PROTEZIONE DEI DATI E SERVIZI CLOUD PUBBLICI PER L'ARCHIVIAZIONE A FINI DI POLIZIA – IL CASO SPECIFICO DI DATI RACCOLTI ATTRAVERSO MICROCAMERE PER PROTEGGERE L'ORDINE PUBBLICO E LA SICUREZZA

Roma, 28 aprile 2016

White paper di
Luca Bolognini
Avvocato, Presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei dati

Abstract

Il presente documento si inserisce nell'ormai consolidato dibattito sulla compatibilità di soluzioni *cloud* con la disciplina in materia di protezione dei dati personali. In particolare, è diretto ad approfondire, concisamente, un aspetto non frequentemente esplorato, quello della compatibilità nel settore delle attività di polizia per scopi connessi con la protezione dell'ordine pubblico e della sicurezza. Il tema è per sua natura ampio, si è perciò scelto di focalizzare l'attenzione su un aspetto di interesse ben circoscritto, quello dell'adozione di *cloud* IaaS per l'archiviazione del materiale girato attraverso "*body cam*„ o "microcamere„ in dotazione a forze di polizia. La scelta appare appropriata, se si considera sia la già avviata sperimentazione di questi dispositivi nel recente passato sia l'esigenza di ampia disponibilità di risorse per l'archiviazione che si presta particolarmente all'utilizzo di soluzioni *cloud*, tenuto conto del notevole numero di dispositivi di registrazione, del fatto che essi sono tendenzialmente ad alta definizione, del numero di ore di girato, il che richiede la disponibilità di imponenti risorse informatiche per la memorizzazione.

Si ritiene superfluo ai fini del presente lavoro ripercorrere i rapporti tra normativa in materia di protezione dei dati personali e tecnologia *cloud*. La

tematica è infatti ben nota e consolidata. Piuttosto sarà effettuata una specifica, ancorché rapida, ricognizione della parte speciale del d.lgs. 30 giugno 2003, n. 196 (di seguito anche "codice privacy„ o "cod. priv.") in materia di trattamenti di polizia. Si tratta in particolare del titolo II, parte II, cui va aggiunto l'art. 175[1].

Accanto all'analisi normativa condotta sul codice privacy saranno concisamente sviluppate altre due linee di approfondimento:

- quella ricostruttiva del quadro normativo primario applicabile ai sistemi informatici in dotazione alle forze di polizia. Si tratta soprattutto, se non esclusivamente, della disciplina in materia di Centro elaborazione dati (CED) cd. "interforze", che assorbe, per rilevanza, la normativa di settore, come emerge dal richiamo espresso fatto agli artt. 53 – 57 cod. priv.;

- quella amministrativistica, sia pure in maniera assai stringata, posto che la soluzione di archiviazione in esame si pone al servizio di pubbliche amministrazioni.

Si trarranno conclusioni positive dal quadro normativo sopra concisamente accennato, circa il legittimo uso di servizi cloud per l'archiviazione dei dati trattati con microcamere indossabili, anche laddove (sia pure con alcune precisazioni e cautele) i server siano collocati al di fuori dell'area UE/SEE. Nella parte finale del lavoro si esaminerà la questione della corretta allocazione dei ruoli attivi di trattamento tra i vari soggetti coinvolti e si darà conto delle specifiche contrattuali attese, nel rispetto del migliore inquadramento della materia.

1 Si segnala che non ci si occuperà dell'Allegato C al codice relativo a trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia, in quanto tuttora non emanato, per mancanza dei necessari decreti ministeriali attuativi. Si tratta dei decreti del Ministero della Giustizia di cui all'art. 46, co. 2 cod. priv. relativo ai trattamenti per finalità di giustizia e di quello del Ministero dell'Interno ai sensi dell'art. 53, co. 3 cod. priv. relativo ai trattamenti per finalità di polizia. Potrà perciò accadere che il quadro normativo subisca cambiamenti in futuro.

1. Finalità del trattamento con microcamere indossabili.

Ogni analisi in materia di protezione dei dati personali muove da un corretto inquadramento delle finalità. Orbene, ai sensi dell'art. 53, co. 1, cod. priv. "*si intendono effettuati per finalità di polizia i trattamenti di dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati*". Ne segue che il trattamento attraverso microcamere indossabili si inserisce senza difficoltà nella generale finalità di polizia. Ciò trova puntuale conferma in una decisione del Garante su analoga questione, cfr. GPDP, Parere in tema di uso di microcamere indossabili da parte della polizia del 31 luglio 2014, doc. web n. 3423775. Ci si muove in definitiva nell'ambito dei trattamenti con strumenti elettronici, in particolare ICT, per finalità di polizia. Più nello specifico, nel presente lavoro ci occupiamo della funzione di protezione dell'ordine e della sicurezza pubblica.

2. Ricostruzione essenziale della normativa in materia di servizi informatici di polizia

Le principali fonti normative di riferimento appaiono le seguenti:

- L. 1 aprile 1981, n. 121, artt. 6-11, recante: *"Nuovo ordinamento dell'Amministrazione della pubblica sicurezza"*, che disciplina l'istituzione del Centro elaborazione dati (il già detto "CED") "interforze", indicando per linee essenziali la tipologia dei dati raccolti e i flussi;

- D.P.R. 3 maggio 1982, n. 378, recante: *"Approvazione del regolamento concernente le procedure di raccolta, accesso, comunicazione, correzione,*

cancellazione ed integrazione dei dati e delle informazioni, registrati negli archivi magnetici del centro elaborazione dati di cui all'art. 8 della legge 1 aprile 1981, n. 121", che disciplina più nello specifico operazioni di raccolta, accesso, comunicazione, correzione, cancellazione e integrazione dei dati e delle informazioni;

- L. 26 marzo 2001, n. 128, art. 21, recante "*Interventi legislativi in materia di tutela della sicurezza dei cittadini*", che disciplina il conferimento da parte delle Forze di polizia al CED delle notizie, delle informazioni e dei dati acquisiti nel corso dell'attività di prevenzione e repressione dei reati.

3. Nello specifico: il CED interforze e le informazioni trattate

Per realizzare il coordinamento organizzativo dei dati connessi con l'attività di polizia, è istituito ai sensi dell'art. 8 della L. 121/1981 il già detto CED interforze presso il Dipartimento di pubblica sicurezza, Direzione centrale della polizia criminale, del Ministero dell'interno.

L'attività di classificazione e raccolta dei dati presso il CED, ai sensi degli artt. 6, co. 1, lett. a) e 9 L. 121/1981 e art. 1 del D.P.R. 378/1982, è finalizzata al soddisfacimento delle esigenze inerenti alle attività di tutela dell'ordine e della sicurezza pubblica e prevenzione e repressione dei reati e della criminalità da parte della polizia di sicurezza e della polizia giudiziaria. Il CED, in particolare, assolve allo scopo di fornire un punto di convergenza per le iniziative investigative al fine di incrociare informazioni utili e tenere una traccia storica degli elementi di indagine[2]. Nello specifico, le operazioni di trattamento svolte presso il CED consistono nella "*raccolta, elaborazione,*

2 Le principali applicazioni informatiche sono rese disponibili nell'ambito del Sistema di indagine (SDI) che consente di collegare le informazioni contenute nei diversi *database* riorganizzandole secondo un modello relazionale di base di dati focalizzato sui reati e sulle notizie di reato.

classificazione e conservazione negli archivi magnetici delle informazioni e dei dati" conferiti dalle Forze di polizia[3] nell'attuazione e nell'esercizio delle attribuzioni in materia di ordine e sicurezza pubblica, e nella "*loro comunicazione ai soggetti autorizzati*".

Una risorsa *cloud* potrebbe dunque, in prima approssimazione, fornire supporto all'operazione di conservazione dei dati suddetti nel CED. Tuttavia, occorre preliminarmente individuare quale tipologia di informazioni confluisca effettivamente nel CED. Orbene, risulta dal disegno normativo primario che il centro non archivi tanto le fonti originarie quanto piuttosto *estrapolazioni* di dati dalle medesime, oppure, che è lo stesso, estrazioni di contenuti *essenziali*, come se il legislatore avesse disegnato il CED più come una sorta di mappa o centro di smistamento e di re-indirizzamento, che non sposta le fonti originarie ma dirigendo verso quelle l'investigatore. Più nello specifico, ai sensi degli artt. 6, co. 1, lett. a) e 7 L. 121/1981 sono trattate nel CED "*le informazioni e i dati risultanti da documenti... conservati dalla pubblica amministrazione o da enti pubblici, o risultanti da... indagini di polizia*". Ancora più chiaramente l'art. 21 L. 128/2001 menziona il "*contenuto di atti, informative e documenti prodotti dalle Forze di polizia e i dati essenziali delle altre notizie qualificate di reato*". Tendenzialmente perciò nel CED non viene archiviata l'intera documentazione dell'attività compiuta dagli agenti (es: verbali di identificazione, di arresto, ecc.), che tende a rimanere invece

3 Art. 16, L. 121/1981 – Forze di polizia "*Ai fini della tutela dell'ordine e della sicurezza pubblica, oltre alla polizia di Stato sono forze di polizia, fermi restando i rispettivi ordinamenti e dipendenze:*
a) l'Arma dei carabinieri, quale forza armata in servizio permanente di pubblica sicurezza;
b) il Corpo della guardia di finanza, per il concorso al mantenimento dell'ordine e della sicurezza pubblica.
Fatte salve le rispettive attribuzioni e le normative dei vigenti ordinamenti, sono altresì forze di polizia e possono essere chiamati a concorrere nell'espletamento di servizi di ordine e sicurezza pubblica il Corpo degli agenti di custodia e il Corpo forestale dello Stato.
Le forze di polizia possono essere utilizzate anche per il servizio di pubblico soccorso". Naturalmente, andranno ricompresi anche gli agenti di polizia municipale ove autorizzati dal Prefetto, ex art. 5 L. 65/1981.

presso gli uffici o comandi di polizia. Ulteriori conferme si leggono agli artt. 4, 5, co. 2 e 7, co. 1 D.P.R. 378/82.

Ciò non comporta che tale struttura "sintetica" del CED non possa subire modifiche o integrazioni ove opportuno, tuttavia va preso atto che, allo stato, appare corretto ritenere che, in un'ideale architettura della rete, un servizio *cloud* come quello in esame non debba, o non debba necessariamente, allacciarsi direttamente al CED, quanto piuttosto ai comandi delle forze dell'ordine che fanno diretto uso delle microcamere e che conservano appunto le fonti originarie di informazioni. Comunque, sullo stretto piano della normativa in materia di protezione dei dati personali, le garanzie previste dal codice privacy, sono applicabili sia al CED sia a qualsiasi altro sistema informatico o banca dati in uso alle forze di polizia. Sono ugualmente estese a questi eventuali diversi sistemi informatici (che allo stato comunque non risultano oggetto di normativa primaria) le tutele già operanti in relazione al CED interforze, come disposto dall'art. 56 cod. priv.[4]. In sostanza perciò, il quadro normativo esistente appare insensibile rispetto alla specifica architettura che si vorrà adottare nel collegamento del *cloud* a sistemi informatici e telematici di polizia e che potrà tradursi anche nella creazione di una nuova banca dati *ad hoc*. Da notare che verosimilmente ciò richiede, ove siano sviluppati specifici strumenti di riconoscimento facciale e di comparazione delle immagini per la consultazione della banca dati, l'adozione preventiva, ai sensi dell'art. 55 cod. priv., delle garanzie previste

4 Pienamente ammissibile la costituzione di ulteriori banche dati per finalità di polizia. Tale possibilità è peraltro già contemplata all'art. 54, co. 3 cod. priv. È stato osservato: *"Quale che sia il regime di tali banche dati diverse dal CED, soprattutto con riguardo alla loro istituzione non appare chiaro ma ciò che conta è che […] il Codice non vieta la possibilità di creare o mantenere banche dati per il più efficace espletamento delle finalità connesse, ex art. 53, alla sicurezza ed ordine pubblico e alla prevenzione, accertamento e repressione dei reati, ma esige la loro conformità ai principi fondamentali in tema di trattamento dei dati personali"*, cfr. BORRELLO, FROSINI, MANETTI, *Attività delle forze di polizia e trattamento dei dati personali*, Maggio Editore, Santarcangelo di Romagna, 2012, p. 60.

dall'art. 17 cod. priv., ossia l'esecuzione di una verifica preliminare presso il Garante per la protezione dei dati personali.

4. Procedure per l'accesso al CED: vincoli e autorizzazioni

Ai fini della determinazione delle attività eventualmente esternalizzabili in *cloud* si pone la questione fondamentale di comprendere se vi siano limiti e prescrizioni normative da rispettare in relazione alle operazioni compiute sulle informazioni e se questi limiti e prescrizioni si riflettano negativamente sulla esternalizzazione in *cloud*. Ci si limiterà alla normativa primaria, anche per l'oggettiva difficoltà di richiamare esaustivamente tutte le eventuali norme tecniche di dettaglio emanate ai sensi dell'art. 12 del D.P.R. 378/82 dalla commissione di cui all'art. 8, co. 3, L. 121/81.

Giova notare che l'accesso ai dati del CED è particolarmente presidiato, essendo consentito, *ex* artt. 9 L. 121/81 e 9 D.P.R. 378/82 solo ai funzionari dell'ufficio per il coordinamento e la pianificazione addetti al settore, a personale appartenente alle forze di polizia munito di apposita autorizzazione rilasciata dal direttore del predetto ufficio[5] e, con alcune limitazioni, agli agenti di pubblica sicurezza della polizia municipale[6] e agli ufficiali e agenti di polizia giudiziaria appartenenti al Corpo delle capitanerie di porto[7]. Per i dati "*particolarmente riservati, che attengono alla lotta contro la criminalità comune ed organizzata nonché alla lotta contro il terrorismo e l'eversione*" (art. 3, co. 1, lett. b), D.P.R. 378/82) l'accesso, come previsto dall'art. 9, co. 2, può essere limitato ai soli capi degli uffici o ai responsabili di servizi o reparti operativi, all'uopo delegati, muniti di particolari chiavi di accesso. Da ultimo,

5 Es. funzionari preposti alla direzione degli uffici centrali e funzionari della Polizia di Stato, dirigenti dei servizi di sicurezza, ufficiali di polizia giudiziaria etc.
6 Cfr. Art. 10*bis*, D.P.R. n. 378 del 3 maggio 1982
7 Cfr. Art. 8*bis*, D.L. n. 92 del 23 maggio 2008

ai dati del CED può accedere, nei limiti e nei modi stabiliti dal D.P.R. in argomento, l'autorità giudiziaria avanti alla quale è pendente un procedimento, previa esibizione di apposita attestazione circa l'attinenza della richiesta al procedimento stesso.

È fondamentale in particolare rilevare che ai sensi del combinato disposto dell'art. 13 del D.P.R. 378/1982 e dell'art. 21, co. 2, della L. 128/2001 gli operatori tecnici addetti al CED devono:

- essere muniti di apposito nulla osta di segretezza;

- osservare le norme di sicurezza (da stabilirsi dalla commissione tecnica).

Inoltre, coloro che originano l'atto, provvedono all'inserimento o vi hanno avuto accesso devono essere identificati con sicurezza e tracciati, anche facendo ricorso a firma digitale e chiavi biometriche.

A ben vedere, queste misure di sicurezza disegnano il perimetro di un'area ben protetta verso l'esterno e fortemente strutturata al proprio interno, che tuttavia non si pone di per sé in termini incompatibili con l'esternalizzazione della mera operazione di archiviazione delle informazioni su *cloud*, tenuto conto del fatto che in effetti nessuna operazione di accesso ai dati o di immissione di dati sarebbe effettuata da personale del *cloud provider*. Anche l'accesso ai dati avverrebbe solo all'interno della già detta area protetta, richiamando i dati dal *cloud* attraverso i terminali di consultazione. Del resto, il legislatore non ha disposto limitazioni in merito alla collocazione fisica di risorse di archiviazione. Volendo cercare una rappresentazione plastica e assai schematica, si può immaginare appunto che da quest'area protetta fuoriesca un lungo cavo, ugualmente protetto, collegato con un imponente *hard disk* esterno (il *cloud*). È appena il caso di dire che si tratta di un'immagine soltanto simbolica ed esemplificativa, che parrà inaccettabile

al tecnico informatico, tuttavia essa aiuta a inquadrare con la necessaria astrazione l'architettura che verrebbe disegnata e le ragioni di compatibilità del servizio di archiviazione, che funge da risorsa esterna, di mera archiviazione, rispetto a una "bolla" chiusa e particolarmente presidiata.

Va aggiunto che, naturalmente, è altamente opportuno, se non proprio indispensabile, che i dati viaggino già cifrati dal terminale del CED, o da altro sistema ICT di polizia, al *data center* del *cloud provider*. Infatti, l'elevato livello di sicurezza impostato dal legislatore per quella che si è definita l'"area protetta" non può essere inficiato da un livello inadeguato di sicurezza nella trasmissione da *client* a *server*. Considerata sia la tipologia dei dati trattati sia il loro valore strategico, è anche chiaro che la cifratura adottata dovrà essere particolarmente robusta e attestarsi al più elevato livello consentito dallo stato dell'arte tecnologico.

5. Informatizzazione della pubblica amministrazione

Chiarito in definitiva che non si ravvisano nella normativa primaria ragioni ostative all'esternalizzazione della memorizzazione su *cloud* dei filmati girati con microcamere indossabili, occorre aggiungere che in linea generale la scelta di soluzioni *cloud*, anche qualora questa importi trasferimento di dati oltre l'area UE/SEE, non si scontra con la normativa amministrativistica, sempre che le videocamere siano utilizzate esclusivamente per la funzione di ordine e sicurezza pubblica (ossia con l'esclusione per esempio delle funzioni connesse con la polizia giudiziaria). Infatti, il principale corpo normativo applicabile e la relativa normativa secondaria di applicazione, vale a dire il

d.lgs. 7 marzo 2005, n. 82 (cd. "codice dell'amministrazione digitale" o "CAD") non si applica alla predetta funzione, ai sensi dell'art. 2, co. 6[8].

Tuttavia, benché il CAD a rigore non trovi applicazione, vale comunque la pena di menzionarne l'art. 68, co. 1, lett. d), che indica quelli che possono intendersi come criteri generali e utili guide per la Pubblica Amministrazione. In senso generale, infatti, le Pubbliche Amministrazioni possono scegliere di dotarsi di una soluzione *cloud* e dovrebbero anzi optare per la stessa quando essa si mostri, per caratteristiche di sicurezza e per risparmio di costi, competitiva rispetto a soluzioni più tradizionali. La scelta, effettuata nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, deve essere operata tenendo conto di una serie di elementi:

- costo complessivo del programma o soluzione;

- valutazione dei costi di acquisto, implementazione, mantenimento e supporto;

- livello di utilizzo nella soluzione scelta di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione;

- garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio, tenuto conto della tipologia di software acquisito.

Va aggiunto quantomeno anche il puntuale rispetto delle prescrizioni in materia di continuità operativa e *disaster recovery*, essenziali in ambito

8 Qualsiasi applicazione delle microcamere che vada oltre alla funzione di ordine e sicurezza pubblica si colloca oltre il perimetro del presente paper e importa l'applicazione di leggi e normativa secondaria differente (cfr. per es. D.P.C.M., 3 dicembre 2013), che può condurre a conclusioni affatto diverse.

amministrativo ma ugualmente fondamentali anche in materia di sicurezza ai sensi del codice privacy.

Non è questa la sede per un'analisi granulare in materia amministrativistica, può semplicemente dirsi che soluzioni *cloud*, per le loro caratteristiche di economicità, scalabilità, traduzione dei costi fissi in servizi, allocazione a un terzo (il cloud provider) di una serie di attività (manutenzione, rinnovo parco macchine, attuazione di misure di sicurezza, ecc.) costituiscono una scelta certamente compatibile, quantomeno in astratto, con le esigenze sopra esposte.

6. Il trasferimento di dati in area extra UE/SEE non adeguata alla luce del codice privacy

Annodando pertanto i fili dell'analisi fin qui sviluppata, può dirsi che l'archiviazione *in cloud* di materiale filmato per finalità di polizia non trovi impedimenti evidenti nella normazione primaria. Si tratta di un passaggio chiave anche in materia di protezione dei dati personali, posto che requisito fondamentale del trattamento lecito è che appunto esso non contrasti con la normativa in essere, come espressamente prevede l'art. 11, co. 1, lett. a) cod. priv.. Ciò posto, va dato atto che la disciplina di parte speciale del codice privacy in materia di trattamenti per finalità di polizia registra una serie di deroghe a norme di parte generale. In particolare, ai sensi dell'art. 53, sono derogati gli articoli: 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi 1-5, e artt. 39-45 e 145[9]-151. Ai fini che qui strettamente interessano, è dunque esclusa l'applicabilità degli artt. 42-45 relativi al trasferimento di dati all'esterno

9 Da notare che, senza deroga delle disposizioni richiamate, i diritti dell'interessato ricevono espressa tutela anche ai sensi dell'art. 10, commi 3-5 L. 121/81. Il comma 4 fissa a 30 giorni il riscontro all'interessato, ancorché non possa parlarsi propriamente di "interpello preventivo", non essendo previsto lo specifico strumento del ricorso al Garante.

dell'area UE/SEE verso paesi con inadeguata protezione dei dati personali. Nulla osta pertanto alla collocazione del *cloud* anche in paesi siffatti, pure in assenza dell'adozione delle condizioni che in linea generale renderebbero lecito il trasferimento, come l'utilizzo delle *standard contractual clause*. Va osservato comunque che la *ratio* di tale deroga sembra verosimilmente da cercarsi nell'esigenza di rendere leciti flussi di dati per ragioni di collaborazione tra Stati in materia di polizia, e che dunque piegarla alla diversa esigenza di utilità di archiviazione dei dati è scelta che non va esente da perplessità, anche in termini di abuso del diritto. Più ragionevole appare allora cercare una soluzione *cloud* che almeno tendenzialmente mantenga all'interno dell'area UE/SEE l'archiviazione e solo in via eccezionale preveda l'utilizzo anche di server stranieri, che andrebbero preferibilmente collocati comunque in paesi con i quali l'Italia ha rapporti di collaborazione e di fiducia. Non va infatti dimenticato che uno dei punti di attenzione da osservare quando si adotta una soluzione *cloud* (qualsiasi soluzione, il discorso è in termini generali) è la possibilità di accesso d'imperio alle informazioni archiviate da parte delle autorità nazionali del paese sul cui territorio insiste il data center o da quelle alla cui sovranità è sottoposto il fornitore di tecnologia *cloud*, anche a prescindere da trattati bilaterali o multilaterali. È evenienza che si è già verificata del resto[10]. Questo profilo dovrebbe essere oggetto di esame congiunto tra il committente e il fornitore di tecnologia *cloud*. L'adozione di misure di sicurezza come l'utilizzo di tecniche crittografiche che riflettano il migliore stato dell'arte rappresenta una scelta che mitiga il rischio, non dell'acquisizione ma quantomeno della lettura in chiaro.

10 Nel caso di richieste al titolare del trattamento fondate in diritto, ad esempio su accordi multilaterali o bilaterali, invece *nulla quaestio*: la localizzazione dei server è evidentemente irrilevante.

7. Ulteriori considerazioni in materia di codice privacy

Sembra opportuno sviluppare due rapide considerazioni per completare, sia pure nei termini molto sintetici del presente lavoro, lo sguardo d'insieme in materia di applicazione del codice privacy.

La prima riguarda il fatto che ai sensi delle deroghe già dette non è dovuta informativa all'interessato per trattamenti di polizia. L'interessato tuttavia vede intatti i suoi diritti, fatta eccezione per alcune modalità del loro esercizio e per lo specifico strumento del ricorso al Garante. Coerenza normativa richiede allora che l'interessato sia comunque informato circa l'identificazione del titolare e del responsabile del trattamento e sulle modalità concrete per l'accesso alle informazioni che lo riguardano, entro i limiti consentiti, relative ai filmati registrati attraverso microcamere indossabili, conformemente a quanto già ora avviene per l'accesso ai dati del CED.

L'altro punto riguarda, con stretta aderenza al tema del trattamento attraverso microcamere, l'applicazione dei principi privacy. In particolare, corre l'obbligo di notare che la posizione espressa dall'Autorità Garante nel già citato provvedimento proprio in tema di microcamere non persuade completamente, laddove autorizza, a parere dello scrivente Istituto, una frammentazione eccessiva e, soprattutto, soggettiva del girato, ossia effettuata sulla base di scelte del tutto unilaterali di attivazione/interruzione da parte delle forze di polizia in campo. Il pregio dello strumento di videoregistrazione risiede invece proprio nella terzietà della cifratura, nella neutralità e nella continuità del girato, che è anche garanzia di obiettività

dello stesso. Diversamente, si corre il rischio di limitare il girato a singoli episodi la cui raccolta viene decisa da soggetti che sono immersi nel loro stesso flusso, i quali episodi, svincolati dalla concatenazione di cause che li hanno preceduti e di effetti che hanno prodotto, giovano assai poco alla congruenza narrativa e alla corretta contestualizzazione. In definitiva, utilizzando un'efficace espressione inglese, pare assolutamente auspicabile evitare una sorta di *"cherry-picking„* di fatti salienti selezionati entro un *continuum* di azioni, che costituirebbe il modo meno congruo, ad avviso di chi scrive, per realizzare le finalità del trattamento e potrebbe addirittura finire per pregiudicare o per sporcare il complessivo valore probatorio (per eccessiva "vicinanza della prova", alterabile), creando peraltro conflitto con principi costituzionali e tutele fondamentali europee.

Dunque, se da un lato, occorre limitare, per ragioni di proporzionalità e minimizzazione, la registrazione di immagini a situazioni che la rendano strettamente necessaria, dall'altro, una volta decisa la registrazione, questa non dovrebbe essere interrotta e ripresa arbitrariamente. Sistemi di microcamere che limitino la gestione discrezionale del dispositivo, garantendo una continuità di registrazione e la sua conservazione cifrata, per un certo tempo, una volta attivate le microcamere appaiono allora preferibili.

8. Allocazione dei ruoli attivi di trattamento e disciplina contrattuale

A questo punto dell'analisi, non emergendo contrasto normativo in merito all'utilizzo di tecnologia *cloud* per la memorizzazione dei filmati registrati per finalità di polizia, anche ricorrendo a *cloud* pubblico con trasferimento dei dati extra UE/SEE verso paesi inadeguati (pur con le cautele già dette),

restano solo da considerare gli aspetti più squisitamente applicativi e in particolare quello dell'allocazione dei ruoli e delle sue conseguenze.

Nessun dubbio che il fornitore di servizi *cloud* sia responsabile del trattamento. A partire dall'opinione 5/2012 del Gruppo di lavoro dei garanti europei (di seguito "WP29"), ciò costituisce ormai posizione consolidata. L'allocazione del ruolo di titolare del trattamento appare invece più complessa. In un provvedimento del Garante in materia di dispositivo tradizionale di videosorveglianza, la titolarità è stata individuata in capo alla locale Questura e non in capo al Ministero dell'Interno[11]. Lo schema di ragionamento appare astrattamente applicabile per analogia al trattamento mediante microcamere indossabili, che potrebbe condurre all'individuazione come titolari dei singoli comandi delle forze dell'ordine che fanno uso delle stesse. Non è tuttavia da escludere una situazione di contitolarità tra i comandi e il Ministero dell'Interno, a seconda di come si articolerà concretamente il potere decisorio sull'uso degli strumenti.

Per quanto riguarda il trattamento di dati personali presso il CED interforze, premesso comunque che quest'ultimo non sembra essere, in base a quanto già notato, lo snodo privilegiato a cui collegare il *cloud* (sebbene una tale possibilità non debba essere esclusa per ragioni pratiche di funzionalità della rete), l'allocazione dei ruoli attivi di trattamento non è del tutto chiara. Per legge, ai sensi dell'art. 10, co. 3 L. 121/81, i diritti dell'interessato, concernenti il trattamento svolto dal CED, vanno esercitati nei confronti della Direzione centrale della polizia criminale presso il Dipartimento della pubblica sicurezza del Ministero dell'Interno. Non è chiaro tuttavia, non essendo rinvenibile informativa in tal senso[12], se la Direzione centrale predetta rivesta il ruolo di responsabile per il riscontro all'interessato o quello

11 GPDP, 27 giugno 2013, doc. web. n. 1065136.
12 Ciò come notato è conforme all'esonero ai sensi dell'art. 53, co. 1, lett. a).

di titolare del trattamento. Ugualmente, non può essere esclusa una situazione di contitolarità tra la Direzione e il Ministero o, addirittura, tra questi ultimi e i comandi delle forze dell'ordine che fanno uso dei sistemi di microcamere. Del resto, il Garante già in una delle sue primissime decisioni ha ammesso la configurabilità di situazioni di titolarità congiunta tra Ministeri e Direzioni[13]. Ne segue la necessità di un approfondimento granulare, non ulteriormente sviluppabile in questa sede, condotto, auspicabilmente, in collaborazione con l'Autorità Garante (sul punto potrebbe essere utilizzato lo strumento del parere), volto appunto a identificare con precisione la titolarità del trattamento.

9. Conseguenze contrattuali dell'allocazione dei ruoli

Inquadrato comunque il fornitore di *cloud* nel ruolo di responsabile del trattamento, punto che non genera perplessità, discendono specifiche conseguenze che investono il rapporto contrattuale con il titolare (sia esso il Ministero o altro soggetto, anche eventualmente in situazione di contitolarità), espressamente individuate nella citata opinione WP29 n. 5/2012.

Va chiarito che, ancorché il WP29 sia un mero organismo consultivo, le prescrizioni ivi indicate hanno rilevanza, specialmente ove esse si risolvano in violazioni del principio di finalità (cfr. p. es. ivi pp. 14, 20), dal momento

13 GPDP, 9 dicembre 1997, doc. web. n. 39785: *"… Il Garante ha… precisato che gli enti, le persone giuridiche e le pubbliche amministrazioni articolate in direzioni generali o in sedi centrali, decentrate o periferiche (ad esempio, servizi, dipartimenti, aree anche geografiche, ecc.), sono 'titolari' nel loro complesso dei trattamenti. Tuttavia, se la singola direzione generale o area esercita, tramite i propri organi, un potere decisionale reale e del tutto autonomo sulle finalità e sulle modalità dei trattamenti effettuati nel proprio ambito, non condizionato da scelte effettuate a livello centrale o di vertice, la medesima direzione o area potrebbe essere considerata come titolare dei trattamenti (ovvero, a seconda dei casi, come contitolare, assieme al Ministero)".* Il provvedimento ha poi trovato conferma e applicazione generale in GPDP, 14 giugno 2007, doc. web n. 1417809, § 3.1. Cfr. comunque GPDP, 14 febbraio 2002, doc. web. n. 1063684, nel quale, sia pure in relazione alla specifica fattispecie ivi trattata, il titolare è individuato nel Ministero dell'Interno, mentre il Dipartimento di pubblica sicurezza ricopre il ruolo di responsabile.

che potrebbero avere l'effetto di modificare l'allocazione dei ruoli, facendo fuoriuscire il fornitore di *cloud* dal ruolo di responsabile e collocandolo piuttosto in quello di titolare (congiunto) del trattamento. Ciò avrebbe conseguenze di rilievo e si porrebbe verosimilmente in contrasto sia con le disposizioni di rango primario in precedenza richiamate in relazione al CED interforze (ovviamente nei limiti in cui siano applicabili) sia comunque in relazione ai principi sanciti in Costituzione e nella Carta dei diritti fondamentali dell'Unione Europea. Determinerebbe in ogni caso attriti, non facilmente risolvibili, con le disposizioni del codice privacy. In definitiva: collocato, come deve essere, il *cloud provider* nel ruolo di responsabile, occorre farne discendere le conseguenze contrattuali previste assai puntualmente dal WP29.

Si tratta, con estrema concisione, delle seguenti. Il fornitore di *cloud* deve:

1. accettare di rispettare i principi del d.lgs. 196/03 e della Direttiva 95/46/CE (in futuro, del Regolamento Generale sulla Protezione dei Dati UE, per quanto applicabili, e della Direttiva Data Protection per attività giudiziaria e di polizia) e i diritti degli interessati, cfr. p. 20 opinione *cit.* (di seguito ogni riferimento si intende fatto ad essa), indicando altresì con chiarezza quali sono le misure di sicurezza rispettate, cfr. p. 12, n. 2 e pp. 20, 22. Fondamentale, tra le misure, l'isolamento dei dati personali da altri dati, cfr. p. 15, n. 3.4.3.5.. Va specificato che è corretto ritenere, in via prudenziale, che il responsabile del trattamento assicuri l'osservanza sia delle misure di sicurezza previste nel codice privacy, segnatamente di quelle elencate all'Allegato B del medesimo, sia di quelle determinate dal luogo di stabilimento del responsabile in base al disposto dell'art. 17(3) Dir. 95/46/CE. Il coordinamento di questa disposizione con la normativa italiana non è stato infatti mai oggetto di definitivo chiarimento. Giova comunque

considerare che le misure di sicurezza necessarie previste dall'ordinamento italiano sono del tutto ordinarie e, in linea generale, tecnologicamente banali;

2. assicurare trasparenza sui propri subfornitori, individuandoli e indicandone la collocazione geografica e le misure di protezione assicurate, e garantendo al titolare diritto di opposizione relativamente a singoli subfornitori, cfr. p. 20. Il consenso iniziale ai subfornitori specificati dal responsabile potrà invece anche essere dato in via generale all'inizio del rapporto;

3. allo stesso modo, per ragioni di trasparenza, indicare la localizzazione geografica dei data center che possono trattare i dati, cfr. p. 12, n. 9.

4. stipulare un contratto con i subfornitori che vincoli questi ultimi alle medesime obbligazioni verso il titolare del trattamento applicate al fornitore di cloud, cfr. p. 20;

5. assicurare rispetto, anche per ciò che riguarda la filiera dei subfornitori, del principio di finalità. Inoltre, il fornitore di servizi *cloud* deve assicurare vigilanza sui propri dipendenti e collaboratori e che essi siano vincolati da obblighi di riservatezza, cfr. p. 13, n. 7. A tal fine dovrebbe essere prevista una tracciatura delle operazioni, estesa anche alla filiera, cfr. p. 13, n. 12;

6. una volta che i dati debbano essere per qualsiasi ragione cancellati, assicurare, anche in relazione a tutta la filiera, l'adozione di strumenti di cancellazione sicura e completa dei dati, cfr. p. 12, n. 3 e p. 20;

7. prevedere chiari SLA (Service Level Agreement) e PLA (Privacy Level Agreement)[14]. Questi, oltre a essere indicati dal WP29, op. cit. p. 12, n. 1 e p. 21, sono richiesti anche dalla normativa amministrativistica, per lo meno

14 Nella valutazione degli SLA è fondamentale comprendere quali sono gli *effettivi* elementi presi in considerazione, in maniera da comprendere il reale significato delle percentuali di servizio garantite dal fornitore di tecnologia cloud. Comprenderle esattamente non è infatti sempre immediato.

in riferimento ai fondamentali principi di continuità operativa (CO) e *disaster recovery* (DR) e quindi analogicamente, pur non imperativamente, applicabili anche ai trattamenti di pubblica sicurezza. Inoltre, SLA e PLA costituiscono strumento oggettivo per un confronto tra varie offerte *cloud*. Permettono infine di determinare con precisione l'eventuale inadempimento del fornitore di soluzioni *cloud*;

8. accettare penali contrattuali, cfr. p. 12, n. 1 e p. 21;

9. consentire l'accesso ai dati soltanto al titolare o su autorizzazione di questi. Per l'effetto, il fornitore di servizi *cloud* dovrebbe impegnarsi contrattualmente, anche rispetto alla propria filiera, ad informare preventivamente il titolare, nei limiti in cui ciò non sia normativamente consentito, di eventuali richieste di accesso formulate da parte di autorità statali terze, incluse autorità di polizia e di sicurezza nazionale (cd. LEA, Law Enforcement Authority), impegnandosi altresì ad attendere la decisione del titolare del trattamento e a opporsi nel frattempo alla richiesta dell'Autorità terza, cfr. specificamente p. 13, n. 13 e pp. 21, 23;

10. informare il titolare di ogni violazione della sicurezza dei dati (*data breach*), cfr. p. 13, n. 8 e p. 21. Ciò va fatto entro un tempo definito e descrivendo essenzialmente l'evento, le misure di contratto adottate e la stima della compromissione determinatasi;

11. assicurare la cooperazione con il titolare, in particolar modo relativamente alla gestione della propria filiera e all'esercizio dei diritti degli interessati, cfr. p. 13, n. 10 e p. 20;

12. garantire un *audit* di terze parti indipendenti sul servizio *cloud* e la tracciatura delle operazioni sui dati, fermo restando che sono esclusi accessi

da parte del personale del fornitore di tecnologia *cloud*, della sua filiera e di terzi sui dati conferiti in cloud, cfr. p. 21[15];

13. il fornitore del *cloud* dovrebbe inoltre garantire la portabilità dei dati, cfr. p. 16, n. 3.4.3.6[16]. Il requisito della portabilità si connette in modo stretto anche con quello dell'interoperabilità;

14. dovrebbe altresì dotarsi di certificazioni internazionalmente riconosciute e reputate. Peraltro, nell'ottica della prossima entrata in vigore del Regolamento europeo in materia di protezione dei dati personali, tale aspetto è destinato ad avere sempre maggiore rilievo. Cfr. anche p. 14, n. 14;

15. è raccomandabile l'adozione da parte del fornitore di misure di potenziamento della privacy. Queste ultime del resto sono assimilabili alle misure idonee di protezione, dunque sono dovute. A pag. 22 dell'opinione citata è richiamata, fra le altre, l'importanza della cifratura. Questa dovrebbe essere, nel caso di specie, effettuata già all'origine dal titolare verso il responsabile;

16. il fornitore di tecnologia *cloud* deve infine portare preventivamente a conoscenza del titolare eventuali modifiche rilevanti del servizio, cfr. p. 13,

15 Si evidenzia infine la connessione tra il tema dell'audit e quello dell'*accountability* (cfr. p. 16, n. 3.4.4.7) e in definitiva il collegamento con la necessaria predisposizione di un sistema di tracciatura.

16 La portabilità è strettamente connessa al concetto del mantenimento del controllo da parte del titolare sui dati personali che conferisce nel cloud, dal momento che solo attraverso la garanzia della portabilità il titolare può essere veramente libero di gestire le vicende del proprio rapporto contrattuale con il cloud provider senza condizionamenti e limitazioni e dunque mantenendo un pieno potere decisionale rispetto ai dati conferiti. Gli aspetti relativi alla portabilità dei dati, compresi quelli che riguardano il formato aperto o proprietario della loro codifica vanno chiariti in sede contrattuale. Il tema della portabilità dei dati è strettamente legato a quello della possibilità di migrare verso diverso fornitore di tecnologia cloud in tempi rapidi e senza eccessive difficoltà: ciò riguarda sia l'assenza di vincoli tecnici di *vendor lock-in* sia l'assenza di vicoli giuridici. Su quest'ultimo punto va considerata l'eventuale disciplina del recesso contenuta nel contratto con il cloud provider. Corollario privacy della libertà di migrazione è la garanzia che i dati conferiti al cloud provider che viene abbandonato siano effettivamente cancellati da questi, con una tempistica certa e con metodi sicuri e che tale tempistica non impatti negativamente nella migrazione ad altro fornitore.

n. 11. Ai sensi del diritto italiano peraltro non è possibile la modifica unilaterale di una prestazione contrattuale stipulata tra le parti.

Non è invece necessario stipulare *standard model clause* per il trasferimento in area extra UE/SEE non adeguata o provvedersi di altri strumenti che assicurino la liceità del trasferimento, a mente della deroga già detta, cfr. art. 53, co. 2, lett. a) del codice privacy.

10. Ulteriori elementi contrattuali di attenzione

L'elencazione precedente discende dall'allocazione dei ruoli di trattamento. Pare tuttavia opportuno menzionare, sia pure molto concisamente, altri profili su cui è commendevole una disciplina contrattuale. Ragioni di spazio impediscono una trattazione estesa, ci si può limitare ai seguenti:

Legge applicabile, giurisdizione, notificazione

Ai sensi degli artt. 4(1)(a) Dir. 95/46/CE e 5.1 cod. priv., la legge applicabile al trattamento è quella del titolare, dunque quella italiana. Tuttavia un conto è la legge applicabile al trattamento, altro la legge che disciplina il rapporto contrattuale tra titolare e responsabile. È opportuno a tal fine specificare l'applicazione della legge italiana.

È altresì opportuno specificare anche la giurisdizione applicabile in via esclusiva, individuandola in quella del giudice italiano. Ne discenderà comunque la competenza territoriale nazionale ai sensi dell'art. 25 c.p.c.

È opportuno che le parti definiscano un indirizzo in Italia per la notificazione di atti al responsabile, nella persona di un procuratore o di un institore ai sensi dell'art. 77 c.p.c., al fine di evitare la complessità, l'onerosità e la lunga tempistica delle notificazioni all'estero.

Dovrebbe essere altresì prevista come lingua che le parti usano per le reciproche comunicazioni e per gli atti giudiziari o amministrativi l'italiano, in modo da evitare i costi di traduzione.

Tali elementi possono costituire peraltro altrettante ragioni che spingono a preferire un dato fornitore *cloud* rispetto a un altro.

Solidità del cloud provider e coperture assicurative

Altra fondamentale cautela contrattuale consiste nel verificare la solidità economica del fornitore e comprendere quali sono le sue eventuali coperture assicurative

11. Conclusioni

Alla luce dell'analisi svolta, non si ravvisano ragioni ostative nella normativa primaria italiana per escludere il ricorso a soluzioni di archiviazione in *cloud* pubblico di dati personali raccolti per finalità di polizia, mentre eventuale normativa secondaria emanata dal Ministero dell'Interno, peraltro in parte di difficile reperibilità, non costituisce un limite rilevante, posto che il potenziale conflitto rispetto all'adozione di soluzioni *cloud* sarebbe comunque superato dallo stesso Ministero emanante.

La liceità in base alla normativa primaria vale anche nel caso di eventuale trasferimento del data center del fornitore *cloud* in area esterna allo spazio UE/SEE, pur, al limite, in mancanza di condizioni di adeguatezza, posto che esiste espressa deroga in tal senso all'art. 53, co. 1, lett. a) cod. priv.. Vanno tuttavia richiamate le precisazioni già fatte e non bisogna sottovalutare il rischio di accessi da parte dell'Autorità straniera extra-UE che esercita sovranità sul luogo in cui il data center è collocato o sul fornitore di servizi *cloud*.

È altresì opportuno notare che le deroghe previste per i trattamenti svolti per finalità di polizia all'art. 53 cod. priv. non comportano limitazioni dei principi del trattamento e delle principali garanzie dell'interessato, pur nel necessario bilanciamento con l'attività di protezione dell'ordine e della sicurezza pubblici.

Le considerazioni già svolte in materia di liceità della soluzione *cloud* rispetto alla normativa primaria vanno completate con il rilievo che nulla osta neppure in ambito amministrativo, nel caso si volesse considerare per analogia la normativa derivante dal Codice dell'Amministrazione Digitale. Le Amministrazioni devono anzi in generale valutare l'impiego di tecnologia *cloud* in concorrenza con soluzioni di esternalizzazione tradizionali, anche tenendo conto di una serie di specifiche di applicazione comune in ambito amministrativo (continuità operativa e disaster recovery, SLA, interoperabilità, ecc.). Del resto, non può tacersi che a livello europeo si assiste, almeno a far data dal 2012, a un'intensa iniziativa di promozione di tecnologie *cloud* in ogni settore, proprio in considerazione dei vantaggi in termini non solo di costi ma anche di solidità tecnologica e di sicurezza.

Va notato che le modalità concrete di collegamento del servizio in *cloud* con i sistemi informativi in essere presso le forze di polizia dovranno essere decise dal Ministero dell'Interno. È ipotizzabile, come già detto, che il *cloud* sia direttamente collegato ai comandi delle forze dell'ordine che faranno uso del sistema di microcamere indossabili, piuttosto che al CED. Sono tuttavia possibili soluzioni diverse, determinate anche da considerazioni di praticità nella gestione della rete. In generale, appare opportuno fare uso delle convenzioni-tipo su parere conforme del Garante previste espressamente dall'art. 54, co. 1 cod. priv.

È importante che sia correttamente allocata la titolarità del trattamento, in relazione alla possibilità di titolarità congiunte tra più forze o istituzioni di pubblica sicurezza. Si segnala anche l'opportunità che sia quindi pubblicata una nota di chiarimento, ad esempio sul sito del Ministero, che dichiari l'allocazione dei ruoli così determinata. Ciò infatti permetterebbe all'interessato l'esercizio corretto dei suoi diritti in relazione alle immagini registrate, posto che se esiste una deroga rispetto all'art. 13 cod. priv. nessuna deroga sostanziale è posta all'art. 7. Evidentemente, sul punto è necessario assicurare la compatibilità dell'esercizio dei diritti dell'interessato con lo svolgimento dell'attività di indagine. Il passaggio, di particolare complessità, andrebbe sviluppato in base a un'apposita consulenza giuridica e con il parere del Garante per la protezione dei dati personali.

Venendo da ultimo al profilo del rapporto contrattuale tra titolare del trattamento e fornitore del servizio *cloud*, si ribadisce l'esigenza di predisporre un articolato tessuto di regole di collaborazione e trasparenza, in armonia con le precisazioni del Gruppo di lavoro ex art. 29.

www.istitutoitalianoprivacy.it/it

info@istitutoitalianoprivacy.org