Evento del 23 febbraio 2021

App e nuove tecnologie.

Quali rischi per i dati personali?

Le App nel rapporto di lavoro.

Intervento a cura dell’Avv. Alessandro Mariani

componente della Commissione Privacy dell’Ordine degli Avvocati di Roma

Il potere di controllo del datore di lavoro.

L'articolo 41 della Costituzione prevede la libertà di iniziativa economica del datore di lavoro, purchè esercitata nel rispetto della libertà e dignità umana.

L'attività lavorativa dei dipendenti può essere controllata dal datore di lavoro nel rispetto delle sue direttive, con dei limiti.

Limiti al potere di controllo del datore di lavoro.

Riservatezza;

Dignità personale;

Libertà di espressione e di comunicazione.

Il datore di lavoro può effettuate il trattamento dei dati personali dei propri dipendenti - diversi da quelli sensibili purché siano rispettate le condizioni di liceità previste dal Regolamento UE 2016/679.

Come bilanciare i contrapposti diritti dal datore e del lavoratore?

Osservanza della disciplina prevista dallo **Statuto dei Lavoratori:**

È vietato il controllo lesivo dei diritti inviolabili;

E’ vietato ogni tipo di controllo occulto.

In presenza di determinate condizioni i divieti sono attenuati.

Sviluppo tecnologico ed evoluzione delle tecniche lavorative.

Introduzione dei **controlli a distanza** anche per verificare l'adeguatezza della prestazione lavorativa.

Bilanciamento con il **diritto del datore di lavoro a tutelare i beni aziendali**.

Tutela dei dati personali. Come effettuare il controllo sui lavoratori?

Il controllo deve risultare necessario o indispensabile rispetto ad uno scopo determinato;

il controllo deve essere finalizzato a garantire la sicurezza o la continuità aziendale, o a prevenire e reprimere illeciti;

il datore di lavoro deve informare preventivamente i dipendenti sui limiti di utilizzo degli strumenti e delle sanzioni previste nel caso di violazione di tali limiti;

il datore di lavoro deve adottare forme di controllo strettamente proporzionate;

i dati raccolti devono essere protetti in modo adeguato.

Il datore deve individuare la base giuridica del trattamento dei dati.

adempimento di obblighi derivanti da un contratto di lavoro;

adempimento di obbligazioni previste dalla legge;

interesse legittimo del datore di lavoro (valutazione di impatto e diritto di opporsi al trattamento).

GDPR art. 88 e adeguamento decreto 101 del 4 luglio 2018.

Gli Stati possono emanare regole particolari atte a garantire la protezione dei diritti e delle libertà dei dipendenti durante i trattamenti dei dati nel contesto del rapporto di lavoro, attraverso accordi collettivi o disposizioni legislative, con trasparenza e con una adeguata protezione dei dati personali.

Il controllo del datore di lavoro nell'ambito del trattamento di dati del lavoratore può avvenire ad esempio fin dalla valutazione dei candidati ed al momento dell'assunzione, quando valuta le prestazioni lavorative, quando pianifica ed organizza la prestazione lavorativa, in ambito di salute e sicurezza dell'ambiente di lavoro, per la protezione dei beni del dipendente, e fino alla conclusione del rapporto di lavoro.

Con D.Lgs. 10 agosto 2018, n. 101 è stato disposto l'adeguamento al GDPR.

Strumenti di lavoro e strumenti di controllo. Con il Jobs Act cosa è cambiato?

Con D.Lgs n. 151 del 14 settembre 2015 (Jobs Act) è stato riscritto l'art. 4 dello Statuto dei Lavoratori ed è stato stabilito un regime diverso a seconda del tipo di strumento:

strumenti che consentono il controllo del lavoratore quali ad esempio la videosorveglianza;

strumenti di lavoro quali ad esempio il personal computer o lo smartphone.

Limiti ai divieti su impianti e strumenti di controllo a distanza.

L'installazione di impianti audiovisivi ed altri strumenti dai quali deriva anche la possibilità di controllo a distanza dell'attività dei lavoratori è vietata, a meno che non ricorrano due condizioni:

- esigenze organizzative e produttive, di sicurezza del lavoro e tutela del patrimonio aziendale;

- preventivo accordo sindacale o autorizzazione amministrativa in DTL (necessità del consenso dei lavoratori Cass. Sez III Penale sent. 17 gennaio 2020 n. 1733).

Strumenti di lavoro.

La novità della riforma è data dal secondo comma dell'articolo 4, il quale prevede che le garanzie non si applicano agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (es. smartphone, tablet, personal computer), ed agli strumenti di registrazione degli accessi e delle presenze. In tali casi l'installazione non richiede alcun accordo sindacale.

L'eccezione è limitata agli strumenti che "*immediatamente servono al lavoratore per adempiere alle mansioni assegnate*". Il Ministero del Lavoro, con nota del 18 giugno 2015, ha stabilito che nel momento in cui lo strumento viene modificato (ad esempio, con l'aggiunta di software di localizzazione), non si considera più rientrante nella categoria.

Alcune interpretazioni discordanti in merito si posso avere sul GPS installato sull'auto aziendale che potrebbe essere considerato servente rispetto alle mansioni assegnate (nel caso in cui il datore di lavoro utilizza il GPS per stabilire chi deve recarsi dal cliente in base alla vicinanza ma nel contempo potrebbe essere utilizzato per controllare il lavoratore stesso dal GPS si può ricavare che lavoratore è fuori zona senza motivazione).

Informazioni raccolte tramite strumenti d lavoro.

Il comma 3 stabilisce che le informazioni raccolte tramite gli strumenti di cui al comma 1 e 2, sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che al lavoratore sia data adeguata informazione delle modalità d’uso degli strumenti e di effettuazione dei controlli.

Il Ministero del Lavoro ha chiarito che, occorre informare i lavoratori circa l'esistenza e le modalità d'uso degli strumenti di controllo, con riferimento alla finalità e alle modalità del trattamento dei dati, alla natura obbligatoria e facoltativa del conferimento dei dati, alle conseguenze di un eventuale rifiuto, ai soggetti cui tali dati possono essere comunicati e ai responsabili aziendali del trattamento dei dati, nonchè dei diritti dei lavoratori, in mancanza i dati non possono essere utilizzati a nessun fine.

Le App con mail aziendale

La casella aziendale è uno strumento di lavoro.

Il datore di lavoro deve poter accedere in qualsiasi momento alla casella di posta elettronica aziendale in uso al dipendente.

L'accesso del datore di lavoro è legittimato anche dalla necessità della continuità aziendale, ad esempio nel caso in cui il lavoratore sia in malattia.

Le App nel lavoro a domicilio. Il fenomeno del BYOD (bring your own device).

Nel lavoro in smart working da casa spesso viene autorizzato l'uso dei propri dispositivi da parte del dipendente.

Il datore di lavoro deve autorizzare l'accesso alla rete informativa aziendale, e il dipendente può archiviare dati aziendali sul proprio dispositivo con enormi rischi, quali la perdita dei dati in caso di smarrimento o furto del dispositivo.

Potrebbero sorgere problemi anche nel caso di malfunzionamenti del dispositivo, se il dipendente lo porta in riparazione presso un'azienda che, in teoria, potrebbe estrarre i dati aziendali dal dispositivo.

Rischi nel monitoraggio della strumentazione informatica dei lavoratori.

Le app con la casella di posta elettronica, il telefonino, la navigazione su Internet e le ricerche online.
Se forniti dall'azienda gli strumenti elettronici sono dotazioni aziendali e quindi controllabili dal datore ed inutilizzabili a fini personali.

