Questioni interpretative

Controlli a distanza: la disciplina prima e dopo la riforma

Luca D'Andrea e Engles Moriconi

Le recenti e costanti innovazioni tecnologiche hanno portato con sé innumerevoli vantaggi e possibilità nel contesto lavorativo; vantaggi declinabili sia per il lavoratore, sia per la controparte datoriale. In realtà molte e molto incidenti sono state anche le problematiche indotte da certe tipologie di apparecchiature e sistemi informatici. Si fa riferimento in concreto a strumenti quali computer, cellulari, smartphone, badge, tecnologie biometriche, Rfid, Nfc, tecnologie satellitari, Gps, droni e molto altro ancora.

Tra le tante questioni, una di quelle che maggiormente risente del continuo progresso tecnologico è sicuramente quella attinente al tema dei controlli "a distanza" attivabili attraverso impianti audiovisivi e di monitoraggio informatico, vietati dall'art. 4 dello Statuto dei lavoratori nella previgente formulazione, e ammessi, a certe condizioni dalla stessa norma recentemente riscritta ad opera dell'art. 23 del D.Lgs. 14 settembre 2015, n. 151, nell'alveo del più complesso progetto di riforma del Jobs Act.

Scopo principale di questo approfondimento vuole essere quello di ricostruire la fattispecie normativa in questione prima e dopo la predetta modifica, cercando di individuare, col suffragio giurisprudenziale, una serie di possibilità concrete che il datore può legittimamente predisporre verso i suoi dipendenti.

Ciò perché la summenzionata possibilità ha dato luogo ad un contenzioso vastissimo in ragione dei confliggenti interessi che si scontrano in una fattispecie di tal fatta: da una parte infatti l'interesse dell'imprenditore alla libera iniziativa economica, con tutto quello che ne consegue in tema di interesse all'esatto adempimento della prestazione e alla salvaguardia del patrimonio aziendale, dall'altra l'interesse del lavoratore al rispetto

della riservatezza e della dignità anche sul posto di lavoro, il tutto inequivocabilmente sancito ai commi 1 e 2 dell'art. 41 della Carta costituzionale.

Proprio questo incontro-scontro tra potere del datore e diritti del lavoratore individua il metodo di soluzione dei contenziosi a riguardo, configurando, mediante la tecnica del bilanciamento degli interessi in gioco, caso per caso, un ruolo risolutivo e creativo da parte della giurisprudenza.

Il precedente impianto normativo

In questa prima fase è indispensabile perciò ricostruire l'impianto normativo del vecchio articolo in esame, ergendolo poi a base portante per qualsiasi riflessione casistica fino al 2015.

Quest'ultimo, cioè l'art. 4, legge n. 300/1970 nella stesura originaria, in linea di principio imponeva un vero e proprio **divieto assoluto** di usare gli strumenti per il controllo a distanza.

«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.* (Omissis).

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma,

Jobs Act

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».

Come si vede, a fronte del divieto assoluto posto al primo comma, al secondo, la norma flexibilizza questa disposizione attraverso una forma di codeterminazione preventiva tra datore e rappresentanze sindacali (ovvero, in mancanza, attraverso l'autorizzazione amministrativa dell'Ispettorato del lavoro) al ricorrere, nel caso di specie, di esigenze organizzative e produttive, ovvero di sicurezza del lavoro. In mancanza della procedura autorizzativa, anche di natura sindacale (eventualmente con l'intervento della commissione interna, qualora le rappresentanze aziendali dovessero mancare) o amministrativa, i dati e le prove raccolte per il tramite di tali apparecchi saranno inutilizzabili sia a fini civili, anche disciplinari, sia a fini penali, posta l'illegittimità della sorveglianza, come affermato pacificamente dalla dottrina e dalla giurisprudenza civile.

Va aggiunto, da un punto di vista di introduzione sistematica, che la disciplina dei controlli a distanza e della vigilanza dei lavoratori, si arricchisce delle norme di cui all'art. 3 (previsione, modalità e limiti della funzione di vigilanza personale all'interno dell'ambiente di lavoro) e dell'art. 8 (divieto di indagini sulle opinioni personali del lavoratore e su ciò che non rileva ai fini della sua attitudine professionale) dello Statuto lavoratori, nonché, in uno spettro più ampio, del *corpus* normativo del Codice della privacy (D.Lgs. 30 giugno 2003, n. 196) che, nel Titolo VIII e cioè nella parte settoriale riservata al lavoro e alla previdenza sociale, recepisce e richiama formalmente gli articoli 4 e 8 dello Statuto, la cui violazione viene significativamente sanzionata penalmente dall'art. 171 dello stesso Codice privacy, sempre per recepimento delle pene stabilite dall'art. 38 dello Statuto dei lavoratori.

Tale discutibile tecnica legislativa del "doppio richiamo" è comunque chiaro segno della netta interdipendenza ed osmosi tra la disciplina lavoro-

stica e quella della tutela della riservatezza con riguardo ai controlli a distanza e dell'attribuzione delle competenze di controllo, vigilanza e sanzionatorie anche all'apparato amministrativo e "giudiziario" istituito e disciplinato dal Codice privacy (Autorità garante, Nucleo speciale privacy della Guardia di Finanza, ecc., ...).

Entrando ora nel merito della problematica, le questioni interpretative si originano proprio dai presupposti del divieto, già di per sé poco concreti.

Come ci suggerisce la giurisprudenza (1) primo presupposto logico-ontologico ai fini dell'operatività del divieto in esame, consiste nella c.d. pertinenza diretta o indiretta con "l'attività dei lavoratori".

L'appena richiamata espressione ingloba non solo le mansioni deducibili dal rapporto di lavoro, bensì l'intero comportamento sul luogo dello stesso, dilatando così tempi e luoghi del divieto in capo al datore (pause pranzo, sale relax potrebbero talvolta esservi ricompresi).

A questo proposito, a titolo esemplificativo, il Tribunale di Torino con sentenza del 9 gennaio 2004 (in *Giur. piem.*, 2004, 131), ha statuito che il controllo automatico delle telefonate da terminale aziendale con annessa registrazione del numero e della durata non esclude la predetta pertinenza, pertanto in concreto è consentito, in quanto il controllo stesso non attinge all'«attività lavorativa» tutelata dal divieto di cui all'art. 4, ma alla condotta illecita del lavoratore, che esula dall'applicazione di detta norma, e che è configurabile nel caso di telefonata ingiustificata da parte del lavoratore (si è trattato di un caso di "controllo difensivo" di cui si tratterà più avanti).

E ancora, ulteriore presupposto poco chiaro è riscontrabile nell'oggetto legato alla vasta accezione di apparecchiatura nel campo tecnologico (apparecchiatura di qualsiasi tipo). Anche in questo caso si intravedono, nella dimensione pratica, una serie di difficoltà applicative della norma; solo per fare un esempio sono inquadrabili come apparecchiature sia le tecnologie hardware, componenti fisicamente individuate o comunque individuabili, sia quelle software, le quali al contrario non si estrinsecano in un supporto fisico,

(1) Cass. civ., sez. lav., 3 aprile 2002, n. 4746; Cass. civ., 3 marzo 2002; Trib. Milano, 5 luglio 2006; Cass. pen., sez. III, 15 dicembre 2006, n. 8042.

bensi rappresentano programmi di controllo e monitoraggio di natura informatica (Blues, Super Scout, Ubidesktop, Gary T Marx solo per fare alcuni tra centinaia di esempi).

A questo riguardo, come è facilmente riscontrabile dall'esame della generalità dei contenziosi, anche in relazione alle linee guida tracciate nel 2007 (2) dall'Autorità garante dei dati personali, anche i software rientrano nella nozione di «apparecchiature» disciplinate dall'art. 4.

D'altro canto la fraintendibile accezione, almeno inizialmente, aveva creato una certa difficoltà interpretativa, ora, come visto, risolta.

Muovendo adesso alla **ragione del divieto prescritto**, questa è chiara: il presupposto della norma, che si inserisce nel solco tracciato dal legislatore e ripreso dalla giurisprudenza e dalla dottrina (3), 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 (così Cass. n. 8250/00 cit.).

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

La stessa *ratio* è affermata nell'interessante documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro adottato dal Gruppo dei garanti europei il 29 maggio 2002 (WP 55) «... se è vero che le nuove tecnologie costituiscono un'evoluzione positiva per quanto riguarda le risorse a disposizione dei datori di lavoro, gli strumenti di vigilanza elettronica si prestano ad essere utilizzati in modi che ledono i diritti e le libertà fondamentali dei dipendenti. Non va dimenticato che con l'arrivo delle tecnologie dell'informazione è di vitale importanza che i lavoratori godano tutti degli stessi

diritti, indipendentemente dal fatto che lavorino in linea oppure no. ... *La dignità umana del lavoratore va anteposta a qualsiasi altra considerazione*. Nell'esaminare questo problema è importante non dimenticare di questo fatto e degli *effetti negativi che le attività di vigilanza possono produrre sulla qualità della relazione professionale tra i dipendenti e il datore di lavoro nonché del lavoro stesso*».

Ancora una volta l'attività della giurisprudenza (4) traccia nuove formule e meccanismi interpretativi, atti a dirimere controversie in tema di illegittimi licenziamenti e illegittimi esercizi del potere disciplinare in genere sulla base dei dati raccolti tramite detti controlli: i magistrati parlano di «*modalità non eccessivamente invasive*», ad esempio *in relazione alla continuità temporale del monitoraggio, alla personalità dello stesso, alludendo ad un giudizio di proporzione e ragionevolezza tra i contrapposti interessi in gioco*, da applicarsi caso per caso riferendosi alle circostanze di fatto e di diritto che si manifestano.

Nella sostanza quindi, sembra potersi dire che i limiti che vengono posti al divieto di cui al primo comma, trovano giustificazione ed esplicitazione nella previa codeterminazione sindacale, dal momento che consente l'ingresso nella fattispecie di ulteriori ed antitetici interessi in gioco: quelli di natura produttiva e organizzativa ovvero di sicurezza del lavoro. Tale flessibilizzazione può avere luogo solo perché legittimata in concreto e in via preventiva da organismi che si fanno promotori proprio di quegli altri interessi che, come visto, fondano il divieto d'uso di determinati impianti.

In realtà la massiccia casistica contenziosa, pone degli interrogativi e delle questioni ulteriori, le quali, a determinate condizioni, legittimano il ricorso alle apparecchiature in esame, indipendentemente dal previo accordo, sia esso sindacale, sia esso amministrativo: si faccia riferimento a quello che, a detta di molti, è il più grande dilemma in tema di controlli "a distanza", cioè quello dei c.d. "**controlli difensivi**" prima accennati.

(2) Garante privacy, Del. n. 13 del 1° marzo 2007 in G.U. n. 58 del 10 marzo 2007.

(3) Relazione ministeriale all'art. 4, legge n. 300/1970; Cass. 17 giugno 2000, n. 8250; Cass. 17 luglio 2007, n. 15892; Cass. 23 febbraio 2012, n. 2722; in dottrina, C. Zoli, *Il controllo a di-*

stanza del datore di lavoro: l'art. 4, Stat. Lav. tra attualità e esigenze di riforma, in Riv. it. dir. lav., 2009, I, 485 ss.; A. Minervini, *I controlli sul lavoratore e la tutela dell'azienda in Il lavoro nella giurisprudenza*, n. 4/2014, pag. 314.

(4) Per es. Cass. civ., sez. lav., 27 maggio 2015, n. 10955.

Jobs Act

Come avremo modo di constatare, trattasi di una deroga, introdotta per via giurisprudenziale, alla logica di divieto appena esposta, e alla logica della codeterminazione pattizia delle esigenze che avrebbero reso flessibile tale divieto, laddove risorgano ulteriori e diverse esigenze nella fattispecie concreta, atte a legittimare i controlli a distanza e le loro risultanze anche, senza il rispetto della procedura tassativamente individuata al secondo comma del vecchio art. 4.

Tale categoria, così definita poiché tesa a verificare eventuali condotte illecite del lavoratore, si manifesta nella prassi attraverso sistemi di controllo per aree riservate o mediante apparecchi di rilevazione telefonate, financo attraverso sistemi di tracciamento Gps. Questi monitoraggi, così come chiarito a più riprese dalla giurisprudenza (5), esulano dall'ambito di operatività ex art. 4, Stat. lav. se non diretti all'esclusivo accertamento dell'esatto adempimento della prestazione lavorativa (può esserlo solo "sussidiariamente"), bensì mirino a preservare il patrimonio aziendale.

Il principio di tendenziale ammissibilità di tali controlli così recita: «il datore di lavoro può legittimamente esercitare i c.d. **controlli difensivi**, ossia quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti non riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto, bensì la tutela di beni estranei al rapporto stesso (6)». Tale statuizione è comunque da integrarsi, si ritiene, con i predetti principi di non eccessiva invasività, non continuità e anelasticità, oltre all'implementazione portata da un altro presupposto fattuale: *il dipendente così controllato deve aver già commesso o quantomeno deve sussistere un fondato sospetto di compimento di una data condotta illecita, la quale mini appunto il patrimonio aziendale; a questo proposito non basterà che tali illeciti siano meramente "supposti o ipotizzati", bensì occorrerà un indizio di una certa rilevanza (7).*

La questione si sposta quindi, oltre che sul controllo in sé, anche sull'utilizzabilità, per qualsiasi fine, dei dati così raccolti.

In particolare, ai fini della classificazione o meno del controllo come difensivo, la valutazione non potrà che essere *ex post*, relativamente alle circostanze che lo stesso accerta ed estrinseca; se con il medesimo dovesse venir accertata la condotta illecita, eccolo allora rientrare nella fattispecie in analisi, non operando di conseguenza l'art. 4; diversamente, nella circostanza per la quale il monitoraggio non dovesse dare alcun riscontro in tal senso, lo stesso sarebbe stato in sostanza posto in essere solo per verificare l'adempimento della prestazione di lavoro, decadendo a quel punto dalla sua posizione di deroga legittima e tornando ad operare il divieto ex art. 4, e quindi, così, la sua violazione.

In definitiva ci troviamo di fronte ad un ipotesi di *sanabilità ex post del mezzo*, qualora questo abbia dato esiti positivi relativi all'eventuale condotta illecita.

Ovvero, in alternativa, si ritiene che siano ammissibili anche 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. L'evidente finalità di deterrenza li direziona verso soggetti generici e a titolo di prevenzione appunto.

Diversi, quantomeno concettualmente, sono quei controlli difensivi che invece vengono posti in essere dal datore in presenza di *sospetti qualificati*, ossia gravi (importanza e serietà dell'indizio), precisi (verso soggetto/i determinati) e concordanti (implica una pluralità di indizi tutti gravi e precisi confluenti in un'unica direzione probatoria): c.d. **controlli difensivi successivi**. In questo caso la finalità è repressiva ed in quanto tale diretta contro soggetti determinati.

Anche questi casi sono svincolati dalla applicazione delle procedure di cui al vecchio articolo 4 secondo la univoca giurisprudenza.

Ora è bene riportare una ulteriore *species* dei controlli difensivi: quelli c.d. "**occulti**", così definiti poiché predisposti all'insaputa dei lavoratori, sia mediante l'installazione di determinate apparecchiature, sia anche ad opera di personale inter-

(5) Cass. civ., sez. lav., 27 maggio 2015, n. 10955; Cass. civ., sez. lav., 23 febbraio 2012, n. 2722 e Cass. civ., sez. lav., 1° ottobre 2012, n. 16622.

(6) Cass. civ., sez. lav., 23 febbraio 2012, n. 2722.

(7) Si veda la massima contenuta in App. Bologna 20 settembre 2012 (non pubblicata).

no o addirittura estraneo all'organizzazione aziendale (es. mediante ricorso ad agenzie investigative private).

Anche quest'ultima categoria viene ormai "tendenzialmente ammessa" sulla base delle stesse argomentazioni prima espresse che legittimano il *genus* "controllo difensivo"; in particolare la recentissima giurisprudenza di Cassazione n. 10955/2015, la quale si aggiunge ad un nutrito filone che corre lungo la stessa direzione (8), li ammette «in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa restando comunque necessario che le attività di accertamento si esplicino con modalità che contemperino l'interesse del datore al controllo e alla difesa dell'organizzazione con il *rispetto delle garanzie di libertà e dignità dei dipendenti*, ed in ogni caso rispettino i *canoni generali della correttezza e buona fede contrattuale*».

In un contesto di tal fatta è stata quindi ritenuta «legittima l'attività di controllo posta in essere dal responsabile del personale, autorizzato dai vertici aziendali, alla creazione di un falso profilo facebook di donna al fine di verificare la presenza su tale piattaforma del dipendente *durante l'orario di lavoro*, in quanto avente ad oggetto non l'attività lavorativa più propriamente detta ed il suo esatto adempimento, bensì l'eventuale perpetrazione di comportamenti *illeciti, già manifestati* (9) da parte del dipendente».

Nel caso in esame la creazione del falso profilo non viola di per sé né la buona fede né la correttezza nell'esecuzione del rapporto di lavoro, poiché «*non invasiva e nemmeno induttiva all'infrazione*»; afferendo a comportamenti illeciti già verificatisi (10) o al fondato sospetto circa il loro verificarsi (11), ed *essendo questi potenzialmente lesivi del patrimonio aziendale*, il controllo in esame conduce quindi all'esclusione dell'operatività dell'art. 4 con conseguente sua ammissibilità "occulto" o meno che esso sia.

Come d'altro canto ritenuto da autorevole dottrina, «... in realtà però deve considerarsi che è pur

sempre l'attività lavorativa, quale oggetto del controllo "a distanza", a segnare il discrimine tra controlli assoggettati alla disciplina posta dalla disciplina ivi in commento e controlli che invece ne fuoriescono. Se è l'attività lavorativa (ossia svolta nell'orario di lavoro) che, in quanto espletata in violazione di norma di legge o di contratto, si attegge a condotta illecita, trova comunque applicazione l'art. 4; se si tratta invece di un'attività illecita, ma che di per sé non sia significativa quanto alla valutazione della prestazione lavorativa svolta (nel senso di valutazione del suo diligente adempimento, n.d.a), allora tale articolo non trova applicazione (12)», con conseguente liceità del controllo a distanza, anche in difetto di contratto collettivo o autorizzazione amministrativa.

Tale impostazione è da ritenersi applicabile per tutte le specificazioni descritte di controllo "difensivo".

Quindi, come nel caso del profilo facebook, ciò che ha condotto la Cassazione a considerare lecito il controllo a distanza, per giunta occulto, e senza il preventivo accordo sindacale, è dato dalla circostanza che con esso si è giunti (*ex post*) ad accertare non solo e non tanto un inadempimento del lavoratore ai propri obblighi professionali, ovvero sia un semplice e mero illecito disciplinare, ma quanto, *un illecito disciplinare "qualificato" o "rafforzato nel senso che esso ha causato anche un danno al patrimonio aziendale*» (13), (la pressa bloccata da una lamiera incastrata in quanto lasciata incustodita), ovvero, come in altri casi affrontati, *un danno al patrimonio altrui o di terzi* (es. il denaro di colleghi custodito negli armadietti efratti e aperti dal lavoratore, nella vertenza decisa da Corte di Appello Roma 23 maggio 2015, in *La.Gi.* 2015, Fasc. 8/9, pag. 855), ovvero ancora un danno all'immagine aziendale o l'immagine altrui (come nel caso del capo-netturbino, sorpreso dal proprio Gps veicolare ad intrattenersi presso bar o locali di tavola calda ben oltre il limite contrattuale della pausa lavorativa, deciso dalla recentissima

(8) Cass. 9 giugno 1990, n. 5599; Cass. 2 marzo 2002, n. 3039; Cass. 10 luglio 2009, n. 16196.

(9) Utile richiamarsi alla precedente nota 7.

(10) Cass. 9 luglio 2008, n. 18821; Cass. 14 febbraio 2011, n. 3590; Cass. 2 marzo 2002, n. 3039.

(11) Cass. 14 febbraio 2011, n. 3590; Cass. 29 aprile 2001, n. 9576; Cass. 4 marzo 2014, n. 4984.

(12) G. Amoroso e al., *Diritto del lavoro. Lo Statuto dei lavoro*

ratori e la disciplina dei licenziamenti, vol. II, 2009, pag. 46.

(13) Di questo avviso anche Vittoria Amato, *Legittimità del controllo difensivo occulto attraverso i social networks in Lavoro e giurisprudenza*, n. 10/2015, pag. 900; nel commento alla sentenza della Cassazione 27 maggio 2015, n. 10955, si parla di "incidenza" degli illeciti posti in essere, facendo presumere sia la portata concreta lesiva degli stessi rispetto al patrimonio aziendale.

Jobs Act

Cass. 12 ottobre 2015, n. 20440, o come nel caso di messaggi di posta elettronica intercettati dal sistema di sorveglianza, con i quali il lavoratore bancario forniva a soggetti terzi informazioni riservate acquisite in ragione del servizio, avvantaggiandosene, mediante il compimento di operazioni finanziarie, così Cass. 23 febbraio 2012, n. 2722).

Quindi, nel concreto bilanciamento dei contrapposti interessi di cui sopra si è parlato, la tutela dell'interesse all'integrità del patrimonio e dell'immagine (aziendale o altrui) prevale sempre sull'interesse alla dignità e alla riservatezza del lavoratore, che quindi non sono incompressibili.

Nella realtà, alla luce di tutta la giurisprudenza (e la dottrina) esaminata, si può trarre un comune denominatore posto a fondamento della ritenuta liceità del controllo difensivo non concordato, affatto diverso dall'invocata tutela del patrimonio o dell'immagine aziendale o altrui, che sono, a ben vedere, utilizzati come emblemi meramente formali o appigli strumentalmente invocati.

La realtà riscontrata nei fatti è la seguente: se lo strumento di controllo difensivo, anche occulto, in concreto, accerta degli illeciti disciplinari gravi e sanzionabili con il licenziamento, ancor meglio se riprovevoli sotto il profilo del c.d. minimo etico richiedibile al lavoratore, lo strumento utilizzato viene considerato lecito e attingibile come prova.

Differentemente, se il fatto accertato dal controllo a distanza, non è così grave da costituire giusta causa di licenziamento, anche se attinto da (meno grave) illiceità, anche sotto il profilo della riprovazione morale, esso travolge il sistema di controllo e la sua validità/utilizzabilità.

A conferma di tale assunto, valga l'esame di Cass. 1° dicembre 2012, n. 16622, la quale ha dichiarato illecito il controllo di telefonate effettuato con il sistema Blues 2000 e l'inutilizzabilità dei relativi tabulati (con conseguente illegittimità del licenziamento) dai quali si è accertato che il lavoratore telefonista addetto ad un servizio di soccorso stradale e automobilistico, aveva in sostanza riattaccato il telefono in faccia all'utente per 460 volte in tre mesi di lavoro, e aveva intrattenuto n. 136 telefonate personali: è evidente che in questo caso, a parità di invasività e di oc-

cultezza del controllo, l'elemento differenziale è dato dal fatto che, tutto sommato, che un telefonista faccia qualche telefonata personale e non risponda alle richieste di soccorso per cui è pagato, evidentemente, tutto sommato non configura quell'illecito così moralmente disprezzabile, come quello del lavoratore che si attarda al bar o a chattare con una misteriosa dama, senza peraltro considerare e far menzione di come si possa essere gravemente appannata l'immagine aziendale (e di conseguenza prodotto il danno da mancata acquisizione dell'ordine di soccorso) nei confronti di quei 360 potenziali clienti che si sono visti riattaccare il telefono senza aver potuto neppure formulare la richiesta di soccorso.

Il tutto, come si è dimostrato, solo all'esito di una valutazione effettuata *ex post*.

Allora, in sintesi, per la liceità (con ragionevole grado di incontestabilità) del controllo "difensivo" non autorizzato, anche occulto, occorre che esso tenda a confermare gravi fatti illeciti, già emersi o denunciati, che configurino giusta causa di licenziamento in relazione alla violazione di norme che compongono il c.d. "minimo etico" che si pretende in un certo ambiente lavorativo, meglio se producenti un danno patrimoniale all'azienda.

Per una volta, nei limiti appena esposti, la linea sembra essere quella del *favor* al datore di lavoro, ribaltando la radicata tendenza opposta nella branca giuslavoristica.

Qui, come in altri casi esaminati e che si esamineranno, l'elasticità pro datore, si manifesta attraverso il varco della tutela dell'integrità patrimoniale-aziendale o dei lavoratori (14).

Allora, d'altro canto, con uno sforzo classificatorio, potrebbe ricondursi questa "apertura" nei confronti dei controlli "difensivi" ad ipotesi di "cause di esclusione" ovvero di "scriminanti" del reato (quale pur sempre è la violazione dell'art. 4), quali l'esercizio del diritto - la tutela della proprietà o dell'immagine aziendale - o la legittima difesa - dell'integrità patrimoniale o della sicurezza dei lavoratori - *ex art. 51 e 52, c.p.*

Proseguendo quindi nell'analisi delle pronunce giurisprudenziali che si sono occupate della materia, occorre riportare il ruolo assunto dalla sentenza della Cassazione n. 5599/1990, la quale,

(14) Dello stesso avviso la Cass. pen., sez. II, 16 gennaio 2015, n. 2890.

operando in ambito estraneo agli apparati audiovisivi o tecnologici, pur confermando il divieto di principio di cui all'art. 4, *legittima i controlli "occulti" anche se svoltisi "di notte" e "clandestinamente" purché siano svolti dal datore, o da un suo preposto, in quanto "ben noti" al lavoratore*, andando così a fortificare quell'orientamento che, ai fini dell'ammissibilità di un dato controllo datoriale, anche per il tramite di tecnologie e apparecchiature informatiche, presuppone un onere di garanzia a carico dell'imprenditore stesso che si esprime nella previa ed *adeguata informativa ai propri dipendenti circa le modalità e le tempistiche di monitoraggio "a distanza"*.

A fronte di tale possibilità concessa al datore di lavoro resta fermo in ogni caso il divieto di ricostruire l'attività e la prestazione del prestatore anche tramite apparecchiature *software* quali lettura e registrazione sistematica della messaggistica e-mail, riproduzione ed eventuale memorizzazione delle pagine web visitate ad esempio usando *cache dei proxy*, lettura e registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo, analisi occulta di pc portatili affidati in uso e molte altre ancora di cui mi occuperò più avanti; in tal senso ad intervenire è stato il Garante per la protezione dei dati personali nel

2007 attraverso la già citata Delibera n. 13 del 1° marzo 2007.

Certo, tale divieto si arresta di fronte ad un intervento di controllo sulla messaggistica elettronica del lavoratore, con il quale si accerti che lo stesso si serva di tale strumento per diffondere notizie riservate e svolgere operazioni con suo illecito profitto (v. Cass. n. 2722/12 cit.), a conferma della reale portata dell'indirizzo giurisprudenziale, sul quale si è detto sopra.

Il nuovo art. 4, Stat. lav. modificato dall'art. 23, D.Lgs. n. 151/2015

Occupandoci adesso del riscritto articolo in analisi ad opera dell'art. 23 del D.Lgs. n. 151/2015, nell'ambito di un disegno volto alla semplificazione delle disposizioni in materia di rapporto di lavoro, si menzionerà, al di là della formale novella, cosa cambia in sostanza a livello normativo, provando ad ipotizzare ed anticipare nuovi possibili scenari giurisprudenziali, tenendo presente che allo stato non si rinvencono pronunce giurisprudenziali che hanno statuito e applicato la norma in questione.

La norma, recata dall'art. 23, D.Lgs. n. 151/2015 che al primo comma dispone la sostituzione dell'art. 4 dello Statuto dei lavoratori, recita così:

Il nuovo art. 4, Stat. lav.

Art. 4 (*Impianti audiovisivi e altri strumenti di controllo*)

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 periodo precedente **possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa**, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, **del Ministero del lavoro e delle politiche sociali**.

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**.

L'articolo 23 del D.Lgs. n. 151/2015 al secondo comma, ha modificato anche la sanzione penale della violazione dell'art. 4, Stat. lav., contemplata dall'art. 171 del Codice privacy:

«Il comma. L'articolo 171 del Decreto legislativo 30 giugno 2003, n. 196, è sostituito dal seguente: Art. 171 (*Altre fattispecie*). - 1. La violazione delle disposizioni di cui all'articolo 113 e

all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300/1970».

La prima notazione che balza all'occhio è di carattere lessicale: la norma sostituisce infatti la nozione di «apparecchiatura» con quella di «strumento». Si potrebbe anche affermare che, a que-

Jobs Act

sto riguardo, nulla cambia, stante in ambo i casi la genericità del termine, in realtà, a nostro avviso, la scelta può giustificare una ancor maggiore apertura interpretativa, dal momento che *la nozione di strumento meglio si adatta, anche in futuro, con ogni possibile ed eventuale deriva tecnologica* (15). Non sembra essere un caso che le giurisprudenze più recenti ma non ancora formalmente applicative della novella (16), parlino di strumenti, con riferimento agli illeciti contestati dal datore, preferendo il nuovo termine poiché più vicino ai diversificati riscontri tecnologici concreti.

Seconda considerazione, ben più rilevante, consiste nell'eliminazione del divieto assoluto di utilizzo di strumenti di controllo a distanza, imposto dal vecchio primo comma dell'art. 4, rendendo *regola positiva*, non più eccezione, la legittima possibilità dello stesso in virtù di *esigenze organizzative e produttive, di sicurezza del lavoro ed ora anche espressamente di tutela del patrimonio aziendale*, andando a prendere spunto da un orientamento ormai fortemente consolidato e prima sviscerato, anche se tale inclusione sembrerebbe giungere, al netto di quanto osserveremo in seguito, a risultati opposti a quelli cui era pervenuta la giurisprudenza, esaminata.

Infatti, mentre con riferimento alla pregressa giurisprudenza (17), la formula *«tutela del patrimonio aziendale»* veniva sfruttata quale causa di deroga all'art. 4 (per i controlli "difensivi"), ciò implicando la non necessità di stipulare un previo accordo sindacale, ora, in relazione alla codificazione della medesima formula nel riscritto articolo, questa sembrerebbe imporsi quale presupposto di attivazione, ed eventualmente conclusione, della procedura di codeterminazione sindacale/amministrativa, salvo quanto appreso si osserverà.

Tale nuova formulazione rivela quindi una rinnovata *ratio*, contenente una disciplina positiva delle ipotesi e delle modalità in cui l'utilizzo di detti strumenti è lecito e non più un espresso divieto seppur flessibilizzato.

Non ci sentiamo peraltro di dedurre, da tale formulazione "in positivo", la scomparsa della compressione assoluta del potere di controllo sull'attività dei lavoratori, caposaldo del vecchio art. 4 a tutela della riservatezza e della dignità di ciascun dipendente, come sembra ritenere una certa dottrina: «affermare che una certa attività è vietata e disciplinare poi i casi in cui a tale divieto è consentito derogare non è lo stesso che limitarsi a disciplinare (regolandoli) i casi in cui tale attività è consentita. (*Omissis*). Non è una differenza di poco conto, quantomeno ove si voglia privilegiare una valutazione sistematica della materia» (18).

In realtà, poiché l'art. 4 contempla pur sempre un'ipotesi di reato, i principi di legalità, tassatività e precisione che condizionano sia il legislatore che l'interprete, non ci consentono di escludere che di divieto comunque si tratti, beninteso nei limiti in cui non operino le "scriminanti" codificate delle esigenze organizzative o produttive, della sicurezza del lavoro o della tutela dell'integrità del patrimonio aziendale.

Nel frattempo possiamo allora paventare l'ipotesi che tale resa "normativa" all'integrità patrimoniale possa aprire la strada verso un controllo a distanza come forma d'efficientamento aziendale, in quanto prosecuzione logico-ontologica del potere direttivo?

