lavorativi dai propri dipendenti (o dirigenti).

Per una precisione di linguaggio dobbiamo dire che i sistemi MDM gestiscono dispositivi e Sim totalmente aziendali.

Siamo in presenza, quindi, di un importante tassello che completa la protezione delle comunicazioni aziendali.

Ovviamente, anche in questo caso, prima dell'installazione di questi programmi, l'azienda dovrà seguire la stessa procedura che abbiamo visto nel caso del SIEM.

Call center

Su questo tema, di grande rilievo anche pratico, riteniamo opportuno dare un quadro generale di riferimento sulle normative che devono essere osservate e le tutele che devono

essere garantite per limitare il controllo a distanza dei lavoratori e salvaguardarne i dati personali.

Le indicazioni più precise ci sono fornite dal Garante per la protezione dei dati personali e da una sua pronuncia, scaturita da una segnalazione di illiceità di trattamento dei dati dei dipendenti.

In particolare si parte dagli strumenti informatici di cui si è dotata l'azienda per poi giungere a conclusioni riguardanti i relativi e conseguenti obblighi in merito.

La disciplina in materia di controlli a distanza.
Il trattamento dei dati reso possibile dal menzionato sistema per le sue specifiche caratteristiche consente all´operatore di visualizzare le informazioni utili alla gestione del contatto dell´abbonato, in particolare "anagrafica, tipologia di abbonamento, tecnologie disponibili e l´elenco delle telefonate evase, riportante l´ora e la durata della chiamata; ma rende possibili anche altre operazioni di trattamento con riguardo ad informazioni riferibili all´operatore che, di volta in volta, gestisce la chiamata.

In base a quanto emerso nel corso degli accertamenti, il sistema è funzionale a specifiche esigenze organizzative e produttive della società (in particolare, quella di migliorare la qualità del servizio reso nei rapporti con la clientela) e, contrariamente a quanto prefigurato nella segnalazione, non risulta direttamente

preordinato a realizzare un controllo individualizzato e massivo, anche in base a quanto dichiarato, infatti, tali operazioni di trattamento non avrebbero la precipua "finalità di monitoraggio dell´attività degli operatori".

Tuttavia, come accertato, l'applicativo può consentire di risalire in ogni momento all'operatore che ha gestito il contatto telefonico con il cliente. Anche se, infatti, i dati raccolti non risultano associati immediatamente al nominativo dei dipendenti interessati, è tuttavia possibile che le unità organizzative autorizzate possano procedere all'associazione tra i dati raccolti riferiti alla chiamata e alle modalità di evasione della stessa ed un interessato identificabile tramite il "codice operatore" nonché attraverso l'incrocio e la consultazione di informazioni conservate in sistemi separati.

Il sistema, quindi, non si limita a consentire la mera associazione tra la chiamata e l'anagrafica del cliente per facilitare l'attività di gestione della richiesta, come si trattasse di un mero archivio informatico ad uso dei soli rapporti con la clientela, ma consente "ulteriori elaborazioni", ad esempio: memorizzazione di dati personali, anche degli operatori, ed estrazioni di report, relativi all'attività telefonica in generale ad opera di diverse funzioni aziendali. Ciò consente di ricostruire, anche indirettamente, l'attività effettuata dagli operatori e rappresenta uno sistema idoneo a realizzare un controllo, anche solo potenziale e in via indiretta, dell'attività lavorativa

(cfr., Ispettorato nazionale del lavoro, circolare n. 4 del 26.7.2017, Indicazioni operative sull'istallazione e utilizzazione di strumenti di supporto all'attività operativa ordinaria dei Call Center.

Pertanto, oltre alla disciplina di protezione dei dati, deve essere *rispettata anche la disciplina lavoristica in materia di impiego di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori* (Statuto dei Lavoratori)".