Tale monitoraggio deve essere limitato sia nel tempo che per tipologia. Inoltre le misure di sicurezza relative ai dispositivi da remoto, quali il monitoraggio dei movimenti del mouse, l'utilizzo di webcam o di tecnologie di screen capture, sono considerate illegittime.

La mail privata del dipendente, in quanto è dato personale e strumento identificativo, non è mai controllabile dall'azienda anche se utilizzata sul luogo di lavoro.
La navigazione in Internet tramite gli strumenti aziendali può essere limitata o vietata purché non sussista un trattamento illecito dei dati dei lavoratori. Quindi, possono essere applicati appositi filtri per impedire gli accessi a determinati siti, ma i sistemi devono essere configurati in modo da cancellare periodicamente i dati personali (accessi ai siti). Un monitoraggio sistematico della navigazione su Internet dei lavoratori deve ritenersi illecito.

La rilevazione della presenza dei lavoratori.

Alcuni strumenti possono comportare l'indiretto monitoraggio della presenza e dell'attività dei lavoratori sul luogo di lavoro, tali trattamenti sono legittimi in quanto finalizzati a tutelare la perdita o la sottrazione di informazioni aziendali riservate, occorre però adeguata informativa.

La videosorveglianza ed iltrattamento dei dati.

Il video monitoraggio dei lavoratori è considerato illecito in quanto sproporzionato rispetto alla tutela dei diritti degli interessati.

La Geolocalizzazione dei veicoli.es. i

Il trattamento dei dati di geolocalizzazione dei veicoli aziendali (satellitari GPS) è legittimo per la tutela della sicurezza dei veicoli e dei lavoratori, o anche per la pianificazione in tempo reale dell'attività lavorativa.

Illecita è la geolocalizzazione nel caso in cui i veicoli aziendali possano essere usati anche per finalità private.

Il dipendente deve poter disabilitare il monitoraggio nel momento in cui svolge un'attività di natura personale con l'auto aziendale.

Bisogna applicare un'informativa all'interno del veicolo, che ricordi al dipendente l'esistenza del dispositivo di monitoraggio e le modalità di blocco temporaneo.

l Garante in passato ha stabilito che la necessità di tracciare gli spostamenti di un cellulare o un tablet è giustificata da «esigenze organizzative o produttive o per la sicurezza sul lavoro». A garanzia del lavoratore, però, se il sistema di geolocalizzazione è attivo deve essere segnalato da un'icona lampeggiante sullo schermo. Servirebbe una comunicazione da parte del datore di lavoro che il dispositivo viene tracciato.

Il Garante Privacy ha poi chiarito che i datori di lavoro possono utilizzare gli strumenti GPS con lo scopo di localizzare i dipendenti in Mobile Working e sono dotati di telefono aziendale, purché adottino opportuni accorgimenti volti a non invadere la sfera privata del lavoratore e rispettino stringenti misure di sicurezza.

L'obiettivo è di consentire non tanto il controllo dei movimenti dei dipendenti quanto di garantire il coordinamento e la tempestività degli interventi tecnici in caso di necessità. I datori di lavoro devono poter accedere alle funzioni di geolocalizzazione dello smartphone, ma senza accedere ad altri dati come traffico telefonico, SMS, posta elettronica o traffico voce. Il lavoratore deve essere al corrente della possibilità di essere localizzato dal proprio datore di lavoro, per mezzo di una app che deve essere ben visibile sullo schermo dello smartphone.

Alcuni limiti ai controlli sui dipendenti.

Per le App bisogna distinguere tra uso lavorativo e uso personale.

La possibilità di controllare l'uso di un'App sarebbe anche legata all'account utilizzato.

Nel caso di Skype dovrebbe esserci una distinzione tra una chiamata per motivi di lavoro (si può esercitare un controllo) e una privata.

Cosa dice il Garante della Privacy sulle comunicazioni elettroniche?

