AIDP
ASSOCIAZIONE ITALIANA PER LA DIREZIONE DEL PERSONALE
Lombardia

Deloitte. Legal

Il controllo dei lavoratori e la tutela della privacy: internet, posta elettronica e social network.

Esigenze di controllo e diritto alla riservatezza dei lavoratori. Come agire correttamente in base alla normativa vigente ed alle modifiche dell'art. 4 dello statuto dei lavoratori, alla luce del jobs act.

Tipologia di controlli pre e post-assunzione che possono essere effettuati sul candidato/dipendente, alla luce della normativa GDPR e giuslavoristica.

Milano, 12 novembre 2021

Avv. Luca Failla
Head of Employment & Benefit
Deloitte Legal Italy

LA GESTIONE DEL PERSONALE ALLA LUCE DELLE ULTIME NOVITÀ NORMATIVE – 2021

STRUMENTI DI LAVORO, TECNOLOGIA E CONTROLLI DATORIALI

I TEMI PIÙ CALDI

QUALI SCENARI DEL FUTURO DEL LAVORO?

GLI INTERROGATIVI PIÙ FREQUENTI

- **Quali saranno i lavori del futuro?**
- **Dove ci sta portando la tecnologia?**
- **Come bilanciare il *diritto alla riservatezza* del lavoratore con l'obiettivo di efficienza/produttività/controllo aziendale ?**
- **Quali i *confini* del controllo datoriale in un contesto di continuo progresso tecnologico?**

LE ULTIMISSIME NOVITA' E I CASI PIU' ECLATANTI già implementati dalle aziende…

Amazon brevetta un braccialetto elettronico: così controllerà merce e dipendenti

Trasmette gli ordini al polso dei lavoratori pronti a scattare per la consegna. Ma sorgono dubbi sulla privacy

Amazon, l'algoritmo gestisce il lavoro: proiettori per smistare merci e gilet coi sensori anche in Italia

Visita a uno dei centri distributivi più evoluti del colosso americano. Brady: «Abbiamo messo a punto un gilet attrezzato con sensori che, una volta indossato, fa sì che gli scaffali si muovano tenendo una distanza di sicurezza dal lavoratore»

IL LAVORO NELLA «GIG ECONOMY»

«Noi, schiavi di un algoritmo per guadagnare 800 euro al mese»

Dipendere da un algoritmo. Cosa ci dice il caso Foodora sul futuro del nostro lavoro

La proposta della Cgil: l'algoritmo di Deliveroo e Foodora crea discriminazioni, contrattiamolo

Amazon, "dipendenti licenziati in base all'algoritmo che misura la produttività"

Il sito americano The Verge pubblica la lettera di un avvocato della società che ammette come sia una macchina a generare "automaticamente eventuali avvisi o risoluzioni riguardanti la qualità o la produttività". In base ai "tassi di produttività" siano stati licenziati "centinaia di lavoratori" dello stabilimento di Baltimora, negli Stati Uniti.

Il sito americano rivela che tra agosto 2017 e settembre 2018 in questa struttura Amazon ha licenziato "300 dipendenti" per non aver rispettato le quote di produttività.

A Baltimora lavorano in tutto circa **2.500 impiegati:** vuol dire che in un anno è stato cacciato più del **10% del proprio personale per motivi di produttività**, perché non ha spostato i pacchi abbastanza velocemente.

Facebook in ufficio? Il datore di lavoro potrebbe spiarvi e licenziarvi. Legittimamente

Cassazione: il dipendente può essere "spiato" su Facebook

Il caso: un lavoratore sorpreso lontano dalla "pressa" a utilizzare il proprio cellulare. La sentenza: i controlli 'occulti' aziendali possono essere utilizzati non per controllare l'attività lavorativa ma per smascherare eventuali danni al patrimonio aziendale. Gli accertamenti non devono essere eccessivamente invasivi

Cassazione Lavoro: sì al falso profilo del datore di lavoro su Facebook per accertare l'illecito del dipendente

(Corte di Cassazione Sentenza 27 maggio 2015, n. 10955)

La creazione, da parte di preposto aziendale e per conto del datore di lavoro, di un falso profilo facebook, al fine di effettuare un controllo sull'attività del lavoratore, già in precedenza allontanatosi dalla postazione lavorativa per parlare al cellulare, esula dal divieto di cui all'articolo 4 dello Statuto dei lavoratori, trattandosi di controllo difensivo, volto alla tutela dei beni aziendali.

Nel caso in esame, un operaio è stato licenziato dal proprio datore di lavoro in quanto durante il proprio turno veniva sorpreso a chattare e ad utilizzare facebook.

In particolare, nell'agosto del 2012, il dipendente si era allontanato dal posto di lavoro per una telefonata privata di circa 15 minuti che gli aveva impedito di intervenire prontamente su di una pressa, bloccata da una lamiera, che era rimasta incastrata nei meccanismi; nello stesso giorno era stato trovato, nel suo armadietto aziendale, un dispositivo elettronico acceso e in collegamento con la rete elettrica e, nei giorni successivi, in orari di servizio, si era intrattenuto con il suo cellulare a conversare su facebook.

Licenziata per un post su Facebook: per la Cassazione è "giusta causa"

Postare una fotografia, un commento, finanche apporre un like, possono divenire motivo di legittima contestazione disciplinare e di licenziamento

Lavoratrice licenziata per aver pubblicato sulla propria bacheca virtuale di Facebook frasi con cui esprimeva il disprezzo per l'azienda presso cui era impiegata

«La condotta di postare un commento su Facebook realizza la pubblicizzazione e la diffusione di esso, per la idoneità del mezzo utilizzato a determinare la circolazione del commento tra un gruppo di persone, comunque, apprezzabile per composizione numerica, con la conseguenza che, se, come nella specie, lo stesso è offensivo nei riguardi di persone facilmente individuabili, la relativa condotta integra gli estremi della ***diffamazione*** *e come tale correttamente il contegno è stato valutato in termini di* ***giusta causa*** *del recesso, in quanto idoneo a recidere il* ***vincolo fiduciario*** *nel rapporto lavorativo» (****Cassazione civile, sez. lav., 27 aprile 2018, n. 10280).***

Lavoratore licenziato per aver pubblicato sulla propria bacheca virtuale di Facebook (condividendo il contenuto con «tutti», dunque senza alcun filtro nella selezione della *privacy* del pubblico del post) gravissime offese ed insulti sessisti e diffamatori indirizzati ad un suo collega

«I commenti pubblici su facebook espressi nei confronti di collega di lavoro ed aventi contenuto altamente offensivo, discriminatorio e denigratorio sono astrattamente idonei ad integrare il reato di cui all'art. 595 c.p., ***in ogni caso motivano la decisione datoriale di risolvere il contratto senza preavviso avendo irrimediabilmente inciso sul vincolo fiduciario del rapporto****» (****Tribunale civile di Roma, sez. lav., 8 febbraio 2020, n. 1269)***

Il Tar ha confermato la sospensione del lavoro e della paga nei confronti di un dipendente per aver espresso un giudizio di disvalore attraverso un **like postato su Facebook** ad un articolo contenente pesanti critiche sul suicidio di un detenuto presso la medesima casa circondariale.

*«Il danno all'immagine e alla reputazione del datore di lavoro attraverso l'uso dei social network giustifica l'irrogazione della sanzione disciplinare della sospensione dal lavoro, integrando gli estremi della violazione dell'obbligo di fedeltà e dei principi di correttezza e buona fede nella regolamentazione del rapporto di lavoro» (**TAR Lombardia Milano, Sez. III, Ord. 3 marzo 2016, n. 246)***

Post su Facebook contro i diretti superiori e i vertici aziendali: legittimo il licenziamento (*Cassazione civile sez. lav., 13/10/2021, n.27939)*

Offese ai capi su Facebook, scatta il licenziamento. Per la Cassazione è giusto

▲ (reuters)

La sentenza spiega che il post pubblico, a differenza della chat privata, è sufficiente per ledere il vincolo fiduciario del rapporto di lavoro

Post su Facebook contro i diretti superiori e i vertici aziendali: legittimo il licenziamento (*Cassazione civile sez. lav., 13/10/2021, n.27939)*

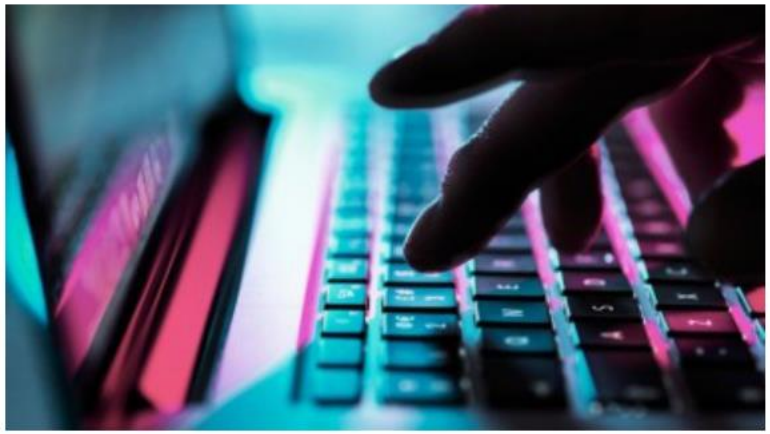
- La pubblicazione di un post sul profilo personale di *Facebook* è idonea a determinare la circolazione del messaggio tra un gruppo indeterminato di persone
- Confermata dunque la decisione della Corte di Appello di Roma che, nel novembre 2018, ribadendo il contenuto gravemente offensivo e sprezzante (nei confronti dei superiori e degli stessi vertici aziendali) delle dichiarazioni, espresse a mezzo di tre e-mails e di un messaggio pubblicato, nell'ottobre del 2016, su *Facebook* respingeva il ricorso presentato dal lavoratore avverso il suo licenziamento per giusta causa, a nulla rilevando che la pubblicazione del *post* fosse destinata alla comunicazione esclusiva con i propri «amici»
- A detta della Corte, infatti, tali dichiarazioni integrerebbero **insubordinazione grave** e, in ogni caso, giusta causa di licenziamento in ragione del loro carattere plurioffensivo e dell'idoneità delle stesse a precludere «*la proseguibilità del rapporto, per l'elisione del legame di fiducia tra le parti, anche considerato il ruolo aziendale del predetto addetto*».

LA POLICY AZIENDALE AFFISSA IN UN ESPOSITORE ACCANTO AL DISTRIBUTORE DEL CAFFÈ E PUBBLICATA NELL' «INTRANET» AZIENDALE CONSENTE AL DATORE DI LAVORO DI UTILIZZARE LE INFORMAZIONI RACCOLTE MEDIANTE APPARECCHIATURE UTILIZZATE DAI DIPENDENTI A FINI DISCIPLINARI

(Tribunale Venezia 6 agosto 2021, n. 494)

NEW

FIRSTNet
SecurityConsulting



Notizie

LICENZIATO IL DIPENDENTE CHE NAVIGANDO SU SITI NON SICURI CAUSA UN ATTACCO INFORMATICO

Autore / Fonte: FIRSTNet/ilSole24Ore (21/09/2021)

LA POLICY AZIENDALE AFFISSA IN UN ESPOSITORE ACCANTO AL DISTRIBUTORE DEL CAFFÈ E PUBBLICATA NELL' «INTRANET» AZIENDALE CONSENTE AL DATORE DI LAVORO DI UTILIZZARE LE INFORMAZIONI RACCOLTE MEDIANTE APPARECCHIATURE UTILIZZATE DAI DIPENDENTI A FINI DISCIPLINARI

(Tribunale Venezia 6 agosto 2021, n. 494)

- All'esito del controllo effettuato su tutti i PC aziendali da un consulente informatico e da un'agenzia investigativa è emerso che il dipendente aveva fatto «*uso intenso del pc a fini personali mediante memorizzazione di dati personali quali files e foto … nonché accesso ad internet per leggere la posta personale e per interessi privati (tra cui il frequente accesso a vari siti pornografici), accesso a files personali contenuti in chiavette usb e memorie di massa esterne, con conseguente sottrazione di tempo all'attività lavorativa e rischio per la sicurezza informatica*»
- Il Tribunale ha ritenuto che «*il datore di lavoro può utilizzare per fini connessi al rapporto di lavoro le informazioni raccolte mediante le apparecchiature utilizzate dai dipendenti, se sussistono i requisiti espressi dai commi 1 e 2 del predetto art. 4 Stat. Lav.: condizione essenziale, a tal fine, è che venga fornita idonea notizia ai dipendenti circa le modalità di uso degli strumenti di lavoro e di effettuazione dei controlli cd. difensivi, nel rispetto di quanto previsto dal Codice della Privacy*».
- Ritenuto soddisfatto requisito della Policy aziendale depositata in atti e resa nota tramite affissione «*in un espositore accanto al distributore del caffè e anche presente in un'apposita cartella del server aziendale accessibile a tutto il personale*».

LE INFORMAZIONI TRATTE DALLA "CHAT" AZIENDALE, DESTINATA ALLE COMUNICAZIONI DI SERVIZIO DEI DIPENDENTI, COSTITUISCONO UNO STRUMENTO DI LAVORO MA SONO INUTILIZZABILI SENZA ADEGUATA INFORMAZIONE PREVENTIVA

(Cass. 22 settembre 2021, n. 25731)

filodiritto
curiosi per diritto

Dipendenti, offese via social e chat aziendale. Quando il datore di lavoro può licenziare?

LE INFORMAZIONI TRATTE DALLA "CHAT" AZIENDALE, DESTINATA ALLE COMUNICAZIONI DI SERVIZIO DEI DIPENDENTI, COSTITUISCONO UNO STRUMENTO DI LAVORO MA SONO INUTILIZZABILI SENZA ADEGUATA INFORMAZIONE PREVENTIVA

(Cass. 22 settembre 2021, n. 25731)

❑«*La "chat" aziendale, destinata alle comunicazioni di servizio dei dipendenti, è qualificabile come strumento di lavoro ai sensi dell'art. 4, comma 2, st.lav. novellato, essendo funzionale alla prestazione lavorativa, con la conseguenza che le informazioni tratte dalla "chat" stessa, a seguito dei controlli effettuati dal datore di lavoro, sono inutilizzabili in mancanza di adeguata informazione preventiva ex art. 4, comma 3, st.lav.*»

❑Nella specie, la S.C. ha confermato la sentenza di merito che aveva annullato il licenziamento comminato a una lavoratrice - per avere quest'ultima inviato ad una collega, su una "chat" aziendale, messaggi offensivi nei confronti, tra l'altro, di un superiore gerarchico -, sul presupposto che il datore fosse venuto a conoscenza dei messaggi stessi in occasione di un controllo tecnico del quale non era stata data alcuna preventiva comunicazione alla lavoratrice medesima

SI PUÒ ANCORA PARLARE DI CONTROLLI DIFENSIVI CON RIFERIMENTO AI CONTROLLI TECNOLOGICI FINALIZZATI ALLA TUTELA DI BENI ESTRANEI AL RAPPORTO DI LAVORO, PER EVITARE COMPORTAMENTI ILLECITI ?

(Cassazione civ. sez. lav. sentenza 22 settembre 2021, n. 25732)

Lavoro

LICENZIAMENTO

Il controllo difensivo ex post ad opera del datore di lavoro sul PC aziendale

SI PUÒ ANCORA PARLARE DI CONTROLLI DIFENSIVI CON RIFERIMENTO AI CONTROLLI TECNOLOGICI FINALIZZATI ALLA TUTELA DI BENI ESTRANEI AL RAPPORTO DI LAVORO, PER EVITARE COMPORTAMENTI ILLECITI ?

(Cassazione civ. sez. lav. sentenza 22 settembre 2021, n. 25732)

- Licenziamento per giusta causa di una lavoratrice accusata di aver diffuso nella rete aziendale un virus proveniente da un file scaricato da internet sul pc aziendale in dotazione, per motivi personali
- Secondo «*la ricorrente la datrice di lavoro … non avrebbe potuto utilizzare tali dati a fini disciplinari in quanto, in assenza di un'adeguata informazione delle modalità di effettuazione dei controlli, l'ulteriore utilizzo per fini connessi al rapporto di lavoro ne è precluso*»
- La Corte d'Appello di Roma aveva respinto il ricorso della lavoratrice statuendo la non configurabilità della violazione dell'art. 4 Stat. Lav., atteso che il controllo sul computer aziendale si era reso necessario per verificare l'origine del virus che aveva infettato il sistema informatico del datore di lavoro e dunque si trattava di un cd. controllo difensivo
- La Corte di Cassazione ha cassato con rinvio la sentenza del gravame statuendo il seguente principio di diritto: «*Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto. Non ricorrendo le condizioni suddette la verifica della utilizzabilità a fini disciplinari dei dati raccolti dal datore di lavoro andrà condotta alla stregua dell'art. 4 L. n. 300/1970, in particolare dei suoi commi 2 e 3*»

ADOZIONE DI ORDINANZA-INGIUNZIONE PER L'APPLICAZIONE DI UNA SANZIONE AMMINISTRATIVA NEI CONFRONTI DEL COMUNE DI BOLZANO: L'ILLICEITA' DEL TRATTAMENTO DEL DATO PREGIUDICA IL CONTROLLO ANCORCHE' IN PRESENZA DI ACCORDO SINDACALE

(Provvedimento del Garante Privacy n. 190 del 13 maggio 2021)

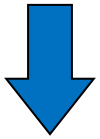
Privacy e GDPR | Privacy e sicurezza

Controlli su navigazione Internet dei dipendenti: Garante Privacy sanziona il comune di Bolzano

ADOZIONE DI ORDINANZA-INGIUNZIONE PER L'APPLICAZIONE DI UNA SANZIONE AMMINISTRATIVA NEI CONFRONTI DEL COMUNE DI BOLZANO: L'ILLICEITA' DEL TRATTAMENTO DEL DATO PREGIUDICA IL CONTROLLO ANCORCHE' IN PRESENZA DI ACCORDO SINDACALE

(Provvedimento del Garante Privacy n. 190 del 13 maggio 2021)

- Il Comune aveva adottato, fin dal 2000, un sistema che consentiva il tracciamento generalizzato (ed ex ante) degli accessi ad Internet da parte dei dipendenti e la memorizzazione, per trenta giorni, di informazioni di natura personale
- Nel corso delle verifiche istruttorie del procedimento era emerso che, sul sito web dell'Ente, non era presente alcuna specifica informativa relativa ai trattamenti dei dati personali dei dipendenti né, in quelle rese disponibili, vi era alcun riferimento al trattamento dei dati personali relativi alla navigazione in Internet da parte degli stessi.
- L'adempimento degli obblighi informativi nei confronti del dipendente (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce una specifica condizione per il lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali (v. art. 4, comma 3, l. 20 maggio 1970, n. 300)

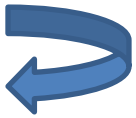


Il Garante ingiunge il Comune al **pagamento della somma di € 84.000,00 a titolo di sanzione amministrativa** pecuniaria per le violazioni degli artt. 5, 6, 9, 88 e 35 del Regolamento, nonché 113 e 114 del Codice

CONTROLLI SUI LAVORATORI
CORTE EUROPEA DEI DIRITTI DELL'UOMO 17 OTTOBRE 2019
(Rìbalda and others c. Spain- n.1874/13 and 8567/13)

La sentenza ha ritenuto legittima l'installazione di telecamere nascoste per controlli difensivi, diretti alla protezione dei beni aziendali :

ammette l'utilizzabilità in giudizio delle *indagini difensive*



NB. Ancora una volta i Giudici di Strasburgo sono stati chiamati a valutare il bilanciamento tra l'interesse alla **privacy dei lavoratori** e interesse del datore di lavoro **alla protezione dei beni aziendali**

PRIVACY E RAPPORTO DI LAVORO

IL NECESSARIO BILANCIAMENTO DEGLI INTERESSI IN GIOCO

PRIVACY E RAPPORTO DI LAVORO

Il bilanciamento necessario…degli interessi in gioco

Diritto alla privacy del lavoratore

Tutela della riservatezza
(Art. 12 Dichiarazione dei Diritti dell'Uomo)
Diritto al rispetto della vita privata e familiare
(Art. 8 Convenzione Europea dei Diritti dell'Uomo)
Divieti di controllo e di indagine sulle opinioni dei lavoratori
(Artt. 2, 3, 4, 5, 6, 8 Statuto dei Lavoratori)

Potere direttivo datoriale

Libera iniziativa economica privata
(Art. 41 Cost.)
Rapporto di subordinazione
(Art. 2094 Cod. Civ.)
Obbligo di diligenza
(Art. 2104 Cod. Civ.)
Obbligo di fedeltà
(Art. 2105 Cod. Civ.)
Potere di controllo a distanza
(Art. 4 Statuto dei Lavoratori)

PRIVACY e STRUMENTI TECNOLOGICI

NUOVI STRUMENTI TECNOLOGICI posti a disposizione dei dipendenti

Di per sé tali strumenti hanno la intrinseca caratteristica di rendere astrattamente possibile un **controllo a distanza** dell'attività lavorativa dei lavoratori (es. accessi internet, siti visitati e relative tempistiche)

Il necessario **bilanciamento** tra diritto alla riservatezza e potere direttivo datoriale (a cui accede il potere di controllo a distanza) si fa ancora più complesso alla luce delle

Quali i punti di caduta e contemperamento degli opposti interessi?

Procedura di consultazione sindacale – amministrativa (art. 4 l. 300/70)

Informativa ex art. 13 GDPR

IL CONTROLLO DEI LAVORATORI E I PROFILI DI PRIVACY

Ogni forma di controllo sui lavoratori/raccolta di dati presuppone, inevitabilmente, il trattamento dei dati personali dei lavoratori stessi. Da ciò deriva l'applicabilità del D.Lgs. n. 196/2003 e dunque l'obbligo di verificare, caso per caso, se lo strumento di controllo sia stato installato e utilizzato anche in conformità delle prescrizioni dettate dal Codice della privacy a pena di…INUTILIZZABILITÀ DEL DATO !

Nel rispetto dei principi generali di liceità, finalità, esattezza, pertinenza, non eccedenza, etc… (cfr. ex art. 11 D.Lgs. n. 196/2003, oggi art. 5 GDPR) e degli adempimenti previsti, quali informativa, consenso, etc…

REVISIONE DELLE INFORMATIVE PRIVACY/RACCOLTA DEL CONSENSO ex art. 13 GDPR

IL DATO PERSONALE E IL TRATTAMENTO

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (cd. «i**nteressato**»), Art. 4 GDPR

Dati sensibili: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, Art. 9 GDPR

Trattamento: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali o insiemi di dati personali, Art. 4 GDPR

es. *raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*

Art. 5 «GDPR»

I CRITERI GUIDA DEL TRATTAMENTO DATI NELL'AMBITO DEL RAPPORTO DI LAVORO

I dati personali devono essere trattati secondo i seguenti principi:

- **liceità, correttezza e trasparenza**;
- **limitazione della finalità** (determinate, esplicite e legittime)
- **minimizzazione dei dati** (adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati)
- **esattezza** (se necessario, devono poter essere aggiornati cancellati o rettificati)
- **limitazione della conservazione (**per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati)
- **integrità e riservatezza** (approntare misure di sicurezza finalizzate alla protezione, da trattamenti non autorizzati/illeciti e dalla perdita/distruzione /danno accidentali)

Art. 6 «GDPR»

Il rapporto di lavoro quale circostanza in cui sussiste un «*legittimo interesse*» al trattamento anche a prescindere dal consenso

Principi guida in materia di liceità del trattamento

Il trattamento è lecito quando:

- l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità
- è **necessario <u>all'esecuzione di un contratto</u> di cui l'interessato è parte**
- è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
- è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica

nel caso del rapporto di lavoro il trattamento avviene in funzione della necessaria esecuzione del contratto… **MA…talvolta è bene raccogliere un espresso consenso**

Art. 9 «GDPR»

Il consenso è necessario per il trattamento di DATI SENSIBILI (cd. «Categorie particolari di dati» nel GDPR)

- È **vietato** trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- Salvo che **l'interessato abbia prestato il proprio CONSENSO esplicito al trattamento di tali dati personali per una o più finalità specifiche**

*«qualsiasi **manifestazione di volontà libera, specifica, informata e inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento»*, *Art. 4 «GDPR»*

PRIVACY E STATUTO DEI LAVORATORI IN TEMA DI CONTROLLI A DISTANZA

Art. 114 D.Lgs. 196/2003

(anche nella formulazione post D.Lgs. 101/2018 attuativo del GDPR)

Garanzie in materia di controllo a distanza

*«Resta fermo quanto disposto dall'**articolo 4 della legge 20 maggio 1970, n.300**»*

Art. 4 L. 300/1970

(…)

Le informazioni raccolte ai sensi del primo e del secondo comma 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 »

ADOZIONE DI ORDINANZA-INGIUNZIONE PER L'APPLICAZIONE DI UNA SANZIONE AMMINISTRATIVA NEI CONFRONTI DEL COMUNE DI BOLZANO: L'ILLICEITA' DEL TRATTAMENTO DEL DATO PREGIUDICA IL CONTROLLO ANCORCHE' IN PRESENZA DI ACCORDO SINDACALE

(Provvedimento del Garante Privacy n. 190 del 13 maggio 2021)

- Il Comune aveva adottato, fin dal 2000, un sistema che consentiva il tracciamento generalizzato (ed ex ante) degli accessi ad Internet da parte dei dipendenti e la memorizzazione, per trenta giorni, di informazioni di natura personale
- Nel corso delle verifiche istruttorie del procedimento era emerso che, sul sito web dell'Ente, non era presente alcuna specifica informativa relativa ai trattamenti dei dati personali dei dipendenti né, in quelle rese disponibili, vi era alcun riferimento al trattamento dei dati personali relativi alla navigazione in Internet da parte degli stessi.
- L'adempimento degli obblighi informativi nei confronti del dipendente (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce una specifica condizione per il lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali (v. art. 4, comma 3, l. 20 maggio 1970, n. 300)

Il Garante ingiunge il Comune al **pagamento della somma di € 84.000,00 a titolo di sanzione amministrativa** pecuniaria per le violazioni degli artt. 5, 6, 9, 88 e 35 del Regolamento, nonché 113 e 114 del Codice

QUALE STRUMENTO CARDINE
PER REALIZZARE IL CONTEMPERAMENTO
DEGLI OPPOSTI INTERESSI COINVOLTI?

LA POLICY o REGOLAMENTO AZIENDALE (2086/2104 c.c.)

… STRUMENTO CON CUI LE AZIENDE POSSONO DARSI LE

«REGOLE DEL GIOCO»

Quale argine alla discrezionalità/incertezza giudiziale

POLICY DATA PRIVACY AZIENDALI

1. ***fissare le MODALITÀ DI UTILIZZO/CONTROLLI degli STRUMENTI TECNOLOGICI***
2. ***prevedere le relative SANZIONI DISCIPLINARI***

- Individuare ad es. la posta elettronica aziendale come uno strumento di lavoro
- utilizzo di internet esclusivamente per fini professionali e non personali
- segnalare le modalità di accesso alla posta elettronica del dipendente in caso di assenza prolungata dello stesso
- segnalare eventuali blocchi di accesso a siti internet
- divieto di *download* di programmi o app esterne salva autorizzazione
- segnalare che l'azienda si riserva di accertare e segnalare eventuali abusi
- menzionare le tempistiche di realizzazione dei controlli a campione (periodicità giornaliera/settimanale/mensile)
- individuare chiaramente la tempistica di conservazione dei dati

WARNING: la violazione delle regole prescritte integra comportamento disciplinarmente sanzionabile ai sensi del Codice disciplinare aziendale con previsione delle specifiche e relative SANZIONI

(*Segue*) LA POLICY O REGOLAMENTO PRIVACY

Il datore di lavoro deve:

- dare al lavoratore adeguata **informazione** delle modalità d'uso degli strumenti e di effettuazione dei controlli (articolo 13 GDPR);

- adottare le misure necessarie a garanzia dei lavoratori riguardanti l'onere di specificare le **modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori medesimi**, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità, vengano effettuati controlli (Provvedimento GPDP 1 marzo 2007);

- adottare un ***disciplinare interno (REGOLAMENTO)*** redatto in modo chiaro e senza formule generiche, da **pubblicizzare** adeguatamente (es. verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico (Provvedimento GPDP 1 marzo 2007).

IL QUADRO NORMATIVO

NORME LAVORISTICHE

NORME PRIVACY

Il quadro normativo generale: la varietà delle fonti normative

- **Costituzione**
  - ✓Art. 2: diritti inviolabili dell'uomo
  - ✓Art. 41: diritto alla libera iniziativa imprenditoriale

- **Codice Civile**
  - ✓Art. 2086: potere gerarchico datoriale
  - ✓Art. 2087: tutela dell'ambiente e delle condizioni di lavoro
  - ✓Art. 2104: obbligo di rispettare direttive dal datore di lavoro

- **Statuto dei Lavoratori (L.300/70)**
  - ✓Art. 2: divieto di controllo delle guardie giurate
  - ✓Art. 3: personale di vigilanza
  - ✓Art. 4: controllo a distanza
  - ✓Art. 5: accertamenti sanitari
  - ✓Art. 6: visite personali di controllo
  - ✓Art. 8: divieto di indagine sulle opinioni
  - ✓Art. 15: divieto di discriminazioni

- **Codice della Privacy**
  - ✓D.Lgs. 196/2003, come oggi modificato dal D.Lgs. 101/2018 a seguito dell'entrata in vigore del Regolamento Europeo 679/2016 (cd. «**GDPR**»)

POTERE DI CONTROLLO E VIGILANZA DEL DATORE DI LAVORO NEL CODICE CIVILE

Art. 2086 c.c. →

Direzione e gerarchia nell'impresa

L'imprenditore è il capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori

Art. 2087 c.c. →

Tutela delle condizioni di lavoro

L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.

