Garante per la protezione dei dati personali - Provvedimenti n. 401 dell'11 settembre 2014 e n. 448 del 9 ottobre 2014

L'Autorità Garante per la protezione dei dati personali ha dato il via libera a due società telefoniche per l'utilizzo dei dati di localizzazione geografica, rilevati da una *APP* attiva sugli *smartphone* forniti in dotazione ai propri lavoratori, a condizione che vengano adottate adeguate cautele a protezione della vita privata dei soggetti coinvolti. L'utilizzo di dati geolocalizzati può, di fatto, comportare rischi specifici per la libertà, i diritti e la dignità dei dipendenti, e il datore di lavoro non può considerare i sistemi di geolocalizzazione come strumenti per seguire o monitorare il comportamento o gli spostamenti del suo personale dipendente.

Graziano GARRISI, avvocato specializzato in diritto delle nuove tecnologie, Privacy e modelli organizzativi 231. Membro del Direttivo ANORC e vice coordinatore nazionale di ABIRT.

UTILIZZO DEI DATI DI LOCALIZZAZIONE DELLO *SMARTPHONE* IN DOTAZIONE AL DIPENDENTE

di Graziano GARRISI

La problematica relativa alla geolocalizzazione dei lavoratori dipendenti è stata da sempre al centro di particolari attenzioni da parte dell'Autorità Garante per la protezione dei dati personali, soprattutto per i rischi che questa particolare tipologia di trattamento comporta in capo ai soggetti interessati. Se, poi, questa attività viene effettuata attraverso l'utilizzo di *smartphone* e *tablet* - che generalmente contengono grandi quantità di dati di natura riservata o personale e riguardano direttamente o indirettamente gli utenti o terzi soggetti (es. indirizzi, dati sulla localizzazione geografica, informazioni bancarie, foto, video) - i rischi per la privacy diventano veramente elevati. Dalla gestione aziendale di questi nuovi strumenti e applicazioni, infatti, può derivare un controllo occulto o a distanza dei lavoratori e, più in generale, problematiche relative al corretto trattamento dei dati.

Con due provvedimenti specifici, emanati sulla base di una richiesta di verifica preliminare (art. 17 del D.Lgs. 196/2003), l'Autorità ha dato il via libera a due società telefoniche per l'utilizzo dei dati di localizzazione geografica, rilevati da una *APP* attiva sugli *smartphone* dati in dotazione ai lavoratori, purché vengano adottate adeguate cautele a protezione della vita privata dei soggetti coinvolti. Infatti, poiché lo *smartphone* è uno strumento che segue la persona nei suoi vari spostamenti, senza distinzione tra tempo di lavoro e tempo libero (riservato esclusivamente alla vita personale dell'interessato al trattamento), l'utilizzo di dati geolocalizzati può comportare di fatto rischi specifici per la libertà, i diritti e la dignità dei dipendenti, e il datore di lavoro non può considerare i sistemi di geolocalizzazione come strumenti per seguire o monitorare il comportamento o gli spostamenti del suo personale dipendente.

In particolare, gli strumenti utilizzati dalle due società telefoniche presentano le seguenti caratteristiche:

- nel primo caso (provvedimento dell'11 settembre 2014), si tratta di dispositivi dotati di GPS (*Global Positioning System*) capaci di effettuare la localizzazione geografica dei dipendenti e comunicare al sistema WFM (*Work Force Management*) la propria posizione con una periodicità temporale prestabilita pari a 15 minuti. Il dato relativo alla geolocalizzazione così raccolto non viene acquisito in modo permanente dal sistema, ma viene automaticamente cancellato in modo tale da rendere disponibile solo l'ultimo dato di localizzazione pervenuto (tant'è che la nuova posizione rilevata annulla e sostituisce la precedente). Di fatto, tramite l'attivazione di tale funzionalità non si ha a disposizione l'intero tracciamento del percorso del dipendente e il sistema mantiene solo i dati *master* (ad esempio siti, attrezzature, ecc.), mentre i dati transazionali (ad esempio il dettaglio dei WO) vengono eliminati dal sistema dopo 16 giorni dalla chiusura. I dati personali complessivamente trattati dal sistema sono solo cognome, nome, *Service Area*, *Skill* tecnico (es. *radio*, *transmission*, *power*, ecc.), *Home Base* (ovvero il luogo dove il tecnico prende servizio), attività svolta, dato dell'ultima localizzazione rilevato tramite funzionalità GPS dell'applicazione;
- nel secondo caso (provvedimento del 9 ottobre 2014), la localizzazione avviene attraverso un sistema di *Work Force Management* (WFM) già esistente ed è attivata attraverso l'installazione di *ClickSoftware*. I dati in trattati dalla società attraverso tale sistema sono l'ID del dispositivo aziendale affidato al tecnico, il numero di telefono aziendale, le coordinate GPS del tecnico durante lo svolgimento dell'attività operativa, le coordinate GPS della *Home Base* del tecnico per la determinazione dell'area di competenza.

Pertanto, facendo un riepilogo dei principali spunti che emergono da tali provvedimenti, in termini di condizioni di liceità del trattamento e rispetto dei principi *privacy* (che, si ritiene, possano essere sussumibili anche in altri casi diversi da quelli esaminati dall'Autorità Garante), possiamo affermare che detti trattamenti possono avvenire solo alle seguenti condizioni e nel rispetto delle sotto indicate finalità:

- ottimizzare la gestione e il coordinamento degli interventi effettuati dai dipendenti sul campo, incrementandone la tempestività a fronte delle richieste dei clienti, soprattutto in caso di

emergenze e/o calamità naturali;
- rafforzare le condizioni di sicurezza del lavoro, permettendo l'invio mirato di eventuali soccorsi - soprattutto in aree remote o non facilmente raggiungibili - e comunque supportare più rapidamente i lavoratori in caso di difficoltà;
- soddisfare, in generale, esigenze organizzative e produttive o di sicurezza del lavoro;
- rispettare la disciplina vigente in materia di controlli a distanza dei dipendenti e, quindi, adottare le garanzie previste dall'art. 4, comma 2, della L. 300/1970 (che, si ricorda, prevedono o il raggiungimento di un accordo con le rappresentanze sindacali aziendali o l'ottenimento di un'autorizzazione della DTL del luogo in cui ha sede la società titolare); in questi casi, andando un po' in controtendenza rispetto alle indicazioni generali in tema di geolocalizzazione fornite dai Garanti europei, il relativo trattamento può avvenire - in base alle pronunce in esame fornite dall'Autorità Garante in seguito alle verifiche preliminari presentate - anche senza il consenso degli interessati (in applicazione del principio del bilanciamento di interessi ai sensi dell'art. 24, comma 1, lett. g) del *Codice Privacy*), perché finalizzato al perseguimento di un legittimo interesse volto a soddisfare esigenze organizzative, produttive e legate alla sicurezza del lavoro;
- rispettare il principio di pertinenza e non eccedenza, evitando di effettuare la rilevazione continuativa di dati relativi alla localizzazione geografica dei tecnici e memorizzando solo l'ultima informazione relativa alla localizzazione del dispositivo al termine di una determinata sessione di lavoro (con cancellazione automatica della rilevazione precedente)[(1)];
- limitare le informazioni visibili o utilizzabili dalla *APP* solo a quelle di geolocalizzazione e impedire l'accesso ad altri dati (ad esempio: sms, posta elettronica, traffico telefonico) ultronei rispetto alla finalità perseguita.

Sullo schermo dello *smartphone*, inoltre, deve comparire in maniera sempre ben visibile una specifica icona che indichi ai dipendenti se la funzione di localizzazione è attiva oppure no.

Molto importante, infine, è il richiamo al rispetto di specifici e ulteriori obblighi da parte del datore di lavoro, consistenti nel rispetto di adempimenti che fanno parte dell'impianto normativo classico dell'attuale legge italiana in materia di corretto trattamento dei dati personali:
- **Adempimenti generali**: tali trattamenti possono avvenire da parte del datore di lavoro solo se preceduti da una idonea informativa comprensiva di tutti gli elementi di cui all'art. 13 del *Codice Privacy*, in modo tale che l'utilizzatore interessato sia messo a conoscenza delle specifiche finalità e modalità del trattamento - anche in riferimento all'esercizio dei diritti ex art. 7 e ss. del Codice - relativamente ai loro dati personali rilevati dal dispositivo utilizzato[(2)].
- **Adempimenti speciali**: notificazione all'Autorità Garante ai sensi dell'art. 37 comma 1, lett. a) del *Codice Privacy* (tale obbligo, si ricorda, è pesantemente sanzionato dall'art. 168 del Codice);
- **Adempimenti necessari**: rispetto delle prescrizioni e raccomandazioni contenute nel provvedimento del Garante per la protezione dei dati personali n. 13 del 1° marzo 2007 "*Linee guida per posta elettronica e internet*" (si tratta, come è noto, di una misura di sicurezza c.d. "necessaria")[(3)];
- **Adempimenti organizzativi**: rispetto delle misure di sicurezza di cui agli artt. 31 e ss. del Codice ovvero delle misure di sicurezza minime e idonee al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati.

Nel complesso, pertanto, l'Autorità Garante ha ritenuto i sistemi posti alla sua attenzione conformi al principio di liceità, perché consentono di ottimizzare la gestione degli interventi tecnici, incrementando la velocità di risposta alle richieste dei clienti - soprattutto in caso di emergenze o calamità naturali - e poiché la localizzazione geografica rafforza le condizioni di sicurezza dei dipendenti permettendo l'invio mirato di soccorsi in caso di difficoltà. Il sistema risulta, poi, conforme anche ai principi di necessità, pertinenza e non eccedenza, perché la rilevazione dei dati di geolocalizzazione non è continuativa e l'ultima rilevazione cancella quella precedente.

Ad avviso di chi scrive e alla luce del richiamo al rispetto delle "*Linee guida per posta elettronica e internet*", sarà necessario soffermare l'attenzione anche sulla corretta regolamentazione interna di tali strumenti e aggiornare/adottare un Regolamento interno (o *privacy policy* interna), redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente ai dipendenti e da sottoporre ad aggiornamento periodico, che contenga anche le specifiche indicazioni circa l'utilizzo che può essere fatto di tali strumenti da parte del datore di lavoro e degli stessi dipendenti.
Tali provvedimenti, infine, si ritiene che debbano essere letti in coordinamento anche con l'attività portata avanti dalle Autorità Garanti europee per la protezione dei dati personali relativamente alle problematiche *privacy* derivanti dall'utilizzo delle *APP* da parte degli utenti della rete che usano *smartphone* e *tablet*[(4)]. ©

NOTE

1. È stata altresì prescritta una ulteriore misura di sicurezza a tutela degli interessati nei casi in cui il sistema consenta, agli utenti autorizzati all'accesso, la visualizzazione in tempo reale dei dati di localizzazione: tale eventuale trattamento di dati in tempo reale, infatti, deve avvenire solo in presenza di specifiche esigenze, ad esempio legate al verificarsi di situazioni di emergenza e/o di pericolo per il dipendente, e individuate all'interno di appositi protocolli che identifichino anche i soggetti legittimati ad accedere con tale modalità al sistema.
2. In un caso è stato anche affermato che il datore di lavoro deve informare i propri dipendenti sui casi nei quali è consentita la disattivazione della funzione di localizzazione nel corso dell'orario di lavoro, nonché circa le eventuali conseguenze nel caso in cui la disattivazione avvenga con modalità non consentite.
3. Si tratta di un provvedimento (*docweb* n. 1387522) che rappresenta un esemplare contemperamento degli interessi alla cui tutela il *Codice Privacy*, da un lato, e lo Statuto dei Lavoratori, dall'altro, sono preposti: da un lato la tutela della riservatezza e della dignità del lavoratore, dall'altro le esigenze del datore di lavoro relative all'organizzazione, alla produzione e alla sicurezza. Ciò consente al datore di lavoro di sottoporre il dipendente solo a controlli indiretti, attraverso l'uso di tecnologie informatiche, ma sempre nei limiti tracciati dal Garante e purché si tratti di "controlli difensivi", quelli cioè che si rendono necessari, e pertanto giustificati e legittimi, per garantire la tutela del patrimonio aziendale.
4. I Garanti europei, riuniti nel gruppo di lavoro "*Article 29 Data ProtectionWorking Party*", hanno emanato il parere n. 2 del 2013, che prende in esame i rischi fondamentali per la protezione dei dati derivanti dalle applicazioni per terminali mobili e il rapporto esistente tra le numerose applicazioni mobile presenti sul mercato e la tutela della privacy degli utenti coinvolti. ◊