Provvedimento del 20 giugno 2024 [10028498]

[doc. web n. 10028498]

Provvedimento del 20 giugno 2024

Registro dei provvedimenti
n. 374 del 20 giugno 2024

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 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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 (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 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 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, doc. web n. 1098801;

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. Introduzione.

L'Autorità ha appreso da fonti pubbliche che il Comune di Forlì (di seguito, il "Comune") aveva messo a disposizione dei cittadini un'applicazione informatica, denominata "Falco – Città protetta", sviluppata dalla FMI S.r.l. (di seguito, "FMI" o la "Società"), che consentiva ai cittadini inviare segnalazioni alla Polizia locale in merito a situazioni di degrado o che destavano un certo livello di

allarme sociale, comunque non tale da richiedere una chiamata di emergenza al 112.

Una volta ricevuta una segnalazione, il personale della Polizia locale addetto alla visione delle immagini di videosorveglianza, provenienti dalle telecamere installate sul territorio comunale per finalità di tutela della sicurezza urbana, poteva monitorare la situazione nella specifica area interessata dalla segnalazione ed eventualmente inviare una pattuglia in loco per effettuare verifiche, essendo, peraltro, temporaneamente acquisita la posizione GPS e il numero di telefono del dispositivo del segnalante.

Da una pagina informativa pubblicata sul sito web della FMI (https://www.fmi.fc.it/falco/), risultava, inoltre, che, a seguito della ricezione di una segnalazione, la Polizia locale avrebbe potuto anche inviare dei droni nell'area interessata per effettuare gli opportuni controlli.

In relazione al trattamento dei dati personali degli interessati, il Comune si qualificava come titolare del trattamento, indicando la FMI quale responsabile del trattamento (v. l'informativa sul trattamento dei dati personali al tempo pubblicata sul sito web istituzionale del Comune, all'indirizzo https://www.fmi.fc.it/privacy-falco/#1651136340326-95cb6497-1535), mentre la FMI si qualificava a sua volta quale titolare del trattamento (v. la diversa informativa al tempo pubblicata sul sito web della Società, all'indirizzo https://www.fmi.fc.it/privacy-falco).

2. L'attività istruttoria.

In riscontro a una richiesta d'informazioni dell'Autorità (v. nota prot. 37217 dell'8 luglio 2022), il Comune, con nota del 18 luglio 2022 (prot. n. 0083196/2022), ha dichiarato, in particolare, che:

> "con deliberazione di Consiglio Comunale n. 111 del 19/12/2018 e con successivo contratto n. 91 del 6/6/2019, venivano affidate a FMI […], […] [le funzioni di] gestione del sistema di videocontrollo del Comune […] e connesse alla vigilanza urbana […; con] detto contratto, all'art. 39, veniva individuata FMI quale titolare del trattamento dei dati personali per gli ambiti di propria competenza";
>
> "con deliberazione di Giunta del Comune […] n. 200 del 23/06/2021, facente seguito al trasferimento a FMI anche della funzione di supporto tecnologico alla progettazione e gestione dei sistemi di videosorveglianza, disposta con deliberazione di Giunta dell'Unione di Comuni della Romagna Forlivese n. 93/2018 […], si approvava il progetto definitivo/esecutivo "Città Protetta 2020 – 2° e 3°stralcio" […], redatto dalla […] FMI […] e si disponeva la presentazione dello stesso alla Prefettura [competente], in virtù di quanto previsto dal D.L. 20 febbraio 2017 n.14 […], [e] si incaricava FMI […] per l'attuazione del progetto su indicato e per la sua successiva gestione e rendicontazione";
>
> "[tale] progetto […] comprende al suo interno l'applicazione Falco […]. […] [Il] Sistema Falco si compone di una applicazione Web su server centralizzato e di una app che viene eseguita sui cellulari Android ed IOS (Apple); quest'ultima fornisce funzionalità sia proprie che in collegamento al sistema di videosorveglianza […] di proprietà del Comune […], gestito a livello tecnologico da FMI in base alle convenzioni in essere";
>
> "l'app "Falco", dopo essere stata scaricata sul cellulare di un utente, permette alle persone di verificare se si trovano in una zona videosorvegliata oppure no, in caso affermativo l'utente può decidere di inviare una segnalazione di tipo "alert" alle Centrali Operative, mettendo in evidenza […] la telecamera che riprende il cittadino che ha attivato la segnalazione. Questo permette di moltiplicare gli occhi di vigilanza sulla città, al fine di segnalare situazioni di degrado, o che destino preoccupazione, ma che non necessitino della chiamata al 112, che rimane la modalità principe per richiedere soccorso immediato alle Forze dell'Ordine. Falco quindi non mira a sostituirsi alla funzione del 112 bensì ad integrarla, permettendo ai singoli

cittadini di segnalare situazioni che meritano di essere evidenziate specialmente alla Polizia Locale, aumentando la percezione della sicurezza cittadina nella popolazione, come evidenziato dal Questore e dal Prefetto in sede di valutazione del progetto al [Comitato provinciale per l'ordine e la sicurezza pubblica] […]";

"Falco dispone anche di una applicazione lato server, messa a disposizione della Polizia Locale, con la quale si potrà effettuare il tracciamento di tutte le segnalazioni anonimizzate inviate tramite la app sul cellulare al fine di individuare quali zone presentano maggiori o minori segnalazioni nel tempo, al fine di poter integrare l'analisi del Comando di Polizia Locale rispetto alle zone da presidiare maggiormente in città";

"il sistema "Falco" non effettua alcun tracciamento dei percorsi effettuati dai cittadini, né memorizza i loro spostamenti. Solo in caso venga effettuata una segnalazione volontaria dal cittadino stesso, viene memorizzato temporaneamente (per 7 giorni) il numero di telefono associato alle coordinate geografiche (statiche) della segnalazione ed al timestamp, per permettere alle Centrali Operative di richiamare eventualmente il soggetto che ha effettuato la segnalazione. Trascorsi 7 giorni, il numero di telefono associato alle coordinate viene cancellato dagli archivi, di fatto anonimizzando pienamente il dato di cui rimarranno a disposizione, per soli fini statistici, le coordinate gps statiche della segnalazione ed il timestamp in cui è stata effettuata, senza alcun riferimento diretto o indiretto al soggetto che l'ha effettuata";

"l'applicazione, così come pensata e strutturata da FMI […], ha costituito, quindi, parte integrante di un progetto sulla sicurezza urbana presentato al Comitato [provinciale per l'ordine e la sicurezza pubblica]. Nel 2021 il progetto venne approvato e ritenuto meritevole dal Comitato tecnico, dalla Prefettura e dalla Questura, in quanto iniziativa valida per aumentare la percezione della sicurezza da parte dei cittadini; venne co-finanziato dal Ministero dell'Interno associato ad altri interventi di videosorveglianza nel progetto "Città Protetta 2020" nell'ambito di un bando per la videosorveglianza e la sicurezza nelle città […]";

"quando nel 2021 il progetto venne presentato in Prefettura, il Comune […] aderiva ancora all'Unione di Comuni della Romagna Forlivese per lo svolgimento delle funzioni di polizia locale. In seguito al recesso del Comune di Forlì dall'Unione (1/1/2022) ed alla conseguente riacquisizione delle competenze in tema di polizia locale, il Comune ha deciso l'utilizzo dell'app Falco per il supporto e la valorizzazione delle attività legate al servizio di polizia locale";

"Falco veniva caricata in versione beta da FMI sugli store di Apple e Google a dicembre 2021. […] Nella versione beta di aprile 2022 l'applicazione avrebbe consenti[to] al cittadino solo di: 1. effettuare una segnalazione specificandone la tipologia fra le categorie proposte da Falco (abbandono rifiuti, atti vandalici e graffiti, incidente stradale, violenza domestica, bullismo, altra segnalazione); 1. Effettuare una chiamata al 112 premendo il relativo tasto (112) con reindirizzamento alla tastiera del cellulare dell'utente. Lato back-end, come anticipato, era possibile solo risalire temporaneamente (per 7 giorni) al numero di telefono associato alle coordinate geografiche della segnalazione ed al timestamp, per permettere alle Centrali Operative di richiamare eventualmente il soggetto che ha effettuato la segnalazione";

"si specifica che in questa fase la Polizia Locale non ha proceduto al trattamento e alla gestione di alcuna segnalazione, se non a campione, e solo per supportare FMI nella fase di test dell'applicazione, in attesa di direttive esplicite per la Centrale Operativa circa la regolazione "privacy" e del manuale di istruzione dell'applicativo";

