CONTROLLI DIFENSIVI DEL LAVORATORE E PRIVACY

Argomento molto delicato, come sappiamo, attiene al conciliare i cd. “controlli difensivi” del datore di lavoro, previsti dalla normativa in materia di tutela dei dati personali, con i rischi derivanti dalle pratiche finalizzate all’ottenimento fraudolento di informazioni aziendali operate da dipendenti ovvero ex dipendenti.

1. Il controllo dei lavoratori ed i profili di privacy – quadro generale.

Come è noto, se non in casi eccezionali, i datori di lavoro non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, e ciò anche dopo la modifica operata dall’art. 23 del d. lgs. 151/2015, uno dei 4 decreti attuativi del Jobs Act, a modifica dell’art. 4 della L. 300/70 (cd. Statuto dei lavoratori).

Il Garante della Privacy mantiene un atteggiamento critico (più ancora della giurisprudenza di merito e di legittimità) sulla lettura e sulla registrazione sistematica delle e-mail dei dipendenti così come sul controllo sistematico della navigazione in internet da parte del lavoratore.

Ciò costituirebbe, di fatto, un controllo a distanza dell’attività lavorativa vietato dallo Statuto dei lavoratori ed ancor prima dai principi della nostra carta costituzionale.

L'articolo 41 della Costituzione statuisce, infatti, la libertà di iniziativa economica del datore di lavoro purché venga esercitata nel rispetto della libertà e della dignità umana. Il datore di lavoro, pertanto, ha il potere di stabilire le regole per l'esecuzione e la disciplina del lavoro che i lavoratori sono tenuti a rispettare, pena l'irrogazione di sanzioni disciplinari. In conseguenza di ciò il datore di lavoro ha il potere di verificare che l'attività lavorativa venga svolta in conformità alle direttive da lui impartite, ma non senza limiti.

I limiti al potere di controllo del datore di lavoro discendono dal contrapposto diritto dei lavoratori al rispetto della loro riservatezza, dignità personale, libertà di espressione e comunicazione.

E’ necessario contemperare diritti contrapposti e, conseguentemente, regolamentare i poteri del datore di lavoro, la cui disciplina è principalmente prevista dallo Statuto dei Lavoratori.

Tale normativa prevede un rigoroso divieto dei cd. “controlli difensivi” quando si rilevino, in qualche modo, lesivi dei diritti inviolabili dei lavoratori, scoraggiando ogni tipo di controllo nascosto, salvo che sussistano determinate condizioni, variamente affrontate sia dalla giurisprudenza che dal Garante.

E' chiaro che le nuove tecnologie consentono una vasta implementazione dei controlli a distanza nei confronti dei lavoratori fino a verificarne quasi minuto per minuto la correttezza dello svolgimento della prestazione lavorativa.

Gli organi preposti hanno, pertanto, inteso adeguare la normativa e l'interpretazione della stessa, nel tentativo di salvaguardare i contrapposti diritti:

la tutela della privacy del lavoratore da un lato ed il diritto del datore di lavoro alla tutela dei beni aziendali, dall'altro.

2. Modifiche normative all'art. 4 della L. 300/1970 – cd. statuto dei lavoratori: ampliamento dei controlli a distanza – limiti e obblighi datoriali.

La normativa, così come riformata dal D. Lgs n. 151 del 14 settembre del 2015 (Jobs Act), ha cambiato l'art. 4 dello Statuto dei Lavoratori, che è la norma principale in materia. In particolare, il Jobs Act ha stabilito un regime diverso a seconda che si tratti di impianti (es. videosorveglianza) o di strumenti di lavoro (personal computer, smartphone).

Prima della modifica normativa era del tutto vietato utilizzare apparecchiature per il mero controllo dell'attività lavorativa (controllo programmato) con una leggera attenuazione in presenza di specifiche esigenze organizzative, produttive o di sicurezza ed, in ogni caso, quando gli impianti fossero autorizzati dalle rappresentanze sindacali o, in mancanza, dal Ministero del Lavoro. I comportamenti del dipendente ripresi o verificati per il tramite delle attrezzature di controllo, fuori dai casi summenzionati, non potevano costituire il motivo determinante di attivazione di una procedura disciplinare.