Tanto, in considerazione del fatto che le accertate caratteristiche del sistema e il novero delle operazioni di trattamento da questo rese possibili non risultano in via esclusiva funzionali alla mera gestione del contatto con il cliente e, dunque, al mero svolgimento della prestazione lavorativa; pertanto, il sistema così configurato non può essere considerato "strumento utilizzato dal lavoratore per rendere la prestazione lavorativa", quanto piuttosto rientra tra quegli strumenti organizzativi, dai quali può indirettamente derivare il controllo a distanza dell´attività dei lavoratori, con conseguente necessità di attivare le procedure ivi previste (art. 4, L.300/70).

Rispetto quindi alle condizioni di liceità di cui al predetto articolo 4, se da un lato le finalità che la società intende perseguire nel caso concreto risultano riconducibili alle "esigenze organizzative e produttive […]", dall'altro non risultano essere state attivate le garanzie procedurali prescritte dalla legge e la società ha dichiarato di non aver stipulato

specifico accordo sindacale in relazione all'applicativo. Da ciò consegue l'illiceità del trattamento in esame.

Il Garante riconferma quindi la regola che, in queste situazioni, deve essere seguita la procedura indicata dall'art.4 dello Statuto dei lavoratori.

Accordo sindacale su assistenza in cuffia e monitoraggio della sala operativa (14 maggio 2021)

In questo caso parliamo di un call center interno all'attività dell'azienda, in cui il tema centrale è quello, certamente delicato, di un controllo in tempo reale della sala operativa. In più l'azienda chiede ai propri dipendenti l'accettazione di un affiancamento in cuffia, giustificato come un supporto tecnico per i lavoratori al fine di migliorarne la loro efficienza.

Le esigenze aziendali sono state così individuate:

1) necessità di abbattere i tempi di durata delle telefonate per operatore per evitare rischi di insoddisfazione della clientela;
2) necessità di intensificare il processo di formazione ed addestramento del personale, con specifiche azioni di affiancamento svolte dai responsabili o dal personale più esperto su determinati prodotti o applicativi;

3) necessità di ottenere, essendo stata introdotta la modalità di lavoro agile in forma strutturale, una maggiore interazione tecnologica per ridurre i possibili problemi derivanti dalla lontananza fisica;
4) necessità quindi di utilizzare strumenti tecnologici che possono determinare anche un preterintenzionale controllo a distanza dell'attività dei lavoratori, pur avendo come finalità la formazione degli stessi e la migliore organizzazione del lavoro.

Tutto questo viene realizzato con l'"implementazione del sistema Reitek" con nuove funzionalità, che consentiranno ai responsabili e coordinatori di:

a) svolgere l'affiancamento in cuffia degli operatori;
b) effettuare il monitoraggio della sala.

L'affiancamento in cuffia consentirà di:

- supportare tecnicamente gli operatori nello svolgimento della loro attività;
- analizzare i fabbisogni formativi individuali di ogni singolo operatore nello svolgimento della propria attività ed in funzione delle necessità rilevate;

Il monitoraggio della sala, ovvero la visualizzazione in tempo reale da parte dei responsabili operativi del cosiddetto "cruscotto operatori", consentirà di rilevare lo stato degli

operatori collegati, impegnati in altre attività o in pausa e senza identificazione nominativa.

Le garanzie per i lavoratori sono state altrettanto importanti.
Innanzitutto viene escluso qualsiasi utilizzo del sistema mirato ad un singolo lavoratore, in modo da non costituire una "forma illecita di controllo a distanza sulla sua attività".
Conseguentemente l'azienda si impegna a non utilizzare i dati raccolti con il nuovo sistema ai fini disciplinari.