OBBLIGHI DEL LAVORATORE NEL CODICE CIVILE

Art. 2104 c.c.

Diligenza del prestatore di lavoro

*Il prestatore di lavoro deve usare la **diligenza** richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.*
Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo o dai quali gerarchicamente dipende

Art. 2105 c.c.

Obbligo di fedeltà

Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio".

Art. 2106 c.c.

Sanzioni disciplinari

"L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo alla applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione".

La Legge 20 maggio 1970, n. 300

LA TUTELA DELLA LIBERTÀ E DELLA DIGNITÀ DEL LAVORATORE

I limiti legali al potere di controllo e vigilanza Artt. 2 e 3 St.Lav.

- **Art 2**:«Il datore di lavoro può impiegare le guardie particolari giurate, di cui agli articoli 133 e seguenti del testo unico approvato con regio decreto 18 giugno 1931, n. 773, soltanto per scopi di tutela del patrimonio aziendale. Le guardie giurate non possono contestare ai lavoratori azioni o fatti diversi da quelli che attengono alla tutela del patrimonio aziendale. E' fatto divieto al datore di lavoro di adibire alla vigilanza sull'attività lavorativa le guardie di cui al primo comma, le quali non possono accedere nei locali dove si svolge tale attività, durante lo svolgimento della stessa, se non eccezionalmente per specifiche e motivate esigenze attinenti ai compiti di cui al primo comma, in caso di inosservanza da parte di una guardia particolare giurata delle disposizioni di cui al presente articolo, l'Ispettorato del lavoro ne promuove presso il questore la sospensione dal servizio, salvo il provvedimento di revoca della licenza da parte del prefetto nei casi più gravi».

- **Art. 3**:«I nominativi e le mansioni specifiche del personale addetto alla vigilanza dell'attività lavorativa debbono essere comunicati ai lavoratori interessati».

I limiti legali al potere di controllo e vigilanza Art. 6 St.Lav.

Art. 6 : «Le visite personali di controllo sul lavoro sono vietate fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti.

In tali casi le visite personali potranno essere effettuate soltanto a condizione che siano eseguite all'uscita dei luoghi di lavoro, che siano **salvaguardate la dignità e la riservatezza del lavoratore** e che avvengano con l'applicazione di sistemi di selezione automatica riferiti alla collettività o a gruppi di lavoratori.

Le ipotesi nelle quali possono essere disposte le visite personali, nonché, ferme restando le condizioni di cui al secondo comma del presente articolo, le relative modalità debbono essere concordate dal datore di lavoro 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»

I limiti legali al potere di controllo e vigilanza Art. 6 St.Lav.

L'Installazione di «totem» (tipo scanner/metal detector) all'ingresso della sede lavorativa per il controllo di oggetti di pertinenza del dipendente (ad esempio, borsa) che accede ai locali di lavoro, finalizzata a proteggere il patrimonio aziendale, è ispezione personale e, dunque, soggiace alla disciplina dell'art. 6 St. Lav.?

Due orientamenti giurisprudenziali:

- il **primo orientamento**, basandosi sulla definizione di "visita personale" ritiene che l'art. 6, Legge n. 300/70, si riferisca solo alle verifiche corporali sul lavoratore (ex plurimis: Cass., Sez. lav., 10.2.1988, n. 1461) così che l'ispezione sulle cose non rientri nella sfera di applicazione delle norme in esame
- il **secondo orientamento** è esattamente opposto e, rifacendosi alla sentenza della Cassazione n. 5902/1984, ritiene che l'art. 6 dello Statuto dei Lavoratori si estende anche a quegli effetti personali (come portafogli, borsette, borselli) che possono essere considerati come diretta pertinenza della persona, ed appartenenti al normale utilizzo di accessori dell'abbigliamento, sulla base delle ordinarie abitudini o mode.

I limiti legali al potere di controllo e vigilanza Art. 6 St.Lav.

Ministero del Lavoro, nota del 8.11.2016 n. 20546

«*L'esecuzione di controlli a campione sul contenuto delle borse di dipendenti e visitatori dei negozi attraverso sistemi di selezione imparziale che rendano causale l'individuazione del soggetto da controllare) può essere effettuata solo in seguito alla procedura di autorizzazione normativamente prevista, ed attraverso opportuni meccanismi di selezione imparziale specificamente richiesti dalla norma e predisposti dall'azienda, in modo da rendere casuale l'individuazione del soggetto da ispezionare*»

I limiti legali al potere di controllo e vigilanza Art. 6 St.Lav.

Le “perquisizioni” devono dunque seguire la procedura autorizzativa ovvero essere oggetto di accordo sindacale e sono consentite solo a patto che:

a) **siano indispensabili ai fini della tutela del patrimonio aziendale**, avuto riguardo a: a) L’intrinseca qualità degli strumenti di lavoro (quali, ad esempio, telefoni cellulari, tablet, personal computers trapani, calibri elettronici, navigatori portatili per autovetture, ecc) o delle materie prime (come, ad esempio, metalli preziosi- rame, argento, oro, platino, o stoffe- seta), o dei prodotti (quali l’elettronica di consumo, l’abbigliamento di sartoria, oppure software, cosmetici e profumi costosi, ecc) b) l’impossibilità di prevenire i furti se non attraverso le perquisizioni personali);

b) **siano eseguite all’uscita dei luoghi di lavoro**;

c) **siano salvaguardate la dignità e riservatezza del lavoratore**

d) **avvengano con l’applicazione di sistemi di selezione automatica riferiti alla collettività o a gruppi di lavoratori**

I limiti legali al potere di controllo e vigilanza Art. 8 St.Lav.

Art. 8: «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**»

Art. 4 S.L. (come sostituito dall'art. 23 D.lgs. 14 settembre 2015, n. 151)

« ***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 disposizione di cui al primo comma ***NON*** *si applica agli strumenti utilizzati dal lavoratore per* ***rendere la prestazione lavorativa*** *e* agli ***strumenti di registrazione degli accessi e delle presenze.***

Le informazioni raccolte ai sensi del primo e del secondo comma ***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 CONTROLLI PRE-ASSUNTIVI

I CONTROLLI PRE-ASSUNTIVI
Il caso: è legittima la richiesta del certificato penale e del certificato dei carichi pendenti prima di assumere un lavoratore?

NOZIONE

Il **certificato penale** è un estratto delle sole registrazioni penali iscritte al casellario giudiziale e contiene la storia delle condanne penali passate in giudicato di un cittadino

Il **certificato dei carichi pendenti** consente la conoscenza dei procedimenti penali in corso a carico di un determinato soggetto e gli eventuali relativi giudizi di impugnazione

I CONTROLLI PRE-ASSUNTIVI
Il caso: è legittima la richiesta del certificato penale e del certificato dei carichi pendenti prima di assumere un lavoratore?

PROBLEMATICHE

Necessità di bilanciare le esigenze del datore di lavoro di valutare l'idoneità del candidato allo svolgimento delle mansioni con i principi dell'ordinamento penalistico a tutela dell'imputato e del condannato in procedimenti penali

- Art. 27 comma 2 Cost.: presunzione di non colpevolezza sino alla condanna definitiva
- Art. 27 comma 3 Cost.: funzione rieducativa e riabilitativa della pena

I CONTROLLI PRE-ASSUNTIVI
Il caso: è legittima la richiesta del certificato penale e del certificato dei carichi pendenti prima di assumere un lavoratore?

DISCIPLINA

- il **certificato penale del casellario giudiziale deve essere richiesto** dal soggetto che intenda impiegare al lavoro una persona per lo svolgimento di attività professionali o attività volontarie organizzate che comportino "contatti diretti e regolari con minori", al fine di verificare l'esistenza di condanne per taluno dei reati di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quinquies e 609-undecies del codice penale, ovvero l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con minori (art. 25bis D.P.R. 313/2020)

I CONTROLLI PRE-ASSUNTIVI
Il caso: è legittima la richiesta del certificato penale e del certificato dei carichi pendenti prima di assumere un lavoratore?

I PRINCIPI DELLA GIURISPRUDENZA

- opera il generale divieto (art. 8 L. 300/1970) in capo al datore di lavoro - perlomeno quello privato - di chiedere carichi pendenti o casellario giudiziale. In casi eccezionali (ad esempio in presenza di lavori particolarmente delicati, soprattutto se implicano rapporti con il pubblico) - disciplinati dai CCNL - il datore di lavoro può chiedere il certificato penale, o casellario giudiziale (**Cassazione n. 19012/18 del 17 luglio 2018**).

I CONTROLLI PRE-ASSUNTIVI
Il caso: è legittima la richiesta del certificato penale e del certificato dei carichi pendenti prima di assumere un lavoratore?

I PRINCIPI DELLA GIURISPRUDENZA

- è pienamente valida - e coerente con l'impianto costituzionale in cui si collocano le imprese che operano in regime di libero mercato - la previsione per cui il processo selettivo finalizzato all'assunzione imponga, tra le altre condizioni, la consegna del certificato di carichi pendenti, anche qualora il CCNL non includa tra i documenti preassuntivi tale certificato. Questo meccanismo selettivo è espressione, ad avviso della Corte, del principio di rango costituzionale della libertà di iniziativa economica, dal quale discende la legittimità di un percorso selettivo che, al fine di permettere la valutazione sull'idoneità del candidato a svolgere le mansioni oggetto del contratto di lavoro, subordini l'assunzione ad appositi adempimenti da parte del candidato (**Cassazione ordinanza n. 17167/2020**).

Il punto di equilibrio tra potere datoriale e riservatezza

IL CONTROLLO A DISTANZA
ART. 4 Statuto dei Lavoratori

IL DIVIETO DI CONTROLLO A DISTANZA
Art. 4 L. n. 300 del 1970

ATTIVITÀ DEI LAVORATORI

Comportamento complessivo tenuto dal lavoratore in azienda, comprendente sia il momento dell'**effettiva prestazione**, sia le "**licenze comportamentali**" (pause)

CONTROLLO A DISTANZA

➢La distanza si riferisce sia alla dimensione **spaziale**, sia a quella **temporale**

➢ È **irrilevante** che il controllo sia **costante** o **discontinuo** (può essere anche ***ex post***) (comma 1)

Esigenze organizzative e produttive o attinenti alla sicurezza

L'apparecchiatura deve essere strettamente **necessaria per lo svolgimento dell'attività produttiva**

Possibilità di controllo a distanza

Il controllo deve essere **"preterintenzionale":** conseguente, cioè, ad una funzione accessoria ed ineliminabile dell'apparecchiatura (comma 2)

IL DIVIETO DI CONTROLLO A DISTANZA
Art. 4 L. n. 300 del 1970

Controllo diretto:

Si realizza attraverso l'installazione di strumenti finalizzati unicamente al controllo a distanza sull'attività lavorativa dei dipendenti.

Tale tipologia di controllo è sempre vietata

Controllo «preterintenzionale:

Quando gli strumenti pur se installati in presenza di:

i) esigenze di carattere organizzativo produttivo;

ii) di sicurezza sul lavoro;

iii) o tutela del patrimonio aziendale

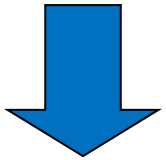
rendano comunque possibile un controllo a distanza sull'attività dei dipendenti.

Tale tipologia di controllo è legittima se:

- (Profilo sostanziale) Istallazione risponda ad esigenze di carattere organizzativo e produttivo o per la sicurezza o tutela patrimonio;
- (Profilo Procedurale) sia stata autorizzata tramite accordo sindacale o in mancanza provvedimento ITL.

IL DIVIETO DI CONTROLLO DEI LAVORATORI: ***RATIO***

Scopo primario del titolo I dello Statuto dei lavoratori, intitolato «*della libertà e dignità del lavoratore*», è quello di **impedire che l'inserzione all'interno dell'apparato produttivo si traduca nella compromissione dei diritti fondamentali della persona**.



Ciò è confermato dalla **Relazione ministeriale** che chiarisce che "*la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, va[da] mantenuta in una dimensione «umana» e cioè non esasperata 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".* (Senato della Repubblica, V legislatura, doc. 738, 2).

Art. 4 S.L. precedente alla riforma

*« **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 la Direzione Territoriale del Lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.*
Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, la Direzione Territoriale del Lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.
Contro i provvedimenti della DTL, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale»

Art. 4 S.L. (come sostituito dall'art.23 D.lgs. 14 settembre 2015, n. 151)

*« **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 disposizione di cui al primo comma non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
Le informazioni raccolte ai sensi del primo e del secondo comma 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 »

Art. 4 S.L. (come sostituito dall'art. 23 D.lgs. 14 settembre 2015, n. 151)

« ***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 disposizione di cui al primo comma ***NON*** *si applica agli strumenti utilizzati dal lavoratore per* ***rendere la prestazione lavorativa*** *e* agli **strumenti di registrazione degli accessi e delle presenze.**

Le informazioni raccolte ai sensi del primo e del secondo comma ***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* »

La nuova disposizione prevede che gli strumenti di controllo a distanza, dai quali derivi anche la possibilità di controllo dei lavoratori, possono essere installati esclusivamente:

- per esigenze organizzative e produttive
- per la sicurezza del lavoro
- ***LA TUTELA DEL PATRIMONIO AZIENDALE***

1. NOVITÀ IN SINTESI

COSA CAMBIA? → Anche i "controlli difensivi" volti alla tutela del patrimonio aziendale dovranno necessariamente passare, pena l'inutilizzabilità dalla procedura autorizzativa ex art. 4 St. Lav. ?

2. NOVITÀ IN SINTESI

- In 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.
- Confermata **l'autorizzazione della Direzione Territoriale del Lavoro** in mancanza di accordo. Nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, competenza del Ministero del lavoro e delle politiche sociali.

N.B. La gestione delle pratiche in materia di videosorveglianza è in carico alla Direzione Generale della tutela delle condizioni di lavoro e delle relazioni industriali (***Nota della Direzione Generale per l'Attività Ispettiva n. 3500 del 22 febbraio 2016***).

3. NOVITÀ IN SINTESI

❑**Legittimo impiego <u>senza</u> necessità di accordo sindacale o autorizzazione amministrativa.:**

1. **degli strumenti ad uso del lavoratore** per *"rendere la prestazione lavorativa*",

e

2. degli **strumenti di registrazione degli accessi e delle presenze**

❑Utilizzazione dei dati raccolti per **(tutte le !)** finalità inerenti al rapporto di lavoro (e quindi <u>anche</u> **fini disciplinari**)

❑Obbligo di rispetto della disciplina in materia di **privacy** con la necessità di (ri)**dare al lavoratore adeguata informazione** delle modalità d'uso degli strumenti e di effettuazione dei controlli **(informativa privacy e rispetto dei principi di necessità, pertinenza, finalità, correttezza, non eccedenza**

Sindacato del giudice del lavoro in caso di contenzioso

Inutilizzabilità del dato raccolto

QUESTIONI APERTE

❑**Ampia utilizzabilità dei dati raccolti anche sul piano disciplinare**

1. come cambia il contenuto dei **nuovi accordi** ex art. 4;
2. cosa succede agli **accordi già stipulati**;

❑Autorizzazioni ex DTL già in essere: quale sorte? Nuove autorizzazioni: quali contenuti ? Opposizioni ancora possibili ?

❑**Strumenti di lavoro**: cosa si intende per **strumenti** utilizzati dal lavoratore *"**per rendere la prestazione lavorativa**"*;

❑**Strumenti di registrazione degli accessi e delle presenze**: cosa si intende (es. *badge, sistemi di accesso alle aree, aree di parcheggio*):

❑ **controlli difensivi :** sono ancora possibili ?

PROCEDURA:
ACCORDO SINDACALE O AUTORIZZAZIONE ITL/MINISTERO

CONDIZIONI DI LEGITTIMITÀ: ACCORDO O AUTORIZZAZIONE

Il nuovo art. 4, comma 1, Stat. Lav.

«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 PROCEDURA PER L'INSTALLAZIONE (ADEMPIMENTI DEL DATORE DI LAVORO)

❑ **ACCORDO SINDACALE**

A tale fine è sufficiente la sottoscrizione da parte dellE RSU o delle RSA

in difetto di accordo

❑ **AUTORIZZAZIONE ITL**

La procedura di autorizzazione da parte dell'ITL all'installazione degli impianti di controllo a distanza dell'attività dei lavoratori deve concludersi entro il **termine di 60 giorni (DPCM 22 DICEMBRE 2010 N. 275);**

nel caso di imprese con unità dislocate in territori che sarebbero di competenza di diverse Direzioni territoriali

❑ **AUTORIZZAZIONE MINISTERO DEL LAVORO**

IL CONSENSO ORALE O SCRITTO DELLA TOTALITÀ DEI LAVORATORI NON BASTA

*«È da ritenere **penalmente illecita**, ai sensi dell'art. 4 l. n. 300 del 1970, l'installazione di impianti audiovisivi o di altri strumenti dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori quando essa **non** sia stata **preceduta da un apposito accordo** con le rappresentanze sindacali o, in mancanza, da una autorizzazione della competente Direzione territoriale del lavoro*
*… **a nulla rilevando** al contrario che, in luogo dell'accordo o dell'autorizzazione, sia stato acquisito **il consenso, orale o anche scritto, della totalità dei lavoratori interessati**»* **(Cassazione penale sez. III, 06/11/2019, n. 1733)**

è rivisto il precedente orientamento per cui l'accordo della totalità dei lavoratori era ritenuto sufficiente quale scriminante…

L'installazione nel luogo di lavoro di un sistema di videosorveglianza mediante telecamere (c.d. controlli a distanza) non costituisce reato, ai sensi del combinato disposto degli art. 4 e 38 legge n. 300/1970 (Statuto dei lavoratori), laddove, pur in assenza di autorizzazione sindacale e di autorizzazione della DTL, risulti **comprovato l'assenso all'installazione da parte della totalità dei lavoratori dell'azienda** (Cass. 17.4.2012, n. 22611, conf. Cass. 12.11.2013, n. 4331)

ECCEZIONI ALLA STIPULAZIONE DELL'ACCORDO: GLI STRUMENTI DI LAVORO

Art. 4 l. 300/70
(come sostituito dall'art. 23 D.lgs. 14 settembre 2015, n. 151)

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 disposizione di cui al primo comma ***NON*** *si applica agli strumenti utilizzati dal lavoratore per* ***rendere la prestazione lavorativa*** *e* agli **strumenti di registrazione degli accessi e delle presenze.**

Le informazioni raccolte ai sensi del primo e del secondo comma ***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* »

ECCEZIONI ALL'ACCORDO O AUTORIZZAZIONE: GLI STRUMENTI DI LAVORO

La disposizione di cui al 1 comma non si applica agli

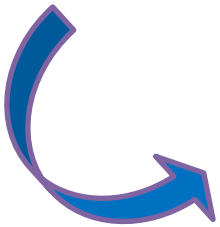
*1. strumenti utilizzati dal lavoratore **per rendere la prestazione lavorativa,** e*

*2. strumenti di registrazione degli **accessi** e delle **presenze***

1. STRUMENTI IN DOTAZIONE AL DIPENDENTE

Strumenti informatico/tecnologici in dotazione al dipendente *per* ***RENDERE*** *la prestazione lavorativa*:

Pc, notebook, smartphone, blackberry, ecc. ⟶ strumenti di universale applicazione necessitati dalla moderna organizzazione del lavoro ma non certo "*strumenti di controllo*" a distanza per i quali occorre avviare procedure applicative o sindacali



TALI STRUMENTI POTRANNO ESSERE UTILIZZATI/IMPEGATI DAI DIPENDENTI SENZA DOVER ACCEDERE AD UN ACCORDO SINDACALE OVVERO A PREVENTIVA AUTORIZZAZIONE AMMINISTRATIVA

N.B. L'assenza di autorizzazione non fa venir meno il rispetto dei principi generali in tema di tutela della privacy nonché gli obblighi di corretta informazione al lavoratore in ordine ai rischi di controllo

GLI STRUMENTI DI LAVORO : COME IDENTIFICARLI CORRETTAMENTE ?

- ***PERSONAL COMPUTER: inclusi software applicativi; mail; internet?***
- ***LAPTOP***
- ***TABLET inclusivo di software e applicativi***
- ***SMARTPHONE***
- ***AUTO AZIENDALE: telepass, sistema di geolocalizzazione satellitare (GPS)***
- ***DRONI***
- ***ALTRO ?***

LA CORRETTA IDENTIFICAZIONE DEGLI STRUMENTI DI LAVORO

Il criterio guida per capire se sussista un controllo?

Nota ministero del lavoro 18 giugno 2015

«*nel momento in cui* ***lo strumento in dotazione viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione*** «***per rendere la prestazione lavorativa***»*: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione –> legittimi solo alle condizioni di cui all'art. 4*».

PROVA NEGATIVA PER SOTTRAZIONE

Valutare la **funzionalizzazione specifica** dello strumento all'attività lavorativa e se questo si ponga in **rapporto di univoca e teleologica necessità** con la stessa… se così non è sussiste una finalità «altra» di controllo…

2. BADGE E STRUMENTI DI ACCESSO AL LUOGO DI LAVORO

Strumenti di registrazione degli accessi e delle presenze (es. *badge, sistemi di accesso alle aree, aree di parcheggio*):

TALI STRUMENTI POTRANNO ESSERE UTILIZZATI SENZA DOVER ACCEDERE AD UN ACCORDO SINDACALE OVVERO A PREVENTIVA AUTORIZZAZIONE AMMINISTRATIVA

N.B. L'assenza di preventiva autorizzazione/accordo non fà venir meno il rispetto dei principi generali in tema di tutela della privacy nonché gli obblighi di corretta informazione al lavoratore in ordine ai rischi di controllo.

Anzi… la partita domani si sposta sul terreno della privacy.

UTILIZZABILITÁ DEI DATI RACCOLTI: ANCHE A FINI DISCIPLINARI !!

Il nuovo art. 4, comma 3, Stat. Lav.

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

Cosa cambia: negli accordi ex art. 4 non potrà più essere utilizzata la formula secondo cui i dati raccolti **NON** potevano essere utilizzate ai fini disciplinari ….

E I VECCHI ACCORDI EX ART. 4 L. 300/70 GIA FIRMATI CHE LA VIETAVANO CHE FINE FANNO ?

IL CONTROLLO DEI LAVORATORI E I PROFILI DI PRIVACY

Ogni forma di controllo sui lavoratori/raccolta di dati presuppone, inevitabilmente, il trattamento dei dati personali dei lavoratori stessi. Da ciò deriva l'applicabilità del D.Lgs. n. 196/2003 (come modificato dal D.Lgs. n. 101/2018 di adeguamento al GDPR, Regolamento UE 679/2016) e dunque l'obbligo di verificare, caso per caso, se lo strumento di controllo sia stato installato e utilizzato anche in conformità delle prescrizioni dettate dal Codice della privacy

…A PENA DI…

INUTILIZZABILITÀ DEL DATO «*a tutti i fini connessi al rapporto di lavoro*» e, quindi, **anche ai fini disciplinari e sanzionatori**

Nel rispetto dei principi generali di liceità, finalità, esattezza, pertinenza, non eccedenza, etc… (cfr. ex art. 11 D.Lgs. n. 196/2003, oggi art. 5 GDPR) e degli adempimenti previsti, quali informativa, consenso, etc…

REVISIONE DELLE INFORMATIVE PRIVACY/RACCOLTA DEL CONSENSO ex art. 13 GDPR

Alcune definizioni in termini di PRIVACY …

IL DATO PERSONALE E IL TRATTAMENTO

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (cd. «i**nteressato**»), Art. 4 GDPR

Dati sensibili: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, Art. 9 GDPR

Trattamento: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali o insiemi di dati personali, Art. 4 GDPR

es. *raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*

Art. 5 «GDPR»

I CRITERI GUIDA DEL TRATTAMENTO DATI NELL'AMBITO DEL RAPPORTO DI LAVORO

I dati personali devono essere trattati secondo i seguenti principi:

- **liceità, correttezza e trasparenza**;
- **limitazione della finalità** (determinate, esplicite e legittime)
- **minimizzazione dei dati** (adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati)
- **esattezza** (se necessario, devono poter essere aggiornati cancellati o rettificati)
- **limitazione della conservazione (**per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati)
- **integrità e riservatezza** (approntare misure di sicurezza finalizzate alla protezione, da trattamenti non autorizzati/illeciti e dalla perdita/distruzione /danno accidentali)

Art. 6 «GDPR»

Il rapporto di lavoro quale circostanza in cui sussiste un «*legittimo interesse*» al trattamento anche a prescindere dal consenso

Principi guida in materia di liceità del trattamento

Il trattamento è lecito quando:

- l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità
- è **necessario <u>all'esecuzione di un contratto</u> di cui l'interessato è parte**
- è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
- è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica

nel caso del rapporto di lavoro il trattamento avviene in funzione della necessaria esecuzione del contratto… **MA…talvolta è bene raccogliere un espresso consenso**

Art. 9 «GDPR»

Il consenso è necessario per il trattamento di DATI SENSIBILI (cd. «Categorie particolari di dati» nel GDPR)

- È **vietato** trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- Salvo che **l'interessato abbia prestato il proprio CONSENSO esplicito al trattamento di tali dati personali per una o più finalità specifiche**

*«qualsiasi **manifestazione di volontà libera, specifica, informata e inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento», Art. 4 «GDPR»*

PRIVACY E STATUTO DEI LAVORATORI IN TEMA DI CONTROLLI A DISTANZA

Art. 114 D.Lgs. 196/2003

(anche nella formulazione post D.Lgs. 101/2018 attuativo del GDPR)

Garanzie in materia di controllo a distanza

*«Resta fermo quanto disposto dall'**articolo 4 della legge 20 maggio 1970, n.300**»*

Art. 4 L. 300/1970

(…)

Le informazioni raccolte ai sensi del primo e del secondo comma 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 »

LA POLICY AZIENDALE AFFISSA IN UN ESPOSITORE ACCANTO AL DISTRIBUTORE DEL CAFFÈ E PUBBLICATA NELL' «INTRANET» AZIENDALE CONSENTE AL DATORE DI LAVORO DI UTILIZZARE LE INFORMAZIONI RACCOLTE MEDIANTE APPARECCHIATURE UTILIZZATE DAI DIPENDENTI A FINI DISCIPLINARI

(Tribunale Venezia 6 agosto 2021, n. 494)

- All'esito del controllo effettuato su tutti i PC aziendali da un consulente informatico e da un'agenzia investigativa è emerso che il dipendente aveva fatto «*uso intenso del pc a fini personali mediante memorizzazione di dati personali quali files e foto … nonché accesso ad internet per leggere la posta personale e per interessi privati (tra cui il frequente accesso a vari siti pornografici), accesso a files personali contenuti in chiavette usb e memorie di massa esterne, con conseguente sottrazione di tempo all'attività lavorativa e rischio per la sicurezza informatica*»
- Il Tribunale ha ritenuto che «*il datore di lavoro può utilizzare per fini connessi al rapporto di lavoro le informazioni raccolte mediante le apparecchiature utilizzate dai dipendenti, se sussistono i requisiti espressi dai commi 1 e 2 del predetto art. 4 Stat. Lav.: condizione essenziale, a tal fine, è che venga fornita idonea notizia ai dipendenti circa le modalità di uso degli strumenti di lavoro e di effettuazione dei controlli cd. difensivi, nel rispetto di quanto previsto dal Codice della Privacy*».
- Ritenuto soddisfatto requisito della Policy aziendale depositata in atti e resa nota tramite affissione «*in un espositore accanto al distributore del caffè e anche presente in un'apposita cartella del server aziendale accessibile a tutto il personale*».

SANZIONI

VIOLAZIONE DELL'ART. 4 ST.LAV.

I controlli a distanza del datore di lavoro sull'attività lavorativa sono leciti solo se conformi a:

- Art. 4 comma 2 Statuto dei lavoratori (accordo con RSA/RSU o autorizzazione ITL/min. Lavoro)
- Disciplina legge sulla privacy

In caso di violazione: quali conseguenze?

- **Profilo «processuale»**: inutilizzabilità (ANCHE AI FINI DISCIPLINARI) del dato acquisito dal datore di lavoro attraverso gli accertamenti svolti sul lavoratore

- **Profilo "sindacale"**: condotta antisindacale (art. 28 St. Lav.)

- **Profilo «civilistico»**: responsabilità civile nei confronti dei lavoratori interessati

- **Profilo «penale»:** responsabilità penale (art. 38 St. Lav. e art. 171 D.Lgs.196/2003 – ammenda da 154 Euro a 1.549 Euro, oppure arresto da 15 giorni ad 1 anno – possibile oblazione *ex* art. 162 bis c.p.).

1. INUTILIZZABILITÀ DEL DATO ACQUISITO
Giurisprudenza

«*Un'apparecchiatura di controllo predisposta per il vantaggio dei dipendenti, ma utilizzabile anche in funzione di controllo dell'osservanza da parte di questi dei loro doveri di diligenza nel rispetto dell'orario di lavoro e della stessa correttezza della esecuzione della prestazione lavorativa, (…) non era stata concordata con le rappresentanza sindacali, né era stata autorizzata dall'Ispettorato del Lavoro.*

Posto che il riferimento all'attività lavorativa, oggetto della fattispecie astratta, non riguarda solo le modalità del suo svolgimento, ma anche il quantum della prestazione, il controllo sull'orario di lavoro, risolvendosi in un accertamento circa la quantità di lavoro svolto, si inquadra, per ciò stesso, in una tipologia di accertamento pienamente rientrante nella fattispecie prevista dal secondo comma dell'articolo 4.