"contestualmente al formale distacco del Comune […] dall'UCRF, si procedeva alla nomina del [Responsabile della protezione dei dati – "RPD"] […, che], nel mese di aprile 2022 rappresentava all'amministrazione l'urgenza di accelerare la regolarizzazione dei progetti di videosorveglianza e dell'applicazione Falco connessa. Agli incontri partecipavano anche i referenti della società FMI […] in qualità di titolare del trattamento";

"[…] l'ente ha strutturato un percorso di allineamento [ai fini della] regolarizzazione di tutti i processi, complessivo dei seguenti step: 1. Prioritaria individuazione delle basi giuridiche del trattamento di videosorveglianza e di gestione delle applicazioni connesse nel regolamento di competenza del Consiglio comunale e negli ulteriori eventuali atti amministrativi generali (delibere di giunta, determine dirigenziali, accordi con l'UTG etc.); 2. Dettaglio nel medesimo regolamento dei principi generali e delle finalità dei sistemi, delle modalità del trattamento e dei diritti fondamentali degli interessati; 3. Rinvio dei dettagli organizzativi a provvedimenti secondari, come il disciplinare tecnico, strumento fondamentale per dare maggiore robustezza alla base giuridica; 4. Apertura dello strumento regolamentare verso possibili accordi interforze e innovazione tecnologica con valutazione di coinvolgimento della Prefettura nell'utilizzo condiviso dell'app Falco, stante le valutazioni di apprezzamento ricevute dal Comitato Ordine e Sicurezza Pubblica, dalla Prefettura e dalla Questura al momento della presentazione del progetto nel 2020 e che hanno portato all'ottenimento del finanziamento da parte del Viminale; 5. Realizzazione di una valutazione dei rischi e di una valutazione di impatto privacy limitatamente ai sistemi di videosorveglianza; 6. Adozione di una valutazione dei rischi e di una valutazione di impatto per l'applicazione Falco in sperimentazione, con eventuale attivazione del meccanismo della consultazione preventiva ex art 36 [del Regolamento] in caso di [valutazione d'impatto] con esito del rischio alto; 7. Redazione degli atti a cascata, fra cui nomine, formazione e istruzioni agli autorizzati ex art. 29 [del Regolamento], nomine ex art. 28 [del Regolamento], etc.";

"alla [luce] delle valutazioni svolte con la [RPD], l'Ente procedeva con la perimetrazione dei processi seguendo responsabilmente la timeline definita, ovvero partendo dalla primaria e assoluta necessità di individuare e perimetrare in maniera corretta la base giuridica di trattamento, non banalmente individuabile nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, parr. 1, lett. c) ed e), e 3, del Regolamento, nonché 2-ter del Codice) […]";

"in una delle prime fondamentali riunioni, tenutasi in data 26 aprile 2022 […] si è scelto di esplicitare in maniera maggiormente chiara e trasparente agli interessati tramite un'informativa privacy che l'applicazione si trovava in fase di sperimentazione e che questa si sarebbe protratta (almeno) fino al 31 maggio 2022, con valutazione di proroga";

"nell'informativa pubblicata sul sito istituzionale […] il Comune […] individuava FMI […] quale responsabile del trattamento […] per i trattamenti collegati all'app. Falco. Le normali incongruenze riscontrate [dall'] Autorità in virtù della differente informativa pubblicata sul sito di FMI (che si indicava, invece, titolare del Trattamento) sono la cartina di tornasole della fase transitoria che si stava attraversando. Ad oggi, infatti, la titolarità del trattamento rimane in capo alla società FMI […], essendo ancora in itinere la formalizzazione dei passaggi strutturali (condivisione dei processi con la Prefettura, sottoscrizione di patti, valutazione del rischio, DPIA dedicate etc.), all'esito dei quali il Comune […] diventerà autonomo titolare del trattamento, all'interno di un perimetro ben definito di basi giuridiche, finalità del trattamento e conseguente individuazione dei ruoli assunti da parte di terzi soggetti, fra cui, appunto, FMI […] individuata quale responsabile […] del trattamento ex art. 28 [del Regolamento]. L'informativa resa sul sito del Comune delinea una situazione che, pur se formalmente inesatta (stante la titolarità ancora in capo a FMI), descrive una situazione ibrida di fatto esistente";

“nella medesima riunione del 26 aprile 2022 ai referenti tecnici di FMI, veniva suggerito di ridimensionare ulteriormente […] “pro tempore", la portata dell’applicazione anche da un punto di vista tecnico, riportandola ad una fase embrionale. Fra le richieste, quelle di: - Ridurre i tempi di conservazione delle segnalazioni da 7 giorni a 24 ore; - Anonimizzare in maniera istantanea le segnalazioni all’arrivo sul server; - Riordinare le categorie di segnalazione opzionabili, in attesa di futuri ed eventuali accordi con la Prefettura, limitandole a: abbandono rifiuti, atti vandalici e graffiti, incidente stradale. - Disattivare il pulsante “altra segnalazione” per evitare l’invio di informazioni potenzialmente contenenti dati personali ultronei non trattabili”;

“lo step immediatamente successivo è stato il coinvolgimento della Giunta per la condivisione di tutti i processi. In data 6 luglio 2022 con Delibera di Giunta n. 237 veniva approvato il “Progetto di definizione strategica e normativa dell'impianto di videosorveglianza comunale con varchi di lettura targhe e nuove tecnologie dedicato alla sicurezza urbana integrata”;

“il disciplinare tecnico, ulteriore atto amministrativo generale, è l’ulteriore strumento suggerito dalla [RPD] del Comune e [da un consulente esterno] per l’ulteriore innalzamento dei profili di liceità del trattamento”;

“inoltre, si è anche consigliato il coinvolgimento della Prefettura - contestualmente alla presentazione del progetto di sicurezza urbana integrata e del collegamento interforze - con richiesta di rilascio di parere in merito alla necessità o meno di una loro integrazione per l’utilizzo dell’app. co-finanziata dal Viminale. La Prefettura di Forlì-Cesena è stata formalmente coinvolta nel percorso sopra delineato, a seguito di nota del Sindaco del Comune […] in data 13/07/2022 […]”;

“una volta messi a terra questi processi, perimetrata bene la base giuridica e realizzata la valutazione di impatto, si sarebbe proceduto con la formalizzazione delle nomine ex art. 28 [del Regolamento] (quella relativa alla gestione Falco già in possesso del Comune in versione bozza), le nomine ex art. 29 [del Regolamento] per gli autorizzati al trattamento e gli atti a cascata fra cui, molto importanti, le istruzioni da fornire agli operatori di polizia locale deputati all’utilizzo dell’applicazione. Da aprile 2022 a luglio 2022, il Comune […] procedeva, quindi, a produrre i regolamenti e gli atti per allinearsi alle normative vigenti”;

“l’8 giugno 2022 la società FMI comunicava via mail all’ente che l’applicazione Falco era stata riattivata per la parte dedicata alla possibilità di inviare segnalazioni. […] La Polizia Locale continuava e continua tuttora a non gestire alcuna segnalazione, fermata nella sua operatività da mancanza di direttive esplicite e dal manuale di istruzioni, come risultante da comunicazione della Sezione Centrale Operativa del Corpo di Polizia Locale di Forlì, in data 13 luglio 2022 […];

“a seguito [dell’avvio dell’istruttoria da parte del Garante] […] l’Ente chiedeva ad FMI di procedere immediatamente alla disabilitazione dell’applicazione, […] con pec indirizzata alla società FMI […] in data 12 luglio 2022 […]”;

“fra le ulteriori richieste fatte alla società FMI quelle di: - Anonimizzare tutte le segnalazioni giunte ed attualmente presenti nel database di Falco conservate da meno di sette giorni, così come era stato fatto nel primo depotenziamento; - Rimuovere l’App dagli Store, con blocco del download; - Disabilitare la possibilità di inviare segnalazioni per tipologia (rendendo inattiva l’applicazione anche sugli smartphone degli utenti che in precedenza avevano eseguito il download); - Disabilitare il bottone “112”. Queste modifiche tecniche sono state effettuate da FMI […] in data 11 luglio 2022 (come risultante da relazione in data 15/07/2022 a firma del Responsabile Sviluppo Tecnologico di FMI […])”;

“finalizzati i processi, l’intenzione del Comune […] è quella di valutare la sottoscrizione di due diverse nomine ex art. 28 [del Regolamento] con la […] FMI […], aventi ad oggetto una l’impianto di videosorveglianza generale, l’altra l’app. Falco nello specifico. Allo stato, la nomina relativa all’app. Falco è stata consegnata al Comune dal DPO in versione bozza in attesa che venga ultimato l’iter per il passaggio della titolarità dalla società al Comune”;

