Ius Laboris Italy Global HR Lawyers
Toffoletto De Luca Tamajo

IMPIANTI AUDIOVISIVI ED ALTRI STRUMENTI DI CONTROLLO. LA RIFORMA DELL'ART. 4 DELLO STATUTO DEI LAVORATORI: ASPETTI GIUSLAVORISTICI E TUTELA DELLA PRIVACY

26 settembre 2016

UNIONE DEGLI INDUSTRIALI DELLA PROVINCIA DI VARESE

Avv.ti Prof. Andrea Morone - Marco Sideri

IL POTERE DI CONTROLLO

Il potere del datore di lavoro di esercitare un controllo sul lavoratore è insito

- nel potere direttivo (art. 2104 cod. civ.)
- nel potere disciplinare (art. 2106 cod. civ.)
- nella definizione di subordinazione (art. 2094 cod. civ.)

IL POTERE DI CONTROLLO

Si contrappongono:

- l'esigenza e il potere di esercitare un controllo da parte del datore di lavoro

- il diritto del lavoratore a vedere tutelata la propria riservatezza e la propria dignità

LE FONTI - LO STATUTO DEI LAVORATORI (LEGGE 300/1970)

- Art. 2 - Guardie giurate
- Art. 3 - Personale di vigilanza
- Art. 4 - Impianti audiovisivi
- Art. 5 - Accertamenti sanitari
- Art. 6 - Visite personali di controllo
- Art. 8 - Divieto di indagini sulle opinioni

LE FONTI - IL CODICE PRIVACY (D.LGS. 196/2003)

- Principio di necessità (art. 3)
- Diritto di accesso (art. 7)
- Liceità / inutilizzabilità (art. 11)
- Informativa (art. 13)
- Consenso (art. 23)
- Eccezioni al consenso (art. 24)

LA PARTICOLARITÀ DEI CONTROLLI A DISTANZA

Diversamente dalle forme di controllo “diretto”, i controlli a distanza possono risultare meno trasparenti perché

- non si sa chi sta controllando
- e non si sa quanto sta controllando

Da qui la maggiore severità della loro disciplina

IL «VECCHIO» ART. 4 STAT. LAV.

«**Impianti audiovisivi.**

È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

[…]»

IL «VECCHIO» ART. 4 STAT. LAV.

- Era un divieto generale di controllo a distanza della prestazione lavorativa
- L'eccezione del secondo comma (c.d. «*controllo preterintenzionale*») non riguardava comunque il controllo della prestazione ma l'istallazione di «*impianti*» e «*apparecchiature*»

L’AVVENTO DELL’INFORMATICA

L’informatica:

- ha reso di uso comune strumenti (computer, smartphone, tablet) che hanno messo in crisi la chiara distinzione tra strumenti di lavoro e strumenti di controllo, che invece era sottintesa all'art. 4
- ha fatto sì che le imprese avessero un interesse specifico a monitorare costantemente i propri sistemi informatici, al fine di verificarne il regolare funzionamento e di evitare intrusioni esterne e quindi a prescindere dal controllo sui lavoratori

IN PRATICA

Il controllo della prestazione era

- vietato
- sempre o spesso possibile anche in ragione del progresso tecnologico
- teoricamente soggetto ad accordo sindacale o ad autorizzazione dell'Ispettorato del Lavoro

Da qui la discussa categoria dei «***controlli difensivi***»

I CONTROLLI “DIFENSIVI”

La categoria del controllo difensivo:

- costituiva una «stampella giurisprudenziale» per una norma difficilmente conciliabile con il progresso tecnologico sui luoghi di lavoro
- si prestava ad alterne pronunce (anche a seconda della gravità della violazione), essendo controversa la necessità dell'autorizzazione sindacale o amministrativa
- presupponeva un controllo solo episodico in relazione ad un fondato sospetto di pericolo per il patrimonio aziendale

L'ASCESA DEI CONTROLLI "DIFENSIVI"