Il contenuto di comunicazioni di tipo elettronico o telematico scambiate dai dipendenti nell'ambito del rapporto di lavoro godono di garanzie di segretezza tutelate anche a livello costituzionale.

Il caso era stato sollevato da una lavoratrice licenziata per aver effettuato delle chiamate su Skype con alcuni clienti.

La dipendente aveva fatto ricorso contro l'acquisizione illecita di dati da parte del datore di lavoro.

Il punto di vista differente: tutto ciò che è effettuato in orario di lavoro sarebbe connesso all'attività lavorativa e quindi possibile oggetto di controllo.

Dispositivo e account.

Uno dei limiti dei decreti attuativi del Jobs Act, è che non viene definita la differenza tra un dispositivo e i diversi account di un'applicazione che su questo possono esistere.

Il Garante suggerisce che è l'azienda a dover definire a monte le applicazioni che un lavoratore può avere sul proprio dispositivo.

Per quanto riguarda la mail sembra chiaro che l'account aziendale possa essere controllato dal datore di lavoro.

La mail privata invece continuerebbe a essere considerata inviolabile.

Potranno sorgere problemi nel caso dell'utilizzo di un account personale per motivi di lavoro.

SMS e Whatsapp.

Gli SMS, essendo attività connaturate allo smartphone e non riconducibili a un account personale, potrebbero essere controllabili.

Le chat su Whatsapp e le altre app per scambiare messaggi, dovrebbero ricadere all’interno dei dati coperti dal segreto, perché fanno riferimento ad un account specifico.

La cronologia su internet.

Quando si naviga su smartphone o tablet non si può fare riferimento a una chiara identità o a un account posseduti dalla persona. Essendo il browser uno strumento presente sul dispositivo, sembrerebbe tracciabile in quanto il lavoratore sarebbe consapevole della sua presenza e della conseguente possibilità di essere controllato. Per prevenire ogni problema l'azienda potrebbe decidere una lista dei siti non visualizzabili al lavoro.

Le App social usate durante l'orario di lavoro.

Numerose ordinanze hanno ritenuto legittimo il licenziamento se si usa impropriamente l'App con i social:

postare fotografie scattate durante l'orario di lavoro accompagnate da commenti offensivi nei confronti dell'azienda, perche

nel momento in cui si decide di pubblicare determinate informazioni e foto sul proprio profilo, si accetta automaticamente il rischio che queste possano essere viste da soggetti terzi e quindi utilizzate in Tribunale.

Non è possibile il licenziamento per diffusione di informazioni, reperite o meno su Internet, riguardanti dati sensibili come l'orientamento o la vita sessuale di un dipendente (cit. Corte di Cassazione – sentenza n. 21107/2014), a pena la nullità del licenziamento per motivi discriminatori. Stesso discorso per il licenziamento basato sulla intercettazione di conversazioni sulle chat, tipo Skype.

Il Jobs Act ed il difficile equilibrio tra uso delle tecnologie e Privacy.

Il datore di lavoro è legittimato a fornire in uso ai propri dipendenti strumenti di lavoro anche informatici/telematici (e ad utilizzare i dati raccolti tramite tali strumenti) senza passare dalla preventiva autorizzazione delle Organizzazioni Sindacali o dell'Ispettorato del Lavoro.

Ciò, a condizione che venga data adeguata protezione ai dati personali raccolti, attraverso una idonea informativa ed il rispetto della normativa privacy.

Le condizioni del Garante.

Il trattamento dei dati effettuato tramite sistemi software, non percepibili dall'utente (c.d. in background), ed idonei a porre in essere operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminati di tutti gli accessi a internet o al servizio di posta elettronica da parte degli utenti, si ponesse in violazione dei principi di necessità, pertinenza e non eccedenza previsti dal Codice Privacy.

