Federazione Regionale USB Liguria

Genova.Gruppo Iren e Privacy

Genova, 24/10/2023

il Problema della Privacy troppo spesso è stato trascurato nel Gruppo Iren per arrivare oggi ad una situazione che -a nostro parere presenta diverse situazioni discutibili.

il datore di lavoro sarebbe autorizzato a controllare i risultati del lavoro, non la persona"… dopo **la raccolta dei dati sui clienti, le aziende multiservizi stanno passando alla raccolta dei dati sui dipendenti. Non abbiamo evidenza in IREN di violazioni palesi, altrimenti avremmo proceduto con una denuncia ma un dato di fatto è l'utilizzo di Teams ai fini del controllo della presenza degli addetti amministrativi sdoganato peraltro da un accordo firmato dalle segreterie nazionali confederali con il** gruppo (accordo sullo smart working in IREN) permetta un tipo di controllo che **a nostro parere è illecito**.

Tali trattamenti sono da ritenersi in via di principio sproporzionati e quindi **non lecitamente utilizzabili**… Questo vale ancor più all'interno delle abitazioni private o dei luoghi pubblici presso i quali ad esempio il lavoratore smart opera; ad oggi quindi il controllo da parte del datore di lavoro nel nostro paese è tollerabile **fin quando non è lesivo delle prerogative della persona.**

Occorre ricordare che l'uso di software, atti a acquisire screenshot delle interazioni sui social o delle schermate del computer, non è consentito se non in base ad un fondato sospetto reato o di illecito.

Qualora il trattamento non sia soggetto a restrizioni e non sia trasparente, sussiste il rischio elevato che il legittimo interesse del datore di lavoro al miglioramento dell'efficienza e alla protezione dei beni aziendali si trasformi in un monitoraggio ingiustificabile e intrusivo (Commissione Europea cit. WP249 – Parere 2/2017 sul trattamento dei dati sul posto di lavoro).**quindi non avere mai ad oggetto la mera prestazione lavorativa del dipendente e rispettare la dignità e la riservatezza del lavoratore;**

Ne consegue ad esempio che l'utilizzo dell'applicativo Teams viene spesso travisato in IREN probabilmente per una scarsa formazione dei quadri intermedi o aspiranti tali che utilizzano le nuove tecnologie per rilevare la presenza del dipendente attraverso lo "stato" o coinvolgerlo in "room" di ore ed ore (pratica che nel vecchio mondo veniva descritta come "fiato sul collo") … uscendo un po dal tema non possiamo non citare le riunioni al di fuori della fascia di compresenza e addirittura -a volte- del normale orario di lavoro o nell'ora di pausa, che dopo il periodo del lock down sono diventate una abitudine.

Il Garante della Privacy, nell'audizione del 13 maggio 2020, ha dichiarato che "Il ricorso alle tecnologie non può rappresentare l'occasione per il monitoraggio sistematico del lavoratore. Deve avvenire nel rispetto delle garanzie sancite dallo Statuto a tutela dell'autodeterminazione del lavoratore (…)". Va inoltre assicurato – in modo più netto di quanto già previsto – anche quel diritto alla disconnessione, senza cui si rischia di vanificare la necessaria distinzione tra spazi di vita privata e attività lavorativa, annullando così alcune tra le più antiche conquiste raggiunte per il lavoro tradizionale (…)Il minimo comun denominatore di queste garanzie va individuato nel diritto alla protezione dei dati: presupposto necessario di quella libera autodeterminazione del lavoratore che ha rappresentato, come si è detto, una delle più importanti conquiste del diritto del lavoro".

Il lavoro da remoto può essere più produttivo, ma occorre disciplinarlo farlo anche con il **"diritto alla disconnessione" che non è solo una formula di tre parole vuote da aggiungere agli accordi sindacali** che poi prevedono come nell'accordo firmato dai nazionali con il Gruppo Iren esattamente l'opposto dalla fascia di presenza obbligatoria allo sdoganamento di TEAMS…

Qualora un'Azienda sia intenzionata ad utilizzare applicazioni di geolocalizzazione su smartphone per rilevare le presenze andrà presentata una richiesta di verifica preliminare al garante della Privacy (DLGS 196/2003 art.17); occorre poi notificarlo al garante della privacy ai sensi dell'art.37 comma 1 lettera a; fornire informativa ai dipendenti ai sensi dell'articolo 13 del codice ed effettuare la designazione degli incaricati e responsabili di tale trattamento…

A tale proposito il Garante nel 2016 (provvedimento n.350) ha stabilito che i dati da GPS con le posizioni del lavoratore non possono essere conservate e che comunque

sull’applicazione usata dal dipendente deve esser visibile la geolocalizzazione quando attiva.

In ogni caso comunque tali applicazioni non deve in alcun modo influire sui dati personali di posta sms traffico e navigazione in rete. Mentre è possibile rilevare le presenze attraverso i badge è comunque vietato l’utilizzo di dati biometrici o altri che permettano il controllo a distanza, e a questo punto ci chiediamo quanto siano leciti i solleciti di capi e capetti sul **“dove sei, cosa fai?”** che tanti piccoli Kapò in erba adottano in **IRETIgas** in **Ireti Acqua** ma anche in **Smart solutions** utilizzando il GPS. Un dato certo è che le posizioni del lavoratore tramite GPS NON possono essere archiviate o utilizzate successivamente. Vanno comunque rispettate le procedure previste all’art.4 legge 300 (accordo sindacale o INL) tuttavia il garante (217 n.138) ha sentenziato che il GPS è un elemento “aggiunto” agli strumenti di lavoro non utilizzato in via primaria ed essenziale, tale aspetto quindi può esser oggetto di contenzioso legale. Generalmente se viene richiesta l’autorizzazione all’INL viene rilasciata purchè sia permesso all’autista di attivare e disattivare l’apparato e in caso di funzionamento a tempo che sia visibile allo stesso tramite una spia luminosa il funzionamento dell’apparato.**E’ fatto divieto comunque di conservare dati che permettano il controllo sulla condotta del dipendente alla guida,** quindi la funzione si limita esclusivamente alla compilazione dei dati indispensabili altri dati possono essere trattati solo se in forma anonima (non legati al singolo operatore). E’ lecito quindi controllare tramite GPS quale sia il veicolo più vicino ad una zona ove sia richiesto un intervento ma è molto discutibile ogni utilizzo teso all’identificabilità degli autisti o meglio quando utilizzati il monitoraggio continuo dell’attività del dipendente; il dipendente inoltre deve avere la possibilità di disattivare il sistema durante le pause.

BLACKBOX su veicoli aziendali:

La raccolta dei dati deve essere utilizzata **esclusivamente per esigenze organizzative e per la sicurezza,** l’utilizzo di tali apparecchi (che permette peraltro una riduzione dei premi pagati per le polizze assicurative) rientra comunque nei sistemi di controllo a distanza del lavoratore tutelato dalla legge 300, occorre quindi prima della installazione un accordo con le RSU e in caso di esito negativo le aziende devono chiedere autorizzazione all’Ispettorato del Lavoro, Poste Italiane (dove non si era raggiunto un accordo) ha passato la richiesta al garante e le condizioni poste dagli enti competenti sono state:

1: informativa al personale in merito a motivazioni e modalità di funzionamento

2: all’impianto non può essere apportata alcuna modifica o elemento aggiuntivo non conforme all’art.4 legge 300 1970.

3: i dati scaricati dai dispositivi devono essere dati all’azienda in forma aggregata. E’ esplicito divieto dell’azienda richiedere e acquisire dati in forma non aggregata in modo che si possa risalire alla singola prestazione lavorativa.

4: E’ esclusa ogni altra finalità (oltre a sicurezza e esigenze organizzative) dei dati raccolti.

5: Deve essere rispettata tutta la normativa in materia di raccolta e conservazione delle immagini.

POSTA ELETTRONICA SKYPE, TEAMS, telefoni aziendali:

Per le caselle di posta “generiche” il lavoratore è tenuto a fornire la password al proprio superiore gerarchico ma per quanto riguarda le caselle di posta “nominali” queste sono uno spazio a disposizione “personale” e rientrano quindi nelle tutele degli spazi tutelati da riservatezza, infatti è escluso in modo assoluto la possibilità di controllo a meno che non sia stato perpetrato un reato. Sono vietati quindi i programmi atti a monitorare anche occasionalmente la posta in base all’articolo 4 della legge 300 1970. Il Garante con sentenza 2015 n.345 ha stabilito inoltre che le comunicazioni di tipo elettronico (skype o simili) sono assistite dalle garanzie di segretezza tutelate a livello costituzionale. Il Datore non può quindi monitorare tali conversazioni rispettando i limiti di **pertinenza e non eccedenza** (Codice Privacy art.11 comma 1).

Il controllo dei tabulati telefonici non rientra nelle tutele previste dall’art.4 della legge 300, il contenuto delle telefonate è invece tutelato anche con l’art.15 della Costituzione se non per motivi giudiziari. Tuttavia nel 2002 la Cassazione ha stabilito che i controlli difensivi delle aziende tesi ad accertare l’abuso del telefono aziendale, oltre a poter costituire causa di licenziamento NON rientrano nelle tutele dell’art.4 legge 300 (sentenza 4746 del 2002) mentre in merito ad una imputazione contabile viene definito caso per caso se lo stesso rientra o meno nelle tutele della legge 300… un argomento nuovo da approfondire e anche qui serve la voce di chi lavora contro la voce del padrone.

USB Lavoro Privato Genova - USB Gruppo Iren

#GRUPPO IREN #IRETIGAS #IREN ACQUA #SMART SOLUTIONS