



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Parere sulla valutazione di impatto del Ministero dell'Interno relativo ad un sistema di telecamere indossabili (body-cam), 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 - 22 luglio 2021 [9690691]

VEDI ANCHE [Newsletter del 10 settembre 2021](#)

[doc. web n. 9690691]

Parere sulla valutazione di impatto del Ministero dell'Interno relativo ad un sistema di telecamere indossabili (body-cam), 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 - 22 luglio 2021

Registro dei provvedimenti
n. 290 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, come modificato dal decreto legislativo 10 agosto 2018, n. 101 (di seguito anche "Codice");

VISTO il decreto legislativo 18 maggio 2018, n. 51, recante attuazione della 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 (di seguito anche "Decreto");

ESAMINATA la valutazione preventiva di impatto sulla protezione dei dati personali (di seguito anche "DPIDPIA") del sistema indossabile di videoripresa nei servizi di ordine pubblico (body-cam) del Ministero dell'interno ed i 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 Ministero dell'Interno-Dipartimento della pubblica sicurezza, ha inviato a questa Autorità la valutazione d'impatto sulla protezione dei dati ed un "disciplinare operativo" relativi 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 pubblica, in occasione di eventi o manifestazioni pubbliche.

Occorre ricordare che, in precedenza, il predetto 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 (cfr. provv. 31 luglio 2014, reperibile nel sito internet dell'Autorità, doc. web n [3423775](#)).

Successivamente, nel corso del 2015, il medesimo Dipartimento ha chiesto a questa Autorità un parere sulla sperimentazione, per un periodo di sei mesi, dell'impiego di microcamere da applicare sulla divisa degli operatori che espletano attività di controllo del territorio e di polizia stradale impiegati nei servizi di "squadra volante" delle Questure di Torino, Milano, Roma e Napoli e nelle sezioni di Polizia stradale delle stesse città. Il Garante ha espresso il parere richiesto, indicando condizioni e limiti di tale sperimentazione (cfr. provv. 24 aprile 2015, prot. n. U0012155).

Il Ministero precisa che il sistema di body-cam "a regime", oggetto del presente parere, si discosta dalla precedente sperimentazione, per il ricorso ad una nuova architettura di sistema.

Il parere è reso tenendo conto degli approfondimenti effettuati in piena collaborazione con i competenti uffici del Ministero, 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, in particolare per quanto riguarda i tempi di conservazione dei dati e di cancellazione di quelli irrilevanti.

RILEVATO

2. La struttura del sistema.

La soluzione tecnologica è basata sui seguenti elementi: videocamere indossabili; server centrale, ubicato presso il Centro elettronico (CEN) della Polizia di Stato sito in Napoli; totem multimediali presso i Reparti mobili (ove sono alloggiati un personal computer, software di gestione, docking station per la gestione e la ricarica delle videocamere e le Network Attached Storage (unità NAS) per l'archiviazione delle registrazioni; postazioni di lavoro presso i Gabinetti di polizia scientifica interregionali, regionali e provinciali (personal computer e software di gestione).

Presso il Centro elettronico nazionale (CEN) della Polizia di Stato sono previsti 2 Server di tipo blade all'interno di enclosure e 2 switch Dell Force, mentre presso i 15 Reparti mobili sono distribuite: a) 700 body-cam; b) 91 Docking station con 8 alloggiamenti collegato con hub USB 3.0 a 10 porte; c) 15 switch Dell EMC con porte RJ45 10/100/1000 Gigabit; d) 15 NAS equipaggiati con HD da 2,5", con buffer da 128 MB e 2TB di capacità ciascuno (2 gruppi da 3 unità SSD); e) 15 UPS.

