Esportazione forense e conservazione corretta dei tracciati delle *body cam*

L'esigenza di dotare gli operatori di polizia di un dispositivo indossabile di videosorveglianza, sorge dalla necessità di tutelare gli stessi agenti da situazioni di pericolo per l'incolumità propria e altrui, nonché per consentire un puntuale **accertamento di fatti di reato**.

È evidente quindi che, al fine di raggiungere tali scopi, non è sufficiente che una *body cam* effettui delle riprese eccellenti, al passo con la più evoluta tecnologia video. Piuttosto, è necessario che le registrazioni possano essere utilizzate in ambito forense e quindi utili a testimoniare l'accaduto.

Le videoriprese: prove e fonti di prova

Le riprese dei sistemi di videosorveglianza e, di conseguenza anche quelle realizzate con *body cam*, in ambito giudiziario generalmente rientrano tra le **prove documentali**. Disciplinate dall'articolo 234 c.p.p., consistono nell'acquisizione da parte del giudice di "*scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia o qualsiasi altro mezzo*". Nulla di diverso, rispetto a ciò che rappresentano i filmati di telecamere, comprese quelle indossabili.

> ***Art. 234 c.p.p.***
> ***Prova documentale***
>
> 1. *E' consentita 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.*
> 2. *Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia.*
> 3. *E' vietata l'acquisizione di documenti che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti.*

Nell'attuale processo penale italiano, la prova si forma nella fase dibattimentale ed è assunta dal **Giudice** che decide se ammetterla o meno, quindi se utilizzarla per valutazione della verità processuale, oppure escluderla.

Diversamente, nella fase iniziale di un procedimento penale, quella delle **indagini preliminari**, salvo casi particolari, la polizia giudiziaria assume le **fonti di prova**. Proprio la polizia giudiziaria, di solito è l'organo che per primo viene in contatto con i filmati della videosorveglianza e, addirittura, indossando le *body cam*, spesso, è addirittura "autore" di registrazioni di interesse investigativo.

Come si è detto, l'acquisizione delle fonti di prova avviene nel primo *step* del procedimento e consentono poi al pubblico ministero di esercitare (eventualmente) l'azione penale, conducendo tali fonti dinanzi al giudice del dibattimento che determinerà se siano idonee

o meno ad essere assunte quale prova.

Il compito di assicurare le fonti di prova spetta innanzitutto alla polizia giudiziaria, che deve adoperarsi in tal senso e deve farlo, certo in modo tempestivo, ma soprattutto corretto, al fine di non inficiare il valore probatorio di tale elemento e di conseguenza la sua utilizzabilità in ambito forense.

Un aspetto fondamentale è la possibilità di garantire in qualsiasi momento la "**catena di custodia**", anche per le prove digitali. Lo stesso articolo 354 comma 2, c.p.p., al secondo periodo, prevede l'adozione di particolari misure tecniche finalizzate alla conservazione dei dati digitali. Non solo, anche tali da impedire l'alterazione e l'accesso abusivo, provvedendo altresì all'immediata duplicazione su adeguati supporti e con procedure che assicurino la conformità all'originale.

La **tracciabilità** delle operazioni svolte sulle fonti di prova e la garanzia di immodificabilità e corrispondenza all'originale, conferirà maggiori strumenti al giudice per valutare opportuna e corretta l'ammissione dei filmati quali prove documentali.

Certo, la mole di informazioni e dati digitali impiegati oggigiorno dalla polizia giudiziaria è ormai tale da costituire la quotidianità nell'attività investigativa. Anche per questo motivo, non è sempre possibile far scendere in campo i tecnici informatici o affidarsi a reparti specializzati. Tuttavia, è sempre possibile adottare semplici, ma funzionali accorgimenti.

L'articolo 55 c.p.p. usa l'imperativo "deve", escludendo il trattarsi di una mera facoltà e limitando la discrezionalità in capo alla polizia giudiziaria.

Il dato digitale originale: la funzione di *hash*

Come si è detto sin qui, per poter garantire la correttezza delle procedure svolte e rendere in qualsiasi momento conoscibili e tracciabili le operazioni svolte sulle riprese, è fondamentale essere in grado di dimostrare la genuinità del documento informatico.

Tra i metodi utilizzati in ambito forense, il sistema più rapido e semplice, almeno per le operazioni compiute al livello di attività di indagine da parte della polizia giudiziaria, è quello che consiste nel calcolo del codice o dell'**impronta di *hash***: si tratta di una stringa di lunghezza variabile, utilizzata in informatica forense e generalmente calcolata con gli algoritmi SHA1 – *Secure Hash Algoritm* (genera un codice di 160 bit) e MD5 – *Message Digest* (genera un codice di 128 bit).

Questa funzione matematica che, applicata ad un determinato documento informatico, attraverso particolari algoritmi, restituisce un codice identificativo univoco per quel *file*.
Dal codice generato è di fatto impossibile ricostruire il *file* da cui è stato originato, ma al contrario, qualsiasi modifica al documento originale – anche le più insignificanti – produrrà codici di *hash* differenti, evidenziando alterazioni, volontarie o meno, del *file* originale.

Download automatizzato vs. esportazione manuale

Come noto, sul mercato sono presenti differenti tecnologie di videosorveglianza indossabile: diversi dispositivi *body cam*, con differenti funzionalità e differenti modalità di gestione dei filmati.

I dispositivi meno evoluti, magari saranno dotati di sistemi di crittazione dei dati, ma richiederanno comunque un intervento umano al fine di eseguire il *download* delle registrazioni e di determinare la genuinità degli stessi, tracciando "manualmente" le operazioni di gestione degli stessi filmati.

Altri sistemi, si interfacciano con ***software* di gestione delle prove digitali**, capaci di svolgere in modo completamente automatizzato e certificato, ogni operazione sui documenti di interesse investigativo.

È il caso di "Reveal – DEMS 360": il *download* dei filmati registrati, avviene con la semplice allocazione della *body cam* nell'apposita *docking station* al termine del servizio. Con questa operazione, oltre a "dissociare" il dispositivo dall'operatore cui era stata assegnata, il *software* procede in modo totalmente autonomo alla memorizzazione dei filmati (su server, fisico o *in cloud*), liberando anche la memoria della *body cam*. Contestualmente alla memorizzazione del filmato, l'applicativo genera la relativa impronta di *hash*, che da quel momento identificherà il video originale. La conservazione avverrà secondo i parametri impostati di *default* ed ogni operazione svolta dagli utenti autorizzati, sarà tracciata dai *files di log*.

Il *software* citato, permette una completa gestione delle prove digitali, a partire dai filmati registrati dalle *body cam*, ma anche l'integrazione con ulteriori documenti di interesse investigativo, organizzandole in fascicoli digitali corrispondenti ai singoli "casi".

L'applicativo mette a disposizione degli operatori di polizia anche altre funzionalità che possono essere utili nell'attività di indagine: tra queste la possibilità di offuscare determinate aree del filmato, al fine di renderle disponibili senza violazione della *privacy*, ma anche possibilità di sviluppare il tracciato GPS del filmato, qualora la *body cam* supporti tale tecnologia.

È quindi palese quanto un *software* progettato per gestire in modo sicuro le registrazioni delle *body cam*, garantendo la **genuinità dei dati** in qualsiasi momento possa costituire uno strumento performante nell'organizzazione di un ufficio di polizia che voglia ottimizzare l'attività del personale, conseguendo al contempo la massima efficienza ed efficacia nell'attività investigativa.

Conclusione

Nell'individuare gli strumenti di lavoro da fornire al personale è sempre necessario effettuare scelte che tengano conto di tutti gli aspetti in gioco. Al di là delle prestazioni e delle funzionalità delle telecamere indossabili, è importante valutare attentamente anche le modalità con cui le *body cam* permettono di gestire le registrazioni. Il *software* con cui si interfacciano non è un aspetto secondario e, in ogni caso, è opportuno tenere conto delle esigenze di garanzia che la procedura penale richiede.

Una pessima gestione dei filmati, infatti, unita ad una valida strategia difensiva, porterà i difensori degli indagati a screditare il valore delle fonti di prova e le modalità di acquisizione da parte della polizia giudiziaria: la dimostrazione della tesi difensiva orientata a verificare che le procedure degli agenti siano tali da comportare rischi di alterazione e di inaffidabilità, porterebbe inevitabilmente il Giudice a maturare dubbi e quindi, potenzialmente, ad escludere il filmato dalle prove ammesse.

La migliore registrazione, da cui emergono in modo chiaro ed inequivocabile i fatti, è del tutto vana se non è utilizzabile in ambito forense.