Parere sulla valutazione di impatto relativa al sistema dell'Arma dei Carabinieri "C-CAM" per l'acquisizione, la gestione e la conservazione delle immagini realizzate nel corso dei servizi di ordine pubblico attraverso i dispositivi digitali portatili di videoripresa - 22 luglio 2021 [9690902]

[doc. web n. 9690902]

Parere sulla valutazione di impatto relativa al sistema dell'Arma dei Carabinieri "C-CAM" per l'acquisizione, la gestione e la conservazione delle immagini realizzate nel corso dei servizi di ordine pubblico attraverso i dispositivi digitali portatili di videoripresa - 22 luglio 2021

Registro dei provvedimenti
n. 291 del 22 luglio 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia, 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 anche "Regolamento");

VISTO il decreto legislativo 30 giugno 2003, n.196, recante il Codice in materia di protezione dei dati personali, integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101 (di seguito anche "Codice");

VISTA la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

VISTO il decreto legislativo 18 maggio 2018, n. 51, recante l'Attuazione della direttiva (UE) 2016/680 (di seguito anche "Decreto");

ESAMINATA la valutazione di impatto sulla protezione dei dati personali (di seguito anche "DPIA") del sistema informativo "C-CAM" per l'acquisizione, la gestione e la conservazione delle immagini realizzate nel corso dei servizi di ordine pubblico attraverso i dispositivi digitali portatili di videoripresa dell'Arma dei Carabinieri (di seguito, anche "Arma" o "Comando") e dei relativi allegati.

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell´ufficio del Garante per la protezione dei dati personali;

Relatore la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. Il Comando Generale dell'Arma dei Carabinieri ha inviato a questa Autorità la valutazione di impatto sulla protezione dati relativa al sistema informativo "C-CAM" per l'acquisizione, la gestione e la conservazione delle immagini realizzate nel corso dei servizi di ordine pubblico attraverso i dispositivi digitali portatili di videoripresa, oggetto dell'attuale provvedimento.

Con la medesima nota, il medesimo Comando Generale ha trasmesso, altresì, la DPIA relativa ad un analogo sistema da impiegare nell'ambito dei servizi di prevenzione generale, che sarà oggetto di un successivo provvedimento di questa Autorità.

Si premette che il Ministero dell'interno-Dipartimento della pubblica sicurezza ha autonomamente presentato a questa Autorità la DPIA relativa ad un sistema di telecamere indossabili da parte dei Reparti mobili della Polizia di Stato, per la documentazione audio e video di situazioni critiche per l'ordine e la sicurezza, in occasione di eventi o manifestazioni pubbliche. Tale sistema, oggetto di contestuale, ma distinto provvedimento, presenta notevoli analogie con quello oggetto dell'attuale provvedimento, non solo per quanto riguarda le finalità ma anche dal punto di vista strutturale, salvo le differenze imputabili alle specifiche strutture organizzative delle due Forze di Polizia.

La oggettiva connessione tra i due sistemi è posta in luce dalla stessa DPIA presentata dall'Arma dei Carabinieri, ove si rileva che "Il trattamento di dati personali oggetto della presente [DPIA] si inserisce nell'ambito delle attività avviate in seno al Ministero dell'Interno - Dipartimento della pubblica sicurezza, per disciplinare l'utilizzo di videocamere indossabili (body-cam) da parte dei militari dei Reggimenti/Battaglioni mobili cieli' Arma dei Carabinieri, per la documentazione video e audio di situazioni "critiche" per l'ordine e la sicurezza pubblica in occasione di eventi o manifestazioni pubbliche." (pag. 8).

Occorre anche ricordare che, in precedenza, il Dipartimento della pubblica sicurezza ha sperimentato l'uso di un sistema di ripresa visiva attraverso l'assegnazione di microtelecamere a personale specificamente individuato dei Reparti Mobili della Polizia di Stato di Torino, Milano, Roma e Napoli, per l'eventuale ripresa di quanto avviene in situazioni di criticità, rispetto al quale il Garante ha precisato condizioni e limiti del trattamento (31 luglio 2014, prot. U0023672).

Il presente parere è reso tenendo conto degli approfondimenti effettuati in piena collaborazione con i competenti uffici dell'Arma, anche nel corso di incontri tecnici di lavoro, e si riferisce a una versione aggiornata della valutazione di impatto redatta all'esito delle predette interlocuzioni, trasmessa per il tramite del Dipartimento della p.s., in particolare per quanto riguarda i tempi di conservazione dei dati e di cancellazione di quelli irrilevanti.

RILEVATO

2. Finalità del trattamento e scenari di utilizzo.

L'Arma rappresenta che i militari dei reggimenti/battaglioni mobili dell'Arma dei Carabinieri sono specificamente addestrati per fronteggiare situazioni di criticità, anche particolarmente complesse, sotto il profilo dell'ordine e della sicurezza pubblica, contrastando condotte violente e in grado di realizzare il turbamento dell'ordine pubblico, per ristabilire il libero esercizio dei diritti costituzionalmente garantiti in occasione di eventi o manifestazioni pubbliche.

La necessità di documentare tali tipologie di azioni illecite, spesso indirizzate proprio contro gli operatori dei reggimenti/battaglioni dell'Arma, ha determinato il Comando Generale dell'Arma dei Carabinieri a individuare nelle videocamere lo strumento indispensabile per raccogliere, in un "teatro operativo" particolarmente complesso, preziosi elementi probatori in ordine a condotte di natura penale, nonché per l'applicazione delle misure di prevenzione personali, quali quelle riguardanti l'ambito delle manifestazioni sportive, come il DASPO. Tali strumenti svolgono pure un effetto deterrente, specialmente per quanto riguarda le aggressioni rivolte direttamente agli operatori di polizia.

Pertanto, la finalità del trattamento in oggetto consiste nel raccogliere e conservare elementi di prova audio-video o fotografici riguardanti condotte illecite, rilevanti sotto l'aspetto penale o per l'applicazione di misure di prevenzione, perpetrate in occasione di eventi o manifestazioni pubbliche. Il sistema non prevede operazioni di trattamento successive alla raccolta incompatibili con lo scopo iniziale.

2.1. La struttura del sistema

L'architettura hardware è costituita dai seguenti componenti:

a) le videocamere indossabili usate per l'acquisizione di foto e filmati successivamente trasferiti nei totem per lo stoccaggio e gli altri trattamenti;

b) gli apparati periferici dedicati ai trattamenti in discussione e posizionati presso le sedi dell'Arma, denominati totem. I totem sono dotati di personal computer ('PC totem') dotati di 'software di gestione', di collegamento al server centrale ubicato presso il centro telematico dell'Arma, e di docking station per la gestione e la ricarica delle videocamere. La conservazione dei documenti acquisiti (filmati e foto) avviene, fisicamente, in dispositivi di memorizzazione dedicati (NAS – network attached storage), dotati di un certo numero di unità disco in configurazione ridondata. A differenza dei totem del sistema body cam, i totem dell'Arma sono equipaggiati anche di un lettore di tessere di riconoscimento personale, di un DVD writer e di un lettore del codice a barre delle videocamere;

c) i notebook; i reggimenti/battaglioni che effettuano servizio di ordine pubblico saranno dotati anche di un notebook per la condivisione delle immagini con l'Autorità di Pubblica Sicurezza, nella persona del dirigente del servizio di ordine pubblico, nell'immediatezza dei fatti e direttamente sul posto per il tramite della Polizia Scientifica. I Comandi Provinciali, di Gruppo, di Reparto territoriale e di Compagnia, presso cui il sistema sarà utilizzato nell'ambito dei servizi di prevenzione generale, non saranno dotati del notebook;

d) le postazioni di lavoro ubicate presso gli Uffici delle sedi di utilizzo del sistema C-Cam, da cui sarà possibile accedere anche ai contenuti archiviati nei totem delle altre sedi;

e) un 'server centrale' per l'indicizzazione, la ricerca e l'accesso ai documenti già archiviati nei totem e ubicato presso il Comando Generale dell'Arma dei Carabinieri.

Altre componenti di supporto al trattamento, rilevanti sul profilo della sicurezza informatica sono:

a) un meccanismo per tener traccia delle responsabilità (assegnazioni/acquisizione delle registrazioni, e degli accessi), c.d. watermarking. L'associazione della videocamera al militare è effettuata abbinando il numero seriale della videocamera al numero di matricola del militare, che verrà 'registrato … nel sistema'. La non ripudiabilità (o 'imputabilità') delle registrazioni effettuate sarà garantita dall'apposizione sul filmato del 'CIP del militare'. Inoltre, i documenti (filmati e foto) acceduti dalle postazioni di lavoro recheranno in sovraimpressione la matricola del militare che opera l'accesso e la visualizzazione (v. anche par. 4 e par. 6);

b) copie prodotte per condividere i documenti informatici acquisiti (foto e filmati digitali) con le altre forze di polizia e con la magistratura.

2.2. Fonti normative

Molteplici sono le fonti normative indicate dall'Arma quale fondamento del trattamento in argomento: l'articolo 16 della legge aprile 1981. n. 121, che individua l'Arma dei Carabinieri quale forza armata in servizio permanente di pubblica sicurezza, impegnata nello svolgimento di tutte le attività a tutela dell'ordine e della sicurezza pubblica, con particolare riguardo al controllo del territorio; l'articolo 161 del d .Lgs. 15 marzo 2010, n. 66 ("Codice dell'Ordinamento Militare"), che attribuisce all'Arma dei Carabinieri lo svolgimento delle funzioni di polizia giudiziaria e funzioni di sicurezza pubblica; l'articolo 57 del codice di procedura penale che, a seconda del grado, qualifica i Carabinieri quali Ufficiali o Agenti di polizia giudiziaria, cui peraltro risalgono, avuto riguardo alle condotte costituenti reato, specifici obblighi di assicurazione delle fonti di prova (art. 55 c .p.p.) e di acquisizione, ai sensi dell'art. 234, comma 1, c.p.p., di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.

Ulteriore esplicito riferimento alla documentazione video fotografica è rinvenibile nel decreto legge 20 febbraio 2017, n. 14, convertito con modificazioni dalla legge 18 aprile 2017, n. 48, considerata condizione per procedere al cosiddetto "arresto in flagranza differito". L'articolo 10, comma 6-quater, recita, infatti, che nel caso di reati commessi con violenza alle persone o alle cose, compiuti alla presenza di più persone anche in occasioni pubbliche, per i quali è obbligatorio l'arresto ai sensi dell'articolo 380 del codice di procedura penale, quando non è possibile procedere immediatamente all'arresto per ragioni di sicurezza o incolumità pubblica, si considera comunque in stato di flagranza ai sensi dell'articolo 382 del medesimo codice colui il quale, sulla base di documentazione video fotografica dalla quale emerga inequivocabilmente il fatto, ne risulta autore, sempre che l'arresto sia compiuto non oltre il tempo necessario alla sua identificazione e, comunque, entro le quarantotto ore dal fatto.

Ulteriore disposizione rilevante è l' articolo 23, comma 1, del D.P.R. n. 15 del 2018, che consente la possibilità di utilizzare sistemi di ripresa fotografica, video e audio per finalità di polizia ove necessario per documentare: - una specifica attività preventiva o repressiva di fatti di reato; - situazioni dalle quali possano derivare minacce per l'ordine e la sicurezza pubblica o un pericolo per la vita e l'incolumità dell'operatore, o specifiche attività svolte durante il servizio che siano espressione di poteri autoritativi degli organi, uffici e comandi di polizia.

2.3. I dati trattati e gli interessati

Interessati sono le persone successivamente identificabili cui si riferiscono i filmati o le immagini fotografiche riprese con le videocamere. I dati raccolti fanno riferimento alle seguenti informazioni personali: - registrazione audio e video relativa alla persona, successivamente identificabile in base all'aspetto e ad altri elementi specifici; - immagine in modalità foto relativa alla persona, successivamente identificabile in base all'aspetto e ad altri elementi specifici; - data e ora della registrazione; - coordinate GPS della registrazione.

2.4. Modalità di impiego del sistema

Le videocamere sono consegnate, prive di dati archiviati nella memoria, dal militare qualificato come operatore al personale del Reggimento/Battaglione mobile che riveste la funzione di "Comandante di Squadra", all'atto di intraprendere il servizio, previa operazione di associazione del dispositivo. L'associazione è effettuata tramite abbinamento seriale della camera con la matricola del militare, che verrà registrata nel sistema.

Il Comandante di Squadra verifica l'efficienza dell'apparato e il livello di carica della batteria; rende edotti della disponibilità della particolare dotazione, da annotare nell'ordine del servizio, la Centrale Operativa dell'Arma dei Carabinieri competente territorialmente e il responsabile del contingente dell'Arma nel servizio di ordine pubblico, che informa nel senso il dirigente del servizio di ordine pubblico.

Il personale cui è assegnata la videocamera è addestrato e istruito sul suo utilizzo, anche avuto riguardo agli aspetti legati alla protezione dei dati personali. L'attività di istruzione è adeguatamente documentata.

L'avvio della registrazione da parte dei Comandanti di Squadra è disposto dal dirigente del servizio di ordine pubblico, quando l'evolversi degli scenari faccia intravedere l'insorgenza di concrete e reali situazioni di pericolo di turbamento dell'ordine e della sicurezza pubblica o comunque siano perpetrati fatti costituenti reato. La registrazione può essere avviata d'iniziativa anche dal Comandante di Squadra cui è assegnata la videocamera, per l'urgente necessità di documentare episodi che configurino turbative dell'ordine pubblico o fatti di reato e non sia oggettivamente possibile chiedere l'intervento del dirigente del servizio di ordine pubblico, che comunque deve essere informato appena possibile.

La registrazione è interrotta al termine dell'intervento, e comunque su disposizione del dirigente del servizio di ordine pubblico ovvero autonomamente dal Comandante di Squadra, in caso di necessità e oggettiva impossibilità del dirigente del servizio di ordine pubblico, informando quest'ultimo non appena possibile.

L'avvio e il termine delle riprese sono documentati dalle informazioni automaticamente sovraimpresse nel filmato (ora e data).

Nelle relazioni di servizio, nei verbali e nelle annotazioni di polizia giudiziaria dovrà essere richiamato il nome del file generato automaticamente dal sistema, recante, tra l'altro, il "CIP" del militare utente e l'identificativo della videocamera.

2.5. Operazioni successive di trattamento

I dati personali oggetto del trattamento sono raccolti con le videocamere e registrati nel supporto di memoria dell'apparato.

Al termine del servizio l’operatore ritira il dispositivo dal Comandante di squadra, provvedendo al trasferimento nello storage dei contenuti multimediali registrati.

Il download dei file avviene direttamente sul NAS, dotato di software di gestione dedicato, integrato nel totem multimediale del Reparto. I metadati estratti dai file memorizzati nel NAS (nome del file, data e ora, codice della videocamera, reparto ove risiede il dato, ecc.) sono poi inviati in maniera automatica al server centrale ubicato presso il Comando Generale dell'Arma dei Carabinieri. Al termine del download, i file sono cancellati automaticamente dalla memoria della videocamera. La cancellazione dei dati avviene unicamente collegando il dispositivo al totem multimediale. Altre funzioni di cancellazione sono disabilitate.

E’ possibile scaricare le registrazioni delle videocamere direttamente nei notebook in dotazione ai Comandanti dei contingenti dell'Arma, utilizzati per condividere le immagini con i dirigenti del servizio di ordine pubblico, per il tramite del personale della Polizia Scientifica, qualora emerga l'esigenza dell'Autorità di pubblica sicurezza di disporre dei filmati nell'immediatezza dei fatti e direttamente sul posto. In tale caso, il file d'interesse dell'Autorità di Pubblica Sicurezza viene scaricato su una memoria di massa estraibile, attraverso l'apposizione sul filmato/immagine della dicitura "Copia per l'Autorità di pubblica sicurezza". L'operazione di estrazione di copia non rimuove, né altera il filmato originale presente sulla videocamera. Le registrazioni devono, infatti,

essere conservate per il successivo download sul NAS del Reparto. Di tali operazioni viene dato atto con apposito verbale.