2.1. Finalità del trattamento e scenari di utilizzo.

Il Ministero rappresenta che il personale del Reparto mobile è addestrato e impiegato per effettuare, “in prima linea”, l’azione di contrasto delle condotte violente e di turbamento dell’ordine pubblico e ristabilire “il libero esercizio dei diritti costituzionalmente garantiti in occasione di eventi o manifestazioni pubbliche”. La necessità di documentare le predette azioni illecite, spesso indirizzate proprio contro gli operatori del Reparto mobile, ha determinato l’Amministrazione a individuare nelle videocamere indossabili “lo strumento indispensabile per raccogliere, in un teatro operativo particolarmente complesso, preziosi elementi probatori in ordine a condotte di natura penale”, o per “l’applicazione delle misure di prevenzione personali, anche riguardanti l’ambito delle manifestazioni sportive (DASPO)”. Vi sarebbe, infine, un effetto deterrente del sistema, “specialmente per quanto riguarda le aggressioni rivolte direttamente agli operatori di polizia” (pag. 32 della DPIA).

2.2. Fonti normative.

Molteplici sono le fonti normative indicate dal Ministero quale fondamento del trattamento in argomento e in particolare: l’articolo 55, comma 1, c.p.p., che prescrive alla polizia giudiziaria - tra l’altro - di “... compiere gli atti necessari per assicurare le fonti di prova ...”; l’articolo 234, comma 1, c.p.p., che consente alla polizia giudiziaria “... l’acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo ...”; l’articolo 10, comma 6-quater, del decreto legge 20 febbraio 2017, n. 14, convertito dalla legge 18 aprile 2017, n. 48, (in materia di sicurezza nelle città), secondo cui “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 ... ».

Con riferimento alle disposizioni specifiche in materia di dati personali, la DPIA richiama l’articolo 23, comma 1, del d.P.R. n. 15 del 2018 (regolamento adottato ai sensi dell’articolo 57 del Codice, recante l’individuazione delle modalità di attuazione dei principi in materia di protezione dei dati personali rispetto al trattamento dei dati effettuato, per finalità di polizia, da organi, uffici e comandi di polizia), secondo cui “... L’utilizzo di sistemi di ripresa fotografica, video e audio per le finalità di polizia di cui all’articolo 3, è consentito 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 poste in essere durante il servizio che siano espressione di poteri autoritativi degli organi, uffici e comandi di polizia”.

Infine, viene richiamato il decreto del Ministro dell’interno 24 maggio 2017, recante “Individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirci, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell’esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell’articolo 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196” (Gazz. Uff. 24 giugno 2017, n. 145) che, alla scheda n. 21, denominata “Bodycam 2. Ripresa audio video nei servizi di ordine pubblico”, prevede espressamente il trattamento in argomento.

2.3. I dati trattati e gli interessati.

I dati raccolti ineriscono alle seguenti informazioni personali: registrazione audio e video relativa alla persona, identificabile in base all'aspetto e ad altri elementi specifici; immagine in modalità foto relativa alla persona, identificabile in base all'aspetto e ad altri elementi specifici; data e ora della registrazione; coordinate GPS della registrazione.

Gli interessati sono le persone (identificate o identificabili) cui si riferiscono i filmati o le immagini fotografiche riprese con le videocamere.

2.4. Modalità di impiego.

Le videocamere sono consegnate (prive di dati archiviati nella memoria) al personale del Reparto mobile appositamente designato, come da ordine e foglio di servizio. Ogni body-cam riporta il proprio numero identificativo su un'etichetta esterna. La consegna è annotata in un registro, che documenta l'abbinamento dell'identificativo della videocamera all'operatore che la riceve. Le immagini (video e fotografiche) riportano in sovraimpressione le informazioni riguardanti la data, l'ora e l'identificativo della videocamera.

Al Capo contingente o, quando questi non sia previsto nel servizio, al Capo squadra, è consegnata una busta sigillata contenente la password per consentire la eventuale visualizzazione delle registrazioni sul display delle videocamere consegnate per il servizio.

L'avvio della registrazione da parte degli operatori del Reparto mobile è di regola disposto dall'Ufficiale di pubblica sicurezza responsabile del servizio (o di un settore), 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 anche d'iniziativa dal Capo contingente o dal Capo squadra cui sono assegnate le videocamere, 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 dell'Ufficiale di pubblica sicurezza responsabile del servizio, che comunque deve essere informato appena possibile. Può, infine, essere avviata direttamente dai componenti della squadra dotati di 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 Capo squadra, del Capo contingente o dell'Ufficiale di pubblica sicurezza responsabile del servizio. Il Capo squadra di riferimento deve essere informato appena possibile.

