UNIONE POLIZIA LOCALE ITALIANA
Articolo disponibile all'indirizzo: www.unionepolizialocaleitaliana.it/2021S04/

I PERMESSI ZTL NON DEBBONO RIVELARE L'IDENTITÀ DEL TITOLARE. SANZIONE A ROMA CAPITALE DI 350.000€.

di Massimiliano Mancini (massimiliano.mancini@hotmail.it)[a]

ABSTRACT: *I permessi per accedere alle zone a traffico limitato di Roma Capitale sono stati realizzati con un QR Code che, che consente a chiunque, mediante l'utilizzo di una generica applicazione per cellulari di conoscere i dati personali del titolare o dell'utilizzatore. Il Garante per la protezione dei dati, con provvedimento dell'11 febbraio 2021, ha elevato a carico dell'amministrazione cittadina la sanzione di 350.000 €.*

KEYWORDS: #privacy #GDPR #Garante #GarantePerLaPrivacy #GarantePerLaProtezioneDeiDati Personali #valutazionedimpatto #dpia #pia #trattamentodatipersonali #ztl #sanzioniprivacy #RomaCapitale #SanzioneRomaCapitale #MassimilianoMancini #EspertiUPLI #UPLI #UnionePoliziaLocaleItaliana

INDICE

I FATTI

Il Garante ha appreso da fonti di stampa e da una segnalazione che l'amministrazione capitolina di Roma Capitale ha rilasciato permessi cartacei da esporre sui veicoli per l'accesso e la sosta nelle zone a traffico limitato (ZTL), che riportano sul frontespizio un QR code, che consente a chiunque, mediante l'utilizzo di una generica applicazione per dispositivi mobili di conoscere i dati personali relativi al titolare del permesso Z.T.L. o al suo utilizzatore.

L'ISTRUTTORIA

Gli accertamenti del Garante hanno nel dettaglio che i QR code codificano indirizzi web in formato URL del tipo *https://permessiweb.atac.roma.it/VerifyPermit.aspx?PID=nnn&Source=xyz*, che includono al loro interno due parametri: il primo (denominato "PID"), identificativo del singolo permesso, costituito da una sequenza numerica, il secondo (denominato "Source"), che indica l'eventuale validità temporanea del permesso.

In questo modo chiunque avrebbe potuto collegarsi all'indirizzo web del servizio di verifica dei permessi Z.T.L., accedendo così ai dati relativi al singolo permesso, tra cui: la denominazione sociale o istituzionale (es. Questura di Roma, scuola elementare) oppure il nome e il cognome (nel caso di persona fisica) del titolare del permesso, il nome e il cognome dell'utilizzatore del permesso, la categoria del richiedente (es. artigiano, lavoratore orari notturni), nonché la targa del veicolo autorizzato.

Il Garante ma ha anche accertato che, semplicemente incrementando o diminuendo l'identificativo numerico del parametro denominato "PID" nel permesso all'interno dell'indirizzo web del servizio di verifica, era possibile persino visualizzare anche i dati personali relativi ad altri permessi Z.T.L.

[a] Segretario Generale UPLI, criminologo, già comandante dirigente di Polizia Locale e Provinciale, DPO/RPD e consulente privacy in enti pubblici e aziende private esperto in DPIA.

Il 20 maggio 2019 si è svolta l'audizione presso il Garante, ai sensi dell'art. 166, comma 6[1], richiesta da Roma Capitale, che ha rappresentato che "Roma Servizi per la Mobilità ha sempre ribadito […] la funzionalità dei contrassegni muniti di QR Code per il controllo da parte degli agenti accertatori e che le misure tecniche all'epoca adottate fossero rispondenti alla normativa vigente, [constatando] l'inidoneità delle stesse solamente a seguito di quanto è emerso al momento degli addebiti del Garante", e da Atac, che ha chiarito che fornisce a Roma Servizi esclusivamente un servizio di hosting e di manutenzione di data base e connettività e che non ha accesso ai dati personali trattati nei server messi a disposizione.