Per tale ragione il controllo operato è stato effettuato illegittimamente e quindi i risultati non possono essere posti a fondamento dell'intimato licenziamento» (***Cass. 17 Luglio 2007 n. 15892***)

2. INUTILIZZABILITÀ DEL DATO ACQUISITO
Giurisprudenza

«***Non può essere attribuito alcun valore probatorio ai dati acquisiti in violazione dell'art. 4 S.L. che sono dunque inutilizzabili in causa*** *(nella fattispecie il datore di lavoro aveva licenziato una lavoratrice sulla base di dati raccolti mediante un controllo dei collegamenti e dei siti internet in via continuativa con strumenti informatici centralizzati – cd. SUPER SCOUT-, non accessibili al lavoratore, e aveva conservato la registrazione dei dati per un certo periodo di tempo)»* (***Corte d'Appello di Milano, 30 settembre 2005 n. 668***)

«*Costituisce strumento di controllo "preterintenzionale" a distanza dell'attività dei lavoratori,* ***soggetto alla disciplina dell'art. 4 comma 2 l. n. 300 del 1970****,* ***un'apparecchiatura di rilevamento delle presenze attivata mediante tessera magnetica (badge*** *), sicché, in caso di mancato esperimento della procedura di cui all'art. 4 comma 2 St. lav., non sono utilizzabili in sede disciplinare i dati acquisiti tramite la stessa» (****Trib. Napoli 29 settembre 2010; contra Trib. Napoli 23 settembre 2010****)*

3. INUTILIZZABILITÀ DEL DATO ACQUISITO
Giurisprudenza

«*Viola la normativa sulla privacy il datore di lavoro che controlla il dipendente disponendone il pedinamento e l'accesso all'account di posta elettronica senza dare atto delle ragioni e delle effettive modalità del controllo. Non può essere configurato come legittimo ai sensi dell'art. 4, comma 2 st. lav. il controllo effettuato sull'account email del dipendente in assenza dell'adeguata informazione prevista dall'art. 4, comma 3 st. lav. Le predette violazioni comportano l'inammissibilità delle risultanze ottenute dai controlli occulti e, dunque, l'inutilizzabilità delle informazioni acquisite*» (***Tribunale Milano, 13 maggio 2019, n. 17778***)

ADOZIONE DI ORDINANZA-INGIUNZIONE PER L'APPLICAZIONE DI UNA SANZIONE AMMINISTRATIVA NEI CONFRONTI DEL COMUNE DI BOLZANO: L'ILLICEITA' DEL TRATTAMENTO DEL DATO PREGIUDICA IL CONTROLLO ANCORCHE' IN PRESENZA DI ACCORDO SINDACALE

(Provvedimento del Garante Privacy n. 190 del 13 maggio 2021)

- Il Comune aveva adottato, fin dal 2000, un sistema che consentiva il tracciamento generalizzato (ed ex ante) degli accessi ad Internet da parte dei dipendenti e la memorizzazione, per trenta giorni, di informazioni di natura personale
- Nel corso delle verifiche istruttorie del procedimento era emerso che, sul sito web dell'Ente, non era presente alcuna specifica informativa relativa ai trattamenti dei dati personali dei dipendenti né, in quelle rese disponibili, vi era alcun riferimento al trattamento dei dati personali relativi alla navigazione in Internet da parte degli stessi.
- L'adempimento degli obblighi informativi nei confronti del dipendente (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce una specifica condizione per il lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali (v. art. 4, comma 3, l. 20 maggio 1970, n. 300)

Il Garante ingiunge il Comune al **pagamento della somma di € 84.000,00 a titolo di sanzione amministrativa** pecuniaria per le violazioni degli artt. 5, 6, 9, 88 e 35 del Regolamento, nonché 113 e 114 del Codice

IN CONCLUSIONE….

Per poter essere utilizzati dal datore di lavoro i dati e/o le informazioni riguardanti i dipendenti devono essere stati:

- ✓ **raccolti lecitamente (accordo ex art. 4 l.300/70 ovvero autorizzazione ispettorato o Ministero) ovvero in alternativa derivanti da *badge/accessi presenze* o da strumenti di lavoro**

- ✓ **trattati lecitamente ex GDPR Privacy (informativa e consenso se dovuto, correttezza, continenza etc)**

IN DIFETTO DI UNA DI QUESTE CONDIZIONI IL DATO È INUTILIZZABILE

I cd. «CONTROLLI DIFENSIVI» IN TEMA DI

- VIDEOSORVEGLIANZA
- INTERNET
- POSTA ELETTRONICA AZIENDALE

I cd. «Controlli difensivi»

categoria di matrice giurisprudenziale finalizzata a legittimare:

- ✓ controlli finalizzati all'accertamento di **comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa** (Cass. 4746/2002, Cass. 2722/2012)
- ✓ controlli ammessi nel caso di già accertato verificarsi dell'illecito, ma anche in ragione del **solo sospetto** o della **mera ipotesi** che tali illeciti siano in corso di esecuzione (Cass. 4984/2014)
- ✓ per giurisprudenza maggioritaria, preferibilmente ammissibili i controlli ***ex post*** a fronte della sussistenza di **elementi indiziari** circa la commissione di illecito (da ultimo Cass. 13266/2018)
- ✓ controlli da realizzarsi con modalità **non eccessivamente invasive** e **rispettose delle garanzie di libertà e dignità dei dipendenti** (Cass. 10955/2015)

Siamo **fuori** dall'ambito di applicazione dell'art. **4 St. Lav.**

non è necessaria **autorizzazione** sindacale/amministrativa

QUALE SORTE PER I CONTROLLI DIFENSIVI?

❑Se prima della riforma la giurisprudenza consentiva con difficoltà il "superamento" della procedura sindacale/autorizzazione in tutti i casi in cui i controlli – anche occulti – fossero diretti ad accertare NON l'esatto adempimento della prestazione bensì **comportamenti illeciti e lesivi del patrimonio e dell'immagine aziendale**

(ipotesi non tipizzata dal legislatore)

dopo il Jobs Act

❑La **tutela del patrimonio aziendale** rientra tra le ipotesi tassative in cui poter installare strumenti di controllo…

previo accordo sindacale con le RSA/RSU/autorizzione ITL

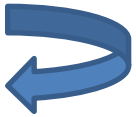
(ipotesi tipizzata dal legislatore - art. 4, comma 1)

***conseguenze*: quale spazio per i controlli difensivi oggi ?**

CONTROLLI SUI LAVORATORI
CORTE EUROPEA DEI DIRITTI DELL'UOMO 17 OTTOBRE 2019
(RÌBALDA AND OTHERS C. SPAIN- N.1874/13 AND 8567/13)

…. la Corte ha osservato che non vi era alcuna violazione dell'art. 8, ovvero al diritto della vita privata e familiare in considerazione delle seguenti circostanze :

a)l'area ricoperta dalla riprese (limitata alla casse e zone limitrofe e non a spogliatoi e bagni);
b)periodo di tempo delle riprese attive (10 giorni);
c)finalità delle riprese (esclusivamente diretta alla documentazione degli atti illeciti);
d)inesistenza di altri strumenti di controllo alternativi, ma meno invasivi



La Corte ha superato **l'assenza della preventiva informazione in relazione alle telecamere nascoste,** aderendo altresì alla impostazione dei Giudici nazionali, che avevano riconosciuto che la mancata informazione sulle telecamere non pregiudica la possibilità di valutare proporzionato il trattamento, valutato alla luce del quadro complessivo.

(SEGUE) CONTROLLI SUI LAVORATORI
CORTE EUROPEA DEI DIRITTI DELL'UOMO 17 OTTOBRE 2019
(RÌBALDA AND OTHERS C. SPAIN- N.1874/13 AND 8567/13)

Utilizzabilità in giudizio delle prove: anche in caso in violazione della disciplina della protezione dei dati?

La Cedu, nella sentenza in esame statuisce che le telecamere nascoste non hanno violato l'articolo 6 della convenzione Europea dei Diritti dell'uomo, intitolata al diritto a un equo processo, basate su prove legittimamente formate.
La sentenza nega la violazione dell'articolo 6 se al lavoratore sia data la possibilità di contestarne l'autenticità delle immagine e, comunque, di presentare opposizioni (come nel caso di specie era avvenuto).

(SEGUE) CORTE EUROPEA DEI DIRITTI DELL'UOMO 17 OTTOBRE 2019 (DICHIARAZIONE DI ANTONELLO SORO, PRESIDENTE DEL GARANTE PER LA PRIVACY)

LA SORVEGLIANZA OCCULTA NON DIVENTI PRASSI ORDINARIA)

« La sentenza della Grande Camera della Corte di Strasburgo se da una parte giustifica, nel caso di specie, le telecamere nascoste, dall'altra conferma però **il principio di proporzionalità** *come requisito essenziale di legittimazione dei controlli in ambito lavorativo.*

L'installazione di telecamere nascoste sul luogo di lavoro è stata infatti ritenuta ammissibile dalla Corte solo perché, nel caso che le era stato sottoposto, ricorrevano determinati presupposti: vi erano ***fondati e ragionevoli sospetti*** *di furti commessi dai lavoratori ai danni del patrimonio aziendale, l'area oggetto di ripresa (peraltro aperta al pubblico) era alquanto circoscritta, le videocamere erano state in funzione per un periodo temporale limitato, non era possibile ricorrere a mezzi alternativi e le immagini captate erano state utilizzate soltanto a fini di prova dei furti commessi* (…)

CONTROLLO POSTA E PC AZIENDALE

CORTE EUROPEA DEI DIRITTI DELL'UOMO 12 gennaio 2016 (Barbulescu c. Romania)

La sentenza ha ritenuto legittimo il controllo del datore di lavoro sull'account e-mail del lavoratore poiché:

a. Vi era una policy interna che vietava l'utilizzo a fini personali degli strumenti di lavoro aziendali;

b. Vi era stata una informativa da parte del datore di lavoro riguardo al controllo effettuato sulle mail/posta ecc..

c. Il controllo era stato effettuato nell'ambito di un procedimento disciplinare e il lavoratore aveva affermato di aver utilizzato la posta solo a fini professionali.

CORTE EUROPEA DEI DIRITTI DELL'UOMO 5 SETTEMBRE 2017 (BARBULESCU V. ROMANIA)

A distanza di un anno, la **Grand Chambre della Corte** ha riformato la prima decisione del 2016 ed ha **ritenuto illegittimo il controllo del datore sull'account e-mail del lavoratore** ritenendo invece

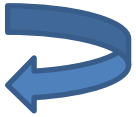
violazione dell'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza).

ed in particolare …

CORTE EUROPEA DEI DIRITTI DELL'UOMO 5 SETTEMBRE 2017 (BARBULESCU V. ROMANIA)

…. la Corte ha osservato che i Giudici Nazionali rumeni **non avevano adeguatamente tutelato il diritto al rispetto della vita privata e della corrispondenza del lavoratore,** non avendo accertato:

a.se il lavoratore avesse ricevuto preventivamente l'avviso da parte del suo datore di lavoro della possibilità che le sue comunicazioni potessero essere monitorate;
b.se egli fosse stato **informato** della natura e/o della portata della monitoraggio, e/o del grado di intrusione nella sua vita personale e nella sua corrispondenza;
c.la sussistenza di ragioni specifiche a giustificazione dell'introduzione di misure di controllo e/o se potevano esistere misure di controllo meno invasive nella vita personale e nella corrispondenza.



in sintesi, **come prescrive anche il riformato art. 4, ultimo comma dello Statuto**, **la società avrebbe dovuto comunicare anticipatamente le forme modalità di esecuzione del controllo delle comunicazioni del lavoratore al fine di evitare violazioni della privacy.**

CONTROLLO PC AZIENDALE

6000 ACCESSI IN RETE IN 18 MESI, DEI QUALI BEN 4500 SOLO SU FACEBOOK DURANTE L'ORARIO DI LAVORO, COSTITUISCONO GIUSTA CAUSA DI LICENZIAMENTO (*TRIBUNALE DI BRESCIA SENTENZA N. 782/2016)*

*il datore di lavoro si è **limitato a stampare la cronologia** ed il **tipo di accesso ad internet** dal computer della dipendente, il che non richiede l'installazione di alcun dispositivo di controllo, né implica la violazione della privacy, trattandosi di dati che vengono registrati da qualsiasi computer e che sono stati stampati al solo fine di verificare l'utilizzo di uno strumento messo a disposizione dal datore di lavoro per l'esecuzione della prestazione.*

***Né può ipotizzarsi una violazione dell'art. 4 della legge n. 300 del 1970**, trattandosi di attività di controllo non della produttività ed efficienza nello svolgimento dell'attività lavorativa, ma attinenti a **condotte estranee alla prestazione**"*

LA POLICY AZIENDALE AFFISSA IN UN ESPOSITORE ACCANTO AL DISTRIBUTORE DEL CAFFÈ E PUBBLICATA NELL' «INTRANET» AZIENDALE CONSENTE AL DATORE DI LAVORO DI UTILIZZARE LE INFORMAZIONI RACCOLTE MEDIANTE APPARECCHIATURE UTILIZZATE DAI DIPENDENTI A FINI DISCIPLINARI

(Tribunale Venezia 6 agosto 2021, n. 494)

- All'esito del controllo effettuato su tutti i PC aziendali da un consulente informatico e da un'agenzia investigativa è emerso che il dipendente aveva fatto «*uso intenso del pc a fini personali mediante memorizzazione di dati personali quali files e foto … nonché accesso ad internet per leggere la posta personale e per interessi privati (tra cui il frequente accesso a vari siti pornografici), accesso a files personali contenuti in chiavette usb e memorie di massa esterne, con conseguente sottrazione di tempo all'attività lavorativa e rischio per la sicurezza informatica*»
- Il Tribunale ha ritenuto che «*il datore di lavoro può utilizzare per fini connessi al rapporto di lavoro le informazioni raccolte mediante le apparecchiature utilizzate dai dipendenti, se sussistono i requisiti espressi dai commi 1 e 2 del predetto art. 4 Stat. Lav.: condizione essenziale, a tal fine, è che venga fornita idonea notizia ai dipendenti circa le modalità di uso degli strumenti di lavoro e di effettuazione dei controlli cd. difensivi, nel rispetto di quanto previsto dal Codice della Privacy*».
- Ritenuto soddisfatto requisito della Policy aziendale depositata in atti e resa nota tramite affissione «*in un espositore accanto al distributore del caffè e anche presente in un'apposita cartella del server aziendale accessibile a tutto il personale*».

LE INFORMAZIONI TRATTE DALLA "CHAT" AZIENDALE, DESTINATA ALLE COMUNICAZIONI DI SERVIZIO DEI DIPENDENTI, COSTITUISCONO UNO STRUMENTO DI LAVORO MA NON SONO UTILIZZABILI SENZA ADEGUATA INFORMAZIONE PREVENTIVA

(Cass. 22 settembre 2021, n. 25731)

- «*La "chat" aziendale, destinata alle comunicazioni di servizio dei dipendenti, è qualificabile come strumento di lavoro ai sensi dell'art. 4, comma 2, st.lav. novellato, essendo funzionale alla prestazione lavorativa, con la conseguenza che le informazioni tratte dalla "chat" stessa, a seguito dei controlli effettuati dal datore di lavoro, sono inutilizzabili in mancanza di adeguata informazione preventiva ex art. 4, comma 3, st.lav.*»

- Nella specie, la S.C. ha confermato la sentenza di merito che aveva annullato il licenziamento comminato a una lavoratrice - per avere quest'ultima inviato ad una collega, su una "chat" aziendale, messaggi offensivi nei confronti, tra l'altro, di un superiore gerarchico -, sul presupposto che il datore fosse venuto a conoscenza dei messaggi stessi in occasione di un controllo tecnico del quale non era stata data alcuna preventiva comunicazione alla lavoratrice medesima

LICENZIAMENTO PER GIUSTA CAUSA DI UNA LAVORATRICE ACCUSATA DI AVER DIFFUSO NELLA RETE AZIENDALE UN VIRUS PROVENIENTE DA UN FILE SCARICATO DA INTERNET SUL PC AZIENDALE IN DOTAZIONE, PER MOTIVI PERSONALI

"Sono utilizzabili a fini disciplinari i dati informatici risultanti dal controllo sul computer aziendale del dipendente, controllo indotto dalla necessità di verificare l'origine di un virus che aveva infettato il sistema informatico datoriale"

La Corte d'Appello di Roma ha affermato la legittimità del controllo da parte del datore di lavoro del personal computer della dipendente in quanto questo è avvenuto non durante lo svolgimento dell'attività lavorativa ma *ex post* e quale effetto indiretto di operazioni tecniche condotte su strumenti di lavoro appartenenti al datore di lavoro e finalizzate all'indifferibile ripristino del sistema informatico aziendale. In tale quadro di riferimento perde quindi ogni importanza **l'eccepita inutilizzabilità probatoria di controparte dei dati informatici acquisiti.** ***(Corte di Appello di Roma, 22/03/2019, n.1331)***

SI PUÒ ANCORA PARLARE DI CONTROLLI DIFENSIVI CON RIFERIMENTO AI CONTROLLI TECNOLOGICI FINALIZZATI ALLA TUTELA DI BENI ESTRANEI AL RAPPORTO DI LAVORO, PER EVITARE COMPORTAMENTI ILLECITI ?

(Cassazione civ. sez. lav. sentenza 22 settembre 2021, n. 25732)

❑Licenziamento per giusta causa di una lavoratrice accusata di aver diffuso nella rete aziendale un virus proveniente da un file scaricato da internet sul pc aziendale in dotazione, per motivi personali

❑Secondo «*la ricorrente la datrice di lavoro … non avrebbe potuto utilizzare tali dati a fini disciplinari in quanto, in assenza di un'adeguata informazione delle modalità di effettuazione dei controlli, l'ulteriore utilizzo per fini connessi al rapporto di lavoro ne è precluso*»

❑La Corte d'Appello di Roma aveva respinto il ricorso della lavoratrice statuendo la non configurabilità della violazione dell'art. 4 Stat. Lav., atteso che il controllo sul computer aziendale si era reso necessario per verificare l'origine del virus che aveva infettato il sistema informatico del datore di lavoro e dunque si trattava di un cd. controllo difensivo

❑La Corte di Cassazione ha cassato con rinvio la sentenza del gravame statuendo il seguente principio di diritto: «*Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto. Non ricorrendo le condizioni suddette la verifica della utilizzabilità a fini disciplinari dei dati raccolti dal datore di lavoro andrà condotta alla stregua dell'art. 4 L. n. 300/1970, in particolare dei suoi commi 2 e 3*»

QUANDO LE INFORMAZIONI SONO RACCOLTE ED UTILIZZATE LEGITTIMAMENTE AI FINI DISCIPLINARI?

1. **Rispetto dell'art. 4 s.l. = accordo sindacale/autorizzazione ITL che legittima raccolta e utilizzo informazioni**

2. **Dati raccolti mediante strumento di lavoro/registrazione presenze o accesso**

3. **trattamento dei dati raccolti conforme al GDPR (informativa etc.)**

4. **siamo in presenza di un *controllo difensivo* che giustifica la raccolta dei dati anche al di fuori dell'art. 4 s.l.**

107

INTERNET E
POSTA ELETTRONICA AZIENDALE

CONTROLLO POSTA e PC AZIENDALE

Cassazione civile, sez. lav., 10/11/2017, n. 26682

Caso: legittimo il controllo della **posta elettronica aziendale** di un dipendente accusato di aver inviato una serie di e-mail contenenti **espressioni scurrili** nei confronti del legale rappresentante della società

*«la **duplicazione periodica dei dati contenuti nei computer aziendali**, preventivamente nota ai dipendenti, esula dal campo di applicazione dell'art. 4, comma 2, st.lav., se effettuata a **tutela di beni estranei al rapporto di lavoro**, quali **l'immagine dell'azienda e la tutela della dignità di altri lavoratori**, e non riguardi l'esatto adempimento delle obbligazioni discendenti dal rapporto stesso»* (*Idem* Cassazione civile, sez. lav., 23/02/2012, n. 2722 nel caso di divulgazione di notizie riservate)

Cassazione civile, sez. lav., 28/05/2018, n. 13266

Caso: legittimo controllo del **PC aziendale** per accertare **attività extra-lavorative** (dipendente sorpreso giocare al PC)

«*esulano dall'ambito di applicazione dell'art. 4, comma 2, st.lav. i **controlli difensivi** da parte del datore se diretti ad accertare comportamenti illeciti e lesivi del patrimonio e dell'immagine aziendale, **tanto più se disposti "ex post**", ossia **dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa***

CONTROLLO PC AZIENDALE

NELL'ARCO DI SOLI DUE MESI LO STESSO DIPENDENTE AVEVA EFFETTUATO BEN 27 CONNESSIONI, DELLA DURATA COMPLESSIVA DI 45 ORE (*CASS. 15 GIUGNO 2017, N. 14862)*

NON sussiste una violazione della normativa sulla privacy: la società si era limitata a verificare l'esistenza di accessi indebiti alla rete ed i relativi tempi di collegamento, **senza compiere alcuna analisi dei siti visitati** dal dipendente durante la navigazione o della **tipologia dei dati scaricati**;

I «*dettagli del traffico*» NON costituiscono «dati personali»**, non contenendo alcun riferimento alla persona dell'utente, alle sue scelte o attitudini politiche, religiose, culturali, sessuali;

NON sussistono i presupposti del controllo a distanza della prestazione lavorativa di cui allo Statuto dei Lavoratori, che si concreta solo nell'attività che ha ad oggetto la prestazione lavorativa e il suo esatto adempimento, **restando del tutto esclusa dal campo di applicazione della norma quella attività che sia volta ad individuare la realizzazione di comportamenti illeciti da parte del dipendente**, idonei a ledere l'integrità del patrimonio aziendale e la sicurezza degli impianti.

CONTROLLO PC AZIENDALE

6000 ACCESSI IN RETE IN 18 MESI, DEI QUALI BEN 4500 SOLO SU FACEBOOK DURANTE L'ORARIO DI LAVORO, COSTITUISCONO GIUSTA CAUSA DI LICENZIAMENTO (*TRIBUNALE DI BRESCIA SENTENZA N. 782/2016)*

*il datore di lavoro si è **limitato a stampare la cronologia** ed il **tipo di accesso ad internet** dal computer della dipendente, il che non richiede l'installazione di alcun dispositivo di controllo, né implica la violazione della privacy, trattandosi di dati che vengono registrati da qualsiasi computer e che sono stati stampati al solo fine di verificare l'utilizzo di uno strumento messo a disposizione dal datore di lavoro per l'esecuzione della prestazione.*

***Né può ipotizzarsi una violazione dell'art. 4 della legge n. 300 del 1970**, trattandosi di attività di controllo non della produttività ed efficienza nello svolgimento dell'attività lavorativa, ma attinenti a **condotte estranee alla prestazione**"*

CONTROLLO PC AZIENDALE

“Sono utilizzabili a fini disciplinari i dati informatici risultanti dal controllo sul computer aziendale del dipendente, controllo indotto dalla necessità di verificare l'origine di un virus che aveva infettato il sistema informatico datoriale”

La Corte d’Appello di Roma ha affermato la legittimità del controllo da parte del datore di lavoro del personal computer della dipendente in quanto questo è avvenuto non durante lo svolgimento dell’attività lavorativa ma *ex post* e quale effetto indiretto di operazioni tecniche condotte su strumenti di lavoro appartenenti al datore di lavoro e finalizzate all’indifferibile ripristino del sistema informatico aziendale. In tale quadro di riferimento perde quindi ogni importanza **l’eccepita inutilizzabilità probatoria di controparte dei dati informatici acquisiti.** ***(Corte di Appello di Roma, 22/03/2019, n.1331)***

TUTTAVIA...
Un orientamento più stringente …

Cassazione 23.02.2010 n. 4375

Caso «Super Scout»

In tema di controllo del lavoratore, i programmi informatici che consentono il ***monitoraggio della posta elettronica e degli accessi ad 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, anche in relazione al rispetto delle direttive aziendali che limitano le connessioni telematiche predette per finalità personali; ne consegue che* ***i dati acquisiti da tali programmi****, ove per gli stessi non siano rispettate le condizioni legittimanti di cui all'art. 4 comma 2 l. n. 300 del 1970 (quali l'accordo con le rappresentanze sindacali o la commissione interna o, in mancanza, l'autorizzazione dell'ispettorato del lavoro),* ***non sono utilizzabili nel procedimento disciplinare*** *instaurato nei confronti del lavoratore in relazione a violazioni disciplinari emergenti da tali dati*

CONTROLLO POSTA E PC AZIENDALE

CORTE EUROPEA DEI DIRITTI DELL'UOMO 12 gennaio 2016 (Barbulescu c. Romania)

La sentenza ha ritenuto legittimo il controllo del datore di lavoro sull'account e-mail del lavoratore poiché:

a. Vi era una policy interna che vietava l'utilizzo a fini personali degli strumenti di lavoro aziendali;

b. Vi era stata una informativa da parte del datore di lavoro riguardo al controllo effettuato sulle mail/posta ecc..

c. Il controllo era stato effettuato nell'ambito di un procedimento disciplinare e il lavoratore aveva affermato di aver utilizzato la posta solo a fini professionali.

CORTE EUROPEA DEI DIRITTI DELL'UOMO 5 SETTEMBRE 2017 (BARBULESCU V. ROMANIA)

A distanza di un anno, la **Grand Chambre della Corte** ha riformato la prima decisione del 2016 ed ha **ritenuto illegittimo il controllo del datore sull'account e-mail del lavoratore** ritenendo invece

violazione dell'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza).

ed in particolare …

CORTE EUROPEA DEI DIRITTI DELL'UOMO 5 SETTEMBRE 2017 (BARBULESCU V. ROMANIA)

…. la Corte ha osservato che i Giudici Nazionali rumeni **non avevano adeguatamente tutelato il diritto al rispetto della vita privata e della corrispondenza del lavoratore,** non avendo accertato:

a.se il lavoratore avesse ricevuto preventivamente l'avviso da parte del suo datore di lavoro della possibilità che le sue comunicazioni potessero essere monitorate;
b.se egli fosse stato **informato** della natura e/o della portata della monitoraggio, e/o del grado di intrusione nella sua vita personale e nella sua corrispondenza;
c.la sussistenza di ragioni specifiche a giustificazione dell'introduzione di misure di controllo e/o se potevano esistere misure di controllo meno invasive nella vita personale e nella corrispondenza.

in sintesi, **come prescrive anche il riformato art. 4, ultimo comma dello Statuto**, **la società avrebbe dovuto comunicare anticipatamente le forme modalità di esecuzione del controllo delle comunicazioni del lavoratore al fine di evitare violazioni della privacy.**

GPS

LOCALIZZAZIONE GPS LECITA

Cassazione 12 ottobre 2015, n. 20440

CASO: **legittimo il licenziamento** disciplinare irrogato al coordinatore di altri dipendenti addetti alla nettezza urbana in vari comuni per aver sostato al bar **oltre il limite delle pause dal lavoro**.
In particolare, il licenziamento era stato intimato in base agli elementi acquisiti in esito alle indagini di investigatori privati, nonché ai rilevamenti di un sistema satellitare GPS installato sull'autovettura affidatagli per l'esecuzione della prestazione lavorativa.

La Cassazione ha ritenuto che i controlli di cui sopra debbano considerarsi quali "***controlli difensivi",*** cioè intesi a rilevare mancanze specifiche dei lavoratori e **comportamenti degli stessi estranei alla normale attività lavorativa**. Tali controlli sono eseguibili anche mediante agenzie investigative private.

LOCALIZZAZIONE GPS ILLECITA !

Cassazione 5 ottobre 2016, n. 19922

CASO: contestato di aver registrato nel rapporto di giro alcune ispezioni che in realtà non erano state effettuate perché il veicolo risultava altrove nell'orario indicato, come rivelato nel sistema satellitare GPS installato nella vettura.

La Corte di Cassazione, confermando la sentenza di II grado, ha ribadito ha confermato **l'illegittimità dei controlli** di cui sopra effettuati in violazione della legge e dell'art. 4 L.300, nonché la loro conseguente **inutilizzabilità** come fonti di prova di inadempimento contrattuale.

La Cassazione ha affermato che il GPS, siccome consentirebbe un controllo quasi illimitato sui lavoratori, ben oltre l'ordinaria attività lavorativa, non può essere considerato come uno strumento finalizzato alla tutela del patrimonio e dell'immagine aziendale, venendo così meno la nozione di "controllo difensivo".