“[…] nessun dato personale è mai stato realmente trattato dalla Polizia Locale, che si è limitata unicamente a contattare a campione qualche utente, che nella maggior parte dei casi ha riferito di aver fatto un tentativo per vedere come funzionava l'applicazione […]; la sperimentazione in realtà non è terminata in data 31 maggio 2022, poiché la parte lato server di Falco, con relativo software dedicato alla gestione del dato da parte della Polizia Locale, non è mai entrato in funzione a pieno regime con una regolamentazione organizzativa precisa, formale ed adeguata”;

“l’applicazione memorizza […] solamente la posizione attiva al momento della segnalazione nel caso in cui l’utente abbia fornito il consenso alla condivisione di questo dato con l’applicazione Falco nel menù del suo cellulare. Non vengono effettuati trattamenti di percorsi degli utenti a nessun titolo e per nessun motivo”;

“l’applicazione […] [utilizza] l’impianto [di videosorveglianza] […]. L’obiettivo, […] non era quello di pervenire ad un’attivazione automatica di determinate telecamere a seguito della segnalazione, bensì quello di porre in primo piano, negli schermi della centrale operativa, filmati comunque già presenti al momento della segnalazione operata dal cittadino”;

“diversamente da quanto dichiarato da FMI nell’informativa pubblicata sul loro sito, non esiste nessun collegamento fra l’Applicazione Falco e l’utilizzo di droni, né ci sono automatismi tra i droni e il software per la gestione di Falco. Per cui il riferimento ai droni contenuto nell'informativa di FMI è assolutamente errato”;

“il Comune si trova ad oggi in itinere con la redazione della [valutazione d’impatto sulla protezione dei dati] […]”;

“le segnalazioni ricevute da Falco dal momento della prima attivazione in via sperimentale (aprile 2022), comprensive delle numerose prove di test e funzionalità effettuate da FMI in fase di verifica delle varie versioni dell’applicativo, sono n° 568. Sono tutte anonimizzate alla data del 11/7/2022; quelle più vecchie di 7 giorni lo erano già in precedenza in seguito alla funzionalità implementata lato server che ne prevede la cancellazione automatica. Dalla data della riattivazione (8 giugno 2022) solo 86 segnalazioni sono state ricevute da Falco di cui: - 16 per segnalazioni rifiuti abbandonati; 41 Altro (non è specificato cosa riguardino, si segnala solo una situazione di disagio generico di un cittadino che non trova una segnalazione idonea a quello che vuole esprimere), spesso si tratta di prove fatte per curiosità; - 16 chiamate fatte al 112 tramite app. falco; - 4 segnalazioni per graffiti - 5 segnalazioni per vandalismo - 1 per zona dove si consuma alcol - 1 per zona dove si usano droghe - 2 segnalazioni per incidente stradale. Dalla reportistica del software non risulta trattata dalla Polizia Locale nessuna di queste segnalazioni effettuate, nemmeno dopo la riattivazione del 9 giugno, a causa delle problematiche organizzative espresse nei paragrafi precedenti”;

“di fatto - l’applicazione non è mai effettivamente uscita dalla fase di test e la polizia locale non ha trattato alcun dato da essa derivante per la gestione delle segnalazioni […]”.
In riscontro a un’ulteriore richiesta d’informazioni dell’Autorità (v. nota prot. 0082766 del 17 dicembre 2022), il Comune, con nota dell’11 gennaio 2023 (prot. n. 0003022/2023), ha dichiarato, in particolare, che:

"l'informativa sul trattamento dei dati personali è stata predisposta su indicazione del [RPD] del Comune […] nel mese di aprile 2022 e messa a disposizione degli interessati sul sito web istituzionale del Comune nella versione iniziale in data 22 aprile 2022 e in quella aggiornata in data 2 maggio 2022";

è stata, altresì, "fornita agli interessati direttamente all'interno dell'applicazione informatica "Falco"" dalla FMI;

"il Comune, titolare del trattamento, ha aderito alle prospettazioni del proprio [RPD] […] e del consulente incaricato […] chiedendo a FMI […] in data 12 luglio 2022 […] l'immediata sospensione dell'applicazione e la ponderazione dei rischi per i diritti e le libertà dell'interessato, con valutazioni e conseguenti determinazioni che la società partecipata ha assunto in piena autonomia";

è stato stipulato un "protocollo d'intesa tra la Prefettura [competente] e il Comune […], Prot. 80936 del 7/12/2021, concernente il finanziamento statale ai sensi del D.L. 20 febbraio 2017 n. 14 […], del progetto "Forlì Città Protetta 2020", il quale comprende l'applicazione "Falco"".

Con nota del 10 maggio 2023 (prot. n. 0075074), l'Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, ha notificato al Comune, in qualità di titolare del trattamento, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, per aver:

- agito in maniera non conforme ai principi di "responsabilizzazione" e "protezione dei dati fin dalla progettazione e per impostazione predefinita", in violazione degli artt. 5, par. 2 (in combinato disposto con l'art. 24) e 25 del Regolamento;

- omesso di fornire agli interessati un'informativa sul trattamento dei dati nel periodo intercorrente tra il mese di dicembre 2021, in cui l'applicazione è stata resa disponibile online, e il 21 aprile 2022, e, successivamente a tale periodo, per aver fornito agli utenti informazioni non corrette in merito ad alcuni aspetti essenziali del trattamento, avendo agito in violazione degli artt. 5, par. 1, lett. a), e 13 del Regolamento;

- omesso di stipulare un accordo sulla protezione dei dati con FMI, in violazione dell'art. 28, par. 3, del Regolamento;

- omesso di redigere una valutazione d'impatto sulla protezione dei dati, in violazione dell'art. 35, par. 1, del Regolamento;

- agito in maniera non conforme al principio di "integrità e riservatezza" e in violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento, in relazione alla configurazione delle modalità di accesso al sistema informatico di gestione delle segnalazioni.

Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, dalla l. 24 novembre 1981, n. 689).

Con nota del 6 giugno 2023 (prot. n. 0071601/2023), il Comune ha presentato una memoria difensiva, dichiarando, in particolare, che:

il Comune "ha sempre e costantemente agito in assoluta buona fede; ogni errore o mancanza, eventualmente riscontrati, sono il frutto della strutturazione in itinere [del] processo […] legato ai trattamenti videosorveglianza […] [in un periodo in cui] il Comune si è trovato ad affrontare in un solo momento sia l'attuazione del progetto Città Protetta, sia l'integrale rifacimento di ogni adempimento privacy, conseguente all'avvenuta separazione

del corpo di Polizia locale da quello dell'Unione, con un personale gravemente ridimensionato ed in assenza della figura del Comandante della Polizia Locale, provvisoriamente sostituito da un Dirigente ad interim, già gravato da altri rilevanti incarichi dirigenziali";

"[…] l'intempestività della nomina ex articolo 28 in capo alla FMI (poi formalizzata ad agosto 2022) è stata causata dalla transitorietà di questa fase";

"nessun dato personale è mai stato realmente trattato dalla Polizia Locale. Da un punto di vista sostanziale, il danno per i diritti e le libertà dei cittadini è pressoché nullo. Le segnalazioni ricevute da Falco, dal momento della prima attivazione in via sperimentale fino a luglio 2022, comprensive di test e prove di funzionalità effettuate in gran parte dalla stessa FMI in fase di verifica, sono state in totale 568, tutte anonimizzate alla data del 11 luglio 2022; peraltro, quelle più vecchie di 7 giorni erano già state in precedenza. cancellate, grazie a una funzionalità di cancellazione automatica. Dalla data di riattivazione del 8 giugno 2022 (l'applicazione si presentava in versione ulteriormente depotenziata: si rimanda infatti alle precedenti note, ove si illustrava che, in assenza di un accordo con la Prefettura, venivano mantenute attive soltanto tre voci selezionabili da parte del cittadino) e sino al 11 luglio 2022 (dunque a fronte di soli 33 giorni di attivazione effettivi), sono state ricevute da Falco solo 86 segnalazioni, trattandosi perlopiù di prove e beta test. Dalla reportistica del software non risulta trattata dalla Polizia Locale nessuna di queste segnalazioni […]";

"[…] l'app Falco (riaccesa per 33 giorni unicamente al fine di proseguire i test) è sempre rimasta nella sua versione beta, con l'invio di segnalazioni perlopiù da parte dei dipendenti FMI al fine di testare le varie funzionalità, e con la messa a disposizione sui principali store unicamente ai fini di valutare la resa front-end dell'applicazione. Lo si ribadisce: il caricamento dell'app negli store non ne ha rappresentato l'attivazione definitiva, ma si trattava della necessaria fase di test, fondamentale al fine di poter valutare tecnicamente la tenuta dell'applicazione prima della release ufficiale";