Non è ammessa la registrazione continua delle immagini nel corso del servizio e tantomeno quella episodica riferita ad eventi non connotati dal requisito della "criticità".

La registrazione è interrotta quando venga meno la necessità di documentare gli eventi e, in ogni caso, su disposizione dell'Ufficiale di pubblica sicurezza responsabile del servizio. Può anche essere interrotta su disposizione del Capo contingente o del Capo squadra, quando siano venute meno le necessità e l'Ufficiale di pubblica sicurezza responsabile del servizio sia oggettivamente impossibilitato a intervenire, dovendo comunque essere informato appena possibile. Può infine essere interrotta dal componente della squadra quando venga meno la necessità di documentare gli eventi e sia oggettivamente impossibilitato a contattare il Capo contingente o il Capo squadra o l'Ufficiale di pubblica sicurezza responsabile del servizio.

In ogni atto che documenti il servizio (relazioni, annotazioni, ecc.) il personale del Reparto mobile riporta i dati relativi alle registrazioni effettuate (inizio, fine, identificativo della videocamera, ecc.).

2.5. Operazioni di trattamento.

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

Al rientro dal servizio, gli operatori restituiscono la videocamera al Reparto mobile. Gli apparati sono immediatamente collegati al totem multimediale (docking station) a cura dell'operatore appositamente autorizzato al trattamento da parte del dirigente del reparto, per il download dei file. Il download dei file avviene sul NAS integrato nel totem multimediale del Reparto mobile. Con il download i file sono cancellati automaticamente dalla memoria della videocamera; la cancellazione di tali dati avviene unicamente collegando il dispositivo al totem multimediale (altre funzioni di cancellazione sono disabilitate).

I metadati estratti dai file memorizzati nel NAS (nome del file, data e ora di origine, codice identificativo della videocamera, Reparto mobile ove risiede il dato, indirizzo IP del NAS che ospita il dato, HASH del file, coordinate GPS della registrazione), sono poi inviati in maniera automatica al server centrale ubicato presso il CEN della Polizia di Stato.

In via ordinaria, la visione ed estrazione di copia dei file multimediali avviene tramite connessione al server centrale del CEN che indicizza i metadati, per mezzo delle postazioni client della Polizia scientifica. Gli utenti della Polizia scientifica per accedere al sistema sono autenticati con username e password e abilitati a svolgere dette operazioni. Il flusso di comunicazione è cifrato con protocollo SSL.

Il server centrale del CEN consente agli utenti autorizzati di operare ricerche tramite i metadati disponibili e di accedere e prelevare dati dai NAS attestati presso i Reparti mobili.

Presso il server centrale sono mantenuti in memoria file di log non modificabili, relativi agli accessi e alle operazioni compiute dagli utenti. I file di log sono conservati senza limitazioni temporali. 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).

Per urgenti esigenze di polizia giudiziaria o di pubblica sicurezza, l'Ufficiale di pubblica sicurezza responsabile del servizio può anche disporre che le registrazioni siano copiate sul personal computer della Polizia scientifica, per averne l'immediata disponibilità. In tal caso i dati non vengono cancellati dalla memoria della videocamera, in quanto devono essere successivamente trasferiti sul NAS del Reparto mobile. Le registrazioni di cui è estratta copia possono essere visionate dal predetto ufficiale di pubblica sicurezza, al quale può anche essere fornita copia ove richiesta. Nella relazione di servizio degli operatori della Polizia scientifica deve essere dato atto di tali operazioni.

Le registrazioni acquisite direttamente dalla Polizia scientifica possono essere successivamente trasmesse al Capo ufficio della competente unità organizzativa della Questura che le abbia formalmente richieste. I personal computer dei Gabinetti di Polizia scientifica per ricevere i file direttamente dalle videocamere devono essere dotati di specifico software di gestione e autorizzati a livello di rete (indirizzi IP statici) per accedere al server centrale del CEN di Napoli. Gli utenti della Polizia scientifica per accedere al sistema sono autenticati con username e password individuale e autorizzati. I dati "scaricati" sui personal computer dei Gabinetti di polizia scientifica per le immediate esigenze delle Questure, sono cancellati una volta venuta meno la necessità che ne ha giustificato la raccolta immediata (es. dopo che le registrazioni rilevanti ai fini di polizia giudiziaria e di pubblica sicurezza sono state trasmesse ai competenti uffici della Questura). In ogni caso tali registrazioni devono essere cancellate quando quelle "corrispondenti" sono state memorizzate nel NAS del Reparto mobile.