«*Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art.* ***4 legge 300 del 1970****, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o, come nella specie, gli apparecchi di rilevazione di telefonate ingiustificate*»

Cass. 3 aprile 2002, n. 4746

IL LORO DECLINO

«*L'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i c.d. controlli difensivi trovino applicazione le garanzie dell'**art. 4**, **secondo comma, legge 20 maggio 1970 n. 300***»

Cass. 1 ottobre 2012, n. 16622

E LA NUOVA ASCESA

«*I controlli difensivi "occulti" sono tendenzialmente ammissibili in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa restando comunque necessario che le attività di accertamento si esplichino con modalità che contemperino l'interesse del datore al controllo e alla difesa dell'organizzazione con il rispetto delle garanzie di libertà e dignità dei dipendenti, ed in ogni caso rispettino i canoni generali della correttezza e buona fede contrattuale*»

Cass. 27 maggio 2015, n. 10955

UNA RECENTE INTERESSANTE SENTENZA

- Controllare l'attività di un dipendente attraverso l'utilizzo dei *social network* non è attività indirizzata a monitorare la prestazione (art. 4, co. 2 St. lav.) ma può ben essere considerata attività valida al fine di verificare eventuali illeciti posti in essere dal lavoratore.

- Fattispecie concreta: dipendente licenziato perché allontanatosi in maniera prolungata dalla postazione per una telefonata privata, con conseguente mancato pronto intervento; lo stesso intratteneva durante l'orario di lavoro conversazioni personali su Facebook con un falso profilo di donna creato dal datore di lavoro.

(Cass. 27 maggio 2015, n. 10955)

LE MODIFICHE LEGISLATIVE

Una delle deleghe del Jobs Act riguarda la «*revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore*»
(art. 1, comma 7, lett. f, legge delega n. 183/2014)

LA DISCIPLINA - I CONTROLLI A DISTANZA
IL NUOVO ART. 4 STAT. LAV.

Un chiarimento preliminare

Gli strumenti installati esclusivamente a fini di controllo e la sorveglianza esasperati «*dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro*» **era** e **rimane illecita** per contrasto con norme costituzionali che prescindono dall'art. 4 dello Statuto.

Così come continua ad essere illecito l'utilizzo di strumenti che abbiano come unico scopo quello di esercitare un controllo sui lavoratori.

LA NORMA - PRIMO COMMA
(SECONDO COMMA NELLA PRECEDENTE FORMULAZIONE)

«***Impianti audiovisivi e altri strumenti di controllo***

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».

LA NORMA - SECONDO COMMA

«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»

Gli strumenti di cui alla norma sono concetti **inediti** per la legislazione giuslavoristica

e molto attuali (*smart working*, *social network*)

LA NORMA - TERZO COMMA

«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 (Codice Privacy)».

Questi nuovi obblighi si applicano a **ogni** trattamento effettuato dal datore di lavoro sulla base dei controlli

senza *policy* e se non viene rispettata la legislazione sulla *privacy* il trattamento è illegittimo, così come le sue conseguenze

EFFETTI DEL CONTROLLO ILLECITO

Se il controllo avviene in contrasto con l'art. 4

- le sue risultanze non possono essere utilizzate (ad esempio il licenziamento intimato è illecito per insussistenza del fatto contestato)
- ai sensi dell'art. 171 del d.lgs. n. 196/2003 si applicano le sanzioni previste dall'art. 38 Stat. lav. (ammenda da euro 154 a euro 1.549 oppure arresto da 15 giorni ad un anno)
- gli ispettori controllano (e sanzionano) la presenza di sistemi illecitamente attivi (Nota Min. Lavoro, 1 giugno 2016, n. 11241)

IL CAMBIAMENTO: I SOGGETTI

Prima

- Il datore di lavoro
- Le rappresentanze sindacali
- L'Ispettorato del lavoro

Oggi

- Diventa centrale il **lavoratore** al quale occorre fornire «*adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli*»

SEGUE: GLI STRUMENTI

Prima

- «*impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza*»

Oggi

- Si aggiungono gli «*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*»

SEGUE: LA TECNICA LEGISLATIVA

Prima

- Un divieto con eccezioni

Oggi

- La prescrizione di modalità di controllo lecite (che espressamente prevede che i dati raccolti ai sensi dei commi 1 e 2, a determinate condizioni, «*sono utilizzabili a tutti i fini connessi al rapporto di lavoro*»)

SEGUE: LA *PRIVACY*

Prima

- Era il Codice Privacy a richiamare (e confermare) il contenuto dell'articolo 4 dello Statuto dei lavoratori («*Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300*» - art. 114).

Oggi

- È l'articolo 4 a richiamare il rispetto del Codice Privacy come condizione di utilizzabilità dei dati

Che impatto ha sulla produzione regolamentare dell'Autorità Garante?

I CONTROLLI E GLI ACCORDI

- Il controllo a distanza sulla prestazione lavorativa non era previsto

- Ogni accordo relativo ad un potenziale controllo era necessariamente collettivo e a forma vincolata (RSA o DTL)

Gli accordi sottoscritti sono stati negoziati sulla base di una norma che non esiste più

Ora il controllo sulla prestazione lavorativa è possibile relativamente agli «*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*» (art. 4, commi 2 e 3)

MA

- Deve essere preventivamente regolato da una precisa *policy* interna

- Deve rispettare i requisiti della normativa sulla *privacy*

QUINDI

LE POLICY - GLI STRUMENTI DI LAVORO

- Gli strumenti di lavoro
- Le loro caratteristiche
- Il loro utilizzo

vanno individuati e formalizzati

GLI STRUMENTI DI LAVORO

Per essere strumento di lavoro ai sensi della normativa in esame un apparecchio deve:

- essere in relazione diretta con lo svolgimento della prestazione
- essere definito tale in anticipo e secondo procedura
- essere analizzato e descritto in modo trasparente

GLI STRUMENTI DI LAVORO

L'articolo 2, comma 4, è un'**eccezione** alla regola generale

«*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***»

GLI STRUMENTI DI LAVORO

Accordo sindacale e autorizzazione amministrativa non servono

Per gli strumenti:

- **utilizzati dal lavoratore per rendere la prestazione**
- **di registrazione degli accessi e delle presenze**

Il nuovo articolo 4 è la prima norma di legge a **introdurre** queste definizioni

quindi

«*STRUMENTI UTILIZZATI DAL LAVORATORE PER RENDERE LA PRESTAZIONE LAVORATIVA*»

- Lo «*strumento di lavoro*» è inteso in senso oggettivo e in **relazione diretta** con la prestazione
- Non esiste una **definizione univoca** di «*strumento di lavoro*»
- La definizione dipende dall'**attività** del dipendente. Deve trattarsi di uno strumento che serve per svolgere la prestazione lavorativa.

«*STRUMENTI DI REGISTRAZIONE DEGLI ACCESSI E DELLE PRESENZE*»

- Gli strumenti di registrazione di accessi e presenze si devono limitare a registrare **accessi** e **presenze**
- Ogni ulteriore caratteristica non rientra nell'eccezione di cui al comma 2 e quindi le relative ipotesi ricadono nel comma 1

CHI DECIDE COSA È STRUMENTO DI LAVORO?

L'imprenditore

- Fornisce lo strumento
- Dirige la prestazione lavorativa
- Conosce le caratteristiche e le potenzialità di controllo delle apparecchiature di cui dota i suoi dipendenti

e decide cosa inserire nella *policy*

LA POLICY SUGLI STRUMENTI E SUI CONTROLLI

Per gestire in modo efficace la strumentazione fornita ai dipendenti l'imprenditore deve regolamentarla in anticipo:

- nelle procedure aziendali di informazione (art. 4, comma 3)
- sulla base della prestazione resa dai dipendenti
- con una descrizione approfondita degli strumenti e degli apparecchi di rilevazione

Il dipendente deve sapere cosa gli viene fornito e come funzionano gli strumenti

SEGUE…

La *policy* definisce l'ampiezza dei possibili controlli

- Lo strumento deve essere descritto nel suo funzionamento
- Il funzionamento e le caratteristiche devono essere compatibili con la prestazione
- Lo strumento deve essere necessario per lo svolgimento delle mansioni assegnate

Non tutti gli strumenti di lavoro sono utili al **solo** fine di rendere la prestazione

La maggior parte dei moderni strumenti elettronici sono **apparecchi complessi**

LE POLICY - I CONTROLLI

Pertanto i controlli sugli strumenti di lavoro (e sugli altri dispositivi citati nella norma, ad esempio i *badge* di entrata)

vanno previsti e regolamentati

LE POLICY - IPOTESI LEGITTIME DI CONTROLLO

- Controllo sui cellulari aziendali
- Controllo sui PC aziendali
- Controllo sui *tablet* aziendali
- Installazione di impianti audiovisivi sul posto di lavoro ma solo per rilevanti e predeterminate ragioni organizzative e produttive (sicurezza dei dipendenti o tutela del patrimonio aziendale
- Geolocalizzazione, solo nel rispetto dei principi fondamentali in materia di trattamento dei dati personali (il lavoratore deve essere stato informato; la funzione di localizzazione deve essere ben visibile sul cellulare del dipendente)

IPOTESI ILLEGITTIME DI CONTROLLO

- *Smartphone*, PC e tablet privati del dipendente
- *E-mail* private e navigazione internet del dipendente (fatti salvi casi eccezionali «Linee guida del garante Privacy per posta elettronica e internet», marzo 2007)
- Monitoraggio sistematico delle pagine internet visualizzate dal dipendente

IL CONTROLLO SUCCESSIVO E GIUDIZIALE

gli organi ispettivi

in sede di accesso o verifica

il Garante Privacy

in sede di ricorso sull'utilizzo dei dati

il Giudice

in caso di controversia giudiziale

Controllano e giudicano il contenuto degli accordi e delle *policy*

IL «NUOVO» TRATTAMENTO DEI DATI

Il caso:

Non è irragionevole e non viola il diritto al rispetto della vita privata, familiare, del domicilio e della corrispondenza sancito dall'art. 8 della Convenzione, un controllo da parte del datore sullo scopo dell'utilizzo dell'account di messaggistica aziendale, purché sussista una **preventiva informativa** al dipendente sia in merito all'uso **esclusivamente professionale** del mezzo quanto alla **sanzionabilità** dell'impiego per scopi personali.

C.E.D.U. - Sez. IV, 12 gennaio 2016 - Fattispecie di licenziamento motivato dall'uso privato di e-mail aziendale

IL «NUOVO» TRATTAMENTO DEI DATI

La dichiarazione del Garante Privacy:

Si richiede «*al datore di lavoro di informare i lavoratori delle condizioni di utilizzo della mail aziendale (e anche della stessa rete, in orario di lavoro o comunque con gli strumenti messi a disposizione dal datore), dei controlli che il datore di lavoro si riserva di effettuare per fini legittimi, nonché delle eventuali conseguenze disciplinari suscettibili di derivare dalla violazione di tali regole…*»

«*Principi che restano validi anche dopo la riforma dei controlli datoriali operata dal Jobs Act e anche rispetto agli strumenti di lavoro che, pur sottratti alla procedura concertativa, restano comunque soggetti alla disciplina del Codice Privacy. E, in particolare, ai principi di necessità, finalità, legittimità e correttezza, proporzionalità e non eccedenza del trattamento, nonché all'obbligo di previa informativa del lavoratore, ribaditi proprio dalla Corte europea dei diritti umani, con la sentenza di ieri*» (CEDU - Sez. IV, 12 gennaio 2016)

Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali, 13 gennaio 2016

LE PRIME REAZIONI

La giurisprudenza - Il caso

Una lavoratrice con mansioni di segretaria è stata licenziata per giusta causa perché, dalla **cronologia** internet del computer utilizzato per lo svolgimento della prestazione, figuravano 6.000 accessi, negli ultimi 18 mesi lavorativi, a *social network,* giochi, musica ed altre attività **tutte estranee** allo svolgimento dell'attività lavorativa

Tribunale di Brescia, sent. n. 782/2016, pubbl. il 13 giugno 2016, Giudice Dott.ssa Corazza

LE PRIME REAZIONI

La giurisprudenza

Raccogliere dati al fine di verificare l'**utilizzo** di uno **strumento** messo a disposizione dal datore di lavoro per l'esecuzione della prestazione lavorativa non comporta violazione della normativa *privacy* né dell'art. 4 dello Statuto dei Lavoratori, poiché i dati sono ottenuti **senza l'installazione di alcun dispositivo di controllo** e riguardano la verifica di **condotte estranee alla prestazione**, non della produttività e dell'efficienza nello svolgimento della prestazione lavorativa

Tribunale di Brescia, sent. n. 782/2016, pubbl. il 13 giugno 2016, Dott.ssa Corazza

LE PRIME REAZIONI

Il Garante Privacy

«*Le nuove norme vanno interpretate alla luce del principio di proporzionalità riaffermato di recente dalla Corte europea dei diritti dell'uomo rispetto al controllo della mail aziendale in orario di lavoro. La Corte ha ribadito che i controlli datoriali sono ammissibili soltanto se strettamente proporzionati e non eccedenti lo scopo di verifica dell'adempimento contrattuale, limitati nel tempo e nell'oggetto, previsti da preventive policy aziendali, mirati, mai massivi, e fondati su precisi presupposti».*

Relazione 2015 - Discorso del Presidente Antonello Soro
«La protezione dei dati - diritto di libertà», 28 giugno 2016

LE PRIME REAZIONI

Il Garante Privacy

«*La possibilità del controllo dell'adempimento della prestazione, mediante gli strumenti "di lavoro", diverrebbe in tal modo "effetto naturale del contratto", in senso civilistico, in quanto finirebbe con il discendere naturalmente dalla costituzione del rapporto di lavoro*».

Audizione del Presidente Antonello Soro presso la Commissione Lavoro della Camera dei Deputati (9 luglio 2015) e del Senato (14 luglio 2015) sugli schemi di decreti legislativi attuativi del c.d. Jobs Act (ripresi nella Relazione sull'Attività del 2015 del Garante Privacy)

LE PRIME REAZIONI

Il Garante Privacy - il caso:

I dipendenti di un Ateneo hanno lamentato il controllo a distanza posto in essere dall'ente universitario e la conseguente violazione della propria privacy, in assenza di un'adeguata informativa. L'Ateneo ha risposto che l'attività di monitoraggio delle comunicazioni elettroniche era attivata saltuariamente e solo in caso di rilevamento di software maligno e di violazioni del diritto d'autore o di indagini della magistratura.

Provvedimento n. 303 del 13 luglio 2016

LE PRIME REAZIONI

Il Garante Privacy

L'istruttoria del Garante Privacy ha invece evidenziato che i dati così raccolti erano chiaramente riconducibili ai singoli utenti, anche grazie al tracciamento puntuale degli indirizzi Ip (Indirizzo Internet) e dei Mac Address (identificativo hardware) dei pc assegnati ai dipendenti.

I software adottati dall'Ateneo, infatti, consentivano la **verifica costante** e **indiscriminata** degli accessi degli utenti alla rete e all'e-mail.

Provvedimento n. 303 del 13 luglio 2016

LE PRIME REAZIONI

Il Garante Privacy

«*Tali software* ***non possono essere considerati «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa»****. In tale nozione, infatti - e con riferimento agli strumenti oggetto del presente provvedimento, vale a dire servizio di posta elettronica e navigazione web - è da ritenere che possano ricomprendervi solo servizi, software o applicativi* ***strettamente funzionali alla prestazione lavorativa****, anche sotto il profilo della sicurezza […]. Altri strumenti pure utili al conseguimento di un'elevata sicurezza della rete aziendale, invece, non possono normalmente consentire controlli sull'attività lavorativa, non comportando un trattamento di dati personali dei dipendenti, e di conseguenza non sono assoggettati alla disciplina di cui all'art. 4 Stat. lav. Ciò considerato, i sistemi ed applicativi in uso presso l'Università esulano senza dubbio dal perimetro degli «strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa» e comportano, quindi, un trattamento in contrasto con quanto previsto dal predetto art. 4».*

Provvedimento n. 303 del 13 luglio 2016

LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET (DEL. N. 13/2007)

In generale è necessario attenersi ai seguenti principi:

- principio di necessità (i sistemi informativi e i programmi informatici devono essere configurati in modo tale da ridurre al minimo l'utilizzo di dati personali e di dati identificativi)
- principio di correttezza (le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori)
- principio di pertinenza e non eccedenza (il datore di lavoro deve trattare i dati nella misura meno invasiva possibile)

LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET (DEL. N. 13/2007)

Opportunità di dotarsi di un disciplinare interno ("*policy* aziendale"), da pubblicizzare con modalità analoghe al codice disciplinare, nel quale specificare ad esempio:

- i comportamenti non tollerati nell'utilizzo di internet (ad es. il *download* di *software* o di *file* musicali);
- se e in quale misura è consentito utilizzare per ragioni personali internet e la posta elettronica;
- quali informazioni sono memorizzate temporaneamente e chi è legittimato ad accedervi;
- se e in quale misura il datore di lavoro si riserva di effettuare controlli, in conformità della legge, anche al fine di verificare la funzionalità e la sicurezza del sistema e le relative modalità;
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre per l'utilizzo indebito della posta elettronica e di internet;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore.

LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET (DEL. N. 13/2007)

Ad esempio, il Garante ritiene illegittimo il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza mediante:

- lettura e 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*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera.

IMPIANTI DI VIDEOSORVEGLIANZA E GPS: MODULO UNIFICATO ISTANZA DI AUTORIZZAZIONE

- Indicazione della motivazione: esigenze di sicurezza, tutela del patrimonio, esigenze organizzative e/o produttive, “altro” (?)
- indicazione del numero di dipendenti
- eventuale presenza di una rappresentanza sindacale aziendale o mancato raggiungimento di un accordo con le rappresentanze sindacali aziendali

PRIVACY - LA NUOVA NORMATIVA EUROPEA

4 maggio 2016: pubblicati in Gazzetta Ufficiale dell'Unione Europea

- il Regolamento europeo in materia di protezione di dati personali

  Regolamento 2016/679

- la Direttiva europea in materia di trattamento dei dati personali nei settori di prevenzione, contrasto e repressione dei crimini

  Direttiva 2016/680

Le due fonti prevedono un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri UE

LE FONTI

- Il Regolamento sostituisce la Direttiva 95/46/CE relativa alla «*tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*»
- La nuova Direttiva europea sostituisce la Decisione quadro 977/2008/CE «*sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale*»
- In Italia la legislazione corrispondente è attuata nel Codice Privacy

Il Regolamento esiste e sarà direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018

IL DPO

Il Regolamento prevede un nuovo soggetto: il Data Protection Officer o «*Responsabile della protezione dei dati*»

Il DPO (art. 37)

- può essere dipendente o consulente del titolare
- deve in ogni caso essere «*adeguatamente coinvolto*» in tutte le questioni riguardanti la privacy
- riceve le «*risorse necessarie*» e «*nessuna istruzione*» per svolgere i propri compiti
- è il punto di contatto con le autorità di controllo e il consulente del titolare per il trattamento

SEGUE - IL DPO

- può essere unico per un «*gruppo imprenditoriale*» e va valutata la necessità o meno della nomina
- deve essere «*facilmente*» raggiungibile da ciascuno stabilimento (e quindi da ogni dipendente o interessato)
- dovrà possedere qualifiche (formali?), formazione e poteri (effettivi) in materia di protezione dei dati con riferimento a ogni giurisdizione
- si interfaccia con le autorità di controllo

LE SANZIONI

Il Regolamento inasprisce le sanzioni per la violazione delle norme in materia di protezione dei dati e prescrive modalità di trattamento e utilizzo degli stessi

- La protezione dei dati personali deve essere integrata nei sistemi aziendali e connessa ad ogni aspetto del loro utilizzo fino dalla progettazione

- I sistemi aziendali e in generale ogni trattamento di dati deve essere tale da assicurare il rispetto delle norme del Regolamento come default: la garanzia di un trattamento lecito deve essere una caratteristica costante dei sistemi attraverso cui il dato viene trattato e trasmesso

VIOLAZIONI E SANZIONI

Il Regolamento si occupa di definire modalità e requisiti di un trattamento lecito e introduce oneri in capo ai titolari e agli incaricati dello stesso e procedure di reclamo a disposizione dei soggetti

- è sempre possibile proporre reclami e ricorsi giurisdizionali effettivi
- chi subisce danni a causa di violazioni del regolamento ha diritto al risarcimento da titolare e incaricato
- le autorità di controllo possono prescrivere modalità di trattamento e hanno poteri di indagine e verifica

SEGUE - VIOLAZIONI E SANZIONI

In aggiunta alle procedure di reclamo ed indagine il Regolamento prevede «*sanzioni amministrative pecuniarie*» (art. 83)

- regolate e misurate a seconda della gravità e consistenza delle violazioni (inclusi dolo o colpa nel commetterle)
- di misura massima individuata in «*euro 20.000.000*» o, per le imprese, il «*4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*»

I DATI PERSONALI DEI DIPENDENTI

Come nel Codice Privacy in vigore è prevista la possibilità di prevedere «*con legge o tramite contratti collettivi*» norme nazionali specifiche relativamente al rapporto di lavoro (art. 88 e 9, lett. b), in particolare:

- con finalità di assunzione o esecuzione del contratto
- sulla parità e diversità sul posto di lavoro
- circa il trasferimento dei dati personali nell'ambito di un gruppo di imprese
- sui sistemi di monitoraggio sul posto di lavoro

Le normative nazionali devono essere adottate entro il 25 maggio 2018 e ogni «*successiva modifica*» va notificata alla Commissione

PRIVACY - LE NOVITÀ

Ci sono importanti novità legislative che hanno come riferimento la privacy e la modalità di attuazione

- il lavoro agile o «*smart working*» comporta la gestione di dati e strumenti in continuo movimento tra datore di lavoro e dipendente
- l'onere di preventiva regolamentazione di aspetti rilevanti del rapporto di lavoro è oggi esteso a ipotesi diverse e di grande importanza pratica (sicurezza sul lavoro, responsabilità per i reati, controllo a distanza)
- ci sono fattispecie che è possibile regolamentare solo attraverso idonee policy condivise con i dipendenti
- l'utilizzo dei dati rilevati da apparecchiature di controllo e strumenti di lavoro è condizionato al «*rispetto di quanto disposto*» dal Codice Privacy (art. 4 l. 300/1970)

CHE FARE

- verificare i flussi di dati, la gestione e la relativa divisione dei compiti tra funzioni aziendali
- valutare quali sono gli strumenti in uso presso la Società e il loro funzionamento
- redigere policy adeguate ed efficaci
- verificare la relazione tra le procedure in essere, anche a livello di Gruppo
- valutare l'impatto dei futuri adempimenti in materia di protezione dei dati personali in termini di costi e organizzazione

GRAZIE