VIDEOSORVEGLIANZA

VIDEOSORVEGLIANZA E FURTI

Cassazione penale, sez. III, 10/10/2017, n. 4564

Caso: sottrazione di documentazione aziendale e **violazione della riservatezza**

*«Pur volendo astrattamente ammettere l'esigenza del controllo difensivo dedotto, resta il fatto che la telecamera era stata incontestabilmente collocata nel condizionatore posto all'interno dell'ufficio ove la lavoratrice lavorava in solitudine e che le riprese ne avevano **leso la riservatezza**, avendo la donna riferito che in quel periodo, poiché infortunata al ginocchio, molto spesso doveva applicare una pomata»*

VIDEOSORVEGLIANZA E FURTI

Cassazione civile, sez. lav., 08/11/2016, n. 22662

Caso: furto del dipendente dalla **cassaforte aziendale**

*«non è soggetta alla disciplina dell'art. 4, comma 2, St. Lav., l'installazione di impianti ed apparecchiature di controllo poste a tutela del patrimonio aziendale dalle quali **non derivi anche la possibilità di controllo a distanza dell'attività lavorativa**, né risulti in alcun modo compromessa la dignità e riservatezza dei lavoratori»*

Cassazione civile, sez. lav., 02/05/2017, n. 10636

Caso: furto del dipendente di prodotti **alimentari dal magazzino**

*«La collocazione, da parte dell'azienda, di strumenti di controllo all'interno di locali dove si siano verificati dei **furti** integra un'ipotesi di **controllo difensivo a distanza**, **estraneo all'ambito di applicazione dell'art. 4 dello statuto** dei lavoratori qualora attuato con modalità non invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, con conseguente **legittimità del licenziamento per giusta causa** intimato al lavoratore di cui si sia, mediante le riprese, accertata la responsabilità dei furti».*

SOCIAL NETWORK

SOCIAL NETWORK

L'indagine sui contenuti pubblicati sui Social Network è **diversa** rispetto al monitoraggio degli accessi ai siti Internet visitati dai dipendenti in orario di lavoro

I social network sono una sorta di «***bacheca aperta***» al pubblico, una «***piazza immateriale***» che consente un numero indeterminato di "accessi" anche da parte dello stesso datore di lavoro

I messaggi vengono immessi *on line* non necessariamente dal PC aziendale, ma anche attraverso i personali strumenti di connessione ad Internet del dipendente (*smartphone, tablet* ecc.)

SOCIAL NETWORK

Profilo "personale": ove le immagini e le informazioni restano all'interno di un profilo o di un gruppo chiuso -> il trattamento dei dati rientra tra quelli per fini esclusivamente personali, non destinati ad una comunicazione sistematica o alla diffusione, indicati all'art. 5, comma 3, del Codice Privacy, e perciò esclusi dall'applicazione della disciplina codicistica. **I dati contenuti sul profilo non possono essere utilizzati dal datore di lavoro.**

Profilo "pubblico": accessibile a chiunque o quando i contenuti siano oggetto di indicizzazione su motori di ricerca -> si applica integralmente il Codice Privacy con la conseguenza che se il lavoratore presta il consenso ex art. 23 **i dati contenuti sul proprio profilo possono essere liberamente utilizzati dal datore di lavoro (ANCHE A FINI DISCIPLINARI)**

SOCIAL NETWORK

Cassazione civile, sez. lav., 27 aprile 2018, n. 10280

CASO: lavoratrice licenziata per aver pubblicato sulla propria bacheca virtuale di Facebook frasi con cui esprimeva il disprezzo per l'azienda presso cui era impiegata

«La condotta di postare un commento su Facebook realizza la pubblicizzazione e la diffusione di esso, per la idoneità del mezzo utilizzato a determinare la circolazione del commento tra un gruppo di persone, comunque, apprezzabile per composizione numerica, con la conseguenza che, se, come nella specie, lo stesso è offensivo nei riguardi di persone facilmente individuabili, la relativa condotta integra gli estremi della ***diffamazione e come tale correttamente il contegno è stato valutato in termini di giusta causa del recesso, in quanto idoneo a recidere il vincolo fiduciario nel rapporto lavorativo***».

SOCIAL NETWORK

TAR Lombardia Milano, Sez. III, Ord. 3 marzo 2016, n. 246

CASO: il Tar ha confermato la sospensione del lavoro e della paga nei confronti di un dipendente per aver espresso un giudizio di disvalore attraverso un **like postato su Facebook** ad un articolo contenente pesanti critiche sul suicidio di un detenuto presso la medesima casa circondariale.

«Il danno all'immagine e alla reputazione del datore di lavoro attraverso l'uso dei social network giustifica l'irrogazione della sanzione disciplinare della sospensione dal lavoro, integrando gli estremi della violazione dell'obbligo di fedeltà e dei principi di correttezza e buona fede nella regolamentazione del rapporto di lavoro»

Cassazione Lavoro: sì al falso profilo del datore di lavoro su Facebook per accertare l'illecito del dipendente

Corte di Cassazione - Quarta Sezione Lavoro, Sentenza 27 maggio 2015, n. 10955

La creazione, da parte di preposto aziendale e per conto del datore di lavoro, di un falso profilo facebook, al fine di effettuare un controllo sull'attività del lavoratore, già in precedenza allontanatosi dalla postazione lavorativa per parlare al cellulare, esula dal divieto di cui all'articolo 4 dello Statuto dei lavoratori, trattandosi di controllo difensivo, volto alla tutela dei beni aziendali.

Nel caso in esame, un operaio è stato licenziato dal proprio datore di lavoro in quanto durante il proprio turno veniva sorpreso a chattare e ad utilizzare facebook.

In particolare, nell'agosto del 2012, il dipendente si era allontanato dal posto di lavoro per una telefonata privata di circa 15 minuti che gli aveva impedito di intervenire prontamente su di una pressa, bloccata da una lamiera, che era rimasta incastrata nei meccanismi; nello stesso giorno era stato trovato, nel suo armadietto aziendale, un dispositivo elettronico acceso e in collegamento con la rete elettrica e, nei giorni successivi, in orari di servizio, si era intrattenuto con il suo cellulare a conversare su facebook.

Post su Facebook contro i diretti superiori e i vertici aziendali: legittimo il licenziamento (*Cassazione civile sez. lav., 13/10/2021, n.27939)*

- La pubblicazione di un post sul profilo personale di *Facebook* è idonea a determinare la circolazione del messaggio tra un gruppo indeterminato di persone
- Confermata dunque la decisione della Corte di Appello di Roma che, nel novembre 2018, ribadendo il contenuto gravemente offensivo e sprezzante (nei confronti dei superiori e degli stessi vertici aziendali) delle dichiarazioni, espresse a mezzo di tre e-mails e di un messaggio pubblicato, nell'ottobre del 2016, su *Facebook* respingeva il ricorso presentato dal lavoratore avverso il suo licenziamento per giusta causa, a nulla rilevando che la pubblicazione del *post* fosse destinata alla comunicazione esclusiva con i propri «amici»
- A detta della Corte, infatti, tali dichiarazioni integrerebbero **insubordinazione grave** e, in ogni caso, giusta causa di licenziamento in ragione del loro carattere plurioffensivo e dell'idoneità delle stesse a precludere «*la proseguibilità del rapporto, per l'elisione del legame di fiducia tra le parti, anche considerato il ruolo aziendale del predetto addetto*».

LE INFORMAZIONI TRATTE DALLA "CHAT" AZIENDALE, DESTINATA ALLE COMUNICAZIONI DI SERVIZIO DEI DIPENDENTI, COSTITUISCONO UNO STRUMENTO DI LAVORO MA SONO INUTILIZZABILI SENZA ADEGUATA INFORMAZIONE PREVENTIVA

(Cass. 22 settembre 2021, n. 25731)

❑«*La "chat" aziendale, destinata alle comunicazioni di servizio dei dipendenti, è qualificabile come strumento di lavoro ai sensi dell'art. 4, comma 2, st.lav. novellato, essendo funzionale alla prestazione lavorativa, con la conseguenza che le informazioni tratte dalla "chat" stessa, a seguito dei controlli effettuati dal datore di lavoro, sono inutilizzabili in mancanza di adeguata informazione preventiva ex art. 4, comma 3, st.lav.*»

❑Nella specie, la S.C. ha confermato la sentenza di merito che aveva annullato il licenziamento comminato a una lavoratrice - per avere quest'ultima inviato ad una collega, su una "chat" aziendale, messaggi offensivi nei confronti, tra l'altro, di un superiore gerarchico -, sul presupposto che il datore fosse venuto a conoscenza dei messaggi stessi in occasione di un controllo tecnico del quale non era stata data alcuna preventiva comunicazione alla lavoratrice medesima

AGENZIE INVESTIGATIVE

… E IL CONTROLLO ATTRAVERSO AGENZIE INVESTIGATIVE?

NO CONTROLLO DELLA PRESTAZIONE, SI CONTROLLO COMPORTAMENTI ILLECITI

Cassazione civile sez. lav., 11/06/2018 n. 15094

«*Le agenzie investigative per operare lecitamente* ***NON*** *devono sconfinare nella* ***vigilanza dell'attività lavorativa vera e propria****, (…) resta* ***giustificato l'intervento in questione solo per l'avvenuta perpetrazione di illeciti e l'esigenza di verificarne il contenuto, anche laddove vi sia un sospetto o la mera ipotesi che illeciti siano in corso di esecuzione***

Dove il controllo demandato all'agenzia investigativa non abbia ad oggetto l'adempimento della prestazione lavorativa e sia espletato al di ***fuori dell'orario di lavoro, esso è legittimo, come nel caso di verifica sull'attività extralavorativa svolta dal lavoratore in violazione del divieto di concorrenza, fonte di danni per il datore di lavoro ovvero nel caso di controllo finalizzato all'accertamento dell'utilizzo improprio, da parte di un dipendente, dei permessi L. n. 104***»

Il caso: **Tribunale Padova, 04/10/2019**

Il datore di lavoro sanziona disciplinarmente un proprio dipendente, contestandogli la falsa attestazione della propria presenza in ufficio in periodi temporali in cui, durante l'orario di lavoro, egli si trovava al di fuori della sede lavorativa per svolgere attività extra-lavorative.

Il datore di lavoro, per la contestazione dei fatti, si è avvalso di una agenzia di investigazione privata.

Il Giudice del lavoro ha fornito le seguenti indicazioni interpretative:

— il diritto vivente consolidatosi in seno alla giurisprudenza sia di merito (v. Corte d'Appello di Roma, sent. 13.2.2013, est. G. Poscia; Tribunale di Velletri, sent. 26.3.2006, F. Anzilotti; Tribunale di Venezia, ord. 8.10.2018, B. Bortot), sia di legittimità, ha tradizionalmente elaborato un'interpretazione marcatamente estensiva della norma in esame, in particolare stabilendo che il rigoroso divieto di controllo occulto sancito dall'art. 3 sull'attività lavorativa svolta al di fuori dei locali aziendali non opera nel caso in cui il ricorso ad investigatori privati sia finalizzato a verificare comportamenti che possono configurare condotte illecite, quali ad esempio la violazione del divieto di concorrenza, fonte di danni per il datore di lavoro (vedi Cass. n. 12810/2017), ovvero l'utilizzo improprio, da parte di un dipendente, di permessi di cui all'art. 33 della legge n. 104/1992 (vedi Cass. n. 4984/2014), e a maggior ragione nel caso in cui si tratti di comportamenti che possano configurare ipotesi penalmente rilevanti (vedi Cass. n. 5269 e 14383/2000). ***Si tratta, nella sostanza, dell'estensione all'ambito applicativo dell'art. 3 della dottrina dei cosiddetti "controlli difensivi", tradizionalmente elaborata con riferimento all'interpretazione dell'art. 4 dello Statuto dei Lavoratori nella formulazione precedente alla novella introdotta dall'art. 23, comma 1 del decreto legislativo n. 151/2015****;*

— resta invece fermo l'assoggettamento al rigoroso regime interdittivo stabilito dall'art. 3 di ogni controllo diretto a verificare il corretto adempimento da parte del lavoratore degli obblighi contrattuali imposti dal contratto di lavoro, in particolare con riferimento al diligente adempimento delle mansioni pattuite (vedi Cass. n. 21621/2018) nel caso in cui i fatti non siano qualificabili alla stregua di fattispecie illecite assistite da autonoma rilevanza civile, amministrativa ovvero penale;

— ***qualunque conclusione voglia trarsi in merito alla perdurante compatibilità della dottrina dei controlli difensivi rispetto alla nuova formulazione dell'art. 4 introdotta dal Jobs Act (v. Tribunale di Roma, ord. 13.6.2018, D. Conte, e di avviso contrario Tribunale della Spezia, ord. 25.11.2016, G. Romano), essa non è di per sé estendibile all'art. 3 dello Statuto dei Lavoratori****, atteso che mentre la regolamentazione introdotta dal novellato art. 4, quantomeno in linea di principio, tende a definire una compiuta ed autosufficiente disciplina normativa in punto di liceità del controllo tramite impianti tecnologici ed utilizzabilità delle informazioni ottenute per mezzo di quest'ultimi, l'art. 3, rimasto immutato nella sua originaria formulazione, non presenta alcuna analogia strutturale rispetto all'art. 4 novellato.*

L'IMPOSTAZIONE PIÙ STRINGENTE DEL GARANTE IN TEMA DI CONTROLLO

- NAVIGAZIONE INTERNET
- POSTA ELETTRONICA
- GPS

1. Il CONTROLLO DI INTERNET e della POSTA ELETTRONICA AZIENDALE

Linee Guida del Garante per posta elettronica e internet DEL. N. 13 del 1° marzo 2007

- Il datore di lavoro ha l'onere di informare, chiaramente e in modo particolareggiato, i dipendenti su quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengono effettuati controlli anche in accordo con le organizzazioni sindacali, utilizzando ad esempio un disciplinare interno, chiaro e aggiornato affiancato da un'idonea informativa
- I controlli da parte del datore di lavoro per motivi organizzativi o di sicurezza sono leciti solo se sono rispettati i principi di pertinenza e non eccedenza
- I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad internet e al traffico telematico, la cui conservazione non sia necessaria
- I datori di lavoro privati e gli enti pubblici economici possono trattare i dati personali del lavoratore, diversi da quelli sensibili, per il legittimo esercizio di un diritto in sede giudiziaria, a fronte della manifestazione di un libero consenso o per un legittimo interesse

2. Il CONTROLLO DI INTERNET e della POSTA ELETTRONICA AZIENDALE

Provvedimento del Garante Privacy – 18 ottobre 2012

- Il datore di lavoro può effettuare controlli mirati al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro.

- Nell'esercizio di tale prerogativa, occorre rispettare la libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i principi di correttezza, di pertinenza e non eccedenza di cui all'art. 11, comma I, del Codice.

- Prima della messa in funzione dell'impianto l'azienda dovrà dare apposita informativa scritta al personale dipendente in merito all'attivazione dello stesso, al posizionamento delle telecamere ed alle modalità di funzionamento, dovrà informare i clienti con appositi cartelli e inoltre dovrà nominare un incaricato della gestione dei dati videoripresi

- Il lavoratore non risultava essere stato previamente informato in riferimento al trattamento dei dati personali che avrebbe potuto essere effettuato in attuazione di eventuali controlli sull'utilizzo del pc concessogli in uso per esclusive finalità lavorative, con particolare riferimento alle modalità e alle procedure da eseguire per gli stessi.

3. Il CONTROLLO DI INTERNET e della POSTA ELETTRONICA AZIENDALE

Provvedimento del Garante Privacy in tema di trattamento dei dati personali, mediante controllo occulto da parte del datore di lavoro – 5 febbraio 2015

- Il datore di lavoro aveva installato un sistema proxy al fine di monitorare per 24 ore tutto il traffico entrante e uscente dalla rete web aziendale, con esclusivo riferimento all'attività delle singole macchine.

- Il Garante evidenzia che «la specifica e accertata funzione del sistema, configurata in modo da consentire la registrazione, con una significativa profondità temporale, dei dati relativi alla navigazione web effettuata dalla singola macchina (IP) e quindi del lavoratore cui la stessa è stata attribuita in via esclusiva» permetteva all'azienda « di estrapolare i dati di dettaglio relativi a URL visitata, IP sorgente e orario di connessione»

4. Il CONTROLLO DI INTERNET e della POSTA ELETTRONICA AZIENDALE

Provvedimento del Garante Privacy in tema di controllo indiscriminato di e-mail e Internet – 13 luglio 2016, n. 303

Un'università raccoglieva e conservava, per un periodo di 5 anni, i file di log relativi al traffico internet contenenti, tra gli altri, il MAC (Access Control Address), l'indirizzo IP, nonché informazioni relative all'accesso ai servizi internet, all'utilizzo della posta elettronica ed alle connessioni di rete di una serie di utenti tra cui docenti, ricercatori, personale tecnico amministrativo e bibliotecario, studenti, dottorandi, specializzandi e assegnisti di ricerca, professori a contratto e visiting professor.

Il Garante ha sostenuto che tale trattamento era stato «effettuato per il tramite di apparati differenti (dalle ordinarie postazioni di lavoro) e di sistemi software che consentono, con modalità non percettibili dall'utente e in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore, operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminati degli accessi ad internet o al servizio di posta elettronica». Pertanto, «tali software non possono essere considerati "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"».

5. VIDEOSORVEGLIANZA

Provvedimento del Garante in materia di videosorveglianza – 8 aprile 2010

- Non devono essere effettuati controlli a distanza al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa

- Prima della messa in funzione dell'impianto l'azienda dovrà dare apposita informativa scritta al personale dipendente in merito all'attivazione dello stesso, al posizionamento delle telecamere ed alle modalità di funzionamento, dovrà informare i clienti con appositi cartelli e inoltre dovrà nominare un incaricato della gestione dei dati videoripresi

- La conservazione delle immagini deve essere limitata alle 24 ore, salvo in alcuni casi per peculiari esigenze tecniche o per la particolare rischiosità dell'attività svolta dal titolare del trattamento. Il sistema deve essere programmato per la cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto

6. VIDEOSORVEGLIANZA

Provvedimento del Garante in materia di videosorveglianza – 8 aprile 2010

QUALI TEMPI DI CONSERVAZIONE DEI DATI?

- **poche ore o, al massimo, le ventiquattro ore successive alla rilevazione**, fatta salva specifica richiesta investigativa dell´autorità giudiziaria o di polizia giudiziaria.

- Solo in particolare rischiosità dell´attività svolta dal titolare del trattamento (ad esempio, luoghi come le **banche** per identificare gli autori una rapina o per i comuni ai fini della tutela della **sicurezza urbana**) può ritenersi ammesso un tempo più ampio di conservazione comunque non superiore ala settimana

- è necessaria specifica Richiesta al garante per l´allungamento dei tempi di conservazione dei dati **oltre i sette giorni**, adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita (es. provvedimento garante 7 aprile 2016 autorizza **15 giorni**, provvedimento 25 giugno 2015 autorizza fino a 7 mesi)

- Il sistema impiegato deve essere programmato in modo da operare l´integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto,

7. VIDEOSORVEGLIANZA

Provvedimento del Garante in materia di videosorveglianza – 8 aprile 2010

LUOGHI E CIRCOSTANZE DI RACCOLTA DEI DATI?

- Queste garanzie vanno osservate sia **all´interno degli edifici**, sia in **altri luoghi di prestazione di lavoro** (es. telecamere installate su autobus le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull´attività lavorativa degli addetti).

- Ê inammissibile l´installazione di sistemi di videosorveglianza in **luoghi riservati esclusivamente ai lavoratori o non destinati all´attività lavorativa** (ad es. bagni, spogliatoi, docce, armadietti e luoghi ricreativi).

8. LA VIDEOSORVEGLIANZA

Ispettorato Nazionale del Lavoro Circolare n. 5/2018

«le condizioni poste all'utilizzo delle strumentazioni devono essere necessariamente correlate alla specifica finalità individuata nell'istanza ***senza, però, particolari ulteriori limitazioni di carattere tecnico che talvolta finiscono per vanificare l'efficacia dello stesso strumento di controllo****. L'eventuale ripresa dei lavoratori, di norma, dovrebbe avvenire in via incidentale e con carattere di occasionalità ma nulla impedisce, se sussistono le ragioni giustificatrici del controllo (ad esempio tutela della "sicurezza del lavoro" o del "patrimonio aziendale"),* ***di inquadrare direttamente l'operatore, senza introdurre condizioni quali, per esempio, "l'angolo di ripresa" della telecamera oppure "l'oscuramento del volto del lavoratore».***

9. LOCALIZZAZIONE GPS

Provvedimento del Garante Privacy – 4 ottobre 2011, n. 370

Provvedimento del Garante Privacy – 9 ottobre 2014, n. 449

- Il Garante autorizza i datori di lavoro pubblici e privati all'uso di localizzatori al solo scopo dell'organizzazione del lavoro, anche senza il consenso del lavoratore ma solamente dopo accordi sindacali o autorizzazione delle direzioni del lavoro.

- Il Garante autorizza la localizzazione attraverso il telefono portatile aziendale sul quale, la compagnia telefonica che ha chiesto la pronuncia, ha installato un'applicazione attraverso cui individuare la collocazione del lavoratore.

10. LOCALIZZAZIONE GPS

Circolare dell'Ispettorato nazionale del lavoro n. 2/2016

L'Ispettorato fornisce indicazioni circa la corretta lettura dell'art. 4 Stat. lav. per quanto attiene all'installazione di apparecchiature di localizzazione satellitare GPS montate su autovetture aziendali.

L'ispettorato sostiene che «si può ritenere che i sistemi di geocalizzazione rappresentino un elemento "aggiuntivo" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma, per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro».

Tali apparecchiature possono essere installate solo previo accordo stipulato con la rappresentanza aziendale ovvero, in assenza di tale accordo, previa autorizzazione da parte dell'Ispettorato nazionale del lavoro.

Eccezioni:
- se i sistemi di localizzazione sono installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa;
- l'installazione è richiesta da specifiche normative di carattere legislativo o regolamentare.

11. LOCALIZZAZIONE GPS

Provvedimento del Garante Privacy 28 giugno 2018

localizzazione con modalità proporzionate rispetto al diritto alla riservatezza degli interessati, in particolare con riferimento alla **periodizzazione temporale** della rilevazione della posizione geografica, ai **tempi di conservazione** dei dati

*«la raccolta di **informazioni particolareggiate sull'attività dei singoli veicoli monitorati dal sistema e, indirettamente, sull'attività degli autisti** cui i veicoli sono affidati, quali la ricostruzione su mappa dei percorsi effettuati **comprese le pause**, con una **periodicità della rilevazione estremamente ravvicinata (ogni 120 secondi)**, non sono proporzionate con gli scopi rappresentati dalla società che potrebbero essere utilmente e legittimamente perseguiti con la raccolta di informazioni assai più limitate. Né risulta conforme al principio di proporzionalità la integrale **conservazione** dei dati raccolti per un **esteso periodo di tempo (365 giorni)** in relazione alle finalità perseguite».*

Implementare e garantire l'utilizzo di «***dispositivi di disattivazione della rilevazione geografica»:***

- durante le pause consentite dell'attività lavorativa

- momenti vita privata laddove la vettura sia affidata per **uso promiscuo**

12. LOCALIZZAZIONE GPS E SMARTPHONE AZIENDALE

Provvedimento del Garante Privacy n. 350/2016

La **rilevazione della presenza dei lavoratori** sul luogo di lavoro può essere effettuata dal datore anche tramite **un'applicazione installata sullo *smartphone*** dei lavoratori, tesa a rilevare ed associare le coordinate geografiche della posizione di questi ultimi a quella del luogo di lavoro.

➢il trattamento dei dati (numero identificativo dei dipendenti, orario di inizio e fine della prestazione e posizione del lavoratore) rientra tra gli interessi legittimi del datore di lavoro (tra cui, il risparmio di costi di gestione e l'incremento della certezza delle rilevazioni)

➢il datore di lavoro sarà tenuto ad adottare alcuni **accorgimenti rispetto dei principi di pertinenza e non eccedenza del trattamento**

Ad esempio:

- configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva;
- la cancellazione delle coordinate geografiche della posizione del lavoratore;
- il divieto di trattamento degli altri dati personali del lavoratore presenti sul proprio dispositivo (es. mail, sms ecc.).

UN CASO PARTICOLARE: IL DATO BIOMETRICO

- il riconoscimento biometrico, installato su sistemi basati sull'elaborazione dell'impronta digitale o della topografia della mano con lo scopo di impedire l'utilizzo della macchina a soggetti non autorizzati (es: **accesso ai locali aziendali tramite rilevamento dell'impronta digitale per scopi di sicurezza**), necessario per avviare il funzionamento della stessa, può essere considerato uno strumento indispensabile a "*rendere la prestazione lavorativa*" e, pertanto, nel caso di specie si può prescindere, ai sensi del comma 2 dell'art. 4 della l. n. 300/1970, sia dall'accordo con le rappresentanze sindacali sia dal procedimento amministrativo di carattere autorizzativo (**Circolare INL n. 5/2018**)

- Sotto il profilo Privacy, per il trattamento dei dati biometrici acquisiti occorre rispettare le linee guida fornite dal **Garante con provvedimento del 23 novembre 2006**:
  - Dare ai lavoratori adeguata informativa;
  - Acquisire e trattare i dati biometrici e, conseguentemente, utilizzare il sistema di controllo degli accessi esclusivamente per le finalità dichiarate nell'istanza, ossia per esigenze di tutela del patrimonio aziendale
  - Conservare i dati acquisiti per un periodo di tempo limitato

Se il trattamento dei dati biometrici e l'installazione dei sistemi che acquisiscono tali dati rispettano queste previsioni, NON È NECESSARIO ACQUISIRE PREVENTIVA AUTORIZZAZIONE DEL GARANTE NÉ ATTIVARE LA PROCEDURA DI CUI ALL'ART. 4 COMMA 1 ST. LAV.

QUANDO LE INFORMAZIONI SONO RACCOLTE ED UTILIZZATE LEGITTIMAMENTE AI FINI DISCIPLINARI?

1. Rispetto dell'art. 4 s.l. = accordo sindacale/autorizzazione ITL che legittima raccolta e utilizzo informazioni

2. Dati raccolti mediante strumento di lavoro/registrazione presenze o accesso

3. trattamento dei dati raccolti conforme al GDPR (informativa etc.)

4. siamo in presenza di un *controllo difensivo* che giustifica la raccolta dei dati anche al di fuori dell'art. 4 s.l.

GRAZIE DELL'ATTENZIONE

Avv. Luca Failla
lufailla@deloitte.it

Deloitte.
Legal

- Important notice
- This document has been prepared by Deloitte Legal – Società tra Avvocati a r.l. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte Legal – Società tra Avvocati a r.l. to supply the proposed services.
- The information contained in this document has been compiled by Deloitte Legal – Società tra Avvocati a r.l. and may include material obtained from various sources which have not been verified or audited. This document also contains material proprietary to Deloitte Legal – Società tra Avvocati a r.l. Except in the general context of evaluating the capabilities of Deloitte Legal – Società tra Avvocati a r.l., no reliance may be placed for any purposes whatsoever on the contents of this document. No representation or warranty , express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte Legal – Società tra Avvocati a r.l. or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document.
- Other than stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or insurance saving, no such conditions of confidentiality applies to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.
- This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.
- Deloitte Legal – Società tra Avvocati a r.l., a company, registered in Italy with registered number 10788500964 and its registered office at Via Tortona no. 25, 20144, Milan, Italy, is an affiliate of Deloitte Central Mediterranean S.r.l., a company limited by guarantee registered in Italy with registered number 09599600963 and its registered office at Via Tortona no. 25, 20144, Milan, Italy.
- Deloitte Central Mediterranean S.r.l. is the affiliate for the territories of Italy, Greece and Malta of Deloitte NSE LLP, a UK limited liability partnership and a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL, Deloitte NSE LLP and Deloitte Central Mediterranean S.r.l. do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.
-

Lecito il falso profilo del datore di lavoro su Facebook per accertare l'illecito del dipendente (*Corte di Cassazione 27 maggio 2015, n. 10955)*

- La creazione, da parte di preposto aziendale e per conto del datore di lavoro, di un falso profilo *Facebook*, al fine di effettuare un controllo sull'attività del lavoratore, già in precedenza allontanatosi dalla postazione lavorativa per parlare al cellulare, esula dal divieto di cui all'articolo 4 dello Statuto dei lavoratori, trattandosi di controllo difensivo, volto alla tutela dei beni aziendali.

- Nel caso in esame, un operaio è stato licenziato dal proprio datore di lavoro in quanto durante il proprio turno veniva sorpreso a chattare e ad utilizzare *Facebook*

- In particolare, nell'agosto del 2012, il dipendente si era allontanato dal posto di lavoro per una telefonata privata di circa 15 minuti che gli aveva impedito di intervenire prontamente su di una pressa, bloccata da una lamiera, che era rimasta incastrata nei meccanismi; nello stesso giorno era stato trovato, nel suo armadietto aziendale, un dispositivo elettronico acceso e in collegamento con la rete elettrica e, nei giorni successivi, in orari di servizio, si era intrattenuto con il suo cellulare a conversare su *Facebook*

Post su Facebook contro i diretti superiori e i vertici aziendali: legittimo il licenziamento (*Cassazione civile sez. lav., 13/10/2021, n.27939)*

- La pubblicazione di un post sul profilo personale di *Facebook* è idonea a determinare la circolazione del messaggio tra un gruppo indeterminato di persone
- Confermata dunque la decisione della Corte di Appello di Roma che, nel novembre 2018, ribadendo il contenuto gravemente offensivo e sprezzante (nei confronti dei superiori e degli stessi vertici aziendali) delle dichiarazioni, espresse a mezzo di tre e-mails e di un messaggio pubblicato, nell'ottobre del 2016, su *Facebook* respingeva il ricorso presentato dal lavoratore avverso il suo licenziamento per giusta causa, a nulla rilevando che la pubblicazione del *post* fosse destinata alla comunicazione esclusiva con i propri «amici»
- A detta della Corte, infatti, tali dichiarazioni integrerebbero **insubordinazione grave** e, in ogni caso, giusta causa di licenziamento in ragione del loro carattere plurioffensivo e dell'idoneità delle stesse a precludere «*la proseguibilità del rapporto, per l'elisione del legame di fiducia tra le parti, anche considerato il ruolo aziendale del predetto addetto*».