Infine, nell'immediatezza degli eventi, le registrazioni possono essere visionate direttamente sul display della videocamera da parte dell'Ufficiale di pubblica sicurezza responsabile del servizio che ne faccia esplicita richiesta al Capo contingente o Capo squadra, in possesso della password

custodita in busta sigillata. Ove non sia stato necessario visionare le immagini sul display della videocamera, Il Capo contingente o il Capo squadra restituiscono la busta sigillata contenente la password. Nel caso sia stato necessario visionare le immagini e pertanto aprire la busta, consegnano anche una relazione. Le password delle videocamere sono di conseguenza "rinnovate". L'operatore del Reparto mobile non dispone della predetta password e, quindi, non può visionare sulla videocamera i contenuti multimediali.

2.6. Soggetti autorizzati al trattamento dei dati.

La DPIA prevede espressamente - alla stregua della pertinente disciplina in materia di protezione dei dati - la designazione delle persone autorizzate al trattamento e, per ciascuno di essi, la definizione degli ambiti di trattamento, a cura dei rispettivi organi di vertice o degli uffici individuati (ad esempio il Dirigente del Reparto mobile provvede per i trattamenti effettuati dai dipendenti incaricati di effettuare le registrazioni con le videocamere e dai "referenti tecnici").

2.7. Durata della conservazione dei dati.

In relazione alle specifiche finalità perseguite con i trattamenti in esame, tenendo conto della composizione tra le esigenze di polizia e quelle contrapposte di tutela dei dati personali, la DPIA individua in sei mesi il termine di conservazione dei dati personali acquisiti. Detto termine si applica ai dati memorizzati nei NAS dei Reparti mobili e al suo spirare le registrazioni sono irreversibilmente cancellate con modalità automatica.

Conformemente a quanto stabilito dall'articolo 10 comma 3, lett. u), del d.P.R. n. 15 del 2018, ai dati raccolti mediante sistemi di ripresa fotografica audio e video nei servizi di ordine pubblico e di polizia giudiziaria, si applicano i diversi termini di conservazione di cui alla lettera b) del medesimo comma, quando i dati personali sono confluiti in un procedimento per l'applicazione di una misura di prevenzione, o quelli di cui alle lettere a), f), g), h) e i), quando i dati personali sono confluiti in un procedimento penale.

2.8. Cancellazione dei dati accidentali.

Le registrazioni avviate accidentalmente, in mancanza del requisito della necessità o avviate in previsione dell'insorgenza di situazioni "critiche" che non si siano poi verificate, sono cancellate tempestivamente dagli "amministratori di sistema" nazionali a seguito della formale richiesta dell'Ufficiale di pubblica sicurezza responsabile del servizio, inviata da questi nel più breve tempo possibile.

L'individuazione concreta dei file multimediali da cancellare dal NAS del Reparto mobile è operata dall'Ufficiale di pubblica sicurezza responsabile del servizio (o di un settore), anche su segnalazione dell'operatore che ha effettuato la registrazione, previa visione delle stesse, anche direttamente sulle body-cam, per la verifica della ricorrenza delle predette condizioni.

Al riguardo la DPIA prevede che il Dipartimento della p.s. dirami ai Questori e, per conoscenza, al Garante apposite Linee guida per gli Ufficiali di pubblica sicurezza impiegati nei servizi di ordine pubblico ove sono utilizzate videocamere indossabili, al fine di assicurare che la raccolta e le operazioni di trattamento delle registrazioni siano effettuati conformemente a quanto disposto dalla valutazione d'impatto.

RITENUTO

3. Consultazione preventiva del Garante.

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.

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, 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" (comma 4).

Nella DPIA si rileva che l'esigenza di gestire adeguatamente i rischi presenti nel trattamento delle immagini raffiguranti persone (identificate o identificabili) riprese in contesti pubblici ove sono commessi atti illeciti, ha determinato il Dipartimento della pubblica sicurezza a svolgere una valutazione di impatto sulla protezione dei dati, per individuare le misure organizzative e tecniche più idonee a mitigare i rischi per i diritti e le libertà degli interessati (pag. 14) e a consultare il Garante pur non ritenendosi necessario (pag. 45) .

Tuttavia, si osserva che nel caso di specie, tenuto conto delle finalità del trattamento, i rischi potenziali per gli interessati che sono ragionevolmente ipotizzabili appaiono elevati o molto elevati, spaziando dalla discriminazione alla sostituzione di identità, al pregiudizio per la reputazione e all'ingiusta privazione di diritti e libertà, per cui, qualora si verificassero in concreto, l'impatto derivante in danno degli interessati sarebbe elevato o molto elevato.

In conclusione, l'attività sottesa alla DPIA e i relativi trattamenti risultano ad elevato rischio per gli interessati, onde si ritiene dovuta la consultazione preventiva dell'Autorità di controllo.

4. 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. Nondimeno, alla luce del provvedimento del Garante del 25 marzo 2021, n. 127 (reperibile nel sito web dell'Autorità, doc. web n. [9575877](#)), occorre specificare nel documento che il sistema non integra dispositivi tecnici specifici diretti a consentire l'identificazione univoca o l'autenticazione di una persona fisica (facial recognition).

5. Durata della conservazione delle immagini.

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, il Ministero dell'interno 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 notizia criminis non sempre è immediatamente percepibile “sul campo” dagli operatori di polizia. Di fatto, occorre sovente esaminare 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 (v. § 2.7).

6. Gestione delle body-cam e raccolta delle immagini.

In relazione agli aspetti concernenti la gestione delle body-cam e della raccolta delle immagini si osserva quanto segue:

- a) il documento va integrato con riguardo alle chiavi di cifratura delle password che consentono al personale autorizzato, qualora le circostanze lo richiedano, di visualizzare le foto e i filmati acquisiti mediante il mini-display integrato nelle videocamere prima che questi siano trasferiti nei totem;
- b) occorre prevedere sistemi che consentano la tracciabilità delle operazioni di cancellazione dei dati personali da parte dei referenti tecnici;
- c) la DPIA prevede che la registrazione possa essere interrotta anche dal componente della squadra, quando venga meno la necessità di documentare gli eventi e sia oggettivamente impossibilitato a contattare il Capo contingente o il Capo squadra o l’Ufficiale di pubblica sicurezza responsabile del servizio. Appare opportuno prevedere che, in questo caso, il superiore gerarchico debba essere comunque informato, appena possibile;
- d) apparenti discrasie riguardano le funzioni di controllo di accesso e di cifratura descritte nel documento e le evidenze documentali che emergono dall’allegata scheda tecnica. In particolare, le specifiche tecniche allegate (pag. 53 della DPIA) non elencano alcuna funzionalità di controllo di accesso tramite password, di cifratura o di altri meccanismi che consentano la copia e il trasferimento dei documenti acquisiti alle sole postazioni autorizzate. Inoltre, la memoria sembrerebbe essere di tipo amovibile, cioè una ‘scheda da 8GB contenuta nella confezione’, a differenza di quanto descritto nella DPIA. Al riguardo si ritiene necessario un chiarimento;
- e) si accenna, inoltre, alla presenza di una ‘interfaccia di espansione’(pag. 18 della DPIA), formulazione questa tecnicamente non comprensibile che andrebbe chiarita.

7. Totem multimediali.

Con riferimento al funzionamento dei c.d. totem multimediali, si osserva quanto segue:

a) in base a quanto riportato nel documento in esame, i totem multimediali sono dotati, tra l'altro, di computer integrati, l'accesso ai quali è protetto da password e su tali computer opera un antivirus (pag. 43 della DPIA). Non è chiaro se tali postazioni siano dotate anche di monitor e tastiera per l'accesso in locale (ad esempio per l'inserimento della chiave di decifratura dei documenti da trasferire dalla videocamera); la DPIA prevede poi che i computer integrati consentano di connettersi al server per eseguire le ricerche sui metadati e di eseguire il download dei contenuti. Al riguardo, occorre indicare con maggior precisione chi può accedere in locale, con quale profilo autorizzativo e quali operazioni possa compiere;

b) appare opportuno specificare in cosa consistano le operazioni di 'manutenzione del totem' affidate ai referenti tecnici e con quale profilo autorizzativo siano effettuate (pag. 21 della DPIA);

c) la DPIA indica che le registrazioni degli accessi e delle operazioni (log) sono mantenute presso il server centrale (pag. 16). Non è chiaro, tuttavia, se presso il server centrale siano conservati anche i log degli accessi e delle operazioni compiute sui totem, comprese le operazioni di manutenzione, e quale sia il meccanismo adoperato a garanzia della loro non modificabilità. Al riguardo appare necessario un chiarimento;

d) andrebbe descritto più chiaramente quale sia il meccanismo di autenticazione informatica adoperato per l'accesso e lo spostamento dalle videocamere ai totem dei documenti acquisiti (filmati e foto), quando posizionate sulle docking station. Andrebbe chiarito, inoltre, il meccanismo hardware o software implementato per garantire che al totem possano essere collegate le sole videocamere autorizzate;

e) per quanto riguarda la protezione dei dati dai rischi di perdita o danneggiamento accidentali o intenzionali, la DPIA indica che i dischi sui NAS dei totem sono in configurazione ridondata e che presso il CEN viene tenuto un backup, ma non è chiaro se tale backup sia relativo anche ai dati custoditi nei totem (pag. 43). La configurazione ridondata dei dischi non è di per sé sufficiente a mitigare tutti i rischi informatici suscettibili di compromettere la disponibilità dei dati (ad esempio, in caso di attacco ransomware la configurazione ridondata replicherebbe la cifratura malevola su tutti i dischi, causando la perdita irreversibile dei dati. Altro esempio è il caso di guasto hardware del controller del dispositivo che pilota i dischi); alla ridondanza fisica dei dischi, vanno affiancate copie di backup dei dati, da custodire su supporti differenti dai NAS dei totem. Al riguardo si ritiene necessario integrare la DPIA sotto tali aspetti.

8. Le postazioni di lavoro della Polizia scientifica.

Le postazioni dei Gabinetti di polizia scientifica possono essere utilizzate per l'estrazione immediata dei documenti dalla videocamera tramite una connessione via cavo USB e uno specifico 'software gestionale', senza attendere il riversamento delle immagini dalle videocamere nei totem. Tale estrazione crea una copia (si ipotizza un duplicato) dei documenti contenuti nella videocamera sulle postazioni della Polizia scientifica.

Ciò premesso, con riguardo al fatto che le postazioni remote sono abilitate al collegamento con il CEN mediante l'assegnazione di indirizzi IP statici, la DPIA dovrebbe prevedere l'insieme delle misure in adozione che rendano improbabile il rischio di IP spoofing.

Inoltre, sebbene la DPIA sottolinei che i computer della scientifica siano dotati di antivirus, non specifica il meccanismo di autenticazione ai desktop e ai notebook adottato, né se i dischi siano o

meno cifrati. Essa va, pertanto, integrata in tal senso.

9. Il server centrale.

La DPIA dovrebbe chiarire se il 'server centrale' sia o meno accessibile via internet o solo tramite intranet/VPN (virtual private network), in particolare dalle postazioni di lavoro in mobilità, cioè i notebook della scientifica. Dovrebbe inoltre individuare i rischi informatici cui tale componente è esposta e chiarire quali siano le precauzioni adottate per mitigarli. A titolo esemplificativo, dovrebbe chiarire le misure adottate contro eventuali attacchi di tipo brute force/dictionary e di SQL injection.

Dovrebbe anche argomentare perché ritiene che una procedura di autenticazione mono-fattoriale basata solo su username e password (pag. 15), sia considerata adeguata ai rischi. Dovrebbe, infine, chiarire se i backup dei dati (pag. 43) sono relativi ai soli metadati o anche ai documenti (video e foto) custoditi presso i totem.

10. Registro delle assegnazioni.

In base a quanto riportato nel documento, l'assegnazione della videocamera di servizio ad un operatore è annotata in un registro abbinando l'identificativo della videocamera all'operatore che la riceve. Ciò al fine di risalire, in caso di necessità, al soggetto che ha effettuato le registrazioni, anche per eventuali responsabilità. Sarebbe, pertanto, opportuno descrivere gli accorgimenti tecnico-organizzativi adottati per garantire la riservatezza e la disponibilità delle informazioni in esso contenute, ed evitarne la modifica non autorizzata.

11. Gestione delle copie delle immagini.

Molteplici sono i casi previsti dalla DPIA in cui possono essere realizzate copie dei filmati e delle foto effettuati tramite le videocamere. Tali dati possono essere copiati nelle postazioni della Polizia scientifica prima di essere trasferiti nei totem (pagg. 15 e 36). Gli operatori di Polizia scientifica possono estrarre copia dei filmati e delle foto già custodite nei totem. Ancora, copia dei file può essere consegnata all'Ufficiale di pubblica sicurezza, 'ove richiesta'. Inoltre, 'le registrazioni acquisite direttamente dalla Polizia scientifica possono essere successivamente trasmesse al Capo ufficio della competente unità organizzativa della Questura che le abbia formalmente richieste' (pag. 22). In generale, tutti gli utenti autorizzati (non meglio specificati) possono accedere ed estrarre copia dei file dai totem (pag. 22).

Tali copie sono trasferite in luoghi informatici diversi dalle videocamere e dai totem protetti con il controllo degli accessi e la registrazione delle operazioni effettuate. Tuttavia, anche le copie sono suscettibili di generare danni per gli interessati, alla stregua dei file da cui traggono origine. Pertanto, la DPIA dovrebbe descrivere le misure adottate per garantire la riservatezza dei duplicati dei documenti altrove trasmessi e custoditi, e gli accessi e le operazioni su tali copie andrebbero ugualmente registrate tramite log.

Occorre anche garantire l'autenticità dei documenti, consentendo di verificare che le copie, altrove conservate, siano esatte ed integre, cioè che non siano state in qualche modo modificate, indebitamente o accidentalmente, nel processo di trasmissione o di conservazione nel nuovo sito.

Sul punto, si dà conto che il Ministero ha previsto che tra i metadati (custoditi nel CEN) dei documenti acquisiti mediante videocamere, figurino anche le impronte digitali (c.d. hash) dei file. Tuttavia, sulla base delle informazioni riportate nella valutazione di impatto, la verifica dell'autenticità della copia di un file non sembrerebbe essere un'operazione eseguibile in maniera intuitiva ed immediata, alla portata di persone senza competenze informatiche specialistiche. Essa, infatti, richiederà la generazione (mediante tool informatici specifici) e il confronto dell'impronta digitale della copia, con l'impronta digitale del file originario, custodita nel database

del CEN.

Resta il dubbio, quindi, che la complessità operativa intrinseca in tale modalità di verifica dell'autenticità possa rivelarsi, all'atto pratico, un disincentivo ad avvalersene.

In generale, occorre rilevare che la trasmissione di copie di documenti al di fuori del perimetro di sicurezza informatica delineato con le misure tecniche descritte nella valutazione di impatto, rende più complesso sul piano organizzativo il mantenimento di un livello di sicurezza del trattamento costantemente elevato ed adeguato ai rischi.

Ciò premesso, valuti, pertanto, l'Amministrazione 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 ad esempio la visualizzazione da remoto dei documenti originali custoditi nei totem, mantenendo, pertanto, un controllo puntuale sugli accessi e, al contempo, fornendo intrinseca garanzia di autenticità e di integrità dei documenti visualizzati.

Peraltro, l'operazione stessa di creare copie (identiche) di uno stesso dato, non solo mina l'efficacia delle misure di sicurezza individuate, ma genera nuovi rischi legati all'integrità e, dunque, all'autenticità del dato che andrà nel tempo garantita. Probabilmente, l'esigenza di consentire la visualizzazione e l'analisi dei filmati e delle foto acquisite ai vari soggetti autorizzati al trattamento andrebbe affrontata con soluzioni tecniche differenti, consentendo, appunto, la visualizzazione solo da remoto e del solo file originario, unica copia esistente e dunque certamente autentica, mediante sandbox (ad esempio, un browser web dotato di appositi plugin, quale il plugin 'widevine', <https://en.wikipedia.org/wiki/Widevine>, che implementa un sistema di protezione dei contenuti già integrato nei principali browser web e free to use), in grado di garantire con ragionevole certezza l'autenticità dei contenuti, impedire l'estrazione di copie identiche e ostacolare la generazione di altri tipi di copie (ad esempio tramite tool di screen recording).

TUTTO CIÒ PREMESSO IL GARANTE

esprime parere favorevole in ordine alla valutazione di impatto sulla protezione dei dati personali del sistema indossabile di videoripresa nei servizi di ordine pubblico (body-cam) trasmessa dal Ministero dell'interno,

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

a) si specifichi che il sistema non integra dispositivi tecnici diretti a consentire l'identificazione univoca o l'autenticazione di una persona fisica (facial recognition) (§ 4);

b) in relazione alla gestione delle body-cam: si specifichino le caratteristiche delle chiavi di cifratura che consentono agli Ufficiali di polizia di visualizzare le foto e i filmati acquisiti mediante il mini-display integrato nelle videocamere; si specifichi attraverso quali accorgimenti è assicurata la tracciabilità delle operazioni di cancellazione delle immagini presenti nelle body-cam da parte i referenti tecnici; si preveda che quando la registrazione può essere interrotta dal componente della squadra oggettivamente impossibilitato a contattare il Capo contingente o il Capo squadra o l'Ufficiale di pubblica sicurezza responsabile del servizio, il superiore gerarchico debba essere comunque informato; si verifichi la corrispondenza delle specifiche dell'allegato tecnico relativo alle videocamere a quanto indicato nella DPIA (§ 6);

c) in relazione ai totem multimediali si precisi: se i computer integrati nei totem multimediali siano dotati anche di monitor e tastiera per l'accesso in locale, specificando chi può accedere in locale, con quale profilo autorizzativo e quali operazioni possa compiere; in cosa consistano le operazioni di manutenzione del totem affidate ai referenti tecnici e con quale profilo autorizzativo siano effettuate; se presso il server centrale siano conservati anche i log degli accessi e delle operazioni compiute sui totem, comprese le operazioni di manutenzione, e quale sia il meccanismo adoperato a garanzia della loro non modificabilità; quale meccanismo hardware o software è stato implementato per garantire che al totem possano essere collegate le sole videocamere autorizzate; specificare se il backup dei dati custodito presso il CEN è relativo anche ai documenti acquisiti (filmati e foto) custoditi nei totem e, in caso contrario, prevedere il backup di questi ultimi dati da custodire su supporti differenti dai NAS dei totem (§ 7);

d) in relazione alle postazioni di lavoro della Polizia scientifica si specifichi: se il meccanismo di autorizzazione delle postazioni della polizia scientifica presso il CEN di Napoli si basi solo sull'indirizzo IP statico, nel qual caso, indicando l'insieme degli accorgimenti tecnico-organizzativi adottati per prevenire attacchi di tipo IP spoofing; il meccanismo adottato di autenticazione ai desktop e ai notebook della scientifica e se i dischi siano o meno cifrati (§ 8);

e) si specifichi se il server centrale sia accessibile via Internet o solo tramite intranet/VPN, in particolare dalle postazioni di lavoro in mobilità, cioè i notebook della scientifica; individuare i rischi informatici cui tale componente è esposta e chiarire quali sono le precauzioni adottate per mitigarli; indicare i motivi per i quali si ritiene che una procedura di autenticazione mono-fattoriale basata solo su username e password sia considerata adeguata ai rischi (§ 9);

f) si individuino accorgimenti tecnico-organizzativi per garantire la riservatezza e la disponibilità delle informazioni contenute nel registro delle assegnazioni ed evitarne la modifica non autorizzata (§ 10);

- E con la seguente raccomandazione:

l) valuti l'Amministrazione 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 originali custoditi nei totem, nei termini di cui al § 11.

Roma, 22 luglio 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Mattei