Il Garante ha ritenuto che "*Tali software non possono essere considerati "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (ai sensi e per gli effetti dell'art. 4, comma 2, l. n. 300/1970…)"*

Il Garante aveva ritenuto vietati hardware e software che consentano: la riproduzione e memorizzazione sistematica di tutte le pagine web visitate dal lavoratore e la lettura e registrazione dei caratteri inseriti tramite la tastiera del PC

Nella nozione di strumento di lavoro, con specifico riferimento ai servizi di posta elettronica e navigazione web "*è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza. Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore.*

Garantire una corretta infomativa ai lavoratori.

Individuati gli strumenti di lavoro, l'obbligazione fondamentale in capo alle aziende e alle pubbliche amministrazioni, è di garantire al lavoratore una corretta informativa sulle modalità d'uso ed i potenziali controlli per ciascuno strumento di lavoro nel rispetto dell'art. 13

Quando opera il ricorso all'accordo sindacale?

Agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze non opera il filtro dell'accordo con le rappresentanze sindacali o dell'autorizzazione dell'INL.

Il nuovo art. 4 St. Lav. prevede, infine, che è consentito un utilizzo delle informazioni raccolte ai sensi dei commi 1 e 2 "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 GDPR.

Definizione distrumento di lavoro.

In particolare, l'INL con circolare del 2016, ha precisato che possono considerarsi strumenti di lavoro gli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità siano stati posti in uso e messi a sua disposizione. il Garante della Privacy con verifica preliminare e 2017, ha confermato che gli strumenti di lavoro sono tutti quei dispositivi utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa, ovvero direttamente preordinati all'esecuzione della prestazione lavorativa.

Esempio di strumento di lavoro.

Sistemi di gestione dell'anagrafica del cliente e dei dati relativi ai rapporti contrattuali in essere con il gestore telefonico che rendono più completa l'informazione e più efficiente la relazione tra il chiamante e l'operatore.

Software del genere, che consentono "il mero accoppiamento fra la chiamata e l'anagrafica del cliente senza possibili ulteriori elaborazioni" possono essere considerati uno strumento utile al lavoratore per rendere la prestazione lavorativa.

Lo strumento di lavoro per il lavoratore nei Call Center.

Il sistema che gestisce le chiamate di un call center dedicato agli abbonati di un dato servizio e che non si limiti ad associare la chiamata e l'anagrafica del cliente per facilitare la gestione della richiesta dell'abbonato, ma consenta ulteriori elaborazioni (es. memorizzazioni di dati personali degli operatori ed estrarre report), non può essere considerato uno strumento di lavoro utilizzato dall'operatore per rendere la prestazione; esso rientra tra gli strumenti diretti a soddisfare esigenze organizzative e produttive del datore di lavoro dai quali può derivare il controllo a distanza dei lavoratori.

Computer aziendali e posta elettronica. Casi.

Alcune pronunce sull'applicabilità degli oneri di cui al comma 1 del nuovo articolo 4 in casi di licenziamento di dipendenti motivati dall'uso improprio di pc e posta elettronica emerso a seguito di controlli sugli accessi internet e sulla mail. Il caso dell'impiegata amministrativa alla quale era stato contestato il prolungato uso per fini personali degli strumenti informatici aziendali, uso che aveva cagionato la contrazione di un virus da parte del sistema informatico della società con conseguente perdita di dati aziendali importanti (Tribunale di Roma, sentenza del 24/03/2017).

Il giudice di merito ha spiegato che devono considerarsi strumenti di lavoro la posta elettronica e il pc concessi in un uso alla dipendente con mansioni di impiegata amministrativa in quanto beni necessari allo svolgimento della prestazione lavorativa. Ne consegue che la loro installazione non richiede gli adempimenti di natura amministrativa e sindacale previsti dal comma 1 dell'art. 4. Inoltre, i dati raccolti possono essere utilizzati dal datore a tutti i fini connessi al rapporto di lavoro, ivi compreso quello disciplinare, purché sia stata data al lavoratore adeguata informazione sulle modalità d'uso di tale strumentazione e di effettuazione dei controlli.

Inutilizzabilità in giudizio dei dati estratti controllando unamail per mancanza di contenuto informativo.

Il giudice ha negato l'utilizzabilità disciplinare e processuale dei dati ricavati dal controllo delle e-mail del dipendente perché la policy aziendale non aveva un contenuto informativo sulle modalità d'uso degli strumenti e di effettuazione dei controlli tale da soddisfare i requisiti richiesti dalla norma (Tribunale di Roma, sentenza del 13/06/2018, n. 57668).

In sostanza, come spiegato del giudice, la policy non può limitarsi a disciplinare l'uso della posta e a mettere in evidenza che la violazione delle regole può dar luogo a problemi di sicurezza informativa e di indebita diffusione di dati riservati, ma deve contenere un chiaro riferimento al possibile svolgimento dell'attività di controllo e alle relative modalità di utilizzo.

Consultazione siti web

Altro caso sul licenziamento di un dipendente a causa di una consultazione di siti web di borsa e finanza che risultava estranea all'oggetto della prestazione lavorativa (Tribunale di Torino, sentenza del 19/09/2018, n. 1664).

Il giudice di merito ha spiegato che l'informativa non deve ridursi ad un adempimento formale rivolto alla generalità dei lavoratori, ma deve essere esaustiva e adeguata: tale non è l'indicazione di istruzioni relative all'uso dello strumento tecnologico, non accompagnate dalla specifica individuazione delle modalità di utilizzo che comportano l'acquisizione dei dati. L'informativa, in sostanza, non è adeguata quando, rivolgendosi alla generalità dei dipendenti, si limiti a prescrivere direttive riguardanti tutte le tipologie di

GPS Aziende di trasporti rifiuti speciali pericolosi.

L’istallazione è stata motivata da ragioni di sicurezza e di tutela dei beni e delle persone, considerato il forte tasso di criminalità dell’area in cui la società svolge l’attività.

Tali dispositivi permettono di visualizzare la posizione degli automezzi, di controllare il percorso, il tempo di guida e la velocità media tenuta da ogni veicolo, di avere un report riassuntivo in tempo reale dello stato degli automezzi, di avere un riassunto dei dati aggregati relativi ai mezzi monitorati e di aggiornare la posizione geografica dell’automezzo ogni due minuti.

Tali modalità di funzionamento del sistema di geolocalizzazione non sono ritenute dal Garante proporzionate agli scopi rappresentati dalla società in quanto questi “avrebbero potuto essere utilmente e legittimamente perseguiti con la raccolta di informazioni più limitate. Né è risultato conforme al principio di proporzionalità la integrale conservazione dei dati raccolti per un esteso periodo di tempo in relazione alle finalità perseguite.

App dimissioni volontarie.

È disponibile da gennaio 2018 l'app "Dimissioni Volontarie" messa a disposizione dal Ministero del Lavoro e delle Politiche Sociali per le dimissioni volontarie e la risoluzione consensuale del rapporto di lavoro.

con il "Jobs Act", a partire dal 12 marzo 2016 le dimissioni volontarie e la risoluzione consensuale del rapporto di lavoro devono essere effettuate in modalità esclusivamente telematica.

Per accedere, i cittadini dovranno essere in possesso di SPID, il Sistema Pubblico di Identità Digitale introdotto sulla piattaforma dei servizi del Ministero dallo scorso 19 maggio 2017. I soggetti abilitati potranno utilizzare le proprie credenziali di accesso al portale dei servizi del Ministero del Lavoro e delle Politiche Sociali.

App Aziendali anti-Covid

Si moltiplicano le app aziendali per il contrasto al covid e si entrano in una fase di convivenza con l’app Immuni, che pure ha ricadute sulla vita lavorativa.

Nuove App sulla salute dei lavoratori.

Esistono App predisposte per smartphone e tablet che consentono di ridurre il rischio di contagio da Covid-19 sui posti di lavoro nel pieno rispetto della privacy dei lavoratori.

Si tratta di App che, una volta attivate dall'azienda ed installate dai singoli dipendenti, attivano una serie di algoritmi capaci di mappare gli ambienti elaborando più segnali da svariati terminali.

Sono uno strumento di verifica, ma non di controllo nel pieno rispetto dell'art. 4 dello Statuto dei Lavoratori in modo assolutamente anonimo, della distanza.

Per il distanziamento sociale in azienda val la pena citare anche i tanti braccialetti in sperimentazione. Vibrano se i lavoratori si avvicinano troppo.

Scaricare vontariamente le App non legittima automaticamente il trattamento.

Ci si chiede quale è la base giuridica da poter invocare per poter utilizzare ovvero trattare i dati che potrebbero emergere dall'utilizzo di qualunque App aziendale di contact tracing.

Il consenso deve essere la base di legittimità residuale ed evitare squilibri tra datore e dipendente.

Al fine di contenere il rischio di contagio sul luogo di lavoro sono disponibili applicativi che non trattano dati personali?

Il datore di lavoro può ricorrere all'utilizzo di applicativi, allo stato disponibili sul mercato, che non comportano il trattamento di dati personali riferiti a soggetti identificati o identificabili.

Ciò nel caso in cui il dispositivo utilizzato non sia associato o associabile, anche indirettamente (es. attraverso un codice o altra informazione), all'interessato né preveda la registrazione dei dati trattati.

Particolari categorie di dati personali trattate.

Il trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante, effettuato da soggetti che svolgono c*ompiti di interesse pubblico o connessi all'esercizio di pubblici poteri,* che per la materia del lavoro e della previdenza, era in precedenza trattato, nell'ambito dell'art.112 de Codice, è stato accorpato in un unicum all'art. 2 sexies. Con riferimento ai *compiti* in materia di *instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro* oltre agli *adempimenti degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro*, ma anche quelli relativi all'accertamento *della responsabilità civile/disciplinare* e *attività ispettiva.*

Trattamento per fini disciplinari.

Risultano abrogati dal decreto gli articoli 24 e 26 del Codice, che rispettivamente alla lett. f) del co.1 ed al co. 2 lett. c), consentivano i trattamenti di dati personali “comuni” e “dati sensibili”, senza il necessario consenso, quando ciò fosse stato finalizzato (e necessario) a *far valere o difendere un diritto in giudizio*.

L´azienda può trattare i dati giudiziari, ma solo se autorizzata dalla legge o dal Garante.

Il Garante per la protezione dei dati personali ha rigettato l´istanza di una società che chiedeva di essere autorizzata ad effettuare un trattamento di dati giudiziari dei propri dipendenti non previsto da una adeguata base giuridica.

Le App per la rilevazione delle presenze. Trattamento dei dati e localizzazione.

Il trattamento dei dati personali connesso all´installazione di una specifica applicazione (contenente una funzionalità di localizzazione geografica) sul dispositivo smartphone dei dipendenti, può essere preordinata all'effettuazione della timbratura del cartellino e la rilevazione delle presenze.

Tale applicazione, è configurata in modo tale da consentire l´accesso (previa autenticazione con user id e password) al dipendente, che cliccherà su icona ingresso per indicare l´inizio dell´attività lavorativa e su uscita per indicare la fine della giornata lavorativa.

Quando l'App viene attivata, questa presenta al lavoratore il nome e cognome che è stato registrato in modo da confermare la sua identità e lo informa del raggio di approssimazione di lettura della posizione fisica che verrà associata alla timbratura. Verificate queste informazioni, il lavoratore potrà decidere il momento in cui effettuare la timbratura selezionando inizio o termine dell´attività. Solo ed unicamente a questo punto la App richiederà allo smartphone le coordinate geografiche della posizione in cui si trova e le trasmetterà al sistema di raccolta delle timbrature unitamente al codice identificativo del lavoratore, al verso di timbratura e alla data e ora di effettuazione.