In secondo luogo il controllo della sala non può sfociare in un "comando a bacchetta", per cui un responsabile aziendale possa ordinare, ad esempio, "tutti ai telefoni" senza tener conto delle legittime esigenze dei lavoratori.
Questo è il motivo per cui la gestione del "cruscotto" deve essere molto articolata. l'azienda, quindi, seguirà i seguenti criteri operativi:

Monitoraggio della sala:
il monitoraggio avverrà in tempo reale senza memorizzazione dei dati nominativi. In caso di richiamo urgente ai telefoni non ci sarà la sola indicazione manichea "ha risposto/non ha risposto", ma la sala sarà monitorata con le seguenti tipologie di status per gli operatori ai quali viene associato ogni volta un codice generato casualmente dal sistema:
1. Operatore disponibile a ricevere o gestire telefonate/chat/ticket;

2. Operatore non disponibile a ricevere o gestire telefonate/chat/ticket).

Gli operatori non disponibili saranno ulteriormente distinti in due tipologie:
a) operatori in pausa (*e quindi non richiamabili ai telefoni*)
b) operatori occupati in attività di back office *(altrettanto non richiamabili ai telefoni*) in caso di attività di gestione delle pratiche off line o consultazione con colleghi.

Passando al secondo tema, è stato messo in chiaro che l'obiettivo dell'affiancamento è quello formativo e non di un controllo dell'attività del lavoratore.

Affiancamento in cuffia senza registrazione:
l'attività di affiancamento coinvolgerà in maniera equa tutti i lavoratori e sarà finalizzata all'obiettivo formativo specifico.
Il lavoratore dovrà essere preavvisato. In caso di condivisione dello schermo il lavoratore potrà utilizzare uno sfondo "istituzionale" messo a disposizione, che impedisca la visualizzazione di spazi e persone diverse dall'operatore.
Dalla prima telefonata di affiancamento il periodo di formazione potrà durare fino a due settimane di effettivo lavoro. Al termine di questo periodo azienda e lavoratore valuteranno l'esito del percorso che, eventualmente, potrà essere reiterato una sola volta per la durata dell'accordo.

L’azienda renderà disponibile agli operatori tale affiancamento in cuffia anche in caso di richiesta che parta da loro stessi. Al termine il responsabile operativo darà al lavoratore un “ritorno” rispetto al suo operato.

Uno dei fattori da mettere in evidenza è la poca leggibilità rilevata dai lavoratori dei pop up, che avvisano dell’affiancamento, quindi quest’ultimo potrà avvenire solo dopo un esplicito consenso da parte dei lavoratori stessi.

Comunque l’intero sistema è sotto osservazione e sperimentazione.

Capitolo 3
Una normativa europea in continua evoluzione affida nuovi importanti compiti alle parti sociali

Come abbiamo visto nella parte normativa, la Comunità Europea sta assumendo un ruolo sempre più centrale su questioni come quelle relative alla trasparenza e alla tutela dei lavoratori dall'inizio alla fine del rapporto di lavoro.

Una Direttiva europea su trasparenza e prevedibilità nei rapporti di lavoro)

A questi criteri si ispira la "Direttiva (UE) 2019/1152 del Parlamento Europeo e del Consiglio".

Il decreto legislativo di attuazione della Direttiva in Italia

L'attuazione della Direttiva in Italia è avvenuta solo poco tempo fa con il varo del decreto legislativo 27 giugno 2022, n. 104, entrato in vigore il 13 agosto 2022. Ci sono voluti, cioè, ben tre anni prima che si emanasse un provvedimento di attuazione.

Questo evidentemente è stato dovuto non solo a motivi tecnici e alla complessità delle norme, ma soprattutto al serrato confronto tra le diverse parti sociali interessate alla nuova normativa.

Molta parte della legge delega è dedicata agli obblighi di informazione del datore di lavoro: sulle tipologie di contratto di lavoro utilizzate, sull'importo iniziale della retribuzione, sulla programmazione dell'orario normale di lavoro e sulle eventuali condizioni relative al lavoro straordinario, sulla durata del congedo per ferie e degli altri congedi retribuiti, sul preavviso di fine rapporto di lavoro ecc.

