GARANTE PROTEZIONE DATI PERSONALI - PROVVEDIMENTO 18 Aprile 2018 N. 232

Verifica preliminare. Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali

(1) Pubblicato nel sito internet del Garante per la protezione dei dati personali.

(2)

(2) Emanato dal Garante per la protezione dei dati personali.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

ESAMINATA la richiesta di verifica preliminare presentata da Sicuritalia S.p.A. ai sensi dell'articolo 17 del Codice;

VISTI gli atti d'ufficio;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la prof.ssa Licia Califano;

PREMESSO

1. Trattamento di dati personali di dipendenti effettuato attraverso la localizzazione di dispositivi smartphone o tablet.

1.1. Sicuritalia S.p.A. (di seguito, la società) ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, in relazione al trattamento dei dati personali connesso alla prospettata installazione dell'applicazione NavNet, completa di funzionalità di localizzazione geografica, sui dispositivi smartphone o tablet consegnati alle guardie particolari giurate incaricate di effettuare i servizi di vigilanza forniti dalla società.

Secondo quanto rappresentato dalla società l'applicazione "verrà attivata dalla guardia mediante l'inserimento del proprio codice identificativo nonché di una password fornita dalla centrale operativa in relazione allo specifico servizio assegnato [...], immediatamente prima l'inizio del turno" (cfr. istanza 6 giugno 2017, punto 5). Le finalità del sistema consisterebbero nella necessità di assicurare: "la sicurezza della pattuglia [...]"; la "razionale assegnazione e distribuzione degli interventi alle pattuglie di zona [...]"; il "corretto svolgimento dell'ordinaria attività di vigilanza/ispezione" (cfr. istanza cit., punto 6). I dati raccolti saranno conservati "per un periodo non superiore alle ore 24, fatte salve speciali esigenze di ulteriore conservazione" (cfr. istanza cit., punto 10).

Considerato che i dispositivi sono presi in consegna dai dipendenti all'inizio del turno e riconsegnati a fine servizio, il trattamento di dati opera esclusivamente nel corso dello svolgimento dell'attività lavorativa.

1.2. In particolare, quanto alle specifiche caratteristiche del sistema che si intende utilizzare, la società ha dichiarato che:

a. a tutela della sicurezza della pattuglia l'applicazione prevede un "comando di invio «aggressione - panico»"; decorsi 30 secondi dall'attivazione del comando è possibile inviare un allarme immediato oppure "impostare un allarme ritardato e annullabile, allo scadere del quale viene inviata una segnalazione in Centrale" (cfr. istanza cit., punto 7);

b. al fine di soddisfare esigenze organizzative il sistema "consente alla Centrale Operativa di assegnare un allarme proveniente dal sito di un cliente alla pattuglia [...] svolgente servizio in prossimità dello stesso"; in questo caso, qualora la guardia giurata accetti l'incarico e raggiunga la destinazione, "può trasmettere in [centrale operativa] la dichiarazione «arrivato sul posto» e al termine dell'ispezione inviare delle dichiarazioni predefinite o digitare manualmente un testo riportando l'esito dell'attività [...]. Tale funzione risulta attivabile per mezzo del sistema di geolocalizzazione [...] e/o per il tramite di una pronta interrogazione manuale" (cfr. istanza cit., punto 8);

c. "la posizione della pattuglia [è rilevata] ogni 120 secondi" ed è prevista la visualizzazione in tempo reale "al fine di garantire il più possibile la sicurezza personale" degli addetti in servizio (cfr. istanza cit., punto 10);

d. ciascun dipendente può visualizzare "successivamente all'inserimento dei dati utenza [...] tutte le attività di ispezione ordinaria [...] da effettuare in [...] giornata nonché le peculiarità di ogni singolo servizio" (cfr. istanza cit., punto 9);

e. i dati raccolti dal sistema ("coordinate del dispositivo e velocità del veicolo") possono essere consultati dagli "addetti alla centrale operativa ed alla direzione IT di Sicuritalia, che verranno debitamente nominati incaricati del trattamento e che saranno muniti ciascuno di apposite credenziali di autenticazione e profili autorizzativi per l'accesso ai dati, in modo particolare con riferimento alla funzionalità di estrazione" (cfr. istanza cit., punto 10);

f. ai dipendenti sarà fornita un'informativa ai sensi dell'articolo 13 del Codice nell'ambito delle attività di formazione circa il funzionamento del sistema (cfr. istanza cit., punto 11);

g. considerato, infine, che il sistema è preordinato a soddisfare "esigenze organizzative e produttive ed in primis a garantire la sicurezza delle [guardie giurate] sempre più esposte ai rischi di aggressione [...]

ne consegue che è escluso l'utilizzo di tali dati da parte della società istante per finalità di controllo dei dipendenti ovvero per scopi disciplinari" (cfr. istanza cit., punto 12).

1.3. A seguito di una richiesta di integrazioni e chiarimenti la società ha rappresentato che:

a. allo stato è già utilizzato un sistema di localizzazione dei "furgoni blindati adibiti a trasporto valori, nonché sulle autovetture adibite a trasporto valori c.d. leggero ([in relazione a] somme fino a Euro 100.000,00 effettuato da una guardia giurata armata e munita del giubbotto antiproiettile a bordo di veicolo leggero radiocollegato con la centrale operativa), in ottemperanza con quanto previsto dall'Allegato D) del Decreto del Ministero dell'Interno n. 269/2010. Il sistema [...] permette la geolocalizzazione del veicolo ogni 500 metri ovvero ogni 120 secondi" (cfr. nota pervenuta l'8.11.2017, punto a);

b. il sistema consente alla guardia giurata di visualizzare sul dispositivo il tipo di intervento da svolgere presso un determinato sito (ad es. se sul perimetro esterno o se anche all'interno); inoltre è possibile "annotare in tempo reale anomalie rilevate presso il sito [...]. Trattasi di circostanze che, se comunicate al cliente tempestivamente, permettono a quest'ultimo di porre rimedio ad eventuali gap nelle procedure di sicurezza e/o porre in essere prontamente gli interventi [...] necessari" (cfr. nota cit., punto b);

c. i dispositivi aziendali non sono assegnati sempre al medesimo dipendente, bensì ritirati ad inizio turno tra quelli disponibili, "spetterà, poi, al capo zona (diretto superiore delle guardie giurate addette ad un corpo di guardia) registrare su un apposito file per ciascun turno a quale guardia ciascun dispositivo è stato assegnato" (cfr. nota cit., punto c);

d. non è prevista l'attivazione della funzionalità "controllo orario sull'entrata in servizio" (cfr. nota cit., punto d);

e. quanto alla periodizzazione temporale della rilevazione della posizione geografica, fissata in due minuti, "il lasso temporale [...] è sembrato un tempo congruo a garantire un efficace intervento [...] nel caso in cui la pattuglia si trovi in una situazione di emergenza" (cfr. nota cit., punto e);

f. in relazione ai soggetti autorizzati ad accedere al sistema in forza presso la direzione IT della società, si è chiarito che, da un lato, questi "(in numero limitato) avranno accesso al sistema con il profilo e le autorizzazioni tipiche dell'amministratore di sistema" per lo svolgimento delle attività legate "alla gestione delle licenze, all'installazione del sistema sui dispositivi periferici, alle verifiche tecniche di funzionamento del sistema, alla verifica di eventuali anomalie, all'implementazione degli aggiornamenti del sistema"; inoltre all'interno della direzione IT "vi saranno altri incaricati (anche questi in numero limitato) cui sarà consentito accedere al sistema al solo fine di redigere la reportistica che contrattualmente il committente chiede di fornire all'esito di ogni intervento [...]. Nel report non sono riportati i dati di geolocalizzazione, ma solo [...] l'orario di esecuzione dell'intervento e la tipologia dello stesso" (cfr. nota cit., punto f);

g. l'accesso in tempo reale ai dati relativi alla localizzazione, da parte dei soggetti autorizzati presenti nella centrale operativa, è previsto in caso di attivazione della procedura di emergenza da parte della guardia giurata, nonché negli altri casi di "interventi di allarme e/o ispettivi" (cfr. nota cit., punto g);

h. nell'ambito del sistema sarà altresì attivata la funzione "eccesso sosta" che prevede l'invio di un allarme alla centrale operativa in caso di "assenza di movimento da parte della guardia per un tempo preimpostato", al fine di poter predisporre un rapido intervento in caso di aggressione o malore (cfr. nota cit., punto h);

i. il "rapportino elettronico" predisposto dai dipendenti è "reso disponibile ai soggetti autorizzati nel momento stesso in cui la guardia giurata lo inserisce nel dispositivo periferico" (cfr. nota cit., punto i);

j. attraverso la funzionalità di interrogazione manuale l'operatore della centrale operativa può solo visualizzare la posizione del dispositivo (cfr. nota cit., punto i);

k. il fornitore del software non ha accesso ai dati relativi alla localizzazione, "solo in via residuale e su richiesta della Direzione IT di Sicuritalia, previa autorizzazione data da quest'ultima, potrà procedere ad interventi di manutenzione straordinaria" (cfr. nota cit., punto j);

l. l'individuazione del termine di conservazione dei dati di localizzazione fissato in 24 ore è stato individuato, in applicazione dei principi di necessità e proporzionalità, analogamente a quanto previsto dal Garante in materia di videosorveglianza; tuttavia "i tempi di conservazione potranno essere allungati in caso di specifiche richieste dell'autorità giudiziaria a fronte dell'avvenuta commissione di illeciti e/o della necessità di svolgere attività investigativa, nonché specifiche esigenze evidenziate in sede contrattuale da committenti titolari di siti soggetti ad elevati rischi di intrusioni/infrazioni" (cfr. nota cit., punto k);

m. a parte i dati di localizzazione, le altre informazioni trattate dal sistema "ed in modo particolare i cosiddetti «rapportini elettronici» saranno conservati per tempi ben più lunghi poiché costituiscono prova dell'adempimento delle prestazioni contrattuali cui la società è tenuta nei confronti dei propri clienti ed il loro scopo [...] è quello di essere utilizzati quale elemento di prova in caso di controversie giudiziali" (cfr. nota cit., punto k);

n. "la società si impegna a procedere alla convocazione delle rappresentanze sindacali dei lavoratori ai fini della sottoscrizione di un accordo sindacale ovvero, in difetto, ad acquisire l'autorizzazione del competente organo del Ministero del Lavoro" (cfr. nota cit., punto l).

2. Liceità del trattamento dei dati di localizzazione nei servizi di vigilanza privata. Bilanciamento di interessi.

2.1. La società che ha presentato istanza al Garante fornisce servizi di vigilanza privata preordinati alla tutela di persone e beni nonché al trasporto e alla custodia di valori, avvalendosi di guardie particolari giurate. Tale attività è regolamentata dall'ordinamento, che stabilisce le caratteristiche necessarie e i requisiti organizzativi e professionali degli istituti di vigilanza privata nonché i requisiti minimi di qualità dei

servizi resi (v. Decreto Ministero dell'Interno, 1° dicembre 2010, n. 269, “Regolamento recante disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualità degli istituti e dei servizi di cui agli articoli 256-bis e 257-bis del Regolamento di esecuzione del Testo unico delle leggi di pubblica sicurezza, nonché' dei requisiti professionali e di capacità tecnica richiesti per la direzione dei medesimi istituti e per lo svolgimento di incarichi organizzativi nell'ambito degli stessi istituti” e spec. All. D“Requisiti operativi minimi degli istituti di vigilanza e regole tecniche dei servizi”).

Tale specifica disciplina, considerata la particolarità dell'attività svolta (avente ad oggetto i c.d. servizi di sicurezza complementare e condizionata al rilascio della licenza prefettizia ai sensi dell'art. 134 del Testo unico delle leggi di pubblica sicurezza - TULPS), prevede - tra l'altro - l'adozione di specifiche misure tecniche in caso di svolgimento di servizi che presentano rischi particolari (con riferimento al trasporto di contante è stabilito che “la centrale operativa [...] monitora la posizione dei mezzi adibiti al servizio [...] mediante il sistema di localizzazione satellitare di cui gli stessi sono, obbligatoriamente, muniti”; con riferimento, invece, al servizio di vigilanza saltuaria è previsto che le guardie giurate sono tenute a comunicare alla centrale operativa “con frequenza prestabilita, la loro posizione, le eventuali novità ed ogni situazione anomala riscontrata”: v. D.M. n. 269/2010 cit., All. D, Sez. III, 3.c e 3.I.2). Il legislatore ha inoltre individuato specifiche caratteristiche dell'attività prestata, distintamente per ciascuna tipologia di servizio (obblighi di collegamento via radio con la centrale operativa, obblighi di documentare l'attività svolta e conservarla a disposizione dell'autorità di pubblica sicurezza per un termine prestabilito, obbligo per la guardia giurata di comunicare novità, fatti o situazioni degni di rilievo, sui quali vedi più avanti punto 3).

Alla luce del richiamato quadro normativo l'adozione di un sistema completo di funzionalità di localizzazione da installare su dispositivi forniti ai dipendenti, al fine di rafforzare la sicurezza di persone e beni, nonché per realizzare miglioramenti nell'efficienza dei servizi, risulta in termini generali lecito. Inoltre, sotto tale profilo, è conforme a quanto stabilito dall'articolo 4, comma 1, della legge 20 maggio 1970, n. 300 (richiamato dall'art. 114 del Codice, la cui osservanza costituisce pertanto condizione di liceità del trattamento) la prospettata attivazione della procedura di garanzia prevista dalla richiamata disciplina in materia di controlli a distanza (v. precedente punto 1.3., lett. n).

Nel caso di specie, infatti, la società svolge attività ulteriori rispetto a quella di trasporto valori (per la quale il citato regolamento ha reso obbligatoria la localizzazione geografica dei mezzi; v. D.M. n. 269/2010 cit., All. D, Sez. III, 3.I.2), in particolare prestando attività di vigilanza, anche con collegamento a sistemi di allarme, in relazione alle quali il sistema di localizzazione dei dispositivi non è direttamente preordinato all'esecuzione della prestazione lavorativa né è previsto espressamente da una norma, con conseguente applicazione del menzionato articolo 4, comma 1 (si veda sul punto, in senso conforme, la circolare n. 2 del 7 novembre 2016 dell'Ispettorato nazionale del lavoro: “in linea di massima e in termini generali [...] i sistemi di geolocalizzazione rappresentano un elemento «aggiunto» agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa”; mentre “solo in casi del tutto particolari - qualora [...] l'installazione sia richiesta da specifiche normative [...] - si può ritenere che [...] finiscano per «trasformarsi» in veri e propri strumenti di lavoro”).

2.2. Ciò considerato, anche alla luce delle successive valutazioni relative alla necessità e proporzionalità dei trattamenti che si intendono effettuare nonché delle misure impartite a tutela degli interessati, si ritiene che i descritti trattamenti possano essere effettuati, nei confronti dei dipendenti, per effetto del presente provvedimento che, in applicazione della disciplina sul c.d. “bilanciamento di interessi” (ai sensi dell'articolo 24, comma 1, lett. g) del Codice), individua un legittimo interesse al trattamento di tale tipologia di dati (che non rientra nel novero dei dati sensibili) in relazione alle finalità rappresentate.

3. Principi di necessità e proporzionalità dei trattamenti. Tempi di conservazione.

3.1. Le modalità di trattamento dei dati personali da parte del sistema tecnologico prospettato prevedono, in particolare, la pseudonimizzazione dei dati delle guardie giurate, che risultano pertanto non già direttamente identificate dal sistema bensì indirettamente identificabili attraverso il raffronto con le credenziali di accesso all'applicazione (codice guardia) e con il file compilato dal capo zona ad inizio turno contenente l'associazione guardia giurata/dispositivo. Inoltre l'accesso in tempo reale ai dati di localizzazione effettuato dal personale autorizzato presente nella centrale operativa è previsto esclusivamente in caso di necessità ed emergenza, ossia in caso di allarme lanciato dalla medesima guardia giurata (v. precedente punto 1.2., lett. a) oppure in caso di avvenuta ricezione di segnalazione di allarme o in caso si rendese necessario procedere ad ispezioni in loco (v. precedente punto 1.3., lett. g), oppure in caso di attivazione della funzionalità “eccesso sosta”, ossia un meccanismo di allarme automatico che scatta in caso di assenza di movimento per un periodo di tempo predeterminato (ritenuto anomalo) (v. precedente punto 1.3., lett. h). Tali modalità risultano conformi ai principi di necessità, pertinenza e non eccedenza in relazione alle finalità perseguite dalla società (art. 11, comma 1, lett. d) del Codice; si veda in proposito quanto stabilito dall'Autorità nei precedenti provv.ti in materia: Provv. 30.11.2017, n. 505, doc. web n. 7522639; Provv. 24 maggio 2017, n. 247, doc. web n. 6495708; Provv. 16.3.2017, n. 138, doc. web n. 6275314; Provv. 11 settembre 2014, n. 401, doc. web n. 3474069 e Provv. 9 ottobre 2014, n. 448, doc. web n. 3505371).

Con riferimento ai rapporti predisposti per i clienti, si prende atto che tali documenti, opportunamente, non contengono i dati di localizzazione.

Alla luce della finalità dei report stessi, conformemente a quanto deciso in precedenti casi, si ritiene che questi non debbano altresì contenere informazioni relative alle singole guardie giurate (direttamente o indirettamente identificate) che hanno svolto l'attività di vigilanza (cfr. provv. 24.5.2017, n. 247, doc web n. 6495708, spec. punto 5.3.).

3.2. Il sistema è configurato in modo da consentire ai soggetti autorizzati la visualizzazione immediata del c.d. rapportino elettronico (v. precedente punto 1.3., lett. i). In proposito, considerato il contenuto di tale rapporto (dichiarazione di chiusura dell'incarico se del caso associato ad immagini raccolte sul posto, ad esclusione della "storia incarico": cfr. istanza cit., All. 5), si ritiene che la società debba individuare, effettuando una selezione in relazione alle funzioni svolte, i soggetti autorizzati all'accesso in tempo reale a tali rapporti, qualora sia necessario effettuare il coordinamento delle attività in corso e/o provvedere tempestivamente, se del caso, ad avvisare i clienti o le forze di polizia in caso di anomalie riscontrate nel corso dell'attività di vigilanza.

Quanto al contenuto delle informazioni relative agli interventi effettuati che devono essere rese immediatamente visibili sul sistema, si invita a tener conto che, in base alla richiamata disciplina di settore, le guardie giurate sono tenute a dare "immediata notizia all'istituto mediante comunicazione alla centrale operativa [...] delle irregolarità riscontrate nel corso del servizio"; inoltre, in termini generali, le guardie giurate devono "compilare, al termine di ogni turno di servizio, un dettagliato rapporto sull'attività svolta solo se vi siano novità, fatti o situazioni degne di rilievo" (D.M. n. 269/2010 cit., All. D, Sez. I, 1b, lett. b) e Sez. III, 3.a).

3.3. Per quanto riguarda la periodizzazione temporale della rilevazione della posizione geografica dei dispositivi si osserva quanto segue.

L'Autorità ha costantemente affermato che, nel rispetto del principio di necessità (art. 3 del Codice), "la posizione del veicolo [sottoposto a localizzazione] non dovrebbe di regola essere monitorata continuativamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il perseguimento delle finalità legittimamente perseguite" (cfr. Provv.to di carattere generale in materia di localizzazione dei veicoli nell'ambito del rapporto di lavoro, 4 ottobre 2011, n. 370, doc. web n. 1850581). Medesimo principio si applica alla localizzazione dei dispositivi mobili, considerato anche che "lo smartphone è, per le proprie caratteristiche, destinato inevitabilmente a "seguire" la persona che lo possiede, indipendentemente dalla distinzione tra tempo di lavoro e tempo di non lavoro" (cfr. provv.to 11.9.2014, n. 401 cit., punto 2).

Nel caso specifico il titolare del trattamento ha fissato la periodizzazione temporale della rilevazione effettuata dal sistema in due minuti, tempo ritenuto congruo rispetto alla rappresentata necessità di predisporre con urgenza interventi a tutela della pattuglia in caso di aggressione oppure a tutela di persone e beni in caso di segnalazione di illeciti in corso. Alla luce della peculiarità dell'attività svolta nell'ambito dei servizi di c.d. sicurezza complementare, nonché tenuto conto della disciplina specifica che regolamenta la materia, tale periodizzazione temporale (in sé estremamente ravvicinata) non contrasta con i principi di necessità, pertinenza e non eccedenza rispetto alle finalità perseguite (artt. 3 e 11, comma 1, lett. d) del Codice; v. provv.to 19.10.2017, n. 432, doc. web n. 7321142, relativo alla localizzazione di veicoli e di dispositivi radio ricetrasmittenti in dotazione alla polizia locale). Tale valutazione è effettuata anche alla luce delle complessive caratteristiche del sistema, e in particolare alla individuazione di un breve termine di conservazione dei dati di localizzazione raccolti (24 ore, salvo eccezioni sulle quali si veda punto 3.4.) nonché della prevista visualizzazione sui monitor della centrale operativa della posizione dei dispositivi, da parte dei soggetti autorizzati, solo in caso di necessità (eventi predeterminati).

Si ritiene tuttavia necessario, a tutela degli interessati, prescrivere alla società di configurare il sistema in modo da oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore sul monitor. Tale misura è finalizzata a minimizzare il rischio di accesso ai dati non necessario e/o non pertinente.

3.4. Quanto ai tempi di conservazione dei dati riferiti alla localizzazione geografica si ritiene che la tempistica individuata (24 ore), sia conforme ai menzionati principi di necessità e proporzionalità. In relazione alle ipotesi di ulteriore conservazione prospettate dalla società (v. precedente punto 1.3., lett. l), fatta salva l'ipotesi di richieste di accesso presentate dall'autorità giudiziaria, la società dovrà individuare in concreto termini più estesi di eventuale conservazione tenendo conto dei parametri indicati (sia temporali che relativi alle finalità della conservazione) dal richiamato D.M. n. 269/2010. Tale disposizione prevede, in particolare, l'obbligo di conservare per due anni a disposizione dell'autorità di pubblica sicurezza i turni di servizio delle guardie giurate nonché "tutta la documentazione relativa all'attività svolta, nonché quella relativa alle guardie giurate" (v. All. D, Sez. I, 1a, lett. a) e n). Inoltre prevede che l'ordine di servizio giornaliero debba essere custodito "per almeno due anni" al fine di poter essere esibito a richiesta di "ufficiali ed agenti di pubblica sicurezza, nell'ambito dell'ordinaria attività di controllo" (v. All. D, Sez. II, 2.a).

L'individuazione di termini di conservazione proporzionati rispetto alla finalità perseguite deve riguardare anche i c.d. rapportini elettronici.

4. Misure ed accorgimenti posti a tutela dei diritti degli interessati.

Considerata la delicatezza dei dati relativi alla localizzazione geografica, seppur in un contesto del tutto peculiare di trattamento quale quello oggetto dell'istanza, è necessario prescrivere alcune misure ed accorgimenti a tutela dei diritti e delle libertà degli interessati.

Considerata la particolarità dei dati trattati, il sistema dovrà essere configurato in modo tale che sul dispositivo aziendale sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva.

Deve inoltre essere prevista la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa, informando correttamente i dipendenti sui casi in cui è consentito disattivare la localizzazione nonché sulle conseguenze degli eventuali abusi.

Come già osservato in precedenza, al fine di minimizzare il rischio di accesso ai dati non necessario e/o non pertinente (a fronte di una periodizzazione assai ravvicinata della rilevazione geografica dei

dispositivi), si prescrive alla società di configurare il sistema in modo da oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore sul monitor presente nella centrale operativa (relativamente a tale funzionalità).

Considerato inoltre che alla centrale operativa hanno accesso soggetti che operano a diverso titolo (v. precedenti punti 1.2., lett. e. e 1.3., lett. f. e g.), la società dovrà individuare profili differenziati di autorizzazione relativi alle diverse tipologie di dati e di operazioni eseguibili.

In applicazione dei principi di necessità e proporzionalità la società dovrà individuare tempi di conservazione dei dati in concreto trattati tenendo conto delle finalità perseguite (v. precedente punto 3.4.). In applicazione dei medesimi principi, inoltre, la società dovrà depurare i rapporti consegnati ai clienti di qualunque riferimento che consenta l'identificazione di dipendenti.

Considerate le operazioni di trattamento che il fornitore del sistema prescelto può effettuare in base alle indicazioni fornite dalla società (v. precedente punto 1.3., lett. k), questa procederà a designare quale responsabile esterno del trattamento il predetto fornitore, fino al 25 maggio 2018 ai sensi e per gli effetti previsti dall'articolo 29 del Codice. Il ruolo del fornitore continuerà a configurarsi come responsabile esterno purché sia strutturato in conformità all'articolo 28 del Regolamento generale sulla protezione dei dati (UE) 2016/679.

Per ciò che riguarda, infine, la funzionalità “eccesso sosta” si prescrive alla società, a tutela della qualità dei dati trattati, di predisporre periodiche verifiche di test sul funzionamento del sistema e l'affidabilità dei parametri adottati (es. il tempo predeterminato di assenza di movimento), in vista della valutazione di eventuali falsi positivi o negativi effettuati dal sistema e la conseguente predisposizione di correttivi.

5. Adempimenti previsti dalla legge.

Resta fermo che la società, prima dell'inizio dei descritti trattamenti, è tenuta in base alla normativa vigente a:

a. fornire ai dipendenti della società coinvolti dai descritti trattamenti un'informativa comprensiva di tutti gli elementi contenuti nell'articolo 13 del Codice (tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione), anche in conformità al principio di correttezza in base al quale il titolare è tenuto a rendere chiaramente riconoscibili agli interessati i trattamenti che intende effettuare (art. 11, comma 1, lett. a), del Codice); in particolare la società è tenuta ad informare circa le consentite condizioni d'uso dei dispositivi smartphone/tablet forniti in dotazione, specificando anche se e a quali condizioni sia consentito l'uso a fini personali, e le conseguenze di eventuali abusi;

b. adottare le misure di sicurezza idonee a preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati;

c. predisporre misure al fine di garantire agli interessati l'esercizio dei diritti previsti dagli articoli 7 e seguenti del Codice. A far data dal 25 maggio 2018 i diritti degli interessati sono disciplinati dagli artt. 15 e seguenti del Regolamento generale sulla protezione dei dati (UE) 2016/679;

d. effettuare la notificazione al Garante ai sensi degli articoli 37 e ss., qualora il trattamento abbia effettivamente inizio prima del 25 maggio 2018 (tenendo conto che tale adempimento non sarà più dovuto in data successiva al 25 maggio p.v.)

Si tenga comunque presente che, a decorrere dal 25 maggio 2018, data di applicazione del citato Regolamento (UE) 2016/679, il titolare del trattamento in ossequio al principio di responsabilizzazione di cui all'art. 24 dovrà valutare autonomamente la conformità del trattamento che intende effettuare alla disciplina vigente, verificando il rispetto di tutti i principi in materia nonché la necessità di effettuare, in particolare, una valutazione di impatto ex art. 35 del citato Regolamento ovvero attivare la consultazione preventiva ai sensi dell'art. 36 del Regolamento medesimo.

TUTTO CIO' PREMESSO IL GARANTE

[Testo del provvedimento]

ai sensi dell'articolo 17 del Codice, a conclusione della verifica preliminare:

1. ammette il trattamento di dati personali da parte di Sicuritalia S.p.A. mediante il sistema di localizzazione geografica dei dispositivi aziendali, illustrato nei termini di cui in motivazione, e prescrive che la società, quali misure necessarie, debba:

a. configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva;

b. configurare il sistema in modo da consentire la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa;

c. configurare il sistema in modo da oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore sul monitor presente nella centrale operativa relativamente a tale funzionalità;

d. individuare profili differenziati di autorizzazione relativi alle diverse tipologie di dati e di operazioni eseguibili;

e. individuare i tempi di conservazione dei dati in concreto trattati tenendo conto delle finalità perseguite;

f. predisporre i rapporti per i clienti privi di qualunque riferimento che consenta l'identificazione di dipendenti;

g. procedere alla designazione quale responsabile esterno del trattamento il fornitore del software NavNet;

h. predisporre periodiche verifiche di test sulla funzionalità "eccesso sosta" e l'affidabilità dei parametri adottati, in vista della valutazione di eventuali falsi positivi o negativi effettuati dal sistema e la conseguente predisposizione di correttivi a tutela della qualità dei dati trattati.

Ai sensi degli articoli 152 del Codice e 10 del decreto legislativo n. 150 del 2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.