Vantaggi per le aziende.

conseguire risparmi di costi e maggiore efficienza;

la società non dovrà più approvvigionarsi dei terminali lettori di badge e non dovrà più provvedere alla loro manutenzione e/o sostituzione anche presso le aziende utilizzatrici;

eliminazione dei contenziosi dovuti a mancato funzionamento o preteso mancato funzionamento dei lettori; verificare in tempi molto più rapidi la presenza di personale nei luoghi di lavoro; ridurre la commissione di illeciti.

Vantaggi per il lavoratore

La funzionalità di geolocalizzazione non consentirà alcun controllo dell´attività lavorativa;

i dati personali trattati mediante l´installazione sui dispositivi di proprietà dei dipendenti dell´applicazione sono identificativo del dipendente, orario di entrata, luogo di timbratura, orario di uscita, dispositivo tramite il quale viene effettuata la timbratura;

l´uso della App non è obbligatorio e sarà data piena libertà di scelta rispetto all´utilizzo della stessa;

fornire una maggiore tutela al lavoratore, che si vedrà conteggiate e retribuite tutte le ore effettivamente lavorate, comprese le ore di straordinario.

Pivacy by design nella registrazione delle presenze.

Per le app utilizzate dai lavoratori aziendali come strumento di registrazione delle presenze il Garante ha espressamente prescritto di perfezionare il sistema nella prospettiva della “privacy by design”, applicando il principio di necessità, soprattutto alla luce dei possibili conseguenti derivanti dal non corretto utilizzo dei sistemi di localizzazione connessi alle suddette applicazioni.

Conclusione

Il Jobs Act che ha modificato l'articolo 4 dello Statuto dei lavoratori, introducendo la possibilità per le aziende di controllare, senza accordo sindacale, i dispositivi utilizzati dai dipendenti.

I lavoratori però dovranno essere informati sulle modalità con cui smartphone, pc e tablet, forniti per essere usati sul posto di lavoro, potranno essere monitorati. I dati ricavati dai controlli saranno utilizzabili per ogni fine connesso al rapporto di lavoro, quindi anche per motivi disciplinari, oltre che organizzativi e di sicurezza.

I criteri da rispettare rimarranno sempre la necessità del trattamento dei dati personali e la corretta informazione ai dipendenti.

I decreti attuativi del Jobs Act porterebbero a utilizzare dati ottenuti per i controlli per valutare l'inadempimento contrattuale del lavoratore.

I magistrati dovranno anche stabilire la differenza tra i dati acquisibili e quelli effettivamente utilizzabili dal datore di lavoro.

…. segue

Il controllo dei lavoratori, ormai, è possibile non solo attraverso le classiche telecamere, ma anche attraverso molteplici dispositivi che devono essere vagliati uno ad uno dal datore. Questi, infatti, è chiamato a stabilire preventivamente se tali dispositivi siano strumenti di lavoro o altro tipo di strumento dal quale derivi la possibilità di un controllo a distanza. Una volta fatta la distinzione, per i secondi bisognerà attivarsi per stipulare un accordo sindacale o, in mancanza, per conseguire l'autorizzazione dell'INL. E' necessario fare molta attenzione alle modalità di raccolta e trattamento dei dati personali rilevati nonché elaborare una policy particolarmente dettagliata: l'inadempimento di tali obblighi rischia di invalidare le prove raccolte contro un lavoratore inadempiente e di renderle inutilizzabili in un eventuale processo.

Va ricordato che la versione riformata dell'art. 4 SL, a seguito dell'ultimo decreto attuativo del Jobs Act, prevede che l'installazione di strumenti di controllo è possibile solo per esigenze organizzative e produttive, di sicurezza del lavoro e tutela del patrimonio aziendale e previo accordo sindacale, che però non è richiesto in caso di strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.