Provvedimento del 7 marzo 2019 [9121890]

VEDI ANCHE: Newsletter del 25 gennaio 2021

[doc. web n. 9121890]

Provvedimento del 7 marzo 2019

Registro dei provvedimenti
n. 81 del 7 marzo 2019

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 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, ("Regolamento generale sulla protezione dei dati", di seguito "Regolamento");

VISTO il decreto legislativo 30 giugno 2003, n. 196, concernente il Codice in materia di protezione dei dati personali, di seguito "Codice";

VISTO il decreto legislativo 10 agosto 2018, n. 101, concernente "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (Regolamento generale sulla protezione dei dati);

ESAMINATE le risultanze istruttorie e la documentazione in atti relativa agli accertamenti in loco effettuati presso Roma Capitale e la società fornitrice di un sistema per la prenotazione e la gestione dei servizi al pubblico erogati allo sportello, nonché la documentazione integrativa fatta pervenire successivamente;

CONSIDERATO che i predetti accertamenti hanno riguardato anche altri soggetti in ordine ai quali il Garante si riserva di effettuare autonome valutazioni sulla base di ulteriori approfondimenti;

CONSIDERATO, pertanto, che il presente provvedimento ha a oggetto i trattamenti di dati personali posti in essere da Roma Capitale per la finalità di prenotazione degli appuntamenti dei servizi erogati ai cittadini e di gestione dell'affluenza del pubblico allo sportello;

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

RELATORE la dott.ssa Giovanna Bianchi Clerici;

PREMESSO

1. Premessa.

Nel corso dell'attività di controllo svolta dal Nucleo speciale Privacy della Guardia di Finanza nel 2018, su iniziativa dell'Autorità, è stato verificato, presso l'ente territoriale Roma Capitale (di seguito, "Ente"), il funzionamento del sistema denominato "TuPassi" (di

seguito, “sistema”), fornito dalla Miropass s.r.l (di seguito “Società”), per la gestione delle prenotazioni dei servizi al pubblico erogati allo sportello.

Il sistema consente agli utenti di prenotare servizi di sportello o fissare appuntamenti, presso soggetti pubblici e privati, utilizzando diversi canali: l’app mobile “TuPassi”, il sito web (www.tupassi.it e www.tupassi.com) oppure, direttamente presso la sede del soggetto che eroga il servizio, mediante l’uso di totem posizionati presso le loro sedi (cfr. verbali 11 e 12 settembre 2018, in atti).

Per usufruire del servizio di prenotazione, tramite app mobile o sito, gli utenti devono preventivamente registrarsi sulla piattaforma della Società, creando un account che consente di fissare o revocare appuntamenti presso tutti i soggetti che utilizzano il servizio di prenotazione (pubbliche amministrazioni, strutture sanitarie pubbliche e private, professionisti, etc.; cfr. pag. 2 verbale 11 settembre 2018).

2. L’attività istruttoria.

Il sistema è utilizzato dall’Ente, in qualità di titolare del trattamento, fin dal 2015, anno in cui era in corso la sua sperimentazione (cfr. nota 7.11.2018, all. nn. 1-6, spec. 5 e 6 relativi alla D.D. 81/2015, prot. n. 2295 e o.d.a. Mepa , prot. n. 6517/2015) ed è attualmente in uso presso “tutti i Municipi del Comune di Roma e da alcune strutture centrali” (cfr. pag. 4, verbale 10 ottobre 2018).

Le verifiche hanno riguardato uno dei Municipi interessati (il Municipio III), che lo utilizza per i seguenti servizi: “Demografico”, “U.R. PAG.”, “Protocollo”, “SUAP”, “Contrassegni invalidi”, “Accesso Re.I.”. In questo ambito, l’applicativo viene utilizzato come sistema di “prenotazione” e come strumento per la più efficiente gestione dell’affluenza di pubblico agli sportelli (cd. “elimina code”, cfr. pag. 4 verbale del 10 ottobre 2018).

Come “sistema di prenotazione”, l’applicativo consente di pianificare l’agenda degli appuntamenti, gestire l’erogazione dei servizi nei confronti dell’utenza, ottimizzare le chiamate allo sportello, estrarre report e statistiche sull’erogazione dei servizi.