2.6. Soggetti autorizzati al trattamento ed i relativi profili

Nella valutazione di impatto sono indicate le figure che effettuano il trattamento dei dati e le attività ad essi consentite.

L'Amministratore Centrale (identificato con il personale della Direzione di Telematica del Comando Generale dell'Arma dei Carabinieri): configura i totem (attribuzione di body-cam e notebook ai reparti interessati); attiva/disattiva i profili utente.

L'Ufficiale Responsabile (identificato per l'Organizzazione mobile dell'Arma dei Carabinieri nel Comandante dei Reggimenti/Battaglioni): identifica gli Ufficiali delegati a svolgere le proprie funzioni, nel numero massimo di due; attribuisce al personale dipendente i profili di "Referente informatico" e quello di "Operatore"; consulta i video e le foto archiviate nel totem di pertinenza del reparto di cui è il Comandante; condivide i video e le foto con soggetti terzi puntualmente identificati.

Il Referente Informatico, si occupa della configurazione delle body cam associate al totem di pertinenza del reparto ove presta servizio (qualità video, nomenclatura file, luminosità ecc. …). L'Operatore, in qualità di custode degli apparati, provvede a consegnare/ritirare le body cam e il notebook agli/dagli utenti finali all'inizio/termine del servizio esterno. L'Utente visualizza i soli contenuti video e foto della body cam assegnata e per i quali si è ricevuta apposita autorizzazione da parte dell'Ufficiale responsabile.

L'accesso ai dati memorizzati nei NAS dei Reggimenti/Battaglioni mobili dell'Arma dei Carabinieri, per le attività di ricerca, visualizzazione e copia dei dati, è possibile per gli Ufficiali Responsabili e per i loro delegati appositamente autorizzati, mediante accesso diretto dal totem del reparto o consultazione attraverso la propria postazione di lavoro. Gli Ufficiali responsabili e i loro delegati possono accedere, attraverso la propria postazione di lavoro, ai file appositamente individuati in ragione delle specifiche finalità connesse con l'incarico rivestito. Le autorizzazioni sono rilasciate in maniera puntuale per ogni singolo file e mai in modalità massiva. In ogni caso la visualizzazione del file può essere effettuata unicamente utilizzando il "player" a ciò dedicato, che contiene la chiave di decifratura, e che può essere scaricato solo su una postazione di lavoro connessa al dominio dell'Arma dei Carabinieri.

Tutti gli utenti, per accedere al sistema, sono autenticati con username e password e preventivamente autorizzati a svolgere dette operazioni. Tutti i flussi di comunicazione sono cifrati con protocollo https.
Il server centrale del Comando Generale dell'Arma dei Carabinieri, dotato di apposito software gestionale, consente agli Ufficiali responsabili e agli utenti da essi autorizzati di operare ricerche tramite i metadati disponibili, nonché di accedere e prelevare dati dai NAS attestati presso i Reggimenti/Battaglioni mobili. È possibile operare la ricerca/visualizzazione esclusivamente dei filmati di propria competenza ovvero per i quali sia stata rilasciata preventiva autorizzazione.

Presso il server centrale sono mantenuti in memoria i file di log non modificabili, relativi agli accessi e alle operazioni compiute dagli utenti e non sono previste limitazioni temporali di conservazione. L'accesso ai file di log è consentito agli amministratori di sistema unicamente al fine della verifica della liceità del trattamento, del controllo interno, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito del procedimento penale.

Il flusso di dati tra il totem multimediale (NAS), le postazioni di lavoro e il server centrale è di tipo protetto, cifrato con protocollo https.

2.7. Durata della conservazione dei dati

I dati memorizzati sui NAS locali sono automaticamente cancellati decorsi sei mesi dall'archiviazione, a meno che non siano selezionati manualmente per essere conservati oltre tale termine in quanto rilevanti per le finalità del trattamento indicate nella DPIA, ossia costituenti elementi di prova audio-video o fotografici riguardanti condotte illecite rilevanti sotto l'aspetto penale o per l'applicazione di misure di prevenzione.

2.8. Cancellazione dei dati accidentali

Allorquando una registrazione sia stata avviata accidentalmente o erroneamente, il Comandante di Squadra deve comunicarlo all'Ufficiale Responsabile o agli utenti da quest'ultimo autorizzati, al fine di procedere all'immediata cancellazione, da documentare con apposita relazione di servizio. Analogamente, previe intese con il dirigente del servizio di ordine pubblico, si procede alla cancellazione delle registrazioni avviate a fronte di una errata valutazione prognostica in ordine all'insorgenza di concrete e reali situazioni di pericolo di turbamento dell'ordine e della sicurezza pubblica, laddove le riprese risultino, a posteriori, inconferenti rispetto alle finalità del trattamento. Alla materiale cancellazione della registrazione procede l'Ufficiale Responsabile o gli utenti da quest'ultimo autorizzati, documentando le attività con apposita relazione di servizio.

OSSERVA

3. Quadro giuridico di riferimento

Il trattamento in oggetto risulta finalizzato alla prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali da parte di autorità competenti e rientra, pertanto, nel capo di applicazione del decreto legislativo 18 maggio 2018, n. 51.

4. Consultazione preventiva del Garante

L’articolo 24, comma 1, lettera b, del Decreto, stabilisce che il titolare del trattamento deve consultare il Garante prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione, trasmettendo al Garante la valutazione di impatto, quando “una valutazione d'impatto sulla protezione dei dati indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, oppure il tipo di trattamento presenta un rischio elevato per i diritti e le libertà degli interessati anche in ragione dell'utilizzo di tecnologie, procedure o meccanismi nuovi ovvero di dati genetici o biometrici”.

Correttamente, nella valutazione di impatto si rileva che in base al d.lgs. n. 51 del 2018 il titolare è tenuto a trasmettere la DPIA al Garante anche nelle ipotesi in cui, all'esito della DPIA, le misure individuate siano state valutate idonee a minimizzare il rischio e ciò allo scopo di consentire comunque a tale Autorità di verificare la conformità del trattamento alla normativa, con particolare riguardo ai rischi per la protezione dei dati personali dell'interessato e alle relative garanzie.

Non appaiono, invece, condivisibili le considerazioni del responsabile del trattamento dei dati in ordine alla insussistenza del trattamento di dati sensibili, in considerazione della circostanza che rischi per i diritti e le libertà degli interessati derivanti dal trattamento sarebbero di livello basso.

Appare, invece, a questa Autorità che i rischi per gli interessati derivanti dai trattamenti in adozione, tenuto conto delle finalità, spaziano dalla discriminazione alla sostituzione di identità, al pregiudizio per la reputazione, all’ingiusta privazione di diritti e libertà. Anche se la probabilità che tali rischi si concretizzino è ragionevolmente bassa tenuto conto del contesto, l’impatto che da essi conseguirebbe in danno degli interessati sarebbe elevato o molto elevato.

Occorre anche considerare che il contesto sociale di utilizzo del sistema in argomento, costituito

da manifestazioni pubbliche, rende estremamente probabile in trattamento delle categorie particolari di dati personali di cui all'articolo 9 del Regolamento UE (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi all'orientamento sessuale della persona), a seconda della specifica motivazione della manifestazione.
Pertanto, l'attività di trattamento in discussione va considerata a elevato rischio per gli interessati e, trovando applicazione l'articolo 24, par. 1, lett. a) del Decreto, si ritiene necessaria la consultazione preventiva.

5. Presupposti di liceità del trattamento.

In considerazione delle finalità del trattamento e delle fonti normative indicate nella DPIA, si ritiene che sussistano i requisiti di liceità prescritti dall'articolo 5 del Decreto.

6. Conservazione dei dati.

La DPIA prevede l'impiego delle immagini in occasione di eventi o manifestazioni pubbliche, limitatamente ai casi in cui "l'evolversi degli scenari [di intervento] faccia intravedere l'insorgenza di concrete e reali situazioni di pericolo di turbamento dell'ordine e della sicurezza pubblica o comunque siano perpetrati fatti costituenti reato" (pag. 19). Si specifica poi, opportunamente, che l'utilizzo del sistema costituisce lo strumento indispensabile per raccogliere, in un teatro operativo particolarmente complesso, "preziosi elementi probatori in ordine a condotte di natura penale", nonché ai fini dell'applicazione "delle misure di prevenzione personali, anche riguardanti l'ambito delle manifestazioni sportive (DASPO)." (pag. 32).

Circa i tempi di conservazione, il Decreto, in attuazione dei principi della direttiva (UE) 680/2016, stabilisce che i dati personali devono essere "adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati" e "conservati con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati" (art. 3).

Il trattamento dei dati in questione richiede, per quanto riguarda la conservazione dei dati trattati, la individuazione di un punto di equilibrio tra le esigenze di tutela dei dati personali - segnatamente, quelle individuate nel predetto articolo 3 – e quelle connesse all'attività di polizia.

Con riferimento a queste ultime, l'Autorità di polizia ha rappresentato che le registrazioni audio e video riproducono di regola immagini relative all'evolversi rapido, disordinato e concitato di manifestazioni pubbliche, cui partecipano gruppi eterogenei di persone che mettono in atto le più disparate condotte, alcune delle quali rilevanti in funzione dell'attività di polizia giudiziaria ovvero di polizia di sicurezza.

Le registrazioni documentano dunque plurime condotte attuate da più persone, embricate le une sulle altre, che per essere comprese nella loro valenza giuridica necessitano di attente analisi e del confronto con altro materiale filmato. L'utile ricostruzione dei fatti necessita in altre parole della "lavorazione" di tutte le registrazioni disponibili riguardanti gli eventi presi in esame. Inoltre, la notitia criminis non sempre è immediatamente percepibile "sul campo" dagli operatori di polizia. Di fatto, occorre sovente osservare successivamente le registrazioni per avere l'esatta qualificazione penale dei fatti e delle circostanze documentate. La visione successiva delle immagini, in altri termini, costituisce molte volte la fonte primaria di acquisizione della notizia di reato.

Le stesse valutazioni riguardano l'acquisizione degli elementi necessari per l'applicazione delle misure di prevenzione personali (avviso orale, foglio di via, daspo, ecc.). Tali misure, come noto, per la loro funzione (preventiva), sono slegate dall'accertamento della commissione di reati e si fondano su indici di pericolosità che non sono necessariamente connessi a un evento precisamente collocato nel tempo. Ciò, pur non considerando che non sono previsti termini per

l’avvio formale del procedimento finalizzato all’applicazione delle misure di prevenzione.

Tutto ciò considerato, il termine di sei mesi indicato nella DPIA quale punto di equilibrio tra le esigenze dell’attività di polizia e quelle di tutela dei dati personali appare ragionevole e rispettoso dei principi previsti dalla disciplina in materia di protezione dei dati personali. Risulta, altresì, rispettato il principio della privacy by default, essendo prevista la cancellazione automatica dei dati personali acquisiti alla scadenza dei sei mesi.

Resta fermo che i dati evidenziati come di interesse a fini di indagine penale o di applicazione di misure di prevenzione all’esito della valutazione saranno acclusi ai relativi procedimenti e sconteranno i pertinenti termini di conservazione previsti dall’articolo 10 del D.P.R. n. 15 del 2018.

7. Registrazioni avviate accidentalmente o comunque effettuate in mancanza del presupposto della necessità.

La DPIA prevede che la individuazione dei filmati inconferenti deve avvenire “prima del posizionamento [della telecamera] nella docking station per impedire che in dati siano riversati nel NAS” (pag. 23), cioè direttamente dalle telecamere, ma ciò sembrerebbe tecnicamente impossibile, poiché secondo la stessa DPIA la cancellazione dei dati dalla telecamera “avviene unicamente collegando il dispositivo al totem multimediale (altre funzioni di cancellazione sono disabilitate)” (pag. 15, evidenze aggiunte). Tale aspetto andrebbe adeguatamente chiarito.

8. Le videocamere indossabili

Si rileva che non è stata allegata alcuna scheda tecnica alla DPIA. Per tale motivo, non è possibile fornire una stima dell’adeguatezza del dispositivo ad adempiere al requisito di esattezza nella raccolta dei dati, tenuto conto del contesto, degli scenari d’uso e delle finalità del trattamento. Almeno la scheda tecnica del dispositivo, elemento cardine attorno al quale è realizzato il sistema in esame, dovrebbe essere allegata alla valutazione di impatto, in accordo con il principio generale di accountability secondo cui il titolare del trattamento è competente per il rispetto dei principi di protezione dati e in grado di comprovarlo.

Inoltre, sebbene la DPIA affermi che ‘il contenuto multimediale delle videocamere è cifrato con chiave AES 128bit’, non vengono fornite indicazioni sulle procedure per la generazione, la conservazione, l’utilizzo e la sostituzione delle chiavi di cifratura, lasciando non documentato un rilevante aspetto tecnico-organizzativo di sicurezza informatica.

Per quanto riguarda la possibilità di accedere al contenuto delle videocamere, la DPIA afferma che le videocamere sono configurate per consentire il trasferimento dei dati acquisiti ai soli dispositivi autorizzati, e cioè le docking station integrate nei c.d. totem e i notebook appositamente configurati. Tuttavia, tale affermazione andrebbe ulteriormente argomentata spiegando come tale controllo d’accesso è tecnicamente realizzato.

9. I totem multimediali.

La DPIA non chiarisce se gli accessi operati dalle postazioni di lavoro al totem che si trovi nel medesimo Ufficio, come ad esempio quelli operati dal PC facente parte del totem stesso, sono comunque intermediati dal server centrale. Sul punto, la DPIA oltre che trattare della gestione dei log degli accessi ai documenti custoditi nei totem quando attuati tramite l’intermediazione del server centrale (v. nel seguito), dovrebbe anche riguardare i log degli accessi e delle operazioni con profilo utente o amministrativo attuati ‘in locale’, cioè gli accessi e le operazioni, effettuati senza l’intermediazione del server centrale e chiarire, anche per tali casi, dove siano custoditi i log, quali informazioni rechino, e come ne sia garantita l’immodificabilità.

Si rileva che i riferimenti della DPIA ai meccanismi adottati per garantire la disponibilità dei dati

non sono approfonditi: sembrerebbe che i NAS siano in configurazione ridondata, probabilmente in raid, ma non è chiaro se sia realizzato un backup dei dati su altri supporti di memorizzazione.

I documenti acquisiti dalle videocamere e trasferiti nei totem sono ivi conservati per un certo periodo, trascorso il quale, se ancora di interesse, sono trasferiti su DVD non riscrivibili. La DPIA non fa cenno a come siano conservati tali supporti e a quali accorgimenti siano adottati per garantire la sicurezza e l'autenticità del contenuto.

10. I notebook

La DPIA non fornisce dettagli sulle misure di sicurezza in esercizio sui notebook. La DPIA dovrebbe chiarire, tra l'altro, se sia abilitata la cifratura della memoria disco interna, e il meccanismo di autenticazione adottato, mono o multi fattoriale, argomentando tali scelte.

11. Le postazioni di lavoro

La DPIA illustra che durante la visualizzazione dei filmati appare in sovraimpressione la matricola del militare che ha avuto accesso al filmato, al fine di 'impedirne la ripresa con dispositivi terzi e la successiva divulgazione' (pag. 30). Invece, altrove nella stessa DPIA si afferma che il watermark apposto in sovraimpressione in fase di 'visualizzazione e copia', riporti solo il CIP (si assume sia la matricola) del militare che ha effettuato la ripresa (pag. 38 della DPIA, punto 1.3 e nota a piè di pagina n.2). Sebbene il meccanismo di watermarking appaia teoricamente idoneo a preservare la riservatezza dei filmati contro il rischio di estrazione di copie che si presterebbero alla comunicazione e diffusione non autorizzate, la DPIA dovrebbe descriverne più approfonditamente la realizzazione per dimostrarne l'efficacia e dirimere le contraddizioni che sembrano emergere nel testo. In effetti, sembrerebbe più ragionevole che il watermark anti-copia riporti la matricola del militare che sta eseguendo l'accesso. Sarebbe stato utile, allo scopo, inserire nella DPIA delle schermate esemplificative (c.d. screenshot) che avessero illustrato il funzionamento di tale meccanismo.

Inoltre, la DPIA dovrebbe chiarire se l'autenticazione alle postazioni è di tipo mono o multi fattoriale. Dovrebbe inoltre chiarire se i documenti all'atto dell'accesso tramite il server centrale siano copiati in locale, cioè sulla memoria disco delle postazioni, e se i file (conservati nei totem ed eventualmente copiati in locale) siano cifrati. Inoltre, dovrebbe chiarire se la chiave di cifratura è la medesima per tutti i file custoditi in tutti i totem e argomentare tali scelte.

12. Il server centrale

Il 'server centrale' o, anche, 'sistema centrale' è ubicato presso il Comando Generale dell'Arma dei Carabinieri. La DPIA chiarisce che non è esposto su Internet, ma è raggiungibile solo dalla rete interna dell'Arma dei Carabinieri. Le funzioni erogate sono raggiungibili tramite protocollo sicuro HTTPS, e i certificati SSL (secure socket layer) sono forniti dall'autorità di certificazione dell'Arma. All'atto del trasferimento dei documenti dalle videocamere nei totem sono generati i metadati dei file (nome, ora e data, codice della videocamera, ufficio presso cui è fisicamente ubicato il dato, etc.), inviati al server centrale, che opera da motore di indicizzazione per le successive ricerche. Presso il server centrale sono conservati i log non modificabili degli accessi e delle operazioni compiute. La DPIA dovrebbe dettagliare quali informazioni rechino detti log e come ne sia garantita l'immodificabilità.

13. Le copie dei documenti

Nell'ambito della comunicazione dei dati tra le Forze di Polizia, in alcuni casi i documenti (filmati e foto) acquisiti tramite le videocamere saranno copiati e trasferiti. In particolare, quando il dirigente del servizio di ordine pubblico abbia urgenza di acquisire nell'immediatezza degli eventi informazioni indispensabili all'assolvimento dei propri compiti, verrà prodotta copia dei documenti

e affidata agli agenti della Polizia Scientifica. La copia dei documenti sarà trasferita mediante "riversamento su memoria di massa estraibile" e vi sarà apposta la "dicitura [...] copia per l'Autorità di pubblica sicurezza". Tali operazioni saranno riportate in un verbale di consegna. Inoltre, copia dei documenti su DVD sarà tramessa all'Autorità giudiziaria a corredo delle eventuali comunicazioni di notizie di reato. Ancora, l'Ufficiale responsabile potrà condividere i documenti d'interesse con altro personale dell'Arma, come ad esempio i superiori nella scala gerarchica, con il Comandante del Reparto operativo di comando Provinciale. Infine, i documenti saranno conservati nei totem per un tempo limitato. Allo scadere del termine di conservazione saranno 'riversati' su CD/DVD riscrivibile.

L'esigenza di produrre copie dei documenti (filmati e foto) reca in sé delle criticità sul profilo della protezione dati, in quanto bisognerebbe garantire anche per tali copie, che spesso vivranno al di fuori del perimetro di sicurezza del sistema informatico C-Cam, i requisiti di sicurezza richiesti dalla norma (art. 25 del Decreto), tra cui il "controllo dei supporti dei dati", il "controllo della conservazione", il "controllo dell'accesso", il "controllo della trasmissione" e il "controllo del trasporto".

Nel caso della conservazione dei documenti su supporti ottici (DVD) e del trasferimento all'Autorità Giudiziaria (su DVD), il Comando dovrebbe chiarire quali soluzioni tecnico-organizzative abbia inteso adottare per assicurare che ai DVD (o al loro contenuto) possa accedere solo il personale autorizzato, e che l'autenticità dei documenti lì memorizzati sia verificabile a posteriori. Ad esempio, il Comando Generale dell'Arma dei Carabinieri potrebbe valutare il ricorso a tecniche di cifratura dei dati contenuti nei DVD per assicurarne la riservatezza, e il ricorso a tecniche di firma digitale per garantirne l'autenticità. Inoltre, potrebbe valutare di utilizzare la tecnica del watermarking anche per le copie di dati da trasmettere alla magistratura, apponendo sul documento da trasferire una filigrana informatica che rechi traccia del soggetto destinatario della copia, attività questa che riduce il rischio che quella copia possa essere estratta, comunicata o persino diffusa a terzi non autorizzati, durante la fase di recapito al destinatario o durante il successivo stoccaggio.