"si ritiene che le azioni del Comune di Forlì oggetto di contestazione siano connotate, tutt'al più, da colpa lieve, derivante dall'intempestività nel dar corso ad adempimenti che, in ogni caso, erano in itinere già ben prima della richiesta di informazione dell'Autorità";

"l'approvazione del progetto in sede di Comitato per l'Ordine e la Sicurezza Pubblica ha portato gli attori a percepire temporaneamente come secondari gli adempimenti privacy";

"è [successivamente] iniziata, a partire dal mese di aprile 2022, una lunga fase di approfondita "messa in discussione" di tutto quanto realizzato fino a quel momento, unitamente alla collaborazione proattiva di un consulente esterno, con la realizzazione di un piano operativo strategico volto alla messa a terra, in tempi ristretti, di tutti gli adempimenti necessari. Tra le altre cose, si ricorda che già da aprile l'app Falco risultava spenta, su iniziativa del Comune […], proprio in quanto era stata fortemente percepita a livello comunale l'importanza di applicare i principi privacy fin dalla fase di progettazione";

"non era possibile nominare responsabili esterni senza aver completato i processi di perimetrazione dei ruoli e delle funzioni e senza previamente comprendere, tramite apposita valutazione dei rischi, quali misure di sicurezza pretendere dalla FMI […], società creatrice del software, prima del definitivo rilascio di quest'ultimo";

"[…] il Comune ordinava ad FMI di procedere con la disattivazione dell'applicazione, già a partire dal 12 luglio 2022. Le ripercussioni negative sui diritti dei cittadini sono state pertanto azzerate con effetto immediato, senza indugi".

3. Esito dell'attività istruttoria.

3.1 I trattamenti di dati personali posti in essere nell'ambito del progetto "Falco".

All'esisto dell'istruttoria, come sopra ricostruita, è emerso che, nell'ambito del c.d. progetto "Falco", il Comune, avvalendosi della FMI, ha realizzato un sistema informatico costituito da una componente del tipo "Web su server centralizzato" e, dal lato dell'utente, da una specifica applicazione informatica per dispositivi mobili (v. nota prot. n. 0083196/2022 del 18 luglio 2022).

L'applicazione informatica denominata "Falco" consentiva agli utenti di verificare la loro presenza in un'area sottoposta a videosorveglianza da parte del Comune, nonché di inviare segnalazioni relative a possibili situazioni di degrado o di generico potenziale rischio - non tali da rendere necessaria una chiamata di emergenza - mettendo in evidenza per gli operatori della Polizia locale, preposti alla visione delle immagini di videosorveglianza, gli specifici filmati trasmessi dalla telecamera presente sul luogo oggetto di segnalazione.

Quanto all'applicazione lato server del sistema Falco, la stessa veniva messa a disposizione della Polizia Locale per il tracciamento di tutte le segnalazioni anonimizzate inviate tramite la predetta applicazione, al fine di individuare quali zone presentassero maggiori o minori segnalazioni nel tempo, facilitando l'analisi del Comando di Polizia Locale in merito alle zone del territorio comunale da presidiare maggiormente. Era possibile solo risalire temporaneamente (per sette giorni) al numero di telefono associato alle coordinate geografiche della segnalazione ed al c.d. timestamp, per permettere alle Centrali Operative di richiamare eventualmente l'utente autore della segnalazione. Trascorsi sette giorni, il numero di telefono associato alle coordinate veniva cancellato dagli archivi, rimanendo disponibili, per soli fini statistici, le coordinate gps statiche della segnalazione ed il timestamp in cui la stata era stata effettuata.

Sul piano temporale:

- l'applicazione "Falco" è stata messa a disposizione nei negozi online "Google Play Store" in data 20 dicembre 2021 e "Apple Store" in data 26 gennaio 2022, in una versione che consentiva all'utente di inviare una segnalazione alla Polizia locale, senza che fosse prevista la possibilità di classificare la stessa con impostazioni predefinite; inoltre, l'utente poteva attivare la funzionalità "tastiera" del telefono preimpostata con il numero 112; le segnalazioni potevano essere volontariamente anonimizzate dall'utente, premendo un apposito tasto, ed erano in ogni caso automaticamente anonimizzate, mediante la cancellazione del numero di telefono associato alla posizione geografica statica del terminale da cui proveniva la segnalazione, dopo sette giorni dalla data di invio della stessa (v. relazione della FMI sub all. 9 alla nota prot. 0003022/2023 dell'11 gennaio 2023);

- in data 6 aprile 2022, l'applicazione è stata modificata come segue: è stata prevista la possibilità di specificare la tipologia di segnalazione da un elenco predefinito di voci (abbandono rifiuti, atti vandalici e graffiti, incidente stradale, violenza domestica, bullismo, altra segnalazione); è stata eliminata la possibilità per l'utente di anonimizzare la propria segnalazione prima del termine di sette giorni; è stata introdotta la possibilità di allegare una fotografia, ma solo se scattata ex novo, ovvero senza la possibilità di scegliere una foto già salvata nel terminale dell'utente (ibidem);

- dalla fine del mese di aprile 2022 l'applicazione è stata disattivata, per poi essere riattivata agli inizi del mese di giugno 2022 (v. relazione del RPD del Comune sub all. 5 alla nota prot. n. 0083196/2022 del 18 luglio 2022);

- in data 11 luglio 2022, a seguito dell'avvio dell'istruttoria da parte dell'Autorità, l'applicazione è stata rimossa dai negozi online (v. relazione della FMI citata) e tutte le segnalazioni

pervenute sono state anonimizzate.

È, inoltre, emerso che durante il normale utilizzo dell'applicazione, veniva inviata ogni 3,5 secondi una richiesta al server contenente un c.d. token firmato digitalmente, associato al numero di telefono dell'utente e alla posizione statica del dispositivo, che sarebbe stato "scartato (eliminato dalla memoria del server) dopo una verifica della firma e della data di scadenza dello stesso, in quanto il suo fine è esclusivamente evitare che i robot contattino in maniera massiva il web service", senza che lo stesso venisse "mai memorizzato nemmeno transitoriamente su un data base, nemmeno di cache o di appoggio"; la coordinata geografica statica non veniva "mai salvata in nessun caso[;] ricevuta la richiesta al webservice, [veniva] confrontata con l'elenco delle aree videosorvegliate (poligoni geometrici salvati nel database) e calcolato se risulta all'interno di una di esse oppure no. Il risultato di questa verifica [veniva] inviato all'app e le coordinate [venivano] eliminate senza essere mai memorizzate in nessun database, né di appoggio né di transito" (v. relazione della FMI sub all. 9 alla nota prot. 0003022/2023 dell'11 gennaio 2023).

Così riassunte le caratteristiche principali del sistema Falco, si osserva che il trattamento di dati personali posto in essere dal Comune, anche con riguardo, più in generale, alla gestione del sistema comunale di videosorveglianza, ha comportato la violazione di talune disposizioni della normativa in materia di protezione dei dati, di seguito in dettaglio illustrate.

3.2. La violazione dei principi di responsabilizzazione e protezione dei dati fin dalla progettazione

Sul titolare del trattamento, in quanto soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati, grava una "responsabilità generale" sui trattamenti posti in essere (cons. 74 del Regolamento). In base al principio di "responsabilizzazione", esso è, infatti, competente per il rispetto dei principi di protezione dei dati (art. 5, par 1, del Regolamento) e deve essere in grado di comprovarlo (art. 5, par. 2, del Regolamento). Ciò anche mettendo in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento (art. 24, par. 1, del Regolamento).

In particolare, in considerazione del rischio che incombe sui diritti e le libertà degli interessati, il titolare del trattamento deve - "fin dalla progettazione" e "per impostazione predefinita" (art. 25 del Regolamento) - adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati, integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati (cfr. "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020, spec. punti 42, 44 e 49).

Nel caso di specie, come sopra evidenziato, l'applicazione "Falco" è stata messa a disposizione nei negozi online "Google Play Store" in data 20 dicembre 2021 e "Apple Store" in data 26 gennaio 2022.

