Nel corso del 2015 il Governo italiano è intervenuto con quattro decreti attuativi che danno corpo al complesso delle norme in materia di jobs act, realizzando un'ampia riforma del diritto e delle politiche del lavoro. In questa sede si pone l'attenzione verso taluni profili tecnico normativi delineati dalla riforma, che incidono ed innovano il formale dettato normativo sul quale si fondava il pregresso sistema di bilanciamento degli interessi, tra controlli datoriali e diritto alla dignità, libertà e protezione dei dati personali.
Nel precedente numero: 1. Premessa, 2. I controlli datoriali e le novità del jobs act.
In questo numero: 3. Controlli preventivi e controlli difensivi, 4. Strumenti di prevenzione e controllo e loro installazione, 5. Conclusioni.

di Francesco Tavone

PREVENZIONE E SICUREZZA DOPO IL JOBS ACT (II PARTE)

3. Controlli preventivi e controlli difensivi

Come anticipato nei paragrafi precedenti, i controlli difensivi, intesi quali riscontri **diretti ad accertare condotte illecite del lavoratore**, erano ammessi dalla giurisprudenza[1] già prima della riforma dell'art. 4 e si ritiene che la nuova formulazione della norma - come detto, più ampia della precedente -, ben si presti a mantenere ferma tale possibilità.
Con alcune specifiche pronunce, la Cassazione ha, inoltre, ammesso da tempo i controlli cosiddetti diretti, anche se occulti, sul comportamento del lavoratore per accertare illeciti che incidono sul patrimonio aziendale, anche in ragione del solo sospetto o della mera ipotesi che degli illeciti siano in esecuzione[2]. Le facoltà di controllo così delineate si spingono oltre le finalità di accertamento di eventuali responsabilità in caso di illecito (o *post factum*) e consentono di entrare, almeno in parte, nel campo della prevenzione degli stessi, vale a dire in un momento che precede, anche di poco, il possibile verificarsi di eventi dannosi[3].
Secondo gli insegnamenti della Suprema Corte, deve comunque trattarsi di accertamenti diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo e resta fermo che le attività di accertamento devono essere svolte con modalità non eccessivamente invasive, oltre che rispettose delle garanzie di libertà e dignità dei dipendenti[4].

Prendendo in esame le principali pronunce della giurisprudenza, è possibile elaborare una mappa di esempi di controlli difensivi ritenuti, di volta in volta, legittimi. **Un primo caso, anche se risalente ai primi anni 2000, riguarda il controllo datoriale posto in essere con apparecchi di rilevazione di telefonate ingiustificate che la Suprema Corte ha considerato ammissibile – e le relative prove utilizzabili in giudizio - perché diretto ad accertare comportamenti illeciti del dipendente.** Nella pronuncia circa la fattispecie oggetto di disamina, gli Ermellini hanno anche fornito un esempio di altri simili strumenti da ritenersi certamente legittimi, indicando i sistemi di controllo dell'accesso ad aree riservate[5].
Analoga pronuncia ha riguardato l'utilizzo smodato del telefono per ragioni personali da parte del lavoratore che ne aveva la disponibilità per lo svolgimento dell'attività lavorativa[6]. Secondo i giudici, è evidente che se il datore di lavoro ha messo a disposizione un telefono per lo svolgimento dell'attività lavorativa ed il dipendente ne fa un uso improprio ed eccessivo per scopi personali, l'illecito comportamento di quest'ultimo ed il danno che cagiona legittimano i controlli dello stesso datore di lavoro.

In altri casi più recenti, la Suprema Corte ha affrontato il tema dell'utilizzabilità nel giudizio penale delle immagini raccolte con videoriprese effettuate con telecamere installate all'interno dei luoghi di lavoro ad opera del datore di lavoro. Le decisioni hanno confermato in più occasioni che "la finalità di controllo a difesa del patrimonio aziendale non è da ritenersi sacrificata dalle norme dello Statuto dei lavoratori" e, quindi, dalla legittimità dei controlli difensivi deriva, anche in assenza di previo accordo sindacale, l'utilizzabilità di prove di reato acquisite mediante riprese filmate. Tale principio riguarda anche il caso in cui sia imputato un lavoratore subordinato[7].
Un'altra interessante disamina della Cassazione ha, poi, riguardato il controllo effettuato da un istituto bancario sulla posta elettronica aziendale. Nello specifico, è stato ritenuto legittimo il controllo della casella di posta elettronica aziendale assegnata al lavoratore, anche senza il rispetto del preventivo accordo sindacale, poiché il dipendente aveva adottato gravi comportamenti lesivi dell'immagine e del patrimonio aziendale[8].

1 In merito alla legittimità dei controlli difensivi, con particolare riferimento all'utilizzo di impianti audiovisivi volti alla tutela del patrimonio aziendale, la Suprema Corte si è espressa in numerose occasioni, tra le quali: Cassazione Sez. Lavoro, n. 4746 del 3 aprile 2002, n. 15892 del 17 luglio 2007, n. 4375 del 23 febbraio 2010 e n. 16622 del 1° ottobre 2012.

2 Si vedano, in particolare, Cassazione Sez. Lavoro, n. 13789 del 23 giugno 2011 e Cassazione Sez. lavoro, n. 10955 del 27 maggio 2015.

3 Cfr. art. 56 del codice penale, con riferimento al tentativo ovvero agli atti idonei, diretti in modo non equivoco a commettere l'illecito.

4 Si vedano sentenze Cassazione cit. nota 18.

5 Cassazione Sez. Lavoro, n. 4746 del 3 aprile 2002.

6 Cassazione Sez. Lavoro, n. 10062 del 2002.

7 In particolare, si veda Cassazione sez. Penale, n. 20722 del 1° giugno 2010 ed anche Cassazione, sez. Penale, n. 34842 del 12 luglio 2011 nonché Cassazione sez. Penale, n. 2890 del 22 gennaio 2015.

8 Cassazione sez. Lavoro, n. 2722 del 23 febbraio 2012.

Sono stati giudicati legittimi anche i controlli del datore di lavoro eseguiti, tra l'altro, con l' ausilio di un sistema satellitare GPS (*global positioning system*). Il dispositivo, che era collocato sull'autovettura aziendale affidata al dipendente per lo svolgimento delle mansioni assegnate allo stesso, è stato interrogato dal datore per rilevare i movimenti del veicolo e constatare condotte illecite e comportamenti comunque estranei alla normale prestazione lavorativa[9].
La decisione non sorprende, soprattutto se si esaminano precedenti trattazioni da parte del Garante per la protezione dei dati personali in cui l'Autorità[10] ha ammesso l'impiego datoriale di sistemi di localizzazione di *smartphone*, previa comunicazione ai lavoratori e nel rispetto di precise condizioni di garanzia. La funzionalità di localizzazione geografica è stata valutata come legittima perché le finalità del trattamento erano sorrette da adeguate esigenze "*di ottimizzare la gestione ed il coordinamento degli interventi effettuati dai tecnici sul campo, incrementandone la tempestività a fronte delle richieste dei clienti, soprattutto in caso di emergenze e/o calamità naturali*" nonché di "*rafforzare le condizioni di sicurezza del lavoro effettuato dai tecnici stessi, permettendo l'invio mirato di eventuali soccorsi .. in caso di difficoltà*".

Le fattispecie sinora esaminate dimostrano l'ampiezza dei possibili impieghi degli strumenti datoriali e, nel contempo, la profondità delle investigazioni interpretative operate dal giudice e dall'Autorità per distinguere modalità d'impiego e finalità accertative legittime da quelli che invece non potevano ammettersi. Con la modifica dell'art. 4 dello Statuto, i casi sopra esposti possono considerarsi una base di principi certamente noti al legislatore delegato e, dunque, acquisiti come punto di partenza per delimitare i nuovi ambiti di applicazione.

Con queste premesse, il potere di controllo datoriale ben si combina con attività di natura preventiva, senza che queste ultime si avvalgano necessariamente di strumenti di controllo a distanza, come avviene, ad esempio, in materia di sicurezza sul lavoro, ove è richiesto dalle norma di legge[11] che il datore organizzi un servizio di prevenzione e protezione.
Inoltre, sempre in quest'ultima materia, è richiesto al datore di valutare tutti i rischi e di adottare contromisure secondo il principio della massima sicurezza tecnologicamente possibile. L'idea da cui muove tale assunto è che se esiste la possibilità di intervenire in un determinato settore con strumenti e tecnologie in grado di prevenire o ridurre dei rischi, il datore di lavoro ha il dovere di farlo. Il principio appare del tutto corretto ancor più se si considera che l'intera materia muove dalla necessità di tutelare la sicurezza, integrità e, in ultima analisi, il bene della vita dei lavoratori.

Ci si chiede se lo stesso ragionamento possa essere ripetuto dal datore, in materia di prevenzione dai rischi di riduzione del patrimonio aziendale, ovviamente in termini di facoltà d'intervenire con gli strumenti più moderni secondo l'evoluzione della tecnologia. Senza anticipare le riflessioni riportate nei prossimi paragrafi, si ritiene che la risposta possa essere di segno positivo e che la linea di confine possa essere determinata, come per i casi sinora trattati, nella necessità di prevenire abusi ed illeciti.

4. Strumenti di prevenzione e controllo e loro installazione

La nuova impostazione normativa in materia di controlli a distanza, come detto, trae le proprie radici dalle interpretazioni giurisprudenziali date alle precedenti disposizioni. Gli aspetti più apprezzabili della riforma dell'art. 4 dello Statuto risiedono nella chiarezza con la quale è stato delineato il quadro dei controlli e delle possibili installazioni ad essi strumentali.
In questo senso, sono individuate sostanzialmente due categorie:
1. gli impianti audio visivi e gli altri strumenti dai quali può derivare il controllo a distanza;
2. gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa".

Per quanto riguarda gli strumenti di controllo preterintenzionale (videosorveglianza ed altri strumenti), escludendo a priori ipotesi – non verosimili - di controllo datoriale effettuato sul corretto assolvimento della prestazione lavorativa, a distanza e con mezzi diversi dall'osservazione diretta dei responsabili aziendali, si ritiene che non vi siano differenze sostanziali nelle possibilità di legittimo impiego, rispetto ai principi e criteri elaborati da dottrina e giurisprudenza in costanza della precedente formulazione normativa.
Oltre alla necessità che prima dell'installazione si sia positivamente svolta la procedura concertativa-autorizzativa, come chiarito dall'Autorità Garante[12], l'eventuale violazione[13] da parte del datore di lavoro dei limiti alla realizzazione dei controlli renderà inutili, in quanto inutilizzabili, i dati così raccolti ai sensi dell'art. 11, c.2 del Codice in materia di protezione dei dati personali.
In merito, si possono formulare molteplici ipotesi di utilizzo di strumenti, per esempio per finalità di tutela del patrimonio aziendale, che si prestano a raccogliere informazioni suscettibili di impieghi ulteriori, quali gli impianti audio visivi dotati di telecamere con algoritmo di lettura delle targhe. Si tratta di *software* preinstallato e configurato (non è un'aggiunta del datore di lavoro), che permette di effettuare l'analisi e la gestione degli accessi di veicoli in aree private. Tali sistemi, in particolare, consentono di azionare dei meccanismi di automazione quali l'apertura di porte o sbarre quando la targa rilevata coincide con una di quelle presenti nell'elenco creato dall'organizzazione.

9 Cassazione sez. Lavoro, n. 20440 del 12 ottobre 2015.

10 Con provvedimento n. 401 dell'11 settembre 2014, in sede di verifica preliminare richiesta da Ericsson Telecomunicazioni S.p.A.. Il documento è consultabile all'indirizzo Internet: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3474069
Con provvedimento n. 448 del 9 ottobre 2014, del tutto analogo al precedente n. 401 dell'11 settembre 2014, l'Autorità ha riportato le medesime considerazioni sopra esposte anche in occasione della verifica preliminare richiesta da Wind Telecomunicazioni S.p.A.. Il documento è consultabile sul sito web del Garante, al seguente indirizzo Internet: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3505371.

11 Si veda, sul punto, l'art. 31 del Dlgs 9 aprile 2008, n. 81, recante "Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro".

12 Il chiarimento è intervenuto in occasione dell'audizione parlamentare dell'Autorità presso le Commissioni 11^ - Lavoro e previdenza sociale - del Senato della Repubblica e XI della Camera dei Deputati.

13 La violazione della procedura concertativa prevista daei commi 1 e 2 dell'art. 4 Stat. Lav. dà luogo a responsabilità penale di natura contravvenzionale, punita ai sensi dell'art. 38 dello Statuto con l'ammenda da 154 a 1.549 euro o con l'arresto da 15 giorni a un anno.

Inoltre, può essere gestito l'invio di immagini o di notifiche a destinatari opportunamente configurati (via SMS, email, FTP *snapshots*). Il sistema appena esemplificato aiuta a comprendere sia le potenzialità di controllo cui può spingersi il datore di lavoro che, pur per finalità legittime, ne faccia uso, sia i corretti limiti d'impiego cui lo strumento è destinato per naturale finalità (tutela del patrimonio attraverso il controllo selettivo degli accessi) e conformemente ai principi dettati in materia di protezione dei dati personali.

Resta fermo che, oltre al rispetto delle norme del Codice privacy, un altro importante caposaldo che il datore di lavoro deve osservare, affinché i controlli siano effettuati in piene condizioni di legittimità, è che sia resa all'interessato adeguata e, ovviamente, preventiva informativa. Soffermandosi brevemente sul concetto di adeguata informazione, è possibile richiamare analoghe forme normative in cui sia richiesto dare notizie ad un destinatario (ad esempio perché fruitore di un servizio). Per queste ipotesi, si trova in alcuni testi di legge il richiamo a forme di comunicazione chiare e comprensibili[14] che, di fatto, sono l'esplicitazione di modalità che si rifanno ai principi generali di buona fede, correttezza e lealtà.
Tali principi, uniti alla necessità che l'informazione sia fornita prima di eventuali controlli, sono peraltro già desumibili dalla disciplina in materia di protezione dei dati personali che il Garante privacy ha evidenziato in numerosi provvedimenti[15] e che rendono incompatibile ogni forma di controllo occulto.

Con l'osservanza di tali presupposti, si apre per il datore la possibilità, molto più ampia rispetto alla precedente, d'impiegare le informazioni raccolte con gli strumenti ordinari, assegnati cioè al lavoratore per normali esigenze lavorative. Alcuni di essi possono essere di uso strettamente personale ovvero più o meno quotidiano, altri messi semplicemente a disposizione dal datore per l'uso comune (ad esempio, le postazioni di lavoro non nominativamente assegnate).

Come detto, i controlli realizzati mediante tali strumenti non devo essere sottoposti alla procedura concertativa-autorizzativa. Secondo i chiarimenti forniti dal Ministero del Lavoro[16], quanto sinora esposto vale solo nei limiti in cui siano impiegate le normali funzionalità degli apparecchi forniti in dotazione, senza alterazioni o modifiche degli stessi che rendano i dispositivi capaci di effettuare il controllo personale del lavoratore. Ciò non toglie che con gli apparati già installati ovvero con quelli già in commercio siano già possibili applicazioni avanzate con le quali sono raccolte e trattate molteplici informazioni. Si pensi, ad esempio, ai sistemi informativi aziendali, dotati di tutti gli strumenti di rete, mail service, connessione ad Internet e tracciabilità dei dati per numerose delle attività svolte. Potenzialmente, quindi, gli apparati ed i software per la loro gestione si prestano a raccogliere informazioni che il datore di lavoro potrebbe utilizzare in attività di controllo ampie ed invasive.
Tali fattispecie sono state già esaminate dal Garante privacy che ha chiarito in numerosi provvedimenti[17], ad esempio, che non sono consentite, al datore di lavoro, la lettura e registrazione sistematica delle e-mail e delle pagine web visualizzate dal lavoratore. Nei provvedimenti dell'Autorità, sono stati ovviamente esclusi dalla facoltà datoriale i cosiddetti controlli massivi ed i casi che gli sono stati sottoposti sono stati esaminati con costante riferimento ai criteri generali che regolano la materia. In particolare, si tratta dei noti principi di legittimità e determinatezza del fine perseguito, nonché di proporzionalità, correttezza e non eccedenza del trattamento.

Del resto, la necessità per un datore di lavoro di avviare campagne di controllo generalizzato appaiono poco utili e costose oltre che ipotizzabili per rari casi. Per tali aspetti, si ritiene che possano essere molto più efficaci le misure di prevenzione[18], adottate senza fini di tracciamento dati, che inibiscano determinate funzionalità come nel caso della navigazione in Internet, verso siti dai contenuti illegali, immorali ovvero potenzialmente pericolosi in quanto utilizzati dagli hacker quale veicolo di diffusione di *malware*.
Simili sistemi di prevenzione con l'applicazione di un blocco o filtro dell'accesso da parte del lavoratore in spazi fisici o virtuali potrebbe, del resto, rispondere ad esigenze organizzative e gestionali utili anche ad altri fini. Nel caso di reati commessi dal dipendente, potrebbe essere di grande beneficio per il datore di lavoro, al fine di non incorrere nella responsabilità dettata dal Dlgs n. 231/2001[19], dimostrare che il reato è stato commesso eludendo fraudolentemente dei presidi di prevenzione (come i filtri sopra citati) previsti nel modello di organizzazione e di gestione aziendale.

5. Conclusioni

Le esigenze datoriali di svolgere, nelle appropriate occasioni, i controlli difensivi vanno valutate e previamente ordinate in modo da costituire regola di normale e comune conoscenza aziendale, contro il rischio, alla luce delle nuove disposizioni, di un utilizzo pervasivo dei controlli sul lavoro. Il maggiore strumento per l'autovalutazione datoriale ancor prima dei chiarimenti che saranno forniti dal Garante Privacy, risiedono nella conformità ai principi dettati dal Codice.
L'equilibrio che l'applicazione di tali principi fornirebbe nel rapporto tra esigenze produttive e dignità del lavoratore è inoltre sorretto dal bilanciamento tra tutela del lavoratore e legittime esigenze datoriali rilevabile nei numerosi provvedimenti dell'Autorità. ©

14 Cfr. art. 67-quater del Dlgs 3 ottobre 2007, n. 221, recante "Disposizioni correttive ed integrative del decreto legislativo 6 settembre 2005, n. 206, recante "Codice del consumo, a norma dell'articolo 7, della legge 29 luglio 2003, n. 229", pubblicato nella Gazzetta Ufficiale n. 278 del 29 novembre 2007.

15 Per tutti, si veda " Linee Guida per l'utilizzo della posta elettronica e di internet nell'ambito dell'attività lavorativa", cit. nota 11.

16 Cfr. nota 14.

17 Per tutti, si veda il provvedimento recante "Linee guida per la posta elettronica e Internet", già citato in nota 11.

18 Nello stesso senso si esprime la Raccomandazione del Consiglio d'Europa del 1° aprile 2015.

19 Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300".