Certamente no, in primo luogo per la permanenza del divieto sul controllo della prestazione come sopra evidenziato, in secondo luogo perché anche i riscontri giurisprudenziali sono di segno fortemente contrario (19), e per esempio la Corte di cassazione del 17 luglio 2007, n. 15892 parla di *«insopprimibile esigenza di evitare condotte illecite, la quale non può giustificare un sostanziale annullamento di ogni forma di garanzia di dignità e riservatezza»* (ovviamente intesa nell'ambito dello svolgimento della prestazione lavorativa).

Pare evidente che l'attività legislativa sia stata guidata da quella creatrice della giurisprudenza, seppur approdando a soluzioni diverse, in un ter-

(15) Almeno ad oggi comunque è evidente lo scarso rilievo della questione.

(16) Cass. civ., sez. lav., 12 ottobre 2015, n. 20440.

(17) Cass. pen., sez. V, 18 marzo 2010, n. 20722; Cass. pen., sez. II, 16 gennaio 2015, n. 2890; Cass., 9 luglio 2008, n. 18821; Cass., 12 giugno 2002, n. 8388; Cass., 14 febbraio 2011, n. 3590; queste ultime tre fra l'altro espressamente cita-

te dalla recente Cass. civ., sez. lav., 27 maggio 2015, n. 10955.

(18) L.A. Cosattini, *Le modifiche all'art. 4, Stat. lav. sui controlli a distanza, tanto rumore; per nulla?* In *Il lavoro nella giurisprudenza*, n. 11/2015, pag. 986.

(19) Si veda l'abbondante giurisprudenza riportata in precedenza relativa alla pertinenza diretta-indiretta.

reno che, alla luce dell'imprevedibilità e repentinà del progresso di stampo tecnologico, abbisogna costantemente di ritocchi che necessariamente passino per il *test* del caso concreto.

Altra significativa novità consiste nella scissione del concetto di «*installazione*» dal concetto di «*impiego*», laddove invece il vecchio articolo di riferimento li poneva, quantomeno a livello interpretativo, sullo stesso piano.

La vecchia formulazione infatti al primo comma, ossia nel momento di configurazione del divieto come assoluto, parlava genericamente di divieto «*d'uso*», mentre al secondo, nel momento di potenziale flessibilizzazione dello stesso per le sole esigenze organizzative e produttive ovvero di sicurezza del lavoro, in un primo momento parlava di «*installazione*» con riferimento all'accordo di natura sindacale per poi parlare di «*modalità d'uso*» in relazione all'autorizzazione eventuale dell'Ispettorato del lavoro.

È evidente perciò che la preventiva procedura autorizzativa, in ambedue le sue possibili manifestazioni, dovesse avere per oggetto sia l'installazione sia l'impiego, non essendo logico prevedere che la fase utilizzativa (modalità di impiego) necessitasse di autorizzazione solo nel caso di intervento dell'Ispettorato del lavoro (ipotesi suppletiva) e non già nel caso di intervento del sindacato (ipotesi principale).

Tale argomento veniva avvalorato dalla considerazione che la fattispecie in questione, configurando pacificamente un reato c.d. di pericolo, si perfezionava già al momento stesso dell'installazione, quale fase astrattamente idonea a minacciare il bene protetto (dignità/riservatezza del lavoratore), mentre restava del tutto irrilevante la concreta lesione del bene per effetto del concreto impiego dello strumento.

Scelta radicalmente diversa invece riguarda il riscritto art. 4 dal momento che non solo la scissione tra «*impiego*» e «*installazione*» è espressa lessicalmente, ma è anche rimarcata disgiuntivamente a livello sintattico («... gli strumenti da cui derivi la ... possibilità di un controllo a distanza dell'attività dei lavoratori possono essere *impiegati esclusivamente per esigenze organizza-*

tive e produttive ... e possono essere *installati previo accordo* collettivo stipulato».

A questo punto, in assenza di riscontri giurisprudenziali, si prospettano due linee interpretative della norma, del tutto diverse, che sottoponiamo. Secondo la *prima impostazione*, si potrebbe affermare che la disposizione è chiara e precisa nel subordinare al previo accordo sindacale *la sola installazione*, laddove, viceversa, l'impiego non solo è espressamente distinto e legato all'esclusiva sussistenza di esigenze organizzative e produttive, di sicurezza del lavoro e anche di tutela del patrimonio aziendale, ma dal legislatore anche anteposto nella costruzione del periodo, nonostante la sua logica consequenzialità all'installazione (prima si installa e poi si impiega), facendo presumere così la non operatività dell'accordo con i sindacati previsto sintatticamente dalla coordinata, parafrasando così il broccardo latino *ubi lex distinguit, nos distinguere debemus*.

Questa linea interpretativa implica anche una riddiscussione del reato dedotto alla violazione della norma in questione, il quale se fino alla presente novella veniva classificato come reato di pericolo, e quindi già l'installazione consuma il reato, poiché già di per sé potenzialmente lesiva del bene giuridico di riservatezza implicante una tutela a priori (20), oggi, alla luce della summenzionata scissione lessicale, la violazione del momento d'installazione resta inquadrabile come *reato di pericolo*, mentre invece una eventuale violazione in concreto delle causali previste ai fini dell'impiego configurerebbe piuttosto un *reato di danno*, solo in concreto dannoso appunto, ridimensionando, in coerenza con la rinnovata *ratio* normativa, i rischi e le responsabilità in capo al datore di lavoro.

E ancora, sempre quanto alla struttura del reato, mentre nel caso dell'installazione, il preventivo accordo sindacale configurerebbe un presupposto di fatto del reato, nel caso dell'impiego, la sussistenza - che potrebbe darsi solo "in concreto" all'atto dell'utilizzo - delle condizioni legittimanti (esigenze organizzative/produttive, sicurezza del lavoro, tutela del patrimonio), rilevarebbe, anco-

(20) A. Minervini, *I controlli sul lavoratore e la tutela dell'azienda*, in *Il Lavoro nella giurisprudenza*, n. 4/2014, pag. 765. A questo riguardo si vedano poi Pret. Milano, 5 dicembre 1984,

in *Orient. giur. lav.*, 1986, pag. 20 e Cass. pen., sez. III, 6 ottobre 2010, n. 37171, in *Dir. prat. lav.*, 2010, 45, 2633.

Jobs Act

ra, ai fini della ricorrenza di quelle cause di esclusione del reato di cui si parlava prima.

Tale argomento è inoltre avvalorato dalla considerazione che, in ossequio ai principi di legalità e tassatività della norma incriminatrice e delle conseguenze che se ne determinano in ordine alla sua interpretazione, è arduo - stanti la chiara lettera e sintassi della norma, nonché la mutata intenzione del legislatore in senso più indulgente verso i controlli - ricomprendere la fase di impiego e la ricorrenza concreta delle condizioni scriminanti, nell'obbligo del preventivo accordo sindacale, senza incorrere nel divieto dell'analogia *in malam partem* in ambito penale, nel senso che in tal modo si configurerebbe il reato nel fatto di chi impiega lo strumento di controllo, pur ricorrendo le condizioni legittimanti, senza il previo accordo sindacale, in difetto di una norma che lo preveda espressamente come reato.

D'altro canto, l'accordo sindacale, ben difficilmente può disporre sull'impiego concreto di strumenti di controllo in funzione, ad esempio, protettiva del patrimonio, in tempi celeri e idonei a consentire di non frustrare la tutela stessa, in situazioni in cui l'immediatezza e la necessità dell'accertamento dell'illecito, alla cui prova è finalizzato il controllo, sono incompatibili con i tempi dello svolgimento di un'intesa sindacale.

Certo ci rendiamo conto che siffatta interpretazione della norma, sostanzialmente escluderebbe il sindacato da ogni possibile valutazione sulle finalità concrete dell'impiego dello strumento di controllo, essendo l'accordo richiesto per la mera "installazione" che sarebbe a questo punto "acausale", con conseguente sollevazione da parte delle Organizzazioni.

Allora è forse più corretto - ed è questa **la seconda linea interpretativa della norma** - ricondurre la distinzione nell'ambito di una interpretazione "estensiva" del termine «*impiegare*», che, inteso nell'ampio senso di "adoperare per una certa finalità", e quindi, enfaticamente e sottolineato il momento teleologico, può ricomprendere nel suo perimetro semantico anche la fase di installazione che comunque presuppone l'individuazione del fine per cui essa è realizzata, oltre che, ovvia-

mente, dell'operatività e del funzionamento concreti dello strumento.

A questo punto l'accordo sull'installazione presupporrebbe anche l'individuazione di massima del fine che la giustifica ed entra nel contenuto dell'accordo sindacale preventivo (*finalità astratta*: es. esigenze di sicurezza in relazione a casi di accessi non autorizzati, manomissioni di strumenti o prodotti, ecc. ...).

Poi, effettuata l'installazione, magari per una certa finalità su cui le parti si sono confrontate, la norma non impedisce che l'impiego, cioè l'utilizzo, dello strumento, con una determinata modalità, sia deciso e realizzato unilateralmente dal datore di lavoro, per una *specificata finalità "concreta"* anche ulteriore e accidentale (es. repressione di illeciti impattanti sul patrimonio aziendale), magari in forma "occulta", allorquando l'urgenza di assicurare elementi di accertamento dell'illecito, renda necessaria una messa in funzione "immediata" dello strumento, incompatibile con l'avvio della procedura di accordo sindacale di cui all'articolo 4, come sopra accennato.

Quanto appena esplicitato, letto in combinato disposto con l'approccio giurisprudenziale relativo ai controlli "difensivi" *ante* riforma, ci permette di chiarire in quali casi e entro quali modalità, alla luce della novella, siano o meno oggi legittimi i controlli difensivi "preterintenzionali" - cioè quelli che tendono a soddisfare esigenze magari inizialmente non codificate nell'accordo sindacale, che si presentano in corso d'opera, valutabili quindi dal solo datore di lavoro in vista del loro utilizzo, come ad esempio quelli che accertano illeciti pregiudizievoli su beni aziendali -, anche "occulti", nonostante la codificazione della tutela del patrimonio aziendale quale presupposto di accordo, al nuovo art. 4 (21).

Più specificamente i controlli difensivi e il relativo filone giurisprudenziale è possibile possa rimanere operativo per quanto riguarda il momento dell'«impiego» (finalità concreta) e quindi delle modalità concrete attinenti il monitoraggio, estendendo ora quella possibilità oltre la mera tutela del patrimonio aziendale anche alla sicurezza del lavoro e alle esigenze organizzative e produt-

(21) L.A. Cosattini, *Le modifiche all'art. 4, Stat. Lav. sui controlli a distanza, tanto rumore; per nulla? In Il Lavoro nella giurisprudenza*, n. 11/2015, pag. 988.

tive, posta oggi la loro equiparazione sul piano normativo.

D'altro canto invece per quanto riguarda l'installazione, il campo di applicazione dei suddetti controlli tesi all'accertamento dell'illecito sembra possa venir ristretto, in ragione dell'espressa e quindi inequivocabile previsione normativa.

In definitiva però non possiamo non ribadire nuovamente la rinnovata *ratio* sottesa alla norma, la quale, come visto, allenta (ma non esclude) la compressione del potere di controllo sull'attività dei lavoratori, fungendo da logica di interpretazione generale per ogni fattispecie a riguardo, anche per quelle dei controlli difensivi, così come per quelle afferenti ad esigenze organizzativo/produktive o di sicurezza del lavoro.

Concludendo in merito alla questione della necessità del preventivo accordo/autorizzazione, stanti i canoni ermeneutici della norma appena esaminati, è possibile affermare che l'accordo dovrà essere sicuramente concluso per disciplinare l'installazione di strumenti audiovisivi o altrimenti di controllo, prevedendo in primo luogo in esso, l'espressa esclusione che la finalità perseguita sia quella del controllo sull'adempimento della prestazione lavorativa, e che ricorra, in astratto, almeno una delle esigenze di cui al comma 1, dell'art. 4, inoltre, individuando e descrivendo le tipologie e le caratteristiche tecniche degli strumenti, la loro ubicazione all'interno dei locali, pure descritti e individuati nella loro fisica consistenza, contemplando inoltre l'impegno del datore di lavoro ad impiegarli solo nella ricorrenza concreta di quelle esigenze di cui abbiamo trattato, la cui valutazione nel caso concreto è, a questo punto, ad esclusivo appannaggio del datore di lavoro.

Certo, dato l'espresso richiamo ad opera del quarto comma del nuovo art. 4 alla normativa Privacy, il datore di lavoro, se è vero che relativamente all'impiego concreto può scavalcare le parti sindacali, dovrà quantomeno predisporre adeguata informativa ex art. 13 del D.Lgs. n. 196/2003 circa i controlli, già al momento dell'installazione degli impianti, riservandosi poi liberamente la possibilità di "impiegarli" al sorgere delle esigenze codificate di sicurezza del lavoro, produttive ed organizzative nonché di tutela del patrimonio aziendale.

Il secondo comma dell'art. 4

Sicuramente una "liberalizzazione" di sostanza c'è però con riferimento al secondo comma dell'art. 4, il quale dispone che il *divieto* di cui al primo comma «*non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*» (tra cui pc, smartphone e tablet) e agli «*strumenti di registrazione degli accessi e delle presenze*». Qui la novella pone una sostanziale novità, dal momento che per accessi si devono intendere non solo quelli fisici (tramite badge), ma anche telematico-informatici (accessi a siti internet, dati, informazioni, ecc.), per i quali ora non sarà più necessario il previo accordo sindacale (esempio classico è quello di telecamere installate nella, o nei pressi della, macchina che legge i badge all'ingresso di un ufficio, necessaria per evitare comportamenti abusivi), salvi i casi nei quali i meccanismi non originari dello strumento raccolgano informazioni ulteriori rispetto al mero accesso (trattasi comunque di miopia normativa dal momento che oggi la maggior parte degli strumenti informatici è già di per sé dotata di sistemi di geolocalizzazione Gps o di tracciamento in genere, motivo per il quale non abbisognano di alcuna modifica dell'impianto originario).

Tale interpretazione è quella ufficialmente fornita anche dal Ministero del lavoro e delle politiche sociali, il quale con nota del 18 giugno 2015 così chiarisce e allo stesso tempo mitiga la portata innovativa letterale a riguardo: «l'espressione «*per rendere la prestazione lavorativa*» comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione: ciò significa che, nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la conseguenza che queste "modifiche" possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione.

La portata di tale disposizione è infatti per certi aspetti ancora più estesa e impattante di quel che

Jobs Act

si possa pensare, poiché per «strumenti utilizzati per rendere la prestazione» non vi rientrano solo quelli di natura informatica (sostanzialmente quelli per cui si è optato per tale liberalizzazione), ma anche tutti gli strumenti fisici di lavoro quali presse autovetture, macchinari, ecc.

Questo si traduce oggi nella possibilità datoriale di sottoporli a controllo anche in assenza di un previo accordo sindacale, potendo quindi avvalersi di un sistema software in grado di tracciare i tempi di lavoro di determinati macchinari senza che ciò configuri monitoraggio della prestazione, in quanto tale di principio illegittimo, e per di più senza che a tal fine sia necessaria la previa codeterminazione.

In particolare si prospetta una diversificazione a seconda che i controlli riguardino gli impianti, ossia finalizzati alla vigilanza sulle prestazioni di lavoro, i quali resterebbero vietati, salvo il caso in cui, con un'autorizzazione sindacale o amministrativa, le telecamere servano per garantire per esempio la sicurezza, piuttosto che i controlli abbiano ad oggetto appunto gli «strumenti» aziendali, i quali pertanto sembrerebbero liberalizzati, posto il non più necessario accordo sindacale o la notifica alla DTL, con conseguente snellimento delle procedure a carico del datore (in questa seconda categoria rientrano anche smartphone, tablet, ecc.).

Il terzo comma dell'art. 4

Anche la precisazione di cui al nuovo terzo comma circa l'utilizzabilità dei dati raccolti segue in parte la giurisprudenza, condizionandola, nel senso di prevedere ora, oltre al generico richiamo alla normativa in materia di privacy (22), anche un vero e proprio obbligo informativo ai dipendenti (23) ai fini della fruizione per qualsiasi fine (24) dei dati conseguiti dal controllo, e non più meramente un onere. In dettaglio, per poter utilizzare per qualsiasi fine, anche disciplinare, i dati raccolti dai sistemi di controllo, il datore dovrà aver adempiuto l'obbligo informativo di cui all'art. 13 del D.Lgs. n. 196/2003, nonché quanto

disposto dall'Autorità Garante con riferimento alla protezione dei dati personali; profili questi su cui seguirà un successivo apposito approfondimento nel presente elaborato.

Qui basterà anticipare che sarà sufficiente in sostanza rendere noto al lavoratore le modalità di attuazione del controllo ai fini della sua legittimità e utilizzabilità, anche per finalità disciplinari, dei risultati da esso tratti, ciò attraverso la *consegna di un documento informativo* per la legittimazione e autorizzazione del controllo. Come sostenuto da molti e riportato dalla dottrina, trattasi di una deregolamentazione dei controlli a vantaggio dell'impresa (25)?

No poiché sulla base di quanto appena riportato il quadro normativo rafforza la posizione del lavoratore, adesso a conoscenza di quali controlli vengono svolti e con quali modalità.

A ben vedere, questo aspetto della disposizione accresce le garanzie per il lavoratore e, allo stesso tempo, tutela con certezza giuridica il comportamento a cui è tenuto il datore, così come precedentemente esplicito.

D'altro canto sicuramente depotenzia la «schermatura» del dato acquisito e quindi la «forza» probatoria del prestatore nella misura in cui oggi, diversamente da ieri, i dati così ottenuti potranno venir utilizzati pacificamente anche per finalità disciplinari, non più meramente civili e penali.

Altra implementazione normativa si riferisce alle imprese con unità produttive separate in diverse province, città, regioni, predisponendo la possibilità di siglare l'accordo (26) per l'installazione degli impianti direttamente con le organizzazioni sindacali nazionali; la disposizione colma un parziale vuoto che caratterizzava la precedente disciplina, favorendo la procedura di codeterminazione sindacale da parte di imprese con più sedi sul territorio italiano, direttamente con le organizzazioni sindacali nazionali. La norma è evidentemente tesa ad evitare la frammentazione di accordi differenti per ciascuna sede di riferimento di una singola azienda, nonché a consentire anche ai sindacati nazionali di esprimere il loro

(22) A proposito di integrazione della normativa *ex art. 4* su cui verterà successivamente un paragrafo *ad hoc*.

(23) Con mezzo «adeguato».

(24) Ora anche per finalità disciplinari.

(25) V. Amato, Legittimità del controllo difensivo occulto attraverso i social networks, in *Il Lavoro nella giurisprudenza*, n. 10/2015, pag. 903.

(26) Si chiarisca che, così come espressamente risposto all'Interpello n. 2975/2005 dal Ministero del lavoro e delle politiche sociali, è sufficiente che tale accordo sia raggiunto con la sola maggioranza delle Rsa, purché siano chiamate ad esprimersi le rappresentanze delle diverse unità produttive ove può essere attivato il controllo «a distanza».

parere, posta l'incidenza della questione, circa i sistemi di videosorveglianza e controllo a distanza installati da imprese con più sedi sul territorio italiano. È bene precisare che, qualora la violazione del riscritto art. 4 dovesse riguardare l'accordo con i sindacati e la relativa procedura autorizzativa, ciò esporrebbe il datore anche alle sanzioni previste per la repressione della condotta antisindacale *ex art. 28* dello Stat. lav., oltre alle previste sanzioni penali *ex art. 38*, Stat. lav.

E ancora, in caso di mancato accordo, la novella prevede la possibilità di conseguire l'installazione previa autorizzazione alternativa della Direzione territoriale del lavoro o del Ministero del lavoro e delle politiche sociali.

L'istanza dovrà essere presentata su iniziativa datoriale e dovrà far menzione dei contenuti tecnici e strumentali degli impianti di controllo a distanza, mentre d'altro canto l'eventuale autorizzazione, richiesta al momento dell'installazione, difficilmente potrà indicare particolari modalità d'uso in concreto degli stessi, essendo stata cancellata la previgente previsione in tal senso, e non essendo oggi previsto il potere dell'Ufficio amministrativo di valutare le esigenze organizzative/produttive ecc., necessarie per l'impiego (27).

Infine la nuova formulazione abroga la possibilità di intentare un contenzioso amministrativo riguardante la decisione assunta dalla Dtl da parte del datore o delle rappresentanze sindacali? Sicuramente la possibilità prima era prevista espressamente nel termine per impugnare di 30 giorni dalla comunicazione del provvedimento, direttamente al Ministro per il lavoro e la previdenza sociale, ma l'assenza esplicita di questa ipotesi non sembra poter escludere anche la normale impugnazione dell'atto al pari di qualsiasi altro atto amministrativo.

Inoltre il meccanismo integrativo vagliato con riferimento alla fattispecie pre-novella, si arricchisce della Raccomandazione del Garante privacy n. 5 del 1° aprile 2015 in tema di utilizzo dei dati personali negli ambiti lavorativi, la quale mira anche a tutelare il datore contro il progresso tec-

nologico. In questa prospettiva essa prevede delle "cautele aggiuntive" per l'imprenditore così riassumibili: l'obbligo di informare preventivamente i lavoratori prima di introdurre sistemi e tecnologie informatiche volte al monitoraggio della loro attività lavorativa, l'adozione di misure interne adeguate sul trattamento dei dati, anch'esse da comunicarsi previamente, la consultazione dei rappresentanti dei lavoratori prima di introdurre qualsiasi sistema di monitoraggio o di modifica di quelli esistenti ed infine l'obbligo di consultazione dei Garanti nazionali in materia di privacy. Allo stesso tempo la Raccomandazione prevede il divieto d'utilizzo di strumenti tecnologici all'esclusivo scopo di controllare attività e comportamenti dei dipendenti, oppure, qualora sia ritenuto necessario, il datore potrà anche installare sistemi di sorveglianza audio-video, purché mai posizionati in zone normalmente non adibite ad attività lavorative (es. spogliatoi, mense, sale relax, ecc.: ciò costituisce un limite rispetto al previgente regime, nel quale le telecamere negli spogliatoi sono state consentite per scoprire un furto di denaro dagli armadietti da Corte App. Roma 23 maggio 2015 cit. *supra*); prevede inoltre il divieto di monitorare le comunicazioni private (28) e molto altro.

Interferenze della fattispecie con la normativa del Codice privacy, con particolare riguardo alla videosorveglianza

Come si è potuto intuire, la fattispecie normativa dei controlli "a distanza", data la complessità e il rilievo degli interessi in gioco, presuppone interferenze e interpretazioni in combinato disposto con altre disposizioni.

Tra queste, specialmente in ragione dell'espresso richiamo - già esaminato - della novella al terzo comma dell'art. 4 relativamente all'utilizzabilità delle informazioni raccolte, spicca il massiccio *corpus* normativo privacy, costituito in primo luogo dal D.Lgs. n. 196/2003 (c.d. Codice privacy) e successive modifiche, e in seconda battuta da una vastissima produzione normativa dell'Au-

(27) *Contra* P. Rausei, *La nuova disciplina dei controlli a distanza fra luci e ombre*, in *Dir. prat. lav.*, n. 38/2015, pag. 2156, che però non sembra aver valorizzato il differente dettato normativo della novella sullo specifico punto.

(28) Il richiamo è all'art. 8, Cedu circa la «vita privata», inclusiva anche dell'attività lavorativa. Francamente questa ulti-

ma interpretazione mi sembra fin troppo garantista ed ingiustamente tale verso il lavoratore, quantomeno come statuizione di principio, posto che l'attività lavorativa si inserisce nel complesso aziendale ed in quanto tale è sicuramente vantaggioso, ma anche costo e responsabilità per l'imprenditore.

Jobs Act

torità Garante *ad hoc* (29), sia con riferimento ad innumerevoli linee guida su specifici ambiti del trattamento del dato personale, sia con riferimento ad interventi e provvedimenti riferibili a soluzioni di contestazioni concrete avviate dai lavoratori sulla base dell'**art. 17, comma 2** del Codice appena menzionato: «*Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica prelimi-*

nare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare».

La disposizione che più si lega operativamente con la fattispecie dei controlli "a distanza", poiché riferibile ai predetti sistematici oneri informativi preventivi del datore di lavoro, è sicuramente l'**art. 13** Codice privacy il quale così recita:

Art. 13 (Informativa) - Codice privacy

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
 - a) le finalità e le modalità del trattamento cui sono destinati i dati;
 - b) la natura obbligatoria o facoltativa del conferimento dei dati;
 - c) le conseguenze di un eventuale rifiuto di rispondere;
 - d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
 - e) i diritti di cui all'articolo 7;
 - f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.
2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.
3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.
4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
5. La disposizione di cui al comma 4 non si applica quando: a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.
- 5-bis. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di *curricula* spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f).

Così come compete tale specifica informativa al datore di lavoro, spetta parimenti a quest'ultimo, sulla base delle citate linee guida per posta elettronica ed internet (Del. 1° marzo 2007 cit.), probabilmente il settore più foriero di contrapposizioni tra le parti, soprattutto dopo l'avvento delle "tecnologie smart", assicurare le funzionalità e il corretto impiego di tali mezzi, definendone modalità d'uso nell'organizzazione dell'attività lavorativa, così come spetta sempre a lui adottare misure idonee di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi e

di dati, anche nella prospettiva di prevenirne un utilizzo indebito.

Tutto ciò poi è corroborato dall'elencazione di tre principi a cui i trattamenti sono assoggettati se vogliono essere ritenuti a norma, oltre alle prescrizioni di cui all'art. 4: principio di **necessità**, principio di **correttezza** e la subordinazione del controllo a **finalità determinate, esplicite e legittime**.

Tali menzionati principi implicano altrettanti oneri al datore, per cui secondo il primo di questi, i sistemi informatici devono ridurre al minimo la raccolta di dati e, a sua volta, tale raccolta

(29) Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati n. 53 del 23 novembre 2006; Linee guida del garante per posta elettronica e internet

n. 58 del 10 marzo 2007; Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 e molti altri ancora.

deve rispettare il **principio di pertinenza e non eccedenza** da valutarsi in concreto, oltre al generico **principio di proporzionalità**; a titolo esemplificativo si riporta il provvedimento dell' Autorità Garante del 4 ottobre 2011 in materia di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro, nel quale tali principi vengono applicati anche richiamando per esempio l'artt. 3 e 11, comma 1, lettera e) del Codice privacy, a testimonianza ancora una volta dell'intima sinergia tra art. 4 e normativa privacy.

Con riferimento all'utilizzo e-mail, occorrerebbe configurare l'impostazione per cui **non rimangono salvati i destinatari e mai restino memorizzate le password di accesso**, a meno che, e ciò è bene che venga specificato dal datore, ciò non sia funzionale all'esatto adempimento della prestazione o alla tutela del patrimonio aziendale o ancora alla sicurezza del lavoro.

Relativamente agli altri due principi, la **correttezza** esplica senz'altro l'onere di rendere noti i controlli ai lavoratori tramite la suddetta informativa privacy ai sensi dell'art. 13 del D.Lgs. n. 196/2003, ben potendo poi configurarsi modalità di controllo anche "occulto" per scongiurare in concreto danni per esempio al patrimonio aziendale; sembra contraddittorio, in realtà sarà premura del datore adempiere preventivamente all'informativa *ad hoc*, a quel punto, al ricorrere dei presupposti di legittimità dei controlli difensivi, anche "occulti", potrà episodicamente servirsi senza doverne dar conto ai dipendenti (l'informativa preliminare riguarderà l'installazione dell'impianto di controllo e le sue caratteristiche, le finalità ed eventualmente le modalità operative: ovviamente l'effettivo utilizzo, ove ne ricorrano i presupposti, non sarà preannunciato).

Relativamente alle finalità determinate ed esplicite ci si riferisce sempre alla predisposizione, ad opera dell'imprenditore, di un regolamento da portare a conoscenza dei dipendenti, nel quale, per esempio, specificare chiaramente se possibile o meno scaricare musica, video o altro, se possibile tenere una propria cartella file, se soggetta a controlli, differenziando tra apparecchi concessi in uso personale, aziendale o condiviso.

Tutto ciò poi andrà ulteriormente implementato con l'**art. 3 Codice privacy**, il quale così recita: «I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in

modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità», statuisce il **principio di necessità** del trattamento dei dati.

In definitiva si viene ad instaurare un *regime di trasparenza rafforzato*, ispirato ad una tutela della "privacy by design" (ossia fino dalla fase di progettazione dei controlli e delle apparecchiature ad essi predisposte), utile, e talvolta risolutivo, non soltanto al lavoratore per il rispetto di diritti a rilievo costituzionale, ma anche per la parte datoriale, la quale avendo tali premure, si premunisce da eventuali contestazioni o evita che determinati dati raccolti a lei necessari, siano altrimenti inutilizzabili.

Si potrebbe perfino osare un vero e proprio nesso di *conseguenzialità tra pubblicità-trasparenza e legittimità del controllo*, quantomeno del mezzo in sé considerato.

A suffragio di una lettura di tal fatta sembra attingibile la sentenza della Cassazione civile, sez. I, 1° agosto 2013, n. 18443, la quale dichiara violato l'art. 4 poiché il datore avrebbe trattato i dati senza alcun consenso e senza aver informato previamente né le Rsa, né l'interessato circa tali operazioni di monitoraggio.

Nella stessa direzione inoltre la Cassazione penale, sez. V, 11 dicembre 2007, n. 47096, la quale ritiene che non sussista violazione del segreto di corrispondenza elettronica se il datore legge le e-mail aziendali dei dipendenti in presenza di un regolamento d'impresa che imponga la comunicazione della password del terminale e dell'accesso di posta al superiore gerarchico; a quel punto il segreto opererebbe solo per la corrispondenza chiusa a lui non diretta.

Oltre all'interferenza con il Codice privacy in realtà l'art. 4 si interseca più o meno direttamente, in virtù del principio sistematico, con le disposizioni ad esso tangenti nello stesso Statuto dei lavoratori: si faccia riferimento agli artt. 3 e 8, Stat. lav.

Per quanto riguarda l'**art. 3, Stat. lav.**, dettando esso il principio generale della riconoscibilità del controllo. Si crea evidentemente un problema in ordine alla pacifica ammissibilità dei controlli difensivi "occulti", stante l'obbligo di informare i lavoratori interessati circa i nominativi e le man-

Jobs Act

sioni specifiche del personale addetto alla vigilanza dell'attività lavorativa. Riteniamo che tale categoria, per tutte le ragioni espresse nella relativa sede, resti comunque legittima al ricorrere delle predette condizioni.

Con riferimento all'**art. 8, Stat. lav.**, il quale così prescrive: «È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore», sorge un altro tipo di osservazione.

La disposizione sancisce il divieto di indagini sulle opinioni ad opera del datore, del quale è utile, ai fini del nostro percorso, riportare una serie di riferimenti giurisprudenziali: nello specifico non costituiscono violazioni la conoscenza "occasionata" da un sistema di controllo informatico aziendale qualora manchi la "volontà diretta" all'acquisizione (Trib. Milano 31-03-2004); allo stesso modo il datore può annotare quotidianamente, per ogni telefono aziendale, chiamate, numero e durata, se tale operazione mira al contenimento dei costi (Trib. Torino 9 gennaio 2004); infine un sistema elettronico di rilevamento presenze ai fini degli adempimenti retributivi-contributivi è da ritenersi legittimo (Pret. Milano 12 luglio 1988).

Tutti questi riferimenti concreti non solo rafforzano l'orientamento "pro datore" che valorizza le esigenze aziendali, quindi spendibile a livello argomentativo anche per l'art. 4, ma inoltre contribuiscono ad avallare le tecnologie qui dedotte anche in relazione agli stessi controlli "a distanza".

Perlomeno in sede processuale ciò potrebbe rappresentare un elemento probatorio in più, di supporto per altri raccolti dal datore (c.d. prova indiziaria).

A tal proposito la seconda giurisprudenza appena riportata ascrivibile al Tribunale di Torino, potrebbe per esempio giocare a favore, in senso contrario al prevalente orientamento, dell'ammissibilità per il software di documentazione ed elaborazione dei costi telefonici aziendali "Blues"

qualora, in aggiunta, ne sia stata data previamente informativa ai dipendenti e se filtrato per non vessare "personalmente" gli stessi.

Trattasi di una mera ipotesi probatoria, non di certo una strada battuta, la quale in sostanza propone l'utilizzabilità del mezzo, per così dire legittimato per altra via, anche in relazione alla fattispecie ex art. 4.

Videosorveglianza

Ora ci si occuperà del settore specifico della videosorveglianza quale possibile strumento di controllo "a distanza", di per sé fattispecie massimamente sensibile, non solo in contesti lavorativi, alla normativa privacy.

Tale ulteriore approfondimento sarà utile per rispondere ad alcuni interrogativi di carattere tecnico-pratico di fronte ai quali un qualsiasi imprenditore può trovarsi rispetto all'installazione e alla fruizione di tali dispositivi.

Come e in che misura è legittima la videosorveglianza in azienda? Dove in concreto possono essere posizionate le telecamere? Quale deve essere il loro orientamento? Cosa possono inquadrare e secondo quali modalità? Quali sono i tempi di conservazione delle immagini e dei dati così prodotti? Che utilizzo si può fare di dette immagini? Assumendo come punto di partenza il dato normativo così come appena modificato ad opera del D.Lgs. n. 151/2015, la videosorveglianza è legittima se l'utilizzo è subordinato alla sussistenza di ragioni organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale, e se l'installazione è subordinata al previo accordo sindacale o sostituito; in ogni caso occorre una **previa adeguata informativa ai dipendenti**, così come inequivocabilmente certifica il provvedimento del Garante in materia di videosorveglianza dell'8 aprile 2010, inserendo l'informativa tra gli adempimenti applicabili sia a soggetti pubblici sia privati.

Sempre da un punto di vista normativo, resta fermo comunque il rispetto di altre disposizioni ordinarie quali le vigenti norme civili e penali in materia di interferenze illecite nella vita privata quale l'art. 615-bis del codice penale (30).

(30) Lo ribadisce l'Autorità garante nel provvedimento dell'8 aprile 2010 in materia di videosorveglianza appunto. La norma così recita: «Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o im-

magini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la *reclusione da sei mesi a quattro anni*.

Alla stessa pena soggiace, salvo che il fatto costituisca più

È comunque evidente che, ancora una volta, il richiamo meramente normativo non sia affatto risolutivo per fornire delle direttrici chiare e precise al datore di lavoro. Ecco allora nuovamente necessaria l'integrazione della fattispecie per via giurisprudenziale, sia quella tradizionale/ordinaria, sia quella riconducibile all'attivazione preliminare dell'Autorità Garante ex art. 17, comma 2 del Codice della privacy evidenziata all'inizio del paragrafo.

È infatti lo stesso Garante a tracciare dei **principi specifici di liceità del trattamento mediante videosorveglianza** proprio nel provvedimento dell'8 aprile 2014.

In particolare si faccia riferimento al **principio di liceità**, previsto sia per i soggetti pubblici (svolgimenti di funzioni istituzionali), sia per i soggetti privati (adempimento obbligo di legge) che risulta soddisfatto con l'osservanza delle procedure e delle condizioni di cui all'art. 4, Stat. lav., quello di **necessità**, già operante come visto al trattamento dati in generale, il quale implica l'obbligo di configurare un sistema che riduca al minimo l'utilizzazione dei dati registrati, quello di **proporzionalità** che si riflette direttamente nelle concrete «modalità di ripresa e dislocazione», nonché nelle «fasi del trattamento», il quale ancora una volta richiamerà ai principi di *non eccedenza e pertinenza rispetto alle finalità perseguite*.

Finalità appunto, anch'esse attenzionate nel medesimo provvedimento e riconducibili alla *protezione e incolumità degli individui, protezione della proprietà, rilevazione, prevenzione e controllo delle infrazioni e anche all'acquisizione di prove*. Tutti scopi perfettamente in linea con le causali ex riscritto art. 4.

Inoltre, salva quale premessa iniziale, l'eventuale inquadrabilità della sorveglianza video nei «controlli difensivi», con tutto quello che ne consegue in termini di legittimità del controllo ed utilizzabilità dei dati raccolti, la Corte di cassazione del 30 gennaio 2014, n. 4331 ha sancito che *l'installazione di una telecamera «diretta verso il luogo*

di lavoro» o su spazi dove i dipendenti hanno «accesso, seppur sporadico», deve essere previamente autorizzata. In realtà, per completezza, seppur cronologicamente anteriore e contro l'orientamento dominante, la giurisprudenza aveva ammesso l'installazione delle stesse nel luogo di lavoro «laddove, pur in assenza di autorizzazione sindacale, risulti comprovato l'assenso da parte della totalità dei lavoratori in azienda» (31).

A questo riguardo, operando ancora una volta in combinato disposto con l'**art. 23, comma 3 del Codice della privacy**, ci accorgiamo che avremo a che fare con un consenso validamente prestato se «informato, libero, espresso, specifico ed avente una forma esteriore».

Nel caso di specie si era in presenza di quattro telecamere, di cui due di queste dirette alle postazioni di lavoro; tutto adeguatamente segnalato anche per mezzo di apposite affissioni. Un'impostazione di tal fatta sembrerebbe attribuire «disponibilità» al diritto di riservatezza, fra l'altro suffragata dalla stessa disciplina di consenso ai fini del trattamento dei dati personali.

Volendo però tornare alla giurisprudenza più recente, la posizione assunta dalla n. 4331/2014 induce inevitabilmente ad una riflessione di principio non trascurabile: la riservatezza si erge quale bene giuridico implicante una tutela a priori, motivo per il quale l'autorizzazione si considera necessaria già per la mera installazione-predisposizione delle apparecchiature potenzialmente lesive.

In quest'ottica il datore di lavoro non potrà montare la videosorveglianza in assenza di accordo sindacale o sostituto amministrativo, lasciandola poi spenta o inattiva, e non potrà nemmeno installare dispositivi finti, posta l'idoneità degli impianti a ledere il bene giuridico anche se non in funzione (a tal proposito si rimanda alla previa distinzione tra «reato di pericolo-installazione» e «reato di danno-impiego»). Nella prassi il problema non è di poco conto, dal momento che potrebbe vedersi addebitata una contestazione l'imprenditore che non abbia ancora provveduto, per

grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o

con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato».

(31) Cass. pen., sez. III, 11 giugno 2012, n. 22611, fortemente criticata dalla dottrina, in particolare vedi A. Bellavista, *Gli accordi sindacali in materia di controlli a distanza sui lavoratori*, in *Il lavoro nella giurisprudenza*, 2014, 8-9, pag. 738.

Jobs Act

esempio, nemmeno ad allacciare elettricamente il sistema.

La riproposizione della questione penalistica circa la scissione installazione-impiego pone un quesito di sistema riferibile al tema delle norme penali "in bianco" con riferimento proprio all'art. 4 in ragione del fatto che, nella prassi, sono proprio i provvedimenti e le linee guida tracciate dall'Autorità Garante, insieme ad un'attività giurisprudenziale fortemente creatrice sul tema, a riempire di contenuto, quantomeno operativo, il medesimo (quanto detto è lampante ripercorrendo proprio quest'ultimo paragrafo).

Relativamente a questo interrogativo, e ad altri, quali per esempio l'esistenza o meno di una legittimazione attiva anche datoriale per adire preliminarmente ex art. 17 del Codice privacy l'Autorità *ad hoc*, che riteniamo possano essere rilevanti in concreto per il tema oggetto d'indagine, ci riserviamo eventualmente un ulteriore e più penetrante approfondimento circa il ruolo assunto da tale Autorità nell'impalcatura del sistema delle fonti di diritto rispetto agli atti "normativi" da essa costantemente prodotti come introduttivamente riportato.

Più concretamente stiamo vagliando la praticabilità - se di interesse da parte della società - dell'ipotesi di poter adire la medesima Autorità da parte del datore per ottenere una sorta di certificato di conformità ex art. 4, Stat. lav. e art. 113, Codice privacy, e correlati con riferimento allo specifico apparecchio, alle specifiche modalità, agli specifici luoghi dedotti dal caso concreto, grimaldello con il quale l'imprenditore potrebbe tutelarsi, in via preventiva, da ogni eventuale contestazione, ciò, talvolta, anche scavalcando l'accordo con i sindacati.

In una prospettiva di tal fatta il Garante enuncia una casistica da assoggettarsi a verifica preliminare: sistemi di videosorveglianza abbinata a rilevamento biometrico, software che consentono il riconoscimento delle persone, sistemi c.d. intelligenti (ossia che rilevano comportamenti o eventi anomali, segnalandoli), sistemi integrati di videosorveglianza, nelle ipotesi di allungamento dei tempi di conservazione delle immagini registrate oltre 7 giorni.

Si è infatti spesso detto, anche in questa indagine, che è molto complesso provare a stabilire

astrattamente la legittimità o meno di un controllo ex art. 4; a conferma di tale impostazione e, ai fini della comprensione dell'importanza che assumerebbe la fattibilità dell'ipotesi appena paventata circa la legittimazione attiva datoriale ex art. 17, comma 2 del D.Lgs. n. 196/2003, si tenga presente che per ottenere l'autorizzazione dello strumento in sede di accordo sindacale/DTL, l'istanza del datore di lavoro dovrà contenere in concreto le planimetrie dei locali e dovrà essere quindi accompagnata da una relazione tecnica di un professionista.

Ciò induce a considerare tale autorizzazione specifica in relazione alla finalità dedotta dal datore di lavoro e alla tipologia strumentale concreta, per cui la stessa si riferirà al numero di telecamere, al tipo (schede tecniche dell'impianto), alla dislocazione e all'angolo visuale delle stesse in relazione alla specificità degli spazi e delle mansioni dedotte in essi.

È evidente quindi la complessità in senso tecnico della procedura, da aggiungersi al massiccio numero delle stesse.

Tale ragione ha indotto il Ministero del lavoro e delle politiche sociali ad una nota il 16 aprile 2012, n. 7162, nella quale si predispose la semplificazione del rilascio dell'autorizzazione amministrativa mediante la possibilità della Dtl di riferirsi esclusivamente alla documentazione prodotta dal datore, evitando di attendere eventuali accessi ispettivi di verifica; questo snellimento si applica per quelle attività dove il rischio di furti e rapine è più alto, *ricomprendendovi espressamente le farmacie, e quindi potendo estendere la deroga anche per le aziende farmaceutiche.*

Proseguendo su questa strada, in merito al posizionamento e all'orientamento della videosorveglianza, ad eccezione dei locali aperti alla clientela, per i quali non sono previste particolari restrizioni se non l'adeguata segnalazione e conservazione, negli ambienti di mero lavoro vige il principio per cui non vanno inquadrate postazioni fisse o zone esclusivamente destinate all'attività lavorativa, salvo che il controllo sia affidato alle Forze dell'ordine, mentre invece per esempio sono ammesse telecamere che sorvegliano porte, finestre o zone di passaggio quali i corridoi (32).

È facile intuire il perché di tale differenziazione e l'origine normativa della stessa (pertinenza di-

(32) Linee guida Ministero lavoro www.lavoro.gov.it.

retta-indiretta, finalità di tutela patrimonio aziendale, ecc.).

A tal proposito a livello di principio non sembrerebbero installabili in zone relax, mense, spogliatoi, armadietti, bagni a meno che non sussistano, per esempio, pericoli di danno e furti oppure non ricadano nella fattispecie del controllo difensivo.

In questa direzione il Tar Lombardia dell'11 luglio 2013, n. 1815, il quale dispone la legittimità della videosorveglianza anche nei locali adibiti per la mensa in ragione di un effettivo pericolo di furti o danni, purché direzionate sulla cassa e non indistintamente. Sempre nel medesimo caso la concertazione sindacale aveva concesso sì l'autorizzazione, ma in presenza di una specifica cautela secondo la quale le telecamere dovevano deviare l'angolo di ripresa se l'acquisizione nitida dell'immagine non fosse stata indispensabile.

La giurisprudenza citata da ultimo è estremamente significativa poiché può rappresentare una sorta di *vademecum* in tema di videosorveglianza sul luogo di lavoro, ribadendo pressoché la totalità dei principi e delle formule finora descritte: *dimensione "umana" della vigilanza sul lavoro*, *necessità di una tecnica di bilanciamento*, *concetto di distanza da intendersi sia in senso spaziale, sia in senso temporale*, *divieto di controllo se all'insaputa del prestatore*, *legittimità dei controlli difensivi*, *incidentalità e occasionalità della ripresa delle postazioni di lavoro*, *discontinuità e occasionalità del controllo*, *circoscrizione delle immagini* e molti altri ancora.

Sempre con riferimento all'inquadratura della videosorveglianza, questa sarà ammissibile anche in assenza di apposita autorizzazione *ex novo* art. 4 se le stesse dovessero riprendere solo luoghi esterni dell'edificio (in quel caso fra l'altro sarebbe anche scontata la *ratio* di tutela riferibile ad un interesse coinvolgente il solo datore di lavoro: tutela del patrimonio aziendale e sicurezza), salvo dovesse venir svolta anche in quegli spazi antistanti, seppur in modo saltuario e occasionale, l'attività di lavoro, quale per esempio zone di carico e scarico merci adiacenti ai capannoni.

Un'ulteriore specificazione della normativa ci viene suggerita poi dal Consiglio di Stato, sez. V, 5 giugno 2015, n. 2773; in particolare si vieta la videosorveglianza dei lavoratori, ancorché finalizzata alla prevenzione e repressione di furti e taccheggi all'interno di un supermarket, qualora

la competenza sia devoluta ad un soggetto titolare anche del potere di avviare azioni disciplinari nei confronti dei dipendenti medesimi. Il caso in questione è molto interessante perché mostra come avviene in concreto il bilanciamento di interessi, i quali, come vedremo, tutti in astratto meritevoli di tutela e previamente suffragati dalla giurisprudenza: la fattispecie prevedeva che a svolgere il controllo sui lavoratori fosse il direttore del personale e che l'orientamento dei dispositivi fosse idoneo a riprendere non solo eventuali taccheggiatori ma anche occasionalmente il passaggio e l'attività dei dipendenti (circostanza che, come prima visto, a volte è ammessa). Ciò aveva indotto il Collegio a decretare l'illegittimità del monitoraggio nel caso di specie adducendo come motivazione la «percezione dei dipendenti di muoversi sotto visione continua e costante del direttore», dimensione vietata poiché troppo invasiva.

Per ritenere compiuto il tema della videosorveglianza si passerà ora a specificare *l'utilizzabilità delle immagini registrate* e *i relativi tempi di conservazione*.

Com'è buona abitudine si parte dal dato normativo il quale presuppone che i dati così raccolti potranno essere utilizzati anche a sostegno di provvedimenti disciplinari, a condizione che al dipendente sia stata data adeguata e previa informativa circa le modalità di impiego delle apparecchiature e circa le modalità di svolgimento dei controlli, nel rispetto, verso tutti i lavoratori, del Codice della privacy. Nello specifico ed operativamente il datore dovrà rendere l'informativa di cui all'art. 13 del Codice della privacy, oltre a dover adottare un disciplinare interno o regolamento aziendale che specifichi il controllo così come previsto dall'Autorità Garante il 1 marzo 2007. Tale specificazione è stata qui riportata ma trova applicazione per ogni tipologia di controllo "a distanza" seguendo la filosofia citata della c.d. "privacy by design".

In relazione alla conservazione delle immagini o dei dati così ottenuti, ci si deve invece necessariamente richiamare all'**art. 11 del Codice privacy** e annesse pronunce dell'Autorità, chiamata più volte a rispondere in concreto anche per prorogare dette tempistiche, come accaduto a titolo esemplificativo col provvedimento del 16 aprile 2014, laddove accertate esigenze di salvaguardia del patrimonio aziendale (sottrazione di circa

Jobs Act

45.000 libri per un valore pari a 961.676 euro) avevano indotto l'Autorità ad un allungamento di conservazione fino a 30 giorni.

Andando per ordine, il sopracitato art. 11, alla lettera e), così recita: «*conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*».

Tale **principio generale di stretta conservazione delle immagini** trova effettivamente conforto in ogni provvedimento-pronuncia dell'Autorità in questione: si pensi al Provvedimento del 26 febbraio del 2009 con il quale è stato disposto il blocco di immagini videoriprese in un supermercato, posto che non si giustificavano nel caso di specie «esigenze particolari atte a giustificare la conservazione per un arco temporale di tre giorni, ribadendo che occorre pertanto commisurare il tempo di conservazione delle immagini alle effettive necessità di raccolta».

Per ovviare a questa formula astratta, il Garante con Provvedimento generale dell'8 aprile 2010 già citato ha previsto specificamente, oltre a dettagliate indicazioni in tema di videosorveglianza, i tempi di conservazione, limitandoli ad un arco temporale di 24 ore successive alla rilevazione e che solo in casi particolari possa giustificarsi una dilatazione dello stesso, non superiore comunque alla settimana; inoltre ha statuito la disposizione della cancellazione automatica al termine del periodo consentito, mediante sovrascrittura delle immagini stesse. Successivamente, precisamente il 29 aprile del 2010, il Garante ha disposto un aggiornamento delle direttive sancendo le ragioni per le quali la conservazione delle immagini può essere protratta oltre le 24 ore: peculiari ragioni tecniche o per particolare rischiosità dell'attività dedotta (es. banca per l'identificazione degli autori di una rapina oppure per esigenze di lotta al terrorismo).

Sanzioni

L'articolo 23, ultimo comma del D.Lgs. n. 151/2015, nel modificare l'art. 171 del D.Lgs. n. 196/2003 conferma in linea generale la **tutela penale** del divieto di operare controlli a distanza con impianti audiovisivi e altri strumenti di controllo non accordati o non autorizzati preventivamente, ma, alla luce della scissione precedente-

mente osservata tra «installazione» e «impiego» e della conseguente configurabilità di due diverse fattispecie di reato, determina una diversa operatività, rispetto al passato, delle sanzioni penali per questo specifico aspetto.

In ogni caso, posto l'interesse sindacale in gioco con riferimento alla possibile conclusione di un accordo di tale natura *ai fini della mera installazione* (quindi non con riferimento, come in passato, all'intero primo comma dell'art. 4), eventuali violazioni attinenti questo specifico momento saranno idonee ad integrare anche l'**art. 28, Stat. lav.** relativo alla **repressione della condotta antisindacale** per cui, laddove il datore non dovesse rispettare gli adempimenti previsti dal Decreto motivato immediatamente esecutivo prodotto dal giudice del luogo relativo alla cessazione del comportamento illegittimo e alla rimozione degli effetti dello stesso, ciò implicherebbe l'integrazione dell'art. 650, c.p., il quale dispone, salvo che il fatto non costituisca più grave reato, l'arresto fino a tre mesi o l'ammenda fino a euro 206.

In primo luogo si osservi la riscrittura ad opera dell'art. 23 del D.Lgs. n. 151/2015, la quale impone la sostituzione del vecchio art. 171 del Codice della privacy con la seguente formulazione: «*Art. 171 (Altre fattispecie) - 1. La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300/1970*».

Il richiamo alla contravvenzione penale stabilita all'art. 38, Stat. lav. resta e, ferma la sanzionabilità penale per violazione dell'art. 113 Codice privacy, non opera più con riferimento alle violazioni dell'art. 114 del medesimo, prevedendo al suo posto l'integrazione della fattispecie di reato per la violazione del riscritto art. 4, espressamente operante fino all'intervento dell'art. 179, comma II dello stesso Codice privacy, il quale andava a sopprimere le parole «4» e «8» dall'art. 38, Stat. lav.

In sostanza, esplicitando la cervelotica tecnica del “doppio richiamo”, con riferimento alla disciplina dei controlli “a distanza”, ieri (dal momento che lo stesso art. 114 del D.Lgs. n. 196/2003, si limita a stabilire che «*Resta fermo quanto disposto dall'art. 4 della legge 20 maggio 1970, n. 300*») come oggi, un'eventuale violazione si struttura come ipotesi di reato punita in combina-

to disposto con l'art. 38 dello Stat. lav.; ne deriva che il datore di lavoro è punito «con la pena alternativa da euro 154 a euro 1.549 o arresto da 15 giorni ad un anno, salvo che il fatto non costituisca più grave reato. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. Quando per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la

pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale».

Da ultimo, peraltro, si tenga presente che non configurandosi una ipotesi di reato "proprio", della quale potrebbe divenire imputabile il solo datore di lavoro, la contravvenzione in argomento è idonea a colpire anche il comportamento dei soggetti deputati al controllo a distanza o comunque addetti all'utilizzo delle apparecchiature e degli impianti, che saranno puniti alla medesima stregua del datore di lavoro.