LA DECISIONE

L'autorità garante per la protezione dei dati personali, ha considerato il comportamento non doloso e ha tenuto conto dell'atteggiamento riparatorio di Roma Capitale, che si è attivata al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, introducendo alcune prime misure tecniche e organizzative ai sensi dell'art. 32 del Regolamento[2].

Si è tenuto inoltre conto però anche delle precedenti violazioni rilevate dall'Autorità nei confronti della stessa Roma Capitale nell'ambito di precedenti procedimenti (provvedimento n. 280 del 17 dicembre 2020 e provvedimento n. 48 dell' 11 febbraio 2021).

Pertanto nella valutazione complessiva degli elementi attenuanti e aggravanti del comportamento del Titolare del trattamento dei dati ha applicato la sanzione pecuniaria, nella misura di euro 350.000,00 (trecentocinquantamila) per la violazione degli artt. 5, 6, 28 e 32 del Regolamento, nonché 2-ter del Codice, quale sanzione amministrativa pecuniaria ritenuta effettiva, proporzionata e dissuasiva ai sensi dell'art. 83, par. 1, del GDPR[3].

---

[1] Decreto legislativo 30/06/2003 n. 196 "*Codice in materia di protezione dei dati personali*", art. 166 (Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori) c. 6: «Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.».

[2] Regolamento UE/2016/679 GDPR, art.32 (Sicurezza del trattamento) c.1: «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.».

[3] Regolamento UE/2016/679 GDPR, art.83 (Condizioni generali per infliggere sanzioni amministrative pecuniarie) c.1: «1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive. 2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32; e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione. 3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie

In considerazione dell'elevato numero degli interessati coinvolti nella illecita diffusione, che si è protratta per più di un anno, ha inoltre applicato la sanzione accessoria della pubblicazione del provvedimento sul sito del Garante, come previsto dall'art. 166, comma 7, del Codice e art. 16, comma 1, del Regolamento del Garante n. 1/2019.

PER ULTERIORI APPROFONDIMENTI SUL TEMA DELLA PRIVACY:

M.Mancini, La notifica del data breach.
https://www.unionepolizialocaleitaliana.it/sito/2021-16/

M.Mancini, I casi di data breach.
https://www.unionepolizialocaleitaliana.it/sito/2021-14/

M.Mancini, I reati di chi tollera la videosorveglianza illegittima.
https://www.unionepolizialocaleitaliana.it/sito/2021-05/

M.Mancini, Nulli e da sanzionare gli accertamenti audiovisivi delle aziende di raccolta rifiuti,
https://www.unionepolizialocaleitaliana.it/sito/2021-03/

M.Mancini, Sanzione di 10 milioni per la videosorveglianza abusiva.
https://www.unionepolizialocaleitaliana.it/sito/2021-01/

M.Mancini, DPIA per videosorveglianza, fototrappole e body cam.
https://www.unionepolizialocaleitaliana.it/sito/2021-02/

M.Mancini, La privacy nelle riprese foto e video.
https://www.unionepolizialocaleitaliana.it/sito/2020-10/

M.Mancini, La privacy nell'attività di polizia.
https://www.unionepolizialocaleitaliana.it/sito/2020-3/

disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. 4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43; b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43; c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4; 5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; b) i diritti degli interessati a norma degli articoli da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49; d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1. 6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. 7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro. 8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo. 9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.».

Ordinanza di ingiunzione nei confronti di Roma Capitale - 11 febbraio 2021 [9562852]

VEDI ANCHE NEWSLETTER DEL 29 MARZO 2021

[doc. web n. 9562852]

Ordinanza di ingiunzione nei confronti di Roma Capitale - 11 febbraio 2021

Registro dei provvedimenti
n. 49 dell'11 febbraio 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, 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 d.lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", come modificato dal d.lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio formulate dal Segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, in www.gpdp.it, doc. web n. 1098801;RELATORE la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. Premessa.