Nel caso di produzione di una copia per la l'Autorità di pubblica sicurezza nell'immediatezza degli eventi, la DPIA accenna al fatto che su tale copia verrà apposta la "dicitura copia per l'Autorità di pubblica sicurezza", affermazione che lascia presumere il ricorso anche in questo caso al meccanismo del watermarking. Tuttavia, tale aspetto andrebbe meglio chiarito e, più in generale, il Comando dovrebbe più dettagliatamente specificare come intenda preservare la riservatezza dei dati, una volta che siano prodotte copie destinate ad altri soggetti, e come garantirne l'autenticità.

TUTTO CIÒ PREMESSO IL GARANTE

esprime parere favorevole in ordine alla valutazione di impatto sulla protezione dei dati personali presentata dal Comando Generale dell'Arma dei Carabinieri relativa al sistema informativo "C-CAM" per l'acquisizione, la gestione e la conservazione delle immagini realizzate nel corso dei servizi di ordine pubblico attraverso i dispositivi digitali portatili di videoripresa,

- a condizione che siano previamente recepite le seguenti indicazioni, idonee a rendere il trattamento conforme alle disposizioni del Decreto:

a) per quanto riguarda l'individuazione e la cancellazione dei filmati inconferenti, si chiarisca l'apparente contraddizione rilevata circa il momento e le modalità con cui avviene tale cancellazione (§ 7);

b) per quanto riguarda le videocamere (§ 8): la scheda tecnica delle videocamere sia allegata alla valutazione di impatto, in accordo al principio generale di

accountability; si descrivano più dettagliatamente le misure tecnico-organizzative progettate per garantire la riservatezza dei dati acquisiti con le videocamere, chiarendo le regole in adozione per la generazione, la conservazione, l'utilizzo e la sostituzione delle chiavi di cifratura; per quanto riguarda la possibilità di accedere al contenuto delle videocamere, si argomenti ulteriormente l'affermazione secondo cui le videocamere sono configurate per consentire il trasferimento dei dati acquisiti ai soli dispositivi autorizzati, e cioè le docking station integrate nei totem e i notebook appositamente configurati, spiegando come tale controllo d'accesso è tecnicamente realizzato; circa la Watermarking in fase di acquisizione delle registrazioni, la DPIA dovrebbe contenere delle schermate (screenshot) che dimostrino il meccanismo di tracciamento delle responsabilità;

c) per quanto riguarda i totem multimediali (§ 9): in relazione ai log degli accessi e delle operazioni attuate 'in locale' (ad esempio mediante il 'PC totem'), si chiarisca dove siano custoditi i log, quali informazioni rechino, e come ne sia garantita l'immodificabilità; si approfondiscano i meccanismi adottati per garantire la disponibilità dei dati e gli aspetti di protezione dei dati dai rischi di perdita o danneggiamento accidentali o intenzionali, nei termini descritti in motivazione;

d) per quanto riguarda i notebook(§ 10), si forniscano dettagli sulle misure di sicurezza in esercizio sui notebook, chiarendo, tra l'altro, se sia abilitata la cifratura della memoria disco interna, e il meccanismo di autenticazione adottato, mono o multi fattoriale, argomentando tali scelte;

e) per quanto riguarda le postazioni di lavoro (§ 11) si chiarisca: se l'autenticazione alle postazioni è di tipo mono o multi fattoriale, motivando tale scelta; se i documenti all'atto dell'accesso tramite il server centrale siano copiati sulla memoria disco delle postazioni di lavoro da cui avviene l'accesso, oppure se siano visualizzati da remoto; se i file siano cifrati sia quando conservati nei totem, sia quando eventualmente copiati in locale; se la chiave di cifratura è la medesima per tutti i file custoditi in tutti i totem, argomentando tali scelte; si chiariscano gli altri aspetti evidenziati rispetto al watermark apposto in sovraimpressione in fase di 'visualizzazione e copia'; si illustri più dettagliatamente il meccanismo del watermarking che interviene all'atto della visualizzazione del documento da parte del militare autorizzato, allegando alla DPIA stessa degli screenshot che dimostrino ciò che viene visualizzato a schermo;

f) per quanto riguarda il server centrale (§ 12) si forniscano maggiori dettagli su quali informazioni rechino i log custoditi nel 'server centrale' e come ne sia garantita l'immodificabilità, nonché sulla composizione dei backup custoditi presso il medesimo 'server centrale', specificando quali dati sono messi in sicurezza con tali backup;

g) per quanto riguarda le copie dei file multimediali (§ 13), nel caso della conservazione dei documenti su supporti ottici (DVD) e del trasferimento all'autorità giudiziaria su DVD, si chiarisca quali soluzioni tecnico-organizzative si sia inteso adottare per assicurare che ai DVD possa accedere solo il personale autorizzato e che l'autenticità del contenuto sia verificabile a posteriori, tenendo conto anche delle indicazioni fornite nel § 13.

- E con la seguente raccomandazione, in analogia a quanto rappresentato al Ministero dell'interno per l'omologo sistema:

l) valuti il Comando la possibilità di realizzare la legittima esigenza di condividere i documenti con tutti i soggetti autorizzati al trattamento, senza il ricorso alla generazione di copie di tali documenti, ma prevedendo altre soluzioni, come ad esempio la visualizzazione da remoto dei documenti originari custoditi nei totem.

Roma, 22 luglio 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Mattei