In caso di prenotazione, oltre ai dati già acquisiti in sede di registrazione dell’account, il sistema acquisisce, nelle varie fasi di gestione dell’appuntamento, il canale utilizzato dall’utente per la prenotazione (app mobile, web, totem), la data e l’ora della prenotazione, la data e l’ora della “chiamata” dell’utente allo sportello e la data e l’ora dell’erogazione della prestazione (“lavorato”) (all. 2, verbale 11 ottobre 2018). All’atto della prenotazione, il sistema rende disponibile all’utente l’elenco dei servizi prenotabili. Una volta che l’utente ha selezionato il servizio e la data dell’appuntamento, il sistema trasmette al server dell’Ente l’informazione. I dati dell’utente che effettua la prenotazione sono acquisiti, tramite la Società, attingendoli dalle anagrafiche già registrate.

Tutte queste informazioni di dettaglio sono conservate anche successivamente alla fruizione del servizio (“lavorato”) o successivamente alla revoca dell’appuntamento (“revocato”) in quanto l’Ente ha configurato il sistema prevedendo la cancellazione dei dati delle prenotazioni solo dopo tre mesi dalla data dell’appuntamento. Infatti, nel corso degli accertamenti, alla data del 11 ottobre 2018, è stato verificato che “la prima agenda disponibile risale al 12 luglio 2018” (cfr. pag. 4 verbale 10 ottobre 2018; cfr. altresì, pag. 2 verbale 11 ottobre 2018).

E’ stato verificato che il sistema consente il trattamento anche di dati riferiti al personale che gestisce le varie richieste dell’utenza (addetti allo sportello, funzionari con altre mansioni e profili di abilitazione differenti). Tali informazioni, sebbene non siano sempre immediatamente visualizzabili (allegati 3 e 4, 6 e 7 al verbale 11 ottobre 2018), sono comunque memorizzate dal sistema e possono essere, in ogni caso, consultate ed esportate, previa selezione dello specifico campo (ad esempio, mediante la creazione di un file excel, pag. 2 e allegato 5 del verbale 11 ottobre 2018).

Per vero, nel corso degli accertamenti è stato verificato come “il sistema non consente [all’Ente] di escludere la memorizzazione delle suddette informazioni relative agli operatori” (cfr. pag. 2 verbale 11 ottobre 2018).

Inoltre, il sistema è idoneo a generare giornalmente diverse tipologie di report, estraibili su file excel, alcuni dei quali non contengono “alcun dato personale degli utenti ma solo quelli degli operatori” (cfr. pag. 4 verbale 10 ottobre 2018). I dati personali dei dipendenti possono ricorrere, in particolare, nei report denominati “per operatore” -ove il nome e il cognome dell’addetto allo sportello sono associati al giorno, al tipo di servizio e al numero complessivo degli appuntamenti lavorati- e in quello classificato “per andamento del servizio” - in cui il nome e il cognome dell’addetto allo sportello sono associati al numero della postazione assegnata nel dato giorno, alla data di prenotazione, all’orario dell’appuntamento, al tempo di chiamata dello stesso e al tempo di attesa, anche calcolato in secondi (cfr. all. n. 8 verbale 18 ottobre 2018).

L'Ente ha fatto presente che "almeno in un caso sono state utilizzate delle informazioni ricavate dai report estratti dal sistema TUPASSI, a richiesta del direttore del Municipio […] limitatamente al numero di prenotazioni nelle diverse sedi municipali con l'intento di valutare quale sede operativa fosse più utile e richiesta dai cittadini […]" precisando che in ogni caso, le "informazioni utili alla valutazione delle performance degli uffici sono effettuate sulla base di altri dati ricavati da altri sistemi" (cfr. pagg. 4 e 5 verbale 11 ottobre 2018).

2.1. L'architettura del sistema e misure di sicurezza tecniche e organizzative.

Il servizio di manutenzione e gestione applicativa del sistema è affidato alla Società, che fornisce, ai soggetti che si avvalgono del servizio, le necessarie componenti software da installare sui propri server.

L'Ente eroga il servizio mediante tre server ubicati presso il proprio Data Center, sito in via Cristoforo Colombo n. 570. I servizi infrastrutturali del Data Center (ambiente di virtualizzazione, servizi di base di backup e monitoraggio) sono affidati alla società DXC Technology in virtù di un contratto di servizio sottoscritto nell'ambito della convenzione quadro CONSIP SPC, lotto 1 (cfr. pag. 6 verbale 10 ottobre 2018).

Il traffico dati tra i server in questione e i totem e i monitor di sala (display) fisicamente distribuiti nelle varie sedi dei Municipi è effettuato mediante protocollo http; il traffico dati dall'operatore di sportello (che utilizza il sistema mediante una interfaccia web) e i server dell'Ente, avviene mediante il protocollo http o https (cfr. pag. 6 verbale 10 ottobre 2018).

L'accesso al sistema da parte degli operatori comunali è consentito a seguito di una procedura di autenticazione basata su "username e password" (cfr. pag.2, verbale 22 maggio 2018, in atti).

Il processo di gestione delle utenze (creazione, modifica del profilo di abilitazione, ecc.) è decentralizzato e demandato a ciascun Municipio, per il tramite di operatori a cui viene concessa una specifica abilitazione ("gestione operatori"). Dalla funzionalità "operatori" è possibile creare e gestire i profili di autorizzazione per gli operatori che accedono al sistema. Dalla stessa funzione si possono consultare i relativi dati personali quali "nome, cognome, user id, qualifica, se dispone delle autorizzazioni di admin e se è abilitato o meno"; dalle verifiche effettuate "la creazione di un nuovo operatore prevede l'inserimento obbligatorio di informazioni […] quali nome, cognome, user id e indirizzo e-mail direttamente riconducibili al dipendente" (cfr. pag. 3 verbale del 11 ottobre 2018).
Durante le attività ispettive, è emersa l'assenza di una procedura organizzativa per il rilascio delle utenze e per la gestione dei profili abilitativi. A riprova di ciò, si evidenzia infatti che, per acquisire l'elenco completo delle utenze abilitate per l'accesso al sistema, è stato necessario accedere direttamente, per tramite dell'amministratore di sistema della Società, alla base dati dell'applicativo (cfr. verbale del 16 ottobre 2018).

Dall'analisi dei dati raccolti, è emerso che in totale risultano 1246 utenze attive (alcune delle quali riconducibili però a personale non più in servizio) di cui 147 operatori riconducibili al Municipio III; 146 sono risultate le abilitazioni attive per la "gestione degli operatori".

Per quanto riguarda invece l'accesso ai server, è stato verificato che l'utenza root dei server, su cui è installato l'applicativo – utenza assimilabile ad un profilo di "amministratore di sistema" - è utilizzata da più tecnici, appartenenti all'Ente, alla Società e alla DXC technology, quindi le credenziali relative all'utenze amministrative sono condivise.

RITENUTO

3. Esiti dell'attività istruttoria.

Sia premesso come, in base alla disciplina di protezione dei dati, il trattamento deve avvenire in modo lecito, corretto e trasparente (art. 5, par. 1, lett. a) del Regolamento) e al ricorrere di una delle condizioni di cui all'art. 6 del Regolamento.

Il sistema utilizzato dall'Ente costituisce uno strumento per perseguire il miglioramento dell'efficienza ed economicità dell'attività amministrativa, attraverso la gestione delle prenotazioni degli appuntamenti dei servizi erogati allo sportello e delle attese; di conseguenza i trattamenti di dati personali effettuati possono essere considerati necessari per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. e) Regolamento) contemplato dall'ordinamento (art. 97 Cost., art. 1 l. n. 241/1990 artt. 1, 10 e 11 d.lg. n. 165/2001).

Alla luce della documentazione in atti e delle dichiarazioni rese nel corso dell'istruttoria (della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice), emerge tuttavia che Roma Capitale, impiegando il suddetto sistema di prenotazione, ha effettuato, fin dal 2015 e almeno fino alla data degli ultimi accertamenti ispettivi, operazioni di trattamento di dati personali degli utenti e dei dipendenti (cfr. paragrafo 2) non conformi alla disciplina in materia di protezione dei dati personali, per le ragioni di seguito indicate. Ciò, sia con riguardo alla disciplina vigente al momento della messa in funzione del sistema (d.lg. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali-di seguito Codice), alla disciplina del Regolamento (UE) 2016/679, in vigore dal 25 maggio 2018, e del Codice così come modificato dal decreto legislativo 10 agosto 2018, n. 101.

3.1. L'informativa agli interessati (utenti e dipendenti).

Dagli accertamenti effettuati, in particolare, simulando "la prenotazione di un servizio presso uno dei Municipi", è emerso che, in nessuna delle fasi di prenotazione/erogazione del servizio, gli utenti ricevono informazioni circa i trattamenti dei loro dati personali effettuati dall'Ente. Una informativa sul trattamento dei dati personali è resa infatti agli utenti esclusivamente da parte della Società, all'atto di creazione dell'account, in merito alle modalità di funzionamento del sistema ed al trattamento dei dati effettuato da parte della Società sviluppatrice, ma non contiene alcun rinvio a un'eventuale informativa del Comune circa il trattamento da questo effettuato nel perseguimento delle proprie diverse finalità. Né la stessa risulta conferita con modalità alternative (ad esempio, mediante l'invio di una eventuale e-mail di conferma della prenotazione dal Comune o dal Municipio selezionato nella predetta simulazione, cfr. relazione di servizio GdF 14 maggio 2018). Nel corso degli accertamenti è stata acquisita un'informativa generale, pubblicata sul sito istituzionale, relativa ai "trattamenti di dati personali degli utenti che consultano il sito … per fini istituzionali, allo scopo di abilitare l'utente che lo richiede, alla fruizione di servizi on-line erogati nel sito www.comune.roma.it nell'area servizi on-line" (cfr. all. 3, verbale 22 maggio 2018), che tuttavia non contiene alcun riferimento specifico alla raccolta, alla conservazione e alle altre operazioni di trattamento dei dati personali degli utenti, acquisiti tramite il sistema in esame.

Ciò detto, in relazione a tale fattispecie, con riferimento ai trattamenti di dati effettuati fino a quella data, è già in corso autonomo procedimento sanzionatorio.

Anche con riguardo ai dipendenti, non risulta che l'Ente abbia fornito la dovuta informativa circa le modalità e le finalità delle operazioni di trattamento rese possibili dal sistema. Ciò, in particolare, avuto riguardo alle informative individualizzate, rese a ciascun lavoratore, né a eventuali documenti informativi resi noti alla generalità dei dipendenti. Alcun riferimento alla raccolta e alle altre operazioni di trattamento dei dati personali dei dipendenti che utilizzano il sistema ricorre infatti nel "Regolamento per l'assegnazione e l'utilizzo delle dotazioni informatiche di lavoro" e di telefonia fissa e nella circolare del 22 marzo 2016, contenente indicazioni operative per l'uso delle postazioni di lavoro, diramata ai dipendenti (prot. n. GU3502) (cfr. nota del 7.11. 2018, cit., spec. all. 7, 8 e 9).

"[L]a comunicazione ai dipendenti interessati dell'attivazione del sistema eliminacode, con il relativo invito a partecipare all'incontro illustrativo/formativo con il referente della società"(cfr. nota integrativa del 5 novembre 2018, prot. 157832, e relativo all. G, relativo alla e-mail del 9 ottobre 2015, in atti) non può essere considerata sostitutiva dell´adempimento in esame, in quanto non reca gli elementi essenziali richiesti dalla disciplina di protezione dei dati (art. 13 del Codice e art. 13 Regolamento; cfr. quanto stabilito in European Court of Human Rights, Grand Chamber, case of Brbulescu v. Romania, Application no. 61496/08, 5 September 2017, spec. n. 140). Infatti, l'illustrazione delle funzionalità del sistema non risulta, in linea di principio, idonea a rendere edotti individualmente gli interessati con riguardo a tutte le operazioni di trattamento effettuate (nella citata e-mail ai dipendenti del Municipio III si legge espressamente: "scopo dell'incontro è l'illustrazione delle funzionalità del nuovo sistema e l'eventuale individuazione dei servizi da inserire nel sistema di prenotazione, oltre agli sportelli anagrafici a cui il sistema è inizialmente indirizzato", facendo rinvio per "ulteriori informazioni" a quanto desumibile dal sito dedicato al sistema; cfr. all. G cit.).

A tal fine non possono rilevare neanche le "due sessioni formative" (il 25 e 28 luglio 2017) organizzate dall'Ente, destinate solo ad alcuni dipendenti (i "referenti" designati dai direttori delle strutture territoriali e dai direttori delle U.O.A. Municipali), aventi ad oggetto alcune funzionalità dell'applicativo non inerenti alle operazioni di trattamento dei dati dei dipendenti (bensì, in particolare, l'"inserimento dei dati di contatto" dei cittadini, le modalità di prenotazione anche mediante tessera sanitaria presso i totem, la "modalità di configurazione delle agende e variazioni degli orari di appuntamento", cfr. all. L, in atti e, nota del 7 novembre 2011 all. n. 11).

Per le ragioni rappresentate, il trattamento risulta quindi essere stato effettuato in contrasto con l'obbligo, posto in capo al titolare del trattamento, di fornire l'informativa agli interessati e ai dipendenti, nonché con il principio di liceità, correttezza e trasparenza

(artt. 5, par. 1, lett. a) e 13 e 14 del Regolamento, già art.13 del Codice).

3.2. La disciplina in materia di controlli a distanza.

Le succitate plurime funzionalità del sistema di prenotazione (pianificazione dell'agenda degli appuntamenti, gestione dell'erogazione dei servizi nei confronti dell'utenza, ottimizzazione delle chiamate allo sportello, ed estrazione di report e statistiche sull'erogazione dei servizi) vanno distinte fra quelle meramente organizzative e quelle organizzative dalle quali potrebbe derivare la possibilità per l'Amministrazione di controllare a distanza l'attività dei suoi dipendenti. È di tutta evidenza come la pianificazione dell'agenda e l'elaborazione del piano di lavoro giornaliero, trattandosi di attività situate a monte e prodromiche dell'effettivo svolgimento della prestazione lavorativa, escludono ex se il controllo a distanza del lavoratore, che, come tale può avvenire solo contestualmente o a posteriori rispetto alla prestazione.

Di conseguenza, nel valutare il rispetto della disciplina relativa all'impiego di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell´attività dei lavoratori" (artt. 114 del Codice e art. 4, comma 1, l. 20 maggio 1970, n. 300, come modificato dall´art. 23 del d. lg. n. 151/2015), essenziale anche ai fini delle valutazioni circa la liceità del trattamento, va tenuta in considerazione la natura promiscua delle funzionalità del sistema, nonché l'oggettiva preminente finalità del suo impiego, consistente nel fornire agli operatori di sportello uno strumento efficiente col quale erogare il proprio servizio all'utenza.

Soltanto l'ultima fase del processo operativo del sistema, ovvero quella di estrazione di report e statistiche sull'erogazione dei servizi potrebbe integrare l'evenienza di un controllo a distanza sui lavoratori da parte dell'Amministrazione. Nel perseguimento delle specifiche finalità, il trattamento dovrà avvenire nell'osservanza delle condizioni di garanzia prescritte dall'articolo 4, comma 1 della legge n. 300 del 1970 (accordo sindacale o in alternativa autorizzazione pubblica), anche per effetto del rinvio operato dall'articolo 114 del Codice, costituisce condizione di liceità del trattamento dei dati personali (art. 5 e 6 par. 1, lett c) e 88, par. 2 del Regolamento e 114 del Codice).

3.3. Corretta definizione del ruolo svolto dalla Società nel trattamento.

Alla luce della documentazione in atti, emerge che il sistema di prenotazione è stato fornito all'Ente, con licenza d'uso, e che la Società Miropass garantisce il servizio di assistenza e manutenzione.
Ai fini del rispetto della normativa in materia di protezione dei dati personali assume, anzitutto, rilievo identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, in particolare quella di titolare e di responsabile del trattamento (artt. 4, par. 1, punto 7 del Regolamento e 28 e 29 del Codice). In particolare, il titolare del trattamento determina le finalità e i mezzi del trattamento. Tale potere si estrinseca, tra l'altro, nella facoltà di affidare a uno o più soggetti, persone fisiche o giuridiche, responsabili del trattamento, il trattamento di dati personali per proprio conto (artt. 4, par. 1, punto 8, e 28 del Regolamento).

Come rilevato anche nell'ambito dell'istruttoria, le funzioni svolte dalla società per assicurare l'assistenza e la manutenzione del sistema comportano anche un trattamento di dati personali di cui l'Ente è titolare.

In tale quadro, l'Ente non ha provveduto designare la Società quale responsabile del trattamento. Sotto questo profilo, infatti, la nota del 27 febbraio 2018 prot. n. GU20180003139 (cfr. allegato n. 2 al verbale del 10 ottobre 2018), peraltro molto successiva rispetto all'inizio del trattamento in esame, non risulta idonea a designare la Società quale responsabile del trattamento né ai sensi dell'art. 29 del Codice, in quanto del tutto priva di elementi essenziali quali i "compiti […] analiticamente specificati per iscritto dal titolare" e le "istruzioni"), né, allo stato, risulta che sia stato osservato quanto richiesto dall'art. 28 del Regolamento con riguardo all'individuazione e al contenuto che deve avere il contratto o altro atto giuridico tra il titolare e un soggetto che effettui un trattamento "per conto del titolare" stesso.

Anche sotto questo profilo, pertanto, il trattamento dei dati personali posto in essere dal Comune non risulta conforme alla disciplina di protezione dei dati personali (art. 29 del Codice con riferimento ai trattamenti al 24 maggio 2018 e, successivamente, art. 28 del Regolamento). La messa a disposizione alla Società di dati personali dei dipendenti dell'Ente ed eventualmente degli utenti che non abbiano effettuato la prenotazione direttamente tramite i servizi della Società (ad esempio, nel caso dei c.d. appuntamenti urgenti prenotati presso gli uffici dell'Ente), dà luogo, in assenza della preposizione a responsabile del trattamento, a una comunicazione illecita di dati personali (cfr. la nozione di "terzo" ai sensi dell' art. 4, par.1, punto 10 del Regolamento; art. 2-ter del Codice).

3.4. Le valutazioni dell'Autorità in ordine ai profili di sicurezza informatica: misure e accorgimenti necessari.

Sulla base di quanto accertato (cfr. paragrafo 2.1), si ritiene che le misure tecniche e organizzative implementate dall'Ente non possano ritenersi adeguate ai sensi dell'art 32 del Regolamento, in particolare per quanto riguarda la gestione delle utenze amministrative (quelle riconducibili ai cd. amministratori di sistema) nonché alla sicurezza delle comunicazioni e alla gestione delle utenze degli operatori.

In particolare, la condivisione delle credenziali dell'utenza di root dei server su cui è installato l'applicativo, rende di fatto inapplicabili diverse prescrizioni contenute nel citato Provvedimento generale sugli amministratori di sistema del 27 novembre 2008, volte a mitigare i rischi connessi allo svolgimento di tali mansioni. Infatti, la particolare criticità del ruolo degli amministratori di sistema deriva non solo dalla capacità di azione di tali soggetti sui dati personali trattati e dalla natura fiduciaria dei relativi compiti, ma anche dalla portata negativa di un'eventuale azione incontrollata di chi dovrebbe essere preposto anche a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico.

Per tali motivi, l'operato di chi agisce con privilegi di "utente amministrativo" deve essere sempre riconducibile ad un soggetto identificabile.

Infine, l'utilizzo del protocollo http per il traffico dati tra i server in questione, i totem, i monitor di sala e, in caso di scelta in tal senso, la postazione dell'operatore di sportello, non garantisce che sia assicurata, su base permanente, la riservatezza dei dati trattati, poiché il protocollo indicato non prevede la cifratura delle comunicazioni end-to-end.

4. Conclusioni.

Per i suesposti motivi, il trattamento dei dati personali effettuato da Roma Capitale attraverso il descritto sistema "TuPassi" risulta illecito per violazione degli artt. 5, 13, 14, 28 e 32 del Regolamento e 13, 29 del Codice (anteriormente alle modifiche apportate dal d.lg. 101/2018) nei termini di cui in motivazione e si ritiene pertanto necessario ingiungere alla suddetta Amministrazione di conformare il trattamento in esame alle disposizioni menzionate della normativa di settore (art. 58, par. 2, lett. d) del Regolamento).

Si rammenta, inoltre, che i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali "non possono essere utilizzati salvo quanto previsto dall'art. 160-bis" (art. 2-decies del Codice).

Alla luce di quanto rilevato con riguardo all'architettura del sistema e alle misure tecniche e organizzative (paragrafo 2.1.) si ritiene anche di ingiungere all'Ente di modificare le politiche di utilizzo dell'utenza root dei server su cui è installato l'applicativo, attuando gli accorgimenti di cui al Provvedimento del 27 novembre 2008, doc. web n. 1577499 ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema") e di adottare adeguate azioni correttive volte a eliminare le criticità, tecniche e organizzative, evidenziate al paragrafo 2.1, con particolare riguardo alla sicurezza delle comunicazioni e alla gestione delle utenze (art. 58, par. 2, lett. d), del Regolamento).

Considerato comunque che il sistema è funzionale alle legittime finalità organizzative, di efficienza ed economicità dell'attività amministrativa, al fine di non pregiudicare l'operatività dell'Ente, lo stesso potrà continuare ad essere utilizzato con le funzionalità non interessate dalle criticità rilevate in motivazione per la prenotazione dei servizi.

5. Indicazioni sulle misure organizzative e tecniche alla società fornitrice del servizio.

Tenuto conto che il sistema descritto è largamente utilizzato per la gestione dell'affluenza di pubblico agli sportelli e per la prenotazione di servizi all'utenza da parte di numerosi soggetti pubblici e privati (enti istituzionali, strutture sanitarie, imprese) e benché nel tenore letterale dell'art. 25 del Regolamento, il rispetto dei principi di privacy by design e by default è inteso come obbligo in capo ai soli titolari del trattamento, si ritiene comunque necessario incoraggiare Miropass s.r.l., in qualità di produttore del servizio, "a tenere conto del diritto alla protezione dei dati" ed "a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati", come previsto dal considerando 78 del Regolamento. Dall'attività istruttoria è infatti emerso come la versione standard dell'applicativo non consenta a chi lo utilizza di configurare "caso per caso" la tipologia dei dati trattati e i tempi massimi di conservazione, e quindi di rispettare i principi applicabili al trattamento dei dati (art. 5, par. 1, spec. lett. a), b), c) ed e) Regolamento).

Per tale motivo, il sistema prodotto dalla Società dovrebbe essere modificato in modo da consentire ai titolari del trattamento,

effettivi destinatari delle disposizioni di cui all'art. 25 del Regolamento, la possibilità di impostare le diverse tipologie di dati personali che intendono raccogliere, nonché i tempi di conservazione diversificati per ciascuna tipologia di dato, in relazione alle finalità concretamente perseguite, nel rispetto dei principi di cui all'art. 5 del Regolamento, mettendo in atto le "misure tecniche e organizzative adeguate" richieste dallo stesso art. 25 del Regolamento.

Per quanto riguarda la gestione dei dati personali riferibili agli utenti (che si avvalgono del sistema per la prenotazione), è altresì opportuno introdurre funzionalità che consentano di impostare i tempi di conservazione, prevedendo la cancellazione di tali dati dal sistema, una volta trascorsi i tempi indicati. In particolare, il sistema dovrà prevedere la possibilità di impostare tempi di cancellazione diversificati, in relazione agli esiti degli appuntamenti o di conservazione, in forma anonima (appuntamenti evasi, appuntamenti revocati, ecc.).

TUTTO CIÒ PREMESSO, IL GARANTE

nei confronti di Roma Capitale, dichiara illecito il trattamento descritto in motivazione (cfr. par. 2) con riferimento alla violazione degli articoli 5, 13, 14, 28 e 32 del Regolamento e 13 e 29 del Codice (anteriormente alle modifiche di cui al d.lg. n.101/2018), e, ai sensi dell'art. 58, par. 2, lett. d) del Regolamento, ingiunge alla suddetta Amministrazione di:

- conformare il trattamento in esame alle disposizioni menzionate del Regolamento e del Codice, come stabilito in motivazione, entro il termine di 90 giorni dal ricevimento del presente provvedimento;

- modificare le politiche di utilizzo dell'utenza root dei server su cui è installato l'applicativo, attuando gli accorgimenti di cui al Provvedimento del 27 novembre 2008, doc. web n. 1577499 ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema");

- adottare adeguate azioni correttive volte ad eliminare le criticità tecniche e organizzative (v. par. da 3.1 a 4).

Ai sensi dell'art. 58, par. 1, del Regolamento, ingiunge a Roma Capitale, entro 90 giorni dalla data di ricezione presente provvedimento, di comunicare le iniziative intraprese al fine di dare attuazione a quanto prescritto nel presente provvedimento e di fornire comunque un riscontro adeguatamente documentato.

Il mancato riscontro alla richiesta ai sensi dell'art. 58 è punito con la sanzione amministrativa di cui all'art. 83, par. 5, lett. e), del Regolamento (UE) 2016/679.

Ai sensi degli artt. 152 del Codice e 78 del Regolamento (UE) 2016/67, nonché dell'art. 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 2019

IL PRESIDENTE
Soro

IL RELATORE
Bianchi Clerici

IL SEGRETARIO GENERALE
Soro