Jobs act e controlli digitali

Il **controllo del lavoratore** da parte del **datore di lavoro** è un tema di grande attualità non soltanto per l'evoluzione informatica e telematica ma, anche, per le recenti modifiche all'articolo 4 dello **Statuto dei Lavoratori** in materia di controlli a distanza ad opera del **Jobs Act**.

Lo Statuto dei Lavoratori è stato il primo testo normativo ad occuparsi dei limiti del controllo a distanza, al quale si sono poi affiancate la giurisprudenza della Corte di cassazione sui **controlli difensivi** consentiti al datore di lavoro, un'articolata disciplina di tutela della **privacy del lavoratore**, le linee guida del Garante Privacy sul controllo della posta elettronica e della navigazione in rete e, infine, una sempre più copiosa giurisprudenza di merito sul **controllo "tecnologico" del dipendente**.

Il Dossier analizza e chiarisce la normativa sul controllo del dipendente da parte del datore di lavoro, che "sembra disposta a strati" e non sempre omogenea. Particolare attenzione è riservata alle posizioni interpretative del Garante Privacy a tutela della dignità e dei diritti del lavoratore, con crescente attenzione all'evoluzione tecnologica e ai nuovi tipi di controllo che ne derivano. .

Il problema cardine resta il delicatissimo equilibrio tra **protezione del patrimonio** e della produttività aziendale, capacità invasiva dei nuovi **sistemi di controllo** e ineludibili **diritti del lavoratore** a svolgere la sua attività in maniera serena, dignitosa e senza pericoli di discriminazione.

Nel Dossier, a cura di Giovanni Ziccardi, professore associato di informatica giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano, tutte le **indicazioni utili** sulle novità in tema di **controlli del lavoratore.**

Nuove tecnologie e controlli a distanza

Modifiche del Jobs Act - 09 Febbraio 2016

Controllo del lavoratore nell'era tecnologica, nuove modalità

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

Con l'avvento della tecnologia e le novità introdotte dal Jobs Act, il datore di lavoro ha, oggi, accresciuto il potere di controllo nei confronti del lavoratore e della sua attività. Gran parte dei processi aziendali si svolgono, infatti, proprio su reti e strumenti tecnologici che il datore di lavoro, e i suoi amministratori di sistema, possono agevolmente controllare. Se prima il controllo dei lavoratori era limitato a un periodo di tempo o a una zona dell'azienda attraverso telecamere o cimici, oggi, invece, il controllo tramite l'elettronica non ha limiti né di spazio, né di tempo.

Le modalità di controllo si evolvono, quasi naturalmente, di pari passo con le tecnologie. Ciò lo si nota anche nel delicato ambito del controllo effettuato dal datore di lavoro nei confronti del lavoratore, sia quando lo stesso opera all'interno dei locali dell'azienda, sia quando svolge le sue mansioni al di fuori dei muri aziendali.

Evoluzione normativa e modalità di controllo

Il tema del **controllo del lavoratore** per il diritto (ma anche per la tecnologia) è un tema tipicamente sviluppatosi negli anni Settanta. Lo Statuto dei Lavoratori, tra le altre cose, cercò di limitare e disciplinare con cura, nell'articolo 4, modalità di controllo che già si erano diffuse dal secondo dopoguerra in avanti e che potevano intaccare direttamente la dignità dei lavoratori. Erano tre, allora, le **modalità tipiche di controllo**.
La prima era la raccolta di dossier, la compilazione di schede, la **catalogazione d'informazioni** che erano ottenute, solitamente, dalle forze dell'ordine o dalle parrocchie. Il caso clamoroso degli schedari della Fiat, rivelatosi davanti al Pretore di Torino durante una banale vertenza di lavoro, rese evidente come il controllo dell'informazione (in particolare dell'appartenenza politica, delle convinzioni religiose, delle abitudini familiari ed extra-familiari) potesse aiutare a controllare la "vita aziendale" in un periodo di grande immigrazione nelle aziende del nord e di preoccupante fermento sindacale.
Il secondo metodo di controllo era più "fisico" e strutturale: si pensi al posizionamento delle **postazioni di lavoro** di modo che tutti i dipendenti fossero visibili, o alla installazione di pareti di vetro che consentissero il controllo in tempo reale dei dipendenti o, ancora, all'inserimento di "spie" e "controllori" nell'organico affinché riferissero al titolare di determinati comportamenti in violazione del patrimonio aziendale o di problemi sorti sul posto di lavoro.
Il terzo modo di controllo, che apparve alla fine degli anni settanta e che era poco diffuso perché ancora molto costoso, ma che rappresentò il collante tra metodi obsoleti di controllo e un'idea più moderna di sorveglianza, fu operato attraverso la **telecamera**. Da telecamere che riprendevano in tempo reale, e non memorizzavano i dati, si passò a strumenti sempre più sofisticati che permettevano di custodire le informazioni per lungo tempo e di recuperarle in caso di necessità. Alle telecamere si affiancarono, negli anni ottanta, strumenti di controllo delle centraline telefoniche o dei telefoni aziendali e del chilometraggio delle vetture concesse in uso ai dipendenti.
Lo Statuto dei Lavoratori fu pensato anche per disciplinare simili tipi di controllo, al fine di evitare discriminazioni sul posto di lavoro e lesioni della dignità del soggetto controllato. Non si focalizzava su quegli strumenti ma prevedeva, con definizioni "aperte", anche futuri metodi di controllo e tecnologie che sarebbero di lì a poco sopravvenute.

Cosa cambia con l'avvento della tecnologia

L'avvento della tecnologia, negli anni Novanta, mutò completamente il panorama e il tipo di controllo. Accanto ai metodi già citati, si iniziarono a compiere **operazioni di verifica sul computer** concesso al dipendente, sui primi telefoni cellulari e, dopo il duemila (con la diffusione di Internet su larga scala anche in Italia), sul traffico di rete.
La differenza tra la sorveglianza moderna (dall'avvento di Internet sino a oggi) rispetto a quella degli anni Settanta riguarda essenzialmente due aspetti: i) il **potere invasivo**, e ii) la difficoltà di separare il controllo dei dati correlati alla mansione lavorativa dalla captazione dei dati privati.

Il primo punto è semplice da comprendere: oggi il controllo si può fare su tutto. Sul computer e sul suo uso, sulle e-mail ricevute e inviate, sulla cronologia della navigazione dei siti web e sui siti web consultati, sui messaggi inviati e ricevuti sullo smartphone, sulle conversazioni in chat, sul posizionamento geografico del soggetto se ha attivato un GPS, e così via. Strumenti innovativi come i droni permetteranno anche di superare le barriere fisiche del controllo.
Il datore di lavoro ha quindi, oggi, un enorme potere di controllo che gli è fornito dalle tecnologie e dal fatto che gran parte delle attività aziendali dei dipendenti si svolgano proprio su quelle reti e tecnologie che lui, e i suoi amministratori di sistema, possono agevolmente controllare.
Se prima, quindi, una telecamera o una cimice o un controllore “fisico” avevano un potere di controllo comunque limitato (a un periodo di tempo, o a una zona dell’azienda), oggi il controllo tramite l’elettronica non ha limiti né di spazio né di tempo. Può essere attivato in tempo reale (mentre il dipendente lavora), può essere differito (quando il lavoratore non è presente), può essere effettuato sugli strumenti usati durante il giorno e poi restituiti.
Il secondo aspetto è anch’esso molto importante per il diritto e per la privacy. Prima era facile separare il controllo di dati aziendali da quello dei dati privati. Oggi l’informatica, e l’uso del computer come strumento personale quotidiano spesso anche in azienda, rendono difficile una tale separazione. In estrema sintesi: i **controlli di oggi tendono a “pescare a strascico” ogni informazione**, ed è poi nella diligenza di chi controlla separare dati correlati alle mansioni aziendali da dati chiaramente personali. Si ricordi che, ad esempio, la navigazione su siti web può rivelare aspetti intimi (politici, sanitari, sessuali) del dipendente semplicemente visionando il tenore del sito cui si è collegato.

Considerazioni conclusive

In un quadro tecnologico così mutato, il diritto fatica a disciplinare ogni aspetto, soprattutto quando diverse norme si sovrappongono. Verso la fine degli anni novanta l’avvento, anche in Italia, di una normativa sulla privacy (che lasciava intatta la disciplina dello Statuto dei Lavoratori) ha rafforzato la tutela del dipendente ma ha, al contempo, creato un po’ di conflitto con una giurisprudenza sui “controlli difensivi” che si stava delineando e che consentiva al datore di lavoro azioni specifiche di controllo al fine di tutelare il patrimonio aziendale.
Le recenti riforme, poi, dello Statuto dei Lavoratori occorse con il Jobs Act, hanno ulteriormente modificato il quadro, creando all’interprete diversi **problemi di coordinamento tra le disposizioni**. Appare quindi opportuno affrontare nel dettaglio, con metodo e gradualmente, sia gli aspetti tecnici dei controlli più moderni sia la disciplina dello Statuto dei Lavoratori, della normativa sulla privacy e la giurisprudenza in tema di potere di controllo del datore di lavoro.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell’ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Punti deboli del sistema - 11 Febbraio 2016

Strumenti elettronici in uso al lavoratore: controlli in locale o da remoto

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

Il mutare continuo delle tecnologie rende difficile codificare le modalità tipiche di controllo esercitabili dal datore di lavoro sull'attività lavorativa del dipendente. Per cogliere i punti deboli del sistema è utile però identificare le categorie di controllo ipotizzabili sugli strumenti aziendali in uso al lavoratore. Una prima distinzione è quella tra controlli con mezzi che operano "in locale" e controlli con strumenti che operano "da remoto". Il primo tipo di controllo consiste nel verificare l'utilizzo dello stesso entrando in possesso del telefono o del personal computer. Il secondo, invece, può svolgersi anche in tempo reale, ossia mentre il lavoratore sta utilizzando lo strumento aziendale.

Non è semplice descrivere, seppur sommariamente, quali siano le modalità tipiche che un datore di lavoro può esercitare nei confronti di un dipendente. Non è semplice perché le tecnologie mutano ogni giorno e consentono azioni di controllo sempre nuove e, ovviamente, sempre più invasive. Si possono, però, evidenziare chiaramente alcune **"categorie" di controllo** che sono molto utili per comprendere anche quali siano i punti deboli del sistema.

Due le categorie di controllo

Una prima distinzione molto opportuna è quella tra controlli portati sullo strumento in uso al lavoratore con mezzi che operano "**in locale**", e controlli portati sullo strumento che utilizza il lavoratore con mezzi che operano "**da remoto**".
Il primo tipo di controllo è fisicamente connesso al dispositivo, e consiste nel verificare l'utilizzo dello stesso semplicemente entrando in possesso del telefono o del personal computer e analizzando le attività. Si tratta di un controllo che è effettuato, ad esempio, a fine giornata (o a fine settimana/mese) quando il telefono, il tablet o il notebook sono restituiti, o riportati in azienda, o il computer non è più in uso e in possesso del lavoratore. La verifica delle informazioni può essere fatta semplicemente "guardando" cosa è successo sul dispositivo, o acquisendo l'intera memoria per poi analizzarla con calma.
Il secondo tipo di controllo avviene da remoto e può accadere anche in tempo reale, ossia mentre il lavoratore sta utilizzando quello strumento. In tal caso le attività si possono vedere semplicemente "ascoltando" (in gergo si dice "sniffando") il **traffico** e le attività che il lavoratore compie quando è connesso a una rete (può essere sia la rete telefonica mobile sia la rete Internet aziendale) senza necessità di essere in possesso del dispositivo. Per meglio chiarire, si pensi, nel primo caso, a un controllo dei numeri chiamati in una giornata dal cellulare (aprendo e visionando il "registro chiamate") e nel secondo caso al controllo dei file di log sul server che mostrano tutti i siti web cui il lavoratore si è connesso in orario di lavoro dai computer dell'azienda.
Tutti e due i controlli possono essere assai invasivi, e si possono intersecare senza problemi tra loro.

Controlli in locale

Il primo tipo di controllo si basa sul principio ben noto per cui ogni attività che un individuo svolge su un dispositivo elettronico lascia delle tracce. Ciò rende semplice, successivamente, recuperare dette tracce di attività anche se sono state cancellate. In pratica, un lavoratore che utilizza per otto ore al giorno un computer, un notebook o uno smartphone lascia **indizi della propria attività** in determinate aree del sistema. Se le attività sono correlate a mansioni lavorative, nessun problema. Se, invece, le attività sono associate ad aspetti privati e personali della vita del

lavoratore, possono sorgere dei problemi in quanto lo strumento elettronico memorizza anche quelle congiuntamente alle attività lavorative. Si pensi a un lavoratore che si collega al sito dell'azienda per svolgere operazioni "legittime" (consultare il catalogo di vendita e proporre dei preventivi) e subito dopo si collega al sito web di un quotidiano sportivo per leggere gli articoli riferiti alla sua squadra del cuore. I due tipi di dati vengono memorizzati entrambi, senza distinzione. Sarà poi il lettore di quelle informazioni a interpretarle.
Un tale tipo di controllo è quindi basato sul comportamento che tiene il lavoratore quando usa gli **strumenti dell'azienda**, e non si presenta quasi mai come occulto per due motivi: il datore di lavoro avverte di solito il lavoratore che gli strumenti a lui concessi in uso sono aziendali e che è nel potere del datore di lavoro effettuare controlli a campione o mirati, e perché la cultura informatica ormai diffusa in tutti rende consapevoli che le nostre attività digitali sono conservate e controllabili.
Controlli occulti in locale, poco diffusi però in ambito lavorativo e aziendale, sono garantiti invece da microspie inserite nel sistema operativo del telefono o del computer che permettono di controllare anche la posizione, tramite l'attivazione del GPS.

Controlli da remoto

Il secondo tipo di controlli è più subdolo e in alcuni casi meno semplice e intuitivo da comprendere da parte del lavoratore. Viene effettuato da un **amministratore di sistema** e coinvolge soprattutto le cosiddette "attività" di rete, ossia i comportamenti che avvengono all'interno di una rete informatica aziendale. In tal caso le possibilità di profilazione del lavoratore sono ancora più accurate per la possibilità di creare delle statistiche di utilizzo o di abitudini – si pensi all'analisi di tutti i siti visitati in un dato periodo di tempo suddivisi per genere – che costituiscono veri e propri "nuovi dati" ricavati da dati esistenti.
Ciò che accomuna questi due tipi di controllo è la possibilità di vedere ogni attività compiuta dal lavoratore. Sono pochissimi i comportamenti che possono essere tenuti nascosti, e richiedono spesso delle strategie ad hoc o l'uso di strumenti specifici per l'anonimato.
La Redazione segnala
Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Impatti del Jobs Act

Jobs Act e modifiche allo Statuto dei Lavoratori: problemi applicativi

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

Con il Jobs Act si è aperta una nuova era nella disciplina dei controlli a distanza. La portata delle modifiche normative è, infatti, di grande impatto pratico e si applica a tutti i rapporti di lavoro subordinato o etero-organizzato. La grande novità è la mancanza dell'indicazione espressa del divieto generale di controllo a distanza sull'attività del lavoratore. Introdotta, inoltre, la categoria degli "strumenti di registrazione degli accessi e delle presenze", anch'essa molto discussa. Viene richiesto, infine, che venga fornita un'adeguata informazione al lavoratore sulle modalità d'uso degli strumenti e sulla effettuazione dei controlli e che sia rispettato il codice della privacy.

Il tema del controllo a distanza dell'attività dei lavoratori, d'attualità sin dagli anni settanta, ha subito un discusso cambiamento normativo nel 2015, si diceva, con l'articolo 23 del Decreto Legislativo n. 151 del 2015, parte del cosiddetto "Jobs Act".
Le modifiche sono importanti ed essenziali e hanno aperto, per così dire, una nuova era nella disciplina di questo aspetto, dal momento che sono intervenute direttamente, per la prima volta, proprio sul testo dell'articolo 4.
I dibattiti parlamentari e gli "scontri" aperti con il Garante per la Privacy sono stati la testimonianza di quanto questa modifica fosse considerata critica da larga parte della società civile, dalle organizzazioni sindacali e dal tessuto imprenditoriale.

Modifiche allo Statuto dei Lavoratori

Il testo del tanto discusso articolo 23, che ha modificato l'articolo 4 dello Statuto dei Lavoratori, è il seguente:
"Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196".
1. L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente: «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.».”

Ambito di applicazione

L'articolo 4 dello Statuto dei Lavoratori, nel testo così come modificato dal D.Lgs. 151/2015 indicato poco sopra, si applica a **tutti i rapporti di lavoro** – subordinato o etero-organizzato – a differenza della nuova disciplina del licenziamento che è invece destinata ad applicarsi solo ai

“nuovi assunti” dal 7 marzo 2015.

Superamento del divieto generale di controllo a distanza

La grande novità, che ha richiamato anche i titoli nelle prime pagine dei quotidiani, è stata la mancanza, nel nuovo articolo 4, di una indicazione espressa di un **divieto generale di controllo a distanza** sull’attività del lavoratore.
Il primo comma della norma che abbiamo riportato poco sopra prevede, infatti, soltanto che “impianti audiovisivi e gli altri strumenti di controllo a distanza 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” previa autorizzazione sindacale o amministrativa; al secondo comma si aggiunge poi che “la disposizione di cui al 1 comma non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa” e “agli strumenti di registrazione degli accessi e delle presenze”.
Gli studiosi di diritto del lavoro hanno notato subito questo cambiamento di regime e questa variazione lessicale che è di fondamentale importanza. Prima, nel nostro ordinamento, era esplicitato un divieto generale di controllo a distanza con, poco dopo, le relative eccezioni. Oggi questo divieto non c’è più: è sufficiente confrontare con attenzione il testo precedente e il testo attuale .
Un aspetto interessante di questa modifica è poi quello della “nuova” categoria degli strumenti di lavoro, ossia se si debbano intendere come dispositivi strettamente correlati all’attività professionale o se, semplicemente, possono essere presenti sui dispostivi forniti al lavoratore.
La categoria degli “**strumenti di registrazione degli accessi e delle presenze**”, introdotta dal nuovo testo, è anch’essa molto discussa. Ci si riferisce a strumenti che controllino solo l’accesso e la presenza in azienda del lavoratore, o si possono estendere anche a quelle tecnologie che individuano l’esatta ubicazione del lavoratore durante la giornata di lavoro? Si pensi alla delicatezza, ad esempio, del seguire un lavoratore che si reca a una funzione religiosa, dal momento che il controllare lo spostamento di una persona può rivelare informazioni sensibili riferite alla stessa.

Controlli preterintenzionali o diretti

Nel nuovo testo sono poi inclusi nella categoria dei controlli preterintenzionali o diretti suscettibili di autorizzazione anche quelli che sono finalizzati alla **tutela del patrimonio aziendale**. Anche questo è un punto importante, che sembra avere incorporato nell’articolo 4 la categoria dei controlli difensivi elaborata dalla giurisprudenza e di cui abbiamo già fatto cenno.

Utilizzabilità dei dati

Interessante, al contempo, la previsione che per l’utilizzabilità dei dati “a tutti i fini connessi al rapporto di lavoro”, oltre al rispetto delle regole relative alla installazione e all’uso delle apparecchiature, vi sia la necessità di dare **adeguata informazione al lavoratore** delle modalità d’uso degli strumenti e della effettuazione dei controlli, e che sia stato rispettato il codice della privacy. Anche la normativa sulla privacy è stata quindi in un certo senso “incorporata” nel quadro, e il riferimento a “regolamenti” o “policy” è essenzialmente motivato dal fatto di voler evitare controlli occulti dell’attività del lavoratore, controlli occulti che oggi, grazie alle nuove tecnologie, sono elementari.
I regolamenti e le policy imporranno al datore di lavoro di descrivere in dettaglio al lavoratore con quali mezzi e con quali modalità saranno effettuati i controlli, e ciò verrà a costituire una ulteriore garanzia.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell’ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.

Divieto di utilizzo di impianti e apparecchiature - 12 Febbraio 2016

Controlli a distanza, Statuto dei lavoratori: i principi originali (e ciò che è rimasto)

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

La regola stabilita dal testo originario dello Statuto dei lavoratori era quella di un vero e proprio divieto di utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività del lavoratore. Tale divieto era superabile solo ove vi fossero esigenze organizzative, produttive o per proteggere la salute del lavoratore negli ambienti dove svolgeva la sua attività preminente. Il testo è stato modificato dal Jobs Act, con interventi che sollevano non pochi dubbi interpretativi.

Che l'articolo 4 dello Statuto dei Lavoratori sia, sin dagli anni settanta, la disposizione più importante nel nostro ordinamento circa le possibilità di **controllo in azienda** e sul posto di lavoro in generale, è cosa ben nota. Ormai noto è anche come il testo originario di questo primo riferimento in materia di controllo a distanza del lavoratore, contenuto nella Legge 20 maggio 1970, n. 300 e che vietava "l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", sia stato modificato di recente, con non poche polemiche, introducendo un nuovo testo che, si vedrà, solleva già non pochi dubbi interpretativi.

Il controllo a distanza prima del Jobs Act

Il legislatore di allora, nel regolamentare l'utilizzo in ambito lavorativo degli strumenti, a quel tempo esistenti, in grado di effettuare un controllo a distanza, scelse di stabilire, quale regola generale, il divieto al loro utilizzo.
In quegli anni si era in presenza, essenzialmente, di due metodi implementati nelle realtà aziendali: la videosorveglianza e il controllo del traffico telefonico. La **videosorveglianza** serviva per tenere sotto controllo la produttività del lavoratore tramite telecamere, mentre il controllo del traffico telefonico era più pensato in un'ottica di tutela del patrimonio aziendale e per evitare la distrazione di risorse del datore di lavoro.
Fu poi aggiunto un secondo comma, al principio generale di divieto, secondo il quale gli impianti e le apparecchiature dai quali fosse derivata anche la possibilità di controllo a distanza dell'attività dei lavoratori, potevano essere installati se "richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro" solo previo accordo con le rappresentanze sindacali aziendali o, in assenza di accordo, mediante il coinvolgimento dell'Ispettorato del lavoro. L'ispettorato del lavoro avrebbe dettato le modalità d'uso degli impianti, con determinazioni che erano impugnabili entro trenta giorni innanzi al Ministro per il lavoro e la previdenza sociale.

La regola che era stabilita dal testo originario dell'art. 4 era, quindi, un vero e proprio **divieto di utilizzo**, divieto superabile solo ove vi fossero particolari esigenze ed esclusivamente al fine di soddisfare dette esigenze. I tre "tipi" di esigenze che consentivano di aggirare i divieti erano **organizzative** (correlate, cioè, al sistema organizzativo dell'azienda), **produttive** (finalizzate, quindi, a tutelare la produzione e il patrimonio) o connesse alla **sicurezza del lavoro** (per proteggere la salute del lavoratore negli ambienti dove svolgeva la sua attività preminente).
La norma, collocata nel Titolo I dello Statuto dei lavoratori, mirava alla tutela della dignità del lavoratore, assicurando che il controllo sull'attività lavorativa fosse operato direttamente da persone fisiche, anziché mediante l'utilizzo di apparecchiature.
Tale seconda tipologia di controllo costituiva infatti, nell'ottica del legislatore, una maggiore invasività. La tecnologia permetteva un controllo sia continuativo (procedura che, di persona, avrebbe richiesto invece maggiori risorse "umane") sia occulto (senza che il lavoratore si rendesse conto di essere osservato), e prospettava delle lesioni della riservatezza del dipendente che apparivano nuove e preoccupanti. Non di meno, simili tecniche potevano causare una **pressione psicologica sul lavoratore** che veniva a condizionare direttamente la prestazione lavorativa, e lo privavano, in fin dei conti, di autonomia, ossia non era più libero di poter gestire il tempo lavorativo senza costrizioni.

Il controllo a distanza dopo il Jobs Act

L'evoluzione delle nuove tecnologie e l'avvento di Internet hanno cambiato radicalmente il quadro, ma l'articolo 4 ha, in un certo senso, "resistito" sino a pochi mesi fa. Il nuovo testo dell'art. 4 dello Statuto dei lavoratori, oggi rubricato "Impianti audiovisivi e altri strumenti di controllo" (in precedenza, si noti, era indicato solo "Impianti audiovisivi"), è così strutturato.

> 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".

Si vedranno, in seguito, i **punti essenziali della modifica**. Si noti però sin d'ora il riferimento alla normativa sulla privacy (che, nel corso degli anni, ha disciplinato l'argomento) e l'indicazione degli **strumenti del lavoratore per "rendere" la prestazione lavorativa** e per registrare gli accessi e presenze che sono apparentemente collocati al di fuori dei sistemi di divieto.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Esigenze aziendali e del lavoratore - 13 Febbraio 2016

Controllo sulle opinioni del lavoratore e nuove tecnologie

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

L'articolo 8 dello Statuto dei lavoratori disciplina il potere di controllo del datore di lavoro basato sulle opinioni del soggetto al fine di proteggere la dignità del lavoratore e evitare possibili discriminazioni. L'articolo regola l'equilibrio tra le esigenze dell'azienda di conoscere il più possibile la vita del lavoratore per comprendere se sia idoneo alla mansione attribuita e i dati privati dello stesso; equlibrio che non deve condizionare, al contrario, l'assunzione e il rapporto di lavoro. Si tratta, quindi, di una norma che ha molte sfaccettature e che presenta due piani interpretativi diversi.

Se l'articolo 4, nell'impalcatura dello Statuto dei Lavoratori, si proponeva di disciplinare i possibili controlli a distanza del dipendente da parte del datore di lavoro, scongiurando soprattutto l'ipotesi dei controlli cosiddetti "occulti", un secondo articolo, l'articolo 8, si doveva prendere cura di un altro tipo di possibile controllo, ossia quello basato (e portato) sulle **opinioni del soggetto**.
Il testo era, sul punto, assai chiaro, sia nel titolo dell'articolo ("Divieto di indagini sulle opinioni"), sia nel corpo dell'articolo stesso ("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").
Come per l'articolo 4, anche nell'articolo 8 vennero mantenuti toni abbastanza ampi e generici per includere ulteriori possibili, future modalità di controllo. Il riferimento alle "opinioni" è strettamente connesso al periodo storico di cui stiamo trattando: in quegli anni il sistema di lavoro in fabbrica, la politica, i flussi migratori dei lavoratori dal Sud al Nord stavano completamente cambiando il panorama e stavano disegnando un quadro sociale e giuridico radicalmente nuovo.

Statuto dei Lavoratori e articolo 8

L'articolo 8, in sintesi, era stato domandato, in seno all'assemblea parlamentare, per tenere sotto controllo e considerare illecite alcune "abitudini" che si erano diffuse nel mondo aziendale circa la **raccolta di informazioni sui lavoratori** che stavano per essere assunti, o che già erano stati assunti e magari rivestivano, all'interno della realtà produttiva, posizioni politiche ben definite.
Il controllare la vita personale del lavoratore, anche con informazioni non attinenti alla sua prestazione lavorativa, permetteva di controllare in futuro politicamente la persona stessa.
Tali informazioni erano tipicamente raccolte nella cerchia di conoscenti della persona presa di

mira, spesso utilizzando **investigatori preposti ad hoc**, e confluivano in “schede” o “informative” che erano in grado di tratteggiare, con un ottimo livello di dettaglio, il profilo del lavoratore.
Apparve subito chiaro il potenziale dannoso di una simile raccolta “istituzionalizzata” di informazioni, e le possibilità di condizionamento futuro del lavoratore. Fu quindi deciso di inserire nello Statuto questo articolo che, però, fu criticato da alcune parti perché troppo generico (e, quindi, capace di fornire una tutela limitata) o perché privo di un elenco, in dettaglio, dei quello basato (e portato)

Controllo sulle opinioni del lavoratore

L’articolo disciplina, per così dire, un necessario equilibrio tra le esigenze dell’azienda di conoscere il più possibile la vita del lavoratore per comprendere se lo stesso sia idoneo alla mansione prevista e il lato privato dello stesso, che non deve condizionare, al contrario, l’assunzione e il rapporto di lavoro. Si tratta, quindi, di una norma che ha molte sfaccettature: vuole **evitare discriminazione**, innanzitutto, ma anche cercare una mediazione tra esigenze conoscitive (e informative) e privacy e dignità del lavoratore tentando di “scremare” i dati non necessari.
L’articolo presenta **due piani interpretativi diversi**. Il primo divieto concerne **indagini effettuate ai fini dell’assunzione**, o nel corso dello svolgimento del rapporto di lavoro, anche a mezzo di terzi, che abbiano a oggetto le opinioni politiche, religiose o sindacali del lavoratore. Il riferimento “anche a mezzo di terzi” è un chiaro cenno all’utilizzo, all’epoca, di agenzie, investigatori o “contatti” presso forze dell’ordine o associazioni utilizzati dagli uffici del personale per compilare la scheda (tenuta segreta) del lavoratore. Oggi, nell’era tecnologica, sono amplissime le possibilità, invece, di recuperare simili dati semplicemente consultando fonti aperte in rete. I dati politici, religiosi o sindacali sono quelli che successivamente la normativa sulla privacy ha definito come “sensibili” , ossia dati particolarmente delicati e capaci di condizionare la posizione in società di un soggetto in caso di diffusione indiscriminata o illecita.
Il secondo aspetto, si noterà, è più ampio, nel momento in cui vieta **l’indagine su “fatti non rilevanti** ai fini della valutazione dell’attitudine professionale del lavoratore”. Volutamente il legislatore, parlando di “fatti non rilevanti”, ha incluso ogni aspetto personale o professionale che non sia però correlato alle mansioni svolte e alla sua attitudine professionale nel caso specifico, aprendo al contempo il fianco a possibili dubbi interpretativi.
La giurisprudenza, soprattutto lavoristica, nel corso degli anni si è occupata di diversi problemi generati da questo importante articolo: la legittimità o meno di colloqui di lavoro o test di assunzione non generici ma approfonditi o mirati sul candidato, la legittimità nelle richieste al lavoratore del suo status di “separato” o “divorziato” o dei suoi precedenti penali, la differenza tra “indagine” e “informazione” e altri aspetti potenzialmente discriminatori.

Gli impatti delle nuove tecnologie

Chiaro è che, con l’avvento delle nuove tecnologie, il quadro è profondamente cambiato. Oggi un datore di lavoro può effettuare un’indagine completa su un potenziale dipendente, o su un dipendente attuale, semplicemente consultando **informazioni in rete** e confidando anche sulle informazioni che lo stesso soggetto ha diffuso in precedenza, spesso consapevolmente. La profilazione di un soggetto, anche con riferimento agli aspetti più intimi, è diventata estremamente facile da effettuare, sia da un punto di vista tecnico sia in un’ottica di gratuità (non è quindi più necessario investire grandi risorse), e ciò impone un ripensamento dell’intero sistema.
Si noti, però, che l’articolo 8 è stato “rafforzato”, a far data dalla fine degli anni novanta, dalla normativa sulla protezione dei dati personali che, pur lasciando intatta l’impalcatura dello Statuto dei Lavoratori, ha aggiunto, soprattutto nelle interpretazioni del Garante, nuove tutele, e **nuove linee interpretative**, sempre volte a proteggere la dignità del lavoratore e a evitare possibili discriminazioni.
La Redazione segnala
Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell’ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di

Gli orientamenti della giurisprudenza - 15 Febbraio 2016

Controlli difensivi, tra tutela del patrimonio e verifica dell'attività lavorativa

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

La categoria dei controlli difensivi, come elaborata dalla giurisprudenza della Corte di cassazione, ha consentito per molti versi di superare alcuni limiti posti dall'articolo 4 dello Statuto dei Lavoratori in materia di controlli a distanza del lavoratore in un'ottica di maggior tutela del patrimonio aziendale. Il tema dei controlli difensivi è stato difatti ampiamente dibattuto dalla Suprema Corte anche anni dopo l'entrata in vigore dello Statuto dei Lavoratori. E' un tema complesso per i margini discrezionali in capo al datore di lavoro ai fini della tutela del patrimonio aziendale e della verifica in concreto dell'adempimento della prestazione lavorativa.

La Corte di Cassazione, nel corso degli anni, ha sistematicamente affrontato il problema dei limiti posti dall'articolo 4 dello Statuto dei Lavoratori, sia analizzando singoli aspetti, sia arrivando a elaborare una categoria fondamentale, quella dei **"controlli" difensivi**, che ha per molti versi smussato alcuni punti in un'ottica di maggior tutela del patrimonio aziendale.
I primi problemi che la Suprema Corte ha dovuto affrontare hanno riguardato alcuni termini definitori: come interpretare, in particolare, i concetti di "distanza", di "attività dei lavoratori" e di "apparecchiature di controllo".

Nozione di distanza

Il termine "distanza", per la Cassazione, ricomprende sia la distanza in senso spaziale che la distanza in senso temporale (Cassazione civile, sez. lav., n. 1236 del 18 febbraio 1983), mentre la locuzione "attività dei lavoratori" ricomprende non solo i comportamenti attuativi della prestazione lavorativa, ma ogni comportamento posto in essere nel corso dell'orario di lavoro.

Concetto di attività dei lavoratori e di apparecchiature di controllo

Con la sentenza n. 15892 del 2007 la Cassazione ha poi notato che "il riferimento all'attività lavorativa, oggetto della fattispecie astratta, non riguarda solo le modalità del suo svolgimento, ma anche il quantum della prestazione" e che pertanto anche "il controllo sull'orario di lavoro, risolvendosi in un accertamento circa quantità di lavoro svolto, si inquadra, per ciò stesso, in una tipologia di accertamento pienamente rientrante nella fattispecie prevista dal richiamato art. 4,

comma 2”.
Maggiori problemi sono stati riscontrati con riferimento al concetto di “apparecchiature di controllo”.

Controlli difensivi

Particolarmente interessante però, si diceva, è la categoria dei “controlli difensivi”, che sfugge all’applicazione dell’art. 4 dello Statuto dei Lavoratori.
Con la sentenza n. 4746 del 2002 la Cassazione ha escluso, infatti, l’applicabilità di detto articolo ai **controlli diretti ad accertare condotte illecite del lavoratore**, i c.d. controlli difensivi. Il ragionamento della Corte, in tal senso, è chiaro: “Ai fini dell’operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell’attività dei lavoratori previsto dall’art. 4 l. n. 300 citata, è necessario che il controllo riguardi (direttamente o indirettamente) l’attività lavorativa, mentre devono ritenersi certamente fuori dell’ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate. Nella specie, pertanto, considerato il tipo di lavoro cui era addetto il […], il tribunale avrebbe dovuto valutare il comportamento del datore di lavoro come inteso a controllare la condotta illecita del dipendente e non l'attività lavorativa svolta dal medesimo”.
Successivamente, con la pronuncia n. 15892 del 2007, la Corte ha tuttavia ammesso un limite, affermando che i controlli difensivi non possono giustificare l’annullamento di ogni garanzia: “Né l’insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore”.
La Corte, nella pronuncia sopracitata, arriva così ad affermare che l’art. 4 dello Statuto dei lavoratori e le procedure in esso previste debbano applicarsi anche ai controlli diretti ad accertare i comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l’esatto **adempimento delle obbligazioni discendenti dal rapporto di lavoro** e non la tutela dei beni estranei al rapporto stesso. Si leggano le parole dei giudici in tal senso: “Tale esigenza ” […] “non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l’esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso ove la sorveglianza venga attuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell’Ispettorato del lavoro. Consegue a tale rilievo la necessità, ex art. 4, comma 2, dello Stat. lav., che l’installazione della contestata apparecchiatura sia oggetto di accordo con le r.s.a. o consentita dall’intervento dell’ufficio pubblico, affinché i dipendenti ne possano avere piena conoscenza e possano eventualmente essere stabilite in maniera trasparente misure di tutela della loro dignità e riservatezza”.
Anche se non è semplice tratteggiare il confine tra tutela di beni estranei al rapporto lavorativo ed esatto adempimento degli obblighi derivanti dal rapporto di lavoro, tale principio è stato riaffermato in numerose pronunce successive e, con la sentenza n. 4375 del 2010, è stato applicato anche ai programmi informatici che consentono il **monitoraggio della posta elettronica e degli accessi ad Internet**. La sentenza, dopo aver definito tale tipologia di controllo come “controllo preterintenzionale”, rientrante perciò nell’ambito di applicazione del secondo comma dell’art. 4 dello Statuto dei lavoratori, ha affermato, richiamando la sentenza già espressa dal giudice di merito, quanto segue: “i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l’attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento (se non altro, nel nostro caso, sotto il profilo del rispetto delle direttive aziendali)”.
La giurisprudenza successiva è costante nell’affermare il principio enunciato dalla Cassazione nel 2007. Il problema è che i concetti di base si prestano a differenti interpretazioni, più o meno restrittive, che possono variare sensibilmente a seconda dei casi concreti, Si veda, a titolo di

esempio conclusivo, il senso della pronuncia della Cassazione n. 2722 del 2012: “Nel caso di specie, infatti, il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull’esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere. Il c.d. controllo difensivo, in altre parole, non riguardava l’esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell’Istituto bancario presso i terzi. In questo caso entrava in gioco il **diritto del datore di lavoro di tutelare il proprio patrimonio**, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall’esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale. Tale situazione, ad una lettura attenta, è già esclusa dal campo di applicazione dell'art. 4 dalla sopra citata giurisprudenza (che già esclude dai controlli difensivi vietati quelli aventi ad oggetto la tutela di beni estranei al rapporto di lavoro, v. Cass. n. 15892 del 2007 cit.)”.
Il tema dei controlli difensivi come elaborato dalla Corte di Cassazione anni dopo l’entrata in vigore dello Statuto dei Lavoratori è molto complesso e dibattuto proprio per i **possibili margini discrezionali** in capo al datore di lavoro per poter non solo tutelare il patrimonio aziendale ma anche verificare in concreto l’adempimento della prestazione lavorativa.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell’ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Eccezioni e limiti - 16 Febbraio 2016

Controlli difensivi e “preterintenzionali”: orientamenti giurisprudenziali

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell’Università degli Studi di Milano**

La Corte di Cassazione, con la sua giurisprudenza, ha mutato un po’ gli equilibri consolidati nell’applicazione delle norme dello Statuto dei Lavoratori, prevedendo eccezioni ai divieti di controllo a distanza previsti dall’art. 4. A fronte delle ampie discussioni sollevate dalle decisioni giurisprudenziali, la Cassazione ha cercato di dettagliare con precisione i limiti di tale stato di

eccezione. Inoltre, la Suprema Corte si è espressa in merito ai controlli "automatizzati" per i quali è possibile che il controllo sull'attività del lavoratore sia "preterintenzionale", ossia avvenga anche se non vi è intenzione diretta di chi controlla.

Il tema dei controlli difensivi come elaborati dalla Corte di Cassazione italiana, cui abbiamo fatto cenno nellarticolo precedente, apre a riflessioni interessanti e, soprattutto, permette di "chiudere" un primo percorso di analisi che dovrà poi necessariamente affrontare, a breve, anche la riforma della privacy avvenuta in Italia a fine degli anni Novanta e il nuovo quadro di protezione dei dati personali e sensibili del lavoratore.

La giurisprudenza della Cassazione

Ricapitolando, la giurisprudenza della Cassazione ha mutato un pò gli equilibri che nei primi vent'anni di Statuto dei Lavoratori si erano in qualche modo stabilizzati, prevedendo delle **eccezioni ai divieti di controllo** previsti dall'articolo 4. Ciò ha sollevato ampie discussioni: era come se divieti fatti uscire "dalla porta" rientrassero, in qualche modo, dalla "finestra" prediligendo le esigenze del datore di lavoro e del suo patrimonio aziendale rispetto a quelle del lavoratore e della sua dignità. Non è quindi una sorpresa che la Corte di Cassazione abbia cercato di dettagliare con precisione i limiti di tale stato di eccezione: per impedire delle distorsioni al sistema.

Percorsi interpretativi

La sentenza 4746 del 2002 che abbiamo citato nell'articolo precedente, e che abbiamo già riportato in stralcio, cerca di stabilire dei limiti utilizzando la locuzione "controlli diretti ad accertare condotte illecite del lavoratore". Posto che non è semplice definire il limite della **locuzione "condotte illecite"** (illecite perché contro una norma di legge? Illecite perché percepite illecite dal datore di lavoro?), il sunto della pronuncia è che l'articolo 4, con i suoi divieti, si dovrebbe applicare solamente in presenza di comportamenti leciti e giustificati del lavoratore. In presenza di qualcosa di illecito, ad esempio con riguardo alla presenza (meglio: all'assenza) del lavoratore in azienda, o a telefonate ingiustificate, o simili, i controlli sarebbero ammessi.
È però chiaro come controllare una condotta illecita di un dipendente possa, al contempo, permettere di controllare senza problemi la sua attività lavorativa "in generale", e che l'unico limite risieda nell'etica e nella buona volontà di chi controlla.
Ciò ha portato la Cassazione, nel 2007, a meglio specificare proprio sul punto delle "**garanzie"**, ribadendo che comunque anche un controllo di tale tipo sulle (presunte) attività illecite del lavoratore non dovrebbe annullare tutte le garanzie previste dallo Statuto dei Lavoratori.
In particolare, sono due, secondo la Cassazione, i valori che dovrebbero rimanere inalterati e "sacri" anche in un simile contesto: la "dignità" del lavoratore, e la sua "riservatezza". Per "dignità" s'intende il fatto che nessun tipo di controllo può comunque essere lesivo dei valori connessi alla natura umana e al suo stare in società. Per "riservatezza" ci si concentra invece sulla protezione della sfera intima del lavoratore.
Un terzo percorso interpretativo, dopo i due sopra indicati, la Corte lo ha fatto ragionando sulla differenza tra il "**controllare l'esatto adempimento delle obbligazioni** discendenti dal rapporto di lavoro" e, al contrario, "controllare la tutela dei beni estranei al rapporto di lavoro". Sono locuzioni che appaiono complesse, ma in realtà sono semplici da comprendere. La prima riguarda quei controlli che comunque possono anche permettere di verificare se il lavoratore sta adempiendo in maniera corretta agli obblighi che derivano dal suo rapporto di lavoro. In poche parole: se sta lavorando bene, in orario, in un'ottica di produttività, etc. La seconda invece riguarda quei controlli che hanno come oggetto d'attenzione non tanto l'esatto adempimento da parte del lavoratore del suo contratto, ma dei **beni aziendali** (che vanno tutelati) che sono di proprietà del datore di lavoro e che sono estranei (formalmente) a tale rapporto.
In sintesi, si domanda la Cassazione, si possono separare questi **due tipi di controllo**, o vi è il rischio che un controllo del secondo tipo (sui beni "esterni" al rapporto di lavoro) permetta comunque anche di controllare l'adempimento del rapporto di lavoro e, quindi, di controllare il lavoratore nella sua attività quotidiana?
Per la Cassazione, se il secondo tipo di controlli (controllo dei beni aziendali) coinvolge comunque

il primo aspetto (il controllo del lavoratore), non si può sfuggire dai vincoli che prevedeva il vecchio testo dell'articolo 4 (accordo con le rappresentanze sindacali, divieto di controlli occulti, etc.).

Controlli automatizzati

Vi è un ultimo aspetto, più correlato all'era digitale, che è stato elaborato dalla Cassazione in anni più recenti, attorno al 2010 e che già abbiamo citato nell'articolo precedente. La Corte si è resa conto che alcuni **controlli "automatizzati"** che verifichino, ad esempio, la posta elettronica del dipendente o gli accessi a Internet e a determinati siti web, non consentono di separare i due aspetti cui abbiamo fatto cenno poco sopra, ossia non permettono di dividere il controllo sui dati che riguardano la prestazione lavorativa del "controllato" da quei dati che servono invece unicamente per verificare la tutela del patrimonio e dei beni aziendali.
Come fare, allora, nel caso di questo controllo all'attività del lavoratore che è, per così dire, "preterintenzionale", ossia avviene anche se non è l'intenzione diretta di chi controlla?
Per la Corte è indubbio che questi tipi di controllo, anche se pensati per tutelare il patrimonio dell'azienda, consentono al datore di lavoro di controllare a distanza e in via continuativa il lavoratore e le modalità di svolgimento del suo rapporto con l'azienda. E ricadevano, quindi, anch'esse nell'ambito dei divieti di controllo previsti dal testo dell'articolo 4 pre-riforma.
È quindi indubbio, per la Corte, il diritto del datore di lavoro di tutelare il proprio patrimonio e la propria immagine, ma controlli difensivi finalizzati in tal senso non possono comunque eludere i divieti previsti dallo Statuto dei Lavoratori.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Casistica del Garante privacy

Norme di coordinamento - 18 Febbraio 2016

Garante privacy e linee guida: dignità del lavoratore e divieto di controlli occulti

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di**

Nella disciplina dei controlli a distanza prevista dal Jobs Act assume rilievo, oltre allo Statuto dei Lavoratori e alla giurisprudenza della Corte di Cassazione, anche il Garante privacy. Al trattamento dei dati sui lavoratori effettuato dal datore di lavoro si applicano i principi elaborati in materia di protezione dei dati personali (necessità, correttezza, trasparenza, pertinenza e non eccedenza). Chiara è la volontà del Garante di fornire non solo alcuni criteri di coordinamento tra le norme sulla privacy e le norme statutarie, bensì quella di interpretare la legge sulla privacy in considerazione delle evoluzioni tecnologiche intervenute.

Come si diceva, si è presentato negli anni un terzo "attore" (dopo il redattore dello Statuto dei Lavoratori e la giurisprudenza della Corte di Cassazione sui controlli difensivi) nell'arena della disciplina dei controlli del dipendente, ed è il **Garante per la Protezione dei Dati Personali** che cerca di applicare la recente normativa in tema di privacy.
Ciò comporta la necessità di coordinare anche queste disposizioni, entrate in vigore alla fine degli anni novanta, e non è cosa facile.

Normativa sulla privacy e Statuto dei Lavoratori

Sulla carta, la situazione sembra semplicissima: gli articoli 113 e 114 del Codice Privacy (d.lgs. n. 196 del 2003), rispettivamente rubricati "Raccolta di dati e pertinenza" e "Controllo a distanza", riportano entrambi la seguente dicitura: "Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300".
Sembra quindi che la normativa sulla privacy non tocchi in alcun modo il tema che ci interessa e, anzi, rimandi senza discussione alle norme dello Statuto dei Lavoratori che già abbiamo visto.
Ma non è così semplice: nel corso degli anni, nonostante la normativa sulla privacy non abbia cambiato il testo dello Statuto dei Lavoratori, il Garante per la protezione dei dati personali ha deciso di stabilire alcuni **importanti principi applicabili ai rapporti di lavoro**, al fine di attuare un coordinamento tra le suddette norme. Tramite diverse decisioni, linee guida e suggerimenti, il Garante ha cercato spesso di adeguare il nuovo quadro portato dall'innovazione tecnologica a un framework giuridico più datato.

Linee guida sull'utilizzo della posta elettronica e di internet

Di particolare rilevanza, per il tema che ci riguarda, sono le Linee guida sull'utilizzo della posta elettronica e di internet del 2007.
Queste linee guida rappresentano una vera e propria svolta, e testimoniano un nuovo atteggiamento del Garante nell'intendere il coordinamento fra le regole generali in materia di privacy e la disciplina gius-lavoristica.
Nelle premesse al documento, è il Garante stesso a evidenziare le ragioni di tale intervento. In particolare, evidenzia cinque esigenze chiare.
La prima è la necessità di riconoscere il fatto che competa ai datori di lavoro assicurare la funzionalità e il **corretto impiego dei mezzi elettronici**, soprattutto posta elettronica e accesso a Internet, da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali.
Un secondo aspetto, nota il Garante, è che spetta sempre ai datori di lavoro **adottare idonee misure di sicurezza** per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità.
Un terzo punto è l'emergenza di un'esigenza di tutela dei lavoratori interessati anche perché l'utilizzazione dei **mezzi tecnologici**, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa.
In quarta battuta, l'utilizzo di Internet da parte dei lavoratori, avverte il Garante, può diventare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della

corrispondenza.
Infine, le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Nuovo ruolo del Garante privacy

Tanto premesso, il quadro normativo relativo alla privacy prevede che si applichino, al trattamento dei dati sui lavoratori effettuato dal datore di lavoro, i principi elaborati in materia di protezione dei dati personali (necessità, correttezza, trasparenza, pertinenza e non eccedenza), nonché l'apposizione di un limite alla possibilità di effettuare tale trattamento, individuabile nell'art. 4 dello Statuto.
Sembra chiara, in tal senso, la volontà del Garante di fornire non solo alcuni criteri di coordinamento tra le norme sulla privacy e le norme statutarie, bensì quella di **interpretare la legge sulla privacy** alla luce dell'art. 4 dello Statuto dei lavoratori, come applicabile in considerazione delle evoluzioni tecnologiche intervenute e dei principi e della legislazione sviluppatasi in materia di trattamento di dati personali.
Così ragionando il Garante giunge, quindi, alla considerazione che, ove l'impiego di apparecchiature volte a realizzare un controllo a distanza sia vietato dall'art. 4 dello Statuto, allora, l'acquisizione di dati personali nell'ambito di tali condotte vietate non può che costituire un trattamento illecito ai sensi della disciplina sulla privacy.
Si tratta di un'impostazione che comporta l'**assunzionedi un nuovo ruolo da parte del Garante**, necessario al fine di coordinare tali norme e reinterpretarle alla luce delle innovazioni tecnologiche intervenute, supplendo così all'inerzia del legislatore.
La Redazione segnala
Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Posta elettronica e traffico web - 20 Febbraio 2016

Garante privacy: dalle linee guida limiti ai controlli del datore di lavoro

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

Le linee guida del Garante privacy sull'utilizzo della posta elettronica e di internet contengono

prescrizioni dettagliate sulla “cattura” di tutte le comunicazioni in entrata e in uscita che riguardino il lavoratore, con particolare riferimento ai messaggi di posta elettronica e al traffico web. L’art. 5 delle linee guida è, invece, dedicato ai programmi che consentono controlli “indiretti”, ossia il controllo preterintenzionale. Infine, in ossequio al principio di trasparenza, un vero e proprio caposaldo in materia di trattamento dei dati personali è la previsione di procedure di informazione con l’adozione di un disciplinare interno.

Accanto a dichiarazioni ampie che stabiliscono, genericamente, l’applicabilità dei principi della legge sulla privacy anche all’ambito lavoristico, nelle linee guida del Garante sono contenuti anche alcuni punti specifici molto interessanti legati all’utilizzo di sofisticati sistemi elettronici per controllare il datore di lavoro.

Controlli diretti

Le prescrizioni dettagliate contenute nel documento citato comprendono molti ambiti.
Uno di particolare interesse, ad esempio, riguarda il divieto di trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire – a volte anche minuziosamente – l’attività di lavoratori.
Il Garante si riferisce, in questo caso **a quattro “interventi tecnologici”** del lavoratore ben precisi:
1) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
2) la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
3) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
4) l’analisi occulta di computer portatili affidati in uso.
Il primo punto riguarda la cosiddetta “cattura a strascico” di tutte le comunicazioni in entrata e in uscita che riguardino il lavoratore, con particolare riferimento ai **messaggi di posta elettronica** sia nei loro contenuti sia nei loro dati esterni (mittente, destinatario, data); se tale “cattura” del traffico è effettuata al di là delle mere esigenze tecniche che la gestione di un sistema/server di posta elettronica richiede, si è in ambito di trattamento illecito dei dati.
Il secondo esempio concerne la cattura del **traffico web**, ossia il tenere traccia non solo dei siti web cui il lavoratore si collega in orario lavorativo ma, anche, di una copia stessa delle pagine.
Il terzo caso coinvolge ogni attività effettuata dai cosiddetti **keyloggers**, ossia programmi che surrettiziamente registrano ogni pressione della tastiera e la spediscono a un destinatario ben preciso (in questo caso: il datore di lavoro). In sintesi, il keylogging permette non solo di carpire password e codici ma anche di “registrare”, ad esempio, intere conversazioni in chat.
Il quarto punto riguarda infine l’inserimento di “microspie” all’interno dei computer portatili affidati in uso al dipendente, microspie che consentano un controllo occulto di tutte le attività, di ogni tipo.

Controlli “indiretti”

L’art. 5 delle Linee Guida è invece dedicato ai programmi che consentono controlli “indiretti”, ossia il c.d. **controllo preterintenzionale**. Anche tale tipologia di controllo determina un trattamento dei dati personali riferiti o riferibili ai lavoratori ed è lecito soltanto se legittimamente attuato ai sensi dello Statuto dei lavoratori.
Su questo punto il Garante è molto chiaro, stabilendo che il trattamento di dati che consegue a un simile approccio tecnologico può risultare lecito, ma rimane comunque ferma la necessità di rispettare le **procedure di informazione e di consultazione di lavoratori** e sindacati in relazione all’introduzione o alla modifica di sistemi automatizzati per la raccolta e l’utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.
Un ulteriore divieto stabilito dalle Linee Guida coinvolge quei datori di lavoro privati e pubblici che cercano di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori, un aspetto che il Garante ritiene particolarmente pericoloso e delicato.

Informazione e disciplinare interno

Infine, un aspetto di fondamentale importanza nelle previsioni contenute nelle Linee Guida, in ossequio al principio di trasparenza, un vero e proprio caposaldo in materia di trattamento dei dati personali, è la previsione di procedure di informazione, per cui il datore di lavoro deve specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli.

Il Garante consiglia l'adozione di un **disciplinare interno** redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro) e da sottoporre ad aggiornamento periodico.

Anche in questo caso, il Garante si premura di fornire dettagliate esemplificazioni di cosa andrebbe specificato nel disciplinare, e in particolare sarebbe opportuno indicare:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il download di software o di file musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per **ragioni personali servizi di posta elettronica o di rete**, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
- se, e in quale misura, il datore di lavoro si riserva di effettuare **controlli in conformità alla legge**, anche saltuari o occasionali, indicando le ragioni legittime –specifiche e non generiche– per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili **modalità di uso personale** di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare le regole 4, 9, 10).

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.

Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.

Scopri la promozione riservata ai professionisti Wolters Kluwer!

Policies e misure a tutela - 22 Febbraio 2016

Protezione dati personali dei lavoratori: limiti dei controlli datoriali dalla UE

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

Sulla protezione dei dati personali dei lavoratori in ambito europeo manca uno specifico intervento normativo. Vi sono però alcuni provvedimenti che indirettamente si occupano del tema. Tra questi la "Raccomandazione in materia di trattamento dei dati personali in ambito lavorativo", elaborata nelle more dell'attuazione del Jobs Act. In tale documento il Consiglio d'Europa ha previsto l'applicazione dei principi stabiliti in materia di tutela dei dati personali anche ai dati del lavoratore trattati dal datore di lavoro, definendo criteri sull'utilizzo di Internet e delle comunicazioni elettroniche.

Per concludere la disamina delle questioni relative alla privacy dei lavoratori e ai limiti dei controlli del datore di lavoro sulla loro attività, è opportuno dare uno sguardo alla **situazione normativa europea** che se, da un lato, non si presenta ancora omogenea, presenta però, dall'altro, alcuni spunti di riflessione molto interessanti.

Quadro normativo europeo

Per onestà intellettuale bisogna subito dire che, nella normativa europea, non è vi è ancora uno specifico intervento concernente la protezione dei dati personali dei lavoratori, ma vi sono alcuni provvedimenti che indirettamente si occupano del tema.
Già nel lontano (tecnologicamente) 1997 la Commissione sfiorò la questione che ci interessa con una comunicazione denominata "The Social and Labour Market Dimension of the Information Society; People First–Next Steps" nel testo della quale si ribadiva la completa applicabilità delle direttive in materia di protezione dei dati personali ai rapporti di lavoro e si ventilava l'ipotesi di una **procedura di consultazione** per valutare le future azioni da intraprendere in materia di protezione dei dati personali dei lavoratori. Il principio di base per cui la normativa sulla privacy si sarebbe applicata anche ai rapporti di lavoro metteva un punto fermo e importante su un approccio che era in linea con quello che già stavano adottando i singoli Stati. Al termine della prima consultazione prevista dalla Comunicazione, la Commissione ne programmò una seconda nel 2004 ma, nonostante i numerosi meeting organizzati e gli studi realizzati dal Gruppo di lavoro per l'articolo 29, nonché i contributi provenienti da esperti della materia, non riuscì a raggiungere lo scopo che si era prefissata, ossia l'adozione di una normativa da applicarsi uniformemente in materia di protezione dei dati personali dei lavoratori.

La Raccomandazione UE sulla privacy in ambito lavorativo

Anche il Consiglio d'Europa, parallelamente, ha affrontato la materia, emanando alcune raccomandazioni tra le quali una molto recente, dell'aprile 2015 ("Raccomandazione in materia di trattamento dei dati personali in ambito lavorativo"), elaborata proprio nelle more dell'attuazione della legge delega per il riordino dei rapporti di lavoro (il cosiddetto Jobs Act 2 italiano).
In detto documento il Consiglio d'Europa ha previsto l'applicazione dei principi stabiliti in materia di tutela dei dati personali anche ai dati del lavoratore trattati dal datore di lavoro. In particolare, si

ribadisce che i datori di lavori dovrebbero ridurre al minimo il trattamento di dati personali dei lavoratori e trattare soltanto quei **dati strettamente necessari** a raggiungere i fini perseguiti in ogni caso individuale. Al contempo, si chiede ai datori di lavoro di sviluppare appropriate misure di sicurezza che assicurino il rispetto dei principi alla base della protezione dei dati e che siano proporzionare al tipo, al volume e alla natura dei dati trattati, al tipo di attività che sono condotte e che garantiscano in ogni momento la protezione dei diritti fondamentali dei lavoratori e la loro dignità e libertà.

In particolare, per quanto riguarda l'**utilizzodi Internet e delle comunicazioni elettroniche**, l'articolo 14 di questo documento prevede alcuni punti molto interessanti.

In primis, è fatto divieto al datore di lavoro di attuare ingiustificate e irragionevoli interferenze nella vita privata del lavoratore. Il lavoratore, poi, deve sempre essere adeguatamente e periodicamente informato dei controlli che subisce o che può subire, mediante l'utilizzo di privacy policy e di regolamenti ad hoc.

Le informazioni fornite mediante le **privacy policies** devono essere costantemente aggiornate e devono indicare la finalità del trattamento (a che fini i dati sono trattati), la conservazione o il periodo di back-up dei dati sul traffico (data retention) e le modalità con cui avviene l'archiviazione delle comunicazioni elettroniche professionali.

Se si è in presenza di trattamento di dati personali relativi a pagine Internet o Intranet accessibili dal dipendente, si chiede di privilegiare l'adozione di **misure preventive**, quali l'uso di filtri che impediscano particolari operazioni e, nel caso in cui sia possibile il monitoraggio di dati personali, occorre preferire un controllo casuale e a campione, e non individuale, mediante l'acquisizione di dati aggregati in forma anonima. Si vuole impedire, in sintesi, che sia allestito un sistema di controllo della navigazione sul web dei dipendenti.

L'accesso alle comunicazioni elettroniche dei dipendenti può poi essere effettuato solo se necessario, solo per motivi legittimi e solamente se i dipendenti sono stati informati preventivamente dell'esistenza di tale tipologia di controllo. Anche in questo caso, come si vede, il legislatore non vede di buon grado i **controlli occulti** su un aspetto così delicato della vita privata delle persone quali sono le loro comunicazioni.

In caso di lavoratori assenti, il documento stabilisce il principio per cui è possibile l'accesso alle comunicazioni elettroniche, per finalità esclusivamente professionali, mediante la preventiva predisposizione di procedure appropriate.

Il contenuto, invio e la ricezione di comunicazioni elettroniche private sul lavoro non deve essere monitorata in nessun caso, e in caso di allontanamento di un dipendente, il datore di lavoro deve adottare le necessarie misure organizzative e tecniche per **disattivare automaticamente il suo account di posta elettronica**. Qualora il datore di lavoro abbia bisogno di recuperare il contenuto di un account di un dipendente per fini organizzativi, deve farlo prima della sua partenza e, quando possibile, in sua presenza.

Tali indicazioni, sebbene non prescrittive, nonché poco dettagliate rispetto a quanto già in più occasioni affermato dal Garante per la protezione dei dati personali, essendo state emanate proprio nel corso del procedimento di modifica dell'art. 4 dello Statuto dei lavoratori non potevano che animare ulteriormente il dibattito tra le istituzioni e le parti sociali, contribuendo alla discussione già originatasi. E hanno meglio dettagliato il quadro che porterà, vedremo, alla riforma italiana dell'articolo 4.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.

Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.

Scopri la promozione riservata ai professionisti Wolters Kluwer!

Nel rispetto dei principi fondamentali - 24 Febbraio 2016

Controlli a distanza: il delicato rapporto tra privacy e Jobs Act

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

La riforma dei controlli a distanza contenuta nel Jobs Act va valutata anche alla luce del delicato rapporto con la normativa a tutela della privacy, che fissa limiti ben precisi anche sul controllo dei dati dei lavoratori. I principi di necessità del trattamento, correttezza, pertinenza e non eccedenza, il divieto di profilazione, la necessaria legittimazione soggettiva al trattamento continueranno a costituire, pur in presenza delle norme del Jobs Act, i principi in base ai quali operare il bilanciamento tra tutela del lavoratore e legittime esigenze datoriali.

Uno degli aspetti più interessanti della nuova riforma portata dal Jobs Act è il delicato rapporto che si è venuto a creare con la normativa a tutela della privacy che, naturalmente, protegge anche la privacy del lavoratore da ingerenze indebite da parte del datore di lavoro.
Mentre la categoria dei "**controlli difensivi**", si è visto, è stata lentamente elaborata dalla giurisprudenza della Corte di Cassazione sino a venire per così dire "incorporata" nel nuovo testo dell'articolo 4, la privacy ha avuto, nell'ordinamento italiano, vita a sé sin dal 1996 e ha creato un quadro molto complesso ma, anche, molto completo.

Parere del Garante privacy

Non appena si è ventilata l'ipotesi di modifica dell'articolo 4, il Garante per la protezione dei dati italiano ha presentato una memoria molto dettagliata al Senato nella quale faceva il punto su diversi problemi interpretativi che sarebbero sorti ma, soprattutto, su alcuni punti che a suo avviso erano "non negoziabili" e su alcuni **diritti irrinunciabili**.
Il Garante è da un lato preoccupato per le modifiche ma, dall'altro, è ben deciso a ribadire i limiti che la legge sulla privacy comunque impone sul punto del controllo dei dati altrui, compresi quelli dei lavoratori. E pur ammettendo una necessità di "modernizzazione" della norma, vede, come ovvio, l'articolo 4 dello Statuto come un "fondamentale **presidio di libertà del lavoratore** rispetto al rischio di una sua totale espropriazione, magari anche con il consenso (inevitabilmente coartato) dell'interessato, in posizione troppo debole per opporvisi."

Rispetto dei principi fondamentali

La parte più interessante della memoria, che ci fa ben comprendere l'approccio del Garante al tema, è quella dove si stabilisce che, comunque, i principi fondamentali stabiliti in materia di protezione dei dati personali rimangono in ogni caso applicabili.
Si riferisce, in particolare, ai **principi di legittimità e determinatezza** del fine perseguito con il trattamento ed i principi di proporzionalità, correttezza e non eccedenza.
Sebbene la violazione di tali principi non comporti una responsabilità penale, nota il Garante, la violazione della disciplina sulla privacy comporterebbe l'**inutilizzabilitàdei dati raccolti**. Ad ogni

modo, il Garante suggerisce una riflessione sull'opportunità di estendere la sanzione penale o di codificarne una autonoma per tale fattispecie.
La memoria del Garante chiarisce, inoltre, alcuni aspetti in relazione all'informativa da fornire al lavoratore, richiamando i principi già affermati negli anni, ed affermando che, essendo il requisito della preventiva informazione del lavoratore un principio già desumibile dalla normativa sulla protezione dei dati personali, il Codice privacy costituirà un limite all'utilizzo di controlli occulti.
Più in generale, le norme del codice continueranno a regolare la materia, individuando un limite alle attività che il datore di lavoro può porre in essere.
I principi di necessità del trattamento, correttezza, pertinenza e non eccedenza, il **divieto di profilazione**, la necessaria legittimazione soggettiva al trattamento ed il rinvio di cui all'art. 113, che hanno consentito al Garante di valutare le **modalità di controllo** attuate dai datori di lavoro, continueranno a costituire i principi in base ai quali operare "un congruo bilanciamento tra tutela del lavoratore e legittime esigenze datoriali".

Considerazioni conclusive

Come si vedrà, il testo definitivo dell'articolo 4 non ha recepito le preoccupazioni e le osservazioni del Garante, ma l'esistenza di tali principi in materia di protezione dei dati personali forniscono indubbiamente una forte garanzia a procedure di controllo occulto o indiscriminato o, comunque, in violazione delle regole. Anche se la tutela della privacy persegue finalità differenti dalla normativa lavoristica, l'attenzione alla dignità e alla non discriminazione dei lavoratori unisce chiaramente le due aree e i due ambiti.
Si può così affermare che il **principio di necessità del trattamento** obbligherà i datori di lavoro a trattare solamente i dati realmente necessari a raggiungere un determinato fine; il **principio di correttezza** impone una sorta di "etica" nella raccolta dei dati e del suo utilizzo; il **principio di pertinenza** e di non eccedenza stabilisce la necessità che non siano raccolti più dati di quelli realmente utili e che i dati raccolti siano strettamente correlati al fine che ci si propone di raggiungere e non ad altri fini; il **divieto di profilazione** impone, infine, che i dati non siano raccolti, in realtà, per creare schede di comportamento dei lavoratori al fine di condizionarli in qualche modo o di discriminarli.
Questa presenza "costante" della normativa in tema di protezione dei dati personali (che continua ad avere vita a sé) anche in fase di riforma delle norme lavoristiche è molto interessante e, soprattutto, costituisce un presidio certo a tutela dei diritti. Sarà quindi molto utile seguire l'evoluzione e analizzare come si paleseranno eventuali "interferenze" tra i due ambiti.
La Redazione segnala
Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Strumenti operativi

Limiti e regole - 26 Febbraio 2016

Uso degli strumenti da parte dei dipendenti: tecniche per la redazione di una policy

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

In materia di controlli a distanza post Jobs Act assumono importanza i regolamenti o policy di sicurezza interni al luogo di lavoro. Tali regolamenti contengono, in particolare, le regole sui limiti di utilizzo del computer aziendale e della posta elettronica, sui dati scaricabili dalla rete e sui siti che si possono visitare. L'approccio migliore nella redazione di una policy è muovere da due aspetti: le criticità generiche, cercando di prevedere i comportamenti sbagliati del dipendente, e le criticità manifeste, ossia usare la policy per regolamentare comportamenti errati che già si sono manifestati.

Nel nuovo quadro disegnato dal Jobs Act avranno sempre maggiore importanza i cosiddetti **regolamenti o policy di sicurezza** interni al luogo di lavoro. Non soltanto le "informative" o policy che spieghino i sistemi elettronici di controllo e di sorveglianza ma, in generale, tutti quei regolamenti che cerchino di prevenire un uso non corretto dello strumento elettronico che possa portare a responsabilità penali o disciplinari.

Nozione di policy di sicurezza interna

Per policy di sicurezza interna a un luogo di lavoro (può essere un'azienda, uno studio professionale, un laboratorio universitario, una biblioteca) s'intende un insieme di regole, più o meno articolato, che dia **informazioni e obblighi** su come usare al meglio le tecnologie al fine di garantire un ambiente sicuro.
Tali regole coprono, di solito, non solo una descrizione dei controlli effettuati (se a campione o mirati, se sui server o sui computer dei dipendenti, se costanti od occasionali), ma anche le basi della sicurezza informatica, con norme di comportamento e di buona condotta, cenni di netiquette e suggerimenti di abitudini che possono migliorare l'attività informatica.

Come redigere un disciplinare

Nella redazione di un simile disciplinare, tipiche sono le regole che riguardano i **limiti di utilizzo** del computer aziendale, della posta elettronica, cosa si può scaricare dalla rete, le regole d'invio di materiale a colleghi, i siti che si possono visitare, il limite di banda che si può impiegare, dove salvare i documenti, come non influenzare o intaccare spazi altrui, l'hardware che si può portare in azienda dall'esterno, i privilegi e il software che si può installare o meno, e così via.
L'approccio migliore nella redazione di una policy che affronti sia i temi del controllo del dipendente sia, in generale, che voglia risolvere i problemi di sicurezza informatica dell'ambiente di lavoro, è muovere da due aspetti: le **criticità generiche**, cercando di prevedere i comportamenti sbagliati del dipendente, e le c**riticità manifeste**, ossia usare la policy per regolamentare comportamenti errati che già si sono manifestati.

Esempio di policy

Prendendo come dominio d'attenzione una tipica **azienda medio piccola**, una policy ipotetica dovrebbe occuparsi dei seguenti aspetti:

1) il computer concesso al dipendente/collaboratore e il suo software (uso consentito, strumenti di controllo installati dal datore di lavoro sul sistema, esempi di uso tipico corretto);
2) eventuali computer esterni fatti entrare nella rete (ammissibilità o meno, parametri di sicurezza richiesti);
3) l'uso di tablet, cellulari e smartphone forniti dal datore di lavoro (suggerimento di utilizzo corretto, comunicazione se su tali strumenti sono inseriti sistemi di controllo);
4) l'indirizzo di posta elettronica lavorativo e l'uso d'indirizzi privati (limiti nell'utilizzo della e-mail aziendale, possibilità di usare un indirizzo "personale" non controllato dal datore di lavoro);
5) la connessione al web e alla rete dell'azienda (come risparmiare le risorse complessive, che comportamenti tenere per non "affaticare" la rete);
6) la gestione dei documenti, salvataggio e sicurezza, condivisione e profili di visibilità degli stessi, lavoro cooperativo e revisioni;
7) la spendita del nome dell'azienda in rete e in contesti pubblici come i social network, i forum di discussione, i blog;
8) la sicurezza generale della rete e del sistema e l'attenzione a virus, accessi dall'esterno, leaks.
Il primo punto riguarda l'ingresso del dipendente nella nuova realtà e la **concessione di un computer**, fisso o portatile che sia. Occorre, quindi, stabilire un insieme di limiti e di modalità corrette di utilizzo, nonché i privilegi per l'installazione di software, che potrebbe mettere a rischio, vedremo, anche un altro aspetto. Le **modalità temporali di utilizzo**, nel caso il computer sia condiviso con un'altra persona e la manutenzione e l'uso del computer stesso, soprattutto se è un computer portatile sono due punti essenziali, così come l'attenzione al lato fisico, la cura del computer in sé, e al lato logico, ossia i programmi che devono essere presenti in tale computer, un aspetto che pone non solo problemi legali ma anche problemi di sicurezza.
I programmi dovrebbero essere forniti dallo studio e non essere scaricati da Internet, anche perché dovrebbero essere i più aggiornati, e si dovrebbe comunque lasciare poco margine in capo al dipendente nella modifica dell'ambiente di lavoro. I software dovrebbero essere strettamente correlati all'attività professionale, quindi sistema operativo aggiornato, programmi di videoscrittura, gestionali aziendali, eventuali client per cloud, client di posta elettronica certificata, strumenti per la connessione a Internet e per la connessione a banche dati e strumenti di sicurezza quali antivirus, firewall, crittografia, videoconferenza. Il tenere il computer pulito da numerosi software inutili aumenta la sicurezza da potenziali vulnerabilità.
In questo primo punto, a nostro avviso, si potrebbero inserire anche le "informative" richieste dal nuovo articolo 4 dello Statuto dei Lavoratori, ossia dare un'informazione esaustiva e corretta (anche con dettagli tecnici) al dipendente su quali tipi di controllo automatizzato vengono effettuati su quel computer che gli viene consegnato. Ciò permette già di far sì che tali controlli non siano occulti.
Il secondo punto riguarda l'ingresso di un computer esterno nella **rete aziendale**, tipicamente un portatile di proprietà del dipendente. Si tratta di un fattore di rischio molto alto che va scongiurato accertandosi, prima, che il livello di sicurezza del software contenuto in quel portatile sia almeno allo stesso livello di quello dello studio. Lo scopo è quello di non introdurre un anello della catena debole che possa servire da testa di ponte per attaccare altri computer.
Per quanto riguarda il terzo punto, i **tablet, smartphone e cellulari** forniti dall'azienda sono altrettanto delicati perché permettono, di solito, di controllare, giustamente, la posta professionale, di dialogare con il gestionale o di scansionare documenti. Presentano, quindi, due **livelli vulnerabilità**: la facilità di smarrimento e il contenuto, fatto di dati sensibili. In questo caso occorrerà valutare la cifratura dei dati, unico modo per proteggersi, e fornire delle regole di buon senso nell'utilizzo degli stessi. Anche in questo caso, opportuno è comunicare al dipendente se tali dispositivi sono soggetti a qualche forma di controllo automatizzato o se sono forniti al dipendente con al interno programmi o app che permettano forme di controllo sulle attività svolte.
Il quarto punto riguarda l'uso corretto della **posta elettronica aziendale**, della eventuale posta elettronica certificata e di eventualmente un indirizzo di posta privata. Importante è una distinzione costante tra la e-mail privata e quella aziendale e evitare di confondere le due. In questa parte della policy è opportuno anche dare istruzioni sui toni delle discussioni e sulla gestione degli allegati, nonché specificare ulteriormente se il datore di lavoro ha installato strumenti di controllo

automatizzato della posta.
Il quinto punto riguarda la **connessione al web dalla rete aziendale**. In tal caso sarebbe opportuno che alcuni filtri fossero già impostati, non tanto per impedire il collegamento ad alcuni siti web ma per sicurezza e per evitare la diffusione di spyware o virus. La connessione a siti correlati solo all'attività aziendale e il divieto di scaricare programmi da Internet sono già due regole che, se rispettate, aumentano sensibilmente il livello di sicurezza. Opportuno è indicare, sempre ai sensi della disciplina lavoristica, se viene controllata la navigazione dei dipendenti e come.
Il sesto punto è puramente organizzativo ma con aspetti di sicurezza, e riguarda la gestione dei **documenti all'interno dell'azienda** e del loro flusso. Il formato, il luogo dove sono salvati, che permette un reperimento in caso di assenza, l'ordine e la comprensione dal titolo e dalla cartella, la scansione, la visibilità e le autorizzazioni per accedere, le modalità di lavoro cooperativo e di revisione che siano efficienti ma che non causino perdite di dati o di versioni precedenti.
Il punto successivo è una questione d'immagine telematica, ossia la spendita del nome dell'azienda in contesti pubblici quali **social network e forum**. Occorre stabilire delle regole perché tale cosa può creare non pochi problemi di reputazione o immagine verso l'esterno.
L'ultimo punto riguarda la rete, la **sicurezza**, i leaks, l'accesso dall'esterno ma, molto più spesso, i problemi che sorgono dall'interno e che possono mettere a rischio il sistema. I virus, il backup, l'eliminazione dei dati cartacei e informatici, ma anche l'ingresso in azienda di dispositivi esterni, un controllo costante delle stampe e dei log di salvataggio per individuare comportamenti sospetti sono strumenti essenziali nelle realtà aziendali complessi.
La modifica dell'articolo 4 con i nuovi obblighi di informare il dipendente circa le attività di controllo non cambierà sostanzialmente l'approccio tipico alle policy ma richiederà semplicemente un maggior dettaglio, in ogni punto, di quel singolo aspetto.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Tracciabilità dei dati - 27 Febbraio 2016

Il licenziamento del lavoratore a seguito di attività svolte su Facebook

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

La giurisprudenza degli ultimi anni si è pronunciata molto spesso in merito agli effetti sul rapporto di lavoro di dichiarazioni e informazioni pubblicate su social network da dipendenti sia di aziende private, sia di enti pubblici. L'analisi dei casi giurisprudenziali evidenzia come, oggi, sia possibile, grazie alla tecnologia esistente, tracciare ogni dato e come, per il diritto, la pubblicazione di frasi, commenti o foto su facebook abbia un potenziale diffamatorio elevatissimo con l'avvio di procedimenti disciplinari che, nei casi più gravi, possono portare fino al licenziamento.

Numerosi casi giurisprudenziali, negli ultimi anni, hanno riguardato dipendenti – sia di aziende private, sia di enti pubblici – che hanno subito sanzioni disciplinari, sino al licenziamento, a seguito di dichiarazioni pubblicate sui loro profili Facebook o a seguito di fatti (ad esempio: assenza dal posto di lavoro) cui si è potuto risalire tramite le informazioni che loro stessi hanno pubblicato sui social network.
I punti interessanti che si possono evidenziare analizzando con cura tali sentenze sono numerosi.

Tracciabilità dei dati

Il primo, molto chiaro, è che ogni attività su Facebook del dipendente può essere tracciata sia dall'interno (ossia analizzando il traffico della rete aziendale nel caso il dipendente abbia aggiornato la sua pagina in orario lavorativo e con strumenti aziendali, o si sia collegato a siti "strani" dal computer dell'azienda), sia dall'esterno (grazie a perizie tecniche mirate) per comprendere, ad esempio, se sia stato veramente lui a scrivere determinate frasi.
Ciò comporta che l'accuratezza tecnologica odierna non possa più consentire al dipendente frasi del tipo "non sono stato io a scrivere quella frase ingiuriosa", o "qualcuno ha avuto accesso al profilo Facebook a mia insaputa". Oggi le tecnologie permettono di imputare con precisione i fatti a una persona determinata nonostante la "scusa" più tipica, in questi casi, sia proprio quella di declinare le proprie responsabilità.

Pubblicazione di dati: rilevanza disciplinare

Un secondo punto è la mancata comprensione, spesso, che non vi è distinzione, su Facebook, tra "pubblico" e "privato", ossia che ogni **frase o commento pubblicata sul social network** può arrivare senza problemi all'attenzione del datore di lavoro anche se, nell'idea del dipendente, è pubblicata in un suo "spazio privato", sulla "sua bacheca personale" o, comunque, è vista come un semplice commento tra amici.
L'idea che i social network e la "bacheca" siano "nostre", ossia siano uno spazio completamente privato, è assolutamente sbagliata. La pubblicità di ogni informazione che circola su Internet porta, al contrario, ad amplificare ogni affermazione e ogni commento, sino a causare una maggiore vulnerabilità e, in alcuni casi, una vera e propria diffamazione su larga scala. È quasi impossibile, a meno che l'autore non voglia veramente ciò, che un'informazione resti, su un social network, riservata o in un ambito amicale.
Nelle sentenze più recenti, i fatti che il giudice si è trovato a dover decidere sono spesso molto simili tra loro. Un dipendente viene accusato di aver pubblicato su Facebook, solitamente dal posto di lavoro o da casa, delle **frasi ingiuriose nei confronti del datore di lavoro**, dell'azienda o dei colleghi.
All'atto della contestazione dei fatti cerca di sostenere di non essere stato lui (con affermazioni del tipo: "è stato un hacker!", o "è stato un collega che aveva la disponibilità del mio computer") o di non aver valutato la portata di ciò che ha pubblicato ("credevo che rimanesse nella cerchia dei miei amici").
L'istruttoria, in queste cause, è di solito molto precisa anche da un punto di vista tecnico, per cui si riesce a ricostruire con precisione chi e quando ha pubblicato determinate informazioni, e la conclusione è di solito il licenziamento.
Un'ordinanza del 1 agosto 2014 del Tribunale di Milano, sezione lavoro, ha deciso sull'impugnazione, da parte di un lavoratore, di un **licenziamento per giusta causa** che gli era stato comminato proprio per attività svolte su Facebook, rigettando il suo ricorso.
La questione era nata da tre fotografie pubblicate sul profilo pubblico del dipendente su Facebook

che erano state scattate all'interno dei locali di una unità produttiva dell'azienda e che presentavano dei messaggi accompagnatori offensivi nei confronti del datore di lavoro. Le foto, inoltre, risultavano chiaramente postate in giorno e orario lavorativo.
Accanto a questo primo comportamento, i tecnici dell'azienda hanno rilevato che dal personal computer aziendale del dipendente erano stati effettuati vari accessi a siti Internet del tutto estranei all'attività lavorativa e, in particolare, dal contenuto pornografico: il datore di lavoro ha allegato, a fini probatori, un elenco accurato di questi siti, con nome, indirizzo e periodo di collegamento.
Per il datore di lavoro sono stati violati i **principi di diligenza, correttezza e buona fede,** oltre ad essere stata lesa l'immagine aziendale e ad avere acceduto a siti non afferenti le mansioni in orario lavorativo. Dal canto suo il dipendente, in prima battuta, si è giustificato denunciando l'intrusione di una persona che sarebbe entrata nel suo profilo violando la sua privacy, cambiando arbitrariamente il testo dei commenti e trasformando alcune foto private in foto pubbliche, per poi cambiare versione e ammettere le sue responsabilità.
In questa vicenda è stata interessante l'accuratezza tecnica con cui il datore di lavoro ha ricostruito le attività del dipendente, riuscendo a ripercorrere nel dettaglio tutte le attività svolte dal computer dell'azienda.
Una seconda ordinanza del tribunale di Ivrea, n. 1008 del 2014, ha affrontato un caso simile, con esiti identici. Il dipendente aveva chiamato in giudizio il datore di lavoro perché sosteneva di essere stato licenziato ingiustamente dopo che aveva postato su Facebook delle frasi ingiuriose nei confronti del datore di lavoro e delle colleghe.
In tal caso, le frasi apparse sul suo profilo avevano avviato un **procedimento disciplinare** nei suoi confronti che si era concluso con il suo licenziamento, provvedimento che il lavoratore reputava troppo grave.
Il giudice di Ivrea, sul punto, denota una mancata percezione, in capo al lavoratore, della gravità del suo comportamento, nonché al contempo una volontà di ledere l'altrui reputazione nel modo più ampio possibile non rimuovendo il post ma lasciandolo online fino a quando non vi è stata una diffida esplicita a rimuoverlo.

Considerazioni conclusive

Questi due casi, simili a tanti altri, rendono chiaro come, oggi, sia possibile, grazie alla tecnologia esistente, individuare con precisione ogni "singolo passo" che possa portare a un determinato fatto elettronico e sia quindi molto complesso, al contrario, sostenere di essere estranei a determinati accadimenti perché gli stessi possono essere provati proprio grazie al digitale.
Al contempo, inizia a essere chiaro come, per il diritto, la pubblicazione di frasi, commenti o foto su Facebook abbia un **potenziale diffamatorio elevatissimo** e, anzi, come oggi, sostengono i giudici, sia lo strumento più potente per diffondere espressioni d'odio o di offesa. In un rapporto di lavoro, ciò comporta inevitabilmente l'avvio di procedimenti disciplinari che, nei casi più gravi, possono portare fino al licenziamento.
Facebook è visto oggi dai giudici come uno strumento simile alla stampa, circa il suo potenziale offensivo e diffamatorio e, quindi, capace di generare danni d'immagine molto elevati e su larga scala, con le relative, inevitabili conseguenze.
La Redazione segnala
Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Limiti e criteri - 29 Febbraio 2016

Controllo dei lavoratori con GPS: quando i dati sono utilizzabili?

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

Il GPS è un sistema elettronico di controllo particolarmente invasivo in quanto, grazie all'uso di satelliti, consente di tracciare tutti gli spostamenti del lavoratore, identificandone la posizione in ogni momento. Le potenzialità di questo strumento, in grado di rivelare anche aspetti della vita privata del lavoratore, rendono necessaria una selezione delle informazioni raccolte dal datore di lavoro e una loro corretta identificazione tra informazioni connesse alla produttività e quelle poste a tutela della dignità del lavoratore. Il Garante per la privacy e la Cassazione hanno fornito alcuni criteri in merito.

Il **GPS**, ossia un sistema di localizzazione che, grazie all'uso di satelliti, è in grado di identificare la posizione di un soggetto con grande precisione e di controllarne gli spostamenti; è uno strumento di controllo estremamente potente. Non è quindi una sorpresa che tale sistema possa essere utilizzato dal datore di lavoro, sul posto di lavoro, per controllare le attività e gli spostamenti dei dipendenti.
Si tratta, però, di un terreno di scontro molto delicato tra "controllo" e "privacy", tra verifica della produttività del lavoratore e tutela della sua dignità, dal momento che il controllare gli spostamenti di un individuo permette di venire a conoscenza di tanti aspetti della vita privata dello stesso.
Inoltre il GPS è giustamente considerato un **sistema elettronico di controllo particolarmente invasivo**, soprattutto se viene attivato all'insaputa del "controllato" sui dispositivi in suo possesso (ad esempio: uno smartphone o un tablet) o sulle autovetture che gli sono concesse in uso.

Le indicazioni del Garante privacy

Il Garante per la Privacy italiano, ad esempio, si è occupato in diverse occasioni del problema, anche con riferimento a grandi società telefoniche o di telecomunicazioni che avevano necessità di verificare in ogni momento la posizione dei dipendenti sia per la gestione delle chiamate sul territorio, sia per motivi di sicurezza, e che li dotavano di telefoni cellulari con, all'interno, attivati sistemi GPS che permettevano un controllo dalla centrale di tutti gli spostamenti. In tal caso, il Garante ha focalizzato l'attenzione sia sulla **consapevolezza, in capo al lavoratore,** di tali tipi di controlli e del loro funzionamento, sia della possibilità di disattivarli nei periodi non attinenti allo svolgimento di mansioni lavorative.
Nel dicembre del 2010 l'autorità Garante italiana ha esplicitamente ribadito il divieto all'uso di sistemi di geo-localizzazione dei lavoratori senza l'**accordodei sindacati** o l'autorizzazione della Direzione provinciale del lavoro. Eravamo, sia chiaro, in vigore della formulazione dell'articolo 4 prima della riforma del Jobs Act, ma il caso è comunque significativo. In quella occasione bloccò il trattamento dei dati effettuato da una società altoatesina che raccoglieva informazioni sui propri dipendenti tramite l'installazione di impianti GPS su alcuni veicoli aziendali. Alcuni lavoratori si erano lamentati di essere controllati mentre si recavano presso i clienti per attività di assistenza

regolarmente programmate, dal momento che il sistema di geo-localizzazione installato dalla società era in grado di rivelare informazioni sui percorsi seguiti, sulle soste effettuate o sulla velocità degli spostamenti del personale. Il Garante ha ricordato che, in base alle norme dello Statuto dei lavoratori (vigenti allora), l'installazione di apparecchiature che possano comportare il controllo a distanza dei dipendenti è possibile solo previo accordo dei sindacati o con l'autorizzazione della Direzione provinciale del lavoro. Nel corso dell'istruttoria è invece emerso che tali procedure non erano state rispettate.
Nel 2011 lo stesso Garante ha consentito, invece, la localizzazione satellitare di alcuni veicoli aziendali, ma solo per migliorare il servizio di trasporto e quantificare in modo corretto i costi al cliente. Nel caso specifico, erano due le finalità del sistema GPS che le aziende intendevano installare sui veicoli della loro flotta. In primo luogo consentire, in caso di necessità, di localizzare il veicolo e trasmettere la posizione rilevata; in secondo luogo, fornire dati per l'elaborazione di un rapporto di guida (tempo di percorrenza, velocità media, distanza e consumo di carburante).
Il Garante ha ritenuto leciti gli scopi perseguiti con l'uso della localizzazione satellitare in quanto volti a rendere più efficiente il trasporto dei prodotti. Ha però precisato che è possibile **trattare i soli dati idonei a rilevare la posizione dei veicol**i e quelli indispensabili alla compilazione del rapporto di guida. Non possono invece essere trattati dati "ulteriori", come quelli tecnici relativi ai giri del motore e alla frenata, che il Garante ritiene non necessari perché suscettibili di controllo sulla condotta di guida del conducente.
Il tenore di queste due decisioni è chiaro: impedire il trattamento di dati "ulteriori", via GPS, che possano comunque fornire informazioni sui soggetti che non siano correlate alle mansioni lavorative. Non è però sempre facile distinguere quali siano i dati raccolti che sono strettamente correlati alle esigenze lavorative e quali, invece, siano più legati ai comportamenti delle persone.

Il parere della Cassazione

Interessante, infine, una sentenza della Corte di Cassazione del 12 ottobre 2015, n. 20440, che si è occupata proprio di un episodio di **licenziamento correlato a controlli effettuati via GPS**.
Al lavoratore, in questo caso, era stato contestato di essersi allontanato, con l'autovettura della società, dai luoghi dove doveva svolgere il proprio lavoro, e ciò era testimoniato dal "tracciato" correlato al sistema GPS che era stato posizionato sulla vettura.
La Corte non ha rinvenuto una violazione della vecchia formulazione dell'articolo 4 dello Statuto dei Lavoratori in quanto ha ravvisato tali azioni di controllo come rientranti nei "controlli difensivi" volti a tutelare il patrimonio aziendale e a rilevare mancanze specifiche e comportamenti estranei alla normale attività lavorativa, nonché illeciti.
La Redazione segnala
Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.
Scopri la promozione riservata ai professionisti Wolters Kluwer!

Nuove tecnologie e sorveglianza - 01 Marzo 2016

Tutela del patrimonio aziendale: limiti dell'attività di controllo del datore di lavoro

di **Giovanni Ziccardi - Professore Associato di Informatica Giuridica presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano**

Le tecnologie attuali consentono attività di sorveglianza sempre più sofisticate e mirate utilizzate dal datore di lavoro per tutelare il patrimonio aziendale da furti di dati, spionaggio industriale o "vendette" da parte di ex dipendenti. Anche tali controlli devono essere condotti nel rispetto dei diritti costituzionalmente protetti. Intercettazioni delle conversazioni via Skype di un dipendente, installazione di app o programmi specifici sui telefoni e utilizzo di sistemi di videosorveglianza: come deve procedere il datore di lavoro per non violare la libertà e la dignità del lavoratore?

Accanto al controllo della posta elettronica, della navigazione in rete e, si è visto, degli spostamenti tramite GPS delle vetture aziendali o dei lavoratori, le tecnologie consentono attività di sorveglianza ancora più sofisticate e mirate che, di solito, vengono utilizzate in azienda per prevenire furti di dati, episodi di spionaggio industriale, "vendette" da parte di ex dipendenti e, in generale, attacchi al patrimonio aziendale.
Questi tipi di controllo sono altrettanto delicati perché toccano anch'essi, come gli altri, diritti costituzionalmente protetti: si pensi alla segretezza nelle comunicazioni o alla libertà di manifestazione del pensiero.

Conversazioni via Skype

Nel settembre del 2015, ad esempio, il Garante per la Privacy si è occupato di un caso riguardante le intercettazioni, da parte del datore di lavoro, delle conversazioni via Skype di un dipendente.
In tal caso, ha stabilito che il datore di lavoro non può spiare le conversazioni Skype dei dipendenti, dal momento che il contenuto di comunicazioni di tipo elettronico o telematico scambiate dai dipendenti nell'ambito del rapporto di lavoro godono comunque di garanzie di segretezza tutelate anche a livello costituzionale. Nel caso di specie, il Garante ha accolto un ricorso proposto da una dipendente che lamentava l'**illecitaacquisizione di conversazioni**, avute con alcuni clienti/fornitori, poste poi alla base del suo licenziamento e ha stabilito che il datore di lavoro non può effettuare alcun trattamento dei dati personali contenuti nelle conversazioni ottenute in modo illecito, ma si deve limitare alla conservazione di quei dati raccolti ai fini di una eventuale acquisizione da parte dell'autorità giudiziaria.
In questo caso si noti, però, che il datore di lavoro aveva installato un software sul computer assegnato alla dipendente in grado di visualizzare sia le conversazioni effettuate dalla ricorrente dalla propria postazione di lavoro prima di uscire dall'azienda, sia quelle avvenute successivamente da un computer collocato presso la propria abitazione.
Si trattava, insomma, di un dispositivo elettronico che era in palese violazione della libertà e della dignità del lavoratore, era occulto (quindi violava il principio di correttezza) e portava alla raccolta di informazioni non pertinenti al rapporto di lavoro.

App o programmi specifici sui telefoni

Un nuovo modo, molto invasivo, per controllare i dipendenti, che già abbiamo anticipato nell'articolo precedente sui GPS, è l'installazione di app o programmi specifici sui telefoni che forniscono al datore di lavoro simili poteri di sorveglianza.
Il Garante privacy, nel novembre del 2014, si è occupato di un caso molto interessante, e altamente tecnologico. Ha stabilito, in sintesi, che due società telefoniche di importanza nazionale potranno utilizzare i dati di localizzazione geografica, rilevati da una app attiva sugli smartphone in

dotazione ai lavoratori, solo a patto che adottino adeguate cautele a protezione della loro vita privata.

Tutela della riservatezza dei dipendenti

Il fine di controllo delle due società è assolutamente lecito: vogliono utilizzare questa tipologia di dati per ottimizzare l'impiego delle risorse presenti sul territorio e migliorare la gestione, il coordinamento e la tempestività degli interventi tecnici.
Occorre, però, pensare anche alla tutela della riservatezza dei dipendenti, e per questo motivo l'Autorità ha elaborato una lista di interessantissime prescrizioni, che valgono anche al di là del caso specifico di cui stiamo trattando, e che cercano di mitigare l'esigenza del controllo con la protezione della privacy del lavoratore.
Nota il Garante, infatti, come lo smartphone, per le proprie caratteristiche, sia destinato a "seguire" la persona che lo possiede, senza distinzione tra tempo di lavoro e tempo di non lavoro.
Il trattamento dei **dati di localizzazione** può presentare, quindi, rischi specifici per la libertà (ad esempio: di circolazione e di comunicazione) e per i diritti e la dignità del dipendente. Per questo motivo, le società dovranno adottare specifiche misure volte a garantire che le informazioni visibili o utilizzabili dalla app siano solo quelle di geolocalizzazione, impedendo l'accesso ad altri dati, quali ad esempio, sms, posta elettronica, traffico telefonico. E dovranno configurare il sistema in modo tale che sullo schermo dello smartphone compaia sempre, ben visibile, un'icona che indichi ai dipendenti che la funzione di localizzazione è attiva.
I dipendenti, poi, dovranno essere ben informati sulle caratteristiche dell'applicazione (ad es., sui tempi e le modalità di attivazione) e sui trattamenti di dati effettuati dalle società.

Sistemi di videosorveglianza

Un tema molto interessante, per concludere questa rassegna "tecnologica", è anche l'utilizzo di sofisticati sistemi di videosorveglianza (ormai completamente "digitale" ed economica, e ben differente da quella che era prevista negli anni Settanta dallo Statuto dei Lavoratori) per controllare i locali dove si svolgono le attività dei dipendenti.
In questo caso, i sistemi di videosorveglianza sono ammessi ma devono sempre essere rispettosi della libertà e della dignità dei lavoratori.
Nel settembre del 2014 il Garante italiano ha stabilito, ad esempio, che un datore di lavoro non può installare delle **telecamere** all'interno degli spogliatoi dei dipendenti, respingendo la richiesta di una società di attivare un sistema di videosorveglianza che avrebbe violato la legittima aspettativa di intimità e la dignità dei lavoratori. Nel caso di specie, un'azienda metalmeccanica riteneva una simile misura necessaria per arginare le numerose e ripetute segnalazioni di effrazioni negli spogliatoi, che l'avevano già indotta a rafforzare gli armadietti, dotandoli di lucchetti, e a installare una telecamera all'ingresso degli stessi.
Alla richiesta presentata al Garante, la società aveva anche allegato alcune denunce di furti avvenuti negli ultimi due anni, nonché un accordo raggiunto con i sindacati aziendali che secondo l'impresa avrebbe consentito l'estensione dell'attuale impianto di videosorveglianza all'interno degli spogliatoi.
Il Garante, però, è stato intransigente e, nel vietare l'attuazione del progetto, ha ritenuto che l'installazione delle telecamere negli spogliatoi dei dipendenti non fosse conforme alle norme sulla protezione dei dati personali. Il sistema, infatti, era configurato in modo tale da prevedere espressamente il minuzioso controllo dell'intera area adibita a spogliatoio, senza alcuna limitazione all'angolo di ripresa, in una zona connotata, invece, da una particolare aspettativa di riservatezza e di tutela della intimità e dignità della persona.

La Redazione segnala

Questo articolo fa parte del dossier **Jobs Act e controlli digitali** realizzato nell'ambito della partnership tra Wolters Kluwer e Vodafone.
Dall'incontro tra il contenuto specialistico di Wolters Kluwer e l'innovazione tecnologica di Vodafone nasce Vodafone e.box Wolters Kluwer Edition: la miglior connessione 4G e Fibra e 3 mesi gratuiti di novità e commenti su diritto, fisco, lavoro e sicurezza con IPSOA Quotidiano, il Quotidiano Giuridico e Sistema Ambiente e Sicurezza.

Wolters Kluwer

Copyright © - Riproduzione riservata