Pillole di Sicurezza

Gli accordi aziendali di geolocalizzazione con dispositivi mobili

Data pubblicazione: 24 giugno 2015

Gli accordi aziendali di geolocalizzazione con dispositivi mobili.

Il ricorso alla tecnologia di geolocalizzazione, e quindi il ricorso a specifici strumenti informatici in ambito aziendale, sta diventando sempre più frequente andando ben oltre l'esigenza di localizzare i veicoli aziendali in caso di furto. Quando si discute in termini di geolocalizzazione in ambito aziendale quindi si ragiona necessariamente in termini di (possibile) controllo dell'attività lavorativa dei dipendenti.

Già dalla lettura di queste primissime righe, in particolare il riferimento all'utilizzo di strumenti [informatici] di lavoro, emerge in maniera chiara quali siano le problematiche sottese all'utilizzo della tecnologia di localizzazione geografica: abbiamo una questione che coinvolge l'immediato futuro (la riforma dell'art. 4 dello Statuto dei Lavoratori contenuta nell'ormai noto Jobs Act); ed un'altra invece contingente in merito alle prescrizioni da seguire nell'attuale quadro normativo.

Per quanto riguarda l'imminente riforma, in quest'articolo ci si limita a sollevare alcune questioni ((già per altro affrontate in un recente articolo a firma di Gabriele Faggioli, Presidente Clusit) in attesa del testo finale che sarà approvato.

Con la proposta di riforma dell'art. 4 dello Statuto del Lavoratori (in materia di controlli a distanza dell'attività lavorativa), a chi scrive, sembra che si stia tentando di compiere un'operazione di acrobazia giuridica alla ricerca di una quadra che a chi scrive sembra ben lungi dal riuscire.

Al primo comma, sia pure con alcune modifiche, si intende mantenere il senso della precedente previsione (cioè, in linea generale -salvo quanto poi precisato nel medesimo articolo, a cui si rimanda-, il divieto da parte del datore di lavoro di controllare l'attività lavorativa dei propri dipendenti); mentre al secondo comma si esclude l'applicazione del divieto *"agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze"*.

Come a dire, ragionando per analogia, che si vieta il controllo di un'entrata, ma si permette il controllo della porta in quanto oggetto per aprire.

A ciò si aggiunga che l'estrema genericità della lettera del citato secondo comma lascerà un tale spazio interpretativo alla giurisprudenza tale da non offrire alcuna garanzia di certezza del diritto (per lo meno sino a quando non si arriverà a orientamenti stabili e condivisi), sempre necessaria e che diviene ancor più indispensabile quando si interviene su diritti fondamentali.

Sia detto subito chiaramente, si ritiene che la disciplina in materia di controllo dell'attività lavorativa vada con ogni probabilità riformata ed aggiornata; tuttavia si stenta a credere che la scelta fatta, ove divenisse legge, sia quella più corretta.

Passando invece ad analizzare la situazione attuale si deve sottolineare come la tecnologia di geolocalizzazione, se correttamente gestita, permetta sia di alzare la soglia di sicurezza per il business dell'impresa, sia di offrire servizi e prodotti in modo sempre più efficace ed efficiente (senza contare la possibilità di intraprendere percorsi di marketing altamente innovativi, che pone ben altri problemi). E'

bene precisare per inciso, come sia evidente che ciò (migliore sicurezza ed efficienza) sarà possibile solo e soltanto nel momento in cui l'impresa va ad adottare tutte le accortezze e best practice richieste per la gestione dei sistemi informatici e telematici che sottendono l'utilizzo e l'implementazione di tali strumenti.

Non è certamente questa la sede per affrontare tale ultima tematica, in quanto ora ci s'intende invece focalizzare sugli aspetti più strettamente legati all'organizzazione dell'attività d'impresa ed alle prescrizioni che devono essere rispettate alla luce delle ultimissime decisioni adottate dal Garante per la tutela dei dati personali.

Si ricorda che secondo l'attuale quadro normativo è fatto divieto al datore di lavoro (art. 4 della L. 300/1970) di predisporre strumenti che permettano allo stesso di monitorare l'attività dei lavoratori: strumenti che vanno dalla videosorveglianza sino ai controlli sui computer aziendali per arrivare, appunto, alla geolocalizzazione.

Senza addentrarsi eccessivamente su tale problematica, estremamente vasta, è tuttavia opportuno rammentare che lo Statuto dei Lavoratori fa comunque salva la possibilità da parte del datore (previo coinvolgimento, però, delle rappresentanze sindacali o dell'ispettorato del lavoro competente) di utilizzare apparecchiature -che per loro natura potrebbero determinare un controllo sull'attività dei lavoratori- volte tuttavia a perseguire esigenze organizzative e produttive o ad assicurare esigenze di sicurezza a tutela dell'azienda. Non solo, ma -ha ormai da tempo spiegato la Corte di Cassazione- all'imprenditore, in presenza di determinate condizioni, è permesso predisporre procedure ed apparecchiature per i c.d. controlli difensivi (sul cui tema si richiama la recentissima sentenza della Corte di Cassazione civile, Sez. Lav., 27/05/2015, n. 10955 in cui è stato considerato legittimo che un imprenditore verificasse, tramite l'apertura di un falso account facebook, l'effettivo comportamento illecito del proprio dipendente).

In tema di controllo a distanza, come noto, è intervenuto anche il Garante per la tutela dei dati personali (in considerazione dell'esplicito richiamo dell'art. 114 del d.lgs 196/2003 all'art. 4 dello Statuto dei Lavoratori).

L'Autorità ha avuto modo di chiarire quale sia il giusto contemperamento tra sicurezza, efficienza aziendale, divieto di controllo dell'attività lavorativa, e tutela della privacy.

In particolare si devono richiamare i provvedimenti in materia di videosorveglianza (dell'aprile 2010) e di utilizzo di internet e posta elettronica in azienda (del marzo 2007) nelle cui premesse il Garante ha ribadito che il citato contemperamento poggia le proprie basi soprattutto sul rispetto dei principi di necessità, pertinenza e non eccedenza.

Provvedimenti a cui, per evidente ragioni, dovrà poi aggiungersi anche il n. 370 del 4 ottobre 2011, relativo all'utilizzo di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro.

Che cosa avviene allora quando un'impresa intende sfruttare i sistemi di geolocalizzazione e, in particolare, quando per far ciò l'azienda ricorre all'utilizzo di smartphone consegnati ai dipendenti?

Il ricorso alla tecnologia di geolocalizzazione permette a molte aziende di fare un salto in avanti nella gestione ed erogazione efficiente e competitiva dei propri servizi e prodotti.

Tra i tanti vantaggi che possono essere individuati, oltre al già richiamato monitoraggio dei veicoli aziendali, è possibile segnalare: l'utilizzo delle c.d. scatole nere nelle auto per quanto concerne il settore assicurativo; la garanzia di elevati livelli di tutela per le attività di soccorso ed intervento; il netto miglioramento dei livelli di servizio; una pianificazione ottimizzata del lavoro; la gestione delle attività d'emergenza mediante la conoscenza della posizione dei tecnici; l'identificazione del tecnico più qualificato e più vicino al sito per il quale è richiesto l'intervento; ed altro ancora.

Tuttavia per poter ricorrere a tali strumenti è necessario rispettare la richiamata normativa in materia di controllo a distanza dei lavoratori così come integrata dai provvedimenti che in materia ha emesso Garante (prescrizioni, queste ultime, che impongono regole molto stringenti), nonché dai principi e dalle indicazioni fornite dalla giurisprudenza. Tutti elementi che è assolutamente necessario conoscere in modo da poter sfruttare le potenzialità offerte dai sistemi di localizzazione geografica e quindi mettersi in condizione da poter redigere un accordo (che potrebbe, appunto, essere definito "di geolocalizzazione") avente ad oggetto l'utilizzo di questi sistemi in ambito aziendale; un accordo che si presenti efficace e che sia predisposto in maniera tale da tutelare sotto ogni aspetto impresa e lavoratori, senza possibilità di poter sollevare eccezioni e contestazioni sul punto.

In merito alla corretta redazione di tal tipo di accordi vanno tenuti in debito conto i provvedimenti adottati dal Garante Privacy sopra richiamati (videosorveglianza, controllo internet ed email e geolocalizzazione), ma anche le recentissime decisioni adottate dall'Autorità in seguito a specifiche istanze alla stessa inoltrate, datate 11 settembre 2014, 9 ottobre 2014 e 22 gennaio 2015.

Il Garante ha accolto le istanze che gli sono state sottoposte partendo dalla verifica sia del rispetto dei principi fondamentali, già sopra richiamati, di pertinenza e necessità, sia della sussistenza e correttezza del giusto bilanciamento di interessi ai sensi dell'art. 24, comma 1, lett. g, del d.lgs 296/2003.

Proprio in ragione di tale verifica il Garante Privacy ha avuto modo di chiarire che il trattamento dei dati personali se ben strutturato secondo le direttive che sono state dettate, non necessita di un previo consenso degli interessati; ciò, evidentemente, solo e soltanto nel momento in cui l'accordo di geolocalizzazione venga strutturato secondo le indicazioni dette.

Per mera esigenza di chiarezza si precisa che si sta discutendo in termini di accordo proprio perché, stante la normativa vigente, al fine di implementare un sistema di geolocalizzazione nei telefoni aziendali si renderà necessario concordare con le rappresentanze sindacali o, in assenza, sede di Ispettorato del Lavoro, tutti gli aspetti relativi all'utilizzo dei sistemi in oggetto in quanto gli stessi potrebbero consentire un controllo sull'attività lavorativa dei dipendenti.

A parere di chi scrive, proprio in ragione del fatto che spesso gli incontri tra datore e lavoratori risultano tutt'altro che semplici e sereni, è opportuno presentarsi con un documento organico che affronti ogni

aspetto di questa delicata questione; documento che, oltre alle indicazioni del Garante, dovrà essere evidentemente e necessariamente redatto tenendo in debito conto la situazione contestuale dell'azienda e del business o servizio offerto.

Si precisa altresì che in considerazione del fatto (a questo punto assolutamente evidente) che il software che si intende installare sul device mobile comporta il trattamento di dati relativi alla localizzazione, l'impresa è tenuta sempre ad effettuare la notificazione ai sensi dell'art. 37, comma 1, lett. a), del Codice della Privacy.

Il Garante per al tutela dei dati personali, in ogni caso, nelle decisioni su indicate ha indicato tutta una serie di accorgimenti da dover adottare in relazione al trattamento dei dati conseguente all'utilizzo di sistemi di localizzazione geografica tramite smartphone aziendale che sono:

1) vanno individuate in maniera chiara e ben comprensibile le ragioni e gli obiettivi in base ai quali l'impresa ha deciso di utilizzare strumenti che permettono la geolocalizzazione;
2) va esclusa interazione con altri sistemi aziendali;
3) va chiaramente identificato il software installato nel dispositivo mobile;
4) il software deve permettere al dipendente di attivarlo e disattivarlo in modo da essere utilizzato soltanto nell'orario di lavoro;
5) l'applicazione deve essere facilmente identificabile sul dispositivo in modo da capire se e quando è attiva;
6) il software deve essere costruito in modo tale da non avviarsi in automatico, da non registrare e/o interagire (anche in background) con le altre applicazione del dispositivo;
7) l'esclusione della possibilità tecnica di accedere alla posizione geografica del dispositivo in un momento dato al di fuori dell'intervallo temporale prestabilito a monte;
8) i dati c.d. transazionali, di natura operativa e che contengono le informazioni relative agli ordinativi di lavoro devono essere memorizzati localmente e quindi essere presenti solo sul dispositivo mobile. Deve essere prevista anche un'operazione di cancellazione che può compiere l'utente che comporta la rimozione dei suddetti dati dal dispositivo mobile;
9) l'invio dei dati di localizzazione non deve essere continua e non deve essere possibile la storicizzazione dei trattamenti, pertanto i dati devono essere man mano eliminati all'arrivo degli aggiornamenti, nonché eliminati a fine giornata lavorativa;
10) si consiglia altresì la creazione di un canale criptato di trasmissione;
11) gli addetti all'accesso ai dati che vengono trasmessi, nonché -in caso di malfunzionamento del sistema- il tecnico che è autorizzato ad intervenire, devono essere previamente e specificatamente individuati ed autorizzati. Deve essere noto l'elenco di questi addetti;

12) tutte le attività relative alla gestione del sistema devono essere registrate e l'eventuale accesso a queste informazioni deve essere correttamente disciplinato nel rispetto del bilanciamento degli interessi tra datore e dipendenti;

13) in relazione ai tempi di conservazione il sistema, relativamente ai dati di localizzazione, deve mantenere solo la località di partenza e l'ultima posizione conosciuta;

14) nessuna informazione storica relativa alla localizzazione deve essere mantenuta nel Sistema;

15) se da una parte non è necessario il consenso dei singoli lavoratori, tuttavia l'azienda è obbligata a rendere nota ed a comunicare efficacemente ai propri dipendenti un'opportuna e completa informativa;

16) devono essere in ogni caso predisposte tutte le opportune misure minime di sicurezza previste dal Codice Privacy (a cominciare dal prevedere che l'accesso dell'utente all'applicazione deve avvenire attraverso un'autenticazione basata su userid e password), nonché quelle relative all'utilizzo di internet e posta elettronica;

17) deve essere previsto che in caso di furto o smarrimento del dispositivo l'immediato blocco dell'utenza mobile, l'eventuale denuncia alle AA.GG. e la richiesta di blocco all'operatore telefonico;

18) deve essere esplicitamente dichiarato che le informazioni riferibili ai possessori dei dispositivi saranno utilizzate per finalità non riconducibili a quelle di controllo degli stessi, tanto che nessun utilizzo dei dati potrà avvenire per finalità diverse da quelle dichiarate, come ad esempio per scopi disciplinari;

19) deve essere esplicitamente chiarito se sia consentito o meno un uso promiscuo del device mobile consegnato dall'azienda

Come si può facilmente arguire le indicazioni fornite dal Garante non sono poche, ma a ben vedere la loro implementazione non si presenta particolarmente gravosa inserendosi perfettamente nel sistema già collaudato di relazione tra Statuto dei Lavoratori e Codice Privacy.

Un'ultima considerazione va tuttavia fatta. Ragionando in termini di security aziendale l'imprenditore dovrà sempre tenere in debito conto le informazioni che l'applicazione potrebbe comunque lasciare all'interno del dispositivo e pertanto si ritiene sia consigliabile, per quanto banale potrebbe sembrare questa affermazione, che i dipendenti vengano formati in merito alla corretta gestione ed utilizzo "in sicurezza" del dispositivo mobile consegnato dall'azienda.

E' infatti chiaro come, sotto il profilo strettamente della sicurezza il ricorso agli smartphone o comunque ai device mobili in ambito lavorativo, porta con sé tutte le problematiche tecniche e di policy che il mondo mobile presenta e che sono ancora lontane dall'essere risolte se non addirittura correttamente affrontate.

Sarebbe infatti interessante conoscere un'analisi tecnica, sotto questi profili, che sia sviluppata passo passo seguendo i punti indicati dal Garante.

Emiliano Vitelli

Emiliano Vitelli, Avvocato, è nato a Latina il 7 marzo 1974. Si è laureato nel 1999 in giurisprudenza presso l'Università di Roma "La Sapienza" con il Prof. Stefano Rodotà con una tesi in "*Aspetti civili della crittografia in rete*". Si è abilitato nel 2003 alla professione forense sostenendo l'esame presso la Corte di Appello di Roma. Si è laureato nel master di "*Sicurezza informatica e disciplina giuridica*" presso l'università di Modena e Reggio Emilia. E' Auditor *ISO 27001:2013* ed *ISO 20000:2011*.

Svolge la propria attività giudiziale sia in materia civile (contenziosi innanzi al Corecom, all'AgCom ed al Garante Privacy, diritto del lavoro e diritto della famiglia, contrattualistica, ecc.) sia in materia penale (truffa, spaccio di stupefacenti, prostituzione, reati informatici, furti di identità, violazione degli obblighi verso i minori, associazione a delinquere, infortuni sui luoghi del lavoro, ecc). Mentre in ambito stragiudiziale si occupa di tutela di marchi, modelli di utilità e brevetti, regolamenti aziendali, D.P.S., Responsabilità amministrativa degli enti, accordi di franchising, somministrazione, non disclosure agreement, concessione in vendita, accordi tra rete di imprese, ecc.