Milano, Giovedì 22 Giugno 2017
ore 16.00

Sede di Unicredit
Piazza Gae Aulenti
Torre B, 10° Piano – Aula Jodice

CONVEGNO

GIDP
ASSOCIAZIONE DIRETTORI RISORSE UMANE

TUTELA DEL PATRIMONIO AZIENDALE

Aggiornamento Investigativo Giuridico e Tecnologico

in collaborazione con

DEFENSIS

AGENDA

16.00 - Saluti di apertura a cura di
Dott. Paolo Citterio, Presidente Nazionale *G.I.D.P./H.R.D.A.*

16.15 - L.104 e Assenteismo: aggiornamento normativo
Avv. Daniele Colombo, *CLC* Studio Legale

16.35 - Caso Aziendale
Ing. Antonio Dragotto, Vice President HR Italy *StMicroelectronics*

16.55 – Il controllo del lavoratore con telecamere occulte
Avv. Alessandra Merenda, *Perroni e Associati* Studio Legale

17.15 - Perizie su strumenti aziendali: la corretta gestione
Avv. Vittorio Pomarici, *BonelliErede* Studio Legale
Avv. Tommaso Faelli, *BonelliErede* Studio Legale

17.45 - Caso Aziendale
Dott. Leonardo Bitetto, HR Manager *Johnson Controls*

18.00 - La parola alle parti sociali
Dott. Filippo Cozzi, Funzionario Area Sindacale, Unità Sanità, Gomma Plastica, Energia e Gas *Assolombarda Confindustria Milano Monza e Brianza*
Dott. Iginio Maletti, Segretario Generale *FIM CISL* Piemonte Orientale

18.20 Sessione di domande e risposte

18.30 Conclusioni e aperitivo

Perizie su strumenti aziendali: la corretta gestione

Avv. Vittorio Pomarici, *Partner, Studio Legale BonelliErede*
Avv. Tommaso Faelli, *Partner, Studio Legale BonelliErede*

Milano, 22 giugno 2017

BonelliErede

I principi applicabili nello svolgimento delle perizie: gli articoli 4 e 8, Statuto dei Lavoratori

Art. 4, Statuto dei Lavoratori

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 […]

La disciplina di cui sopra **non si applica** agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (ossia **telefono cellulare**, **computer**, ecc.), **salvo che** gli stessi vengano **modificati** (ad esempio, con l'aggiunta di appositi *software* di localizzazione o filtraggio) **per controllare il lavoratore**

I principi applicabili nello svolgimento delle perizie: gli articoli 4 e 8, Statuto dei Lavoratori

Art. 4, Statuto dei Lavoratori

Le informazioni raccolte mediante gli strumenti di controllo a distanza **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**

I dati possono essere trattati per tutti i fini connessi con il rapporto di lavoro quindi anche per **finalità disciplinari**
solo in caso di ***compliance*** **con la normativa privacy**

Art. 8, Statuto dei Lavoratori

E' 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**

I principi applicabili nello svolgimento delle perizie: il Codice della Privacy

- **la necessità:** la perizia informatica deve essere necessaria e **non ridondante** per la verifica
- **la trasparenza**: il datore di lavoro deve operare alla luce del sole, informando i dipendenti dell'**esistenza** di apparecchiature che esercitano controlli, le **modalità** con cui queste operano e le **conseguenze** che derivano da violazioni
- **la liceità**: i controlli **non** devono essere **discriminatori o vessatori o per finalità non ammesse dallo Statuto dei Lavoratori**
- **la pertinenza**: le informazioni che vengono raccolte dal datore di lavoro devono essere **funzionali rispetto allo scopo** (legittimo) che persegue
- **la proporzionalità e non eccedenza**: tra i **dati** trattati e le **finalità** del controllo
- **la conservazione funzionale alla finalità**: i dati sono conservati per un **periodo di tempo non superiore a quello necessario** per il completamento del processo di verifica

Gli adempimenti per lo svolgimento delle perizie

Gli adempimenti preliminari

→ **La policy sull'uso degli strumenti IT e sui controlli**

Gli adempimenti per l'avvio e la gestione delle perizie

→ **I contesti dei controlli**

→ **L'informativa preventiva**

→ **La definizione delle persone e dei ruoli**

→ **La conservazione dei dati**

Oltre 200 provvedimenti del Garante della Privacy in materia di controlli dei lavoratori

Policy sull'uso degli strumenti IT e sui controlli: il contenuto e le modalità di pubblicazione

Istruzioni per l'utilizzo di posta elettronica e rete:

- «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 esempio, fuori dall'orario di lavoro, durante le pause, nel tempo di lavoro ma con uso moderato)»

Istruzioni per la «navigazione» in Internet:

- «I comportamenti che sono tollerati rispetto alla «navigazione» in Internet (ad esempio, il *download* di *software* o di *file* musicali) e della tenuta di *file* nella rete interna»

UTILIZZO DEGLI STRUMENTI IT PER FINALITA' ESCLUSIVAMENTE LAVORATIVA O ANCHE PERSONALE?

AMMESSO **VIETATO**

Policy sull'uso degli strumenti IT e sui controlli: il contenuto e le modalità di pubblicazione

Regolamentazione delle ipotesi in cui il datore di lavoro può effettuare controlli e con quali modalità:

- **«Se e in quale misura il datore di lavoro si riserva di effettuare controlli in conformità della legge**, anche saltuari o occasionali, **indicando le ragioni legittime**, specifiche e non generiche, per cui vengono 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 su singoli dispositivi e postazioni)»

Indicazioni ai lavoratori dei tempi di conservazione dei dati:

- **«Le informazioni che sono memorizzate temporaneamente** (ad esempio, i *file* di *log* che vengono registrati) e chi può avere accesso a tali dati, anche dall'esterno»
- «Se e quali informazioni sono 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)»
- «Le prescrizioni per la sicurezza dei dati e dei sistemi (artt. 34 e ss. e allegato B del Codice della Privacy)»

Regolamentazione dei meccanismi utilizzati per garantire la continuità dell'attività lavorativa in caso di assenza del lavoratore

- **«Le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso** (in particolare, nei casi in cui sia programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti»

Policy sull'uso degli strumenti IT e sui controlli: il contenuto e le modalità di pubblicazione

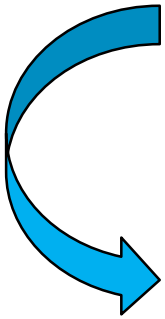
Le conseguenze disciplinari in caso di violazione del corretto utilizzo degli strumenti IT:

- «**Le conseguenze, anche disciplinari**, che il datore di lavoro si riserva di trarre nel caso in cui constati che la posta elettronica e la rete internet sono utilizzate indebitamente»

Pubblicazione: affissione in luogo accessibile a tutti

Policy sull'uso degli strumenti IT e sui controlli - l'accesso al pc aziendale, provvedimento del Garante della Privacy, 2006

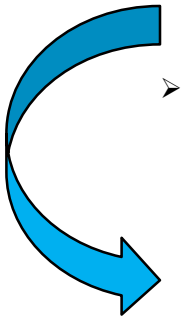
- dopo aver rilevato un utilizzo indebito del telefono aziendale di un dipendente, il datore di lavoro chiede di accedere al contenuto del pc di quest'ultimo, per verificare l'eventuale presenza di cartelle contenenti *files* personali
- di fronte al dipendente, il suo superiore di settore, il responsabile HR e il responsabile IT effettuano le indagini e scoprono alcune cartelle denominate «musica» e «personale»
- il dipendente riceve una contestazione disciplinare, seguita da licenziamento



- **assenza di un disciplinare interno che informi i dipendenti sui possibili controlli che il datore di lavoro può effettuare, né sulle modalità e sulle conseguenze**
- **sarebbe stato sufficiente rilevare la presenza di cartelle la cui denominazione suggeriva la presenza di dati personali sul pc aziendale, vietato dal disciplinare interno, senza accedere al loro contenuto (così effettuando un trattamento indebito di dati anche sensibili)**
- **il Garante della Privacy dispone il divieto di ulteriori trattamenti**

Policy sull'uso degli strumenti IT e sui controlli – trattamento sulle email di dipendenti ed ex dipendenti, provvedimento del Garante della Privacy, 2015

- dopo le dimissioni di alcuni dipendenti, il datore di lavoro aveva comunicato che avrebbe proceduto alla chiusura dei loro account di posta elettronica aziendali e aveva chiesto altresì la restituzione dei computer ed altri strumenti forniti in dotazione
- dato che la società si era resa conto della cancellazione di documenti aziendali dai *device* degli ex dipendenti, aveva mantenuto attivi i loro account di posta elettronica, che permettevano anche il reindirizzo dei medesimi «presso un utente dell'azienda» e non aveva attivato il messaggio automatico di segnalazione al mittente di tale re indirizzamento né aveva dato l'informativa preventiva agli ex dipendenti con riferimento ai controlli che stava effettuando
- la società aveva quindi effettuato accessi ai loro messaggi di posta elettronica per garantire il proprio diritto di difesa



- **l'assenza di un disciplinare sull'utilizzo della posta elettronica aziendale**, in base al quale le caratteristiche essenziali dei trattamenti devono essere preventivamente rese note ai lavoratori, in particolare se effettuati per finalità di controllo, **può comportare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità** rispetto ad alcune forme di comunicazione
- i trattamenti effettuati dalla società hanno comportato una **violazione dei principi di liceità, correttezza e proporzionalità**
- **il Garante della Privacy dispone il divieto di ulteriori trattamenti,** salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria

Contesti dei controlli

Controlli a campione	• **Non per verificare eventuali violazioni** dei lavoratori nell'esercizio della loro attività ma **solo per il miglioramento dei processi produttivi ed esclusivamente su base anonima**
Controlli mirati in caso di «fattori scatenanti»	• **Iniziativa del datore di lavoro**: in caso di evento dannoso o situazione di pericolo per il patrimonio aziendale, il datore di lavoro può verificare i comportamenti anomali, **procedendo con gradualità** • Richiesta di una **pubblica autorità** nell'ambito di procedure o verifiche
Controlli su richiesta della società controllante per applicare una normativa estera	• I trattamenti di dati per adempiere a una normativa estera, che non abbia un corrispondente nella normativa italiana o europea, richiedono la valutazione **preventiva** del Garante della Privacy per l'identificazione di un **legittimo interesse**

Con il GDPR, **la valutazione sulla presenza di un legittimo interesse verrà effettuata direttamente dal titolare**, senza la necessità di coinvolgere il Garante della Privacy

Gli strumenti per effettuare i controlli: l'informativa preventiva

Gli interessati hanno il diritto di essere **informati preventivamente**, e in modo chiaro, sulle verifiche in corso a loro carico e sulle relative modalità di esecuzione

L'informativa può essere ritardata in caso di prevedibile compromissione della verifica

Gli strumenti per effettuare i controlli: definizione delle persone e dei ruoli

Chi dirige le indagini?

L'attività di investigazione permette la verifica *ex post* e mirata

I **soggetti autorizzati** dalla legge a gestire le indagini sono:

- Datore di lavoro
- Investigatori privati autorizzati ai sensi del Testo Unico delle Leggi di Pubblica Sicurezza (c.d. TULPS)
- Avvocati abilitati all'esercizio della professione legale

Le società che offrono servizi di analisi forense, se non hanno l'autorizzazione ai sensi del TULPS, devono essere nominate responsabili del trattamento e seguire le istruzioni del datore di lavoro, dell'avvocato o dell'investigatore privato incaricato

Chi partecipa alle indagini?

La società

A chi possono essere comunicati i risultati delle verifiche?

I dati possono essere condivisi con soggetti appartenenti ai dipartimenti che hanno un ruolo nel processo decisionale durante o a valle della verifica (ad esempio, i dati derivanti dai controlli possono essere condivisi con la casa madre se questa svolge o partecipa all'attività decisionale nei confronti del soggetto indagato)

La conservazione dei dati al termine del rapporto di lavoro: i punti fondamentali

La copia dei dati su un supporto autonomo è consentita ma devono essere informati i lavoratori della possibilità che siano effettuate copie di *back-up*

La conservazione dei dati in azienda o presso terzi è consentita ma il terzo deve essere nominato responsabile

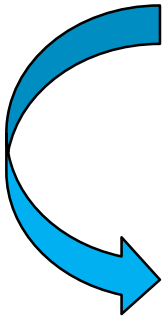
I tempi di conservazione dei dati: la policy dell'azienda deve indicare tempi di conservazione ma ci sono interpretazioni restrittive da parte del Garante della Privacy

Valutazione del caso concreto

Con il **GDPR**, il datore di lavoro, in quanto titolare, dovrà indicare al lavoratore **il periodo di conservazione dei dati personali oppure**, se non è possibile, **i criteri utilizzati per determinare tale periodo** (art. 13)

La conservazione dei dati al termine del rapporto di lavoro: il telefono cellulare, provvedimento del 2015

- a seguito di una sospensione per motivi disciplinari, una dipendente viene invitata a riconsegnare il computer e il cellulare aziendali
- la dipendente viene successivamente licenziata per giusta causa
- a seguito di alcune richieste di accesso ai dati personali e sensibili memorizzati nelle dotazioni informatiche, presentate al proprio ex datore di lavoro, la dipendente presenta ricorso al Garante della Privacy, per ottenere accesso ai dati conservati nei *device* aziendali



- **il Garante della Privacy riconosce il diritto della ex dipendente ad accedere ai dati personali memorizzati nei *device* aziendali riconsegnati**
- **l'ex datore di lavoro aveva provveduto a salvare i dati presenti nei *device* in apposite copie di *back-up*, conservate presso l'azienda e il cui accesso era sotto controllo**
- **il datore di lavoro propone la presa visione del contenuto dei *device* in presenza dell'ex dipendente, del responsabile HR, del responsabile IT e del responsabile dell'area in cui lavorava la ex dipendente**
- **il Garante della Privacy considera questo un procedimento rispettoso dei principi in materia di privacy e, pur riconoscendo il diritto ex art.7, Codice della Privacy all'ex dipendente, non rileva profili di illiceità nel comportamento del datore di lavoro**

Le conseguenze della violazione di legge nello svolgimento di verifiche e perizie: le limitazioni nell'utilizzabilità in giudizio dei dati

La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (art. 160 Codice della Privacy)

L'utilizzabilità delle prove, raccolte in violazione del Codice della Privacy, nel **processo civile** è tendenzialmente **permessa**

L'utilizzabilità delle prove, raccolte in violazione del Codice della Privacy, nel **processo del lavoro** è tendenzialmente **vietata**

Le conseguenze della violazione di legge nello svolgimento di verifiche e perizie: le sanzioni

Sanzioni

- In caso di trattamenti effettuati in assenza di adeguata informativa ai dipendenti, può essere applicata **una sanzione da Euro 6.000 euro a 36.000**

- In caso di trattamenti effettuati in violazione dei principi generali in materia di privacy, tra cui la proporzionalità, la liceità, la correttezza e la trasparenza, può essere applicata **una sanzione da Euro 10.000 a 120.000**

aspetti penali

Le violazioni degli artt. 4 e 8, Statuto Lavoratori, sono punite con l'ammenda da Euro 154 a Euro 1.549 e/o l'**arresto** da 15 giorni a un anno