Da alcune notizie stampa, pubblicate nel mese di dicembre 2018, e da una segnalazione presentata all'Autorità, si è appreso che i permessi per l'accesso e la sosta nelle zone a traffico limitato ("Z.T.L.") di Roma Capitale, da esporre sui veicoli, riportano sul frontespizio un c.d. QR code, che consente a chiunque, mediante l'utilizzo di una generica applicazione per dispositivi mobili (mobile app) in grado di decodificarne il contenuto, di accedere a dati personali relativi al titolare del permesso Z.T.L. o al suo utilizzatore.

2. L'attività istruttoria.

In risposta alla richiesta di informazioni dell'Ufficio, Roma Capitale ha fornito riscontro (nota prot. n. XX dell'XX), per il tramite del

responsabile del trattamento designato, Roma Servizi per la Mobilità S.r.l. (di seguito, “Roma Servizi”).

Nello specifico, il legale rappresentante di Roma Servizi ha rappresentato, tra l’altro, che:

> “svolge per conto di Roma Capitale attività di assistenza e supporto nella gestione dei servizi di mobilità. In particolare e per quanto di interesse, Roma Capitale [le] ha affidato per proprio conto […] lo svolgimento delle attività inerenti al rilascio e al rinnovo dei permessi per l’accesso, la circolazione e la sosta nelle zone a traffico limitato […], la cui disciplina di base è contenuta nella deliberazione della Giunta comunale di Roma Capitale n. XX del XX”;
>
> “nelle attività di rilascio permessi Z.T.L. sono ricomprese quelle consistenti nella stampa e nel rilascio dei relativi contrassegni”;
>
> “un nuovo tipo di contrassegno in formato cartaceo riportante un QR code contenente le informazioni identificative dell’autorizzazione”, nonché “il relativo modello”, sono stati adottati con determinazioni dirigenziali nn. XX e XX del XX e del XX del Dipartimento Mobilità e Trasporti di Roma Capitale, e “l’attuale formato è operativo dal XX”;
>
> le informazioni riportate “in chiaro” (ovvero non codificate nel QR code) sul contrassegno, destinato ad essere esposto, riguardano: la tipologia di autorizzazione (es. accesso, sosta, scarico merci, etc.), la targa del veicolo, il numero del permesso e la validità temporale. Nel QR code sono invece riportate: la categoria del richiedente (es. domiciliato, distributore di merci, proprietario di posto auto, etc.), la ragione o denominazione sociale o istituzionale (in caso di veicolo appartenente a persona giuridica) o il nome e cognome (in caso di persona fisica) del titolare del permesso, nonché il nome e cognome dell’utilizzatore dello stesso;
>
> “tutte le informazioni riportate sul lato del contrassegno destinato ad essere esposto, alcune delle quali visibili solo con QR code, risultano essere necessarie a consentire le attività su strada condotte dalle competenti autorità volte a controllare che i permessi siano usati in conformità alla DGC XX”.

Dagli accertamenti preliminari d’ufficio si è verificato che i QR code, riportati nei permessi Z.T.L. – dieci dei quali sono stati prodotti da Roma Servizi nel corso dell’istruttoria, con nota prot. n. XX dell’XX – codificano indirizzi web in formato URL del tipo https://permessiweb.atac.roma.it/VerifyPermit.aspx?PID=nnn&Source=xyz, che includono al loro interno due parametri: il primo (denominato “PID”), identificativo del singolo permesso, costituito da una sequenza numerica, il secondo (denominato “Source”), che indica l’eventuale validità temporanea del permesso.

Si è, pertanto, accertato che con una generica mobile app, in grado di decodificare il contenuto dei predetti QR code, chiunque avrebbe potuto collegarsi all’indirizzo web del servizio di verifica dei permessi Z.T.L., accedendo così ai dati relativi al singolo permesso, tra cui: la denominazione sociale o istituzionale (es. Questura di Roma, scuola elementare) oppure il nome e il cognome (nel caso di persona fisica) del titolare del permesso, il nome e il cognome dell’utilizzatore del permesso, la categoria del richiedente (es. artigiano, lavoratore orari notturni), nonché la targa del veicolo autorizzato.

È stato, altresì, verificato che, modificando il valore del parametro denominato “PID” (semplicemente incrementando o diminuendo l’identificativo numerico del permesso) all’interno dell’indirizzo web del servizio di verifica, era possibile visualizzare anche i dati personali relativi ad altri permessi Z.T.L., pur non avendo a disposizione il corrispondente QR code. Ciò accadeva in quanto il servizio online di verifica dei permessi Z.T.L. risultava liberamente accessibile, non essendo protetto da alcuna procedura di autenticazione.

Sulla base degli accertamenti tecnici effettuati dall’Ufficio, il predetto servizio di verifica dei permessi Z.T.L. risultava erogato tramite risorse di rete (nomi a dominio e reti IP) riferibili ad Atac S.p.A. – Azienda per la mobilità di Roma Capitale (di seguito, “Atac”).

In risposta a un’ulteriore richiesta di informazioni (nota prot. n. XX dell’XX), Atac ha in effetti confermato di svolgere un servizio di hosting per conto di Roma Servizi cui fornisce hardware e “servizi di DB e connettività” sulla base di un “contratto di service” stipulato il 15 gennaio 2010, a seguito della costituzione di Roma Servizi mediante cessione del ramo di azienda della stessa Atac. Tale servizio, necessario per assicurare alla Roma Servizi, neo costituita, la continuità dei processi produttivi e amministrativi, sarebbe residuale, in quanto Roma Servizi si sta dotando di un proprio sistema informatico attraverso il quale gestire le attività e i servizi previsti dal contratto di servizio con Roma Capitale.

Dall'istruttoria è emerso, in ogni caso, che Roma Capitale non aveva individuato Atac quale responsabile del trattamento.

In relazione a tali violazioni, è stata effettuata a Roma Capitale, titolare del trattamento, la notifica, prevista dall'art. 166, comma 5, del Codice, della violazione degli artt. 5, 6, 28 e 32 del Regolamento, nonché 2-ter del Codice, comunicando l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, invitando l'ente a inviare scritti difensivi o documenti (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla l. n. 689 del 24 novembre 1981).

Con la nota prot. n. XX del XX, Roma Capitale ha inviato al Garante i propri scritti difensivi in relazione alle violazioni notificate, dichiarando, tra l'altro, che:

> ha "autorizzato nel 2016 l'utilizzo del contrassegno sulla affermazione di Roma Servizi per la Mobilità della necessità di utilizzo dello stesso "al fine di consentire al personale di verifica su strada l'effettuazione di controlli in tempo reale migliorando i livelli qualitativi di controllo" […]";
>
> "non risulta errata l'autorizzazione data da Roma Capitale ma l'uso che di tale autorizzazione ne ha fatto Roma Servizi per la Mobilità che non ha utilizzato strumentazioni atte ad evitare la lettura da parte di chiunque dei suddetti dati con una semplice app";
>
> "non è a conoscenza […] di violazioni importanti che abbiano cagionato danni ai cittadini inconsapevoli della consultazione dei dati personali, nessuna rimostranza e/o esposto risulta depositato al protocollo e, per tale motivo, […] ritiene che non vi sia stata una violazione importante dei dati personali, da addebitare alla mancata dotazione di strumentazione idonea per la rilevazione dei dati da parte di Roma Agenzia per la Mobilità";
>
> "dal 2 aprile 2019 è stato disposto il blocco della lettura del QR code sui contrassegni […]", in attesa di una soluzione definitiva che risponda ai rilievi espressi dall'Autorità;
>
> "nella riunione convocata […] in data 18 aprile c.a. sono state date [a Roma Servizi] precise direttive per adeguare tutto il sistema del trattamento dei dati personali alle indicazioni fornite dal Garante";
>
> "Roma Capitale ha autorizzato con nota QG 15700/2019 l'adozione di una modifica strutturale al processo di interrogazione dei permessi con QRCode autorizzando l'accesso e la visura delle informazioni dei permessi esclusivamente ai soggetti già autorizzati da RSM, proposta da RSM […]".

In data 20 maggio 2019 si è, inoltre, svolta, presso il Garante, l'audizione richiesta da Roma Capitale ai sensi dell'art. 166, comma 6, del Codice, in occasione della quale è stato rappresentato che "Roma Servizi per la Mobilità ha sempre ribadito […] la funzionalità dei contrassegni muniti di QR Code per il controllo da parte degli agenti accertatori e che le misure tecniche all'epoca adottate fossero rispondenti alla normativa vigente, [constatando] l'inidoneità delle stesse solamente a seguito di quanto è emerso al momento degli addebiti del Garante".

Nella stessa data si è svolta l'audizione anche di Atac, nel corso della quale la società, ribadendo quanto già precisato negli scritti difensivi, ha rappresentato, con riferimento al trattamento in esame, che fornisce a Roma Servizi esclusivamente un servizio di hosting e di manutenzione di data base e connettività e che non ha accesso ai dati personali trattati nei server messi a disposizione.

3. Esito dell'attività istruttoria.

Ai sensi del Regolamento, il trattamento di dati personali effettuato da soggetti pubblici (come Roma Capitale) è lecito solo se necessario «per adempiere un obbligo legale al quale è soggetto il titolare del trattamento» oppure «per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» (art. 6, par. 1, lett. c) ed e), del Regolamento; cfr. già art. 18, comma 2, del Codice previgente).

È, inoltre, previsto che «gli Stati membri possono mantenere […] disposizioni più specifiche per adeguare l'applicazione delle norme del […] regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto […]», con la conseguenza che, al caso di specie, risulta applicabile la disposizione contenuta nell'art. 2-ter, commi 1 e 3, del Codice, ai sensi

del quale «la diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste» da una norma di legge o, nei casi previsti dalla legge, di regolamento (cfr. anche artt. 19, comma 3, e 74 del Codice previgente).

Il titolare del trattamento è comunque tenuto a rispettare i principi in materia di protezione dei dati, fra i quali quelli di «liceità, correttezza e trasparenza», di «minimizzazione dei dati» e di «integrità e riservatezza», in base ai quali i dati personali devono essere «trattati in modo lecito, corretto e trasparente nei confronti dell'interessato», essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» ed essere «trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati" (art. 5, par. 1, lett. a), c) e f), del Regolamento; cfr. art. 11, comma 1, lett. d), del Codice previgente).

Ai sensi dell'art. 28 del Regolamento, il titolare può affidare un trattamento anche a responsabili del trattamento che presentino garanzie sufficienti con riguardo alla messa in atto di misure tecniche e organizzative idonee a garantire che il trattamento sia conforme alla disciplina in materia di protezione dei dati personali (cfr. art. 29 del Codice previgente). In questo caso, "i trattamenti da parte di un responsabile sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile al titolare e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare" (art. 28, parr. 1 e 3, del Regolamento).

Per quanto concerne la sicurezza del trattamento, l'art. 32 del Regolamento stabilisce che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" e che "nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare […] dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati" (cfr. già artt. 31 e ss. del Codice previgente).

Dalle verifiche compiute sulla base degli elementi acquisiti, anche attraverso la documentazione inviata dagli enti coinvolti, nonché dalle successive valutazioni, l'Ufficio ha accertato la non conformità – con riguardo sia alla disciplina previgente (ovvero al Codice, nel testo precedente alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101), sia all'attuale disciplina in materia di protezione dei dati – del trattamento in esame, effettuato a partire dal 1° dicembre 2016 e protratto fino al mese di aprile 2019.

3.1 La diffusione di dati personali

Quanto ai profili in particolare contestati, risulta, in primo luogo, accertato che i dati personali relativi ai titolari e agli utilizzatori dei permessi Z.T.L. esposti sui veicoli, sono stati resi accessibili a una platea indeterminata di soggetti terzi - i quali potevano leggere i QR code riportati nei permessi attraverso una generica mobile app, disponibile su comuni smartphone in grado di decodificarne il contenuto - dando, pertanto, luogo a una "diffusione" di dati personali (cfr. art. 2-ter, comma 4, lett. b) del Codice).

È stato, inoltre, verificato che accedendo all'indirizzo web del servizio di verifica dei permessi e modificando al suo interno il valore del parametro "PID", era possibile visualizzare i dati personali relativi a permessi Z.T.L. di soggetti a cui era stato rilasciato il permesso, pur non avendosi a disposizione il corrispondente QR code riportato nel permesso ad essi rilasciato.

Dal predetto accertamento è risultato, quindi, che la diffusione dei predetti dati personali, a partire dal 1° dicembre 2016 (data a decorrere dalla quale è operativo, per i permessi Z.T.L, il formato cartaceo riportante un QR code e il relativo servizio online di verifica), è avvenuta in maniera non conforme ai principi di base di protezione dei dati, nonché in assenza di un idoneo presupposto normativo, in violazione degli artt. 5 e 6 del Regolamento e dell'art. 2-ter del Codice.

3.2 La manacata regolazione del rapporto con il fornitore del servizio di hosting

Inoltre, tenuto conto delle dichiarazioni rese, anche nel corso delle audizioni, si osserva che, stante la definizione di "trattamento" (art. 4, par. 1, n. 2), del Regolamento), Atac, che forniva il servizio di hosting e di manutenzione di data base e connettività, ha trattato "dati personali" (art. 4, par. 1, n. 1), del Regolamento), effettuandone la registrazione e la conservazione, la cui trasmissione è implicita nell'uso dei protocolli di comunicazione telematica, quali l'indirizzo IP del dispositivo utilizzato dall'utente, la data e l'ora della connessione e l'indirizzo IP del server che ospitava il servizio in esame. Inoltre, pur non accedendo direttamente

ai dati personali trattati nell'ambito di tale servizio, in quanto fornitore di servizi di hosting, Atac conservava tali dati sulla propria infrastruttura tecnologica, assicurando determinati livelli di servizio in termini di disponibilità dei sistemi e mettendo a disposizione del cliente una serie di strumenti per gestire e monitorare il servizio.

Sulla base degli elementi sopra riportati, deve quindi ritenersi che le operazioni sopra descritte diano luogo a un trattamento di dati personali da parte di Atac (cfr. "Guidelines 7/2020 on the concepts of controller and processor in the GDPR", adottate dal Comitato europeo per la protezione dei dati il 2 settembre 2020, nella versione sottoposta a consultazione pubblica, in particolare, par. 2.1.4, punto 38, nella parte in cui è riportato l'esempio relativo agli "hosting services"), e che, pertanto, il ricorso da parte di Roma Capitale ai servizi offerti da Atac – in assenza di un contratto o altro atto giuridico che disciplinasse il trattamento di dati personali da parte di Atac, quale responsabile del trattamento – sia avvenuto in violazione dell'art. 28 del Regolamento.

3.3 La sicurezza del trattamento

Considerato che sussiste, in via generale, l'obbligo, in capo al titolare del trattamento, ai sensi dell'art. 24 del Regolamento, di adottare misure tecniche e organizzative adeguate affinché il trattamento sia conforme alla disciplina in materia di protezione dei dati personali, dando, altresì, precise e dettagliate istruzioni, in tal senso, al responsabile del trattamento, si rileva, con riguardo al caso di specie, la mancata configurazione di procedure, in grado di limitare l'accesso ai dati personali degli utilizzatori dei permessi Z.T.L. al solo personale effettivamente autorizzato al trattamento necessario per la finalità di interesse pubblico funzionale al controllo della validità dei permessi, con conseguente possibilità che i dati personali fossero liberamente accessibili da parte di chiunque fosse in possesso di uno smartphone dotato di una generica mobile app in grado di decodificare i QR code.

Accedendo all'indirizzo web del servizio di verifica dei permessi e modificando al suo interno il valore del parametro "PID", era inoltre possibile visualizzare i dati personali relativi a permessi Z.T.L. di soggetti a cui era stato rilasciato il permesso, anche non avendo a disposizione il corrispondente QR code riportato nel permesso ad essi rilasciato. In entrambi i casi, l'impropria configurazione del servizio, frutto anche delle mancate istruzioni al responsabile del trattamento dei dati, ha determinato la diffusione di dati personali sopra descritta.

Alla luce di quanto sopra, Roma Capitale si è resa responsabile della mancata adozione, in maniera non conforme al principio di «integrità e riservatezza», di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, creando le premesse per il verificarsi dell'illecita diffusione dei dati personali, in violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento (cfr. sul punto, seppur con riguardo a un diverso contesto, provv. n. 160 del 17 settembre 2020, doc. web n. 9461168, par. 3.4).

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento negli scritti difensivi della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per la determinazione della norma applicabile, sotto il profilo temporale, deve essere richiamato, in particolare, il principio di legalità di cui all'art. 1, comma 2, della l. n. 689/1981, ai sensi del quale le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati». Ciò determina l'obbligo di prendere in considerazione le disposizioni vigenti al momento della commessa violazione, che nel caso in esame – data la natura permanente dell'illecito contestato – deve essere individuato nell'atto di cessazione della condotta illecita, verificatasi successivamente al 25 maggio 2018, data in cui il Regolamento è divenuto applicabile. Dagli atti dell'istruttoria è, infatti, emerso che l'illecito trattamento risulta essersi protratto fino al mese di aprile 2019.

Si confermano pertanto le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato da Roma Capitale, in quanto esso è avvenuto in maniera non conforme ai principi generali del trattamento, in assenza di un'idonea base giuridica, nonché in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio presentato dal trattamento, in violazione degli artt. 5, 6, 28 e 32 del Regolamento, nonché 2-ter del Codice.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa ai sensi degli artt. 58, par. 2, lett. i), e 83,

parr. 4 e 5, del Regolamento medesimo, come richiamato anche dall'art. 166, comma 2, del Codice.

5. Misure correttive (art. 58, par. 2, lett. d), del Regolamento).

Prendendo atto di quanto emerso in sede di audizione e delle misure già introdotte, tenendo conto della circostanza che il servizio di verifica dei permessi Z.T.L. era esposto su rete pubblica e dei conseguenti rischi presentati dal trattamento, che derivano in particolare dalla possibilità di accesso, in modo accidentale o illecito, ai dati personali trattati, risulta necessario ingiungere a Roma Capitale, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di modificare, entro e non oltre 30 giorni dalla data di ricezione presente provvedimento, il sistema di autenticazione informatica utilizzato nell'ambito del servizio di verifica dei permessi Z.T.L., in conformità all'art. 32 del Regolamento, adottando, d'intesa con il responsabile del trattamento, le misure tecniche e organizzative di seguito indicate o altre misure analoghe, anche tenuto conto delle eventuali iniziative intraprese al riguardo nel corso del tempo, che garantiscano comunque un livello di sicurezza adeguato ai rischi presentati dal trattamento concernenti:

a) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le password relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" e che le medesime password siano modificate almeno al primo utilizzo;

b) la capacità di contrastare efficacemente attacchi informatici di tipo brute force sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione.

6. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i), e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie – considerando anche il richiamo contenuto nell'art. 166, comma 2, del Codice – la violazione delle disposizioni citate è soggetta all'applicazione della stessa sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare, tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

In relazione ai predetti elementi, si è valutato l'esteso lasso temporale in cui ha avuto luogo la violazione, nonché il fatto che la stessa abbia interessato un numero elevato di interessati. Risultano, inoltre, precedenti violazioni del Regolamento pertinenti commesse da Roma Capitale.

Di contro, si è tenuto conto che, sebbene la violazione in questione sia stata portata a conoscenza dall'Autorità attraverso diverse notizie stampa pubblicate nel mese di dicembre 2018 e mediante una successiva segnalazione, Roma Capitale si è attivata al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, introducendo alcune prime misure tecniche e organizzative ai sensi dell'art. 32 del Regolamento, essendo stato, in ogni caso, considerato il comportamento non doloso della violazione. Si è tenuto inoltre conto delle violazioni rilevate dall'Autorità nei confronti di Roma Capitale nell'ambito di precedenti procedimenti (provv. n. 280 del 17 dicembre 2020 e provvedimento n. 48 del'11 febbraio 2021).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria, nella misura di euro 350.000,00 (trecentocinquantamila) per la violazione degli artt. 5, 6, 28 e 32 del Regolamento, nonché 2-ter del Codice, quale sanzione amministrativa pecuniaria ritenuta effettiva, proporzionata e dissuasiva ai sensi dell'art. 83, par. 1, del medesimo Regolamento.

In relazione alle specifiche circostanze del presente caso, si ritiene, altresì, – anche in considerazione dell'elevato numero degli interessati coinvolti nella illecita diffusione, che si è protratta per più di un anno - che debba applicarsi la sanzione accessoria della

pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e art. 16, comma 1, del Regolamento del Garante n. 1/2019.

Si ritiene, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

rileva l'illiceità del trattamento effettuato da Roma Capitale per la violazione degli artt. 5, 6, 28 e 32 del Regolamento, nonché 2-ter del Codice, nei termini di cui in motivazione;

ORDINA

a Roma Capitale, in persona del legale rappresentante pro-tempore, con sede legale in Piazza del Campidoglio, n. 1, Roma – C.F. 02438750586 – di pagare la somma di euro 350.000,00 (trecentocinquantamila) a titolo di sanzione amministrativa pecuniaria per le violazioni di cui in motivazione; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

a) a Roma Capitale di pagare la somma di euro 350.000,00 (trecentocinquantamila) – fermo restando quanto disposto dal citato art. 166, comma 8, del Codice – secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

b) a Roma Capitale, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di conformare i trattamenti alle disposizioni del Regolamento, adottando le misure correttive indicate al paragrafo 5 del presente provvedimento, entro e non oltre 30 giorni dalla data di ricezione dello stesso. L'inosservanza di un ordine formulato ai sensi dell'art. 58, par. 2, del Regolamento, è punita con la sanzione amministrativa di cui all'art. 83, par. 6, del Regolamento;

c) a Roma Capitale, ai sensi dell'art. 58, par. 1, lett. a), del Regolamento, e dell'art. 157 del Codice, di comunicare, fornendo un riscontro adeguatamente documentato, entro e non oltre 30 giorni dalla ricezione del presente provvedimento, le iniziative intraprese per conformare i trattamenti a quanto previsto nel predetto paragrafo 5. Il mancato riscontro a una richiesta formulata ai sensi dell'art. 157 del Codice è punito con la sanzione amministrativa, ai sensi del combinato disposto di cui agli artt. 83, par. 5, del Regolamento e 166 del Codice;

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019;

l'annotazione del presente provvedimento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u), del Regolamento, delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, del Regolamento.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 11 febbraio 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE