PRIVACY

Lavoratore localizzabile tramite smartphone

Ciccia a pag. 32

Dal garante privacy decisioni anche su graduatorie scolastiche, furti d'identità e cambiavalute

Lavoratore sempre localizzabile

Lo smartphone aziendale potrà seguire il dipendente

DI ANTONIO CICCIA

Lavoratore localizzabile con lo smartphone aziendale. Ma senza esagerare. Una app, ben visibile sullo schermo, deve ricordare al dipendente la possibilità di essere individuato tramite il dispositivo. Con due decisioni del garante della privacy (n. 401 dell'11 settembre 2014 e n. 448 del 9 ottobre 2014), due società telefoniche sono state autorizzate a utilizzare, senza necessità di acquisire il consenso del dipendente, i dati di localizzazione geografica, rilevati da un'app attiva sugli smartphone in dotazione ai lavoratori, ma con una serie di cautele. Prima fra tutte la trattativa sindacale, prevista dall'articolo 4 dello Statuto dei lavoratori, preventiva all'installazione di sistemi da cui possa derivare un controllo a distanza dei lavoratori.

In materia si contrappongono le esigenze produttive dell'impresa di coordinare meglio gli interventi dei dipendenti (per esempio tecnici chiamati a interventi sul territorio) e di tutela della sicurezza dei dipendenti stessi, e dall'altro lato la tutela della riservatezza. Lo smartphone, per le proprie caratteristiche, è destinato a seguire la persona che lo possiede, senza distinzione tra tempo di lavoro e tempo di non lavoro. Il trattamento dei dati di localizzazione può presentare, quindi, rischi specifici per la libertà, i diritti e la dignità del dipendente. Il bilanciamento viene stabilito imponendo le seguenti precauzioni. Le uniche informazioni a disposizione dell'impresa devono essere i dati di geolocalizzazione, mentre è vietato l'eventuale trattamento di dati ulteriori, come il traffico telefonico, gli sms, la posta elettronica o altro. Sul dispositivo un'icona, ben visibile, deve indicare che la funzionalità di localizzazione è attiva. Il trattamento dei dati in tempo reale è ammesso solo in presenza di situazioni di emergenza o di pericolo per il dipendente, o altre simili, da individuare con apposite policy aziendali. Inoltre i dipendenti devono effettuare periodicamente la pulizia dei dati memorizzati e la società deve effettuare la notifica al Garante (articolo 37 del codice della privacy). I dipendenti devono ricevere l'informativa, e, in particolare, devono sapere quando è consentita la disattivazione della funzione di localizzazione nel corso dell'orario di lavoro

Scuola. Stop alla pubblicazione online di graduatorie scolastiche in cui sia indicata la disabilità dei docenti. Il garante privacy ha dichiarato illecito (provvedimento n. 426 del 25 settembre 2014) il trattamento di dati effettuato da un Ufficio scolastico regionale e ha vietato l'ulteriore diffusione in Internet di informazioni sulla salute e di altri dati non pertinenti riferiti a decine di insegnanti.

Furti di identità. Il garante ha rilasciato pareri favorevoli (provvedimento n. 408 del 18 settembre 2014 e n.445 del 9 ottobre 2014) su due schemi di convenzione relativi al funzionamento del sistema di prevenzione delle frodi nel settore del credito al consumo, con particolare riferimento ai furti di identità. Il sistema è basato su un archivio centrale informatizzato, gestito da Consap Spa, su incarico del Ministero dell'economia e delle finanze (Mef). Il sistema consente di consultare le banche dati di numerosi enti pubblici (Agenzia delle entrate, Ministero dell'interno, ministero dei trasporti e delle infrastrutture, Inps, Inail) e verificare l'identità di chi acquista beni e servizi ed evitare che si usino i dati di terzi malcapitati.

La prima convenzione definisce le regole a cui devono sottostare le società che ricevono una domanda di finanziamento o altri servizi (banche, intermediari finanziari, fornitori di servizi di comunicazione elettronica o di altri servizi, imprese di assicurazione) per poter accedere al sistema.

La seconda convenzione regola invece l'attività dei gestori di sistemi di informazioni creditizie (SIC) e delle imprese che offrono servizi assimilabili, che le banche e gli altri aderenti diretti possono incaricare per l'accertamento, tramite il sistema, la veridicità della documentazione presentata.

Cambiavalute. Il garante della privacy ha dato parere favorevole (provvedimento n. 425 del 25 settembre 2014) a uno schema di decreto del ministro dell'economia, in base al quale chi esercita professionalmente l'attività di cambiavalute dovrà comunicare mensilmente all'organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi (Oam) l'elenco di tutte le negoziazioni effettuate e i dati identificativi dei clienti. L'Oam, che per legge ha il compito di conservare i dati per dieci anni, dovrà anche predisporre idonei sistemi di salvataggio dei dati e di disaster recovery per ripristinare le funzionalità del sistema informatico in caso di incidenti.


ItaliaOggi
Più Iva uguale più evasione
contro i piccoli guasti domestici, arriva eni sos casa