L'accordo con le rappresentanze sindacali costituiva una forma di tutela preventiva dei lavoratori.

Il nuovo comma 1 dell'art. 4 dello Statuto dei Lavoratori stabilisce che è consentito l'utilizzo di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di **controllo a distanza** dell'attività lavorativa a **condizione** che:

1. siano impiegati esclusivamente per **"esigenze organizzative e produttive, per la sicurezza del lavoro o per la tutela del patrimonio aziendale"**;
2. sia concluso preventivamente un "**accordo collettivo"** ovvero, in mancanza di accordo, l'utilizzo degli strumenti sia stato "**autorizzato preventivamente in via amministrativa"**.

Rispetto al passato sono stati effettivamente normati i cosiddetti controlli difensivi, già ammessi da parte della giurisprudenza. E' stato, altresì, espressamente inserito nella norma il concetto di "patrimonio aziendale", termine di tale ampiezza da ricomprendere tutti i beni aziendali, inclusi quindi anche quelli immateriali.

Il legislatore ha, inoltre, consentito il controllo a distanza non solo mediante gli impianti audiovisivi ma, più in generale, attraverso tutti gli strumenti dai quali derivi anche la possibilità di controllo a distanza, ricomprendendo così qualsiasi tipo di tecnologia.

Qualora si voglia procedere alla regolarizzazione dell'azienda per l'utilizzo, a scopi "difensivi", delle apparecchiature di controllo, la procedura da espletare è, in alternativa, quella di sottoscrivere un accordo con le RSU o le RSA ovvero proporre istanza alla Direzione Territoriale del Lavoro territorialmente competente, ovvero, in mancanza di accordo, chiedere autorizzazione al Ministero del Lavoro. Rispetto alla vecchia disciplina, quindi, per poter utilizzare strumenti di controllo in ciascuna unità produttiva, il datore di lavoro non deve più fare ricorso alle singole realtà locali, sindacali o amministrative.

La novità più rilevante è rappresentata dal nuovo comma 2 dell'art. 4 dello Statuto dei Lavoratori che prevede alcune eccezioni ai limiti di cui al comma1. Liceità dei controlli, cioè, anche in assenza di esigenze organizzative e produttive, sicurezza del lavoro o tutela del patrimonio aziendale ed in assenza di accordo sindacale o autorizzazione amministrativa nel caso di impiego di:

– "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (es. cellulari, computer..);

– "strumenti di registrazione degli accessi e delle presenze".

Ciò, comunque, a fronte di idonea informativa fornita ai dipendenti circa le "modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196" (Normativa sulla Privacy).

Pertanto, l'espressione "per rendere la prestazione lavorativa" comporta che l'accordo o l'autorizzazione siano evitabili se, e nella misura in cui, lo strumento viene considerato quale mezzo necessario al lavoratore per adempiere la prestazione: ciò significa che, nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione non necessitanti l'erogazione della prestazione) al solo scopo di controllare il

lavoratore, si fuoriesce dall'ambito della disposizione (Nota del 18 giugno 2015 del Ministero del Lavoro).

Ogni eventuale modifica o integrazione degli strumenti del lavoratore saranno ritenute legittime e potranno avvenire solo alle condizioni sopra ricordate: **la ricorrenza di particolari esigenze organizzative e produttive, l'accordo sindacale o l'autorizzazione in sede amministrativa**.

Nell'ambito del comma 1 sembrerebbero non rientrare anche gli elementi accessori alla strumentazione tecnologica forniti al lavoratore che non siano strettamente funzionali a rendere la prestazione.

Il riferimento alla "registrazione degli accessi e delle presenze**"** è, anch'esso, di ampia portata, ricomprendendo non solo l'ipotesi della rilevazione presenza in ingresso aziendale, ma tutti quegli strumenti di accesso a particolari aree dell'azienda, anche quelli funzionali alla mobilità interna.

Il comma 3 ha, inoltre, stabilito che le informazioni raccolte tramite gli strumenti di cui al comma 1 e 2, **sono utilizzabili a tutti i fini connessi al rapporto di lavoro** a condizione che al lavoratore sia data adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli. Per "fini" naturalmente si intendono anche quelli tipicamente disciplinari.

Il Ministero del Lavoro, a tal proposito, ha chiarito che occorre informare i lavoratori circa l'esistenza e le modalità d'uso degli strumenti di controllo (anche quelli installati con l'accordo sindacale o l'autorizzazione della Direzione Territoriale del Lavoro o del Ministero), e delle modalità di effettuazione dei controlli, che comunque dovranno rispettare quanto disposto dal D. Lgs. 30.06.2003, n. 196 in materia di privacy (finalità e modalità del trattamento dei dati, la natura obbligatoria e facoltativa del conferimento dei dati, conseguenze di un eventuale rifiuto, soggetti cui tali dati possono essere comunicati e responsabili aziendali del trattamento dei dati) nonché dei diritti dei lavoratori. In caso contrario i dati non possono essere utilizzati a nessun fine.

3. Controlli difensivi: caratteristiche generali ed eventuali sanzioni.

In ogni caso si ricorda che il datore di lavoro non può effettuare controlli in maniera indiscriminata: ogni forma di controllo deve, infatti, essere conforme ai principi di liceità, pertinenza, trasparenza e non eccedenza del trattamento dei dati.

Il controllo deve, comunque, avere le seguenti caratteristiche:

1) risultare necessario o indispensabile rispetto ad uno scopo determinato ed avente il carattere dell'eccezionalità (principio di necessità);

2) deve essere finalizzato a garantire la sicurezza o la continuità aziendale, o a prevenire e reprimere illeciti (principio di finalità);

3) deve essere preceduto da una specifica informativa del datore di lavoro nei confronti dei dipendenti sui limiti di utilizzo degli strumenti e delle sanzioni previste nel caso di violazione di tali limiti (principio di trasparenza).

4) deve essere necessario e non eccessivo relativamente alla finialità perseguita (principio di proporzionalità);

5) deve garantire che i dati raccolti siano protetti in modo adeguato (principio di sicurezza).

Le linee guida del Garante per posta elettronica ed Internet precisano gli elementi oggetto dell'informativa preventiva.

In materia di videosorveglianza il Garante detta le regole per tali sistemi, obbligando il datore di lavoro all'adeguata segnalazione dei luoghi videosorvegliati, alla conservazione limitata dei dati (di regola 24 ore), nonché a permette l'accesso ai dati ai lavoratori.

Si consiglia a questo proposito di rivedere e/o riformulare le policy aziendali e le informative privacy/raccolta del consenso adeguandole a quanto previsto dalla nuova disposizione nella materia trattata e per rendere il tutto conforme ai provvedimenti del Garante.

4. Geo-localizzazione satellitare dei veicoli aziendali.

Con recente provvedimento n. 138 del 16 marzo 2017 il Garante per la Protezione dei dati personali ha affrontato il tema della liceità del trattamento dei dati personali nel caso di aziende che, per la specifica attività, qual è quella del settore dell'autotrasporto, utilizzino lo strumento della geo-localizzazione della flotta aziendale.

Nel corso dell'istruttoria il Garante ha riconosciuto il legittimo interesse della società a rilevare la posizione dei propri mezzi per le molteplici finalità indicate, ma solo nel pieno rispetto della privacy dei lavoratori e, comunque, previo accordo sindacale.

Per l'installazione dei sistemi Gps sui mezzi aziendali, qualora siano strumenti che il dipendente utilizza per rendere funzionale la propria attività, non è richiesto alcun accordo sindacale. Considerato che la tecnologia del sistema potrebbe consentire il controllo a distanza dei

lavoratori, anche dopo le modifiche normative già evidenziate al paragrafo n. 2 della presente, per poterlo attivare dovrà prima essere raggiunto un accordo con le rappresentanze sindacali o, in sua assenza, si dovrà richiedere l'autorizzazione all'Ispettorato nazionale del lavoro.

L'Autorità fa presente che, nel caso in cui lo scopo dell'installazione del sistema sia riconducibile a finalità organizzative e produttive nonchè legate alla sicurezza del lavoro ed alla tutela del patrimonio aziendale in conformità con quanto stabilito dall'articolo 4, comma 1, del cd. "Statuto dei Lavoratori" (L. 300/70, come modificato dall'art. 23, d. lgs. 14.9.2015, n. 15) risulta, in termini generali, leciti.

Con il medesimo provvedimento il Garante della Privacy ha ribadito che, prima dell'inizio del trattamento dei dati personali rilevati con il sistema di geo-localizzazione, la società è tenuta, in base alla vigente disciplina sulla privacy ai seguenti adempimenti:

a. effettuare la notificazione del trattamento dei dati al Garante ai sensi dell'articolo 37, comma 1, lett. a), del Codice;

b. fornire ai dipendenti della società coinvolti dai descritti trattamenti, un'informativa comprensiva di tutti gli elementi contenuti nell'articolo 13 del Codice (tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione), anche in conformità al principio di correttezza in base al quale il titolare è tenuto a rendere chiaramente riconoscibili agli interessati i trattamenti che intende effettuare (art. 11, comma 1, lett. a), del Codice);

c. adottare le misure di sicurezza previste dagli articoli 31 ss. del Codice al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati;

d. considerato che la società ha stipulato, ai sensi dell'art. 4, legge 20.5.1970, n. 300, accordi con le rappresentanze sindacali relativamente all'adozione di dispositivi completi di funzionalità di geo-localizzazione, integrare i predetti accordi oppure, in assenza di accordo, richiedere l'autorizzazione all'Ispettorato nazionale del lavoro con riferimento a tutte le finalità perseguite e in relazione alla relative modalità (cfr. par. 2.1.);

e. predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 7 e seguenti del Codice.

Dovranno, altresì, essere definite con attenzione le modalità di raccolta, di elaborazione e di conservazione dei dati di geo-localizzazione e degli altri dati personali, differenziando le tutele in base alla singola finalità perseguita.

5. Recenti provvedimenti del Garante per la Privacy.

Il Garante della Privacy è tornato recentemente su tali argomenti ponendo un freno ed un arresto ad suo precedente indirizzo maggiormente permissivo pro-datoriale.

Con il provvedimento n. 53/2018 il Garante ha ritenuta illegittima la conservazione massiva e senza limiti della corrispondenza email dei propri dipendenti attraverso gli account aziendali.

Il Garante ha espressamente statuito in proposito come: "*La conservazione sistematica dei dati esterni e del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti attraverso gli account aziendali, allo scopo di poter ricostruire gli scambi di comunicazioni tra gli uffici interni nonché tutti i rapporti intrattenuti con gli interlocutori esterni (clienti, fornitori, enti assicurativi, tour operator), anche in vista di possibili contenziosi, effettuata da soggetti diversi dal titolare della specifica casella di posta elettronica per l'intera durata del rapporto di lavoro e successivamente all'interruzione dello stesso, non risulta altresì conforme ai principi di liceità, necessità e proporzionalità del trattamento (v. artt. 3, 11, comma 1, lett. a) e d) del Codice).*"

A ciò si aggiunga come il Garante censuri, espressamente, la violazione dell'obbligo di informativa (art. 13 del D. Lgs. 196/2003) in quanto la società non abbia, nel caso di specie, debitamente informato i dipendenti "*circa le modalità e finalità della descritta attività di raccolta e conservazione dei dati relativi all'utilizzo della posta elettronica, né con una informativa individualizzata né con la messa a disposizione della policy aziendale*".

Con riferimento, da ultimo, ai trattamenti effettuati dopo la cessazione del rapporto di lavoro, il Garante ha ribadito quanto già espresso in precedenti occasioni (provvedimenti n. 456/2015, 136/2015 e 551/2014), ossia che "*gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi*", mentre non è conforme alla normativa sulla privacy, ed ai suoi principi, il comportamento aziendale consistente nel mantenere temporaneamente attivi gli account di posta elettronica.

Si rappresenta, del resto, come l'installazione di impianti audiovisivi e di altri strumenti, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, in violazione delle norme descritte nella presente circolare comporta l'applicazione delle sanzioni previste all'*art. 38* dello Statuto dei Lavoratori:

– salvo che il fatto non costituisca più grave reato, ammenda da € 154,00 a € 1.549,00 o arresto da 15 giorni a 1 anno;

– nei casi più gravi, le pene dell'arresto e dell'ammenda sono applicate congiuntamente;

– quando per le condizioni economiche del reo l'ammenda può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo;

– nei casi più gravi, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna.

Eccetto che nei casi più gravi, è applicabile l'istituto della prescrizione obbligatoria (*art. 15 del D.Lgs. 23.04.2004, n. 124*) per cui al datore di lavoro viene prescritta la cessazione della condotta illecita e, successivamente, in caso di esito positivo, viene ammesso al pagamento di una sanzione.

Spetta all'ispettorato del lavoro il potere-dovere di individuare i casi di maggiore gravità e quindi applicare o meno l'istituto della prescrizione.

Si segnala, da ultimo, che con la circolare n. 5/2018 l'Ispettorato del lavoro ha chiarito le modalità operative di istruttoria sulle istanze presentate dai datori di lavoro per l'autorizzazione alla videosorveglianza dei lavoratori.

6. Novità in tema di Privacy

Il Regolamento UE 2016/679 all'art. 35 ha introdotto la cd. "Valutazione di impatto sulla protezione dei dati" (DPIA "Data Protection Impact Assessment"). In concreto il trattamento dati che prevede l'uso di nuove tecnologie e che può presentare un

"rischio elevato per i diritti e le libertà delle persone fisiche" necessita di una specifica valutazione circa l'impatto dei trattamenti previsti sulla protezione dei dati personali.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

"*a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

b) il trattamento, su larga scala, di categorie particolari di dati personali sensibili o di dati relativi a condanne penali;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico» (art. 35)."

Per praticità elenchiamo alcuni esempi nei quali diviene necessaria ed opportuna la valutazione di impatto sulla protezione dei dati, trattasi di:

- azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc.;
- raccolta di dati tratti dai social media;
- utilizzo di un sistema di videosorveglianza per il controllo del traffico autostradale. Il titolare prevede di utilizzare un sistema intelligente di analisi delle immagini per l'individuazione dei veicoli ed il riconoscimento automatico delle targhe;
- Conservazione per scopi di archiviazione di dati sensibili relativi a interessati coinvolti in progetti di ricerca o studi sperimentali.

Le Autorità di Controllo potranno redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti o meno al requisito di una valutazione d'impatto sulla protezione dei dati.

I contenuti minimi della valutazione (ex art. 35 regolamento UE 2016/679) sono:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

In sintesi, la valutazione di impatto sulla protezione dei dati è una procedura finalizzata a:

- descrivere il trattamento dati;
- valutarne necessità e proporzionalità;
- facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali;
- il tutto attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli.

Le aziende interessate dovranno seguire la seguente procedura:

1) Valutare la sussistenza di un "rischio elevato";

2) consultare il Responsabile della Protezione dei Dati (RPD), se nominato;

3) verificare le prescrizioni di un eventuale codice di condotta al quale si è eventualmente aderito;

4) verificare se consultare i rappresentanti dei lavoratori;

5) redigere l'atto di valutazione di impatto sulla privacy;

6) diffondere, eventualmente per estratto, l'atto di valutazione di impatto sulla privacy;

7) aggiornare periodicamente l'atto di valutazione di impatto sulla privacy.

Il Regolamento prevede, in caso di mancato rispetto di quanto disciplinato l'applicazione di rilevanti sanzioni amministrative pecuniarie per omessa o inidonea valutazione di impatto sulla protezione dei dati.

Il nostro studio legale di riferimento, nelle persone degli **Avv.ti Maria Cristina Bruni e Chiara Caponegro**, unitamente agli altri professionisti e consulenti dell'Associazione, resta disponibile ad ogni ulteriore chiarimento ed approfondimento sulla materia qui trattata e sugli svariati aspetti, oggetto di numerose modifiche legislative e relative interpretazioni giurisprudenziali.

Milano 23 aprile 2018

Avv. Maria Cristina Bruni

Avv. Chiara Caponegro