Una preoccupazione costante, espressa nella Direttiva, è data dal fatto che, nel rapporto datore/lavoratore, è quest'ultimo che rappresenta la parte più debole.
Per questo motivo, ai commi 42/43, si dichiara esplicitamente la necessità di **"…un'adeguata protezione giudiziaria e amministrativa contro un trattamento sfavorevole in risposta a un tentativo di esercitare i diritti sanciti dalla presente direttiva, a un reclamo verso il datore o a un procedimento giudiziario o amministrativo inteso a garantire il rispetto della presente direttiva.**
(43) I lavoratori che esercitano i diritti previsti dalla presente direttiva dovrebbero essere protetti contro il licenziamento o pregiudizio equivalente, come un lavoratore a chiamata che non riceva più lavoro, o contro la preparazione di un

eventuale licenziamento per il fatto di aver cercato di esercitare tali diritti".

Esamineremo ora, sinteticamente, gli ulteriori obblighi previsti per il datore di lavoro nel caso in cui vengano utilizzati *sistemi decisionali o di monitoraggio automatizzati* gestiti da algoritmi ecc.

L'art.4 del decreto legislativo: gli ulteriori obblighi di informazione, ma non solo

Operando con il solito bizantinismo giuridico, con l'art. 4 del decreto, viene creata una costola all'art.1 del d.lgs 152 del 1997, sottotitolata "*Ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati".*

Più precisamente di quali obblighi stiamo parlando?
E' il primo comma dell'articolo ad esplicitarlo: "***Il datore di lavoro o il committente pubblico e privato è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali***

dei lavoratori. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300".

<u>Un diritto di informazione rafforzato</u>

È quanto possiamo evincere dal comma citato e dal successivo.

In primo luogo si ribadisce il diritto soggettivo del lavoratore ad una informazione accurata e precisa su tutto quello che concerne il suo rapporto di lavoro.

Ma in questo caso, nel caso cioè che si utilizzino sistemi decisionali automatizzati, si aggiungono ulteriori obblighi per il datore di lavoro. Tutto questo è ulteriormente specificato e ben articolato nel comma 2 dell'art. 4, che impegna il datore di lavoro a fornire le seguenti informazioni su:

- **A.** ***gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi di cui al comma 1;***
- **B.** ***gli scopi e le finalità dei sistemi di cui al comma 1;***
- **C.** ***la logica ed il funzionamento dei sistemi di cui al comma 1;***
- **D.** ***le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi di cui al comma 1, inclusi i meccanismi di valutazione delle prestazioni;***
- **E.** ***le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità;***

F. ***il livello di accuratezza, robustezza e cybersicurezza dei sistemi di cui al comma 1 e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.***

In buona sostanza il datore di lavoro non si può nascondere dietro gli algoritmi**,** ma deve mettere in chiaro e dare una esatta informazione sui criteri a cui si ispirano i sistemi automatizzati.

Viceversa tutto questo significa che il lavoratore ha il diritto di rendersi parte attiva per richiedere queste informazioni alla parte datoriale.

Si badi bene che, ove quest'ultima non dia riscontro e non risponda alle richieste, il lavoratore può ricorrere all'Ispettorato del lavoro, che a sua volta può comminare sanzioni pecuniarie e diffide.

<u>Il ruolo delle organizzazioni sindacali</u>

Il legislatore si è anche preoccupato del fatto che il lavoratore, lasciato solo, possa essere in difficoltà a far valere i propri diritti.

Allora, oltre ai diritti di informazione che può esercitare il singolo lavoratore, vengono prese in considerazione anche interventi collettivi, che fanno capo alle organizzazioni sindacali.

Lo vediamo nei commi 3 e 6 dell'art.4 del decreto legislativo, di cui stiamo parlando.

In particolare il comma 3 parla della possibilità che il lavoratore, che voglia esercitare i suoi diritti soggettivi di informazione, lo possa fare tramite delega alle "**rappresentanze sindacali aziendali o territoriali"**.

Il comma 6 fa un passo più avanti in quanto prevede che la comunicazione "**delle medesime informazioni e dati deve essere effettuata anche alle rappresentanze sindacali aziendali ovvero alla rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale*".***

Un obbligo quindi di doppia comunicazione, giustificato dall'importanza che viene data all'introduzione di sempre più potenti e raffinate tecnologie nella gestione dei rapporti di lavoro.

CONSIDERAZIONI FINALI

Non a caso abbiamo chiuso il Capitolo precedente con il recentissimo decreto legislativo di attuazione della Direttiva Europea sulla trasparenza e prevedibilità nei rapporti di lavoro. È un sintomo di una preoccupazione crescente, anche a livello istituzionale, per l'utilizzo di strumenti tecnologici sempre più stupefacenti.

Fino a pochi anni fa nessuno avrebbe pensato che si potessero avere a disposizione videocamere altamente evolute e in grado -mediante opportuni programmi- di ottenere una sequenza rapidissima di immagini e di renderle anonime in "near real-time" e, cioè entro il massimo di 500 millisecondi!

Ovviamente questo è solo un piccolo esempio per indicare quanto "corra" la tecnologia. Rispetto a questo andamento le norme che devono garantire i diritti delle persone e, quindi, anche dei lavoratori, sembrano essere in continuo affanno.
Ma non è sempre così.

Negli ultimi anni abbiamo molto discusso dell'Unione Europea e del suo ruolo, a volte problematico, nell'affrontare questioni critiche ed importanti per tutte le persone e gli Stati dell'Unione: basti ricordare la crisi Covid, la gestione dei problemi dell'emigrazione e dell'economia, il Pnrr ecc.

Ma non è, però, possibile ignorare l'impulso che spesso viene dato ai paesi membri da iniziative elaborate a livello europeo, in particolare su questioni inerenti i diritti personali e collettivi.

Tutta la materia relativa alla protezione dei dati personali va annoverata, secondo noi, tra quelle più degne di nota e che hanno prodotto norme di secondo livello (il livello statuale) altamente efficaci.

Dato questo riconoscimento all'Unione Europea e venendo all'Italia, abbiamo potuto vedere come il nostro legislatore sia riuscito ad integrare le disposizioni europee con le nostre normative, tra cui spiccano, ad oltre 50 anni dalla loro entrata in vigore, quelle dello Statuto dei lavoratori.

Ne è scaturito un "combinato disposto" che ha dato al suo complesso una maggiore forza ed efficacia.

Possiamo essere, quindi, totalmente soddisfatti della situazione? Sicuramente no: c'è ancora molto lavoro da fare, soprattutto in termini di conoscenza, sia da parte imprenditoriale che da parte dei lavoratori e delle loro rappresentanze.

Certo ci sono terreni ampiamente esplorati e acquisiti da tempo; oggi tutti, ad esempio, conoscono le procedure da seguire e le norme da rispettare in caso di installazione di videocamere. Non a caso gli accordi sono molti e in continua crescita, siamo in definitiva in una "società videosorvegliata".

Su altri temi non c'è invece una giusta consapevolezza. Basti pensare alla implementazione di sistemi informatici di controllo delle comunicazioni aziendali: non sempre si seguono le procedure che abbiamo indicato nel capitolo specifico.

Questo non va bene. Si deve partire, invece, da un presupposto: l'inserimento delle nuove tecnologie informatiche sui posti di lavoro non è materia da lasciare esclusivamente in mano agli specialisti. Le novità, per funzionare, devono essere conosciute e fatte proprie da tutti quelli che le utilizzano: imprenditori e lavoratori. Solo così si possono limitare gli aspetti negativi, presenti in ogni innovazione.

In definitiva è necessario utilizzare tutti i sostegni, offerti oggi dal legislatore italiano ed europeo, sicuramente in grado di alimentare quello spirito partecipativo, che è assolutamente necessario per gestire i veloci e continui aggiornamenti dei processi produttivi.