Dalla documentazione in atti emerge che:

> l'applicazione "Falco" è stata messa a disposizione "in versione beta" dalla […] FMI, per conto del Comune, sebbene la stessa "dove[sse] ancora essere testata dai tecnici della società" (nota del Comune del 18 luglio 2022, prot. n. 0083196/2022);
>
> già nel mese di dicembre 2021, il RPD del Comune, appena designata, in occasione dei primi incontri con i referenti dell'Ente, rappresentava "l'urgenza all'amministrazione di dare priorità alla regolarizzazione dei progetti di videosorveglianza e dell'applicazione connessa e già attiva […] denominata "Falco"". Veniva, altresì, coinvolto un professionista esterno che

“confermando le valutazioni espresse dalla [RPD] in merito alle criticità riguardanti l’impiego dei sistemi di videosorveglianza e delle relative applicazioni carenti di un’adeguata strutturazione organizzativa” (cfr. la relazione del RPD, sub all. 5 alla nota prot. n. 0083196/2022);

sulla base dei rilievi mossi dal RPD e dal consulente esterno, il Comune, nel mese di aprile 2022, pianificava una serie di azioni per assicurare il rispetto della normativa in materia di protezione dei dati personali, tra cui l’“individuazione delle basi giuridiche del trattamento di videosorveglianza e di gestione delle applicazioni connesse”, la “realizzazione di una valutazione dei rischi e di una valutazione di impatto privacy limitatamente ai sistemi di videosorveglianza”, l’“adozione di una valutazione dei rischi e di una valutazione di impatto per l’applicazione Falco in sperimentazione, con eventuale attivazione del meccanismo della consultazione preventiva ex art 36 [del Regolamento] in caso di [valutazione d’impatto] con esito del rischio alto” e la “redazione degli atti a cascata, fra cui […] [le] nomine ex art. 28 [del Regolamento], etc.” (ibidem);

solo “una volta messi a terra questi processi, perimetrata bene la base giuridica e realizzata la valutazione di impatto” il Comune avrebbe “proceduto con la formalizzazione delle nomine ex art. 28 GDPR (quella relativa alla gestione Falco già in possesso del Comune in versione bozza) […] e gli atti a cascata fra cui, molto importanti, le istruzioni da fornire agli operatori di polizia locale deputati all’utilizzo dell’applicazione” (ibidem).

in data 15 aprile 2022 si teneva una riunione tra il Comune la F.M.I. e, in quella sede, il RPD discuteva dei “profili di liceità dell’app e dello stato dei sistemi [di videosorveglianza] in generale, evidenziando le prime evidenti criticità” (ibidem);

in data 21 aprile 2022, il RPD, di concerto con il consulente esterno, inviava un’email al Comune, “confermando l’urgenza della situazione” (ibidem);

nonostante il RPD avesse invitato il Comune “alla prudenza suggerendo di sospendere il funzionamento dell’applicazione fino alla conclusione di tutti i processi, in special modo la redazione di un disciplinare dedicato e di una [valutazione d’impatto] ad hoc”, l’Ente procedeva dapprima procedeva alla disattivazione dell’applicazione e poi, in data 8 giugno, riattivava la stessa, contravvenendo alle indicazioni del RPD (ibidem);

in data 22 aprile 2022, il RPD scriveva alla referente del Comune “una comunicazione urgente”, contenente “una prima bozza di informativa privacy redatta appositamente per la app Falco”, evidenziando “la necessità che venisse pubblicata sul sito web istituzionale alla relativa sezione e che venisse chiaramente specificato che [la stessa] era riferita a un’applicazione attiva in fase sperimentale” (ibidem);

in data 26 aprile 2022, il RPD invitava “nuovamente e più riprese l’amministrazione alla prudenza”, suggerendo “di sospendere la app in attesa dell’adeguamento alle normative e di depotenziarla allo stato embrionale, in attese di definire tutti i processi” (ibidem);

il RPD sollecitava la necessità di “circoscrivere l’ambito di applicazione alla sola “sicurezza urbana” (con esclusione delle attività legate alla pubblica sicurezza), consigliando di rimuovere le voci “bullismo” e “violenza” dalle tipologie di segnalazioni opzionabili dal cittadino” (ibidem);

nell’aprile 2022, è stata messa a diposizione una versione “beta”, che consentiva al cittadino di “effettuare una segnalazione specificandone la tipologia fra le categorie proposte da Falco (abbandono rifiuti, atti vandalici e graffiti, incidente stradale, violenza domestica, bullismo, altra segnalazione)” e “effettuare una chiamata al 112 premendo il relativo tasto (112) con

reindirizzamento alla tastiera del cellulare dell'utente", sebbene, in questa fase, "la Polizia Locale non ha proceduto al trattamento e alla gestione di alcuna segnalazione, se non a campione, e solo per supportare FMI nella fase di test dell'applicazione, in attesa di direttive esplicite per la Centrale Operativa circa la regolazione "privacy" e del manuale di istruzione dell'applicativo" (ibidem);

il RPD, unitamente al consulente esterno, suggeriva di "aggiornare nuovamente le informative inerenti Falco per allinearle alle scelte fatte, delineando anche un'ideale timeline operativa, ricomprendente la realizzazione di un regolamento VDS ad hoc come base giuridica e i relativi disciplinari, l'eliminazione di tutti i dati personali raccolti e la realizzazione di un'apposita DPIA" (ibidem);

in data 27 aprile 2022, il RPD, di concerto con il consulente esterno, inviava una "nuova dicitura da caricare sul sito, nella sezione dedicata alla app Falco, con rimarco del depotenziamento e della fase sperimentale" e "riepiloga[va], ancora una volta, gli step per adeguare l'informativa" sia del sito sia dell'applicazione (ibidem);

in data 29 aprile 2022, il RPD inviata "una versione aggiornata dell'informativa" (ibidem).

in data 30 aprile 2022, il consulente esterno del Comune "delineava il percorso per regolarizzare i processi, con particolare attenzione all'applicazione falco" (ibidem);

in data 4 maggio 2022, il RPD avvertiva che anche se si procedesse alla "nomina di un responsabile esterno o l'adozione di disciplinare e procedure prima dell'approvazione del regolamento (base giuridica) avrebbe comportato in ogni caso una sanzione, in quanto totalmente carente tutta la parte di privacy by design", ribadendo la necessità di "seguire la […] timeline operativa" (ibidem);

in data 6 luglio 2022, il RPD inviava una comunicazione al Comune, ribadendo "il suggerimento di sospendere la App Falco finché non fosse stato traguardato l'intero percorso di compliance alla normativa – iniziato, ma […] ritenuto comunque non sufficientemente robusto", con particolare riguardo a "l'allegamento della base giuridica e le valutazione del rischio e di impatto" e "ritenev[a] prudenzialmente più corretto che fosse regolarizzato l'intero sistema di [videosorveglianza] e l'architettura del progetto Falco, prima di permetterne l'uso ai cittadini". Contestualmente, il RPD chiedeva a un ingegnere di effettuare "una prima valutazione tecnica della app e dei relativi profili di rischio privacy propedeutici alla valutazione del rischio e alla valutazione d'impatto". Tale ingegnere "oltre a confermare le perplessità emerse, ha rilevato l'alta probabilità che si sarebbe dovuto procedere a una consultazione preventiva del Garante, all'esito di una [valutazione d'impatto] che quasi certamente avrebbe riportato un alto impatto per i diritti e le libertà degli interessati" (ibidem);

in data 11 luglio 2022, il RPD riceveva "copia della Delibera del Consiglio n. 38 del 6 giugno 2022 di approvazione del Regolamento di [videosorveglianza] e della Delibera n. 237 del 6 luglio 2022 con la quale la Giunta ha adottato il progetto di sicurezza urbana integrata" (ibidem);

in data 11 luglio 2022, il Comune chiedeva alla FMI di procedere immediatamente alla disabilitazione dell'applicazione.

Dalla ricostruzione dei fatti occorsi emerge, pertanto, che il Comune, a partire dal mese di dicembre 2021, ha messo a disposizione degli utenti l'applicazione informatica "Falco" nonostante la stessa non fosse stata ancora testata e, successivamente - nonostante le criticità di protezione dei dati in più occasioni evidenziate dal RPD e da un consulente esterno già a partire dal dicembre

2021 e poi in maniera più puntuale nel mese di aprile 2022 (con particolare riguardo alla mancata valutazione della base giuridica applicabile e all'insussistenza di atti interni dell'Ente che disciplinassero compitamente il trattamento, all'analisi dei rischi derivanti dal trattamento, mediante una previa valutazione d'impatto sulla protezione dei dati, alla definizione dei rapporti con il responsabile del trattamento, alle istruzioni operative per gli autorizzati al trattamento e alle categorie di dati personali oggetto di trattamento) - ha continuato ad impiegare la predetta applicazione (con un'interruzione tra la fine di aprile 2022 e l'inizio di giugno 2022), fino all'11 luglio 2022, pur essendo pienamente consapevole di tali criticità.

Deve, inoltre, osservarsi che, nella prima versione dell'applicazione, caricata nei negozi online nel periodo dicembre 2021-gennaio 2022, gli utenti potevano effettuare liberamente una segnalazione, senza che fossero state predeterminate ex ante le situazioni che potessero potenzialmente formare oggetto di segnalazione.

Anche nella successiva versione del 6 aprile 2022, pur essendo stato inserito un elenco predefinito per classificare la segnalazione, è stata comunque lasciata la possibilità di effettuare una segnalazione di altra tipologia non specificamente indicata, così esponendo il titolare del trattamento all'eventualità di raccogliere e trattare dati personali non necessari o non pertinenti rispetto alla finalità perseguita oppure dati personali relativi a categorie particolari (cfr. art. 9 del Regolamento) o a condanne penali e reati (art. 10 del Regolamento), in assenza di base giuridica. Inoltre, consentendo agli utenti di inviare segnalazioni anche in relazione ad episodi di violenza domestica e bullismo - fattispecie di potenziale rilevanza penale (v. art. 610 c.p.) certamente non riconducibili alle funzioni amministrative del Comune - l'Ente si è ulteriormente esposto a tale rischio.

Il Comune ha, pertanto, posto in essere un trattamento di dati personali, mediante l'applicazione "Falco", senza assicurarsi che i profili di protezione dei dati fossero tenuti in debita considerazione "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento", individuando e mettendo in atto misure tecniche e organizzative adeguate rispetto ai rischi derivanti dal trattamento (art. 25 del Regolamento). Ciò anche al fine di assicurare il rispetto dei principi in materia di protezione dei dati (art. 5 del Regolamento) già in fase di progettazione del trattamento e di sviluppo dei sistemi informatici attraverso i quali effettuare lo stesso, nonché al fine di inquadrare correttamente i trattamenti di dati personali posti in essere per quanto concerne l'individuazione della base giuridica applicabile per ciascuna finalità di trattamento.

Le medesime considerazioni valgono anche con riguardo ai trattamenti di dati personali effettuati dal Comune mediante il sistema di videosorveglianza comunale, rispetto al quale sia il RPD sia il consulente esterno avevano reso edotto il Comune delle medesime criticità con riguardo ai profili di protezione dei dati personali. Il Comune ha ciononostante continuato a tenere attivo il proprio impianto di videosorveglianza, pur essendo del tutto consapevole delle predette criticità. Soltanto nei mesi di giugno e luglio 2022 l'Ente ha approvato il proprio regolamento sulla videosorveglianza (v. delibera n. 38 del 6 giugno 2022, sub doc. 8 alla nota prot. n. 0083196/2022 del 18 luglio 2022) e il progetto di c.d. "sicurezza urbana integrata" (v. delibera n. 237 del 6 luglio 2022, sub doc. 9 alla nota prot. n. 0083196/2022 del 18 luglio 2022). Inoltre, come emerge da una nota del RPD del 6 luglio 2022, in atti, il Comune non aveva stipulato un patto per l'attuazione della sicurezza urbana, mediante sistemi di videosorveglianza, con la Prefettura territorialmente competente (come richiesto dall'art. 5, comma 1, lett. a), del d.l. 20 febbraio 2017, n. 14), non aveva proceduto a stipulare un accordo sulla protezione dei dati con il responsabile del trattamento (ovvero la FMI) e non aveva individuato gli autorizzati al trattamento (v. allegato sub doc. 12 alla nota prot. n. 0083196/2022 del 18 luglio 2022).

Alla luce delle considerazioni che precedono, deve concludersi che il Comune ha agito in maniera non conforme ai principi di "responsabilizzazione" e "protezione dei dati fin dalla progettazione e per impostazione predefinita", in violazione degli artt. 5, par. 2 (in combinato disposto con l'art. 24)

e 25 del Regolamento.

3.3 La trasparenza del trattamento

In base al principio di “liceità, correttezza e trasparenza”, i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5, par. 1, lett. a), del Regolamento).

Nel rispetto di tale principio, il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12 del Regolamento; cfr. Gruppo di lavoro art. 29, “Linee guida sulla trasparenza ai sensi del regolamento 2016/679”, WP260 rev.01 dell’11 aprile 2018, fatte proprie dal Comitato europeo per la protezione dei dati con “Endorsement 1/2018” del 25 maggio 2018).

Nel caso di specie, il Comune ha fornito l’informativa sul trattamento dei dati personali agli utenti dell’applicazione “Falco” soltanto in data 22 aprile 2022, pubblicando la stessa sul proprio sito web istituzionale, con successivo aggiornamento della stessa in data 2 maggio 2022.

Pertanto, nel periodo intercorrente tra il mese di dicembre 2021, in cui l’applicazione è stata resa disponibile online, e il 21 aprile 2022, il Comune ha omesso di fornire agli interessati una propria informativa sul trattamento dei dati personali, agendo in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

Non può, peraltro, a tal riguardo, essere tenuta in considerazione l’informativa fornita dalla FMS - erroneamente qualificatasi come titolare del trattamento - alla generalità degli utenti, direttamente all’interno dell’applicazione, sul presupposto che l’applicazione “Falco” può essere utilizzata anche da cittadini di altri Comuni con cui la FMI ha in essere accordi per l’utilizzo del servizio.

Dagli atti risulta, altresì, che, all’interno dell’applicazione, la FMI, su richiesta del Comune, ha inserito una breve informativa sul trattamento dei dati, in data 28 aprile 2022, che non rimandava, tuttavia, a un testo completo della stessa. Successivamente, in data 3 maggio 2022, è stata inserita nell’applicazione una versione più estesa dell’informativa, che corrisponde a quella pubblicata sul sito web istituzionale del Comune in data 2 maggio 2022.

L’informativa del 22 aprile 2022 non era comunque pienamente conforme ai requisiti previsti dal Regolamento (v. art. 13, par. 2, lett. a). Nella stessa si affermava, infatti, che fino al 31 maggio 2022, ovvero in una fase definita come sperimentale, i tempi di conservazione delle segnalazioni sarebbero stati limitati a ventiquattro ore. Tale circostanza non trova, tuttavia, riscontro nella relazione della FMI (sub all. 9 alla nota prot. 0003022/2023 dell’11 gennaio 2023), in cui, con riguardo alla richiesta dell’Autorità di chiarire le differenze, in termini di funzionalità dell’applicazione, tra le diverse versioni della stessa succedutesi nel tempo, si dà conto soltanto di una prima versione dell’applicazione del periodo dicembre 2021-gennaio 2022 (con tempi di conservazione delle segnalazioni pari a sette giorni) e di una seconda versione della stessa, rilasciata in data 6 aprile 2022, con il medesimo tempo di conservazione pari a sette giorni (con la sola disabilitazione della possibilità per l’utente di anonimizzare la propria segnalazione prima del termine di sette giorni).

Le medesime considerazioni valgono anche per la successiva versione dell’informativa del 2 maggio 2022, ove si afferma che, durante la fase sperimentale dell’applicazione, che terminerà il 31 maggio 2022, “i tempi di conservazione dei dati sono azzerati”, circostanza che non trova riscontro nella predetta relazione della FMI.

Inoltre, in nessuna delle due versioni dell’informativa si dà conto della circostanza che, durante l’utilizzo dell’applicazione, la stessa acquisiva le coordinate geografiche statiche del dispositivo

ogni 3,5 secondi.

Alla luce delle considerazioni che precedono, deve concludersi che il Comune, nel periodo intercorrente tra il mese di dicembre 2021, in cui l'applicazione è stata resa disponibile online, e il 21 aprile 2022, ha omesso di fornire agli interessati una propria informativa sul trattamento dei dati personali, e, successivamente a tale periodo, ha fornito agli utenti informazioni non corrette in merito ad alcuni aspetti essenziali del trattamento, avendo agito in violazione degli artt. 5, par. 1, lett. a), e 13 del Regolamento.

3.4 La mancata definizione dei rapporti con il responsabile del trattamento

Ai sensi dell'art. 28, par. 3, del Regolamento, "i trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del 26 diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento, 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 del trattamento", e che preveda tutti gli impegni previsti dal medesimo art. 28, par. 3, del Regolamento (cfr. cons. 81 del Regolamento).

Il contratto o il diverso atto giuridico devono essere "stipulato in forma scritta, anche in formato elettronico" (art. 28, par. 9, del Regolamento).

Come chiarito dal Comitato europeo per la protezione dei dati, "poiché il regolamento stabilisce con chiarezza l'obbligo di stipulare un contratto scritto, qualora non sia in vigore nessun altro atto giuridico pertinente si ha una violazione del [Regolamento], ovvero dell'"articolo 28, paragrafo 9, del [Regolamento]". Considerato che "sia il titolare sia il responsabile del trattamento hanno la responsabilità di garantire l'esistenza di un contratto o di un altro atto giuridico che disciplini il trattamento", l'autorità di controllo compente "potrà infliggere una sanzione amministrativa pecuniaria sia al titolare sia al responsabile del trattamento" ("Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, par. 103).

Pertanto, laddove, come nel caso di specie, sussista "un rapporto titolare-responsabile del trattamento […] anche in assenza di un [valido] accordo di trattamento per iscritto" - in quanto il soggetto che tratta i dati effettua in concreto il trattamento non per proprie finalità ma per conto del soggetto committente, nell'ambito di un'attività da questi esternalizzata e nell'esecuzione di un contratto di servizi o di altro analogo rapporto giuridico in essere tra le parti (cfr. la definizione di "responsabile del trattamento" di cui all'art. 4, par. 1, n. 8, del Regolamento) - "ciò implic[a] […] una violazione dell'articolo 28, paragrafo 3, del [Regolamento]" (ibidem).

Ciò premesso, si evidenzia che, come emerso nel corso dell'istruttoria, il Comune ha nel tempo affidato alla FMI l'esecuzione di una serie di servizi, ovvero:

> con deliberazione di Giunta Comunale n. 333/2017, le attività di manutenzione e supporto alla gestione dei sistemi automatici di videocontrollo delle infrazioni al Codice della Strada per accessi alla ZTL e quelli di rilevazione del movimento merci;
>
> con deliberazione di Consiglio Comunale n. 111 del 19/12/2018 e con successivo contratto n. 91 del 6/6/2019, alla gestione del sistema di videocontrollo del Comune e connesse alla vigilanza urbana. In tale contratto veniva individuata FMI quale "titolare del trattamento per gli ambiti di propria competenza";
>
> con deliberazione di Giunta Comunale n. 200 del 23/06/2021, la manutenzione degli impianti e delle apparecchiature tecniche dei sistemi di videosorveglianza da realizzarsi nell'ambito del progetto "Città Protetta 2020 – 2° e 3° stralcio", che include anche l'applicazione "Falco".

Sebbene la FMI, nell'ambito della fornitura di una pluralità di servizi in favore del Comune, abbia trattato e tratti dati personali per conto e nell'interesse dello stesso, agendo, pertanto, in qualità di "responsabile del trattamento" (art. 4, par. 1, n. del Regolamento), il Comune ha omesso di stipulare con la stessa un contratto sulla protezione dei dati personali, così come richiesto dall'art. 28 del Regolamento.

A tal riguardo, si osserva che, in data 26 aprile 2022, la stessa FMI aveva chiesto al Comune di "essere inquadrata come responsabile esterno ex art. 28 [del Regolamento], con conseguente necessità di sottoscrivere le apposite nomine" (cfr. la relazione del RPD, all. 5 alla nota prot. n. 0083196/2022). In data 28 aprile 2022, il RPD del Comune e il consulente esterno dello stesso evidenziavano, inoltre, la necessità che "FMI [fosse] inquadrata come responsabile esterno del trattamento" (ibidem). Ed ancora, in data 4 maggio 2022, il RPD inviava "una comunicazione al referente FMI, in risposta alla sua richiesta di invio delle nomine ex art. 28, evidenziando che solo a seguito del recepimento del regolamento di [videosorveglianza] […] e di tutti gli atti conseguenti, in particolare disciplinare e dpia, [il Comune avrebbe] potuto procedere con le nomine". Ciononostante, come dichiarato dal Comune, la formalizzazione dell'accordo è avvenuta soltanto "ad agosto 2022".

Il Comune, in qualità di titolare del trattamento, ha, pertanto, omesso, fino al mese di agosto 2022, di stipulare un accordo sulla protezione dei dati con la FMI, che - in quanto società a completa partecipazione pubblica, affidataria di molteplici servizi da parte del Comune - agiva in concreto in qualità di responsabile del trattamento, in violazione dell'art. 28, par. 3, del Regolamento.

3.5 L'omessa valutazione d'impatto sulla protezione dei dati

In caso di rischi elevati per gli interessati - derivanti, ad esempio, dall'utilizzo di nuove tecnologie - il titolare del trattamento deve effettuare una valutazione d'impatto sulla protezione dei dati, al fine di adottare, in particolare, le misure adeguate ad affrontare tali rischi, consultando preventivamente il Garante, ove ne ricorrano i presupposti (v. artt. 35 e 36 del Regolamento).

Nel caso di specie, l'utilizzo dell'applicazione "Falco" comportava la raccolta di dati sulla posizione geografica degli utenti, nonché implicava la possibilità che, anche in caso di accessi abusivi o non autorizzati, soggetti terzi potessero venire a conoscenza delle segnalazioni effettuate, con possibili conseguenze per gli interessati anche di tipo ritorsivo. Come sopra illustrata, non poteva, peraltro, escludersi la raccolta di dati personali relativi a reati, che per loro natura hanno particolare delicatezza.

Sebbene, dunque, i trattamenti derivanti dall'impiego di tale applicazione, messa a disposizione potenzialmente di tutti i cittadini, presentassero un rischio elevato per i diritti e le libertà delle persone fisiche, il Comune non ha redatto una valutazione d'impatto sulla protezione dei dati prima di iniziare i trattamenti in questione (cfr. le "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679", adottate dal Gruppo di lavoro art. 29 il 4 aprile 2017, WP 248 rev.01, fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018, con particolare riguardo ai criteri dei dati aventi carattere altamente personale, come quelli relativi all'ubicazione o il cui trattamento può comportare gravi ripercussioni sulla vita quotidiana dell'interessato, nonché del trattamento di dati su larga scala).

Il Comune ha, pertanto, agito in violazione dell'art. 35, par. 1, del Regolamento.

3.6 La sicurezza del trattamento

L'art. 5, par. 1, lett. f), del Regolamento stabilisce che i dati personali devono 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 o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (principio di "integrità e riservatezza").

In applicazione di tale principio, l'art. 32 del Regolamento, concernente la sicurezza del trattamento, prevede 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 […]" (par. 1) 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 distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" (par. 2) (cfr. cons. 83 del Regolamento).

All'esito dell'attività istruttoria è merso che gli operatori della Polizia locale del Comune, "in assenza di credenziali personali per la consultazione delle segnalazioni effettuate dagli utenti, in carenza di specifica disposizione di servizio del Vice Comandante […]", accedevano ai dati raccolti mediante l'applicazione Falco "utilizzando la password generica fornita da FMI", non disponendo, pertanto, di specifiche e personali credenziali di autenticazione per accedere al sistema informatico (v. nota della Polizia locale del Comune del 13 luglio 2022, in atti).

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, che comportava l'acquisizione e la gestione delle segnalazioni effettuate dagli utenti, con raccolta di dati personali, relativi al segnalante, come il numero di telefono e la posizione del dispositivo, si ritiene che le predette modalità di accesso al sistema informatico non possa considerarsi adeguate sotto il profilo della sicurezza (cfr. provv. 10 giugno 2021, n. 236, doc. web n. 9685947).

L'utilizzo di utenze non nominali, da parte di più soggetti, impedisce, infatti, di attribuire le azioni compiute in un sistema informatico a un determinato soggetto, con pregiudizio, anche per il titolare e il responsabile del trattamento, che sono di fatto privati della possibilità di controllare l'operato dei soggetti che agiscono sotto la propria autorità.

Inoltre, allorquando un'utenza non nominale, come quella in questione, venga utilizzata da più soggetti, possono determinarsi situazioni in cui non c'è coerenza tra i profili di autorizzazione attribuiti e le effettive esigenze di operatività per la gestione dei sistemi, rendendo così possibile, a un soggetto non autorizzato, di operare, in assenza di una specifica volontà del titolare o del responsabile del trattamento, nell'ambito dei sistemi e servizi di trattamento (v. provv. 4 aprile 2019, n. 83, doc. web n. 9101974; 14 gennaio 2021, n. 4, doc. web n. 9582744).

Peraltro, l'utilizzo di "credenziali di autenticazione in uso esclusivo dei soggetti che operano sotto la sua autorità o quella del responsabile del trattamento" nel regime normativo previgente era espressamente prevista quale misura minima di sicurezza alla cui adozione erano tenuti tutti i titolari di trattamento (ai sensi del disciplinare tecnico di cui all'allegato B al Codice, nel testo anteriore alle modifiche di cui al d.lgs. n. 101/2018), la cui violazione comportava anche l'applicazione di una sanzione penale (cfr. art. 169 del Codice, nel testo anteriore alle modifiche di cui al d.lgs. n. 101/2018).

Per tali ragioni, alla luce delle modalità di accesso al sistema informatico di gestione delle segnalazioni, con le caratteristiche sopra descritte, il Comune ha agito in maniera non conforme al principio di "integrità e riservatezza" e in violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria 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.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dal Comune, per aver trattato dati personali in violazione degli artt. 5, par. 1, lett. a) e f), e par. 2 (in combinato disposto con l'art. 24), 12, par. 1, 13, 25, 28, par. 3, 32 e 35, par. 1, del Regolamento.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento.

5. 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 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).

Nel caso di specie, il Comune ha posto in essere due distinte condotte, che devono essere considerate separatamente ai fini della quantificazione della sanzione amministrativa da applicarsi.

5.1 Le violazioni relative ai trattamenti di dati personali mediante dispositivi video.

Tenuto conto che le violazioni degli artt. 5, par. 2 (in combinato disposto con l'art. 24), 25 e 28, par. 3, del Regolamento, in relazione ai trattamenti posti in essere mediante dispositivi video, hanno avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, la violazione più grave riguarda l'art. 5, par. 2, del Regolamento (in combinato disposto con l'art. 24), soggetta alla sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

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.

Tenuto conto che:

- la violazione riguarda i trattamenti posti in essere, per un esteso arco temporale, mediante dispositivi video (telecamere di videosorveglianza e di controllo delle aree di accesso a ZTL), che possono riguardare un numero molto elevato di cittadini e altri interessati che transitano nel territorio comunale; dall'istruttoria non è, tuttavia, emerso che gli stessi abbiano subito specifici danni in conseguenza di tali trattamenti (cfr. art. 83, par. 2, lett. a), del

Regolamento);

sebbene il Comune non avesse stipulato un accordo sulla protezione dei dati con la FMI, quest'ultima è una società unipersonale a responsabilità limitata a completa partecipazione pubblica, la cui proprietà è comunque riconducibile ai Comuni appartenenti all'Unione dei Comuni della Romagna forlivese, tra cui il Comune di Forlì; inoltre, le parti avevano comunque sottoscritto un contratto di servizi, essendo stati quantomeno in via generale definiti 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 (cfr. art. 83, par. 2, lett. a), del Regolamento);

la violazione ha natura colposa (cfr. art. 83, par. 2, lett. b), del Regolamento);

il trattamento non ha riguardato dati personali appartenenti a categorie particolari (v. art. 9 del Regolamento), dovendosi, tuttavia, considerare che i sistemi di videosorveglianza, installati sulla pubblica via per la tutela della sicurezza urbana, possono comportare il trattamento di dati personali relativi a reati di cui all'art. 10 del Regolamento (cfr. art. 83, par. 2, lett. g), del Regolamento),

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia medio (cfr. Comitato europeo per la protezione dei dati, "Guidelines 04/2022 on the calculation of administrative fines under the GDPR" del 23 maggio 2023, punto 60).

Ciò premesso, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze attenuanti:

il Comune ha un alto grado di responsabilità, avendo sostanzialmente omesso di considerare i profili di protezione dei dati sottesi al trattamento in questione, prima di porre in essere lo stesso e fin dalla progettazione dei sistemi utilizzati (art. 83, par. 2, lett. d), del Regolamento);

il Comune ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria, essendosi, altresì, prontamente attivato per rimediare alle violazioni, anche ricorrendo al supporto del RPD e di consulenti esperti in materia di protezione dei dati (art. 83, par. 2, lett. f), del Regolamento);

non risultano precedenti violazioni pertinenti commesse dal Comune (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 10.000 (diecimila) per la violazione degli artt. 5, par. 2 (in combinato disposto con l'art. 24), 25 e 28, par. 3 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto che l'attività di videosorveglianza in questione ha interessato luoghi pubblici, concretizzando un trattamento di dati personali che "consente [di rilevare] la presenza e il comportamento delle persone nello spazio considerato" (Comitato europeo per la protezione dei dati, "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video" del 29 gennaio 2020, par. 2.1), senza che sia stato garantito, sin dalla progettazione del sistema di videosorveglianza, il complessivo rispetto dei principi di protezione dei dati, si ritiene altresì 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 del Regolamento del Garante n. 1/2019.

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

5.2 Le violazioni relative al sistema "Falco".

Tenuto conto che la violazione degli artt. 5, par. 1, lett. a) e f), e par. 2 (in combinato disposto con l'art. 24), 12, par. 1, 13, 25, 28, par. 3, 32 e 35, par. 1, del Regolamento, in relazione ai trattamenti posi in essere mediante il c.d. sistema "Falco", hanno avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni più gravi riguardano gli artt. 5, 12 e 13, soggette alla sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

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.

Tenuto conto che:

- il trattamento ha riguardato un numero limitato di interessati rispetto al numero totale di residenti nel Comune (circa 116.726), atteso che, come dichiarato dal Comune nel corso dell'istruttoria, le segnalazioni ricevute dal momento della prima attivazione in via sperimentale (aprile 2022), comprensive delle numerose prove di test e funzionalità effettuate da FMI in fase di verifica delle varie versioni dell'applicativo, sono n. 568, mentre dalla data della riattivazione (8 giugno 2022) sono state ricevute n. 86 segnalazioni, per un totale complessivo di n. 654 segnalazioni, incluse quelle di solo test (cfr. art. 83, par. 2, lett. a), del Regolamento);

- sebbene il Comune non avesse stipulato un accordo sulla protezione dei dati con lla FMI, quest'ultima è una società unipersonale a responsabilità limitata a completa partecipazione pubblica, la cui proprietà è comunque riconducibile ai Comuni appartenenti all'Unione dei Comuni della Romagna forlivese, tra cui il Comune di Forlì; inoltre, le parti avevano comunque sottoscritto un contratto di servizi, essendo stati quantomeno in via generale definiti 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 (cfr. art. 83, par. 2, lett. a), del Regolamento);

- la violazione ha carattere colposo (cfr. art. 83, par. 2, lett. b), del Regolamento);

- il trattamento non ha riguardato dati personali appartenenti a categorie particolari (v. art. 9 del Regolamento), dovendosi, tuttavia, considerare che, come sopra illustrato, non poteva del tutto escludersi, per effetto delle segnalazioni presentate dai cittadini, il trattamento di dati personali relativi a reati di cui all'art. 10 del Regolamento (cfr. art. 83, par. 2, lett. g), del Regolamento),

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia medio (cfr. Comitato europeo per la protezione dei dati, "Guidelines 04/2022 on the calculation of administrative fines under the GDPR" del 23 maggio 2023, punto 60).

Ciò premesso, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze attenuanti:

- il Comune ha un alto grado di responsabilità, avendo sostanzialmente omesso di considerare i profili di protezione dei dati sottesi al trattamento in questione, prima di porre in

essere lo stesso e fin dalla progettazione dei sistemi utilizzati, avendo, peraltro, agito, a partire dalla riattivazione dell'applicazione, nel mese di giugno 2022, in maniera contraria agli orientamenti espressi dal RPD (art. 83, par. 2, lett. d), del Regolamento);

il Comune ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria, essendosi, altresì, prontamente attivato per rimediare alle violazioni, anche ricorrendo al supporto del RPD e di consulenti esperti in materia di protezione dei dati (art. 83, par. 2, lett. f), del Regolamento);

non risultano precedenti violazioni pertinenti commesse dal Comune (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 5.000 (cinquemila) per la violazione degli artt. 5, par. 1, lett. a) e f), e par. 2 (in combinato disposto con l'art. 24), 12, par. 1, 13, 28, par. 3, 25, 32 e 35, par. 1, del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto che il trattamento dei dati personali in questione ha avuto luogo in violazione delle predette disposizioni del Regolamento per un esteso arco temporale, si ritiene, altresì, 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 del Regolamento del Garante n. 1/2019.

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

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dal Comune di Forlì per la violazione degli artt. 5, par. 1, lett. a) e f), e par. 2 (in combinato disposto con l'art. 24), 12, par. 1, 13, 25, 28, par. 3, 32 e 35, par. 1, del Regolamento, nei termini di cui in motivazione;

ORDINA

al Comune di Forlì, in persona del legale rappresentante pro-tempore, con sede legale in Piazza Saffi, 8 - 47121 Forlì (FC), C.F. 00606620409, di pagare la complessiva somma di euro 15.000 (quindicimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate 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

al predetto Comune in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 15.000 (quindicimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione del presente provvedimento sul sito web del Garante, ritenendo che ricorrano i presupposti di cui all'art. 17 del Regolamento del Garante n. 1/2019.

Ai sensi degli artt. 78 del Regolamento, 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, 20 giugno 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei