GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 2471134]

**Trattamento di dati personali raccolti tramite telecamere e sistema di geolocalizzazione installati su veicoli aziendali - 7 marzo 2013**

Registro dei provvedimenti
n. 103 del 7 marzo 2013

**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;

VISTA la segnalazione pervenuta il 5 marzo 2012;

VISTO il Codice in materia di protezione dei dati personali;

VISTI i provvedimenti generali del 4 ottobre 2011, n. 370, concernente i sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro nonché del 27 novembre 2008, concernente i titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema;

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 dott.ssa Augusta Iannini;

**PREMESSO**

Accertamenti presso Anas s.p.a. concernenti i trattamenti di dati personali relativi ai lavoratori effettuati mediante il sistema Road management tool (Rmt)

1.1. Con una segnalazione anonima pervenuta il 5 marzo 2012 venivano lamentati, presso il Compartimento per l'Emilia Romagna di Anas s.p.a., controlli a distanza sui lavoratori posti in essere mediante sistemi di geolocalizzazione e di ripresa delle immagini installati su veicoli aziendali. In particolare, nella segnalazione si rappresentava che la menzionata strumentazione – che va a comporre parte del complessivo sistema informativo denominato Road management tool (Rmt), di seguito meglio descritto – verrebbe utilizzata, ad insaputa degli interessati, "per controllarci in ogni momento perché ci chiamano al telefonino per dirci cosa facciamo in quel dato posto e dalla sede guardano e registrano dove esattamente siamo, con chi parliamo e cosa facciamo" e "registrano anche le conversazioni all'interno dell'abitacolo", con la precisazione che "non vi è nessun accordo sindacale per l'uso di queste attrezzature e nemmeno [l'autorizzazione] della direzione provinciale del lavoro".

1.2. Al fine di verificare la fondatezza dei comportamenti ascritti alla società e la liceità dei trattamenti effettuati, il 28 marzo 2012 sono stati svolti accertamenti a Bologna, presso la sede compartimentale Anas oggetto della segnalazione; quindi, resesi necessarie ulteriori verifiche alla luce degli elementi raccolti e delle dichiarazioni ivi rese, altri accertamenti sono stati effettuati presso:

a. la sede legale della società in Roma (nei giorni del 17 maggio 2012 e, ancora, 21 giugno 2012);

b. Tecnositaf s.p.a., società che gestisce per conto di Anas il sistema informativo Rmt (nei giorni 30 e 31 maggio 2012).

1.3. Dagli accertamenti è emerso che Anas si è dotata del sistema Rmt, già funzionante, ancorché (asseritamente) in fase sperimentale, al fine di contribuire alla più efficiente gestione della rete stradale di propria competenza e monitorare in modo più efficace il traffico, specie al verificarsi di criticità (come, ad esempio, in caso di neve, frane o di altri eventi in grado di incidere sulla regolarità nella circolazione).

Componenti del sistema in esame – salvo quanto si dirà in merito alla sua complessiva gestione, in particolare da parte degli amministratori di sistema (cfr. infra parr. 8.1 ss.) – sono le strumentazioni installate a bordo dei veicoli aziendali in uso al personale di sorveglianza della rete stradale nonché ad altro personale tecnico impiegato nelle attività di verifica e manutenzione della sede stradale. Tali strumentazioni, con riguardo al parco veicoli, sono costituite, più precisamente, da:

a. una telecamera − attivabile dal conducente, previa autenticazione (immettendo le proprie credenziali nel dispositivo portatile installato a bordo), ovvero su iniziativa del personale autorizzato (che non immette credenziali) presente nella sala operativa del compartimento presso il quale opera il mezzo. In caso di attivazione della telecamera, che riprende frontalmente la sola sede stradale, le immagini raccolte vengono registrate su un dispositivo di bordo (la cui capacità di memoria è pari a 32 GB, equivalente a circa

sette giorni di riprese video continuative a bassa risoluzione: cfr. verbale 17 maggio 2012, p. 7) per essere successivamente "scaricate" nei server compartimentali, in occasione delle soste dei veicoli presso i centri di ricovero dislocati sul territorio, ovvero nei server della direzione centrale;

b. un ricevitore satellitare GPS, che si attiva e disattiva, rispettivamente, all'accensione e allo spegnimento del mezzo, localizzando su una mappa cartografica collocata presso le sale operative (compartimentali e, in caso di necessità, nazionale) la posizione di ciascun veicolo e l'orario della rilevazione; posizione "contrassegnata da una icona che può assumere i colori rosso, in caso di veicolo con il quadro-comandi spento ovvero fuori copertura GPS; verde, in caso di veicolo con il quadro acceso e connesso alla rete GPS; giallo, in caso di veicolo temporaneamente fuori dalla copertura GPS" (cfr. verbale 28 marzo 2012, p. 4).

Dalle dichiarazioni rese, è emerso che il sistema non dispone di un canale audio (cfr. verbali 28 marzo 2012, p. 5 e 17 maggio 2012, p. 4).

1.4. L'attivazione da remoto della telecamera – che oltre alla contestuale registrazione delle riprese sulla memoria di bordo, consente altresì la visualizzazione in diretta delle immagini presso le sale operative compartimentali (e, se necessario, nazionale) – è segnalata al conducente sul display del veicolo (cfr. verbale 17 maggio 2012, p. 4).

1.5. Anas ha dichiarato che la possibilità di attivare la telecamera da remoto e la registrazione continuativa dei dati di localizzazione dei veicoli sono funzionali allo svolgimento delle proprie attività istituzionali connesse alla sorveglianza e sicurezza stradale nonché ad assicurare la sicurezza dei lavoratori: in caso di necessità, ed in particolare in situazioni di emergenza, la conoscenza della posizione dei veicoli sul territorio consente infatti di coordinare ed ottimizzare gli interventi (cfr. verbale 17 maggio 2012, p. 6).

È stato altresì dichiarato che "al fine di documentare gli interventi dell'Anas in relazione a eventi critici, i file contenenti le immagini riprese dalle telecamere di bordo possono essere trasferiti dal personale della sala operativa compartimentale in una cartella nella quale è consentita la conservazione entro un tempo massimo attualmente stabilito in dieci anni e comunque modificabile in relazione a specifiche esigenze di difesa" (cfr. verbale 17 maggio 2012, p. 4).

Più precisa identificazione delle finalità perseguite mediante il sistema Rmt può rinversi nel "Regolamento per la disciplina della videosorveglianza stradale e della localizzazione satellitare veicolare", diramato dalla società con nota (protocollata) del 13 febbraio 2012.

2. La società, attraverso il sistema di cui si è dotata (ancorché in fase di asserita sperimentazione), tratta dati personali riferibili ai dipendenti essendo le informazioni acquisite, siano esse relative alla posizione del veicolo ovvero ricavate dalle immagini riprese dalla telecamera (nonché dai dati risultanti dal funzionamento coordinato dei dispositivi di rilevazione) "associabili" a ciascun conducente, alla cui identità la società può agevolmente risalire (art. 4, comma 1, lett. b), del Codice) (cfr. Articolo 29 Gruppo di lavoro per la protezione dei dati personali, WP 136, Parere 4/2007 sul concetto di dati personali, adottato il 20 giugno 2007). Ciò anche nel caso di specie, in cui le informazioni non sono immediatamente abbinate dal sistema al nominativo dell'interessato, essendone tuttavia possibile l'identificazione, anche a posteriori, per il tramite della loro combinazione con altri dati (cfr. al riguardo, Provv. 5 giugno 2008, doc. web n. 1531604; Provv. 18 febbraio 2010, doc. web n. 1703103; cfr. altresì, Parere n. 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto del Gruppo di lavoro ex art. 29, direttiva 95/46/Ce, WP115). La società risulta, infatti, in condizione di poter risalire in ogni momento all'utilizzatore del veicolo, sia in ragione dell'autenticazione del conducente mediante le credenziali individuali allo stesso assegnate in caso di attivazione della telecamera, sia attraverso opportune richieste da inoltrare alle competenti funzioni aziendali, posto che ciascun dipendente Anas addetto alla sorveglianza stradale è assegnatario di uno o più dei veicoli geolocalizzati (cfr. verbale 17 maggio 2012, p. 6). Possibilità sussistente anche per il restante personale (cui non è assegnato stabilmente alcun veicolo) che, in base a turni di servizio o su specifico incarico, risulta comunque alla guida del veicolo aziendale di volta in volta utilizzato (cfr. verbale 28 marzo 2012, p. 3).

Profili di illiceità dei trattamenti di dati personali effettuati con il sistema Rmt mediante i veicoli aziendali

3.1. Titolare dei trattamenti di dati personali connessi al complessivo funzionamento del sistema Rmt, ai sensi degli artt. 4, comma 1, lett. f) e 28 del Codice, è Anas. Dagli accertamenti effettuati è risultato che, in tale veste – e salvo quanto si dirà al successivo par. 7 rispetto a società cui sono state affidate in outsourcing talune funzioni concernenti la gestione del complessivo sistema Rmt –, la società ha provveduto a designare al proprio interno i capi dipartimento (e tra questi il capo-compartimento dell'Emilia-Romagna) quali responsabili dei trattamenti di dati personali effettuati a livello compartimentale. Con nota del 13 febbraio 2012, la società ha diramato il "Regolamento per la disciplina della videosorveglianza stradale e della localizzazione satellitare veicolare" e, con successiva nota del 7 marzo 2012, sono state altresì impartite istruzioni ai compartimenti in ordine ai principali adempimenti connessi alla disciplina di protezione dei dati personali da porre in essere per l'avvio della fase operativa del sistema Rmt.

Tuttavia, dalle verifiche effettuate presso il Compartimento per l'Emilia-Romagna, è emerso che i lavoratori complessivamente coinvolti nel funzionamento del sistema in esame non sono risultati designati quali incaricati del trattamento ai sensi dell'art. 30 del Codice (cfr. dichiarazioni rese nel verbale 28 marzo 2012, p. 2) – adempimento cui, come risulta dagli atti, si è provveduto successivamente (cfr. all. n. 1 alla nota integrativa dell'11 aprile 2012, in atti) –, né consta che agli stessi sono state impartite istruzioni in merito al corretto impiego del medesimo ancorché il menzionato Regolamento già contenga al riguardo prescrizioni dirette ai responsabili e agli incaricati del trattamento.

La Direzione centrale Anas ha effettuato presso i vari compartimenti corsi di formazione durante i quali sono state fornite istruzioni circa il funzionamento tecnico del sistema e consegnate le credenziali individuali di autenticazione (cfr. all. 3 verbale 17 maggio 2012).

3.2. Considerata la tardiva designazione presso il Compartimento per l'Emilia-Romagna degli incaricati del trattamento che, in ragione delle mansioni concretamente svolte, risultano legittimati ad avere accesso ai dati personali trattati per il tramite dei menzionati dispositivi di bordo ai sensi dell'art. 30 del Codice, resta impregiudicata ogni valutazione di questa Autorità in ordine alla sussistenza dei presupposti per la contestazione di eventuali violazioni.

4.1. Con riguardo ai trattamenti di dati personali effettuati mediante le menzionate apparecchiature sui veicoli aziendali, ritenuti dalla società rispondenti alle proprie esigenze organizzative e produttive, nonché di sicurezza sul lavoro, tenuto conto delle funzionalità connesse

all'impiego del sistema Rmt, merita evidenziare che entrambi gli strumenti in questione possono indubbiamente concorrere ad una più efficiente gestione del servizio reso dalla società, specie in casi di criticità sulla rete stradale (come rappresentato nel corso degli accertamenti), come pure incrementare la sicurezza per i lavoratori, in particolare ove siano chiamati ad operare in luoghi impervi o in presenza di condizioni ambientali avverse.

Nondimeno, l'impiego di tali strumenti deve comunque avvenire nel rispetto dei principi in materia di protezione dei dati personali e con modalità concretamente idonee a garantire, in particolare, l'osservanza dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (art. 2 del Codice).

4.2. Alla luce degli elementi complessivamente acquisiti agli atti, si ritiene che il trattamento di dati personali effettuato dalla società per il tramite dei menzionati dispositivi di localizzazione satellitare nonché per il tramite del sistema di ripresa delle immagini non sia stato conforme alla disciplina in materia di protezione dei dati personali (nonché alla disciplina di settore richiamata dall'art. 114 del Codice).

In merito occorre infatti preliminarmente rilevare che, a seguito delle verifiche effettuate, ha trovato conferma uno dei profili lamentati nella segnalazione, segnatamente quello relativo alla mancanza di un accordo con le rappresentanze sindacali o di una autorizzazione da parte dei competenti uffici del Ministero del lavoro con riguardo all'installazione e al successivo funzionamento del sistema Rmt. Invero, con nota successiva al primo accertamento ispettivo, la società ha trasmesso il testo di un accordo sindacale con le rappresentanze nazionali sottoscritto il 29 luglio 2011. Esso tuttavia riguarda l'avvio della preliminare fase di sperimentazione del sistema Rmt sulla "rete aziendale di competenza […] per l'autostrada SA-RC nonché del Compartimento per la viabilità per il Lazio (Grande raccordo anulare di Roma e autostrada Roma-Fiumicino)" (cfr. nota dell'11 aprile 2012, e all. 5); lo stesso non ha per oggetto, invece, l'impiego del sistema Rmt nel Compartimento per l'Emilia-Romagna.

Invero, solo in tempi successivi all'accertamento, con l'accordo del 28 maggio 2012 (cfr. verbale 21 giugno 2012, all. 16), la società ha dato attuazione agli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970 e, con comunicazione elettronica del 30 maggio 2012 (all. 16 al verbale 21 giugno 2012), ha altresì provveduto ad inoltrare ai capi compartimento il verbale di accordo per attivare il confronto con le organizzazioni sindacali locali e condividerne i contenuti tra il personale.

4.3. Il mancato rispetto, da parte della società, dei requisiti contemplati dal menzionato art. 4, comma 2, l. n. 300/1970, riverbera i propri effetti anche sulla liceità dei trattamenti effettuati fino al 28 maggio 2012, essendo stati gli stessi effettuati in violazione degli artt. 11, comma 1, lett. a) e 114 del Codice (cfr. Provv. 7 ottobre 2010, doc. web n. 1763071), oltre che (sino a tale data) in assenza di uno dei presupposti di cui agli artt. 23 e 24 del Codice (cfr. Provv. 4 ottobre 2011, n. 370, doc. web n. 1850581). Ne consegue l'inutilizzabilità dei dati riferiti alla prestazione di attività lavorativa trattati sino ad allora in violazione di legge ai sensi dell'art. 11, comma 2 del Codice.

5.1. Tanto premesso, va aggiunto che, per le ragioni di seguito sintetizzate, non è stato possibile all'Autorità accertare il profilo espressamente oggetto della segnalazione – concernente l'improprio utilizzo del sistema Rmt presso il Compartimento per l'Emilia-Romagna quale asserito strumento di controllo vietato dall'art. 4, comma 1, l. n. 300/1970 – mediante l'esame di elementi obiettivi, quali le immagini registrate (per desumere dalle stesse e dalle modalità di impiego, in concreto, elementi di giudizio).

In particolare, nel corso delle attività di accertamento svoltesi il 28 marzo 2012, non è stato possibile visualizzare immagini registrate sull'assunto che le stesse sarebbero conservate "di regola per 24 ore" (cfr. verbale 28 marzo 2012, p. 3), salva la possibilità, in relazione ad eventi critici di volta in volta evidenziati dalle sedi periferiche (ad esempio, in caso di emergenza neve), di "modificare per brevi periodi l'impostazione di sistema […] al fine di consentire a tutti i mezzi di effettuare lo scarico dei dati nei server della società" (cfr. verbale 17 maggio 2012, pp. 2 e 3). Decorso tale intervallo temporale, le immagini verrebbero eliminate dal sistema e non potrebbero essere recuperate (cfr. verbale 28 marzo 2012, p. 3; v. altresì verbale il 17 maggio 2012, pp. 2 e 3).

Peraltro, (già) durante le verifiche del 28 marzo 2012, e segnatamente in occasione degli accessi al sistema Rmt presso la sala operativa del Compartimento di Bologna, sono stati rilevati elementi tali da far dubitare che il dichiarato arco temporale di 24 ore fosse (sempre) stato il tempo effettivo di conservazione dei dati. Infatti, tra le operazioni annotate nel c.d. registro di sala sono state rilevate tre distinte operazioni di modifica dei tempi di conservazione ad opera di un utente "RootRoot" con probabile profilo di amministrazione di sistema (la prima delle quali è annotata nel sistema come "tempo cancellazione file archivio videosorveglianza modificato da 87600 a 24 ore"). Operazione intervenuta poco prima del primo accesso al sistema da parte del personale dell'Autorità incaricato delle verifiche, seguita da due successive operazioni, di segno opposto, con le quali dapprima è stato ripristinato il preesistente ampio termine di conservazione (di 87600 ore, pari a 10 anni) e, quindi, con una successiva operazione, l'arco temporale è stato nuovamente ricondotto alle "dichiarate" 24 ore (cfr. verbale 28 marzo 2012, p. 4).

Per effetto di tali operazioni si è determinata la cancellazione di tutte le immagini in precedenza registrate (il cui termine di conservazione era quello decennale), con la conseguente impossibilità di visualizzarle ed acquisirle al fine di verificare la fondatezza della segnalazione e le effettive modalità di impiego del sistema Rmt presso la sede di Bologna (in chiave di controllo dei lavoratori in violazione dell'art. 4, comma 1, l. n. 300/1970) rispetto alle finalità che la società ha dichiarato di perseguire.

Condotte tenute nel corso degli accertamenti e profili di illiceità dei trattamenti di dati personali effettuati nella gestione del sistema Rmt.

6.1. Considerato l'accaduto e le dichiarazioni rese presso la sede compartimentale di Bologna – dove i rappresentanti della società si sono limitati a dichiarare che "gli operatori di sala presso il Compartimento non possono intervenire sulla configurazione del sistema" (cfr. verbale 28 marzo 2012, p. 4) –, sono state quindi effettuate ulteriori verifiche al fine di chiarire l'accaduto e portare a compimento gli accertamenti relativi alla complessiva liceità delle operazioni di trattamento connesse al funzionamento del sistema Rmt.

6.2. In questa cornice, nel corso del successivo accertamento presso la sede legale di Anas in Roma, la società ha rappresentato che, in coincidenza con le verifiche effettuate presso la sala operativa del compartimento dell'Emilia Romagna, attese le esigenze di costante aggiornamento del sistema Rmt (in ragione del suo impiego ancora in fase sperimentale), sarebbero stati effettuati test di funzionalità dello stesso comportanti la modifica dei tempi di conservazione delle informazioni oggetto di trattamento con riguardo all'intero sistema e, quindi,

coinvolgenti tutti i compartimenti in cui esso si articola. In particolare è stato dichiarato che "erano in corso dei test sulla funzionalità del sistema con modifiche di prova delle impostazioni dei tempi di conservazione delle immagini" riguardante "l'intero sistema e quindi anche gli altri compartimenti". Tali modifiche sarebbero state effettuate mediante un accesso sistemistico ad opera dei dipendenti di Tecnositaf s.p.a., società cui è affidata la "gestione del sistema" e che "cura gli interventi attraverso due propri dipendenti, che svolgono le attività di amministratori di sistema" (cfr. dichiarazioni rese nel verbale 17 maggio 2012, p. 4).

6.3. Tale circostanza non ha tuttavia trovato riscontri obiettivi a fronte delle ulteriori verifiche effettuate dall'Autorità. Essa, infatti, non è stata riscontrata dalla consultazione del registro degli accessi di altro compartimento scelto a campione (cfr. verbale 17 maggio 2012, p. 7, con riguardo all'accesso al modulo eventi della sala operativa Toscana). Né ha trovato conferma in occasione degli ulteriori accertamenti effettuati presso Tecnositaf dai quali è invece risultato che Tecnositaf può effettuare modifiche operative mediante i propri amministratori di sistema "su richiesta di personale Anas" tramite il sistema di gestione richieste (mediante apertura di ticket di servizio, di regola, da parte del responsabile dei sistemi informativi del compartimento, ticket che vengono preventivamente validati dalla direzione centrale di Roma) ovvero su richiesta telefonica da parte dell'help-desk o della direzione generale dei sistemi informativi (cfr. verbale 30 maggio 2012, pp. 3 e 4; v. pure il verbale 21 giugno 2012, pp. 3 e 4).

Con specifico riguardo alla circostanza della modifica del parametro dei tempi di conservazione effettuata il giorno 28 marzo 2012, utilizzando l'utenza "Root Root" presso il server del compartimento dell'Emilia Romagna, il rappresentante di Tecnositaf ha dichiarato che "la modifica non è stata effettuata a seguito di attività programmata o in generale per attività di test, ma su esplicita richiesta di Anas" avente carattere di "urgenza" (verbale 30 maggio p. 4). Stando alle dichiarazioni rese, la modifica sarebbe "stata ripetuta due volte (come da log presenti nel "registro") perché vi era il dubbio che la prima operazione non fosse stata recepita dal sistema" (verbale 30 maggio 2012, p. 4).

6.4. Alla luce degli elementi sopra rappresentati, tenuto conto delle discrasie tra le dichiarazioni rese nelle varie fasi del procedimento di accertamento, delle condotte tenute nonché di quanto emerso all'esito delle verifiche effettuate, l'Autorità provvederà ad inviare gli atti all'autorità giudiziaria per le valutazioni di competenza.

6.5. Inoltre, in conformità ai principi di correttezza (art. 11, comma 1, lett. a), del Codice) nonché di necessità e pertinenza (artt. 3 e 11, comma 1, lett. d), del Codice), e al fine di scongiurare rischi di improprio ed arbitrario utilizzo del sistema Rmt nei confronti dei lavoratori, deve altresì essere prescritto ad Anas, ai sensi degli artt. 143, comma 1, lett. b), 144 e 154, comma 1, lett. c) del Codice, quale misura necessaria, di impartire puntuali istruzioni ai propri responsabili ed incaricati del trattamento, nei termini previsti dall'accordo sindacale e dal Regolamento per la disciplina della videosorveglianza stradale e della localizzazione satellitare veicolare.

Profili di illiceità dei trattamenti di dati personali effettuati nella gestione del sistema Rmt, con particolare riferimento alle operazioni effettuate dagli amministratori di sistema

7.1. Quanto alla complessiva gestione del sistema Rmt, dagli accertamenti effettuati è emerso che Tecnositaf, assicurandone la manutenzione, opera con la qualificazione di "titolare autonomo" del trattamento (cfr. contratto all. n. 14 al verbale del 21 giugno 2012), ancorché la gestione operativa del sistema resti in capo ad Anas (verbale 30 maggio 2012, p. 3). In particolare, "Tecnositaf non interviene in autonomia sui sistemi compartimentali RMT di Anas in produzione, limitandosi a effettuare interventi di tipo manutentivo sul software RMT e a svolgerne le installazioni e gli aggiornamenti sui vari server compartimentali. […] Eventuali modifiche operative vengono pertanto svolte dagli amministratori di sistema Tecnositaf […] sempre su richiesta di personale Anas" (verbale 30 maggio 2012, p. 3).

7.2. Tanto premesso, e tenuto conto del potere decisionale esistente in capo ad Anas in ordine alle finalità e alle modalità del trattamento nonché agli strumenti utilizzati mediante il sistema Rmt (e del quale la società ha in concreto fatto uso, come sopra evidenziato), l'ambito di autonomia del quale Tecnositaf dispone in base all'accordo contrattuale valutato nella sua interezza, induce a ritenere che tale società operi in qualità di responsabile del trattamento, ai sensi dell'art. 29 del Codice (e non in veste di titolare del trattamento, come invece qualificata dall'art. 19 del accordo del 2 febbraio 2010, di cui al menzionato all. 14) (cfr. in merito Provv. 4 ottobre 2011, n. 370, cit.; v. pure Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, adopted on 16 February 2010, p. 8 ss.).

Anas dovrà pertanto provvedere a designare Tecnositaf s.p.a. quale responsabile del trattamento ai sensi dell'art. 29 del Codice, impartendo alla stessa le necessarie istruzioni rispetto al corretto funzionamento (anche in relazione alla designazione degli amministratori di sistema: cfr. parr. 8.1 ss.) del sistema Rmt, in conformità alle prescrizioni già impartite dal Garante con il menzionato Provv. 4 ottobre 2011, n. 370.

8.1. Nell'ambito delle complessive attività di accertamento correlate all'utilizzo del sistema Rmt, con particolare riguardo alla verifica delle menzionate circostanze che hanno determinato la modifica dei tempi di conservazione delle immagini presenti nell'archivio "videosorveglianza" del server del compartimento Anas per l'Emilia Romagna, è stata altresì verificata la modalità di attuazione delle misure prescritte con il provvedimento generale del 27 novembre 2008 (doc web n. 1577499) ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

8.2. In questa cornice, nel corso dell'accertamento ispettivo svolto il 17 maggio 2012, Anas (come detto) ha rappresentato che la gestione e la manutenzione del sistema Rmt "è affidata alla società Tecnositaf s.p.a. la quale cura gli interventi attraverso due propri dipendenti, che svolgono le attività di amministratori di sistema". Ha altresì dichiarato, sempre con riferimento al sistema Rmt, di aver individuato quali amministratori di sistema anche due propri dipendenti, che vi accedono "con le proprie credenziali individuali". Ogni amministratore, per poter operare sull'intero sistema Rmt, deve infatti essere abilitato all'accesso di ciascuno dei 22 server compartimentali che lo compongono.

8.3. A seguito delle verifiche ispettive effettuate presso Tecnositaf il 30 e 31 maggio 2012 è emerso che il sistema Rmt consta di numerose utenze alle quali è stato attribuito il profilo autorizzativo "administrator", che consente di accedere a tutte le funzionalità del sistema medesimo: per ampiezza e tipologia dei privilegi attribuiti, il profilo administrator coincide con la qualificazione di amministratore di sistema di cui al punto 1 del menzionato provvedimento del Garante del 27 novembre 2008.

Dall'esame degli elementi in atti (cfr. documento n. 5, allegato al verbale di operazioni compiute del 30 maggio 2012, "stampa riportante le

utenze abilitate all'accesso agli applicativi compartimentali Anas") emerge che, oltre ai due dipendenti indicati da Anas, risultano abilitati con profilo administrator anche altre sei persone, di cui tre dipendenti Anas e tre dipendenti della società Comp.Sys s.r.l., nonché un'utenza denominata "Root Root" e una denominata "User User". Le sei utenze nominative, ulteriori rispetto a quelle indicate da Anas il 17 maggio 2012, risultano create nel settembre 2011 (in relazione ai dipendenti Anas) e nel gennaio 2012, in relazione dipendenti Comp.Sys – società della quale Anas dovrà valutare l'eventuale designazione quale responsabile del trattamento (non risultando in atti documentazione pertinente al riguardo) –. L'utenza "Root Root" risulta creata il 22 giugno 2011 e l'utenza "User User" il 28 giugno 2011.

Quanto alle utenze degli amministratori indicati da Anas nel verbale del 17 maggio 2012, le stesse sono state create il 16 maggio 2012 per la maggior parte dei server compartimentali.

8.4. Per quanto riguarda i dipendenti Tecnositaf che svolgono le attività di amministratori del sistema Rmt, sulla base delle verifiche ispettive del 30 e 31 maggio 2012 è emerso che i predetti non sono stati formalmente individuati quali amministratori di sistema. Gli stessi, inoltre, accedono al sistema Rmt utilizzando la credenziale condivisa "Root Root".

8.5. Alla luce degli esiti degli accertamenti effettuati, sotto più profili Anas non ha dato attuazione al menzionato provvedimento del Garante del 27 novembre 2008 (come di seguito indicati ai punti a, b e c).

a. Con riferimento alle prescrizioni di cui al punto 2, lettere b) e c), 1° cpv., del provvedimento del Garante del 27 novembre 2008, si osserva che:

i. i dipendenti indicati da Anas nel verbale del 17 maggio 2012 sono stati formalmente individuati con atto del 20 aprile 2012 (allegato n. 1 del verbale di operazioni compiute del 21 giugno 2012). Con tale atto viene individuato quale amministratore di sistema anche un altro dipendente abilitato all'accesso al sistema Rmt. Tuttavia tale individuazione riguarda applicativi diversi dal sistema Rmt;

ii. relativamente ai dipendenti Tecnositaf, Anas ha esibito all'Autorità due documenti, sprovvisti di protocollo, datati rispettivamente 8 aprile 2011 e 31 maggio 2012 (allegati 4 e 5 del verbale 21 giugno 2012), con i quali Tecnositaf stessa comunica gli estremi identificativi degli amministratori di sistema;

iii. riguardo ai dipendenti di Comp.Sys s.r.l., Anas ha esibito al Garante una nota del 9 gennaio 2012, sprovvista di protocollo (allegato 6 del verbale 21 giugno 2012), con la quale Comp.Sys stessa comunica gli estremi identificativi degli amministratori di sistema. Non sono stati esibiti atti di individuazione formale dei predetti dipendenti quali amministratori di sistema;

iv. in relazione agli ulteriori soggetti abilitati all'accesso al sistema Rmt con profilo administrator, Anas ha rappresentato con nota del 4 luglio 2012 che "la designazione degli amministratori di sistema antecedentemente al 20 aprile 2012 veniva effettuata attraverso l'inquadramento negli ordini di servizio della Vice Direzione Sistemi Informativi […]". Tuttavia tali ordini di servizio, allegati alla predetta nota, non recano, con riferimento a ciascun dipendente individuato, l'elenco delle funzioni e degli ambiti di operatività assegnati in relazione ai profili autorizzativi attribuiti e agli applicativi in uso presso la società;

v. non sono state fornite indicazioni in ordine agli utilizzatori della credenziale "User User".

Alla luce di quanto sopra, deve quindi ritenersi che Anas non abbia compiutamente adempiuto alle prescrizioni del Garante, né abbia vigilato sul rispetto dei medesimi adempimenti a cura di Tecnositaf, in tema di individuazione ed elencazione degli amministratori del sistema Rmt.

Anas ha infatti provveduto all'individuazione formale degli amministratori di sistema solamente con un atto del 20 aprile 2012, nel quale peraltro non sono ricompresi tutti gli utenti abilitati all'accesso al predetto sistema con il profilo administrator. I precedenti atti richiamati da Anas per comprovare l'avvenuto adempimento alla prescrizione del Garante non contengono gli elementi richiesti nella prescrizione medesima, essendo stati predisposti per altre finalità.

Quanto a Tecnositaf, è in atti (verbale di operazioni compiute del 31 maggio 2012) la dichiarazione del direttore generale della società circa la mancata individuazione formale degli amministratori del sistema Rmt.

b. Con riferimento alle prescrizioni di cui al punto 2, lettera e), del citato provvedimento, deve evidenziarsi che, in base a quanto dichiarato da Anas nei verbali del 17 maggio e 21 giugno 2012, nonché da Tecnositaf il 30 maggio 2012, dipendenti delle due società accedevano al sistema RMT utilizzando la credenziale non individuale "Root Root".

La natura condivisa dell'utenza "Root Root" è, di per sé, tale da non consentire un'idonea registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema, atteso che tali accessi non possono essere ricondotti ad una singola persona fisica e necessitano, come nel caso delle modifiche operate al limite di conservazione delle immagini presenti nel server compartimentale dell'Emilia Romagna, di una ricostruzione delle attività dei singoli operatori non sempre in concreto praticabile.

Anche sotto questo profilo, pertanto, Anas non ha dato compiutamente esecuzione alla prescrizione del Garante in tema di registrazione degli accessi degli amministratori del sistema Rmt.

c. Con riferimento, infine, alla prescrizione di cui al punto 2, lett. c), 2° cpv, del menzionato provvedimento si rileva che, come

dichiarato da Anas nel verbale del 17 maggio 2012, l'informativa resa dalla società ai propri dipendenti in relazione ai trattamenti di dati personali effettuati mediante il sistema Rmt (allegato 3 del verbale di operazioni compiute del 17 maggio 2012) è costituita dal solo materiale didattico utilizzato nel corso di formazione dei lavoratori coinvolti nel progetto Rmt. Essa non reca alcuna indicazione in ordine agli amministratori del sistema.

D'altra parte, la circostanza che Anas non sia stata in grado di fornire all'Autorità un elenco completo degli amministratori del sistema Rmt che coincida con l'elenco degli operatori abilitati all'accesso al sistema medesimo con il profilo administrator è indicativa del fatto che un elenco del genere non sia stato, in nessuna altra forma, portato alla conoscenza dei dipendenti: anche in questo caso risulta, pertanto, disattesa la prescrizione impartita con il provvedimento del 27 novembre 2008.

8.6. Tanto premesso, il Garante, ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice:

a. prescrive ad Anas di dare integrale attuazione al provvedimento di questa Autorità del 27 novembre 2008 richiamato nelle premesse;

b. si riserva di valutare con autonomo procedimento la sussistenza della violazione di cui all'art. 162, comma 2-ter del Codice.

9. Ai sensi dell'art. 157 del Codice, si invita altresì la società a dare comunicazione al Garante delle misure adottate per conformarsi al presente provvedimento entro 60 giorni dal suo ricevimento.

10. Alla luce delle considerazioni che precedono – riservata la valutazione, con separato procedimento, della sussistenza di violazioni amministrative in capo ad Anas –, il Garante dispone la trasmissione degli atti e di copia del presente provvedimento all'autorità giudiziaria per le valutazioni di competenza.

In caso di inosservanza del presente provvedimento, si renderanno applicabili le sanzioni di cui agli artt. 162, comma 2-ter e 170 del Codice.

**TUTTO CIÒ PREMESSO IL GARANTE**

nei confronti di Anas s.p.a.:

1. dichiara illeciti, nei termini di cui in motivazione, i trattamenti di dati personali effettuati presso il Compartimento dell'Emilia-Romagna mediante il sistema Rmt, a mezzo delle telecamere nonché mediante il sistema di geolocalizzazione installati sui veicoli aziendali, anteriormente alla conclusione dell'accordo con le rappresentanze sindacali, con la conseguente inutilizzabilità dei dati trattati in violazione di legge ai sensi dell'art. 11, comma 2 del Codice (par. 4.3);

2. prescrive, ai sensi degli artt. 143, comma 1, lett. b), 144 e 154, comma 1, lett. c), del Codice, senza ritardo, e comunque entro 60 giorni dal ricevimento del presente provvedimento, quale misura necessaria, di:

a. impartire istruzioni ai propri responsabili ed incaricati del trattamento (par. 6.5);

b. designare Tecnositaf s.p.a. quale responsabile del trattamento ai sensi dell'art. 29 del Codice, impartendo alla stessa le necessarie istruzioni rispetto al corretto funzionamento del sistema Rmt, in conformità alle prescrizioni già impartite con il provvedimento del 4 ottobre 2011, n. 370 (par. 7.2);

c. valutare la necessità della designazione di Comp.Sys s.r.l. quale responsabile del trattamento ai sensi dell'art. 29 del Codice (par. 8.3);

d. dare integrale adempimento al provvedimento di questa Autorità del 27 novembre 2008 richiamato nelle premesse (par. 8.6);

3. ai sensi dell'art. 157 del Codice, invita la società a dare comunicazione al Garante delle misure adottate per conformarsi al presente provvedimento entro 60 giorni dal suo ricevimento (par. 9);

4. si riserva di valutare con autonomo procedimento la sussistenza delle violazioni amministrative previste dal Codice (par. 10);

5. dispone la trasmissione degli atti e di copia del presente provvedimento all'autorità giudiziaria per le valutazioni di competenza (par. 10).

Ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011, 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.

*Roma, 7 marzo 2013*

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia