GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento dell´11 gennaio 2024 [9977020]

VEDI ANCHE Comunicato del 25 gennaio 2024

[doc. web n. 9977020]

Provvedimento dell'11 gennaio 2024

Registro dei provvedimenti
n. 5 dell'11 gennaio 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.

Da notizie di stampa si è appreso che presso il Comune di Trento (di seguito, il "Comune") formerebbero oggetto di sperimentazione, con il supporto della Fondazione Bruno Kessler (di seguito, la "Fondazione" o "FBK"), tre sistemi di intelligenza artificiale, denominati "Marvel", "Protector" e "Precrisis", i cui progetti di sviluppo sarebbero stati finanziati nell'ambito di programmi di ricerca dell'Unione europea, che implicherebbero la raccolta di informazioni in luoghi pubblici attraverso microfoni e telecamere di videosorveglianza, al fine di rilevare potenziali situazioni di pericolo per la pubblica sicurezza.

2. L'attività istruttoria.

Con nota del XX, l'Autorità ha rivolto al Comune una richiesta d'informazioni, ai sensi dell'art. 157 del Codice, in relazione ai trattamenti di dati personali posti in essere nell'ambito dei predetti progetti.

In riscontro a tale richiesta d'informazioni, il Comune, con nota prot. n. XX del XX, ha dichiarato, in particolare, che:

"il Comune […] è partner di tre progetti di sviluppo denominati MARVEL, PROTECTOR e PRECRISIS, finanziati nell'ambito di programmi di ricerca dell'Unione europea";

"[…] grazie all'impiego di appositi algoritmi di intelligenza artificiale sviluppati da[lla] Fondazione […], i dati personali registrati tramite le sorgenti audio e video […] sono automaticamente anonimizzati al momento della raccolta";

"il Comune […] ha effettuato, con il supporto del Responsabile per la protezione dei dati personali ["RPD"], specifica valutazione di impatto [sulla protezione dei dati] […]";

"[…]non vengono utilizzati dati biometrici, in particolare tecnologie atte a effettuare un riconoscimento facciale […]";

"[…] i sistemi […] sono sviluppati nell'ambito di progetti di ricerca […] [ai quali] il Comune […] partecipa e ha partecipato […] in qualità di caso d'uso, mettendo a disposizione la propria infrastruttura […]".

Con specifico riguardo al progetto "Marvel", il Comune ha dichiarato, in particolare, che:

"nell'ambito del progetto europeo MARVEL - Multimodal Extreme Scale Data Analytics for Smart Cities Environments (Grant Agreement - GA n. 957337 - MARVEL dd. 22/07/2020 e successivi emendamenti), coordinato da FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH) - EL, la Fondazione […] è il partner che fornisce parte dell'infrastruttura hardware per il processing dei dati e le tecnologie di anonimizzazione audio/video […]. La data di fine progetto è prevista per il 31/12/2023";

"MARVEL è un progetto che vuole sviluppare un framework di calcolo distribuito, composto di risorse di calcolo all'"edge" e di risorse in "cloud", con l'obiettivo di consentire la percezione e l'intelligenza multimodali per il riconoscimento di scene audiovisive, il rilevamento di eventi e la cosiddetta smart urban security. Tramite la raccolta e l'analisi di dati da streaming audiovisivi multimodali, il progetto intende migliorare la qualità della vita e dei servizi ai cittadini all'interno del paradigma della città intelligente, senza violare i limiti etici e di privacy, in modo responsabile per l'intelligenza artificiale ([…] "AI"). Ciò si ottiene attraverso la combinazione e l'analisi in tempo reale di dati audiovisivi multimodali distribuiti su larga scala e il supporto al processo decisionale automatizzato a tutti i livelli framework di calcolo distribuito";

"per quel che riguarda l'infrastruttura, la Fondazione […] - su indicazione del Comune […] - mette a disposizione due workstations presso i propri laboratori. La prima workstation accede alle telecamere del Comune […] attraverso una VPN (Virtual Private Network - Rete Virtuale Privata). La seconda workstation si collega tramite VPN alla piattaforma di calcolo del progetto (realizzata come "cluster" di nodi di calcolo distribuiti fra i partner di progetto), per mettere a disposizione i flussi video anonimizzati";

"in aggiunta, la Fondazione […] ha progettato e assemblato sei dispositivi per la registrazione dei segnali audio tramite microfoni […]. Tali dispositivi sono stati installati a febbraio 2023 nella rete del Comune […] e sono accessibili dalla Fondazione […] tramite la suddetta VPN. I flussi audio sono gestiti con le stesse modalità dei flussi video";

"nell'ambito del progetto […] MARVEL, la Fondazione […] si occupa dell'acquisizione di dati audio e video. I dati video vengono forniti da 14 telecamere IP di sorveglianza del Comune […], 6 delle quali vengono utilizzate per la realizzazione del prototipo del progetto. La Fondazione […] ha accesso ai flussi video in tempo reale non operativo via VPN per mezzo di credenziali, al fine di accedere in modo sicuro […]. I dati video vengono immediatamente anonimizzati […] sulla workstation della Fondazione […] che accede al flusso video";

"i segnali audio vengono acquisiti da un dispositivo realizzato e installato nell'ambito delle attività di progetto: si tratta di un [c.d. "single board computer"] a cui sono collegati 2 microfoni MEMS. Il dispositivo legge i segnali audio dai microfoni MEMS, li anonimizza e li rende disponibili, solo anonimizzati, tramite un server RTSP. Questa soluzione permette di implementare una componente privacy-by-design, anonimizzando i segnali audio direttamente sul dispositivo […]. Le modalità di accesso ai dati audio anonimizzati sono analoghe a quelle dei dati video";

"i flussi audio e video anonimizzati vengono inoltrati, per il tramite della seconda workstation di cui sopra, alla piattaforma di calcolo del progetto, rendendo i flussi anonimizzati disponibili agli altri partner del progetto";

"su richiesta del Coordinatore e in accordo con il Comune […], la Fondazione […] periodicamente carica i dati audio e video anonimizzati nel data corpus del progetto MARVEL (repository, ospitato nella server farm di uno dei partner di progetto, in cui vengono messi a disposizione i dati per lo sviluppo degli algoritmi di analisi audio-video)".

Con specifico riguardo al progetto "Protector", il Comune ha dichiarato, in particolare, che:

"nell'ambito del progetto europeo PROTECTOR - PROTECTing places of wORship (Grant Agreement - GA n. 101034216 - PROTECTOR | ISFP-2020-AG-PROTECT, dd. 28/02/2021 e successivi emendamenti), coordinato da SAHER (EUROPE) OU - EE, la Fondazione […] è Technical Coordinator e Work Package (WP) Leader ed, in particolare, responsabile dello sviluppo della piattaforma software denominata PROTECTOR Platform. Il progetto è durato 25 mesi, dal 01/04/2021 al 30/04/2023";

"PROTECTOR è un progetto che ha avuto lo scopo di migliorare la protezione dei luoghi di culto a livello urbano attraverso l'analisi dei crimini d'odio e delle minacce terroristiche, nonché la valutazione delle misure di sicurezza e delle risposte date dalle forze dell'ordine in tali contesti. Il progetto ha elaborato una strategia di sicurezza specifica per i luoghi di culto. Inoltre, sono state sviluppate e testate nuove componenti tecnologiche […] secondo i principi della cosiddetta ethics/privacy-by-design, in selezionati luoghi di culto in Belgio (Anversa), Bulgaria (Sofia) e Italia (Trento), al fine di migliorare le capacità di analisi delle forze dell'ordine";

"[…] la piattaforma PROTECTOR si configura come una soluzione che acquisisce dati provenienti da telecamere di videosorveglianza e dati testuali derivati dai social media, li elabora e visualizza informazioni rilevanti per le forze dell'ordine, al fine di identificare rischi e minacce per la sicurezza dei luoghi di culto";

"la piattaforma si compone di vari moduli software, con diverse funzionalità. L'analisi automatica dei dati visuali e testuali viene effettuata attraverso moduli software basati su tecnologie di AI. Relativamente ai moduli per l'analisi di dati visuali si hanno:

componente di rilevamento automatico degli oggetti: modulo basato su tecnologie di object detection ([…]) per il rilevamento e la classificazione di oggetti di interesse (ad esempio: automobili, pedoni, biciclette). Si rileva solo la categoria degli oggetti sulla scena e non la loro specifica identità[;]

componente di tracciamento dei movimenti degli oggetti: modulo per il rilevamento delle traiettorie degli oggetti di interesse (o visual tracking), identificati grazie al modulo descritto in precedenza. Il modulo è basato sul codice open source […], pubblicamente disponibile[;]

componente di rilevamento delle anomalie: modulo per il rilevamento di situazioni anomale in ambito urbano e per la loro categorizzazione (ad esempio: situazioni di criminalità o devianza). Tale componente di rilevamento delle anomalie utilizza librerie pubblicamente disponibili come il modello di visione-linguaggio CLIP e metodologie per il clustering delle traiettorie per identificare anomalie nei movimenti. I moduli di AI sopra descritti per l'analisi dei dati video utilizzano dataset pubblicamente disponibili in letteratura per addestrare i modelli di deep learning, mentre il raffinamento e la valutazione sono effettuati utilizzando i dati acquisiti dalla piattaforma PROTECTOR in forma anonimizzata […]";

"relativamente ai moduli per l'analisi di dati su social networks si hanno:

componente di rilevamento automatico di messaggi d'odio religioso da Twitter e dai commenti di YouTube. L'obiettivo è monitorare eventuali escalation d'odio (in prevalenza di tipo religioso o connesso ad esso) e, pertanto, non vengono acquisite informazioni relative ai profili degli utenti, ma solo informazioni relative al contenuto testuale dei post[;]

componente di analisi delle emozioni rilevate nei post da Twitter e nei commenti di YouTube a tema religioso. Anche in questo caso, l'obiettivo è svolgere un monitoraggio su dati aggregati per comprendere se il discorso online viene caratterizzato da picchi imprevisti di aggressività, rabbia o altre emozioni negative sul tema della religione[;]

componente di rilevamento di disinformazione legata a fake news religiose, finalizzato a monitorare la presenza di disinformazione a tema religioso su Twitter. Per identificare con metodi automatici i messaggi di odio online a tema religioso, vengono utilizzati sia set di dati generici che dati raccolti appositamente per PROTECTOR, tra cui commenti pubblicati su Twitter e YouTube. Tali commenti vengono anonimizzati rimuovendo i nomi degli utenti e sostituendo utenti e url presenti nel testo dei post con USER e URL. Le componenti di analisi per i social media impiegano modelli di linguaggio basati su Transformer: approcci basati su dizionari e ricerche semantiche per rilevare discorsi di odio, emozioni, localizzazioni geografiche e informazioni errate legate a tematiche religiose nei post dei social media sopra-citati";

"nell'ambito del progetto ["Protector"] […], la Fondazione […] si occupa di sviluppare tecnologie di AI per l'analisi di scene di video sorveglianza unicamente a partire da dati visuali, non è invece previsto il processamento di alcun segnale audio";

"[…] per le 11 telecamere IP di sorveglianza statiche del Comune […] coinvolte nel progetto, la Fondazione […] [effettua] l'accesso alla rete interna del Comune […] e al flusso video in tempo reale non operativo per mezzo di specifiche credenziali […]. Una volta stabilita la connessione, la Fondazione […] ha acquisito un flusso video non operativo da ciascuna telecamera coinvolta nel progetto, raggiungendo il suo indirizzo IP";

"i dati video vengono immediatamente anonimizzati effettuando in maniera automatica la sfocatura dei volti e delle targhe dei veicoli, in tal modo rimuovendo gli identificatori personali e garantendo che le persone non possano essere identificate […]. I dati video acquisiti transitano sui sistemi della Fondazione […] per il tempo strettamente necessario all'anonimizzazione e, successivamente, cancellati in modo definitivo";

"i dati anonimizzati relativi alle immagini delle videocamere del Comune […] vengono salvati nei server della Fondazione […] per essere processati dagli algoritmi di AI […]; sono inoltre accessibili attraverso la piattaforma PROTECTOR esclusivamente ai membri del Consorzio e alla Commissione Europea; non è, pertanto, prevista la loro circolazione all'esterno del progetto stesso";

Con specifico riguardo al progetto "Precrisis", il Comune ha dichiarato che "[per] PRECRISIS - PRotECting public spaces thRough Integrated Smarter Innovative Security (Grant Agreement - GA n. 101100539 - PRECRISIS | ISF-2022-TF1-AG-PROTECT dd. 17/02/2023), la Fondazione […] è Technical Coordinator e Work package Leader. Il progetto è ufficialmente iniziato in data 01/05/2023 e ha una durata prevista di 24 mesi. Lo stesso risulta attualmente in fase di attivazione e non è stata sviluppata ancora alcuna componente software basata su AI […;] prima della concreta attivazione di tale progetto, saranno adottate tutte le misure per rendere il trattamento dei dati personali necessari conformi al [Regolamento]".

Il Comune ha poi, più in generale, dichiarato che:

"il trattamento è effettuato esclusivamente per finalità connesse allo sviluppo dei progetti […]";

"la base giuridica per la normale attività di videosorveglianza posta in essere dal Comune, tramite il Corpo di polizia locale, è rinvenibile […] [nell'] art. 6, comma 1, lettera e, [del Regolamento]), ai sensi in particolare di quanto previsto dal [d.l.] n. 11/2009, convertito in [l.] n. 38/2009, il quale attribuisce ai Comuni specifici compiti in materia di sicurezza urbana stabilendo, all'art. 6, comma 7, che "per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico"";

"il trattamento di videosorveglianza è altresì riconducibile alle disposizioni della Direttiva 2016/680 e del decreto legislativo n. 51/2018, così come la normativa specifica riferibile al Corpo di polizia locale e/o al decreto c.d. "Minniti" [ovvero il d.l. 20 febbraio 2017, n. 14]";

"[…] le disposizioni della Direttiva 2016/680 e del decreto legislativo n. 51/2018 diverranno eventualmente applicabili nel momento in cui si concluderà la fase sperimentale e le funzionalità sviluppate tramite i progetti di ricerca saranno rese fruibili nell'utilizzo da parte del Corpo di polizia locale degli impianti di videosorveglianza di proprietà comunale. Allo stato attuale, infatti, tali funzionalità, essendo ancora in fase di sviluppo, non sono state rese disponibili nell'utilizzo di detti impianti; pertanto, la citata base giuridica non è pertinente";

"[…] la funzione generale di interesse pubblico o connesso all'esercizio di pubblici poteri […] è riconducibile anche nell'art. 2 del Codice enti locali (legge regionale 3 maggio 2018, n. 2 e s.m.), ove tra le funzioni amministrative di interesse locale attribuite ai comuni sono annoverabili lo sviluppo culturale, sociale ed economico della popolazione, tra cui rientra – in termini generali - lo sviluppo del progetto "Trento Smart city", in cui rientrano anche i progetti oggetto d'esame";

"trattandosi di progetti di ricerca, sono inoltre state ritenute pertinenti le disposizioni dell'Allegato A.5 del [Codice] contenente le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, in conformità all'art. 89 del [Regolamento]";

"[…] si ritengono infine rilevanti gli accordi convenzionali sottoscritti da Comune […] e Fondazione […] ai fini della partecipazione ai progetti (Grant Agreement e Consortium Agreement di progetto)";

per quanto concerne "la data a partire dalla quale i trattamenti di dati personali realizzati mediante ciascuno dei richiamati sistemi sono stati effettuati è identificabile: per ciò che concerne i video, febbraio 2022; per ciò che concerne gli audio, marzo 2023";

"[…] allo stato attuale i progetti sono ancora in fase sperimentale, in quanto non è ancora stato completato lo sviluppo degli algoritmi di intelligenza artificiale che dovrebbero implementare le funzionalità degli impianti di videosorveglianza mediante l'identificazione e la segnalazione di eventi potenzialmente pericolosi. Si precisa peraltro che, a decorrere dalla data [sopra] indicata […], la raccolta dei flussi audio e video necessari per lo sviluppo degli algoritmi non avviene unicamente in ambienti controllati e con il coinvolgimento di persone che hanno prestato il proprio consenso alla partecipazione al progetto, ma anche in ambiente urbano, ossia tramite le telecamere ed i microfoni installati in alcune piazze e vie della città";

"[…] le aree della città in cui collocare le telecamere e i microfoni sono state selezionate in quanto ritenute […], particolarmente rilevanti in relazione al potenziale verificarsi di eventi significativi ai fini della raccolta di campioni utili all'allenamento/addestramento degli algoritmi";

"[…] la Fondazione […] è partner tecnologico del Comune […] nello sviluppo dei tre progetti di ricerca […] [e la stessa è] stata individuata come l'unico soggetto esterno al Comune […] incaricato di effettuare, mediante la gestione dei flussi audio e video prodotti dai microfoni e dalle telecamere, il trattamento di dati personali finalizzato allo sviluppo degli algoritmi di intelligenza artificiale. Sulla base di tale impostazione, il Comune […] ha proceduto a formalizzare con decreto sindacale la nomina della Fondazione […] quale responsabile del trattamento ai sensi dell'art. 28 del Regolamento […]";

"non si è proceduto alla nomina a responsabili del trattamento degli altri partner progettuali, in quanto è previsto che l'eventuale comunicazione ad essi dei dati utilizzati nell'ambito dei progetti avvenga esclusivamente in forma anonima";

"[…] i dispositivi video (telecamere) precedentemente già presenti e in funzione sul territorio comunale ed attualmente impiegati per lo sviluppo dei progetti consentono unicamente riprese video e pertanto non acquisiscono né acquisivano in passato dati audio";

"i dispositivi audio (microfoni) attualmente impiegati per lo sviluppo dei progetti, per contro, non erano precedentemente già presenti e in funzione sul territorio comunale e sono stati installati nel corso del corrente anno […] a decorrere dalla data sopra indicata";

"i dati analizzati sono anonimizzati alla fonte […], in prossimità dei dispositivi utilizzati per raccogliere tali informazioni, non sono condivisi con terze parti e nemmeno utili per la profilazione dei cittadini. Le situazioni vengono controllate analizzando le informazioni multimediali in tempo reale, utilizzando algoritmi di machine learning. Più semplicemente, attraverso software e algoritmi dedicati all'individuazione di anomalie, che operano confrontando l'audio e il video ricevuti, con un insieme di test audio e video, precedentemente simulati per istruire la macchina a riconoscere situazioni di pericolo.

Una volta riconosciuta l'anomalia, il sistema in corso di sviluppo, potrebbe – in potenza – essere utilizzato per allertare le autorità locali, segnalando il tipo di evento per intervenire più rapidamente e in modo più efficace a supporto della cittadinanza. Rimarrebbe in carico all'operatore della Polizia Locale, che monitora le immagini provenienti dalle telecamere, stabilire se sia necessario intervenire o meno, non è il sistema a determinare quali azioni debbano essere messe in atto per rispondere alle situazioni di potenziali minacce. Il sistema MARVEL non è in grado di analizzare o comprendere le conversazioni, ma solo di associare audio e video a situazioni considerate pericolose";

"ai sensi degli artt. 13 e 14 del Regolamento […], si è provveduto a rendere agli interessati le informazioni relative ai trattamenti effettuati per lo sviluppo dei progetti con le seguenti modalità: collocazione di appositi cartelli con l'informativa semplificata in corrispondenza dei luoghi in cui sono posizionati i microfoni e le telecamere; pubblicazione sul sito web comunale di informativa dettagliata sul trattamento dei dati personali acquisiti. A fini di ulteriore trasparenza, si è inoltre provveduto a informare la cittadinanza sullo sviluppo dei progetti e sulle relative caratteristiche e implicazioni nel corso di apposita conferenza stampa svoltasi in data 8 maggio 2023, alla quale ha fatto seguito la pubblicazione sul sito web comunale di specifico comunicato stampa";

"nell'ambito del progetto […] MARVEL, i segnali audio vengono anonimizzati direttamente alla fonte. I microfoni sono collegati ad [un c.d. "single board computer"] che rileva i segmenti contenenti parlato e modifica le caratteristiche della voce in modo da rendere il parlatore non più riconoscibile, per poi mettere i segnali anonimizzati a disposizione per l'ulteriore elaborazione. […] La rimozione delle caratteristiche della voce utilizza [una specifica] libreria […]";

"nell'ambito dei progetti europei MARVEL e PROTECTOR, i video grezzi vengono anonimizzati per rimuovere le informazioni e/o caratteristiche personali identificabili, inclusi i volti delle persone e le targhe dei veicoli. L'anonimizzazione viene ottenuta rilevando, innanzitutto, i volti e le targhe su ciascun frame video e applicando, successivamente, una sfocatura gaussiana alle regioni rilevate. Per rilevare volti e targhe, viene utilizzato il rilevatore di oggetti generico […], pre-addestrato su [un] dataset pubblicamente disponibile […]. Il rilevatore di volti è stato affinato ulteriormente utilizzando il benchmark […], un dataset pubblicamente disponibile. Il rilevatore di targhe è stato ulteriormente addestrato utilizzando video annotati acquisiti nell'ambito del progetto MARVEL".

In riscontro a un'ulteriore richiesta d'informazioni dell'Autorità (nota prot. n. XX del XX), il Comune, con nota prot. n. XX del XX, ha dichiarato, in particolare, che:

le attività oggetto dell'istruttoria "rientrano nell'ambito di progetti europei - MARVEL, PROTECTOR e PRECRISIS - i cui obiettivi e le cui modalità di svolgimento sono oggetto di specifici "Agreements" sottoscritti per ciascun progetto tra la Commissione Europea, il Coordinatore e i Partner di progetto beneficiari dei finanziamenti";

"il progetto PROTECTOR si è già concluso, il progetto MARVEL si concluderà alla fine dell'anno corrente, mentre il progetto PRECRISIS ha avuto inizio a maggio 2023 e da programma si concluderà ad aprile 2025 […]. Ad oggi, nessuna attività di trattamento di dati personali è stata intrapresa da parte del Comune […] (né da parte della Fondazione […]) relativamente a quest'ultimo progetto, essendo lo stesso ancora in fase di programmazione e analisi di contesto";

"per quanto attiene […] alla partecipazione del Comune […] ai progetti, la base giuridica del trattamento è individuata nelle disposizioni di legge e statutarie (art. 2 legge regionale n. 2/2018, artt. 3 e 7 Statuto del Comune […]) che annoverano tra le funzioni amministrative di interesse locale attribuite ai comuni lo sviluppo culturale, sociale ed economico della popolazione, al quale è certamente riconducibile lo sviluppo del programma "Trento Smart city" (quale progetto strategico del Comune), in cui rientrano i [predetti tre] progetti […]";

"peraltro, anche ai sensi del novellato art. 2 ter comma 1 bis del [Codice], i trattamenti di dati personali effettuati per, e nell'ambito di, tali progetti sono stati considerati necessari per l'esercizio di tali funzioni e il perseguimento delle finalità degli stessi";

"le disposizioni dell'Allegato A.5 del [Codice] contenente le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica sono state richiamate, per attinenza, nel documento "Rispetto dei requisiti etici stabiliti per la partecipazione di persone a progetti europei – MARVEL (Grant Agreement n. 957337) e PROTECTOR (Grant Agreement n. 101034216)" che descrive le misure programmate/adottate sia dal Comune […], sia dalla Fondazione […] per disciplinare il trattamento dei dati personali effettuato nell'ambito dei suddetti progetti, non volendosi in tal modo intendere che sia una base giuridica propria del Comune […]. [La] Fondazione […] partecipa alle attività dei progetti nella sua qualità di ente di ricerca di interesse pubblico senza fini di lucro […] la cui finalità principale consiste nel promuovere, svolgere e sviluppare attività di ricerca scientifica e nel diffondere e valorizzare i risultati della medesima sia nella prospettiva dell'avanzamento della conoscenza, sia del servizio alla comunità locale (artt. 1 e 2 dello Statuto della Fondazione)";

"il personale di ricerca della Fondazione […] uniforma la propria attività di ricerca e studio - anche per i [predetti tre] progetti […] ai principi e alle regole deontologiche […], principi e regole che sono allegate al Codice di Comportamento della stessa Fondazione";

"si conferma che l'anonimizzazione dei dati audio consiste nella sostituzione della voce del parlante, mantenendo quanto più inalterate possibile le caratteristiche del segnale audio, incluso il contenuto semantico del parlato. Questo approccio, rispetto ad una eliminazione integrale delle conversazioni dal segnale audio, risponde all'obiettivo esplicitamente previsto nel Grant Agreement sottoscritto con la Commissione Europea (descrizione del Task 3.1 del Work Package 3, pag. 20-21

dell'Annex 1 (part A) del Grant Agreement) di sviluppare tecniche di anonimizzazione poco intrusive che preservino il contesto acustico e permettano una efficace elaborazione dei segnali senza perdita di informazioni";

"il rischio connesso a questo approccio è stato valutato nel contesto delle attività di screening etico richieste dalla Commissione Europea per il progetto MARVEL e svolte dal Coordinatore - Foundation for Research and Technology Hellas (FORTH - EL) e dai partners responsabili degli aspetti legali, etici, di data protection e di IA - Privanova Sas (FR) e Univerzitet u Novom Sadu Fakultet Tehnickih Nauka (UNS - RS) […] Il rischio è stato classificato come basso nel Deliverable D9.5. Tale deliverable sarà presto oggetto di aggiornamento - da parte del Coordinatore e dei partner sopra menzionati - nel D2.6 e la cui sottomissione è prevista nel mese di dicembre 2023";

"nell'ambito del progetto MARVEL, è importante distinguere due diversi utilizzi delle tracce audio (e video), corrispondenti a due diverse finalità del progetto: il prototipo/dimostratore e il data corpus.

> Il prototipo/dimostratore di progetto, accessibile esclusivamente ai Partner del progetto MARVEL, non è in funzione in modo continuo, ma viene attivato per periodi temporali limitati legati alle specifiche attività di progetto (ricerca, sviluppo, benchmarking, valutazione, ecc.). Il prototipo/dimostratore, oltre a permettere ai Partner di analizzare in tempo reale i segnali audio (e video) anonimizzati, effettua copie temporanee di brevi segmenti audio (e video) anonimizzati associati agli eventi rilevanti, in modo da permetterne la visualizzazione nel cruscotto destinato agli utenti (personale dei Partner di progetto);
>
> il data corpus prevede l'archiviazione delle tracce audio (e video) anonimizzate in uno spazio di archiviazione raggiungibile dai Partner che hanno accesso alla piattaforma del progetto. I dati vengono archiviati con metadati relativi a ora, data e luogo della registrazione. Questi dati permettono analisi "ex-post". Anche in questo caso non si tratta di registrazioni continue, ma di registrazioni che coprono brevi archi temporali";

"[tale] impostazione […] trova espresso riscontro anche nel contratto di nomina a responsabile del trattamento dati personali stipulato tra Comune […] e Fondazione […] e nel documento di analisi allo stesso allegato, in cui è stata prevista la progressiva implementazione da parte di FBK delle seguenti forme di anonimizzazione dei dati audio: rimozione dei segmenti che contengono parlato dai dati registrati sui server FBK; rimozione dei segmenti che contengono parlato dai dati registrati sui dispositivi connessi ai microfoni; conversione della voce dei parlanti registrati sui server FBK […]. La soluzione finale realizzata nel progetto, che prevede la conversione della voce dei parlanti sui dispositivi connessi ai microfoni, risulta migliorativa rispetto alle soluzioni previste nell'allegato menzionato";

"[con riguardo ai] video [nell'ambito del] progetto MARVEL e PROTECTOR […] il rischio connesso all'approccio di anonimizzazione dei filmati tramite l'offuscamento di volti e di targhe è stato valutato nel contesto delle attività di screening etico richieste dalla Commissione Europea per il progetto MARVEL […] [ed] è stato classificato come "basso" […]";

"[tale] impostazione […] ha trovato espresso riscontro anche nel contratto di nomina a responsabile del trattamento dati personali stipulato tra Comune […] e Fondazione […] e nel documento di analisi allo stesso allegato, in cui è stato in particolare rilevato che "per i dati visivi, il contenuto più vulnerabile è il volto di una persona, per il quale non è difficile trovare su Internet immagini campione con relativo identificatore (ID). Chiaramente, potrebbero essere sfruttate altre caratteristiche, come ad esempio i vestiti, un particolare taglio di capelli, o la morfologia del corpo; tuttavia, queste caratteristiche non sono sufficienti per identificare univocamente una persona rispetto ai tratti del viso. Inoltre, la rimozione di tutti i contenuti visivi relativi a una persona deteriorerebbe notevolmente le prestazioni di altre attività degli algoritmi per il monitoraggio di situazioni di potenziale pericolo o ritenute anomale, alcune delle quali potrebbero essere rese non identificabili" e che "nel caso in cui i dati video riguardino delle auto si applicheranno concetti simili, con le targhe che ricoprono il ruolo svolto dai volti per la figura umana"";

"in merito ai messaggi Twitter e ai commenti YouTube raccolti nell'ambito del progetto PROTECTOR, si chiarisce che vengono processati per estrarre informazioni relative al contenuto d'odio o alle emozioni espresse. Conclusa l'analisi, il testo dei singoli messaggi/commenti non viene più utilizzato, non viene integrato nella piattaforma PROTECTOR e non è quindi visibile né accessibile da nessun utente. L'analisi proposta nella piattaforma presenta infatti risultati aggregati e non più riconducibili a messaggi di singoli utenti. Per quanto riguarda gli autori dei messaggi/commenti, gli utenti di YouTube vengono immediatamente cancellati, mentre gli utenti di Twitter vengono pseudonimizzati sostituendo lo username reale con uno user ID random generato automaticamente. Ribadendo che non è stata resa accessibile per attività operative ma solo per scopi dimostrativi ai componenti del consorzio, nella piattaforma, second[o] la logica con cui è stata implementata, i partner del progetto possono visualizzare la rete di interazioni tra utenti (senza nessun tipo di informazione sul contenuto dei messaggi) visualizzando esclusivamente gli user ID random generati; l'accesso a queste informazioni è possibile solo tramite autenticazione. Soltanto le forze dell'ordine coinvolte nel progetto (Polizia Locale - IT, Polizia di Anversa - BE e Ministero dell'Interno della Bulgaria - BG), hanno accesso ad una versione della piattaforma in cui le reti di utenti possono essere visualizzate con i nomi utenti effettivi (senza alcuna informazione sul tipo di messaggi che questi utenti si sono scambiati). […] Si specifica inoltre che la piattaforma non analizza un flusso di messaggi in tempo reale, ma contiene a scopi dimostrativi le analisi relative a messaggi raccolti nell'arco di tre mesi (novembre 2021 - gennaio 2022). L'analisi dei rischi legati all'utilizzo dei messaggi/commenti sui social network è presentata nel Deliverable D4.3. (sezioni 2.1.1.2 e 2.1.1.4). Dettagli sull'autenticazione sono riportati nei Deliverable D4.4. e D4.5";

"relativamente alla condivisione nell'ambito del progetto MARVEL dei contenuti audio e video anonimizzati, le attività tecniche di competenza della Fondazione […] riguardano l'implementazione e l'operatività di una componente software

(server RTSP) che riceve i flussi anonimizzati e li rende disponibili alle componenti che ne fanno richiesta all'interno della piattaforma di progetto. Inoltre, relativamente al data corpus, la Fondazione […] rende disponibili i dati audio e video anonimizzati, corredati da metadati relativi a data, ora e luogo, attraverso un programma (eseguibile Java) fornito dal Consorzio. I dati anonimi sono resi disponibili e accessibili ai partner di progetto per le rispettive attività […]. Relativamente alla condivisione nell'ambito del progetto PROTECTOR dei contenuti video anonimizzati, gli stessi sono accessibili esclusivamente ai Partner di progetto, alla Commissione Europea e ai Revisori del progetto, per il tramite di un dimostratore software, parte della piattaforma PROTECTOR. […].

Con nota del XX (prot. n. XX), l'Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, ha notificato al Comune, 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 posto in essere trattamenti di dati personali in maniera non conforme al principio di "liceità, correttezza e trasparenza", in violazione dell'art. 5, par. 1, lett. a) del Regolamento; in assenza di base giuridica, in violazione degli artt. 6, 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice; omettendo di fornire agli interessati taluni degli elementi informativi richiesti dalla disciplina in materia di protezione dei dati, in violazione degli 13, par. 1, lett. c) ed e), e par. 2, lett. a), b) e d), e 14 del Regolamento; comunicando a terzi dati personali, anche relativi a reati e a categorie particolari (convinzioni religiose), in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice; omettendo di stipulare un accordo sulla protezione dei dati con la Fondazione (responsabile del trattamento), in violazione dell'art. 28 del Regolamento; omettendo di redigere una valutazione d'impatto sulla protezione dei dati conforme ai requisiti previsti dalla normativa in materia di protezione dei dati, in violazione dell'art. 35 del Regolamento.

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 XX (prot. n. XX), il Comune ha presentato una memoria difensiva, dichiarando, in particolare, che:

"a partire dal 1º novembre 2023 si è provveduto a limitare il trattamento dei dati, bloccando ogni attività che possa comportarne la rilevazione o l'utilizzo, eccezion fatta per la mera conservazione anche a fini difensivi";

"le valutazioni che hanno guidato l'operato del Comune […] si sono basate sul fatto che, nel perseguimento del bene pubblico alla sicurezza urbana, vi fosse una piena realizzazione del principio di liceità. Inoltre, quanto ai contenuti delle registrazioni video e audio, la partecipazione ai Progetti europei partiva dall'assunto che gli obiettivi potessero essere raggiunti senza alcun trattamento di dati personali, quindi neppure di dati appartenenti a categorie particolari o relativi a condanne penali e reati";

"le videoregistrazioni e gli audio acquisiti ed elaborati nell'ambito di tali Progetti, sono destinati al c.d. "addestramento" dei software, vale a dire a renderli efficaci nell'attività di riconoscimento delle potenziali situazioni di rischio per la sicurezza delle città";

"[…] il Comune […] ha inteso fornire alcune ore di registrazioni di pubbliche piazze della propria città, sul presupposto che sarebbero state utilizzate solo previa adeguata rimozione di eventuali dati personali";

"senza la garanzia che non venissero utilizzati dati personali, l'Amministrazione comunale non avrebbe mai acconsentito a dare il proprio contributo a tali Progetti. Su tali presupposti, consapevole dei rischi nell'uso di registrazioni video e audio, il Comune […] si è avvalso dell'opera e delle valutazioni compiute da partner tecnici di comprovata competenza ed esperienza – in particolare della Fondazione […]";

"l'adesione del Comune […] ai menzionati Progetti europei dev'essere ravvisata proprio nella volontà di contribuire a portare a termine una ricerca pregevole e, in definitiva (nell'ottica di un suo utilizzo a regime), di migliorare il livello di sicurezza del territorio comunale e la qualità di vita dei suoi cittadini";

"con riferimento ai Progetti "Marvel" e "Protector", il DPO del Comune […] nel XX, nel trattare la questione su espressa richiesta comunale, ha comunicato con parere che "In merito alla verifica della sussistenza della base di liceità del trattamento in riferimento ai Progetti di ricerca, si conferma la sussistenza della stessa con riferimento all'articolo 6, paragrafo 1, lettera e) del Regolamento […]";

"ciò posto, anche in considerazione dei pareri del DPO, il Comune […] ha ritenuto sussistente la liceità del trattamento […] con particolare riguardo alla tutela della sicurezza urbana […]";

"si ritiene più che evidente la buona fede in cui versava l'Ente comunale nel considerare pienamente realizzato anche il principio di liceità in relazione alla "base giuridica" (Considerando n. 41 del [Regolamento]): le molteplici norme nazionali [in materia di sicurezza urbana], volte al perseguimento del bene pubblico alla sicurezza (in piena coerenza con le finalità del Progetto) sono state ritenute un più che adeguato fondamento giuridico legittimante il trattamento";

"tale considerazione, valga quale prova del fatto che un eventuale errore di diritto contestato […] [al Comune], sia stato sostanzialmente inevitabile e, pertanto, "scusabile", alla luce di una serie di elementi positivi, estranei al Comune […], idonei ad ingenerare la convinzione di liceità della condotta, avendo, il Comune stesso, fatto tutto il possibile per osservare le normative citate";

"il Comune […] ha ritenuto, in assoluta correttezza e buona fede, che in entrambi i casi (immagini e suoni) non si effettuasse alcun trattamento (nel caso delle immagini, ulteriore rispetto a quello in corso per finalità di pubblica sicurezza e ordine pubblico)":

"[…] il Comune […] ha orientato le proprie azioni secondo una valutazione di "probabilità e gravità" [del rischio di identificazione degli interessati] […]";

"per i Progetti "Marvel" e "Protector" dall'uso di tali telecamere è stata effettuata l'acquisizione di tracce video di modesta qualità […] Per il Progetto "Marvel" si tratta di complessive 14 telecamere, posizionate in complessivi luoghi (corrispondenti essenzialmente ad alcune piazze della città), con ripresa del medesimo luogo da angolature differenti; per il Progetto "Protector" sono invece state utilizzate complessive 4 telecamere, posizionate in 4 piazze; la risoluzione dei fotogrammi è di 1200x1600 pixel, cioè meno di 2 megapixels […] il video è soggetto ad una elevata compressione delle immagini, che genera i c.d. "artefatti", cioè una alterazione dei dettagli; le telecamere si trovano a un'altezza tra i 3,5 e i 40 metri da terra; in condizioni di scarsa illuminazione (sera, notte e mattino presto) le telecamere funzionano ad infrarossi, sicché in tale frangente registrano solo in bianco e nero e con ridotto contrasto; trattandosi spesso di visione dall'alto e ad un determinato angolo, le persone e gli oggetti vengono ritratti con una distorsione prospettica che ne altera le caratteristiche; da ogni telecamera sono state acquisite tracce video di 1 minuto consecutivo (per "Marvel") o di 3 minuti consecutivi (per "Protector"), con impossibilità di acquisire i minuti precedenti o successivi, sicché tra una traccia e l'altra della medesima telecamera trascorre mediamente un'ora; le tracce erano utilizzate dai ricercatori solo a distanza di tempo dalla registrazione, cioè non in diretta";

"per il Progetto "Marvel" sono state acquisite complessivamente 309 ore di registrazione video (corrispondenti a 13 giorni), riferibili ad un arco temporale di 20 mesi (tra il febbraio 2022 e il 1º novembre 2023, quando è stata bloccata ogni attività); nell'ambito del progetto "Marvel" i ricercatori che potevano accedere ai dati erano circa 60";

"per il Progetto "Protector" sono state acquisite complessivamente 18 ore di registrazione video, riferibili ad un arco temporale di 15 mesi (tra il febbraio 2022 e il 30 aprile 2023); di queste attualmente sono conservate solo 4 ore circa, in quanto nell'ambito del Progetto i dati non erano più necessari; nell'ambito del Progetto "Protector" i ricercatori che potevano accedere ai dati erano circa 90";

"si può stimare che ogni persona nei fotogrammi è composta solo da un ridotto gruppo di pixel, rendendo estremamente limitata la rappresentazione grafica delle caratteristiche fisiche";

"questi elementi, unitariamente ponderati, hanno portato il Comune […] a ritenere – una volta effettuata l'ulteriore anonimizzazione dei volti delle persone e delle targhe dei veicoli (mediante sfocatura o alterazione) – che non fosse in concreto possibile riconoscere delle caratteristiche personali sufficienti per permettere di identificare univocamente i soggetti ritratti. Pertanto, si era persuasi che le circostanze oggettive e gli accorgimenti tecnici fossero tali da escludere un sostanziale trattamento di dati riferibili a persone identificate o identificabili";

"quanto al c.d. "test dell'intruso motivato", si è anche evidenziato lo scarso valore delle informazioni (trattandosi di riprese di modesta qualità, di breve durata ed effettuate in pubbliche piazze)";

"inoltre, anche guardando all'elemento soggettivo, non sussiste alcuna motivazione o interesse (né in capo al Titolare e al Responsabile del trattamento né in capo ai ricercatori che hanno accesso ai dati anonimizzati) alla re-identificazione [degli interessati, atteso che] […] per le finalità istituzionali dei Progetti i dati personali non hanno alcuna utilità";

"le registrazioni audio sono state effettuate attraverso microfoni collegati ad un dispositivo hardware ([c.d. "single board computer"]) installati specificamente per i fini progettuali. Sul dispositivo la Fondazione ha installato il software di anonimizzazione previsto nell'ambito del Progetto "Marvel". Per espressa volontà e conformità ai fini progettuali, i microfoni utilizzati avevano ridotta capacità di captare i suoni, in quanto risultava rilevante solo la registrazione dei rumori intensi (come quelli causati dallo scontro di veicoli, di un'esplosione, ecc.)";

"si tratta di complessivi 6 microfoni, posizionati in 3 luoghi (corrispondenti ad alcune delle piazze della città ove già sono installate le telecamere); da ogni microfono sono state acquisite tracce audio di 1 solo minuto consecutivo, con impossibilità di acquisire i minuti precedenti o successivi, sicché tra una traccia e l'altra del medesimo microfono trascorre circa un'ora; nel complesso sono state acquisite 85 ore di registrazione (pari a meno di 4 giorni), riferibili ad un arco temporale di 8 mesi (tra il marzo e il 1º novembre 2023, quando è stata bloccata ogni attività), tutte nell'ambito del Progetto "Marvel"; le tracce erano utilizzate dai ricercatori solo a distanza di tempo dalla registrazione, cioè non in diretta; inoltre, i microfoni erano stati installati ad un'altezza tra i 3,5 e 7 metri da terra; l'intensità dei suoni captabili veniva ridotta dalla presenza di una scatola protettiva (scatola di derivazione elettrica) all'interno della quale era inserito ogni microfono (per proteggerlo dalle intemperie); agli audio potevano accedere i circa 60 ricercatori di "Marvel"";

"la Fondazione ha comunicato che sulla base di queste tarature tutte le tracce audio risultano composte quasi interamente da silenzio o indistinguibili brusii di sottofondo. Solo in rari attimi sono percepibili altri suoni, riferibili essenzialmente ad eventi straordinariamente rumorosi avvenuti in luogo molto ravvicinato al microfono e sempre limitati nel tempo a circa 1 minuto (principalmente transito di un mezzo pesante, la sirena di un veicolo d'emergenza, ecc.)";

"solo per la rara eventualità di registrazione delle voci di persone, è stata comunque prevista una anonimizzazione alla fonte dei segmenti contenenti parlato, con alterazione delle caratteristiche della voce in modo da rendere l'identità del

parlatore non più riconoscibile. Tale attività di alterazione era compiuta direttamente presso il microfono, così da mettere tracce audio già anonimizzate a disposizione dei ricercatori";

"tutte queste circostanze avevano portato il Comune […] a ritenere che, nell'ambito del Progetto "Marvel", anche per le registrazioni audio non vi fosse stato un sostanziale trattamento di informazioni riguardanti persone identificate o identificabili";

"[…] sempre per le registrazioni dell'audio – considerato che i microfoni erano stati installati in esecuzione ad uno specifico accordo contrattuale contenuto nel Progetto "Marvel", nel cui ambito era già definito l'uso che di essi sarebbe stato fatto – si è ritenuto che al Comune […] non fosse attribuibile alcun speciale ruolo nel definire le finalità e modalità del trattamento";

quanto al trattamento dei "messaggi o commenti degli utenti delle piattaforme web "Twitter" e "YouTube"" nell'ambito del progetto "Protector", "l'Amministrazione comunale trentina non ha mai partecipato ad alcuna decisione inerente tale attività di ricerca, rimanendo anche estranea a qualunque effettiva attività operativa inerente lo stesso. In altri termini, nessun trattamento è mai stato compiuto dal Comune […], oppure nel suo interesse o a suo vantaggio. Infatti, tale attività era prevista nell'ambito del pacchetto di lavoro 3 ("WP 3") che non attribuiva alcun concreto ruolo operativo all'Amministrazione comunale";

"la previsione per la quale i "nomi utenti" degli autori di messaggi pubblicati sulla piattaforma "Twitter" venissero condivisi con alcune pubbliche autorità, era stata prevista nell'interesse degli altri partner istituzionali (come la Polizia di Anversa e il Ministero dell'Interno della Bulgaria), ma non è mai stata richiesta né desiderata dal Comune […]. Infatti tale previsione è rimasta del tutto inattuata, non essendovi mai stato accesso ai dati da parte del Corpo di Polizia locale trentino, né da altro personale del Comune";

"proprio in ragione di tale totale estraneità, nella documentazione redatta dal Comune (valutazione d'impatto, informativa sul trattamento, ecc.) non è stata fatta menzione alcuna di attività di trattamento di dati tratti dal web e, comunque, di dati su convinzioni religiose";

"in ragione di quanto illustrato, il Comune […] ha sempre ritenuto che, relativamente ai dati raccolti sul web, fossero da considerare titolari del trattamento solo coloro che erano direttamente coinvolti in tali operazioni";

"con riferimento alla contestazione di avvenuto trattamento di categorie particolari di dati e dati relativi a condanne penali e reati […] il Comune […] ha fatto affidamento sulla consueta qualificazione delle immagini come dati personali "comuni";

"i dati relativi alle osservazioni di uno svolgimento di eventi in cui possono essere integrati gli estremi di un reato, non sono normalmente considerati un trattamento di dati ai sensi dell'articolo 10 del [Regolamento]; tuttavia, è considerato un trattamento di questo tipo se, in seguito, il corso degli eventi viene separato al fine di documentare, adottare misure successive o denunciare il reato. Nel caso di specie, né il Comune […] né la Fondazione hanno trattato dati giudiziari, non essendo le registrazioni utilizzate allo scopo di isolare o identificare singoli individui (o gruppi di individui) con il fine di procedere ad attività successive da parte delle Autorità pubbliche (es. indagini, arresti, provvedimenti sanzionatori). Si sottolinea, infatti, che ogni segmento video e audio è destinato al solo scopo di "addestrare" il software al riconoscimento di situazioni di pericolo";

"[…] ciò deve valere sia per le videoregistrazioni che per le registrazioni audio, potendosi applicare le medesime argomentazioni";

"per quanto riguarda i dati relativi alle convinzioni religiose, costituenti categoria particolare di dati ex art. 9 del Regolamento, vale quanto detto sopra […], dovendosi affermare l'estraneità del Comune […] al trattamento";

"il Comune prende atto delle considerazioni svolte [dall'] Autorità in ordine al possibile fraintendimento ingenerato nei cittadini conseguente al fatto che non sarebbe risultata chiara la finalità del trattamento dei dati riportata nell'informativa collocata in prossimità dei sistemi di registrazione, e intende adeguare l'informativa che si renderà necessario utilizzare per le future occorrenze";

"le informative, ed in particolare quella di secondo livello, sono state redatte sulla base di modelli forniti dal DPO del Comune […] ed in coerenza con le direttive interne comunali";

"nelle informative di primo e di secondo livello la base giuridica e le finalità del trattamento sono state individuate ed esplicitate in relazione alla base giuridica del trattamento ritenuta rilevante (ciò in particolare per l'informativa di primo livello in cui si fa riferimento alla tutela della sicurezza urbana); a tale riguardo, merita di essere richiamato l'affidamento del Comune […] relativamente al fatto che non fossero effettuati trattamenti ulteriori rispetto a quello già in corso (rilevazione delle immagini per finalità di pubblica sicurezza e ordine pubblico) e, comunque, che non fossero coinvolti dati appartenenti a particolari categorie (art. 9 del [Regolamento]) o relativi a condanne penali e reati (art. 10 del [Regolamento])";

"la mancata indicazione nell'informativa del fatto che la strumentazione fosse in grado di captare anche le conversazioni delle persone, è giustificabile anche dal fatto che, per le caratteristiche intrinseche del sistema di registrazione (come sopra descritto) l'effettiva possibilità di udire rilevanti contenuti semantici era da considerarsi una eventualità pressoché nulla";

"quanto all'assenza di una specifica illustrazione di trattamenti di dati personali che riguardano la pubblicazione di messaggi sulla piattaforma "Twitter" o commenti sulla piattaforma "YouTube" nell'ambito del Progetto "Protector", si richiama quanto sopra indicato [in merito al ruolo svolto dal Comune]";

"le informative sono state impostate ed effettuate in piena buona fede, dando informazioni e rassicurazioni alla cittadinanza, in linea a quanto sopra detto, sull'assunto che i dati fossero anonimizzati, anche grazie alla competenza ed esperienza di FBK; da ciò deriva l'informativa di secondo livello priva del riferimento alla comunicazione dei dati a soggetti terzi";

"oltre alle informative di primo e di secondo livello, che sono state redatte sulla base degli accordi di progetto (Grant Agreement) e secondo i modelli condivisi con il DPO, sono state promosse forme di divulgazione pubblica dei Progetti tra cui comunicati stampa, comunicati sul sito istituzionale del Comune, diffusione delle informazioni riguardanti i Progetti anche tramite social network del Comune e del Sindaco (inclusa la conferenza stampa dell'8 maggio 2023) e sono stati divulgati video di presentazione dei Progetti su YouTube";

"con riferimento all'informativa ex art. 13 del GDPR […] il Comune ha confidato nel parere del DPO";

"è stata avviata anche la stesura della valutazione di impatto, di cui è stata completata la redazione già in data 19 gennaio 2022 (quando è stata condivisa per la prima volta con il DPO, come risulta dallo scambio di email [in atti]). La valutazione d'impatto è stata successivamente inserita nell'applicativo informatico contenente il registro delle attività di trattamento […] nel marzo 2023, solo dopo aver ottenuto il parere definitivo del DPO sulla valutazione stessa ([in atti]). Quindi, si ritiene di aver documentato il fatto che il Comune aveva provveduto ad effettuare la valutazione di impatto prima dell'inizio dei trattamenti (febbraio 2022 per la parte video, marzo 2023 per la parte audio) e che la valutazione stessa è riconducibile all'Ente";

"[…] si è provveduto debitamente a coinvolgere il Responsabile della protezione dei dati. Il DPO, dopo lunga e attenta interlocuzione con il Comune, aveva espresso parere positivo […]";

"l'atto di nomina [della Fondazione quale responsabile del trattamento] è stato formalizzato con decreto sindacale, sottoscritto digitalmente dal Sindaco […] il 3 febbraio 2022 […]. Il decreto è stato quindi trasmesso a FBK, la quale ne ha restituito copia controfirmata il 7 febbraio 2022 dal proprio legale rappresentante per accettazione della nomina […]. Per mero errore materiale la copia dell'atto già trasmessa [all'] Autorità non conteneva la data di protocollo originale, ma comunque conservava le corrette date di apposizione delle due firme digitali";

"si precisa che la nomina conteneva un allegato […], denominato "Rispetto dei requisiti etici stabiliti per la partecipazione di persone a progetti europei - MARVEL (Grant Agreement n° 957337) e PROTECTOR (Grant Agreement n° 101034216)", il quale, unitamente alla stessa nomina controfirmata per accettazione, costituisce un accordo congiunto, disciplinante le regole da seguire per il trattamento dei dati, in particolare per la fase di anonimizzazione. Infatti, si ribadisce che tale allegato è stato redatto congiuntamente con la Fondazione, la quale, in particolare, ha contribuito anche indicando le specifiche tecniche di anonimizzazione che riteneva adeguato applicare";

"in data 1º novembre 2023, il Comune […] ha immediatamente contattato i Partner dei Progetti al fine di renderli edotti delle osservazioni formulate [dall'] Autorità. In tale occasione è stato chiesto che venisse immediatamente sospesa ogni attività del Progetto "Marvel" (l'unico in corso di sperimentazione) che coinvolgesse l'acquisizione e l'elaborazione delle registrazioni in questione";

"tale richiesta di sospensione è stata prontamente riscontrata positivamente, con conseguente blocco di ogni attività di trattamento di dati derivanti dalle registrazioni acquisite nelle pubbliche piazze della città di Trento, salvo la mera conservazione dei dati anche a fini difensivi";

"si conferma che, nell'ambito del progetto "Protector", i dati non vengono più raccolti da inizio maggio 2023 e che, in ogni caso anche per tale Progetto, è stata bloccata ogni attività di trattamento".

In occasione dell'audizione, richiesta ai sensi dell'art. 166, comma 6, del Codice e tenutasi in data XX (v. verbale prot. n. XX della medesima data), il Comune ha dichiarato, in particolare, che:

"il Comune, nell'ambito dei due progetti, era uno dei partner e non un leader; ogni partner era infatti chiamato a dare il proprio contributo, ognuno per l'ambito di propria competenza";

"il Comune ha confidato nel fatto che i trattamenti posti in essere nei due progetti di ricerca europei potessero essere ricondotti al quadro giuridico in materia di sicurezza urbana e alle specifiche competenze che lo stesso attribuisce al Sindaco";

"in tale quadro, il Comune era interessato a dotarsi di tecnologie volte a individuare ex ante eventuali rischi per la sicurezza urbana e, a tal fine, ha fatto affidamento sulla Fondazione, soggetto altamente qualificato, ai fini dell'individuazione delle migliori tecnologie da impiegare nell'ambito dei due progetti europei e alle misure da porre in essere al fine di garantire il rispetto del diritto alla protezione dei dati dei soggetti interessati";

"i due progetti, in quanto volti a rafforzare la sicurezza urbana nel territorio comunale, erano strumentali a conseguire il bene pubblico";

"il Comune, anche per quanto concerne le tecniche di anonimizzazione da impiegarsi nell'ambito dei due progetti, aveva fatto affidamento sulla Fondazione, in quanto partner tecnologico che poteva offrire le più elevate garanzie in virtù delle proprie conoscenze specialistiche, senza che ciò abbia comportato una deresponsabilizzazione del Comune, che ha interloquito con la Fondazione al fine di individuare le misure più opportune";

"per quanto attiene alla trasparenza del trattamento, si è cercato di porre in essere tutte le iniziative per assicurare la piena consapevolezza da parte dei cittadini";

"con riguardo alla valutazione d'impatto, non esiste un modello predefinito dalla legge per eseguire la stessa, avendo il Comune in buona fede ritenuto che la metodologia utilizzata fosse idonea".

Con successive note del Comune (prot. n. XX) e del RPD dello stesso, inviate in data XX ad integrazione di quanto dichiarato in audizione, sono state sostanzialmente ribadite le difese prospettate dall'Ente e sopra già illustrate.

3. Esito dell'attività istruttoria.

3.1 I trattamenti di dati personali effettuati nell'ambito dei progetti "Marvel" e "Protector".

Dalle dichiarazioni rese dal Comune nel corso dell'istruttoria, nonché dalla complessiva documentazione in atti, è emerso che il Comune, agendo in qualità di titolare del trattamento, con il supporto della Fondazione, quale responsabile del trattamento, ha partecipato a due progetti di ricerca, denominati "Marvel" e "Protector", finanziati con fondi europei, con l'obiettivo di sviluppare soluzioni tecnologiche volte a migliorare la sicurezza in ambito urbano, secondo il paradigma delle c.d. "città intelligenti" (smart cities).

In particolare e in sintesi:

il progetto "Marvel" ("Multimodal Extreme Scale Data Analytics for Smart Cities Environments"), che sarebbe dovuto terminare in data 31 dicembre 2023, prevede l'acquisizione di filmati estratti dalle telecamere di videosorveglianza già installate nel territorio comunale per finalità di sicurezza urbana (v. artt. 4 e 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14; cfr. art. 7, commi 7 e 8, del d.l. 23 febbraio 2009, n. 11), nonché dell'audio ottenuto da microfoni appositamente collocati sulla pubblica via ai fini del progetto. Tali dati, che ad avviso del Comune sarebbero immediatamente anonimizzati dopo la raccolta, vengono analizzati al fine di rilevare in maniera automatizzata, mediante tecniche di intelligenza artificiale, eventi rilevanti ai fini della salvaguardia della pubblica sicurezza (es. assembramenti, aggressioni, scippi, risse, ecc.). Nell'ambito di tale progetto, il Comune ha impiegato complessivamente 14 telecamere; da ogni telecamera sono state acquisite tracce video di 1 minuto consecutivo con un intervallo medio di 1 ora tra una traccia e l'altra. Sono state acquisite complessivamente 309 ore di registrazione video (corrispondenti a 13 giorni), riferibili ad un arco temporale di 20 mesi (tra il febbraio 2022 e il 1º novembre 2023). Quanto all'acquisizione dell'audio, sono stati installati complessivamente 6 microfoni, posizionati in 3 luoghi delle città dove risultano già installate delle telecamere. Da ogni microfono sono state acquisite tracce audio di 1 solo minuto consecutivo, con intervalli di circa un'ora tra una traccia e l'altra. Nel complesso sono state acquisite 85 ore di registrazione, riferibili ad un arco temporale di 8 mesi (tra il marzo e il 1º novembre 2023);

il progetto "Protector" ("PROTECTing places of wORship"), che è terminato il 30 aprile 2023, prevedeva, oltre all'acquisizione di filmati da telecamere di videosorveglianza (senza segnale audio), anche la raccolta e l'analisi, mediante le predette tecniche di intelligenza artificiale, di messaggi d'odio pubblicati sulla piattaforma "Twitter" (ora denominata "X") e commenti pubblicati sulla piattaforma "YouTube", al fine di rilevare eventuali emozioni negative (aggressività, rabbia o altre emozioni negative sul tema della religione), elaborando, mediante le predette tecniche di intelligenza artificiale, informazioni ritenute d'interesse per le Forze dell'ordine, al fine di identificare rischi e minacce per la sicurezza dei luoghi di culto. Nell'ambito di tale progetto, il Comune ha impiegato complessivamente 4 telecamere, posizionate in 4 piazze; da ogni telecamera sono state acquisite tracce video di 3 minuti consecutivi con un intervallo medio di 1 ora tra una traccia e l'altra. Sono state acquisite complessivamente 18 ore di registrazione video, riferibili ad un arco temporale di 15 mesi (tra il febbraio 2022 e il 30 aprile 2023); di queste attualmente sono conservate solo 4 ore circa.

Atteso che le telecamere di sicurezza urbana e i microfoni collocati sulla pubblica via sono stati impiegati con lo specifico obiettivo di individuare e analizzare fatti rilevanti ai fini della tutela della pubblica sicurezza, che possono quindi integrare fattispecie di reato, e considerato che gli utenti che postano messaggi/commenti d'odio sulle piattaforme Twitter ("X") e YouTube, analizzati al fine di rilevare minacce per la sicurezza dei luoghi di culto, possono commettere specifici reati (v., ad esempio, l'art. 604-bis c.p. in materia di propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa), il Comune, nell'ambito dei due progetti, ha posto in essere un trattamento di dati personali relativi a reati (v. art. 10 del Regolamento e 2-octies del Codice).

Non può, invece, essere accolta la tesi difensiva del Comune, secondo la quale le immagini di videosorveglianza non possono essere di per sé considerate dati personali relativi a reati, salvo che le stesse, una volta acquisite, non vengano successivamente effettivamente utilizzate per accertare una fattispecie di reato. Come sopra evidenziato, le immagini di videosorveglianza sono state, infatti, acquisite da telecamere già installate sul territorio comunale per la tutela della sicurezza urbana, ovvero per la specifica finalità di "prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria" (art. 5, comma 2, lett. a), del d.l. 20 febbraio 2017 , n. 14). Al riguardo, ancorché in relazione alle particolari categorie di dati personali dell'art. 9 del Regolamento, il Comitato europeo per la protezione dei dati ha chiarito che "la videosorveglianza non sempre è considerata un trattamento di categorie particolari di dati personali [...;] tuttavia, se le riprese video sono trattate per ricavare categorie particolari di dati, si applica l'articolo 9" ("Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del

GDPR", adottate il 7 luglio 2021, punti 62 e 63). Parimenti, le telecamere di videosorveglianza in questione sono state installate dal Comune al fine precipuo di individuare e documentare fattispecie di reato connesse ai fenomeni di criminalità diffusa e predatoria, e anche nell'ambito dei progetti "Marvel" e "Protector" le immagini sono state utilizzate al fine specifico di addestrare gli algoritmi di intelligenza artificiale a riconoscere potenziali situazioni di rischio per la pubblica sicurezza.

Inoltre, atteso che i predetti messaggi/commenti acquisiti dalle reti sociali riguardano l'ambito religioso e possono rivelare le convinzioni religiose dei relativi autori o di terzi menzionati in detti messaggi, il Comune ha anche posto in essere un trattamento di dati personali appartenenti a categorie particolari (v. art. 9 del Regolamento e 2-sexies del Codice).

Per quanto attiene al progetto "Precrisis", si prende, invece, atto che il Comune ha dichiarato che allo stato non viene posto in essere alcun trattamento di dati personali, "essendo lo stesso ancora in fase di programmazione e analisi di contesto".

3.2 Il ruolo del Comune e della Fondazione ai fini della normativa in materia di protezione dei dati.

Nell'ambito dei predetti progetti, il Comune ha affermato di agire in qualità di titolare del trattamento, mentre la Fondazione avrebbe rivestito il ruolo di responsabile del trattamento, essendo stata designata come tale dal Comune.

A tal riguardo, si osserva che, ancorché anche la Fondazione figuri tra i partner dei progetti in questione, negli accordi stipulati per la fruizione dei fondi comunitari (c.d. "grant agreements") il Comune viene identificato come soggetto leader e coordinatore ai fini della conduzione delle sperimentazioni nel proprio territorio, mentre la Fondazione viene considerata un partner di supporto, in grado di offrire competenze e tecnologie di cui il Comune non dispone (v. il "Grant Agreement" del progetto "Marvel", allegato alla nota del Comune del 18 ottobre u.s., cit., ove si afferma che "il Comune […] sarà il leader del caso d'uso di Trento, incentrato sul monitoraggio delle aree urbane pubbliche. Condurrà le attività pilota guidando i WP6 [Esperimenti sociali di vita reale nell'ambiente delle smart cities]" (pag. 98), mentre "FBK offrirà le sue soluzioni attuali e la ricerca di nuove tecniche nel campo delle Smart City […] [e] contribuirà […] in modo significativo ai WP6 [Esperimenti sociali di vita reale nell'ambiente delle smart cities] partecipando […] alle attività di […] sperimentazione" (pag. 86); per quanto riguarda il progetto "Protector", v. il relativo "Grant Agreement", allegato alla medesima nota, ove si afferma che "[la Fondazione] definirà i criteri dei test pilota ed elaborerà una matrice di valutazione […] Il primo test pilota sarà condotto a Trento, Italia e sarà coordinato [dal Comune]" (pag. 18)).

D'altra parte, lo stesso Comune ha dichiarato nel corso dell'istruttoria che "la Fondazione […] è il partner che fornisce parte dell'infrastruttura hardware per il processing dei dati e le tecnologie di anonimizzazione audio/video", che "su indicazione del Comune […] - mette a disposizione due workstations presso i propri laboratori", che "si occupa dell'acquisizione di dati audio e video", che è "responsabile dello sviluppo della piattaforma software denominata PROTECTOR Platform", essendo dunque "partner tecnologico del Comune […] nello sviluppo dei tre progetti di ricerca […] individuata come l'unico soggetto esterno al Comune […] incaricato di effettuare, mediante la gestione dei flussi audio e video prodotti dai microfoni e dalle telecamere, il trattamento di dati personali finalizzato allo sviluppo degli algoritmi di intelligenza artificiale" (nota del XX).

Si rileva, altresì, che, come dichiarato dal Comune e come sopra illustrato, i filmati video in questione vengono ottenuti dalle telecamere di videosorveglianza che risultano già installate nel territorio comunale per il perseguimento di finalità di sicurezza urbana, rispetto alle quali il Comune, e non anche la Fondazione, agisce quale titolare del trattamento. Anche in relazione ai microfoni impiegati per la captazione del segnale audio nell'ambito del progetto "Marvel", si osserva che solo il Comune, e non anche la Fondazione, poteva assumere la decisione di installare tali dispositivi sulla pubblica via, in quanto Ente locale con poteri di amministrazione sul proprio territorio.

Pertanto, il Comune ha esercitato un'"un'influenza determinante sulle finalità e i mezzi [essenziali] del trattamento" ("Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", cit., punto 30), avendo, pertanto, agito in qualità di "titolare del trattamento" (art. 4, par. 1, n. 7, del Regolamento).

Non rileva invece, se non ai fini della valutazione dell'elemento soggettivo, che il Comune abbia ritenuto in buona fede – anche sulla base della consulenza tecnica che gli sarebbe stata fornita in tal senso dalla Fondazione – che la partecipazione ai due progetti non avrebbe comportato un trattamento di dati personali, difesa che, peraltro, confligge con la circostanza che il Comune si è qualificato sin dal principio come titolare del trattamento, ha designato la Fondazione quale responsabile del trattamento e anche nelle proprie memorie difensive ha sostenuto la sussistenza di una base giuridica idonea a giustificare i trattamenti di dati personali effettuati nell'ambito dei due progetti.

Quanto al trattamento dei dati personali contenuti nei messaggi o commenti degli utenti delle piattaforme "Twitter" ("X") e "YouTube" nell'ambito del progetto "Protector", si osserva che il Comune ha negato la propria titolarità di tale trattamento soltanto nelle memorie difensive -presentate dopo la notifica della violazione di cui all'art. 166, comma 5, del Codice - avendo, invece, nel corso dell'istruttoria sostenuto la propria piena partecipazione al progetto "Protector", tanto che – a fronte delle richieste d'informazioni di questa Autorità – lo stesso ha illustrato gli specifici trattamenti di dati personali posti in essere nell'ambito dello stesso.

In ogni caso, la difesa del Comune non può essere accolta, non essendo dirimente che l'Ente non abbia direttamente posto in essere specifiche attività di trattamento in tale ambito. Infatti, decidendo di partecipare al progetto "Protector", mettendo a disposizione il proprio territorio e le proprie infrastrutture ai fini dello stesso e beneficiando dei complessivi risultati della ricerca, il Comune ha deciso le finalità e i mezzi del trattamento anche con riguardo alle informazioni ricavate dalle predette reti sociali. D'altra parte, il Comune era pienamente consapevole dei trattamenti in questione (si veda la pagina del sito web istituzionale del Comune dedicata al progetto Protector, ove si afferma che "in PROTECTOR si svilupperà un set di componenti tecnologiche

avanzate in grado di analizzare fonti eterogenee di dati (telecamere di sorveglianza, siti web, social networks, etc.) e li combinerà attraverso il supporto di strumenti ICT basati su tecniche di intelligenza artificiale per fornire "alerts" in caso di incremento del rischio relativo alla sicurezza dei luoghi di culto" - https://www.comune.trento.it/Aree-tematiche/Smart-city/Progetti-d-innovazione-conclusi/Protector) e la Polizia locale del Comune era stata fin dall'inizio identificata quale soggetto sperimentatore assieme alla Polizia di Anversa e al Ministero dell'Interno della Bulgaria, ognuno per il rispettivo contesto nazionale e per il proprio ambito territoriale di riferimento.

Non trova, inoltro, riscontro in atti l'affermazione del Comune secondo la quale "tale attività era prevista nell'ambito del pacchetto di lavoro 3 ("WP 3") che non attribuiva alcun concreto ruolo operativo all'Amministrazione comunale" (v. memoria difensiva). Dal c.d. "Grant Agreement" relativo al progetto "Protector", in atti, emerge, infatti, che tra i soggetti coinvolti in tale pacchetto di lavoro sono inclusi "FBK" (ovvero la Fondazione) e "TN" (ovvero il Comune) (pag. 68; v. anche pag. 101).

Più in generale, il "Grant Agreement" menziona "TN" (ovvero il Comune) tra i soggetti responsabili della "gestione e coordinamento di tutte le attività relative al progetto "Protector"", tenuti a fornire "supervisione su tutte le attività di progetto e i risultati". Inoltre, il Comune è responsabile dell'esecuzione del progetto sul proprio territorio e del coordinamento del primo "test pilota" relativo al progetto "Protector" (pag. 33; v. anche pag. 106).

Per le medesime ragioni, non rileva che "la previsione per la quale i "nomi utenti" degli autori di messaggi pubblicati sulla piattaforma "Twitter" venissero condivisi con alcune pubbliche autorità, era stata prevista nell'interesse degli altri partner istituzionali (come la Polizia di Anversa e il Ministero dell'Interno della Bulgaria), ma non è mai stata richiesta né desiderata dal Comune" (v. memoria difensiva), avendo il Comune consapevolmente partecipato al progetto nei termini prospettati nel "Grant Agreement" e avendo, pertanto, accettato - al di là dei propri interni desiderata - anche l'ambito di condivisione dei dati ivi previsto (v. la nota del XX, in cui il Comune dichiara che "soltanto le forze dell'ordine coinvolte nel progetto (Polizia Locale - IT, Polizia di Anversa - BE e Ministero dell'Interno della Bulgaria - BG), hanno accesso ad una versione della piattaforma in cui le reti di utenti possono essere visualizzate con i nomi utenti effettivi (senza alcuna informazione sul tipo di messaggi che questi utenti si sono scambiati)".

Inoltre, la circostanza che la Polizia locale del Comune non abbia mai effettivamente acceduto a tali dati non è dirimente, atteso che la titolarità del trattamento non presuppone necessariamente la disponibilità dei dati o il compimento di operazioni materiali di trattamento. La Corte di Giustizia dell'Unione europea ha, infatti, in più occasioni chiarito che qualsiasi persona fisica o giuridica che influisca, per fini che le sono propri, sul trattamento di tali dati e partecipi pertanto alla determinazione delle finalità e dei mezzi di tale trattamento può essere considerata titolare di detto trattamento, non essendo necessario che le finalità e i mezzi del trattamento siano determinati mediante orientamenti scritti o istruzioni da parte del titolare del trattamento, né che quest'ultimo sia stato formalmente designato come tale, né che abbia materialmente compiuto operazioni di trattamento (v., da ultimo, sent. C-683/21, Nacionalinis visuomenės sveikatos centras, del 5 dicembre 2023; v. anche C-807/21, Deutsche Wohnen, del 5 dicembre 2023; C-40/17, Fashion ID GmbH & Co.KG contro Verbraucherzentrale NRW eV, del 29 luglio 2019; C-25/17, Jehovan todistajat, del 10 luglio 2018; C-210/16, Wirtschaftsakademie Schleswig-Holstein, del 5 giugno 2018; v. anche le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", cit., spec. par. 56).

D'altra parte, la responsabilità del titolare del trattamento "si estende, come sottolineato dal considerando 74 del [Regolamento], a qualsiasi trattamento di dati personali effettuato direttamente o che altri abbiano effettuato per loro conto" (C-807/21, cit., punto 38). Poiché, un titolare del trattamento è responsabile non solo dei trattamenti di dati personali che effettua direttamente, ma anche di quelli effettuati per suo conto, "tale titolare del trattamento può vedersi infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83 del RGPD in una situazione in cui i dati personali sono oggetto di un trattamento illecito e non è siffatto titolare del trattamento, bensì un responsabile del trattamento, di cui esso si è avvalso, che ha effettuato tale trattamento per conto del titolare", ove si possa "ragionevolmente ritenere che tale titolare abbia […] acconsentito al trattamento" (sent. C-683/21, cit., punti 84 e 85).

Quanto alla Fondazione, che ha assunto una posizione servente rispetto al raggiungimento degli obiettivi dei due progetti, fornendo il proprio contributo limitatamente ai profili scientifici, tecnologici e organizzativi, si ritiene che la stessa abbia, invece, agito quale "responsabile del trattamento" (art. 4, par. 1, n. 8, del Regolamento). Essa è stata, peraltro, considerata come tale dallo stesso Comune, che ha a tal fine predisposto uno specifico accordo sulla protezione dei dati, ai sensi dell'art. 28 del Regolamento.

3.3 Le tecniche di anonimizzazione impiegate.

Preliminarmente si osserva che non è controverso che il Comune, nell'ambito dei due progetti di ricerca, abbia posto in essere un trattamento di dati personali nella fase di raccolta d'informazioni ritenute d'interesse (filmati di videosorveglianza; audio proveniente dai microfoni; messaggi/commenti/profili ottenuti da reti sociali).

Il Comune ha, infatti, sostenuto nel corso dell'istruttoria di aver impiegato – successivamente alla raccolta di tali dati - delle tecniche di anonimizzazione volte a mitigare l'impatto dei due progetti sui diritti e le libertà fondamentali degli interessati.

D'altra parte, come di recente ribadito dal Garante, anche l'acquisizione e la temporanea memorizzazione di dati personali, come l'immagine del volto ripresa da dispositivi video, ancorché per una ridotta frazione temporale, costituisce un trattamento di dati personali (v. provv.ti 13 aprile 2023, nn. 122 e 123, doc. web nn. 9896808 e 9896412, relativi al trattamento, posto in essere da soggetti pubblici, in assenza di idonea base giuridica, di dati personali contenuti in filmati ottenuti mediante dispositivi video, nell'ambito di un progetto che prevedeva l'impiego di algoritmi di rilevamento dei volti basati su reti neurali convoluzionali; v. anche, in senso conforme, il precedente provv. 21 dicembre 2017, n. 551, doc. web n. 7496252).

Inoltre, sul presupposto che i dati - dopo essere stati sottoposti a tali tecniche di anonimizzazione - potessero considerarsi sottratti all'ambito di applicazione della normativa in materia di protezione dei dati (v. cons. 26 del Regolamento), il Comune ha condiviso gli stessi con soggetti terzi partecipanti a vario titolo ai progetti (v. il successivo par. 3.6).

Ciò premesso, si osserva che, contrariamente a quanto sostenuto dal Comune, le tecniche da esso impiegate, successivamente alla raccolta dei dati, non possono considerarsi idonee a realizzare un'effettiva anonimizzazione degli stessi.

In particolare, nell'ambito del progetto Marvel, sul presupposto che i microfoni installati sulla pubblica via possono captare anche conversazioni, il Comune ha affermato che "l'anonimizzazione dei dati audio consiste nella sostituzione della voce del parlante, mantenendo quanto più inalterate possibile le caratteristiche del segnale audio, incluso il contenuto semantico del parlato".

Al riguardo, si osserva come la sola sostituzione della voce del soggetto parlante non è in alcun modo idonea ad anonimizzare i dati personali correlati a una conversazione, atteso che dal contenuto della stessa è possibile ricavare informazioni relative sia al soggetto parlante sia a terzi e che tali informazioni possono rendere identificabile il parlante, i suoi interlocutori o i soggetti terzi a cui si fa rifermento nel discorso.

Oltre a ciò si deve osservare che, tenuto conto dell'ampia varietà di argomenti che vengono usualmente affrontati nelle conversazioni, non possono essere a priori esclusi trattamenti di dati personali relativi a reati o a categorie particolari o comunque riguardanti soggetti vulnerabili (minori, lavoratori, soggetti fragili, ecc.).

Che il Comune fosse consapevole di tale rischio emerge, d'altra parte, anche della circostanza che il Responsabile della protezione dei dati, interpellato dal Comune con riferimento ai progetti in questione, aveva messo in evidenza, seppur fornendo un parere complessivamente positivo, che "l'utilizzo di microfoni audio che registrano le voci e le conversazioni dei cittadini in modalità che consenta l'identificazione degli stessi, costituisce indubbiamente una modalità di utilizzo del sistema della videosorveglianza particolarmente invasiva" (v. relazione del XX), che "l'impatto nei confronti dei cittadini rispetto alla registrazione delle voci e delle conversazioni sarà comunque "percepito" in modo significativo" (ibidem) e che "la raccolta "audio" dei dati personali rappresenta un elemento di particolare "criticità" rispetto all'invasività della riservatezza dei cittadini" (v. relazione del XX).

Venendo alle tesi difensive prospettate dal Comune, deve osservarsi che soltanto nelle proprie memorie - presentate dopo la notifica della violazione di cui all'art. 166, comma 5, del Codice, e non anche nel corso dell'istruttoria, nonostante le puntuali richieste d'informazioni rivolte dall'Ufficio dell'Autorità - il Comune ha alluso a una limitata capacità dei microfoni in questione a captare le conversazioni, in regione di specifiche caratteristiche tecniche dei dispositivi (rilevanza dei soli rumori intensi; collocazione dei microfoni in una "scatola protettiva" che riduceva l'"intensità dei suoni captabili") e degli accorgimenti adottati (installazione dei microfoni a un'altezza "tra i 3,5 e 7 metri di altezza"), tanto che la Fondazione ha "comunicato che sulla base di queste tarature tutte le tracce audio risultano composte quasi interamente da silenzio o indistinguibili brusii di sottofondo". Al riguardo, deve osservarsi che il Comune non ha prodotto in atti documentazione in grado di comprovare tale circostanza. L'asserita inadeguatezza dei microfoni a captare le conversazioni in maniera comprensibile non risulta, d'altra parte, coerente con lo scopo stesso del progetto, in relazione al quale il Comune ha beneficiato di finanziamenti. Il progetto "Marvel" prevedeva, infatti, espressamente la raccolta dell'audio delle conversazioni intercorse nella pubblica via. Tanto che nel documento "Rispetto dei requisiti etici stabiliti per la partecipazione di persone a progetti europei - MARVEL (Grant Agreement n° 957337) e PROTECTOR (Grant Agreement n° 101034216)", allegato all'accordo sulla protezione dei dati con la Fondazione (in atti), l'Ente si era premunito di specificare che "le conversazioni contenute nei dati audio non potranno in alcun modo essere oggetto di analisi garantendo la privacy dei cittadini". Infatti, la documentazione relativa al progetto esplicitava che "questo approccio [ovvero la sostituzione della voce del parlante, mantenendo quanto più inalterate possibile le caratteristiche del segnale audio, incluso il contenuto semantico del parlato], rispetto ad una eliminazione integrale delle conversazioni dal segnale audio, risponde all'obiettivo esplicitamente previsto nel Grant Agreement […] (descrizione del Task 3.1 del Work Package 3, pag. 20-21 dell'Annex 1 (part A) del Grant Agreement) di sviluppare tecniche di anonimizzazione poco intrusive che preservino il contesto acustico e permettano una efficace elaborazione dei segnali senza perdita di informazioni" (nota del XX; v. anche il documento "D2.1 Collection and analysis of experimental data", pagg. 57-58, in https://www.marvel-project.eu/deliverables/, ove si afferma che "l'anonimizzazione audio mira a rimuovere qualsiasi informazione sull'identità del parlante da un flusso audio [...] Tuttavia, la conversione vocale non rimuove il contenuto parlato dell'enunciato, che può potenzialmente contenere informazioni identificative (ad esempio, nomi/indirizzi/ecc.) e come tale potrebbe non essere la tecnica appropriata"; v. anche il documento "D3.3 E2F2C Privacy preservation mechanisms", pagg. 26-27, in https://www.marvel-project.eu/deliverables/, ove si afferma che "l'obiettivo finale dell'anonimizzazione audio [è quello di preservare] il contenuto del parlato [e di rimuovere] l'identità del parlante)".

Per quanto attiene ai file video utilizzati nell'ambito dei progetti "Marvel" e "Protector", il Comune ha affermato che la tecnica di anonimizzazione impiegata consiste unicamente nell'offuscamento dei volti delle persone e delle targhe dei veicoli ripresi. Anche in questo caso, tale tecnica non può ritenersi idonea ad assicurare l'effettiva anonimizzazione dei dati, atteso che gli interessati sono comunque potenzialmente identificabili tramite altre caratteristiche fisiche o elementi di contesto (come, ad esempio, corporatura, abbigliamento, posizione nella scena filmata, caratteristiche fisiche particolari, ecc.) o informazioni detenute da terzi (come, ad esempio, notizie di stampa relative a fatti di cronaca, informazioni fornite da persone presenti nella scena filmata, ecc.) o ancora informazioni desumibili, ad esempio, dalla localizzazione della telecamera (aree prospicenti determinati esercizi commerciali, studi medici o scuole) o, infine, informazioni relative al percorso effettuato da una determinata persona individuata nelle immagini video mediante le predette caratteristiche fisiche e gli elementi di contesto, stante la possibilità di seguire i suoi spostamenti fra le diverse telecamere installate.

Così come per le registrazioni audio, soltanto nelle memorie difensive - presentate dopo la notifica della violazione di cui all'art. 166, comma 5, del Codice, e non anche nel corso dell'istruttoria, nonostante le puntuali richieste d'informazioni rivolte

dall'Ufficio dell'Autorità - il Comune ha alluso alla circostanza che - in considerazione delle caratteristiche tecniche dei dispositivi impiegati ("risoluzione […] di 1200x1600 pixel"; "elevata compressione delle immagini, che genera […] una alterazione dei dettagli"; modalità a infrarossi in condizione di scarsa illuminazione, con conseguente funzionamento "a bianco e nero e con ridotto contrasto") e delle misure adottate (telecamere a "un'altezza tra i 3,5 e i 40 metri da terra"; angolo di visuale "dall'alto", con conseguente "distorsione prospettica") - non fosse "in concreto possibile riconoscere delle caratteristiche personali sufficienti per permettere di identificare univocamente i soggetti ritratti". Anche a tal riguardo, deve osservarsi che il Comune non ha prodotto in atti documentazione in grado di comprovare tale circostanza. L'asserita insufficiente qualità delle riprese video non risulta, d'altra parte, coerente con lo scopo stesso del progetto, in relazione al quale il Comune ha beneficiato di finanziamenti. La difesa dell'Ente risulta poi ulteriormente incoerente, atteso che i dispositivi video impiegati nell'ambito dei due progetti coincidono con le telecamere già installate dal Comune per finalità di sicurezza urbana, ovvero per la "prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria" (art. 5, comma 2, lett. a), del d.l. 20 febbraio 2017 , n. 14), dovendosi, pertanto, escludere che i filmati di videosorveglianza non fossero idonei - per qualità e livello di dettaglio - a consentire un'identificazione degli interessati, anche sulla base di elementi di contesto. D'altra parte, l'ottenimento di immagini a scarsa risoluzione, tale da non consentire all'osservatore di distinguere specifici elementi delle scene riprese, avrebbe certamente compromesso le stesse finalità del progetto e la possibilità di addestrare gli algoritmi di intelligenza artificiale a riconoscere situazioni di potenziale rischio per la pubblica sicurezza (si vedano, a tal riguardo, le dichiarazioni del Comune, rese nella nota del XX, in merito alle caratteristiche tecniche della piattaforma relativa al progetto "Protector", ovvero che la stessa dispone di una "componente di rilevamento automatico degli oggetti", di una "componente di tracciamento dei movimenti degli oggetti", di una "componente di rilevamento delle anomalie", funzionalità queste che il Comune non avrebbe potuto sfruttare in alcun modo nell'ambito del progetto a fronte di un segnale video di qualità talmente degradata da impedire non solo l'identificazione delle persone ma anche la comprensione degli elementi di contesto della scena ripresa).

Ciò chiarito, deve osservarsi che l'inadeguatezza delle predette tecniche a garantire una piena anonimizzazione dei dati era ben nota al Comune, tenuto conto che, come affermato nel corso dell'istruttoria, nella documentazione redatta ai fini delle valutazioni etiche e di protezione dei dati nell'ambito dei due progetti era stato evidenziato il rischio di identificazione degli interessati, ancorché erroneamente classificato come "basso". Inoltre, per quanto concerne i filmati, nell'atto di designazione della Fondazione quale responsabile del trattamento, redatto dal Comune, si afferma che, ai fini della identificazioni degli interessati, i cui volti sono sottoposti ad offuscamento, "chiaramente, potrebbero essere sfruttate altre caratteristiche, come ad esempio i vestiti, un particolare taglio di capelli, o la morfologia del corpo", sebbene tali caratteristiche non siano state erroneamente ritenute "sufficienti per identificare univocamente una persona rispetto ai tratti del viso".

Deve, a tal proposito, osservarsi che per "identificazione", "non si intende solo la possibilità di recuperare il nome e/o l'indirizzo di una persona, ma anche la potenziale identificabilità mediante individuazione, correlabilità e deduzione" (Gruppo di Lavoro Art. 29, "Parere 05/2014 sulle tecniche di anonimizzazione", WP216; cfr. anche provv. 18 luglio 2023, n. 311, doc. web n. 9920562; 2 marzo 2023, n. 65, doc. web n. 9874480; 25 febbraio 2021, n. 68, doc. web n. 9567429; 2 luglio 2020, n. 118 e 119, doc. web n. 9440042 e n. 9440025).

Peraltro, nel caso delle conversazioni, gli interessati possono essere direttamente identificati, allorquando nel discorso si faccia esplicitamente riferimento a una determinata persona, ad esempio menzionandone il nome e il cognome.

Con riferimento al trattamento, nell'ambito del progetto "Protector", dei messaggi pubblicati sulla piattaforma "Twitter" (ora denominata "X") e dei commenti pubblicati sulla piattaforma "YouTube", al fine di estrarre informazioni relative al contenuto d'odio o alle emozioni espresse, il Comune ha affermato che il contenuto di tali messaggi, una volta analizzato, è stato cancellato.

Anche i dati relativi agli utenti di "YouTube" (nomi utente), autori dei predetti commenti, sono stati immediatamente cancellati, mentre i dati relativi agli utenti di "Twitter" ("X") (nomi utente) sono stati soltanto pseudonimizzati, essendo stato sostituito ciascun nome utente reale con un "ID" generato casualmente e automaticamente. Pertanto, con riferimento alle reti di utenti su "Twitter" ("X"), coinvolti nella pubblicazione di messaggi d'odio, il Comune ha effettuato una mera pseudonimizzazione e non un'anonimizzazione.

A tal proposito, deve evidenziarsi che la disciplina in materia di protezione dei dati personali trova applicazione anche con riguardo ai dati oggetto di pseudonimizzazione, intendendosi per tale "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (cons. 26 e art. 4 punto 5 del Regolamento). Ciò significa che l'uso di "informazioni aggiuntive" può portare all'identificazione delle persone, motivo per cui i dati personali pseudonimizzati devono comunque considerarsi quali dati personali. In altri termini, la pseudonimizzazione, in quanto tecnica volta alla protezione del dato, non equivale ad anonimizzazione (v. il cons. 26 del Regolamento e l'art. 32, par. 1, lett. a), del Regolamento, ove si cita la "pseudonimizzazione" tra le possibili misure tecniche volte a garantire un livello di sicurezza adeguato al rischio; cfr. provv. 27 gennaio 2021, n. 34, doc. web n. 9549165). Pertanto, come recentemente ribadito dalla Corte di giustizia dell'Unione europea, "dall'articolo 4, punto 5, del [Regolamento], in combinato disposto con tale considerando 26 di tale regolamento, risulta che i dati personali che sono stati soltanto oggetto di pseudonimizzazione e che potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di informazioni supplementari devono essere considerati informazioni su una persona fisica identificabile, ai quali si applicano i principi relativi alla protezione dei dati" (sent. C-683/21, Nacionalinis visuomenės sveikatos centras, 5 dicembre 2023).

Il dato anonimo è, invece, tale solo se non consente in alcun modo l'identificazione diretta o indiretta di una persona, tenuto conto di tutti i mezzi (economici, informazioni, risorse tecnologiche, competenze, tempo) nella disponibilità di chi (titolare o altro soggetto) provi a utilizzare tali strumenti per identificare un interessato.

Peraltro, le Forze di polizia coinvolte nel progetto (Polizia Locale del Comune di Trento; Polizia di Anversa; Ministero dell'Interno della Bulgaria) hanno avuto accesso a una versione della piattaforma in cui le reti di utenti su Twitter ("X") potevano essere visualizzate con i nomi utente mostrati in chiaro, seppur senza alcuna informazione sul tipo di messaggi che questi utenti si sono scambiati (v. successivo par. 3.6).

Alla luce di tutte le considerazioni che precedono, deve concludersi che - diversamente da quanto prospettato dal Comune e nonostante le misure da esso adottate, per il tramite della Fondazione, al fine di ridurre il rischio di identificazione degli interessati - le registrazioni video, i file audio contenenti conversazioni e le informazioni relative alle reti di utenti sulla piattaforma "Twitter" ("X"), sottoposte a pseudonimizzazione, devono considerarsi informazioni relative a persone fisiche comunque identificabili, che, conseguentemente, costituiscono "dati personali" (art. 4, par. 1, n. 1), del Regolamento), il cui trattamento, per l'intero ciclo di vita del dato nell'ambito dei due progetti, avrebbe dovuto rispettare i principi di protezione dei dati (artt. 5 e 25 del Regolamento) e fondarsi su un'idonea base giuridica che potesse giustificare lo stesso (artt. 6, 9 e 10 del Regolamento; artt. 2-ter, 2-sexies e 2-opties del Codice).

3.4 La liceità e la correttezza del trattamento.

Il trattamento dei dati personali deve avvenire nel rispetto delle disposizioni del Regolamento e del Codice.

Per "dato personale" si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")". Inoltre, "si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4, par. 1, n. 1 del Regolamento).

Il trattamento di dati appartenenti a categorie particolari, tra i quali figurano i dati relativi alle convinzioni religiose (v. art. 9, par. 1, del Regolamento), è di regola vietato, fatte salve le eccezioni espressamente previste dall'art. 9, par. 2, del Regolamento.

In tale quadro, i soggetti pubblici, in conformità al principio di "liceità, correttezza e trasparenza" (art. 5, par. 1, lett. a), del Regolamento), possono trattare dati personali, anche relativi a categorie particolari di dati (cfr. art. 9, par. 1, del Regolamento), se il trattamento è 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), nonché art. 9, par. 2, lett. g), del Regolamento e 2-ter e 2-sexies del Codice).

Con specifico riguardo al trattamento dei dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza, si evidenzia che esso può avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati (art. 10 del Regolamento), ovvero solo qualora il trattamento sia autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento (art. 2-octies, commi 1 e 5, del Codice).

In relazione ai trattamenti di dati personali effettuati per il perseguimento di finalità di ricerca scientifica, trova applicazione l'art. 89 del Regolamento, ai sensi del quale "il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati", in base al quale i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. c), del Regolamento).

Per quanto concerne le attività di ricerca scientifica che hanno ad oggetto le particolari categorie di dati di cui all'art. 9 del Regolamento, il par. 2, lett. j), del medesimo articolo ammette che tali dati possano essere trattati per finalità di ricerca scientifica sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, in conformità al predetto art. 89, par. 1, del Regolamento.

Il trattamento dei dati personali per finalità di ricerca scientifica deve, in ogni caso, essere effettuato nel rispetto delle disposizioni del Codice (104 e ss.), delle Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (all. 5 al provv. 5 giugno 2019, n. 146, doc. web n. 9124510), nonché delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (all. A5 al Codice), che costituiscono condizione essenziale di liceità e correttezza dei trattamenti effettuati per tale finalità (v. artt. 2-quater e 106 del Codice e 21, comma 5, del d.lgs. 10 agosto 2018, n. 101).

Così brevemente riscostruito il quadro giuridico rilevante in materia di protezione dei dati, si evidenzia che il Comune ha sostenuto nel corso dell'istruttoria di aver impiegato le predette tecniche di anonimizzazione al fine di mitigare l'impatto dei due progetti sui diritti e le libertà fondamentali degli interessati, non essendo, pertanto, in discussione che il Comune abbia raccolto e trattato dati personali nell'ambito dei due progetti.

In merito ai presupposti di liceità del trattamento dei dati personali nell'ambito dei progetti "Marvel" e "Protector", il Comune ha affermato che "la base giuridica del trattamento è individuata nelle disposizioni di legge e statutarie (art. 2 legge regionale n. 2/2018, artt. 3 e 7 Statuto del Comune […]) che annoverano tra le funzioni amministrative di interesse locale attribuite ai comuni lo sviluppo culturale, sociale ed economico della popolazione, al quale è certamente riconducibile lo sviluppo del programma "Trento Smart city" (quale progetto strategico del Comune), in cui rientrano i [predetti tre] progetti […]".

Le predette disposizioni, che attribuiscono al Comune una competenza del tutto generica e meramente programmatica ai fini della promozione dello sviluppo culturale, sociale ed economico della popolazione, non possono ritenersi idonee a soddisfare i requisiti di qualità della base giuridica ai fini degli artt. 5, par. 1, lett. a), 6, par. 1, lett. e), e parr. 2 e 3, e 9, par. 2, lett. g), del Regolamento (v. anche cons. 41), nonché 2-ter, 2-sexies e 2-octies del Codice.

Come, infatti, affermato dalla Corte di giustizia dell'unione europea, ai sensi dell'art. 52, par. 1, prima frase, della Carta dei diritti fondamentali dell'Unione europea ("CDFUE"), eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima, che comprendono, segnatamente, il diritto al rispetto della vita privata, garantito dall'art. 7 della Carta, e il diritto alla protezione dei dati di carattere personale, sancito dall'art. 8 della Carta, devono essere previste dalla legge, il che implica, in particolare, che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato. In particolare, "per soddisfare il requisito di proporzionalità, che trova espressione nell'articolo 5, paragrafo 1, lettera c), del regolamento […] la normativa su cui si fonda il trattamento deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura [prevista] e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente [i] dati contro il rischio di abusi. Tale normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che preveda il trattamento di tali dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario" (sent. C-175/20, Valsts ieņēmumu dienests, 24 febbraio 2022, par. 83).

A tal proposito, la Corte ha, inoltre, affermato che la normativa recante una misura che consenta un'ingerenza siffatta deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissino requisiti minimi, di modo che le persone i cui dati personali siano stati trattati dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abusi (v. C-175/20, cit., par. 55; v. art. 6, par. 3, del Regolamento, nonché cons. 45 dello stesso; con riguardo a casi affrontati dal Garante in ambito pubblico in relazione al tema della base giuridica e ai presupposti di liceità per il trattamento di dati personali mediante di sistemi di intelligenza artificiale o, più in generale, di nuove tecnologie basate su logiche algoritmiche, v., tra gli altri, provv.ti 13 aprile 2023, nn. 122 e 123, doc. web nn. 9896808 e 9896412; 30 luglio 2022, n. 276, doc. web n. 9808839; 24 febbraio 2022, n. 78, doc. web n. 9751895; 22 dicembre 2021, n. 453, doc. web n. 9738520; 16 settembre 2021, n. 317, doc. web n. 9703988).

Inoltre, eventuali limitazioni ai diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali (e artt. 7 e 8 della CDFUE) "possono […] essere apportate, [oltre che] a condizione che, conformemente all'articolo 52, paragrafo 1, della Carta, esse siano previste dalla legge" e "rispettino il contenuto essenziale dei diritti fondamentali nonché il principio di proporzionalità. In virtù di tale principio, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a obiettivi di interesse generale riconosciuti dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Esse devono operare nei limiti dello stretto necessario e la normativa che comporta l'ingerenza deve prevedere norme chiare e precise che disciplinano la portata e l'applicazione della misura in questione" (C-184/20, Vyriausioji tarnybinės etikos komisija, 1° agosto 2022, par. 64).

Analogamente, la Corte Europea dei Diritti dell'Uomo ha in più occasioni ribadito che "un'ingerenza [nel diritto al rispetto della vita privata e familiare] può essere giustificata ai sensi dell'articolo 8, paragrafo 2 [della Convenzione europea dei diritti dell'uomo – "CEDU"], solo se essa è conforme alla legge, se persegue uno o più degli obiettivi legittimi a cui si riferisce il paragrafo 2 dell'articolo 8 e se è necessaria in una società democratica per raggiungere tali obiettivi" ("Glukhin v. Russia", "application no. 11519/20", 4 luglio 2023, par. 75). Tale ingerenza si verifica anche allorquando siano impiegati dispositivi video in luoghi pubblici che prevedono la registrazione delle immagini ("Peck v. United Kingdom", "Application no. 44647/9", 28 gennaio 2003, punto 59; v. anche, ancorché in un contesto diverso, "Perry v. United Kingdom", "application no. 63737/00", 17 luglio 2003, punto 38).

La legge deve in ogni caso soddisfare i necessari requisiti di "qualità" della base giuridica, con la conseguenza che "nel contesto della raccolta e del trattamento dei dati personali, è pertanto essenziale disporre di norme chiare e dettagliate che disciplinino l'ambito e l'applicazione delle misure, nonché di garanzie minime riguardanti, tra l'altro, la durata, l'archiviazione, l'utilizzo, l'accesso di terzi, le procedure per preservare l'integrità e la riservatezza dei dati e le procedure per la loro distruzione, fornendo così garanzie sufficienti contro il rischio di abuso e arbitrarietà" ("Glukhin v. Russia", cit., par. 77). Ciò tenendo, altresì, conto che "la necessità di tali garanzie [, volte a impedire qualsiasi uso dei dati personali che possa essere in contrasto con le garanzie di all'art. 8 della CEDU], è ancora maggiore quando si tratta di proteggere i dati personali sottoposti a trattamento automatizzato […] e soprattutto quando la tecnologia disponibile diventa sempre più sofisticata" (ibidem, par. 75).

Oltre che contemplata dalla legge, ogni ingerenza da parte delle pubbliche autorità nei diritti fondamentali delle persone, tra i quali il diritto alla protezione della vita privata, deve essere, infatti, prevedibile, nel senso che la legge deve essere sufficientemente chiara nei suoi termini per dare ai singoli un'indicazione adeguata sulle circostanze e le condizioni in cui le autorità sono autorizzate a ricorrere alle misure previste dalla legge (v. "Copland v. United Kingdom", "Application no. 62617/00", 3 aprile 2007, par. 46).

È, peraltro, irrilevante che l'ingerenza riguardi attività o condotte che si svolgono in un luogo pubblico. Come, infatti, anche di recente ribadito dalla Corte Europea dei Diritti dell'Uomo, "il concetto di "vita privata" è un ampio e non suscettibile di una definizione esaustiva [e] non esclude le attività che si svolgono in un contesto pubblico", atteso che "esiste […] una zona di interazione di una persona con gli altri, anche in un contesto pubblico, che può rientrare nell'ambito della "vita privata" ("Glukhin v. Russia", cit., par. 64; v. anche sentenza "Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland", "application no. 931/13", 27 giugno 2017, parr. 129-131)

Le considerazioni sopra riportate, corroborate dalla giurisprudenza delle due Corti, valgono anche in relazione a forme di ingerenza da parte delle pubbliche autorità che sono prospettate ai consociati come soltanto meramente propedeutiche allo sviluppo di nuove tecnologie, come, nel caso di specie, l'addestramento di algoritmi di intelligenza artificiale (v. a tal riguardo, ancorché con riferimento all'utilizzo di sistemi di riconoscimento facciale per finalità di polizia, le "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement", adottate dal Comitato europeo per la protezione dei dati il 26 aprile 2023, ove si evidenzia che "l'articolo 52, paragrafo 1, della Carta stabilisce il requisito di una base giuridica specifica. Tale base giuridica deve essere sufficientemente chiara nei suoi termini per fornire ai cittadini un'indicazione adeguata delle condizioni e delle circostanze in cui le autorità sono autorizzate a ricorrere a qualsiasi misura di raccolta di dati e sorveglianza segreta. Deve indicare con ragionevole chiarezza l'ambito e le modalità di esercizio del relativo potere discrezionale conferito alle autorità pubbliche, in modo da garantire alle persone il grado minimo di protezione previsto dallo Stato di diritto in una società democratica. Inoltre, la legittimità richiede adeguate garanzie per assicurare, in particolare, il rispetto dei diritti dell'individuo ai sensi dell'articolo 8 della [CDFUE]. Questi principi si applicano anche al trattamento dei dati personali ai fini della valutazione, dell'addestramento e dell'ulteriore sviluppo dei sistemi [di riconoscimento facciale]"; con riguardo ai requisiti di qualità della base giuridica, nel diverso contesto sanitario, v. anche il recente "Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale", adottato dall'Autorità il 10 ottobre 2023, doc. web n. 9938038, par. 1; v., altresì, i provv.ti 13 aprile 2023, nn. 122 e 123, cit., relativi al trattamento, da parte di soggetti pubblici, in assenza di idonea base giuridica, di dati personali contenuti in filmati ottenuti mediante dispositivi video, nell'ambito di un progetto che prevedeva l'impiego di algoritmi di rilevamento dei volti basati su reti neurali convoluzionali).

Nel caso di specie, come sopra evidenziato, non è stata comprovata la sussistenza di alcun quadro giuridico, idoneo per rango e qualità, a giustificare i trattamenti di dati personali posti in essere da un soggetto pubblico, quale il Comune, titolare del trattamento, nell'ambito dei progetti di ricerca scientifica "Marvel" e "Protector", e la conseguenza ingerenza nei diritti e nelle libertà fondamentali delle persone i cui dati sono stati raccolti e trattati.

Il Comune ha, infatti, dichiarato di aver confidato in buona fede che i trattamenti in questione potessero essere ricondotti al quadro giuridico in materia di sicurezza urbana. Tuttavia, diversamente da quanto ritenuto dall'Ente, l'art. 5, comma 2, lett. a), del d.l. 20 febbraio 2017, n. 14, consente ai Comuni "l'installazione di sistemi di videosorveglianza" ai soli fini di "prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria", previa stipula di un accordo per l'attuazione della sicurezza urbana con la Prefettura territorialmente compente. Tale disciplina di settore - che in ogni caso non contempla l'utilizzo di microfoni per l'acquisizione del segnale audio - prevede, pertanto, uno specifico vincolo di finalità del trattamento (v. art. 5, par. 1, lett. b), del Regolamento), non essendo, pertanto, di regola ammesso l'utilizzo delle immagini di videosorveglianza, da parte degli Enti locali, per finalità di trattamento ulteriori, specialmente nel caso in cui esso si ponga in contrasto con la ragionevole aspettativa degli interessati (v., in tal senso, proprio con riferimento all'ambito della videosorveglianza per finalità di sicurezza urbana, provv. 20 ottobre 2022, n. 341, doc. web n. 9831369).

Il Comune ha, altresì, invocato l'art. 2-ter, comma 1-bis, del Codice, sul presupposto che i trattamenti posti in essere siano necessari per l'esercizio delle funzioni istituzionali dell'Ente. A tal proposito, deve evidenziarsi che tale disposizione del Codice impone comunque il "rispetto dell'articolo 6 del Regolamento" e, pertanto, anche i requisiti di qualità della base giuridica di cui ai parr. 2 e 3, che, come sopra detto, non si rinvengono nelle generiche disposizioni indicate dal Comune. L'art. 2-ter del Codice non trova poi, in ogni caso, applicazione al trattamento di dati relativi a categorie particolari.

Si rileva poi che il Comune ha considerato "pertinenti le disposizioni dell'Allegato A.5 del [Codice] contenente le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, in conformità all'art. 89 del GDPR", seppur avendo precisato di non ritenere che tali disposizioni costituiscano "una base giuridica propria del Comune". In altri termini, il Comune avrebbe recepito i principi e le regole di condotta di cui alle predette Regole deontologiche, ai fini della definizione delle modalità di svolgimento dei due progetti, senza riconoscere la diretta applicabilità delle stesse al caso di specie.

A tal proposito, si osserva che il Comune non ha comprovato che tra le proprie competenze istituzionali figuri anche l'attività di ricerca scientifica, non potendo, pertanto, lo stesso essere considerato un "istituto o ente di ricerca" ai fini dell'art. 1, par. 1, lett. d), delle predette Regole deontologiche; né il Comune ha comprovato di aver agito, nell'ambito dei due progetti, attraverso il proprio Ufficio di statistica, istituito ai sensi del d.lgs. 322/1989. La finalità di ricerca scientifica non è annoverata tra le competenze istituzionali del Comune e, pertanto, i trattamenti di dati personali in questione non possono ritenersi autorizzati ai sensi del quadro giuridico europeo e nazionale che definisce, tra le altre, i presupposti soggettivi e oggettivi per effettuarli (v. artt. 6 e 89 del Regolamento; art. 106 del Codice; Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica).

A ciò si aggiunga che tra i criteri individuati a livello internazionale e nazionale per riconoscere la natura di ente di ricerca in capo a un determinato soggetto vi è, in primo luogo, lo scopo istituzionale perseguito, che deve contenere un riferimento all'attività di ricerca, individuato sulla base di quanto indicato nella legge o in altro atto istitutivo dell'organizzazione, oppure nello statuto, regolamento o altro atto organizzativo (cfr. art. 5-ter del d.lgs. 14 marzo 2013, n. 33 e le Linee guida, adottate in attuazione del relativo comma 3, dal Comitato di indirizzo e coordinamento dell'informazione statistica – Comstat; cfr. parere del Garante adottato con provv. 21 giugno 2018, n. 388, doc. web n. 9023239). Con particolare riferimento alle particolari categorie di dati (art. 9 del Regolamento) e ai dati relativi a reati (art. 10 del Regolamento), il Comune non ha, altresì, indicato alcun quadro giuridico che preveda espressamente e disciplini in dettaglio i tipi di dati, le operazioni eseguibili e le misure appropriate e specifiche da adottare in relazione ai trattamenti effettuati per le attività di ricerca scientifica svolte nell'ambito dei predetti progetti, difettando, pertanto, anche sotto tale profilo, le condizioni di liceità previste dagli art. 9, par. 1, lett. g) e j), e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice.

Né possono assumere rilevanza gli accordi contrattuali stipulati tra il Comune, gli altri partner dei progetti e la Commissione europea. Si osserva, infatti, a tal proposito, che tali accordi attribuiscono ai beneficiari delle sovvenzioni la responsabilità di

assicurare il rispetto della normativa in materia di protezione dei dati (v. art. 39.2 del "Grant Agreement" relativo al progetto Marvel e art. 23.2 del "Grant Agreement" relativo al progetto "Protector"; v. anche l'art. 4.4 del "Consortium Agreement" relativo al progetto "Marvel", ove si legge che "ciascuna Parte è tenuta a garantire che la raccolta, il trattamento e la condivisione dei dati personali e/o di categorie particolari di dati personali siano conformi al Regolamento […] e ad altre normative […] in materia di dati personali. Le Parti garantiranno pertanto la sussistenza di una base giuridica […] in conformità con il GDPR prima di condividere qualsiasi dato personale e/o categorie speciali di dati personali", nonché l'art. 10.8 del "Consortium Agreement" relativo al progetto "Protector", ove si legge che "le Parti devono trattare i dati personali in conformità alle leggi nazionali e dell'UE applicabili in materia di protezione dei dati (compresi, a titolo esemplificativo e non esaustivo, gli obblighi di autorizzazione o notifica). Ciascuna Parte dichiara e garantisce che tutti i dati personali richiesti per l'utilizzo nel Progetto e da essa raccolti, trattati o ulteriormente utilizzati saranno raccolti, trattati o ulteriormente utilizzati in conformità con tutte le leggi e i regolamenti pertinenti (e, se del caso, con le linee guida etiche locali) in materia di raccolta, utilizzo, trasporto e successiva distruzione dei dati personali").

Alla luce delle considerazioni che precedono, deve concludersi che il Comune, nell'ambito dei progetti "Marvel" e "Protector", ha trattato dati personali, anche relativi a reati e appartenenti a categorie particolari (convinzioni religiose), contravvenendo alla ragionevole aspettativa di riservatezza degli interessati, in maniera non conforme al "principio di liceità, correttezza e trasparenza" e in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice.

3.5 La trasparenza del trattamento.

Nel rispetto del principio di "liceità, correttezza e trasparenza", il titolare del trattamento deve adottare misure appropriate per fornire all'interessato, prima di iniziare il trattamento, tutte le informazioni richieste dal Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (artt. 5, par. 1, lett. a), 12, 13 e 14 del Regolamento).

Allorquando siano impiegati sistemi di videosorveglianza, il titolare del trattamento, oltre a rendere l'informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve fornire agli interessati anche delle "informazioni di secondo livello", che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]" ed "essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale […] o affissa in un luogo di facile accesso" (Comitato europeo per la protezione dei dati, "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", del 29 gennaio 2020, in particolare par. 7; ma si veda già il "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010, doc. web n. 1712680, in particolare par. 3.1, nonché, da ultimo, la FAQ del Garante n. 4 in materia di videosorveglianza, doc. web n. 9496574; cfr., altresì, provv.ti 20 ottobre 2022, n. 341, doc. web n. 9831369; 28 aprile 2022, n. 162, doc. web n. 9777974, 7 aprile 2022, n. 119, doc. web n. 9773950, 16 settembre 2021, n. 327, doc. web n. 9705650 e 11 marzo 2021, n. 90, doc. web n. 9582791).

Le informazioni di primo livello (cartello di avvertimento) "dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento" (Linee guida del Comitato, cit., par. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato. Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi) (Linee guida del Comitato, cit., par. 115). La segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

Nel corso dell'istruttoria, il Comune ha sostenuto di aver adempiuto gli obblighi informativi nei confronti degli interessati installando dei cartelli, contenenti un'informativa di primo livello sul trattamento dei dati (v. all. 1 alla nota prot. n. XX del XX), in prossimità delle telecamere e dei microfoni collocati nella pubblica via, nonché pubblicando un'informativa estesa sul trattamento dei dati sul proprio sito web istituzionale (https://www.comune.trento.it/content/download/1465552/13956310/file/INFORMATIVA%20PUBBLICO%20MARVEL_Rivista-1.pdf, come riportato nella predetta nota del XX).

Con riferimento all'informativa sul trattamento dei dati di primo livello, si rileva che la stessa, pur menzionando i progetti "Marvel" e "Protector" ("è ammessa la conservazione per un periodo massimo di sei mesi decorrenti dalla data della rilevazione, in relazione alle finalità di tutela della sicurezza urbana connesse allo sviluppo dei progetti europei Marvel (grant agreement n° 957337) e Protector (grant agreement n° 101034216) e di ulteriori progetti finanziati dall'unione europea"), non fa specificamente riferimento alla finalità di trattamento connessa alla ricerca scientifica, lasciando erroneamente intendere agli interessati che anche i trattamenti di dati personali, posti in essere nell'ambito dei due progetti, siano riconducibili alle finalità di sicurezza urbana; tanto che, nelle proprie memorie difensive, il Comune ha preso atto del "possibile fraintendimento ingenerato nei cittadini conseguente al fatto che non sarebbe risultata chiara la finalità del trattamento dei dati" e ha fatto presente la propria intenzione di "adeguare l'informativa che si renderà necessario utilizzare per le future occorrenze". Né può essere accolta la difesa del Comune, secondo la quale "nelle informative […] sono state individuate ed esplicitate in relazione alla base giuridica del trattamento ritenuta rilevante", atteso che, come sopra illustrato, il Comune ha posto in essere trattamenti di dati personali per una specifica finalità di trattamento, ovvero la ricerca scientifica, distinta da quella di sicurezza urbana, il cui quadro giuridico di riferimento (d.l. 20 febbraio 2017, n. 14), come detto, non è applicabile al contesto in questione. La condotta del Comune ha, pertanto, comportato la violazione dell'art. 13, par. 1, lett. c), del Regolamento

Inoltre, per quanto l'informativa contenga un riferimento all'audio, gli interessati non sono stati messi in condizione di comprendere che anche il contenuto delle proprie conversazioni sarebbe stato acquisito e trattato ai fini del progetto Marvel, aspetto che è certamente da considerarsi uno degli impatti più consistenti del trattamento. Anche in relazione a tale profilo, non può accogliersi l'argomento utilizzato dal Comune in sede di memoria difensiva, ovvero che "la mancata indicazione nell'informativa del fatto che la strumentazione fosse in grado di captare anche le conversazioni delle persone, è giustificabile anche dal fatto che, per le caratteristiche intrinseche del sistema di registrazione (come sopra descritto) l'effettiva possibilità di udire rilevanti contenuti semantici era da considerarsi una eventualità pressoché nulla", tenuto conto che, come sopra diffusamente illustrato, la possibilità di acquisire il contenuto di conversazioni non era comunque in radice esclusa e che, nella documentazione relativa al progetto, l'acquisizione di tale contenuto costituiva uno specifico elemento di interesse ai fini dell'addestramento degli algoritmi di intelligenza artificiale volti al riconoscimento di situazioni di pericolo per la pubblica sicurezza.

Quanto ai tempi di conservazione dei dati, nel cartello in questione si legge che "i dati audio e video sono conservati per un periodo di sette giorni decorrenti dalla data della rilevazione", ragionevolmente con riferimento alla finalità di sicurezza urbana. Al tal proposito, si deve rilevare che l'art. 7, comma 8, del d.l. 23 febbraio 2009 consente "la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione". Tale termine non può, invece, trovare applicazione in relazione all'audio, la cui raccolta non è consentita dal quadro normativo in materia di videosorveglianza per finalità di sicurezza urbana. Con specifico riguardo ai progetti "Marvel" e "Protector", nel medesimo cartello si afferma che "è ammessa la conservazione per un periodo massimo di sei mesi decorrenti dalla data della rilevazione", termine che non trova, tuttavia, riscontro nelle dichiarazioni rese dal Comune nel corso dell'istruttoria e che risulta comunque incongruente rispetto all'asserita immediata anonimizzazione dei dati. Risulta, pertanto, violato l'art. 13, par. 2, lett. a), del Regolamento.

In merito alla menzione dei diritti degli interessati, l'informativa di primo livello si limita a menzionare il solo diritto di accesso ai dati, facendo un generico riferimento agli "altri diritti riconosciuti dalla legge", senza un espresso rinvio agli artt. 15-22 del Regolamento, risultando conseguentemente violato anche l'art. 13, par. 2, lett. b), del Regolamento. Deve, infatti, evidenziarsi che la menzione in forma sintetica nell'informativa di primo livello dei diritti degli interessati è consentita solo nella misura in cui il cartello contenga un chiaro riferimento all'informativa estesa di secondo livello per un'illustrazione completa di tali diritti (v. il cartello informativo esemplificativo proposto dal Comitato europeo per la protezione dei dati al par. 116 delle richiamate "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", ove si legge che "in qualità di interessato, puoi esercitare diversi diritti, in particolare il diritto di richiedere al titolare del trattamento l'accesso o la cancellazione dei dati personali. Per maggiori informazioni sulla videosorveglianza e sui tuoi diritti, consulta l'informativa completa fornita dal titolare […]" (v. anche l'analogo cartello esemplificativo pubblicato sul sito web del Garante in data 3 dicembre 2020, doc. web n. 9496244). Nel caso di specie, il Comune ha, invece, omesso di fornire agli interessati chiare indicazioni in merito alle modalità con la quali gli interessati avrebbero potuto consultare l'informativa completa sul trattamento dei dati personali.

Infatti, nel far presente la possibilità di consultare "l'informativa completa sul trattamento dei dati personali", oltre che presso la sede del Comune, il cartello informativo di primo livello rimanda al "sito internet istituzionale del Comune", senza indicare la specifica pagina/sezione di tale sito su cui l'informativa completa può essere reperita, così, di fatto, ostacolando la possibilità per gli interessati di accedere alla stessa (si veda, peraltro, il cartello informativo proposto, a titolo esemplificativo, ai punti 115-116 delle predette Linee guida del Comitato, in cui si prospetta anche la possibilità - senza che sussista un obbligo al riguardo - di inserire un c.d. "QR Code", proprio allo scopo di facilitare la possibilità per gli interessati di accedere rapidamente e agevolmente all'informativa di secondo livello).

In merito, invece, all'informativa di secondo livello, si osserva che la stessa fa riferimento "al trattamento dei dati personali acquisiti mediante utilizzo degli impianti di videosorveglianza di proprietà del Comune […] impiegati per lo sviluppo dei Progetti Europei MARVEL (Grant Agreement n° 957337) e PROTECTOR (Grant Agreement n° 101034216)", senza menzionare i microfoni impiegati nell'ambito del progetto "Marvel" per la raccolta dell'audio.

Peraltro, nel far riferimento, in prosieguo, alle "sorgenti video/audio", si omette di specificare che l'audio potrebbe riguardare anche le conversazioni intercorse tra le persone presenti sulla pubblica via, aspetto che è certamente da considerarsi uno degli impatti più consistenti del trattamento.

L'informativa omette poi del tutto di illustrare i trattamenti di dati personali che riguardano gli utenti che hanno pubblicato messaggi sulla piattaforma "Twitter" (X) o commenti sulla piattaforma "YouTube" nell'ambito del progetto "Protector", anche per quanto concerne la comunicazione delle informazioni relative alle reti di utenti "Twitter" (X) alla Polizia di Anversa e al Ministero dell'Interno della Bulgaria, nonché al trattamento delle medesime informazioni da parte delle Polizia Locale del Comune. In riferimento a tali interessati, ovvero agli autori dei predetti messaggi/commenti, risulta, pertanto, complessivamente violato l'art. 14 del Regolamento, tenuto conto che tali dati personali non sono raccolti presso gli interessati.

Quanto alla base giuridica del trattamento, l'informativa riporta che "il trattamento è effettuato per l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6 del regolamento UE n. 2016/679", base giuridica che, per le ragioni sopra illustrate, non è applicabile in riferimento ai progetti di ricerca "Marvel" e "Protector". L'informativa prospetta, peraltro, il conferimento dei dati come obbligatorio, sull'erroneo presupposto che nell'ambito dei due progetti sarebbero perseguite "finalità di tutela della sicurezza urbana e del patrimonio pubblico, ai sensi di quanto previsto dall'art. 6, commi 7 e 8, del decreto legge 23 febbraio 2009 n. 11 (convertito con legge 23 aprile 2009 n. 38) e dall'art. 3, comma 2, del regolamento per l'utilizzo degli impianti di videosorveglianza". Risulta, pertanto, violato l'art. 13, par. 1, lett. c), del Regolamento.

Per quanto concerne l'ambito di comunicazione dei dati, il Comune, sul presupposto di aver impiegato adeguate tecniche di anonimizzazione dei dati, ha omesso di informare gli interessati che i propri dati personali sono condivisi con gli altri partner dei progetti e, per quanto attiene al progetto "Protector", con la Commissione europea e i revisori di progetto, in violazione dell'art. 13, par. 1, lett. e), del Regolamento.

Da ultimo, si rileva che la sezione "diritti dell'interessato", non contiene alcun riferimento al diritto degli interessati di "proporre reclamo a un'autorità di controllo", in violazione dell'art. 13, par. 2, lett. d), del Regolamento).

In relazione al "termine di conservazione dei dati", si afferma che "i dati sono conservati per un periodo di tempo non superiore a sei mesi decorrenti dalla data di rilevazione"; valgono, pertanto, i medesimi rilievi già effettuati con riguardo all'informativa di primo livello, con la conseguenza che risulta violato l'art. 13, par. 2, lett. a), del Regolamento.

Tenuto conto di tutte considerazioni che precedono, risulta accertato che il Comune ha agito in violazione degli artt. 13, par. 1, lett. c) ed e), par. 2, lett. a), b) e d), e 14 del Regolamento.

Alla luce della gravità, del carattere trasversale e delle conseguenze delle violazioni commesse dal Comune per quanto attiene alla trasparenza del trattamento, con particolare riferimento all'omissione di informazioni di dettaglio in merito al trattamento del contenuto delle conversazioni e alla totale assenza di informazioni destinate agli utenti di "Twitter"("X") e "YouTube", si ritiene che, nel caso di specie, il Comune abbia, altresì, agito in maniera non conforme al principio di "liceità, correttezza e trasparenza", in violazione dell'art. 5, par. 1, lett. a), del Regolamento.

3.6 L'ambito di comunicazione dei dati.

Nel corso dell'istruttoria, il Comune ha affermato che i contenuti audio-video utilizzati nell'ambito del progetto "Marvel", asseritamente anonimizzati, vengono condivisi con i partner del progetto, mentre, nell'ambito del progetto "Protector", tali contenuti, così come i nomi utente pseudonimizzati degli autori dei messaggi/commenti pubblicati sulle piattaforme "Twitter"("X") e "YouTube", vengono condivisi, oltre che con i partner, anche con la Commissione europea e i revisori del progetto.

Tenuto conto di quanto sopra illustrato in relazione all'inadeguatezza delle tecniche di anonimizzazione impiegate (v. par. 3.3), alla natura di dati personali delle informazioni pseudonimizzate (ibidem) e all'assenza di quadro giuridico di riferimento ai fini della conduzione dei due progetti di ricerca (v. par. 3.4), la comunicazione dei dati personali in questione, anche relativi a reati e categorie particolari di dati (convinzioni religiose), è avvenuta in maniera non conforme al principio di "liceità, correttezza e trasparenza" e in assenza di una base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice.

Ciò anche considerato che la presenza di un determinato utente all'interno di una rete di utenti implica che lo stesso abbia pubblicato dei messaggi di odio in ambito religioso (che sono peraltro liberamente consultabili sul profilo dell'utente), con la conseguenza che la comunicazione in questione ha ad oggetto anche dati personali relativi a reati e a categorie particolari di dati (convinzioni religiose).

Inoltre, nell'ambito del progetto Protector, i nomi utente degli autori dei messaggi pubblicati sulla piattaforma "Twitter"("X"), che costituiscono una rete, sono stati condivisi in chiaro con la Polizia di Anversa e con il Ministero dell'Interno della Bulgaria; pertanto, il Comune ha agito, anche in relazione a detto trattamento, in maniera non conforme al principio di "liceità, correttezza e trasparenza" e in assenza di una base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice.

3.7 La valutazione d'impatto sulla protezione dei dati.

In caso di rischi elevati per gli interessati - derivanti, ad esempio, dall'utilizzo di nuove tecnologie e sempre presenti laddove sia effettuata una sorveglianza sistematica su larga scala di una zona accessibile al pubblico (v. art. 34, par. 3, lett. c), del Regolamento) - il titolare del trattamento deve inoltre 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, par. 1, del Regolamento).

Nel caso di specie, il Comune era certamente soggetto all'obbligo di redigere una valutazione d'impatto sulla protezione dei dati, ai sensi dell'art. 36 del Regolamento, prima di avviare i trattamenti connessi ai progetti "Marvel" e "Protector".

Ciò, anzitutto, considerato che, ai sensi dell'art. 35, par. 3, lett. c), del Regolamento, la valutazione d'impatto è sempre richiesta in caso di "sorveglianza sistematica su larga scala di una zona accessibile al pubblico", circostanza che ricorre nel caso di specie, stante l'impiego di telecamere di videosorveglianza e di microfoni installati sulla pubblica via.

Più in generale, non vi dubbio che, tenuto conto, in particolare, dell'utilizzo di nuove tecnologie, come le tecniche di intelligenza artificiale, e della natura dei dati oggetto di trattamento (contenuto delle conversazioni; dati relativi a reati; dati relativi alle convinzioni religiose), il Comune avesse l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati (v. art. 35, par. 1, del Regolamento; cfr. Gruppo di lavoro art. 29, "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", del 4 aprile 2017, in particolare sez. III, ove si chiarisce che una valutazione d'impatto sulla protezione dei dati è richiesta allorquando sussistano almeno due dei nove criteri ivi indicati, che, nel caso di specie, possono rinvenirsi nel "monitoraggio

sistematico", nei "dati sensibili o dati aventi carattere altamente personale", nel "trattamento di dati su larga scala" e nell'"uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative".

Ciò chiarito, si osserva che il Comune ha dichiarato di aver redatto una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento e ha prodotto in atti un documento, denominato "VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI - T-08-012 - Trattamento progetti di ricerca per lo sviluppo di sistemi di videosorveglianza intelligente".

Tale documento risulta essere privo di data e non reca la sottoscrizione né del legale rappresentante del Comune né di altro soggetto a tal fine autorizzato, circostanze che non consentono di verificare che il documento in questione sia stato redatto prima della data di inizio del trattamento e di attribuire lo stesso all'Ente.

A tal proposito, il Comune ha affermato nelle proprie memorie difensive che la valutazione d'impatto sarebbe stata completata "già in data 19 gennaio 2022 (quando è stata condivisa per la prima volta con il DPO […])" e che la stessa sarebbe stata "successivamente inserita nell'applicativo informatico contenente il registro delle attività di trattamento […] nel marzo 2023, solo dopo aver ottenuto il parere definitivo del DPO". Per quanto il Comune ritenga "di aver [pertanto] documentato il fatto che il Comune aveva provveduto ad effettuare la valutazione di impatto prima dell'inizio dei trattamenti (febbraio 2022 per la parte video, marzo 2023 per la parte audio) e che la valutazione stessa è riconducibile all'Ente), deve, invece, osservarsi che l'Ente non ha prodotto alcuna evidenza volta a comprovare l'effettivo inserimento del documento in questione "nell'applicativo informatico contenente il registro delle attività di trattamento" e che tale procedura fosse idonea ad attribuire data certa al documento. In ogni caso, risulta confermata la circostanza che tale documento non è stato validamente sottoscritto dal Sindaco o da altro soggetto munito dei necessari poteri ai fini della necessaria assunzione di responsabilità in merito a quanto in esso rappresentato.

Alla luce delle considerazioni che precedono, si conferma che il Comune non ha comprovato di aver redatto una valutazione d'impatto sulla protezione dei dati prima di porre in essere i trattamenti di dati personali nell'ambito dei progetti "Marvel" e "Protector".

Si osserva poi che, in ogni caso, il documento in questione ha ad oggetto esclusivamente i trattamenti di dati personali connessi all'impiego di "sistemi di videosorveglianza intelligente" e, pertanto, lo stesso non prende in considerazione i trattamenti effettuati nell'ambito del progetto "Protector" con riferimento ai dati personali degli utenti di "Twitter"("X") e YouTube.

Tale documento risulta, più in generale, inidoneo a soddisfare i requisiti di cui all'art. 35, par. 7, del Regolamento, atteso che i progetti "Marvel" e "Protector", di cui non si fa espressa menzione, non vengono puntualmente descritti (v. art. 35, par. 7, lett. a), del Regolamento).

Il documento non contiene, inoltre, alcuna valutazione in merito alla "necessità e proporzionalità dei trattamenti in relazione alle finalità" e in particolare non illustra le ragioni per le quali il Comune non avrebbe potuto condurre i progetti di ricerca scientifica in questione in ambienti urbani simulati, ovvero senza raccogliere e trattare i dati personali delle persone realmente presenti nella pubblica via oppure senza trattare determinate tipologie di dati caratterizzati da particolare delicatezza, come il contenuto delle conversazioni (v. art. 35, par. 7, lett. b), del Regolamento).

La valutazione d'impatto si limita poi a considerare unicamente le possibili violazioni o minacce della sicurezza dei dati, peraltro in riferimento a sistemi informatici e banche dati che non sono chiaramente individuati e descritti, risultando l'analisi effettuata del tutto generica e avulsa dagli effettivi mezzi del trattamento, anche molto sofisticati sotto il profilo tecnologico, impiegati nei due progetti in questione, risultando, pertanto, impossibile comprendere l'effettivo rischio incombente in termini di sicurezza dei dati e l'idoneità delle misure attuate dal titolare per mitigare lo stesso (art. 35, par. 1, lett. d), del Regolamento).

Il documento non prende, invece, in alcun modo in considerazione gli altri rischi per i diritti e le libertà degli interessati (art. 35, par. 1, lett. c), del Regolamento) non connessi alla sicurezza fisica e logica dei dati, specialmente per quanto concerne le possibili conseguenze per gli interessati derivanti dal trattamento di informazioni particolarmente delicate quali il contenuto delle conversazioni, i dati relativi a reati e quelli relativi alle convinzioni religiose. Né vengono analizzate le misure adottate per mitigare tali rischi (art. 35, par. 1, lett. d), del Regolamento).

Infine, si ritiene che, tenuto conto della particolare invasività dei trattamenti relativi alla captazione dell'audio nella pubblica via e della conseguente compressione dei diritti e delle libertà fondamentali degli interessati, il Comune avrebbe dovuto previamente raccogliere le opinioni della cittadinanza in merito all'iniziativa che si intendeva intraprendere (art. 35, par. 9, del Regolamento).

Alla luce delle considerazioni che precedono, si ritiene che il Comune abbia agito in violazione dell'art. 35 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 posto in essere trattamenti di dati personali in maniera non conforme al principio di "liceità, correttezza e trasparenza", in violazione dell'art. 5, par. 1, lett. a) del Regolamento; in assenza di base giuridica, in violazione degli artt. 6, 9 e

10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice; omettendo di fornire agli interessati taluni degli elementi informativi richiesti dalla disciplina in materia di protezione dei dati, in violazione degli 13, par. 1, lett. c) ed e), e par. 2, lett. a), b) e d), e 14 del Regolamento; comunicando a terzi dati personali, anche relativi a reati e a categorie particolari (convinzioni religiose), in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice; omettendo di redigere una valutazione d'impatto sulla protezione dei dati conforme ai requisiti previsti dalla normativa in materia di protezione dei dati, in violazione dell'art. 35 del Regolamento.

Tenuto conto che la violazione, peraltro molteplice, delle predette disposizioni ha 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, tutte le violazioni, ad eccezioni di quella relativa all'art. 35 del Regolamento, sono soggette alla sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, come richiamato anche dall'art. 166, comma 2, del Codice, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

Deve invece considerarsi superata la contestazione relativa alla violazione dell'art. 28 del Regolamento, che era stata mossa nei confronti del Comune sul presupposto che, in riscontro alle richieste d'informazioni dell'Autorità, l'Ente aveva depositato un atto di designazione unilaterale, sottoscritto unicamente dal Sindaco, senza che vi fossero evidenze che la Fondazione avesse accettato tale designazione, impegnandosi ad adempiere agli obblighi ivi previsti. Nelle proprie memorie difensive il Comune ha, infatti, dichiarato che solo "per mero errore materiale" era stata trasmessa all'Autorità una versione non protocollata del documento, che "l'atto di nomina [della Fondazione quale responsabile del trattamento] è stato formalizzato con decreto sindacale, sottoscritto digitalmente dal Sindaco […] il 3 febbraio 2022" e che "il decreto è stato quindi trasmesso [alla Fondazione], la quale ne ha restituito copia controfirmata il 7 febbraio 2022 dal proprio legale rappresentante per accettazione della nomina", dovendosi, pertanto, disporre l'archiviazione del procedimento limitatamente a tale profilo (art. 11 del Regolamento n. 1/2019).

Parimenti, con riguardo alla messa in visibilità in chiaro alla Polizia locale del Comune dei dati relativi alle reti di utenti di "Twitter"("X"), si prende atto di quanto dichiarato dal Comune in merito alla circostanza che, di fatto, non vi è stato "mai […] accesso ai dati da parte del Corpo di Polizia locale trentino" (memorie difensive in atti). Atteso che la Polizia locale - che non ha competenze generali in materia di pubblica sicurezza (cfr. l. 7 marzo 1986, n. 65) - non ha trattato i dati in questione al di fuori delle finalità proprie del progetto di ricerca, ovvero per assumere provvedimenti nei confronti di specifiche persone fisiche, si dispone l'archiviazione del procedimento, limitatamente a tale profilo e alle relative contestate violazioni degli artt. 5, par. 1, lett. a), 6, 9 e 10 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice (art. 11 del Regolamento n. 1/2019).

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

L'art. 58, par. 2, del Regolamento attribuisce al Garante il potere di "ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine" (lett. d), di "imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento" (lett. f), nonché di "ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento […]" (lett. g).

Tenuto conto che il Comune ha dichiarato nella propria memoria difensiva che "a partire dal 1º novembre 2023 si è provveduto a limitare il trattamento dei dati, bloccando ogni attività che possa comportarne la rilevazione o l'utilizzo, eccezion fatta per la mera conservazione anche a fini difensivi" e atteso, dunque, che il Comune, ancorché si sia astenuto dall'ulteriore raccolta di dati personali, conserva tutt'ora dati personali relativi a persone fisiche, ottenuti nell'ambito dei progetti "Marvel" e "Protector", si rende necessario, ai sensi dell'art. 58, par. 2, lett. d), f) e g), del Regolamento:

imporre il divieto di trattare ulteriormente i predetti dati personali (registrazioni video o audio; messaggi/commenti ottenuti da reti sociali; informazioni relative alle reti di utenti sulla piattaforma "Twitter"/"X"); e

ordinare la cancellazione degli stessi.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, il Comune dovrà, inoltre, provvedere a comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione alle prescrizioni impartitegli.

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 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 la violazione delle disposizioni citate è soggetta all'applicazione della 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.

Per quanto attiene alla natura e alla gravità della violazione e alla delicatezza dei dati interessati dalla violazione (art. 83, par. 2, lett. a) e g), del Regolamento), occorre considerare che il trattamento in questione ha interessato luoghi pubblici ed è stato effettuato senza che i soggetti ripresi fossero pienamente consapevoli dell'effettiva finalità di trattamento perseguita e dell'ambito di conoscibilità dei dati, nonché in assenza dei necessari presupposti di liceità, con conseguente pregiudizio dei propri diritti e libertà fondamentali.

Il trattamento ha, inoltre, riguardato, in assenza di sufficiente trasparenza nei confronti degli interessati, anche il segnale audio acquisito mediante microfoni installati sulla pubblica via e dunque anche conversazioni private, il cui contenuto è assistito dalle più elevate garanzie sul piano costituzionale (v. le "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit., in particolare punto 129, ove si afferma che "le soluzioni individuate non dovrebbero prevedere funzioni non necessarie (ad esempio, […] registrazioni audio)", nonché il successivo punto 131, ove si afferma che tra gli elementi che i titolari dovrebbero prendere in considerazione vi è l'"utilizzo appropriato e vietato (dove e quando la videosorveglianza è consentita e dove equando non lo è: ad esempio, uso di telecamere nascoste e registrazione audio oltre che video)").

Tali massive e invasive modalità di trattamento hanno comportato significativi rischi per i diritti e le libertà degli interessati. Ciò non solo con riguardo al diritto alla protezione dei dati ma anche agli altri diritti, di rango costituzionale, connessi alla libera manifestazione del pensiero (art. 21 Cost.; v. anche artt. 9 e 10 CEDU e artt. 10 e 11 CDFUE), alla partecipazione alla vita politica e sociale (artt. 2 e 3 Cost.), alla libertà di riunione (art. 18 Cost.; v. anche artt. 11 CEDU e 12 CDFUE) e alla libertà di manifestare la propria fede religiosa (art. 19 Cost.; v. anche artt. 9 CEDU e 10 CDFUE), di cui il diritto alla riservatezza, in quanto funzionale all'autodeterminazione dell'individuo, costituisce un necessario presupposto. Simili forme di sorveglianza negli spazi pubblici possono, infatti, modificare il comportamento delle persone e condizionare finanche l'esercizio delle libertà democratiche, specialmente quando la sorveglianza contravviene alla ragionevole aspettativa di riservatezza di chi vi è sottoposto.

Alla luce di tali circostanze, si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia alto (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, occorre considerare, quali circostanze attenuanti:

che ancorché i progetti "Marvel" e "Protector" siano stati condotti per un esteso arco temporale (rispettivamente 20 e 15 mesi circa), le registrazioni video non sono state acquisite su base continuativa ma solo in relazione a un numero limitato di ore (309 ore per il progetto "Marvel"; 18 ore per il progetto "Protector", di cui solo 4 ore sono attualmente conservate). Similmente, per quanto attiene all'audio ottenuto dai microfoni installati sulla pubblica via nell'ambito del progetto "Marvel", il Comune ha acquisito nel complesso un numero limitato di ore di registrazione (85, pari a meno di quattro giorni), in un arco temporale di 8 mesi. Inoltre, da ogni microfono sono state acquisite tracce audio di 1 solo minuto consecutivo, che, secondo le dichiarazioni della Fondazione, riportate dal Comune nelle proprie memorie difensive, conterrebbero in gran parte silenzio o rumori indistinguibili;

che il Comune ha agito in buona fede, essendo incorso in un errore in diritto, nella convinzione che i trattamenti in questione potessero essere sussunti nel quadro giuridico in materia di sicurezza urbana e che le misure volte all'anonimizzazione dei dati fossero sufficienti a evitare la possibilità di identificare gli interessati, avendo, peraltro, l'Ente fatto affidamento sulle valutazioni del proprio Responsabile della protezione dei dati (cfr., ancorché in un diverso contesto, il provv. 2 luglio 2020, n. 118, doc. web n. 9440025) e sulla consulenza specialistica ricevuta dalla Fondazione, soggetto dotato di un'elevata competenza nell'ambito della ricerca scientifica;

che il Comune, ancorché non abbia pienamente adempiuto gli obblighi in materia di trasparenza, ha dichiarato di aver promosso "forme di divulgazione pubblica dei Progetti tra cui comunicati stampa, comunicati sul sito istituzionale del Comune, diffusione delle informazioni riguardanti i Progetti anche tramite social network del Comune e del Sindaco" (memorie difensive in atti);

che sebbene il Comune non abbia comprovato la data certa di redazione della valutazione d'impatto sulla protezione dei dati e il documento non fosse pienamente conforme ai requisiti previsti dalla normativa in materia di protezione dei dati, risulta in atti che l'Ente aveva provveduto alla redazione di uno schema di valutazione d'impatto e alla condivisione dello stesso con il Responsabile della protezione dei dati, di cui è stata acquisito il relativo parere.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 50.000 (cinquantamila) per la violazione degli artt. 5, par. 1, lett. a), 6, 9, 10, 13, par. 1, lett. c) ed e), e par. 2, lett. a), b) e d), 14 e 35 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto che l'attività di sorveglianza audio-video 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" ("Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", par. 2.1, cit.), senza che gli interessati fossero pienamente consapevoli dell'effettiva finalità di trattamento perseguita e di tutte le caratteristiche del trattamento, con conseguente pregiudizio dei propri diritti e delle proprie libertà fondamentali, 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 Trento per violazione degli artt. 5, par. 1, lett. a), 6, 9, 10, 13, par. 1, lett. c) ed e), e par. 2, lett. a), b) e d), 14 e 35 del Regolamento, nonché 2-ter, 2-sexies e 2-octies del Codice, nei termini di cui in motivazione;

ORDINA

al Comune di Trento, in persona del legale rappresentante pro-tempore, con sede legale in Via Belenzani, 19 - 38122 Trento (TN), C.F. 00355870221, di pagare la somma di euro 50.000 (cinquantamila) 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:

a) in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 50.000 (cinquantamila) 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;

b) ai sensi dell'art. 58, par. 2, lett. d), f) e g) del Regolamento:

il divieto di trattare i dati personali degli interessati già raccolti nell'ambito dei progetti "Marvel" e "Protector" (registrazioni video o audio; messaggi/commenti ottenuti da reti sociali; informazioni relative alle reti di utenti sulla piattaforma "Twitter"/"X");

la cancellazione dei predetti dati personali;

c) ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, di comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione alle misure imposte; l'eventuale mancato adempimento a quanto disposto nel presente punto può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento;

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, 11 gennaio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei